POLITÉCNICA

UNIVERSIDAD POLITÉCNICA DE MADRID
ESCUELA TÉCNICA SUPERIOR DE
INGENIEROS INFORMÁTICOS

**“Madurez en la Identificación y Evaluación de
Riesgos en Ciberseguridad”**

Tesis Doctoral

Autor: Ángel Marcelo Rea Guamán
Master en Planificación y Dirección Estratégica

Director: Jose Antonio Calvo-Manzano Villalón
Doctor en Informática

2020

DEPARTAMENTO DE LENGUAJES Y SISTEMAS INFORMÁTICOS E INGENIERÍA DE SOFTWARE

ESCUELA TÉCNICA SUPERIOR DE INGENIEROS
INFORMÁTICOS

“Madurez en la Identificación y Evaluación de Riesgos en Ciberseguridad”

Tesis Doctoral

Autor: **Ángel Marcelo Rea Guamán**
Master en Planificación y Dirección Estratégica

Director: **Jose Antonio Calvo-Manzano Villalón**
Doctor en Informática

2020

Dedicatoria y agradecimientos

***“Para el logro del triunfo siempre ha sido
indispensable pasar por la senda de los sacrificios”***

[Simón Bolívar]

Al que ya no está aquí, pero sí en mi corazón y constantemente en mi mente. Mi padre, del que aprendí “a superar los obstáculos” por más incansables que parezcan. A mi madre, quien piensa que el trabajo continuo trae frutos, por estar pendiente de mí y de mi familia. A ambos, gracias, por hacerme partícipe de su proyecto de vida.

A mi familia, porque son mi gran sustento y mis compañeros de aventuras, que han sobrellevado durante todo este tiempo con mucha firmeza el estar lejos de familiares y amigos. Especialmente a **Lupita, “mi esposa”**, compañera de vida incansable en su apoyo con amor y cariño para todas las batallas más importantes. A mis hijos Daky y Samy por haberme acompañado tan lejos de nuestro hogar, por su apoyo, amor y cariño constante.

A mi hermana Ligia Elena por hacerme sentir siempre cerca de casa.

Y, por supuesto, a:

A mi director de tesis, Jose Antonio, por su ánimo, derroche de paciencia, dedicación y permitirme trabajar contigo. Gracias por todas tus aportaciones, consejos y sugerencias que me han ayudado a concluir esta tesis.

A Gonzalo y a Tomás, por sus ideas, sus experiencias compartidas, sus aportaciones, y su dedicación.

A todos los que, de las formas más insospechadas y en los momentos más difíciles, me han apoyado incondicionalmente.

Finalmente, a todo el equipo de la de la Subdirección Nacional de Seguridad Informática del IESS, por facilitarme la participación en el levantamiento de los riesgos de las plataformas administradas por ellos.

Resumen

Ciberseguridad es un término ampliamente utilizado que habla de la seguridad de los sistemas de información y los datos, y se define como la “protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados”. Por lo tanto, es una disciplina que involucra tecnología, personas, información y procesos para permitir operaciones seguras.

Una forma de comenzar a abordar la ciberseguridad es analizar la situación en que se encuentra la organización, a través de la implantación de modelos de madurez relativos a ciberseguridad. Las etapas de madurez van desde una etapa inicial, donde una organización apenas haya comenzado a considerar la ciberseguridad, hasta un escenario dinámico, donde una organización es capaz de adaptarse rápidamente a los cambios en el panorama de la seguridad cibernética en lo relativo a las amenazas, las vulnerabilidades, los riesgos, la estrategia económica o el cambio de las necesidades organizacionales.

Existen una serie de modelos de madurez que utiliza la industria para medir el nivel de una organización. Los principales modelos que son utilizados en los estudios de artículos científicos, identifican a la gestión de riesgos de ciberseguridad como un elemento básico en el nivel inicial de madurez. Los elementos necesarios para gestión de riesgos se describen mediante modelos conceptuales, sin embargo, cada modelo lo hace según su enfoque particular.

Por todo lo anterior, esta tesis doctoral tiene un doble objetivo. En primer lugar, demostrar la necesidad de contar con un marco de trabajo de gestión de riesgos en ciberseguridad, en base de un modelo conceptual que incluya todos los elementos de la gestión de riesgos, sea sencillo de aplicar en distintos ámbitos, empresas de cualquier naturaleza, y que ayude a la organización en la identificación y evaluación de riesgos en ciberseguridad. En segundo lugar, cubrir esta necesidad, desarrollando un marco de trabajo que ofrezca un modelo de proceso genérico, aplicable sobre distintas áreas para la gestión de riesgos en ciberseguridad, que deba seguir una serie de actividades y tareas para que sea eficaz y cumpla adecuadamente su función.

El proceso del marco de trabajo propuesto para la identificación y evaluación de riesgos en ciberseguridad, AVARCIBER (Activos – Vulnerabilidades – Amenazas – Riesgos CIBERseguridad), describe una serie de actividades y tareas secuenciales. Las actividades descritas son: definir un catálogo de los elementos que participan en el modelo conceptual, identificar y evaluar activos, evaluar el nivel de daño que van a producir las vulnerabilidades en cada uno de los activos, identificar las amenazas de ciberseguridad, medir el riesgo, e identificar contramedidas.

Para validar el marco de trabajo descrito anteriormente, se ha implementado un caso de estudio en el Instituto Ecuatoriano de Seguridad Social (IESS) de la ciudad de Quito – Ecuador. La identificación y evaluación de riesgos incluyó identificar y evaluar los eventos inciertos que puedan afectar los recursos de tecnología de la información. Una vez obtenida la línea base, se ha aplicado el marco de trabajo AVARCIBER. Esto ha permitido conocer las ventajas/desventajas y las posibles mejoras del marco de trabajo frente a la forma de trabajar actual (denominada línea base), por lo que podemos indicar que la identificación y evaluación de riesgos en ciberseguridad utilizando el modelo

conceptual AVARCIBER, ha permitido: tener una mejor visión de las relaciones que pueden tener los elementos de la gestión de riesgos en ciberseguridad, tomar decisiones en la criticidad de los riesgos e identificar acertadamente las contramedidas que se deben aplicar.

Abstract

Cybersecurity is a widely used term that talks about the security of information systems and data, and it is defined as the "protection of information assets, through the treatment of threats that put at risk the information that is processed, stored and transported by the information systems that are interconnected". Therefore, it is a discipline that involves technology, people, information and processes to allow safe operations.

One way to start addressing cybersecurity is to analyze the situation in which the organization finds itself, through the implementation of maturity models related to cybersecurity. The maturity stages range from an initial stage, where an organization has only just begun to consider cybersecurity, to a dynamic scenario, where an organization is able to quickly adapt to changes in the cyber security landscape regarding threats, vulnerabilities, risks, economic strategy, or changing organizational needs.

There are a series of maturity models that the industry uses to measure the level of an organization. The main models that are used in the studies of scientific articles, identify cybersecurity risk management as a basic element in the initial level of maturity. The elements necessary for risk management are described through conceptual models, however, each model does it according to its particular approach.

For all of the above, this doctoral thesis has a double objective. First, to demonstrate the need for a cybersecurity risk management framework, based on a conceptual model that includes all the elements of risk management, easy to apply in different areas, companies of any nature, and that helps the organization in the identification and evaluation of cybersecurity risks. Secondly, to cover this need, developing a framework that offers a generic process model, applicable in different areas for the identification and evaluation of risks in cybersecurity, which must follow a series of activities and tasks to be effective and comply properly its function.

The process of the proposed framework for the identification and evaluation of risks in cybersecurity, AVARCIBER (Assets - Vulnerabilities - Threats - Cybersecurity Risks), describes a series of sequential activities and tasks. The activities described are: defining a catalog of the elements that participate in the conceptual model, identifying and evaluating assets, evaluating the level of damage that vulnerabilities will produce in each of the assets, identifying cybersecurity threats, measuring risk, and identifying countermeasures.

To validate the framework described above, a case study has been implemented at the Ecuadorian Social Security Institute (IESS) in the city of Quito – Ecuador. The identification and evaluation of risks included, identifying and evaluating uncertain events that may affect the information technology resources. Once the baseline has been obtained, the AVARCIBER framework has been applied. This has allowed us to know the advantages / disadvantages and possible improvements of the framework compared to the current way of working (called baseline), so we can indicate that the identification and evaluation of risks in cybersecurity using the AVARCIBER conceptual model, has allowed: to have a better vision of the relationships that the elements of risk management in cybersecurity can have, to make decisions on the criticality of the risks, and to correctly identify the countermeasures that must be applied.

1 INDICE DE CONTENIDO

1	INTRODUCCIÓN	1
1.1	Contexto de la Ciberseguridad	1
1.2	Importancia de la Ciberseguridad	3
1.2.1	Las amenazas persistentes avanzadas	4
1.2.2	Las olas de malware	5
1.2.3	Los tipos de ciberatacantes	7
1.2.4	Los tipos de ciberataques	10
1.2.5	Marcos de Ciberseguridad	12
1.3	Objetivos del trabajo de investigación	14
1.4	Aproximación a la solución	15
1.5	Estructura de la tesis doctoral	15
2.	ESTADO DE LA CUESTIÓN.....	17
2.1.	Modelos de Madurez en Ciberseguridad.....	17
2.1.1.	RS de Modelos de Madurez en Ciberseguridad.....	17
2.1.2.	Los Modelos de Madurez en Ciberseguridad.....	23
2.1.3.	Estudio Comparativo Modelos de Madurez en ciberseguridad -CCMM.....	34
2.1.4.	Un Modelo de Madurez en Ciberseguridad	39
2.1.5.	Consideraciones Finales de Modelos de Madurez en Ciberseguridad	43
2.2.	Riesgos en Ciberseguridad.....	43
2.2.1.	Principales Conceptos de Riesgos en Ciberseguridad	44
2.2.2.	RS de Taxonomías de Riesgos en Ciberseguridad.....	49
2.2.3.	Modelo Conceptual de Riesgos en Ciberseguridad	54
2.2.4.	Consideraciones Finales de Riesgos en Ciberseguridad	57
2.3.	Otras Revisiones Sistemáticas.....	57
2.3.1.	RS de Taxonomías de Activos en Ciberseguridad.....	57
2.3.2.	RS de Taxonomías de Vulnerabilidades en Ciberseguridad	60
2.3.3.	RS de Taxonomías de Amenazas en Ciberseguridad.....	64
2.4.	Consideraciones Finales.....	67
3.	PLATEAMIENTO DEL PROBLEMA E HIPÓTESIS DEL TRABAJO	69
3.1.	Visión general del problema	69
3.2.	Aproximación a la solución.....	70
3.3.	Hipótesis del trabajo.....	71
4.	RESOLUCION DEL PROBLEMA	73
4.1.	Modelo Conceptual del Dominio	73

4.1.1. Elementos y relaciones en el modelo conceptual del dominio.....	74
4.2. Marco de trabajo para la Identificación y Evaluación de riesgos en Ciberseguridad.....	79
4.3. Prototipo del Modelo Conceptual	89
4.3.1. Actividad 1: Lanzamiento.....	89
4.3.2. Actividad 2: Identificar y evaluar Activos	91
4.3.3. Actividad 3: Evaluar el nivel de daño para las tuplas Vulnerabilidad – Activo (dimensión) 92	
4.3.4. Actividad 4: Identificación de Amenazas de Ciberseguridad	92
4.3.5. Actividad 5: Medición del Riesgo	94
4.3.6. Actividad 6: Contramedidas.....	95
4.3.7. Resumen del prototipo	95
4.3.8. Conclusiones	96
4.4. Aportaciones realizadas.....	96
5. EXPERIMENTACIÓN	99
5.1. Método de diseño de experimentos de ingeniería del software.....	99
5.2. Caso de estudio	100
5.3. Línea base inicial de los activos de la organización.....	101
5.3.1. Análisis de Riesgos de la Plataforma Host – IESS	106
5.3.2. Actividades del Marco de Trabajo AVARCIBER (Activos– Vulnerabilidades – Amenazas – Riesgos – CIBERseguridad)	145
5.3.3. Comparación resultados línea base inicial y marco de trabajo AVARCIBER (línea base final)	176
5.3.4. Conclusiones	177
5.4. Validación de las Hipótesis de Trabajo.....	178
5.5. Resumen del Capítulo 5	183
6. APORTACIONES, CONCLUSIONES Y LÍNEAS FUTURAS.....	185
6.1. Principales aportaciones.....	185
6.2. Conclusiones	186
6.3. Líneas futuras de investigación	187
7. BIBLIOGRAFÍA.....	189
ANEXOS	197
I. Procedimiento para realizar las revisiones sistemáticas.....	A-1
I.1. Introducción	A-1
I.2. Revisiones sistemáticas	A-1
I.2.1. Razones para realizar revisiones sistemáticas.....	A-1
I.2.2. La importancia de las revisiones sistemáticas.....	A-1
I.3. El proceso de revisión	A-2

I.3.1. La necesidad de una revisión sistemática.....	A-2
I.3.2. Desarrollo de un protocolo de revisión	A-2
I.3.3. Revisión	A-6
I.3.4. Analizar e interpretar los resultados.....	A-8
I.3.5. Informar la revisión.....	A-9
I.4. Observaciones finales.....	A-9
II. Procedimiento para realizar las revisiones sistemáticas	A-11
II.1. Introducción	A-11
II.2. Definición.....	A-11
II.3. Taxonomías descritas.	A-11
II.3.1. Tipos de Activos	A-11
II.3.2. Vulnerabilidades	A-12
II.3.3. Amenazas	A-16
II.4. Observaciones finales.....	A-18
III. Línea Base Inicial de Análisis de Riesgos de la Dirección Nacional de Tecnología de la Información - IESS	A-19
III.1. Introducción	A-19
III.2. Objetivo.....	A-19
III.3. Justificación	A-19
III.4. Alcance	A-20
III.5. Actividades realizadas.....	A-20
III.5.1. Valoración de los Activos	A-20
III.5.2. Valoración del Impacto	A-22
III.5.3. Valoración del Riesgo	A-22
III.6. Análisis de Riesgos de la Plataforma AS400 – IESS.....	A-23
III.6.1. Dependencias de activos	A-23
III.6.2. Identificación y valoración de activos.....	A-24
III.6.3. Identificación y valoración de las vulnerabilidades y amenazas.....	A-26
III.6.4. Gráfica de radar de los riesgos por activo	A-53
III.6.5. Controles o salvaguardas sugeridas	A-54
III.6.6. Conclusiones	A-59
III.7. Análisis de Riesgos de la Plataforma Host – IESS	A-60
III.7.1. Dependencias de activos	A-60
III.7.2. Identificación y valoración de activos.....	A-60
III.7.3. Identificación y valoración de las vulnerabilidades y amenazas.....	A-63
III.7.4. Gráfica de radar de los riesgos por activo	A-79

III.7.5. Controles o salvaguardas sugeridas	A-80
III.7.6. Conclusiones	A-80
III.8. Análisis y Gestión de Riesgos Plataforma Oracle – IESS	A-81
III.8.1. Dependencias de activos	A-81
III.8.2. Identificación y valoración de los activos	A-81
III.8.3. Identificación y valoración de las vulnerabilidades y amenazas.....	A-83
III.8.4. Gráfica de radar de los riesgos por activo	A-102
III.8.5. Controles o salvaguardas sugeridas	A-103
III.8.6. Conclusiones	A-105
III.9. Análisis de Riesgos Plataforma Firewall – IESS	A-105
III.9.1. Dependencias de activos	A-105
III.9.2. Identificación y valoración de activos.....	A-105
III.9.3. Identificación y valoración de vulnerabilidades y amenazas	A-106
III.9.4. Gráfica de radar de los riesgos por activo	A-115
III.9.5. Controles o salvaguardas sugeridas	A-115
III.9.6. Conclusiones	A-117
III.10. Resumen del Anexo III	A-117
IV. Línea base final de Identificación y Evaluación de Riesgos de la Dirección Nacional de Tecnología de la Información - IESS.....	A-119
IV.1. Introducción	A-119
IV.2. Objetivo.....	A-119
IV.3. Justificación	A-119
IV.4. Alcance	A-120
IV.5. Marco de trabajo para la Identificación y Evaluación de riesgos en Ciberseguridad AVARCIBER	A-120
IV.6. Análisis de Riesgos de la Plataforma AS400 – IESS.....	A-129
IV.6.1. Actividad 1: Lanzamiento.....	A-130
IV.6.2. Actividad 2: Identificar y evaluar Activos	A-130
IV.6.3. Actividad 3: Evaluar el nivel del daño para las tuplas Vulnerabilidad -Activo (dimensión)	A-132
IV.6.4. Actividad 4: Identificación de Amenazas de ciberseguridad	A-159
IV.6.5. Actividad 5: Medición del Riesgo	A-184
IV.6.6. Actividad 6: Contramedidas.....	A-184
IV.7. Análisis de Riesgos de la Plataforma Host – IESS	A-187
IV.7.1. Actividad 1: Lanzamiento	A-187
IV.7.2. Actividad 2: Identificar y evaluar Activos	A-188

IV.7.3. Actividad 3: Evaluar el nivel de daño para las tuplas Vulnerabilidad – Activo (dimensión)	A-188
IV.7.4. Actividad 4: Identificación de Amenazas de ciberseguridad	A-198
IV.7.5. Actividad 5: Medición del Riesgo	A-206
IV.7.6. Actividad 6: Contramedidas.....	A-207
IV.8. Análisis y Gestión de Riesgos Plataforma Oracle - IESS	A-209
IV.8.1. Actividad 1: Lanzamiento.....	A-209
IV.8.2. Actividad 2: Identificar y evaluar Activos	A-210
IV.8.3. Actividad 3: Evaluar el nivel de daño para las tuplas Vulnerabilidad – Activo (dimensión)	A-210
IV.8.4. Actividad 4: Identificación de Amenazas de ciberseguridad	A-216
IV.8.5. Actividad 5: Medición del Riesgo	A-220
IV.8.6. Actividad 6: Contramedidas.....	A-221
IV.9. Análisis de Riesgos de la plataforma Firewall - IESS	A-223
IV.9.1. Actividad 1: Lanzamiento.....	A-223
IV.9.2. Actividad 2: Identificar y evaluar Activos	A-224
IV.9.3. Actividad 3: Evaluar el nivel de daño para las tuplas Vulnerabilidad – Activo (dimensión)	A-224
IV.9.4. Actividad 4: Identificación de Amenazas de ciberseguridad	A-232
IV.9.5. Actividad 5: Medición del Riesgo	A-239
IV.9.6. Actividad 6: Contramedidas.....	A-239
IV.10. Resumen del Anexo IV	A-241

2 ÍNDICE DE FIGURAS

Figura 1-1 Costo del delito informático en 11 países (Fuente: Accenture and Ponemon Institute, 2019)	3
Figura 1-2 Muestras descubiertas en el repositorio AV-TEST de 2015 a 2019 (Fuente: AVTEST (IT-Security Institute), 2019)	7
Figura 1-3 Categorías de los ciberatacantes	7
Figura 1-4 Daños causados por las amenazas a la defensa cibernética	10
Figura 1-5 Marcos de Ciberseguridad (Fuente: (Donaldson et al., 2018))	13
Figura 2-1. Frecuencia del nombrado de los Modelos de Madurez en Ciberseguridad	21
Figura 2-2. Elementos de modelo y dominio del modelo de madurez C2M2 (Fuente: Department of Energy, 2019)	26
Figura 2-3. Enfoque recomendado para usar el modelo de madurez C2M2 (Fuente: Department of Energy, 2019)	27
Figura 2-4. Áreas del modelo de madurez de NICE (Fuente: US Department of Homeland Security, 2014).	28
Figura 2-5. Modelo de madurez CCSMM (Fuente: White, 2011)	34
Figura 2-6. Taxonomía para comparar entornos de mejora de procesos (Fuente: Halvorsen & Conradi, 2001).	36
Figura 2-7. Marco del modelo CMMC (vista jerárquica simplificada) (Fuente: US Department of Defense, 2019).	39
Figura 2-8. Niveles y descripciones de CMMC (Fuente: US Department of Defense, 2019).	40
Figura 2-9. Niveles de CMMC y enfoque asociado (Fuente: US Department of Defense, 2019)	40
Figura 2-10. Dominios CMMC (Fuente: US Department of Defense, 2019)	41
Figura 2-11. Proceso simplificado de gestión de riesgos	44
Figura 2-12. Proceso detallado de gestión de riesgos	46
Figura 2-13. Matriz de riesgo simplificado	47
Figura 2-14 Interacción entre los riesgos y los diferentes tipos de controles	47
Figura 2-15 Algunas características de los tipos de control	48
Figura 2-16. Modelo Conceptual de Riesgos de NIST (Fuente: Singh, 2014)	55
Figura 2-17. Entidades y Relaciones de Riesgos empresariales (Fuente: Singhal & Wijesekera, 2010)	55
Figura 2-18. Modelo de riesgos genérico con elementos clave de riesgo de NIST (Fuente: NIST, 2012)	56
Figura 2-19. Tipos de Información de Ciberseguridad (Fuente: Goodwin et al., 2015)	56
Figura 4-1. Relación Activo y Vulnerabilidad	75
Figura 4-2. Relación Activo, Vulnerabilidad y Dimensión_Valoración	76
Figura 4-3. Relación Activo, Vulnerabilidad y Dimensión_Valoración, Amenaza	78
Figura 4-4. Modelo conceptual de identificación y evaluación de riesgos	79

Figura 4-5. Diagrama de Flujo del Marco de Trabajo	80
Figura 4-6. Taxonomía de Tipos de Activos.....	90
Figura 4-7. Taxonomía de Vulnerabilidades.....	90
Figura 4-8. Taxonomía de Amenazas	91
Figura 4-9. Valoración del Impacto del Activo de la Organización	91
Figura 4-10. Valor y Costo del daño de la vulnerabilidad para la tupla Vulnerabilidad – Activo.....	92
Figura 4-11. Asignación de amenazas a las vulnerabilidades de ciberseguridad - activos	93
Figura 4-12. Dupla Amenaza – Vulnerabilidad con valor y el costo del daño de la vulnerabilidad.....	93
Figura 4-13. Amenazas de ciberseguridad con Valores del daño y Costo del daño de la Amenaza.....	94
Figura 4-14. Riesgo de las amenazas de ciberseguridad.....	95
Figura 4-15. Contramedidas a las vulnerabilidades identificadas.....	95
Figura 5-1. Características de los estudios de caso. (Fuente: Wohlin, Höst, & Henningsson, 2003) ...	99
Figura 5-2. Ejemplo de riesgo en función del impacto y la frecuencia.....	105
Figura 5-3. Diagrama de dependencia de equipos de la Plataforma Host-IESS	107
Figura 5-4 Mapa de calor “Main-Frame Z10BC”	131
Figura 5-5. Mapa de calor “Unidad de cartuchos”.....	132
Figura 5-6 Mapa de calor “Storage”	133
Figura 5-7 Mapa de calor “servidor HMC”	134
Figura 5-8 Mapa de calor “Aires de Precisión”	135
Figura 5-9 Mapa de calor “Aires tipo Mochila”	136
Figura 5-10 Mapa de calor “UPS”	138
Figura 5-11 Mapa de calor “servidor Unix Micros”	139
Figura 5-12 Mapa de calor “servidor vtape”.....	140
Figura 5-13 Mapa de calor “switch de paso”	141
Figura 5-14 Mapa de calor “aplicativos alojados en el sistema Host-IESS”	142
Figura 5-15 Reporte de riesgos plataforma Host – IESS por activo	143
Figura 5-16. Comparativa de elementos, asociaciones y resultados de línea base inicial y final (AVARCIBER).....	177
Figura 5-17. Relación entre los elementos del modelo conceptual AVARCIBER.....	179
Figura III-1. Ejemplo de riesgo en función del impacto y la frecuencia.....	A-23
Figura III-2. Diagrama de dependencia de equipos AS400 – IESS.....	A-24
Figura III-3. Reporte de riesgos plataforma AS400 – IESS.....	A-54
Figura III-4. Diagrama de dependencias de equipos Host	A-60
Figura III-5. Reporte de riesgos plataforma Host – IESS	A-79
Figura III-6 Diagrama de dependencia de equipos de la Plataforma Oracle – IESS	A-81
Figura III-7 Reporte de riesgos Plataforma Oracle – IESS.....	A-103

Figura III-8 Diagrama de dependencia de equipos con Firewall – IESS	A-105
Figura III-9 Reporte de riesgos Firewall – IESS.....	A-115
Figura IV-1. Diagrama de Flujo del Marco de Trabajo	A-120
Figura IV-2. Diagrama de dependencias de equipos AS400 – IESS	A-130
Figura IV-3. Matriz de riesgos AS400-IESS	A-184
Figura IV-4. Riesgos por amenazas AS400-IESS.....	A-187
Figura IV-5. Diagrama de dependencia de equipos de HOST – IESS.....	A-187
Figura IV-6. Matriz de riesgos Host-IESS	A-207
Figura IV-7. Riesgos por amenazas Host-IESS	A-209
Figura IV-8. Diagrama de dependencia de equipos de la Plataforma Oracle-IESS.....	A-209
Figura IV-9. Matriz de riesgos de la plataforma Oracle-IESS	A-221
Figura IV-10. Riesgos por amenazas de la plataforma Oracle.....	A-222
Figura IV-11. Topología de la red de conexión de equipos de la plataforma Firewall.....	A-223
Figura IV-12. Diagrama de dependencia de equipos de la plataforma Firewall-IESS	A-223
Figura IV-13. Matriz de riesgos de la plataforma Firewall-IESS	A-239
Figura IV-14. Reporte de riesgos plataforma firewall y equipos dependientes	A-241

3 ÍNDICE DE TABLAS

Tabla 1-1 Estructura de la Tesis Doctoral.....	15
Tabla 2-1. Criterios de inclusión y exclusión (RS Modelos de Madurez de Ciberseguridad – RS CCMM).....	18
Tabla 2-2. Distribución de los Estudios por Fuente (RS MMC).....	19
Tabla 2-3. Estudios clasificados en base a la categorización de Peterson (RS MMC)	19
Tabla 2-4. Modelos de Madurez en Ciberseguridad Identificados (RS CCMM)	20
Tabla 2-5. Niveles de madurez de SSE-CMM.....	31
Tabla 2-6. Niveles de madurez de CCSMM.....	33
Tabla 2-7. Comparación entre los modelos de madurez de la capacidad de ciberseguridad	38
Tabla 2-8. Capacidades CMMC.....	41
Tabla 2-9. Procesos CMMC	42
Tabla 2-10. Criterios de inclusión y exclusión (RS Riesgos de Ciberseguridad – RS RC)	49
Tabla 2-11. Distribución de estudios por fuente (RS RC)	50
Tabla 2-12. Estudios primarios (RS RC)	51
Tabla 2-13. Estudios primarios adicionales (RS RC)	51
Tabla 2-14. Resumen de taxonomías (RS TC)	52
Tabla 2-15. Criterios de inclusión y exclusión de estudios (RS Taxonomía de Activos de Ciberseguridad – RS TAct)	58
Tabla 2-16. Distribución de los estudios por fuente (RS TAct).....	59
Tabla 2-17. Taxonomías de activos en ciberseguridad	59
Tabla 2-18. Criterios de inclusión y exclusión de los estudios (RS Taxonomía de Vulnerabilidades de Ciberseguridad – RS TV).....	61
Tabla 2-19. Distribución de estudios por fuente (RS TV)	61
Tabla 2-20. Estudios primarios que presentan taxonomías de vulnerabilidades de ciberseguridad	62
Tabla 2-21. Criterios de Inclusión y exclusión de los estudios (RS Taxonomías de Amenazas de Ciberseguridad, RS TAm).....	64
Tabla 2-22. Distribución de estudios por fuente (RS TAm)	65
Tabla 2-23. Estudios primarios que presentan taxonomías de amenazas	66
Tabla 4-1. Relación entre entidades de Activos.....	75
Tabla 4-2. Relación de entidades de Vulnerabilidad	77
Tabla 4-3. Relación de entidades de Amenaza	78
Tabla 4-4. Relación de entidades de Incidente y Contramedida	79
Tabla 4-5. Activos y tipos de activos.....	81
Tabla 4-6. Valoración del impacto para un activo	81
Tabla 4-7. Criterios de valoración dimensiones de Seguridad.....	81
Tabla 4-8. Valoración del impacto del Activo	82

Tabla 4-9. Valoración del Costo del Activo	83
Tabla 4-10. Valoración del daño de las vulnerabilidades	83
Tabla 4-11. Tuplas Vulnerabilidad - Activo	83
Tabla 4-12. Valoración del daño de la vulnerabilidad	84
Tabla 4-13. Tuplas de vulnerabilidades – activos, con valor y costo del daño, y costo del activo de las vulnerabilidades.	85
Tabla 4-14. Tripletas Amenazas – Vulnerabilidades – Activos.....	85
Tabla 4-15. Tripletas Amenazas – Vulnerabilidades – Activo con los valores y costo del daño de las amenazas	86
Tabla 4-16. Duplas Amenazas – Vulnerabilidades con los valores y costo del daño de las vulnerabilidades	87
Tabla 4-17. Amenazas con valores totales de daño y costo del daño	87
Tabla 4-18. Probabilidad de ocurrencia de la amenaza.....	87
Tabla 4-19. Valoración del Riesgo	88
Tabla 4-20. Calculo del Riesgo.....	89
Tabla 5-1. Criterios de valoración Confidencialidad , Integridad, Disponibilidad y Criticidad	103
Tabla 5-2 Ejemplo de valoración de impacto	104
Tabla 5-3. Criterios de valoración frecuencia.....	104
Tabla 5-4 Ejemplo de valoración del riesgo	105
Tabla 5-5. Identificación de Activos de la Plataforma Host-IESS.....	107
Tabla 5-6. Valoración de activos en disponibilidad, integridad, confidencialidad y criticidad	108
Tabla 5-7. Identificación de vulnerabilidades y amenazas de ciberseguridad de cada activo	109
Tabla 5-8 Valoración de degradación e impacto.....	116
Tabla 5-9 Tabla resumen de valoración del riesgo	124
Tabla 5-10 Listado de riesgos de Main-FrameZ10BC.....	130
Tabla 5-11. Listado de riesgos de la Unidad de cartuchos.....	131
Tabla 5-12 Detalle de riesgos del Storage	132
Tabla 5-13 Detalle de riesgos del Servidor HMC.....	133
Tabla 5-14 Detalle de riesgos de Aires de Precisión.....	135
Tabla 5-15 Detalle de riesgos de Aires tipo Mochila.....	136
Tabla 5-16 Detalle de riesgos de equipo UPS.....	137
Tabla 5-17 Detalle de riesgos servidor Unix (Micros).....	138
Tabla 5-18 Detalle de riesgos servidor vtape.....	139
Tabla 5-19 Detalle de riesgos switch de paso	141
Tabla 5-20 Detalle de riesgos “aplicativos alojados en el sistema Host-IESS”	142
Tabla 5-21 Tabla de valores de Riesgos de plataforma Host - IESS por activo	143
Tabla 5-22. Contramedidas para la Plataforma Host - IESS.....	144

Tabla 5-23. Parámetros para medir las dimensiones de seguridad AVARCIBER.	146
Tabla 5-24. Parámetros para medir la criticidad en los activos de ciberseguridad AVARCIBER	147
Tabla 5-25. Parámetros para medir el impacto de degradación en los activos de ciberseguridad AVARCIBER	147
Tabla 5-26. Parámetros para medir la criticidad en los activos de ciberseguridad AVARCIBER	147
Tabla 5-27. Valoración del Riesgo AVARCIBER	148
Tabla 5-28. Tipos de activos de ciberseguridad AVARCIBER.....	148
Tabla 5-29. Vulnerabilidades de ciberseguridad.....	149
Tabla 5-30. Amenazas de Ciberseguridad	150
Tabla 5-31. Valoración del impacto para un activo AVARCIBER	151
Tabla 5-32. Dimensiones de seguridad de los Activos de la Plataforma HOST-IESS AVARCIBER	152
Tabla 5-33. Costo del activo HOS - IESS AVARCIBER.....	152
Tabla 5-34. Valoración del daño de las vulnerabilidades AVARCIBER	153
Tabla 5-35. Tuplas Vulnerabilidad – Activo de la plataforma HOST -IESS.....	153
Tabla 5-36. Vulnerabilidades con activos, valor y costo del daño HOST – IESS AVARCIBER	158
Tabla 5-37. Tripletas Amenazas – Vulnerabilidades – Activos con los valores y costo del daño de las vulnerabilidades para HOST - IESS AVARCIBER	165
Tabla 5-38. Duplas Amenazas – Vulnerabilidades con los valores y costo del daño de las vulnerabilidades AVARCIBER	172
Tabla 5-39. Amenazas con totales del valor del daño y costo del daño HOST – IESS AVARCIBER	173
Tabla 5-40. Probabilidad de ocurrencia de la amenaza AVARCIBER.....	174
Tabla 5-41. Valoración del Riesgo HOST – IESS AVARCIBER.....	174
Tabla 5-42. Matriz de Riesgo de la Plataforma HOST - IESS.....	175
Tabla 5-43. Contramedidas para HOST - IESS	175
Tabla 5-44. Relación entre elementos del modelo conceptual AVARCIBER.....	179
Tabla 5-45. Tipo de activos de ciberseguridad utilizados en AVARCIBER	180
Tabla 5-46. Vulnerabilidades, activos, valor y costo del daño HOST – IESS AVARCIBER.....	181
Tabla 5-47. Matriz de Riesgo AVARCIBER.....	182
Tabla 5-48. Contramedidas por vulnerabilidades HOST – IESS AVARCIBER.....	183
Tabla I-1. Criterios de Inclusión y Exclusión	A-6
Tabla I-2. Distribución de los estudios por fuente.	A-7
Tabla I-3. Definiciones del concepto de calidad.....	A-7
Tabla I-4. Estudios Clasificados en base a la categorización de Petersen	A-8
Tabla II-1. Tipos de Activos	A-11
Tabla II-2. Taxonomía de Vulnerabilidades	A-12
Tabla II-3. Taxonomía de Amenazas	A-16

Tabla III-1. Criterios de valoración Confidencialidad, Integridad, Disponibilidad y Criticidad	A-21
Tabla III-2. Criterios de valoración frecuencia	A-22
Tabla III-3. Valoración de activos en disponibilidad, integridad, confidencialidad y criticidad AS400 – IESS.	A-24
Tabla III-4. Impacto de las amenazas en los activos según su degradación AS400 – IESS	A-27
Tabla III-5. Tabla de Valores de Riesgos AS400 – IESS	A-53
Tabla III-6. Salvaguardas sugeridas AS400 – IESS.....	A-54
Tabla III-7. Valoración de activos en disponibilidad, integridad, confidencialidad y criticidad Host – IESS	A-61
Tabla III-8. Impacto de las amenazas en los activos según su degradación Host – IESS.....	A-64
Tabla III-9. Tabla de valores de riesgos Host – IESS	A-79
Tabla III-10. Salvaguardas por activo Host – IESS	A-80
Tabla III-11. Valoración de activos en disponibilidad, integridad, confidencialidad y criticidad Oracle – IESS	A-81
Tabla III-12. Impacto de las amenazas en los activos según su degradación Oracle – IESS.....	A-84
Tabla III-13 Tabla de Valores de Riesgos Oracle – IESS.....	A-102
Tabla III-14. Salvaguardas sugeridas Oracle – IESS	A-103
Tabla III-15 Valoración de activos en disponibilidad, integridad, confidencialidad y criticidad Firewall – IESS.	A-106
Tabla III-16. Impacto de las amenazas en los activos según su degradación Firewall – IESS.....	A-107
Tabla III-17 Tabla de valores de riesgos Firewall – IESS	A-115
Tabla III-18. Salvaguardas sugeridas Firewall – IESS	A-116
Tabla IV-1. Activos y tipos de activos.....	A-121
Tabla IV-2. Valoración del impacto para un activo.....	A-121
Tabla IV-3. Criterios de valoración dimensiones de Seguridad	A-122
Tabla IV-4. Valoración del impacto del Activo.....	A-122
Tabla IV-5. Valoración del Costo del Activo	A-123
Tabla IV-6. Valoración del daño de las vulnerabilidades	A-123
Tabla IV-7. Tuplas Vulnerabilidad – Activo	A-124
Tabla IV-8. Valoración del daño de la vulnerabilidad.....	A-124
Tabla IV-9. Tuplas de Vulnerabilidades – Activos, con valor y costo del daño de las vulnerabilidades, costo del activo.	A-125
Tabla IV-10. Tripletas Amenazas – Vulnerabilidades – Activos.....	A-126
Tabla IV-11. Tripletas Amenazas – Vulnerabilidades – Activo con los valores y costo del daño de las amenazas	A-126
Tabla IV-12. Duplas Amenazas – Vulnerabilidades con los valores y costo del daño de las vulnerabilidades	A-127
Tabla IV-13. Amenazas con valores totales de daño y costo del daño	A-127

Tabla IV-14. Probabilidad de ocurrencia de la amenaza	A-128
Tabla IV-15. Valoración del Riesgo	A-128
Tabla IV-16. Calculo del Riesgo.....	A-129
Tabla IV-17. Costo e impacto en las dimensiones de seguridad de los activos de la plataforma AS400-IESS	A-130
Tabla IV-18. Tuplas Vulnerabilidades - Activos, valor y costo del daño de las vulnerabilidades de la plataforma AS400-IESS.....	A-133
Tabla IV-19. Triplete Amenazas – Vulnerabilidades -Activos con el valor y costo del daño de la Amenaza para plataforma AS400-IESS.....	A-159
Tabla IV-20.- Tupla Amenazas – Vulnerabilidades con los valores y costo del daño de las vulnerabilidades para plataforma AS400-IESS	A-181
Tabla IV-21.- Amenazas con los valores y costo del daño de la amenaza para plataforma AS400-IESS	A-183
Tabla IV-22. Contramedidas para las vulnerabilidades AS400-IESS	A-184
Tabla IV-23. Valores de riesgos de las amenazas AS400-IESS	A-185
Tabla IV-24. Costo e impacto en las dimensiones de seguridad de los activos de la plataforma Host-IESS.	A-188
Tabla IV-25. Tuplas Vulnerabilidades - Activos, valor y costo del daño de las vulnerabilidades de la plataforma Host-IESS	A-190
Tabla IV-26 Triplete Amenazas – Vulnerabilidades -Activos con el valor y costo del daño de la Amenaza de la plataforma Host - IESS	A-198
Tabla IV-27. Tuplas Amenazas – Vulnerabilidades con los valores y costo del daño de las vulnerabilidades para la plataforma Host-IESS	A-205
Tabla IV-28.- Amenazas con los valores y costo del daño de la amenaza para la plataforma Host - IESS	A-206
Tabla IV-29. Contramedidas para las vulnerabilidades plataforma Host-IESS.....	A-207
Tabla IV-30 Valores de riesgos de las amenazas Host-IESS.....	A-208
Tabla IV-31. Costo e impacto en las dimensiones de seguridad de los activos de la plataforma Oracle-IESS	A-210
Tabla IV-32. Tuplas Vulnerabilidades - Activos, valor y costo del daño de las vulnerabilidades de la plataforma Oracle-IESS	A-211
Tabla IV-33. Triplete Amenazas – Vulnerabilidades -Activos con el valor y costo del daño de la Amenaza para la plataforma Oracle-IESS	A-216
Tabla IV-34. Tupla Amenazas – Vulnerabilidades con los valores y costo del daño de las vulnerabilidades para plataforma Oracle-IESS.....	A-219
Tabla IV-35.- Amenazas con los valores y costo del daño de la amenaza para Oracle-IESS	A-220
Tabla IV-36. Contramedidas para las vulnerabilidades de la plataforma Oracle-IESS	A-221
Tabla IV-37. Valores de riesgos de las amenazas de la plataforma Oracle-IESS.....	A-222
Tabla IV-38. Costo e impacto en las dimensiones de seguridad de los activos de la plataforma Firewall-IESS	A-224

Tabla IV-39. Tuplas Vulnerabilidades - Activos, valor y costo del daño de las vulnerabilidades de la plataforma Firewall-IESS	A-225
Tabla IV-40. Triplete Amenazas – Vulnerabilidades -Activos con el valor y costo del daño de la Amenaza para la plataforma Firewall-IESS.....	A-232
Tabla IV-41. Tupla Amenazas – Vulnerabilidades con los valores y costo del daño de las vulnerabilidades para plataforma Firewall-IESS	A-237
Tabla IV-42.- Amenazas con los valores y costo del daño de la amenaza para la plataforma Firewall-IESS	A-238
Tabla IV-43. Contramedidas para las vulnerabilidades plataforma Firewall-IESS	A-239
Tabla IV-44 Valores de riesgos de las amenazas Firewal-IESS	A-240

CAPÍTULOS

1 INTRODUCCIÓN

Esta tesis doctoral se enfoca en el diseño de un marco de trabajo para identificar y evaluar los riesgos de ciberseguridad que facilite la identificación y contribuya a la realización de un análisis de riesgos ágil y preciso en ciberseguridad, así como el impacto que ocasionen en las organizaciones. Así, el objetivo de este primer capítulo es mostrar: 1) el contexto de la ciberseguridad en los sistemas de seguridad de las organizaciones (indicando algunos de sus problemas e impactos); 2) la importancia de la ciberseguridad, descripción de amenazas, atacantes y ataques de ciberseguridad; 3) objetivos del trabajo de investigación. Así, se presenta una solución a esta problemática y se plantea la necesidad de proponer un marco de trabajo para identificar y evaluar los riesgos de ciberseguridad, en un marco adecuado que responda a los objetivos estratégicos institucionales de las organizaciones. El capítulo finaliza con; 4) una descripción de la aproximación a la solución, y 5) un resumen de la estructura de esta tesis doctoral.

1.1 Contexto de la Ciberseguridad

Ciberseguridad es un término ampliamente utilizado que habla de la seguridad de los sistemas y los datos, pero tiene muchas definiciones diferentes. Según la comunidad de seguridad de KAPERSKY (Kaspersky, 2020), se define la ciberseguridad como “la ciberseguridad es la práctica de defender las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos”. Por lo tanto, es una disciplina que involucra tecnología, personas, información y procesos para permitir operaciones seguras. Para que las organizaciones puedan mejorar la seguridad cibernética, la industria y la comunidad técnica han desarrollado modelos de madurez en ciberseguridad que miden las capacidades de seguridad cibernética y las posicionan en diferentes niveles para la mejora continua. Los modelos de madurez de ciberseguridad proporcionan un punto de referencia para evaluar el nivel actual de capacidad de las prácticas, procesos y métodos que tienen implementados las organizaciones.

Según Information Systems Audit and Control Association (ISACA) (Javier et al., 2015), ciberseguridad es: “protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados”.

El interés en la ciberseguridad está en aumento (Donaldson, Siegel, Williams, & Abdul, 2015). A medida que nuestro mundo se vuelve cada vez más interconectado y cada vez más en línea, el daño que las amenazas cibernéticas pueden causar a nuestro mundo cibernético está aumentando dramáticamente, día a día. Para muchos de nosotros en edad adulta, es difícil recordar la vida antes de las computadoras personales, por no hablar de Internet por supuesto; es asombroso considerar cómo toda esta conectividad ha transformado nuestra vida cotidiana. Sin embargo, como el mundo en línea se desarrolló en menos de una generación, la capacidad de proteger el mundo en línea ha tenido aún menos tiempo para desarrollarse y todavía está madurando. Casi cada semana o a diario se escucha y se anuncia sobre la violación de la seguridad cibernética o algún incidente parecido. Según lo descrito por algunos autores, los más comunes son (Kamra & Scott, 2017) (MEP, 2019) (Donaldson, Siegel, & Williams, 2019):

- Información personal comprometida.
- Tarjetas de crédito robadas.
- Registros médicos perdidos.
- Empresas hackeadas (vulneradas).
- Ataques a los sistemas de determinadas naciones.

Da la impresión que los atacantes que perpetran estos crímenes, están actuando con toda la impunidad del caso en la mayoría de las veces, y que no existen las regulaciones legales que

permitan detenerlos. Estos atacantes se están enfocando en las principales industrias y en grandes marcas conocidas para que el efecto tenga más resonancia.

Mientras los ataques afectan a víctimas que están en cualquier parte del mundo, las personas que hacen la piratería están en Rusia, China, Corea, Oriente Medio y en otras partes del mundo. Este problema es realmente global y es muy difícil de detener, por la globalidad de la comunicación y acceso a la información.

Si estos ataques están ocurriendo a los grandes negocios y naciones, que están muy bien reconocidos y bien financiados, ¿qué oportunidad tienen los pequeños negocios y pequeñas naciones perjudicadas, y qué deben protegerse a sí mismas?

Aquellos que están interesados en la ciberseguridad o son responsables de la ciberseguridad en una organización, ciertamente han reconocido que hay un largo camino por recorrer para alcanzar el éxito de la ciberseguridad frente a las amenazas latentes.

Si la solución fuera comprar únicamente una tecnología, entonces sólo habría que conectarla a nuestra red, sentarnos y relajarnos, mientras la tecnología cuida nuestros activos. Tal vez algún día algunos investigadores inteligentes desarrollarán tal tecnología, pero hoy en día no existe. La única manera de abordar la seguridad empresarial o institucional es como un complejo problema de ingeniería con varios sistemas interrelacionados. Las personas, los procesos y las tecnologías disponibles deben ser considerados; deben considerarse el dinamismo, comportamiento y relacionamiento de los sistemas y sus componentes. Deben adoptarse decisiones duras, tanto en términos de compromisos para la eficiencia de las empresas como en términos de asignación de recursos. Es decir, ninguna empresa puede permitirse todas las tecnologías, activos, controles y procesos para una máxima seguridad, simplemente no hay suficientes recursos disponibles. Por lo tanto, deben hacerse compromisos. Tomar esas decisiones inteligentemente, requiere sabiduría. La sabiduría proviene de la educación, la experiencia, y el análisis previo y detallado.

Para estructurar y gestionar un programa efectivo de ciberseguridad en una empresa, un gerente necesita comenzar en algún lugar. La arquitectura de seguridad cibernética de la empresa es un gran punto de partida, para luego empezar a adquirir los conocimientos específicos de dominio adaptados a las actividades cotidianas de ciberseguridad y a la estrategia a largo plazo. Cuando se habla de muchos sistemas y componentes, puede parecer abrumador o innecesario para el propietario de una pequeña empresa o empresario que opera con presupuestos muy bajos. Y es cierto: no todas las empresas pueden darse el lujo de tener todos los elementos de un programa de seguridad integral. Cuando el director ejecutivo es también el financiero, el secretario y el servicio de asistencia de TI (Tecnología de la Información), los recursos necesarios para desarrollar, administrar y mantener una arquitectura de ciberseguridad a gran escala son claramente deficientes. Sin embargo, todas las empresas pueden darse el lujo de tener a alguien pensando en el tema, desarrollando la sabiduría necesaria para tomar las decisiones difíciles y comprender las implicaciones de las decisiones.

La ciberseguridad es un área problemática que va en crecimiento, y es la preocupación de todos. Simplemente saber dónde empezar es un conocimiento valioso. Comprender cómo iniciar, continuar y mejorar es aún mejor. He aquí la importancia de que las empresas, grandes y pequeñas, se beneficien de la recopilación de conocimiento y estrategia.

En los últimos años, los costos por los delitos cibernéticos son significativos. El estudio “The Cost of Cybercrime” (Accenture and Ponemon Institute, 2019), combina la investigación a través de 11 países en 16 industrias. Entrevistaron a 2.647 líderes sénior de 355 empresas para examinar el impacto económico de los ataques cibernéticos. La Figura 1-1 muestra que el costo que implican los ataques cibernéticos en cada país es bastante alto, pero en el caso de los Estados Unidos encabeza la lista con un costo anual promedio del delito cibernético que aumentó en un 29% en 2018 para llegar a US \$ 27,4 millones, en relación al año previo (2017). Pero el mayor aumento del 31% lo experimentaron las organizaciones en el Reino Unido, que crecieron a US \$ 11,5 millones, seguidas de cerca por Japón, que aumentó en un 30% en 2018 para alcanzar los US \$

13,6 millones en promedio para cada organización. Por ello, es importante mostrar la importancia de ciberseguridad, describir los tipos de ataques, ciberatacantes que existen en la actualidad, y que se muestran en la siguiente sección.

Figura 1-1 Costo del delito informático en 11 países (Fuente: Accenture and Ponemon Institute, 2019)

1.2 Importancia de la Ciberseguridad

Inicialmente, las principales amenazas cibernéticas eran virus, gusanos y caballos de Troya. Estas amenazas cibernéticas atacaron al azar computadoras conectadas directamente a Internet, pero plantearon poca amenaza empresarial. Dentro de las redes empresariales con cortafuegos en el exterior y protección antivirus en el interior, la empresa parecía estar protegida y relativamente segura. De vez en cuando ocurría un incidente y los defensores cibernéticos se reunían para combatirlo, una vez que los defensores comprendían el código malicioso, detectarlo y derrotarlo era sencillo.

Entonces, lenta pero seguramente, una transformación comenzó a tener lugar. Los ciberataques comenzaron a entrar dentro de las redes empresariales, y una vez que estaban dentro, operaban subrepticamente. Los ciberatacantes tomaron el control de las máquinas infectadas, y las conectaron a sistemas remotos de mando y control. Ellos capturaron nombres de usuario y contraseñas, y luego los usaron para conectarse a sistemas para robar datos o dinero. Los ciberatacantes aprovecharon vulnerabilidades dentro de la empresa para moverse lateralmente entre los equipos de la red y capturar las credenciales de más y más personas dentro de la empresa. Por último, los ciberatacantes aumentaron los privilegios y obtuvieron el control de las cuentas de administrador de sistemas a cargo de todo. Una vez que estos atacantes obtuvieron el control administrativo de la empresa, eran capaces de hacer lo que quisieran.

En los últimos años, esta tendencia se ha manifestado en brechas cada vez más espectaculares que golpean los titulares de prensa. Algunas de las graves intrusiones realizadas han sido:

- En 2011, accedieron a los sistemas de la empresa RSA Security, y se creía que las claves de seguridad para muchos de sus clientes habían sido robadas (Richmond, 2011). Esta infracción llevó a RSA a reemplazar millones de sus tokens SecureID para restaurar la seguridad de sus clientes. Esta violación es desconcertante porque RSA es una de las marcas de ciberseguridad más antiguas y establecidas.
- En 2013, la red de punto de venta (POS, Point of Sale) de Target se vio comprometida, con la consiguiente pérdida de información personal y números de tarjetas de crédito para más de 40 millones de clientes (Brian, 2014). Los costos de esta intromisión en particular,

probablemente fueron enormes por el daño a la reputación de la organización y también si tomamos en cuenta los juicios que podrían presentar los clientes a la empresa.

- En 2014, Sony Pictures Entertainment, informó de un ciberataque en donde los atacantes se habían infiltrado en su entorno y desactivado casi todos los ordenadores y servidores de la compañía (Barnes & Cieply, 2014). Este ciberataque puso a la empresa de rodillas y dio lugar a la publicación pública de miles de documentos de su propiedad y mensajes de correo electrónico.
- En 2014, una acería alemana se vio afectada por un incidente de piratería que causó un mal funcionamiento de uno de sus altos hornos (Technology & News, 2014). Esto resultó en un daño físico significativo a la planta y a sus instalaciones.
- En 2015, Anthem reportó que sus sistemas de TI habían sido violados y la información personal sobre más de 80 millones de miembros actuales y antiguos de su red de salud estaba comprometida, incluyendo el programa Blue Cross Blue Shield del gobierno de los Estados Unidos (Nakashima, 2015). Los ciberatacantes intentaron obtener información privada de ciertos individuos miembros de este sistema, obligándolos a pedir ayuda inmediata al FBI (Federal Bureau of Investigation).
- En 2016, la campaña de Clinton y el Partido Demócrata fueron objeto de múltiples ataques que causaron el robo de información, por parte de piratas informáticos de Rusia (Redacción, 2016). La Agencia Central de Inteligencia (CIA) concluyó que hubo una inferencia ilegal vía ataques cibernéticos, que dañaron la imagen del partido Demócrata por revelar información muy importante de la campaña electoral.
- En 2017, el software malicioso WannaCry afectó al Servicio Nacional de Salud de Gran Bretaña (Hern, Alex; Gibbs, 2017), algunas de las compañías más grandes de España, incluida Telefónica, así como a computadoras en Rusia, Ucrania y Taiwán, lo que provocó que las computadoras y los datos se bloqueasen y retuviesen por rescate.
- En 2019, los hackers han publicado datos personales vinculados a la canciller Angela Merkel y a cientos de otros políticos en Alemania (Nicola, Stefan; Donahue, 2019) en el mayor escándalo de datos robados de este tipo en el país. La información incluye direcciones de correo electrónico, números de teléfonos móviles, fotos de identificaciones y transcripciones de chat personales.

Estas intrusiones son sólo unas cuantas violaciones de la seguridad cibernética que han ocurrido en la última década. Sin embargo, estas brechas son indicativas de algunas de las principales tendencias. Los ciberatacantes ahora están apuntando a identidades personales, cuentas financieras e información de salud, y obtener esta información de millones o decenas de millones de personas en una sola violación. Los ciber atacantes también están tomando el control de los equipos industriales y causando daño físico a las plantas y al equipamiento de las industrias. Afortunadamente, nadie ha sido herido hasta ahora, pero teniendo en cuenta las tendencias actuales, puede ser sólo una cuestión de tiempo.

Estos titulares parecen indicar que los atacantes han tomado la delantera, al menos por ahora. La pregunta es, "¿qué ha cambiado y cómo pueden los defensores recuperarse?". Por ello, es necesario estar atentos a las diferentes formas de intrusiones que pueden ser ejecutadas por los ciberatacantes. A continuación, se describen algunas amenazas, las formas de ataques y quienes los realizan.

1.2.1 Las amenazas persistentes avanzadas

De hecho, estas violaciones principales apuntan al surgimiento de un nuevo tipo de adversario, la amenaza persistente avanzada (APT, Advanced Persistent Threat). Estos ataques son de gran interés, no porque sean misteriosos o particularmente avanzados, sino porque marcan la profesionalización generalizada de los ciberataques. Un atacante de APT es experto en el arte del ciberataque y aprovecha las tecnologías de TI de manera efectiva para romper las defensas de las empresas y sistemáticamente evitar todas sus protecciones, de una en una. Lo que hace a APT diferente a otros tipos de ciberataque es la persistencia del ataque. De vuelta a los días de los virus

y caballos de Troya, los ciberataques eran generalmente considerados como algo arbitrario. Un desarrollador de software creó un pedazo de malware y lo envió a Internet para propagarse. O se propagó o no lo hizo. Donde propagaba, era generalmente arbitrario, determinado más por la suerte que por cualquier dirección específica del revelador.

APT hace ciberataques mucho más centrados y eficaces porque ahora están bajo el control de un actor inteligente que tiene un objetivo a lograr. Si el objetivo de los atacantes es entrar en un banco o en un negocio, persisten en su ataque e intentan múltiples ángulos y enfoques hasta que tienen éxito. Si su objetivo es entrar en una empresa y robar secretos corporativos, persisten en perseguir esa meta hasta que tengan éxito. Si su objetivo es irrumpir en un gobierno y robar información de seguridad nacional, persisten en tratar de encontrar debilidades en las redes y computadoras del gobierno hasta que las encuentren y explotan estas debilidades.

En un ataque convencional, las defensas sólo necesitan bloquear el malware, y pasará a otros objetivos. Simplemente tener defensas ya no es eficaz cuando un solo error puede ser explotado por un atacante oportunista. Un atacante de APT ajusta constantemente el ataque para superar la última ronda de defensas. Dado con suficiente tiempo, un atacante APT eventualmente conseguirá superar esta defensa. Para evitar que el atacante atraviese las defensas, las defensas deben funcionar perfectamente y mantenerse siempre alerta. Cualquier error por parte de los defensores es rápidamente explotado por el atacante, que está esperando errores. APT requiere un nuevo tipo de método de defensa, uno que se adapte al ataque tan rápidamente como el ataque se adapta a la defensa.

1.2.2 Las olas de malware

Mirando las técnicas, herramientas y tecnologías de los adversarios y las ciberdefensas correspondientes a los últimos 20 años, se puede ver que ha habido varias generaciones, u olas, de tecnologías de malware que infectan computadoras y se propagan en las redes. Éstas pueden agruparse en diferentes categorías basadas en sus características y comportamientos (Donaldson, Siegel, Williams, & Abdul, 2018), incluyendo lo siguiente:

- **Virus estáticos:** la primera ola de malware son virus estáticos que se propagan de un ordenador a otro a través de disquetes y sectores de arranque de discos duros. Estos virus se propagaron, pero pocos de ellos realmente afectaron las operaciones del sistema.
- **Virus basados en la red:** la segunda ola de malware son virus basados en la red que se propagan a través de la Internet abierta de una computadora a otra, aprovechando las debilidades de los sistemas operativos. Los ordenadores a menudo estaban directamente conectados entre sí sin cortafuegos u otras protecciones intermedias.
- **Caballo de Troya:** la tercera ola de malware es un malware troyano que se propaga a través de Internet a través del correo electrónico y de sitios web comprometidos o maliciosos. Este malware puede infectar a un gran número de víctimas, pero lo hace de manera relativamente arbitraria, ya que no está dirigido.
- **Comando y Control:** la cuarta ola de malware incluye funciones de comando y control que permiten al atacante controlar remotamente su operación dentro de la empresa objetivo. Las máquinas comprometidas se convierten en un punto de apoyo dentro de la empresa que puede ser manipuladas por el atacante.
- **Personalizado:** la quinta ola de malware es un malware personalizado desarrollado para un objetivo en particular. El malware personalizado se envía directamente a destinos específicos a través de correos electrónicos de suplantación de identidad, sitios web con control remoto o aplicaciones descargables como aplicaciones móviles. Dado que el malware se personaliza para cada víctima, no es reconocido por las defensas basadas en firmas.
- **Polimórfico:** la sexta ola de malware es un malware polimórfico diseñado no sólo para tomar el control administrativo de las redes de víctimas, sino también para modificarse

dinámicamente de manera que pueda evadir la detección y mantenerse por delante de los intentos de remediarlo.

- **Inteligente:** la séptima ola de malware es un malware con inteligencia para analizar una red de víctimas, moverse lateralmente dentro de ella, escalar privilegios para tomar control administrativo y extraer, modificar o destruir sus datos de destino o sistemas de información. El malware inteligente hace todas estas acciones de forma autónoma, sin necesidad de intervención humana o de control y comando externos.
- **Completamente automatizado, polimórfico:** la octava ola de malware es totalmente automatizado, malware polimórfico que combina las características de la sexta y séptima olas. Este malware toma el control de forma autónoma y evita dinámicamente la detección y remediación para mantenerse un paso por delante de los defensores en todo momento.
- **Firmware y cadena de suministro:** la novena ola de malware toma como base la octava ola, al ofrecer capacidades de malware a través de la cadena de suministro, ya sea incorporado en el firmware del producto o dentro de los productos de software antes de ser enviados. Dicho malware está incrustado en los productos cuando se construyen o en un nivel tan bajo en el firmware del producto que son prácticamente indetectables. Mediante la entrega de malware de esta manera, es difícil para los ciberdefensores diferenciar el malware de la cadena de suministro de las otras características procedentes de la fábrica.

Muchas personas están familiarizadas con las primeras tres olas de ciberataques, que representan la mayoría de las amenazas cibernéticas de consumo y muchos de los ataques cubiertos por la prensa. Las empresas experimentan las olas de malware cuatro, cinco y seis en forma regular y creciente. Sin embargo, estas olas de malware son poco conocidas fuera de campos especializados de ciberseguridad. Los ciberatacantes de estados y naciones usan las ondas de malware siete, ocho y nueve. Esas olas requieren recursos y conocimientos técnicos considerables. Estas olas son sofisticados paquetes de malware diseñados para penetrar en las ciberdefensas más desarrolladas.

Todas estas tecnologías de malware están proliferando con el tiempo. No hace mucho tiempo, las olas cuatro, cinco y seis estaban exclusivamente en el dominio del atacante de estados y naciones. Hoy en día están en manos de los cibercriminales; las olas de malware son luego utilizadas por otros mercados. Es razonable esperar en el futuro que tales herramientas sofisticadas estarán en manos de atacantes casuales también. Los ciberatacantes no están quietos y sus herramientas están en constante evolución.

Según el informe de pruebas de seguridad de la empresa alemana AV-TEST en su informe: "Security Report 2018/2019" (AVTEST (IT-Security Institute), 2019), con la detección de la muestra de malware número 900 millones, el desarrollo de programas de malware ha tomado un gran incremento a mediados de mayo de 2019. A fines de 2018, el número de programas detectados por los sistemas de análisis de AV-TEST todavía era de alrededor de 856,62 millones. En la Figura 1-2, se puede observar que los nuevos descubrimientos de malware en el repositorio de AV-TEST son altos.

Figura 1-2 Muestras descubiertas en el repositorio AV-TEST de 2015 a 2019 (Fuente: AVTEST (IT-Security Institute), 2019)

1.2.3 Los tipos de ciberatacantes

¿Quiénes son estos misteriosos ciberatacantes que invaden los sistemas y causan estos titulares? Obviamente, son personas, en algún lugar del mundo, que eligen crear, distribuir y usar malware u otras herramientas o técnicas para hacer cosas en computadoras que no deberían hacer. Como se muestra en la Figura 1-3, estas personas pueden agruparse en cinco categorías según su intención y objetivos.

Figura 1-3 Categorías de los ciberatacantes

Puede haber una superposición significativa en las herramientas y tecnologías utilizadas por estos grupos. Estas cinco categorías de ciberataque se describen en los siguientes bullets.

- **Amenazas a los activos clave.**

Las amenazas a los activos clave son el malware al azar, los virus, los troyanos, los gusanos, las botnets, el ransomware y otras amenazas que se propagan en la Internet todo el tiempo. Estrictamente por casualidad, las amenazas a los activos no están dirigidas y

pueden terminar dentro de la empresa en cualquier momento. Las amenazas a los activos clave pueden explotar vulnerabilidades u otras debilidades de la ciberdefensa, pero no se ajustan ni se adaptan para sortear las protecciones existentes.

Las amenazas a los activos clave pueden ser destructivas, aunque la cantidad de daño que pueden hacer es generalmente bastante limitada. Sin embargo, también pueden ser el punto de partida para amenazas más peligrosas y específicas. Los ciberataques dirigidos pueden comenzar sus esfuerzos acudiendo a los operadores de botnet, y adquiriendo acceso a computadoras y servidores que ya están comprometidos dentro del entorno de destino. Este acceso adquirido puede facilitar la entrada inicial de los atacantes en la empresa, y ahorrarles tiempo y dinero valioso.

- **Hactivistas.**

El hacking activista, o hacktivismo, consiste en ataques dirigidos. Los hactivistas utilizan la piratería informática para hacer una declaración pública o política. Su objetivo es utilizar el hacking para reforzar su causa o avergonzar a sus adversarios. El hacktivismo puede ser utilizado contra individuos, empresas o gobiernos, dependiendo de la situación y los objetivos particulares de los hactivistas.

Los hactivistas, debido a su ideología activista, rara vez están haciendo daño a alguien o causan daño físico significativo. La mayoría de las veces, los hactivistas simplemente buscan sacar su mensaje y llamar la atención sobre su causa. Los hactivistas llevan a cabo sus ataques con un objetivo explícito de que la prensa lo cubra, comunicando su mensaje y que sus adversarios se sientan avergonzados.

Dado que los hactivistas son frecuentemente individuos que actúan solos o pequeñas organizaciones con recursos limitados, los hactivistas tienden a usar principalmente herramientas y técnicas básicas que están ampliamente disponibles en Internet. Las defensas para protegerse contra estas herramientas y técnicas también suelen estar ampliamente disponibles. Los hactivistas operan aprovechando las vulnerabilidades que no están parcheadas o están abiertas a la explotación. Los hactivistas intentarán e intentarán de nuevo hasta que los defensores cometan un error que les permita lograr su objetivo.

- **Crimen organizado.**

Al igual que el hacktivismo, los ataques contra las organizaciones son los objetivos de organizaciones criminales. Los criminales y las organizaciones criminales han encontrado que hay una manera de hacer mucho dinero en Internet. Hay una serie de factores que hacen que Internet sea particularmente atractivo para los elementos criminales:

- **Fácil acceso:** en una red global interconectada, los llamados barrios buenos y barrios malos están a solo un clic de distancia. Los criminales pueden tocar a cualquiera en el mundo, sin moverse de su sitio.
- **Falta de atribución:** en Internet, puede ser notoriamente difícil rastrear a los atacantes, especialmente cuando toman medidas para cubrir sus huellas. Cuando las víctimas están en un país y los criminales en otro país, se hace más difícil rastrear a los atacantes.
- **Datos al por mayor:** ¿por qué robar dinero de una persona a la vez cuando, con sólo un poco más de esfuerzo, se puede robar el banco en su lugar? Los criminales han descubierto, que, con la consolidación de datos en enormes bases de datos corporativas, el robo de datos al por mayor puede ser sorprendentemente fácil de llevar a cabo.

Estos factores han convertido el robo de datos en un gran negocio. Aquellos que hacen una gran cantidad de robos, pueden conseguir una gran cantidad de dinero. Cuando las tarjetas de crédito robadas o los números de seguridad social valen \$ 1 cada uno en el

mercado negro y los registros médicos valen \$ 10 o más, el atacante que puede robar un millón de registros puede hacer dinero real. Este dinero, a su vez, va a apoyar a toda una industria ilegal de participantes, proveedores y actores de apoyo que están dispuestos a ayudar y prestar sus servicios a cambio de un recorte en el botín.

Al considerar a los ciberdelincuentes, es importante recordar que hay muchas maneras de ganar dinero a través de ataques cibernéticos. Muchos de esos métodos no tienen nada que ver con el robo de números de tarjetas de crédito. Los ciberatacantes pueden obtener el control de las cuentas bancarias de negocios y utilizar la banca en línea para ir sacando el dinero de las cuentas corporativas mediante la transferencia del dinero a sí mismos. Los cibertatacantes pueden cifrar datos corporativos usando malware ransomware y luego chantajear al negocio para recuperar sus datos. Los ciberatrachadores pueden comprometer las cuentas de los empleados y reenviar el depósito directo de las nóminas a sus propias cuentas. No hay límite en cuanto a cómo los cibercriminales creativos consiguen monetizar el hecho de que pueden comprometer personas, cuentas y computadoras en las empresas de sus víctimas.

- **Espionaje.**

Lo que el crimen organizado empieza, los agentes de espionaje lo llevan al siguiente nivel. Los ciberdelincuentes son relativamente fáciles de entender, ya que sus objetivos son sencillos. Los ciberdelincuentes tratan de obtener acceso a computadoras, cuentas y redes, y luego explotan el acceso para robar dinero directamente o robar datos que luego pueden convertirse rápidamente en dinero. El ciberespionaje, por otro lado, es un poco más complejo en sus objetivos y en cómo los lleva a cabo. Ciertamente, hay un conductor financiero, pero otros conductores son mucho menos directos.

El ciberespionaje se centra en robar secretos comerciales para obtener ventajas comerciales o secretos nacionales para obtener ventajas políticas o militares. En el caso de los negocios internacionales, estos dos intereses pueden alinearse estrechamente y las multinacionales pueden verse afectadas por agencias de inteligencia nacionales que trabajan en estrecha colaboración con su competencia internacional. Mientras que, en los Estados Unidos, las empresas y el gobierno tienen una relación de independencia, en muchos países esa relación no siempre es así.

Los secretos robados pueden ser sorprendentes. Todas las empresas tienen las "joyas de la corona" de planos, fórmulas o código de software que se consideran críticos para el éxito. Sin embargo, hay mucha otra información, como organigramas, presupuestos, calendarios de proyectos e incluso reuniones que son de vital importancia para la competencia. Toda esta información puede estar sujeta a esfuerzos de espionaje por parte de los adversarios, particularmente de las multinacionales.

Los practicantes del ciberespionaje usan con frecuencia métodos APT (Advanced Persistent Threat), no porque estos métodos sean la única forma de hacer el trabajo, sino porque tienden a ser muy eficaces contra las empresas con ciberdefensas de estilo heredado. ¿Por qué molestarse en hackear la computadora portátil del CEO cuando, por la misma cantidad de esfuerzo, puede obtener el control de cada computadora portátil en la empresa? Una vez que los agentes obtienen el control administrativo, pueden robar datos propietarios a voluntad.

Las campañas de ciberespionaje pueden llevarse a cabo a nivel de nación-estado, y estas campañas pueden estar formadas por múltiples partes. Desafortunadamente para algunas empresas, su experiencia de ciberespionaje puede ser simplemente porque son un trampolín en una campaña enfocada en llegar a otros objetivos no relacionados. Por ejemplo, los agentes de espionaje pueden hackear un hospital simplemente para obtener información de identidad de uno de sus pacientes que es de interés para ellos. Un sitio web popular puede ser hackeado simplemente porque es frecuentado por personas de las empresas que los agentes de espionaje tienen en el punto de mira. El ciberespionaje es un

problema serio y las campañas pueden involucrar complejas redes de individuos y empresas objetivo mientras los agentes trabajan desde sus puntos de partida hacia sus objetivos.

- **Guerra cibernética.**

Mientras que el espionaje se centra generalmente en el robo de información, la ciberguerra trata de dañar la capacidad de las empresas o gobiernos para operar en el ciberespacio. Este daño se produce al sobrecargar, deshabilitar o destruir los sistemas de TI utilizados por las víctimas, o incluso utilizar esos sistemas de TI para hacer que los sistemas físicos funcionen mal y se dañen a sí mismos o a sus operadores. La posibilidad de ciberintrusiones causando daño físico, lesiones o muerte es desconcertante. Todo está cada vez más informatizado y en red, el daño que se puede hacer desde el ciberespacio sigue aumentando.

La ciberguerra tiene un primo, el ciberterrorismo, que se lleva a cabo utilizando las mismas técnicas, pero por personas u organizaciones terroristas. Mientras que la guerra cibernética se lleva a cabo para apoyar los intereses nacionales, el ciberterrorismo se hace para una agenda activista, o simplemente se puede realizar en aras de la anarquía y la destrucción por su propio bien. Los efectos, particularmente los efectos psicológicos, son los mismos en ambos sentidos. Ambas actividades se realizan utilizando herramientas y técnicas similares, empleando la denegación de servicio, la destrucción de datos o la manipulación del sistema de control para lograr sus objetivos.

1.2.4 Los tipos de ciberataques

Independientemente del objetivo o las técnicas utilizadas, generalmente hay tres cosas que los ciberataques pueden hacer a una empresa o a sus datos, como se muestra en la Figura 1-4. Los ataques cibernéticos comprometen la confidencialidad robando datos, comprometiéndola la integridad mediante la modificación de datos o comprometiéndola la disponibilidad al negar el acceso a datos, servicios o sistemas. Algunos ataques pueden combinar dos o más de estos tipos en un solo ataque, pero estos tres tipos de ciberataque son los bloques de construcción para la mayoría de las actividades cibernéticas malintencionadas. La ciberdefensa debe centrarse en proteger la confidencialidad, integridad y disponibilidad de los datos y los sistemas de TI que lo procesan.

Figura 1-4 Daños causados por las amenazas a la defensa cibernética

- **Confidencialidad: robar datos.**

Violaciones de confidencialidad son las que más a menudo se escuchan en los titulares de hoy en día. Los números de seguridad social, números de tarjetas de crédito, información de cuentas bancarias, registros de salud electrónicos, y secretos corporativos confidenciales y correspondencia ejecutiva son sólo algunos ejemplos de los datos robados a las empresas y vendidos al mejor postor. Los ataques destinados a robar datos a menudo se centran en el sigilo, al menos al principio, para penetrar en la empresa objetivo, llegar a los datos objetivo, e infiltrarse sin ser notado. Por otro lado, una vez que la empresa víctima es consciente de que se está produciendo una violación, los atacantes pueden volverse significativamente más audaces, especialmente para terminar un ataque que ya está en curso.

El incumplimiento de la confidencialidad se centra en obtener acceso a los datos donde reside, que puede ser cualquiera de una serie de lugares en reposo y en tránsito:

- **Bases de datos:** el lugar más obvio para encontrar grandes grupos de datos se encuentra en las bases de datos donde reside. Sin embargo, estos sistemas tienden a estar relativamente bien protegidos dentro de la arquitectura de la empresa.
 - **Copias de seguridad:** deberán realizarse copias de seguridad de las bases de datos empresariales que contengan datos críticos empresariales y de clientes. Curiosamente, estas copias de seguridad terminan frecuentemente en una gran variedad de ubicaciones donde los datos se replican en disco, en cintas, en sistemas de prueba que no son de producción y en instantáneas de máquinas virtuales, todo ello de forma regular. Estas ubicaciones de copia de seguridad secundarias con frecuencia no reciben mucha consideración de seguridad y pueden ser vulnerables a ataques, sobre todo si se almacenan sus datos sin cifrar.
 - **Servidores de aplicaciones:** incluso las bases de datos bien protegidas tienen que hacer que sus datos estén disponibles de alguna manera, y los servidores front-end de aplicaciones con acceso a esos datos suelen conectarse directamente a Internet. Las infracciones de estos sistemas pueden utilizarse para obtener acceso a los datos a través de las aplicaciones, omitiendo el cifrado y otros métodos de protección.
 - **Administradores de Sistemas:** el talón de Aquiles de la mayoría de las empresas son los administradores de sistemas y las credenciales que utilizan para administrar sistemas. Si los atacantes pueden acceder a estas credenciales, pueden pasar por alto todas las demás protecciones de datos y, con frecuencia, lo hacen con poca o ninguna pista de auditoría para revelar sus acciones.
- **Integridad: modificar datos (robar dinero).**

Las infracciones de integridad reciben mucha menos atención que las brechas de confidencialidad en estos días. Es realista esperar que la prominencia de las brechas de integridad aumentará a medida que los ataques sigan ganando en sofisticación. Los ataques de integridad implican la modificación de datos, lo que puede dar lugar a diversos impactos que incluyen lo siguiente:

- Impactos reputacionales si esos datos son información pública como sitios web.
- Impactos de la información financiera si se trata de datos financieros, particularmente para una corporación que cotiza en bolsa.
- Pérdidas de dinero real si los datos que se cambian son números de enrutamiento bancario o mandatos financieros a los bancos que manejan cuentas corporativas.

Algunos ataques de integridad de interés particular incluyen lo siguiente:

- Secuestro: alteración de datos de infraestructura sobre Internet, como nombres de dominio, identidades de medios sociales o ubicaciones de red registradas. Gran parte de los bienes raíces de Internet son puramente de naturaleza electrónica y garantizada por nada más que una dirección de correo electrónico. Algunas de estas propiedades pueden valer miles o incluso millones de dólares.

- Sarbanes-Oxley: a raíz del desastre de Enron (Lugo, 2002), las regulaciones Sarbanes-Oxley fueron desarrolladas para proteger la integridad de los datos financieros publicados por las corporaciones que cotizan en bolsa. Los cambios no autorizados en los datos financieros pueden tener serias consecuencias de auditoría y regulación para la corporación afectada.
 - Banca en línea: con el aumento de la banca en línea, las empresas tienen acceso en línea a cuentas bancarias de negocios que pueden incluir nóminas, inversiones, fondos de acciones y otros activos por miles o millones de dólares. Los atacantes que pueden obtener acceso a las credenciales que controlan estas cuentas pueden robar rápidamente grandes cantidades de dinero. Moviéndolo a través de múltiples intermediarios en varios países se hace imposible rastrear o enjuiciar a los atacantes.
 - Depósito directo: de manera similar, con los servicios de nómina habilitados para Internet y proporcionando acceso en línea a la información de talón de pago y la configuración de depósito directo bancario, los empleados son vulnerables a robos en los que sus cheques de pago son reencaminados a las cuentas de un atacante. Si un solo atacante puede redirigir cheques de pago de un número de individuos con valores altos todos al mismo tiempo, es posible salirse con una gran suma de dinero rápidamente.
 - Vandalismo: actores maliciosos dañan sitios web u otros materiales públicos con la intención de avergonzar a la víctima. Los sistemas orientados a Internet pueden ser difíciles de proteger a la perfección. Una sola vulnerabilidad o error de configuración puede ser todo lo que se necesita para permitir que un atacante ataque.
- **Disponibilidad: denegar acceso.**

El tercer tipo de ciberataque es afectar la disponibilidad de los sistemas y denegar el acceso a ellos. Los ataques que causan la denegación de servicio pueden ser difíciles de diagnosticar, especialmente si los sistemas están dañados, pero no deshabilitados. A menudo, los sistemas se deterioran cuando el ataque causa fallos abrumadores a los sistemas y la infraestructura. En general, los ataques deliberados de disponibilidad pueden agruparse en tres categorías:

- Los ataques DDoS (Distributed Denial of Service) se utilizan para desactivar eficazmente los servicios en la empresa o país víctima. Estas técnicas se han utilizado en los últimos años, y pueden dejar gran parte de las capacidades de Internet de la víctima fuera de línea por algún tiempo hasta que se mitiguen.
- Los ataques de denegación de servicio dirigidos implican hackear a la víctima y luego desactivar los sistemas para los que se han reconstruido o recuperados. Dependiendo de la gravedad del daño causado, el personal de TI puede tardar algún tiempo en recuperar los sistemas y restaurar el servicio, sobre todo si se afectan las copias de seguridad, así como los sistemas primarios.
- Los ataques de Destrucción Física implican el uso de ciberataques para causar la destrucción física. Stuxnet es la incidencia más famosa de este tipo de ataque, donde un ciberataque sabotó centrifugadoras del programa nuclear iraní. A medida que sistemas cada vez más críticos son controlados por computadora, este tipo de ataques se convierten en potencialmente más peligrosos y destructivos con el tiempo.

1.2.5 Marcos de Ciberseguridad

La literatura sobre ciberseguridad presenta excelentes marcos de trabajo. Algunos de los principales marcos de ciberseguridad incluyen los siguientes (Donaldson et al., 2018):

- (ISC)2 Certified Information Security System Professional (CISSP) Common Body of Knowledge (CBK). (The International Information Systems Security Certification Consortium is also known as (ISC)2)
- International Organization for Standardization (ISO) 27001 and 27002, version 2013

- The National Institute of Standards and Technologies (NIST) Risk Management Framework (RMF) and special publication 800-53
- The Council on Cyber Security Critical Security Controls (formerly known as the SANS 20 Controls)

Un objetivo de estos marcos es proporcionar una metodología para hablar sobre ciberseguridad y garantizar que el esfuerzo de ciberseguridad de una empresa abarque los elementos más importantes de protección y defensa. Cada marco divide la ciberseguridad de una manera ligeramente diferente, y cada marco tiene enfoques y prioridades ligeramente diferentes. Sin embargo, al mirar los marcos, hay muchos puntos en común y conceptos similares. La Figura 1-5 muestra una visión general de estos cuatro marcos (se deja la versión inglesa para una mejor comprensión).

(ISC) ² Common Body of Knowledge 10 security domains	ISO 27001 / 27002 v2013 114 controls in 14 domains	NIST SP800-53v4 224 controls in 18 families	Council on Cyber Security Critical Security Controls - 20 controls
1. Access Control 2. Telecommunications and Network Security 3. Information Security Governance and Risk Management 4. Software Development Security 5. Cryptography 6. Security Architecture and Design 7. Security Operations 8. Business Continuity and Disaster Recovery Planning 9. Legal, Regulations, Investigations, and Compliance 10. Physical (Environmental) Security	1. Information Security Policies 2. Organization of Information Security 3. Human Resource Security 4. Asset Management 5. Access Control 6. Cryptography 7. Physical and Environmental Security 8. Operations Security 9. Communications Security 10. System Acquisition, Development, and Maintenance 11. Supplier Relationships 12. Information Security Incident Management 13. Information Security Aspect of Business Continuity Management 14. Compliance	1. Access Control 2. Awareness and Training 3. Audit and Accountability 4. Security Assessment and Authorization 5. Configuration Management 6. Contingency Planning 7. Identification and Authentication 8. Incident Response 9. Maintenance 10. Media Protection 11. Physical and Environmental Protection 12. Planning 13. Personnel Security 14. Risk Assessment 15. System and Services Acquisition 16. System and Communications Protection 17. System and Information Integrity 18. Program Management	1. Inventory of Devices 2. Inventory of Software 3. Secure Configurations for Computers 4. Continuous Vulnerability Assessment and Remediation 5. Malware Defenses 6. Application Software Security 7. Wireless Device Control 8. Data Recovery Capability 9. Security Skills Assessment and Training 10. Security Configurations for Network Devices 11. Network Ports, Protocols, and Services 12. Control of Administrative Privileges 13. Boundary Defense 14. Security Audit Logs 15. Need-to-Know Access Control 16. Account Monitoring and Control 17. Data Loss Prevention 18. Incident Response Capability 19. Secure Network Engineering 20. Penetration Testing and Red Team Exercises

Figura 1-5 Marcos de Ciberseguridad (Fuente: (Donaldson et al., 2018))

Una característica común de estos marcos es que dividen la empresa y su protección en varias áreas funcionales. A veces, las áreas se llaman dominios, a veces se llaman familias, a veces se llaman áreas de control, y a veces se llaman objetivos de control. En general, hay entre 10 y 20 de estas áreas funcionales que permiten la organización lógica y la gestión de un programa general de defensa cibernética.

La segunda característica común es que casi todos los marcos principales aprovechan la metodología de gestión de riesgos. La gestión de riesgos permite a la empresa identificar qué protecciones son necesarias en función de una evaluación objetiva de sus activos, amenazas contra esos activos, vulnerabilidades en la protección de esos activos y riesgos resultantes de las amenazas que se analizan contra las vulnerabilidades. Una vez que la empresa identifica los riesgos, puede considerar mitigaciones para reducir los riesgos, ya sea reduciendo su probabilidad o su gravedad.

La tercera característica común es que todos estos marcos hablan de controles de seguridad. El propósito de un control de seguridad es principalmente reducir la probabilidad o la gravedad de un riesgo, aunque algunos controles de seguridad también pueden servir para detectar la explotación del riesgo o para recopilar datos forenses para respaldar investigaciones posteriores.

La cuarta característica común es que estos marcos proporcionan un mecanismo para auditar, evaluar y validar la presencia o ausencia de los controles descritos en el marco. Algunas veces este mecanismo se realiza mediante estándares documentados para la evaluación, y otras veces

mediante listas de verificación para la auditoría. La mayoría de los marcos contienen dicha guía de evaluación, o el método de evaluación es obvio o bien conocido.

Sobre la segunda característica común, de aprovechar la metodología de gestión de riesgos, es importante que exista un marco de trabajo de gestión de riesgos en ciberseguridad, como el paso inicial para identificar los elementos que lo constituyen y sus relaciones, para poder identificar la metodología de gestión de riesgos adecuada para ciberseguridad.

1.3 Objetivos del trabajo de investigación

En el apartado anterior se ha descrito la importancia de la ciberseguridad, algunas amenazas a las que se está expuesto, tipos de ciberataques y tipos de ciberatacantes, también se muestra los costos que implican los ataques de ciberseguridad y, adicionalmente, se mencionan los marcos de trabajo de ciberseguridad, que como característica común aprovechan la metodología de gestión de riesgos.

Hay varias metodologías utilizadas por las organizaciones para la gestión de riesgos. Todas buscan objetivar el análisis de riesgos y medir el impacto en las organizaciones. El gran reto de todas estas aproximaciones es la complejidad del problema al que se enfrentan; complejidad en el sentido de que hay muchos elementos que considerar, los mismos elementos que son identificados en un marco de trabajo de gestión de riesgos en ciberseguridad, y que, si no se es riguroso, las conclusiones serán de poco fiar. Es por ello que en esta tesis se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del personal que lo aplique.

Los objetivos directos de esta tesis son los siguientes:

1. Desarrollar un marco de trabajo para identificar y evaluar los riesgos de ciberseguridad.

Para alcanzar el objetivo principal se ha planteado un conjunto de sub-objetivos u objetivos secundarios, cuya finalidad es conducirnos, paso a paso, hacia la solución de la problemática planteada.

Así, los objetivos secundarios planteados son:

- Realizar un estudio de los modelos de madurez de ciberseguridad. Para ello, es necesario:
 - Identificar los modelos de madurez de ciberseguridad más nombrados en investigaciones.
 - Comparar los modelos de madurez más representativos.
- Realizar un estudio de los modelos conceptuales de riesgos en ciberseguridad. Para ello, es necesario:
 - Identificar los modelos conceptuales de riesgo en ciberseguridad.
 - Identificar los elementos que describen un modelo conceptual del dominio.
- Realizar un estudio de las clasificaciones de los elementos que participan en la identificación y evaluación de riesgos en ciberseguridad. Para ello, es necesario:
 - Generar una taxonomía de activos.
 - Generar una taxonomía de amenazas de ciberseguridad.
 - Generar una taxonomía de vulnerabilidades de ciberseguridad.
 - Genera una taxonomía de riesgos en ciberseguridad.
 - Realizar una evaluación de probabilidades en base a: incidentes producidos y que hayan sido publicados o se disponga de su información.
- Aplicar el modelo conceptual en un caso de estudio. Para ello, es necesario:
 - Implementar el modelo conceptual del dominio en una organización.
 - Desarrollar un prototipo para gestionar el análisis y evaluación de riesgos en ciberseguridad.

1.4 Aproximación a la solución

En el trabajo de investigación realizado en la tesis se llevarán a cabo las siguientes actividades:

1. Analizar los distintos modelos de madurez en ciberseguridad, su estructura, procesos, estándares y su enfoque en la gestión de la seguridad de TI en las organizaciones. Para ello, se establecerán las bases para realizar un análisis comparativo de los modelos de madurez en ciberseguridad, indicando los criterios más relevantes e importantes y, posteriormente, se realizará el análisis comparativo de los principales modelos definidos.
2. Realizar una revisión sistemática de taxonomías de riesgos en ciberseguridad con objeto de identificar las taxonomías definidas, para poder identificar los modelos conceptuales descritos, e identificar los elementos utilizados y sus relaciones.
3. Analizar los diferentes modelos conceptuales para la gestión de riesgos en ciberseguridad, e identificar los elementos principales y las relaciones entre ellos.
4. Realizar una revisión sistemática de taxonomías de activos, vulnerabilidades y amenazas de ciberseguridad con objeto de completar este estudio e identificar las taxonomías definidas, para poder utilizarlas en las organizaciones.
5. Crear un marco de trabajo de gestión de riesgos en ciberseguridad que identifique los elementos que participan y sus relaciones, y la descripción de las actividades a ser implementadas, para medir el impacto de los riesgos en ciberseguridad en la organización.
6. Validar el marco de trabajo propuesto a través de su aplicación en un prototipo, para ser aplicado en una organización, ya sea pública o privada.

1.5 Estructura de la tesis doctoral

La documentación de esta tesis se encuentra organizada en un conjunto de siete capítulos cuyos contenidos se describen brevemente en la Tabla 1-1.

Tabla 1-1 Estructura de la Tesis Doctoral

CAPÍTULO	DESCRIPCIÓN
1. Introducción	Se describe el contexto de la ciberseguridad, su importancia y problemática actual, y las repercusiones en las organizaciones. También se indican los marcos de trabajo en ciberseguridad, y las características que tienen en común, siendo la gestión de riesgos su principal característica común. Finalmente, se plantean los objetivos globales del trabajo de investigación y su aproximación a la solución.
2. Estado de la cuestión	Se ofrece: 1) una descripción de los modelos de madurez de ciberseguridad, y cómo gestionan los riesgos cada uno de ellos; 2) una revisión y análisis de los modelos de madurez definidos y se hace una comparativa entre ellos, enfatizando en la gestión de riesgos de ciberseguridad; y 3) una revisión y análisis de las taxonomías de riesgos en ciberseguridad, con el fin de obtener información de todos los trabajos relacionados con taxonomías de riesgos en ciberseguridad, e identificar los modelos conceptuales de riesgos utilizados, 4) la identificación de los elementos de estos modelos conceptuales identificados, sus relaciones y actividades descritas. Así mismo, se realizan una serie de conclusiones sobre cada uno de los aspectos, con el objeto de destacar las carencias existentes en cada uno de ellos, las cuales serán desarrolladas en esta tesis doctoral. Finalmente, se realizará una revisión y análisis de las taxonomías de activos, y vulnerabilidades y amenazas de ciberseguridad.

CAPÍTULO	DESCRIPCIÓN
3. Planteamiento del problema e hipótesis de trabajo	Se plantea el problema detectado de los estudios anteriores, describiendo de forma detallada la situación actual de los modelos conceptuales de riesgos en ciberseguridad, que son la base para establecer un marco de trabajo de riesgos en ciberseguridad. Se introduce el proceso de solución propuesta y las hipótesis de trabajo.
4. Resolución	En este capítulo se documenta detalladamente el modelo conceptual de riesgos en ciberseguridad, sus elementos, y sus relaciones, que describen el marco de trabajo de riesgos en ciberseguridad. Se definen las actividades para medir el impacto de los riesgos en ciberseguridad en las organizaciones en base al marco de trabajo definido.
5. Experimentación	En este capítulo, con el fin de aceptar o rechazar las hipótesis formuladas en la presente investigación, se presenta la validación de marco de trabajo de riesgos en ciberseguridad definida. Para ello: (1) se verifica la aplicación del marco de trabajo de gestión de riesgos en ciberseguridad para organizaciones públicas o privadas; (2) se evalúa la validez de marco de trabajo a través de la valoración de la identificación de riesgos y su impacto funcional como económico, y la retroalimentación de la implementación; (3) se analiza el listado de riesgos iniciales de la organización para contrarrestarles con los identificados luego de la aplicación del marco de trabajo y el proceso de gestión de los riesgos, antes y después de la aplicación del marco de trabajo.
6. Conclusiones y Líneas Futuras de Investigación	En este capítulo se exponen las conclusiones de la tesis y sus aportaciones, se presentan los resultados de la tesis y, finalmente, se presenta una propuesta de líneas de investigación futuras derivadas de este trabajo de investigación.
7. Referencias	En este capítulo se recoge toda la bibliografía asociada a esta tesis doctoral.
8. Anexos	Finalmente, en el último capítulo se recoge toda la información de los anexos que soportan este trabajo de investigación.

2. ESTADO DE LA CUESTIÓN

El objetivo de este capítulo es presentar el estado del arte del tema de esta tesis doctoral, la madurez en la identificación y evaluación de riesgos en ciberseguridad, mediante la aplicación del proceso de Revisión Sistemática (RS), así como de la meta-narrativa (consulta, análisis e interpretación de la información obtenida), con la finalidad de conocer el estado actual del tema a investigar, así como los elementos que participan y su relación con el tema de la investigación de esta tesis doctoral.

Este capítulo pretende dar a conocer los conceptos y elementos necesarios para poder entender el tema principal de esta tesis doctoral. Es decir, entender los trabajos previos realizados por los investigadores que contribuirán a los temas que tienen relación con el contexto de la investigación.

Una revisión sistemática de la literatura es un medio para identificar, evaluar e interpretar toda la investigación disponible relevante para una determinada pregunta de investigación, área temática o fenómeno de interés. El proceso de RS está definido en el Anexo I de este documento.

Inicialmente se realiza una búsqueda de los principales modelos de madurez y su comparativa (véase sección 2.1). Puesto que todos los modelos de madurez en su nivel más bajo se enfocan en la gestión de riesgos de ciberseguridad, en la sección 2.2 se presentan los conceptos de riesgos de ciberseguridad y la revisión sistemática realizada sobre taxonomías de riesgos de ciberseguridad, y la descripción de los modelos conceptuales identificados sobre riesgos en ciberseguridad. En la sección 2.3, se describen las revisiones sistemáticas sobre los elementos críticos que deben considerarse en la gestión de riesgos en ciberseguridad, es decir RS de taxonomías de activos, y de vulnerabilidades y amenazas en ciberseguridad. Finalmente, en la sección 2.4 se incluyen las consideraciones finales de lo realizado.

2.1. Modelos de Madurez en Ciberseguridad

Para la revisión sistemática se ha considerado el proceso de revisión sistemática propuesto por Kitchenham (B. A. Kitchenham & Jorgensen, 2004) (B. Kitchenham & Charters, 2007) descrito en el Anexo I.

2.1.1. RS de Modelos de Madurez en Ciberseguridad

Existen una serie Modelos de Madurez de Capacidad de Seguridad Cibernética (CCMM, Cybersecurity Capability Maturity Models), que sirven de referencia dentro de la industria para la evaluación de los niveles de madurez de ciberseguridad de las organizaciones. Por ello, se pretende, a través de una revisión sistemática de la literatura científica, responder a la siguiente pregunta:

¿Cuáles son los principales modelos de madurez en ciberseguridad que existen en el mercado?

A continuación, se muestra el proceso de revisión sistemática para los modelos de madurez en ciberseguridad siguiendo el proceso indicado en el Anexo I.

2.1.1.1 Identificación de las Necesidades

La revisión sistemática permitirá: (1) identificar los diferentes modelos de madurez en ciberseguridad que existen en el mercado, (2) identificar los modelos más nombrados por los estudios realizados.

2.1.1.2 Protocolo de Revisión

En este punto se definen: las preguntas a realizar, las fuentes de bases de datos que deben usarse para realizar la búsqueda, la elaboración de las cadenas de búsqueda según los criterios definidos, y que incluye las palabras claves de las cadenas de búsqueda.

- **Preguntas:** las preguntas a responder son: ¿cuáles son los modelos de madurez en ciberseguridad que existen en el mercado?, ¿cuáles son los principales modelos de madurez en ciberseguridad que se utilizan en los estudios de investigación?
- **Fuentes seleccionadas:** IEEE Computer, Science Direct, SpringerLink, Institute for Scientific Information (ISI) web of knowledge.
- **Las cadenas de búsqueda** fueron las siguientes:
 - “capability maturity model for cybersecurity”.
 - “capability maturity model for information security management system”.
 - “capability maturity model for cybersecurity applied in organizations”.
- **Palabras claves:** las palabras usadas en la cadena de búsqueda incluyen: “maturity model”, “cybersecurity”, “capability”, “information security management system”, “organizations”.

2.1.1.3 Ejecución

En este punto se muestra la búsqueda realizada de los artículos en las bases de datos seleccionadas con las cadenas de búsquedas predefinidas. La revisión se realiza en tres fases. Al resultado de las búsquedas, se les aplican los criterios de inclusión y exclusión establecidos a continuación.

Criterios de selección de estudios, y procedimientos para inclusión y exclusión:

- En la Tabla 2-1 se presentan los criterios de inclusión y exclusión que se han aplicado a los resultados de la búsqueda inicial.

Tabla 2-1. Criterios de inclusión y exclusión (RS Modelos de Madurez de Ciberseguridad – RS CCMM)

Inclusión (I)	Exclusión (E)
I1. Estudios empíricos de modelos de madurez en ciberseguridad y gestión de sistemas de seguridad de la información. Artículos que tratan sobre los factores que condicionan los modelos de madurez en ciberseguridad en las organizaciones.	E1. Artículos que están basados sólo en una opinión particular que no aborde la ciberseguridad.
I2. Artículos que exponen sobre los modelos de madurez en ciberseguridad y gestión de sistemas de seguridad de la información.	E2. Artículos cortos.
I3. Artículos que incluyen en su redacción las palabras claves.	E3. Estudios que no son relevantes para las preguntas de investigación o no están relacionados con el estudio en particular.
I4. Artículos cuyo título, resumen o contenido está relacionado con el tema.	E4. Estudios que no son claros o presentan ambigüedad.
	E5. Publicaciones duplicadas.
	E6. Estudios anteriores a 2012 debido a la reciente aparición de este concepto.

- En una primera fase de la revisión sistemática, haciendo uso de los motores de búsqueda de las bases de datos identificadas y poniendo la cadena de búsqueda elaborada en el protocolo de revisión, se encontraron un total de 12.952 estudios.
- En una segunda fase, se han revisado cada uno de los estudios tomando en consideración los criterios de inclusión y exclusión anteriores, obteniendo un total de 201 estudios relevantes.
- En la tercera fase, se obtuvieron 12 estudios denominados primarios. Para ello, se ha realizado la lectura de los estudios relevantes y se han seleccionado aquellos que respondían a las preguntas formuladas inicialmente. En la Tabla 2-2 se muestran las

fuentes, el número total de artículos, y el número de artículos relevantes y primarios seleccionados por fuente.

Tabla 2-2. Distribución de los Estudios por Fuente (RS MMC)

<i>Fuente</i>	<i>Total</i>	<i>Relevantes</i>	<i>Primarios</i>
IEEE Explore	988	37	3
Science Direct	9558	106	2
SpringerLink	2397	49	5
ISI WoK	9	9	2
Total	12952	201	12

Evaluación de la calidad de los estudios:

Para evaluar la calidad de los estudios, se realizaron las siguientes preguntas:

- ¿Es el estudio primario importante para la investigación que se está realizando?
- ¿Los estudios primarios proveen la suficiente información como para que los resultados se beneficien de la revisión sistemática?
- ¿Los estudios revisados dan un valor agregado a la investigación que se está realizando?

De las preguntas anteriores, se pudo comprobar que los 12 estudios primarios seleccionados son importantes, proveen suficiente información y dan un valor agregado a la revisión sistemática.

Análisis, Interpretación e Informe de los Resultados

Al concluir la ejecución de la revisión sistemática, los resultados se han resumido y analizado. En el análisis, se usan herramientas para determinar la frecuencia del nombrado de los modelos de madurez en ciberseguridad. Para realizar el análisis, los estudios se han clasificado en estudios relacionados con: (1) modelos de madurez en ciberseguridad, (2) modelos más nombrados en los estudios y (3) variantes de los modelos de madurez en ciberseguridad.

Los artículos contienen casos de estudio, experimentos, encuestas, y se presentan en la Tabla 2-3, y se clasifican de acuerdo a los criterios de (Petersen, Feldt, Mujtaba, & Mattsson, 2008).

Tabla 2-3. Estudios clasificados en base a la categorización de Peterson (RS MMC)

<i>Clasificación</i>	<i>Referencia</i>
Propuestas de solución	(Von Solms, 2015), (Adler, 2013), (Ouedraogo, Mouratidis, Dubois, & Khadraoui, 2010)
Búsquedas de evaluación	(Le, 2016), (Barclay, 2014), (Bishop, Miloslavskaya, & Theocharidou, 2015), (Goksen, Cevik, & Avunduk, 2015)
Artículos de opinión	(Hohan, Oлару, & Pirnea, 2015), (Bergmann & Silveira, 2014), (Payette, Anegebe, Caceres, & Muegge, 2015)
Artículos de experiencia	(Siponen, 2002)
Artículos filosóficos	(Lee, Chung, & Choi, 2006)

Una vez seleccionados y analizados cada uno de los estudios primarios, se identificaron los modelos de madurez en ciberseguridad más nombrados en los estudios de investigación y se elaboró una matriz de modelos de madurez en ciberseguridad por número de veces nombrados en los estudios. Durante la revisión de la matriz, se ha observado que algunos modelos de madurez están basados en otros modelos, pero no todos están relacionados con la ciberseguridad. Por ejemplo, se basan en el CMMI para poder adaptarlos a sus necesidades, e inclusive se encontraron

algunos modelos adaptados a un enfoque forense (Cohen, Lowrie, & Preston, n.d.), como: Digital Forensic Organization Core Capability (DFOCC) y Digital Forensic Management Framework (DFMF).

A continuación, se presentan los resultados de la revisión sistemática.

- Modelos de Madurez en Ciberseguridad utilizados en los Estudios: con el fin de conocer los modelos de madurez en ciberseguridad que se utilizan en los estudios de investigación, se seleccionaron los modelos identificados en los estudios primarios (véase Tabla 2-4).

Tabla 2-4. Modelos de Madurez en Ciberseguridad Identificados (RS CCMM)

Modelos	Referencias
CCSMM (Community Cyber Security Maturity Model)	(Le, 2016), (Barclay, 2014)
COBIT (Control Objectives for Information and related Technology)	(Le, 2016), (Goksen et al., 2015), (Bergmann & Silveira, 2014)
CSF-NIST (Cybersecurity Capability Maturity Model – National Institute of Standards and Technology)	(Le, 2016)
C2M2 (Cybersecurity Capability Maturity Model)	(Von Solms, 2015), (Le, 2016), (Adler, 2013), (Payette et al., 2015)
ISEM (Information Security Evaluation Maturity Model)	(Le, 2016), (Lee et al., 2006)
ISM2 (Information Security Maturity Model)	(Le, 2016)
ISM3 (Information Security Management Maturity Model)	(Le, 2016), (Hohan et al., 2015)
NICE-CMM (National Initiative for Cybersecurity Education – Capability Maturity Model)	(Le, 2016), (Barclay, 2014), (Bishop et al., 2015)
SSE-CMM (Systems Security Engineering Capability Maturity Model)	(Le, 2016), (Hohan et al., 2015), (Ouedraogo et al., 2010), (Siponen, 2002), (Lee et al., 2006)

- Frecuencia de Nombrado de los Modelos de Madurez en Ciberseguridad:

Considerando que hay un número de veces que aparece repetido un mismo modelo de madurez en ciberseguridad en los estudios, mediante un procedimiento de conteo se determinó el número de veces que el modelo de madurez se repite. Al tabular los datos, se obtiene la lista de modelos de madurez en ciberseguridad que son más nombrados en los estudios, obteniéndose los modelos de madurez empleados en ciberseguridad ordenados por la frecuencia con que han sido mencionados por los autores. Se identificaron los principales modelos de madurez en ciberseguridad, de acuerdo a la distribución de frecuencias. En la Figura 2-1 se muestra la frecuencia de nombrado de los modelos de madurez en ciberseguridad. En los estudios de investigación, se puede observar que el modelo de madurez en ciberseguridad más utilizado es el SSE-CMM, modelo que ha sido adoptado para ciberseguridad.

Figura 2-1. Frecuencia del nombrado de los Modelos de Madurez en Ciberseguridad

- Variantes de los Modelos de Madurez en Ciberseguridad: debido a que no existen en el mercado modelos de madurez en ciberseguridad por cada área de la industria, muchos de los modelos han sufrido variantes y modificaciones, e inclusive adaptaciones de otros modelos que no fueron elaborados inicialmente para ese propósito. Dentro de los estudios primarios, se encontraron variantes de los modelos. Por ejemplo, el modelo de ciberseguridad C2M2 tiene 2 variantes: el Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) que está enfocado al sector eléctrico, y el Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2) enfocado al servicio de gas y combustibles.

Del análisis realizado de los modelos de madurez en ciberseguridad para implementarlos en la industria, se ha observado lo siguiente:

- “C2M2” Cybersecurity Capability Maturity Model. Es un modelo que está enfocado a ciberseguridad y que debido a su importancia se crearon dos variantes: una, para el sector energético (Von Solms, 2015), (Le, 2016), (Adler, 2013), y otra, para el sector de gas y combustibles (Le, 2016) de los Estados Unidos de Norteamérica (Payette et al., 2015).
- “NICE” Capability Maturity Model (CMM). Es un modelo de ciberseguridad, enfocado en la gestión de la planificación del trabajo de todos los participantes en la gestión de la ciberseguridad, y en los objetivos de la organización (Le, 2016), (Barclay, 2014), (Bishop et al., 2015).
- “SSE-CMM” Systems Security Engineering Capability Maturity Model. Origen de la Norma ISO/IEC 21827:2002 Information Technology – Systems Security Engineering – Capability Maturity Model. Es una de las normas más utilizadas internacionalmente en relación con la definición e implantación de los procesos de seguridad, ya que define en detalle los procesos que deben tenerse en cuenta en cualquier organización que desea implantar un “Proceso Global de Seguridad”. Este modelo es el más mencionado en los trabajos de investigación y es un modelo aplicado a seguridad de la información, pero se ha acoplado en los diferentes trabajos para abordar ciberseguridad (Le, 2016), (Hohan et al., 2015), (Ouedraogo et al., 2010), (Siponen, 2002), (Lee et al., 2006).
- “ISEM” Information Security Evaluation Maturity Model. Es un modelo que nombran los autores por ser uno de los primeros modelos de madurez aplicados a seguridad de la información. Se ha utilizado como parámetro para desarrollar otros modelos de madurez aplicados a ciberseguridad, pero solo se nombra y no se realiza un análisis a fondo por los nuevos paradigmas de tecnología, y porque ya existen nuevos modelos de madurez aplicados a diferentes sectores (Le, 2016), (Lee et al., 2006).
- “COBIT” Control Objectives for Information and related Technology. Es un modelo conocido y aplicado en TI, desarrollado por ISACA, donde se manejan 5 niveles de madurez. Se desarrolló para medir el nivel de madurez en el dominio de gobierno de TI, pero se ha usado de referencia en los trabajos investigados que incluyen al gobierno de

TI como uno de los factores claves de la ciberseguridad, complementando COBIT con otros modelos (Le, 2016), (Goksen et al., 2015), (Bergmann & Silveira, 2014).

- “ISM3” Information Security Management Maturity Model. Lo relevante de este modelo es que se manejan métricas de Seguridad de la Información, que ayudan a mantener a la organización en un nivel de riesgo aceptable, se ajusta tanto a pequeñas como a grandes organizaciones, y es muy utilizado y adaptable para necesidades específicas como ciberseguridad (Le, 2016), (Hohan et al., 2015).
- “CCSMM” Community Cyber Security Maturity Model. Este modelo fue desarrollado por la Universidad de San Antonio Texas, y es un modelo holístico que determina la postura de ciberseguridad en organizaciones, comunidades y naciones (Le, 2016), (Barclay, 2014).

2.1.1.4 Conclusiones de la Revisión Sistemática de Modelos de Madurez en Ciberseguridad

De los resultados obtenidos, podemos diferenciar los modelos que están enfocados a ciberseguridad y aquellos que se han adaptado para su aplicación en ciberseguridad, así como también cuáles son los que se utilizan actualmente en nuevas investigaciones. Se puede indicar que:

- Todos los modelos toman como referencia el modelo CMM.
- Los modelos de ciberseguridad actuales son adaptaciones de otros modelos.
- Los modelos principales usados para ciberseguridad tienen variantes.
- No existe una tendencia por un modelo de ciberseguridad, si no que el modelo más mencionado es un modelo de madurez aplicado a seguridad de la información, SSE-CMM.
- La mayoría de los modelos de madurez son elaborados y auspiciados por entidades estatales y organizaciones de estandarización internacionales.

Durante el análisis de los estudios, se ha observado que cada autor usa un vocabulario diferente para un mismo significado. También se ha identificado que los modelos de ciberseguridad existentes actualmente no son adaptables completamente a las necesidades particulares de las organizaciones. Por ello, se han creado diferentes variantes, donde solo las principales han sido mencionadas en esta revisión, pues la gran mayoría de modelos no están diseñados para abordar de manera única los riesgos de ciberseguridad.

Del análisis realizado, se desprende que el número de modelos mencionados por los autores es muy reducido, identificando que existe un campo no explotado en la actualidad sobre ciberseguridad, ya que entre los artículos revisados solamente una minoría abordaban modelos aplicados a la problemática de ciberseguridad.

A destacar que el modelo ISEM solamente es mencionado porque muchos modelos lo tomaron como referencia, pero no es aplicado actualmente en la industria.

De igual manera, el modelo de COBIT es muy mencionado en los artículos, pero es un modelo que no aborda de manera completa la problemática de ciberseguridad, siendo su enfoque de gobierno de seguridad de TI, pero se ha forzado su uso por la sencillez y facilidad de su implementación.

Por lo que se puede mencionar que los modelos que se pueden considerar para posterior análisis son:

- Cybersecurity Capability Maturity Model (C2M2).
- The National Initiative for Cybersecurity Education (NICE).
- Systems Security Engineering Capability Maturity Model (SSE-CMM).

- Community Cyber Security Maturity Model (CCSMM).

Como conclusión, podemos indicar que en la actualidad existe una deficiencia de modelos de madurez que sean totalmente enfocados en ciberseguridad, de fácil implementación y adaptables a diferentes tipos de organizaciones.

Para complementar la RS, se ha realizado un estudio comparativo de los CCMM (Cybersecurity Capability Maturity Model) más nombrados en los artículos científicos y que pueden ser considerados en posteriores análisis, para determinar los elementos que pueden tener en común estos modelos de madurez y sus diferencias. Como paso previo, es necesario describir que son los modelos de madurez, así como sus particularidades.

2.1.2. Los Modelos de Madurez en Ciberseguridad

En esta sección se han tratado los modelos de madurez en ciberseguridad que fueron identificados de manera previa como relevantes por medio de la revisión sistemática (Rea-Guaman, Sanchez-Garcia, Feliu, & Calvo-Manzano, 2017).

2.1.2.1 Introducción

Un modelo de madurez es un conjunto de características, atributos, indicadores o patrones que representan la capacidad y la progresión en una disciplina en particular. El contenido del modelo típicamente ejemplifica las mejores prácticas y puede incorporar normas u otros códigos de práctica de la disciplina.

Un modelo de madurez, por lo tanto, proporciona un punto de referencia con el que una organización puede evaluar el nivel actual de capacidad de sus prácticas, procesos y métodos, y establecer objetivos y prioridades para la mejora. Además, cuando un modelo es ampliamente utilizado en una industria en particular (y los resultados de la evaluación son compartidos), las organizaciones pueden comparar su desempeño con otras organizaciones. Una industria puede determinar cuán bien se está desempeñando en general, examinando la capacidad de los miembros de la organización.

Para medir la progresión, los modelos de madurez típicamente tienen "niveles" a lo largo de una escala, algunos utilizan una escala de niveles de indicadores de madurez (Maturity Indicator Levels, MILs). Un conjunto de atributos define cada nivel. Si una organización demuestra la consecución de estos atributos, ha logrado tanto ese nivel como las capacidades que representa el nivel. Tener estados de transición medibles entre los niveles permite a una organización utilizar la escala para:

- Definir su estado actual.
- Determinar su futuro, estado más maduro.
- Identificar las capacidades que debe alcanzar para alcanzar ese estado futuro.

Y la información que se va a cuestionar con un modelo de madurez será:

- ¿Qué estamos haciendo?
 - De un conjunto de elementos, cuales cumplimos, cuáles no.
- ¿Cómo lo estamos haciendo?
 - De los elementos que cumplimos, ¿Cómo los cumplimos?
 - Mejor, pero ...
 - Manual, automático ...
 - En papel, o en digital ...
 - En diferido o en tiempo real

La manera en que las organizaciones abordan la capacidad de seguridad cibernética es esencial para contar con una seguridad cibernética eficaz, eficiente y sostenible. Es imperativo tener un enfoque integral y holístico para la construcción de capacidad de seguridad cibernética para fomentar una economía digital segura y competitiva, y para obtener los beneficios que la

participación en el ciberespacio puede aportarles a las organizaciones, a las sociedades y a las personas en todas partes. Para que las personas puedan comprender mejor cómo es la seguridad cibernética eficaz a través de la experiencia y el aprendizaje del mundo, la industria y la comunidad técnica han desarrollado modelos de madurez que miden las capacidades de seguridad cibernética.

Según un estudio realizado por la Berkley Research Group (BGR) (Berkley Research Group, 2016), en los dos primeros trimestres de 2016, BRG llevó a cabo un estudio comparativo acerca de la madurez de la ciberseguridad entre las principales organizaciones mundiales. Los 94 encuestados de 29 países y 12 sectores proporcionaron información sobre el estado de la seguridad digital, tendencias e información sobre los temas internos de las compañías, como el presupuesto asignado a la seguridad y la estructura de la organización. La encuesta consistió en 103 preguntas relacionadas con las prácticas de seguridad digital y se enfocó en seis temas principales: Liderazgo, Gestión de la Información, Gestión de Riesgos, Protección Esencial, Respuesta a Incidentes y Cultura de Seguridad. Sobre el tema de gestión de riesgos, los resultados encontrados fueron los siguientes:

Respecto a la eficacia de la gestión de riesgos en la seguridad digital:

- El 42% de las organizaciones están de acuerdo parcialmente, en que se tenga en cuenta los riesgos de la ciberseguridad durante el proceso de toma de decisiones.
- El 7% de las organizaciones están de acuerdo en que los riesgos de la seguridad digital deben tenerse en cuenta durante el proceso de toma de decisiones.

Respecto a la madurez de la gobernanza de seguridad de la información:

- El 56% de las organizaciones perciben sus capacidades de gobernanza de la información como “poco” o “algo” efectivas.

Respecto a la madurez de la gestión del riesgo de las tecnologías de información:

- El 33% de las organizaciones no han realizado una evaluación del impacto del riesgo para la seguridad digital.

La ciberseguridad es un área problemática que va en crecimiento, y es tema de preocupación para todos. En comparación a como era antes, la ciberseguridad solía ser relativamente simple, la transformación de los ataques e incidentes de ciberseguridad comenzaron a evolucionar de una manera exponencial logrando ingresar a las redes empresariales. La manera en que las organizaciones abordan la capacidad de seguridad cibernética es esencial para contar con una seguridad cibernética eficaz, eficiente y sostenible.

Los Modelos de Madurez de Capacidad de Seguridad Cibernética (CCMM, Cybersecurity Capability Maturity Model) toman en cuenta las consideraciones de seguridad cibernética a través de diferentes áreas/dimensiones de la capacidad, entendiendo que cada dimensión no es necesariamente independiente de las otras. Cada dimensión ofrece una serie de factores e indicadores de capacidad cibernética para que una organización comprenda la etapa de madurez para cada consideración específica. Se han identificado cinco etapas de madurez y estas varían desde una etapa inicial, en la cual una organización puede que haya apenas comenzado a considerar la seguridad cibernética, hasta un escenario dinámico, en el cual una organización es capaz de adaptarse rápidamente a los cambios en el panorama de la seguridad cibernética en relación a las amenazas, las vulnerabilidades, los riesgos, la estrategia económica o el cambio de las necesidades organizacionales.

Existen una serie de marcos de referencia que determina la industria para la evaluación de los niveles de madurez. Los principales modelos de madurez que son utilizados en los estudios de artículos científicos según la revisión sistemática (Rea-Guaman et al., 2017) y los que se han considerado para el análisis detallado son:

- Cybersecurity Capability Maturity Model (C2M2).

- The National Initiative for Cybersecurity Education (NICE).
- Systems Security Engineering Capability Maturity Model (SSE-CMM).
- Community Cyber Security Maturity Model (CCSMM).

A continuación, se describe las características y elementos principales de estos modelos que han sido investigados, así como también su área y enfoque de cobertura.

2.1.2.2 Cybersecurity Capability Maturity Model C2M2

El Departamento de Energía de los EE. UU. (DOE, Department Of Energy) desarrolló el Modelo de Madurez de Capacidad de Ciberseguridad (C2M2) (Department of Energy, 2019) a partir del Modelo de Madurez de Capacidad de Ciberseguridad del Subsector de Electricidad (ES-C2M2) Versión 1.0 al eliminar referencias y terminología específicas del sector. El ES-C2M2 se desarrolló en apoyo de una iniciativa de la Casa Blanca dirigida por el DOE, en asociación con el Departamento de Seguridad Nacional de los Estados Unidos (DHS, Department of Homeland Security) y en colaboración con expertos del sector público y privado.

El C2M2 se centra en la implementación y gestión de prácticas de ciberseguridad asociadas con los activos de información, tecnología de la información (TI, Information Technology) y tecnología de operaciones (OT, Operations Technology) y los entornos en los que operan. El modelo se puede usar para:

- Fortalecer las capacidades de seguridad cibernética de las organizaciones.
- Permitir la evaluación y comparación efectivas y consistentes de las capacidades en ciberseguridad.
- Compartir conocimiento, mejores prácticas y referencias relevantes entre organizaciones como un medio para mejorar las capacidades de ciberseguridad.
- Permitir a las organizaciones priorizar acciones e inversiones para la mejora de la ciberseguridad.

El modelo se compone de 10 dominios y de 4 niveles de madurez. Cada dominio agrupa un conjunto de prácticas de ciberseguridad, y cada nivel define la progresión del modelo de madurez en cada dominio. Los principios que se aplican para establecer los niveles de madurez son:

- Los niveles de madurez se aplican independientemente a cada dominio.
- Los niveles son acumulativos en cada dominio, es decir, para estar en un determinado nivel, la organización debe realizar todas las prácticas en el nivel y en los niveles anteriores.
- Establecer un nivel de madurez objetivo para cada dominio es una estrategia efectiva para usar el modelo para guiar la mejora del programa de seguridad cibernética.
- El desempeño de la práctica y el logro de MIL deben alinearse con los objetivos comerciales y la estrategia del programa de seguridad cibernética de la organización.

Los diez dominios en los que se divide el modelo son los siguientes (con un total de 39 objetivos de segundo nivel):

- Gestión de riesgos (RIESGO).
- Activos, cambios y gestión de la configuración (ACTIVO).
- Gestión de accesos e identidades (ACCESO).
- Gestión de amenazas y vulnerabilidades (AMENAZA).
- Conocimiento de la situación (SITUACIÓN).
- Respuesta a eventos e incidentes (RESPUESTA).
- Cadena de suministro y gestión de dependencias externas (DEPENDENCIAS).
- Gestión del personal (PERSONAL).
- Arquitectura de Ciberseguridad (ARQUITECTURA).
- Gestión del programa de ciberseguridad (PROGRAMA).

Es un modelo muy sencillo y claro que se puede tomar como referencia, los procesos son tan generales que pueden ser aplicados en cualquier otro subsector.

Los Niveles de Madurez son los siguientes:

- El Nivel 0: No se realizan prácticas.
- El Nivel 1: Las prácticas iniciales se realizan, pero pueden ser para este fin.
- El Nivel 2:
 - Características de manejo:
 - Las prácticas están documentadas.
 - Se proporcionan recursos adecuados para apoyar el proceso.
 - El personal que realiza las prácticas tiene habilidades y conocimientos adecuados.
 - La responsabilidad y la autoridad para realizar las prácticas se asignan.
 - Enfoque característico:
 - Las prácticas son más completas o avanzadas que en MIL1.
- El Nivel 3:
 - Características de manejo:
 - Las actividades están guiadas por políticas (u otras directivas organizacionales).
 - Los objetivos de desempeño para las actividades de dominio se establecen y monitorean para rastrear el logro.
 - Las prácticas documentadas para las actividades de dominio están estandarizadas y mejoradas en toda la empresa.
 - Enfoque característico:
 - Las prácticas son más completas o avanzadas que en MIL2.

La Figura 2-2 resume los elementos de cada dominio.

Figura 2-2. Elementos de modelo y dominio del modelo de madurez C2M2 (Fuente: Department of Energy, 2019)

Aplicación del Modelo

El modelo C2M2 es utilizado por una organización para evaluar sus capacidades de seguridad cibernética de manera consistente, para comunicar sus niveles de capacidad en términos significativos y para informar de la priorización de sus inversiones en seguridad cibernética.

La Figura 2-3 resume el enfoque recomendado para el uso del modelo. Una organización realiza una evaluación según lo define el modelo, utiliza esa evaluación para identificar brechas en la

capacidad, prioriza esas brechas y desarrolla planes para abordarlas, y finalmente implementa planes para abordar las lagunas. A medida que se implementan los planes, los objetivos empresariales cambian y el entorno de riesgo evoluciona, y el proceso se repite.

*Figura 2-3. Enfoque recomendado para usar el modelo de madurez C2M2
(Fuente: Department of Energy, 2019)*

El DOE desarrolló el C2M2 a partir del modelo Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) que está enfocado al sector eléctrico. También se generó el Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2) enfocado al servicio de gas y combustibles.

2.1.2.3 The National Initiative for Cybersecurity Education (NICE)

La ciberseguridad es uno de los principales desafíos de seguridad nacional de cualquier país del mundo. Un tema emergente de importancia es cómo las organizaciones perfeccionan, evalúan, incrementan y organizan su fuerza de trabajo. Muchas organizaciones han recurrido a la planificación de la fuerza de trabajo como una manera de entender sus habilidades y capacidades actuales de capital humano en seguridad cibernética, así como las necesidades potenciales de infraestructura.

La Iniciativa Nacional para la Educación en Seguridad Cibernética (NICE) ha evolucionado a partir de la Iniciativa Integral de Seguridad Cibernética (CNCI), Iniciativa 8 - Expandir la Educación Cibernética, para desarrollar una fuerza de trabajo tecnológicamente capacitada y cibernética con los conocimientos y habilidades adecuados. Hacia estos objetivos, el Componente 3 del NICE se centra en la Estructura de la Fuerza Laboral de la seguridad cibernética, específicamente, la gestión del talento y el papel de la planificación de la fuerza de trabajo. La única versión (1.0) del modelo se publica en agosto del 2014 (US Department of Homeland Security, 2014).

A medida que la fuerza de trabajo de ciberseguridad continúa evolucionando y las organizaciones rastrean y gestionan el cambiante entorno de la ciberseguridad, la comprensión de dónde se encuentran las capacidades actuales de planificación de la fuerza laboral y cómo desarrollarse es cada vez más importante.

Un modelo de madurez de la capacidad (CMM) proporciona una estructura para que las organizaciones basen las capacidades actuales en la planificación de la fuerza de trabajo de seguridad cibernética, estableciendo una base para una evaluación consistente. Permite a las organizaciones comparar sus capacidades entre sí y permite a los líderes tomar decisiones mejores y bien informadas sobre cómo apoyar la progresión y qué inversiones hacer en relación con las iniciativas de capital humano de seguridad cibernética.

El CMM de NICE segmenta las actividades clave en tres áreas principales (véase Figura 2-4): 1) proceso y análisis, 2) gobernanza integrada, y 3) profesionales capacitados y tecnología habilitadora.

- El *proceso* representa aquellas actividades asociadas con los pasos reales que una organización toma para realizar la planificación de la fuerza de trabajo y cómo estos pasos se integran con otros procesos empresariales importantes en toda la organización. El *análisis* representa aquellas actividades asociadas con los datos de oferta y demanda, y el uso de herramientas, modelos y métodos para realizar análisis de planificación de la fuerza de trabajo.
- La *gobernanza integrada* representa aquellas actividades asociadas con el establecimiento de estructuras de gobierno, el desarrollo y la provisión de orientación, y la conducción de la toma de decisiones. Es la piedra angular de la estrategia y la visión general de la planificación de la fuerza de trabajo de una organización, así como las asignaciones de responsabilidad, la promoción de la integración y la emisión de directrices de planificación.
- Los *profesionales capacitados* representan las actividades asociadas con el establecimiento de un cuadro profesional de planificadores de la fuerza de trabajo dentro de una organización. La *tecnología habilitadora* representa las actividades asociadas con la accesibilidad y el uso de los sistemas de datos.

Figura 2-4. Áreas del modelo de madurez de NICE (Fuente: US Department of Homeland Security, 2014).

La planificación de la fuerza de trabajo de ciberseguridad de NICE tiene tres niveles de madurez. Estos niveles son:

- El nivel limitado es el nivel más básico, y representa un área de actividad clave o segmento de la capacidad de planificación de la fuerza laboral de una organización que está en su infancia. Este nivel de capacidad está en su inicio de desarrollo y puede estar representado por una organización que tiene un establecimiento limitado de procesos, que carece de orientación clara o que tiene poco en términos de datos y métodos de análisis.

- El nivel progresivo describe un área de actividad clave de algún aspecto de la planificación de la fuerza laboral de seguridad cibernética que una organización ha comenzado a realizar, representada comúnmente por una organización que establece alguna infraestructura para apoyar los esfuerzos de planificación de la fuerza de trabajo.
- El nivel final de madurez en optimización representa un área de actividad clave o segmento de la capacidad de planificación de la fuerza laboral de ciberseguridad que está desarrollado plenamente, que está integrado con otros procesos de negocio y puede soportar diferentes niveles de trabajo y análisis de carga de trabajo. Además, impulsa la toma de decisiones a corto y largo plazo para la fuerza de trabajo de seguridad cibernética.

El CMM de NICE además de describir los tres niveles de madurez en relación con estas tres áreas, proporciona sus actividades correspondientes en cada uno de los niveles de madurez.

Aplicación del Modelo

Para utilizar el modelo, las organizaciones deben tener una comprensión exacta de sus capacidades actuales de planificación de la fuerza laboral, ya que se relacionan con las tres áreas del segmento y con la capacidad de citar pruebas específicas de la realización de actividades relacionadas. La capacidad actual de una organización es el trampolín sobre el cual construir más madurez, usando el CMM para señalar los próximos pasos y puntos de decisión necesarios para la progresión. NICE recomienda un proceso de tres pasos para usar el CMM para determinar la capacidad actual de planificación de la fuerza laboral de ciberseguridad de una organización y progresar la madurez organizacional individual de forma continua:

- Recopilar datos sobre variables cualitativas de CMM.
- Analizar datos y determinar los niveles de madurez actuales por área clave de CMM.
- Determinar las áreas prioritarias para una mayor madurez y desarrollar planes de acción.

2.1.2.4 Systems Security Engineering Capability Maturity Model (SSE-CMM)

El SSE-CMM es un modelo de referencia (CMU, 2003). Se centra en los requisitos para implementar la seguridad en un sistema o serie de sistemas relacionados que son el dominio de Seguridad de Tecnología de la Información (ITS, Information Technology Security). Sin embargo, la experiencia con el modelo ha demostrado su utilidad y aplicabilidad a otros dominios de seguridad distintos del dominio de TI.

Dentro del dominio ITS, el modelo SSE-CMM se centra en los procesos utilizados para lograr la seguridad de la TI, más específicamente en la madurez de esos procesos. La intención es que la organización que hace uso del Modelo SSE-CMM debe usar sus procesos existentes, o sean aquellos basados en cualquier otro documento de orientación de ITS. El alcance abarca:

- Las actividades de ingeniería de seguridad del sistema para un producto seguro o un sistema confiable que aborde el ciclo de vida completo de: definición de conceptos, análisis de requisitos, diseño, desarrollo, integración, instalación, operación, mantenimiento y retiro.
- Los requisitos para desarrolladores de productos, desarrolladores e integradores de sistemas seguros, organizaciones que brindan servicios de seguridad informática e ingeniería de seguridad informática.
- Se aplica a todos los tipos y tamaños de organizaciones de ingeniería de seguridad, desde comerciales hasta gubernamentales y académicos.

La iniciativa SSE-CMM comenzó en abril de 1993 como una necesidad de contar con un modelo de capacidad para Ingeniería de la Seguridad, y en sus inicios fue patrocinado por la Agencia Nacional de Seguridad de los EE.UU. (NSA-National Security Agency), y en la actualidad también lo patrocinan la Oficina del Secretario de Defensa de los EE.UU. y el Centro de Investigación de la Seguridad para las Telecomunicaciones de Canadá (CST-Centre de la sécurité des télécommunications). La primera versión del modelo se publicó en octubre de 1996 y el

método de evaluación en abril de 1997, pero desde 1999 el organismo encargado del desarrollo y promoción del modelo es la Asociación Internacional de la Ingeniería de la Seguridad de los Sistemas (ISSEA International Systems Security Engineering Association), quién publicó la última versión (3.0) del modelo en junio del 2003. El SSE-CMM se ha desarrollado gracias a la colaboración de grupos de compañías con antecedentes de éxito en la construcción de sistemas seguros.

El SSE-CMM divide la Ingeniería de la Seguridad en tres áreas básicas: Riesgo, Ingeniería y Aseguramiento. Aunque estas áreas son dependientes unas de otras, es posible considerarlas de forma separada. En el nivel más simple, el proceso de Riesgo identifica y da prioridad a los peligros inherentes al producto o sistema desarrollado. El proceso de Ingeniería trabaja con las otras disciplinas de ingeniería para determinar e implementar soluciones a los problemas presentados por los peligros. Finalmente, el proceso de Aseguramiento establece la confianza en las soluciones de seguridad y transmite dicha confianza a los clientes.

Las prácticas base

El SSE-CMM contiene 129 prácticas base, organizadas en 22 áreas de proceso. De éstas, 61 prácticas están organizadas en 11 áreas de proceso que abarcan todas las áreas de la ingeniería de seguridad. Las 68 prácticas base restantes, organizadas en 11 áreas de proceso, abordan los dominios del proyecto y la organización.

Las once áreas de proceso de ingeniería de seguridad de sistemas son las siguientes:

- PA01 Administrar los controles de seguridad.
- PA02 Evaluar el impacto.
- PA03 Evaluar los riesgos de seguridad.
- PA04 Evaluar la amenaza.
- PA05 Evaluar la Vulnerabilidad.
- PA06 Construir argumento de aseguramiento.
- PA07 Coordinar la seguridad.
- PA08 Controlar la postura de seguridad.
- PA09 Proporcionar información de seguridad.
- PA10 Especificar las necesidades de seguridad.
- PA11 Verificar y validar la seguridad.

El SSE-CMM también incluye once áreas de proceso relacionadas con las prácticas de los proyectos y la organización. Estas áreas de proceso fueron adaptadas de SE-CMM:

- PA12 Asegurar la calidad.
- PA13 Gestionar la configuración.
- PA14 Gestión de los riesgos del proyecto.
- PA15 Supervisar y controlar el esfuerzo técnico.
- PA16 Planificar el esfuerzo técnico.
- PA17 Definir el proceso de ingeniería de sistemas de la organización.
- PA18 Mejorar el proceso de ingeniería de sistemas de la organización.
- PA19 Gestionar la evolución de la línea de productos.
- PA20 Gestionar el entorno de soporte de ingeniería de sistemas.
- PA21 Proporcionar habilidades y conocimientos continuos.
- PA22 Coordinar con los proveedores.

Las practicas genéricas

Las prácticas genéricas son actividades que se aplican a todos los procesos. Se dirigen a la dirección, medición e institucionalización de un proceso. En general, se utilizan durante una evaluación para determinar la capacidad de una organización para realizar un proceso.

Las prácticas genéricas se agrupan en áreas lógicas denominadas "Características Comunes" que están organizadas en cinco niveles de capacidad, que representan una creciente capacidad organizativa. A diferencia de las prácticas base de la dimensión del dominio, las prácticas genéricas de la dimensión de capacidad se ordenan de acuerdo a la madurez. Por lo tanto, las prácticas genéricas que indican niveles más altos de capacidad de proceso se encuentran en la parte superior de la dimensión de capacidad.

Las características comunes están diseñadas para describir los principales cambios en la forma característica de la organización de realizar procesos de trabajo (en este caso, el dominio de ingeniería de seguridad). Cada característica común tiene una o más prácticas genéricas. Estas características comunes simplemente verifican si una organización realiza todas las prácticas base en un área de proceso.

De la misma manera, las características comunes tienen prácticas genéricas que ayudan a determinar qué tan bien un proyecto gestiona y mejora cada área de proceso como un todo. Las prácticas genéricas se agrupan para enfatizar cualquier cambio importante en la manera de hacer las cosas dentro de una organización.

Los niveles de capacidad

Las características comunes y los niveles de capacidad son importantes, tanto para realizar una evaluación como para mejorar la capacidad de proceso de una organización. En el caso de una evaluación en la que una organización tiene algunas, pero no todas, funciones comunes implementadas en un nivel de capacidad particular para un proceso en particular, la organización generalmente está operando en el nivel de capacidad completado más bajo para ese proceso. Por ejemplo, una organización que realiza todas menos una de las prácticas genéricas de Nivel 2 para algún área de proceso debe recibir una calificación de Nivel 1. Una organización puede no obtener todos los beneficios de haber implementado una función común si está implementada, pero no todas las funciones comunes con niveles de capacidad más bajos. Un equipo de evaluación debe tener esto en cuenta al evaluar los procesos individuales de una organización.

Los niveles de capacidad que describe este modelo son:

- Nivel 1. "Realizado informalmente", se enfoca en si una organización o proyecto realiza un proceso que incorpora las prácticas base.
- Nivel 2. "Planificado y seguido", se centra en la definición, planificación y problemas de rendimiento a nivel de proyecto.
- Nivel 3. "Bien definido", se centra en la adaptación disciplinada de procesos definidos a nivel de organización.
- Nivel 4. "Controlado cuantitativamente", se enfoca en las mediciones que están vinculadas a los objetivos comerciales de la organización. Si bien es esencial comenzar a recopilar y usar medidas básicas del proyecto de manera temprana, no se espera que la medición y el uso de los datos se extiendan a toda la organización hasta que se hayan alcanzado los niveles más altos.
- Nivel 5. "Mejora Continua", aprovecha las ventajas de todas las mejoras en la práctica administrativa observadas en los niveles anteriores, y luego enfatiza los cambios culturales que sostendrán los logros obtenidos.

En la Tabla 2-5, se describen los niveles de madurez, las características comunes y las prácticas genéricas.

Tabla 2-5. Niveles de madurez de SSE-CMM

<i>Nivel de madurez</i>	<i>Prácticas comunes</i>	<i>Prácticas Genéricas</i>
Nivel 1 Realizado informalmente	CC 1.1 Las prácticas base son realizadas	GP 1.1.1 Realizar el proceso
	CC 2.1 Planificación de la ejecución	GP 2.1.1. Asignar recursos

<i>Nivel de madurez</i>	<i>Prácticas comunes</i>	<i>Prácticas Genéricas</i>
Nivel 2 Planificado y seguido		GP 2.1.2 Asignar responsabilidades
		GP 2.1.3 Documentar el proceso
		GP 2.1.4 Proporcionar herramientas
		GP 2.1.5 Asegurar el entrenamiento
		GP 2.1.6 Planificar el proceso
	CC 2.2 Ejecución disciplinada	GP 2.2.1 Utilizar planes estándares y procedimientos
		GP 2.2.2 Gestión de la configuración
	CC 2.3 Verificar la ejecución	GP 2.3.1 Verificar el cumplimiento del proceso
		GP 2.1.2 Auditar los productos de trabajo
	CC 2.4 Dar seguimiento a la ejecución	GP 2.4.1 Dar seguimiento usando métricas
		GP 2.4.2 Tomar acciones correctivas
Nivel 3 Bien definido	CC 3.1 Definición de un proceso estándar	GP 3.1.1 Estandarizar el proceso
		GP 3.1.2 Adaptar el proceso estándar
	CC 3.2 Ejecutar el proceso definido	GP 3.2.1 Usar un proceso bien definido
		GP 3.2.2 Realizar revisiones de defectos
		GP 3.2.3 Usar datos bien definidos
	CC 3.3 Coordinar las prácticas de seguridad	GP 3.3.1 Realizar la coordinación intra-grupal
		GP 3.3.2 Realizar la coordinación entre grupos
		GP 3.3.3 Realizar la coordinación externa
Nivel 4 Controlado cuantitativamente	CC 4.1 Establecimiento de objetivos medibles en la calidad	GP 4.1.1 Establecer objetivos de calidad
	CC 4.2 Gestionar de forma objetiva la ejecución	GP 4.2.1 Determinar la capacidad del proceso
		GP 4.2.2 Usar capacidad de proceso
Nivel 5 Mejorado continuamente	CC 5.1 Mejorar la capacidad de la organización	GP 5.1.1 Establecer objetivos de eficacia del proceso
		GP 5.2.2 Mejora continua del proceso estándar
	CC 5.2 Mejorar la eficacia del proceso	GP 5.3.1 Realizar análisis causal
		GP 5.3.2 Eliminar las causas de defecto
		GP 5.3.3 Mejora continua del proceso definido

Aplicación del Modelo

El SSE-CMM se aplica a todas las organizaciones que practican alguna forma de ingeniería de la seguridad, sin considerar el ciclo de vida, alcance, contexto o especialidad. El modelo puede aplicarse de tres formas generales:

- La “mejora de proceso” permite a una organización de ingeniería de la seguridad obtener una idea sobre su nivel de capacidad de proceso de ingeniería de la seguridad, para diseñar procesos mejorados de ingeniería de la seguridad, y para mejorar su capacidad de proceso de ingeniería de la seguridad.
- La “evaluación de la capacidad” permite a una organización consumidora comprender la capacidad de proceso de ingeniería de la seguridad de una organización proveedora.
- El “aseguramiento” incrementa la confianza en que un producto, sistema o servicio es seguro para soportar demandas con evidencia de que se utilizó un proceso maduro.

El modelo SSE-CMM y el método para aplicar el modelo tratan de que se utilicen como:

- Herramienta para las organizaciones de ingeniería para evaluar sus prácticas de ingeniería de la seguridad y definir las mejoras a ellas.
- Base para las organizaciones de evaluación de la ingeniería de la seguridad (por ejemplo, certificadores de sistemas o evaluadores de productos), con objeto de establecer confidencias organizativas basadas en la capacidad.
- Mecanismo estándar para que los clientes evalúen un proveedor de capacidad de ingeniería de la seguridad.

Las técnicas de evaluación pueden utilizarse en la aplicación del modelo para la auto mejora y en la selección de los proveedores.

2.1.2.5 Community Cyber Security Maturity Model (CCSMM)

Desarrollado por el Centro de Aseguramiento y Seguridad de Infraestructura (CIAS, Center for Infrastructure Assurance and Security), el Modelo de Madurez de Seguridad Cibernética de la Comunidad (CCSMM) está diseñado para atender las necesidades de los estados y comunidades para desarrollar un programa viable y sostenible de ciberseguridad. El CCSMM proporciona un "criterio" para determinar la postura actual de ciberseguridad, una "hoja de ruta" para ayudar a mejorar esa postura y un punto de referencia común para compartir experiencias y lecciones aprendidas. La única versión del modelo (1.0) fue publicada en el año 2006 (White, 2011).

El modelo identifica las características de las comunidades y los estados a medida que maduran sus programas de seguridad cibernética. Utiliza aspectos como el conocimiento de la ciberseguridad, las políticas y procedimientos de seguridad, el intercambio de información dentro de las organizaciones y, entre ellas, la formación y la educación en materia de seguridad cibernética.

Los estados se componen de comunidades y las comunidades están compuestas de organizaciones, y el modelo responde a la vinculación que existe entre el estado, la comunidad y las organizaciones. Hay cinco niveles en el modelo CCSMM para las organizaciones, comunidades y estados que progresan en orden por cada nivel como se muestra en la

Tabla 2-6.

Tabla 2-6. Niveles de madurez de CCSMM

<i>Nivel de Madurez</i>	<i>Característica del nivel</i>
Nivel 1, “Inicial”	Las organizaciones, las comunidades y los estados de este nivel tienen poca o ninguna conciencia de seguridad cibernética, análisis y evaluaciones.
Nivel 2, “Establecido”	El liderazgo de organizaciones, comunidades y estados a este nivel es consciente de las amenazas cibernéticas, los problemas y el imperativo de adoptar la ciberseguridad. También, reconocen la necesidad de capacitación y educación cooperativa en seguridad cibernética.
Nivel 3, “Autoevaluado”	En este nivel, los líderes dentro de las organizaciones, las comunidades y los estados promueven activamente la conciencia de seguridad cibernética y cooperan con otros en el establecimiento de programas de capacitación y educación.

<i>Nivel de Madurez</i>	<i>Característica del nivel</i>
Nivel 4, “Integrado”	Cuando la seguridad cibernética está integrada, se incorpora en cada proceso que tiene una organización, comunidad o estado.
Nivel 5, “Vanguardia”	Para las organizaciones, comunidades y estados a este nivel, la seguridad cibernética es un imperativo empresarial. Entidades a este nivel son capaces de enseñar a otros.

Este modelo realiza una evaluación de alto nivel por estar enfocado a los estados, comunidades y organizaciones, siendo general en cuanto a los procesos organizacionales. El modelo se representa de manera tridimensional, tal como se muestra en la Figura 2-5.

Hay cinco niveles en el CCSMM y las organizaciones, comunidades y estados progresan a través de cada uno de los cinco niveles en orden. La transición de un nivel a otro se conoce como una fase y, por lo tanto, hay cuatro fases en el modelo.

Figura 2-5. Modelo de madurez CCSMM (Fuente: White, 2011)

Como se observa en los niveles anteriores, el modelo está orientado para evaluar la ciberseguridad en comunidades y estados que puede adaptarse a grupos dentro de las organizaciones.

Aplicación del Modelo

Actualmente, CCSMM es el único modelo viable desarrollado para abordar el problema nacional de seguridad cibernética a nivel estatal y local y, por lo tanto, brinda la mejor oportunidad para que un país desarrolle un enfoque organizado para tratar con la ciberseguridad en todo el país. El CIAS da apoyo a los estados que puedan estar interesados en desarrollar sus propios programas.

2.1.3. Estudio Comparativo Modelos de Madurez en ciberseguridad -CCMM

Estos modelos de madurez analizados tienen características y cualidades muy particulares, con enfoques a áreas diferentes en algunos casos y comunes en otros. Para determinar de estos modelos, cuáles de ellos están orientados a ciberseguridad, se ha realizado un estudio comparativo entre ellos, y los resultados encontrados se presentan a continuación.

Para que las organizaciones puedan mejorar sus prácticas de ciberseguridad, la industria y la comunidad técnica han desarrollado modelos de madurez de capacidad de ciberseguridad que permiten medir las capacidades de ciberseguridad de las organizaciones y posicionarlas en

diferentes niveles. Existen modelos de madurez de capacidad de ciberseguridad desarrollados por la industria, en muchos casos desarrollados por entidades estatales con el propósito de ser estándares nacionales / internacionales. Por lo tanto, las organizaciones han decidido desarrollar modelos de madurez de capacidades de ciberseguridad que respondan a sus necesidades particulares. Por lo tanto, es importante responder las siguientes preguntas:

¿Cuáles son las principales capacidades de ciberseguridad y los modelos de madurez utilizados en los estudios de investigación? Esta pregunta ya fue respondida en la RS (Rea-Guaman et al., 2017).

¿Cuáles son las diferencias entre los principales modelos de madurez de la ciberseguridad? Esta pregunta es el enfoque de este apartado. Por lo tanto, el presente análisis se realiza para identificar las principales diferencias, ventajas y desventajas de los modelos de madurez más utilizados en los estudios de investigación, a partir de la revisión sistemática (Rea-Guaman et al., 2017) donde previamente se identificaron cuáles son los modelos más utilizados en los estudios de investigación, teniendo en cuenta que se podrían haber omitir modelos que se están utilizando en la industria, pero que no son mencionados en los estudios de investigación.

A continuación, se describe la metodología de investigación del estudio comparativo, así como la métrica para la comparación y, finalmente, se muestran los resultados y conclusiones obtenidos del estudio comparativo de los modelos de madurez de la capacidad de ciberseguridad.

Metodología utilizada para realizar el estudio comparativo

A partir de los resultados de la revisión sistemática anterior (Rea-Guaman et al., 2017), se identificaron los modelos de ciberseguridad más relevantes, a saber: SSE-CMM, C2M2, CCSMM y NICE. La metodología para poder llevar a cabo el estudio comparativo de los modelos mencionados se ha basado en la taxonomía de los entornos de mejora de software propuesta por Halvorsen y Conradi (Halvorsen & Conradi, 2001).

La taxonomía descrita por Halvorsen y Conradi (Halvorsen & Conradi, 2001) proporciona una lista de veinticinco características relevantes para la comparación de los marcos de mejora de procesos de software (SPI, Software Process Improvement). Las características se agrupan en cinco (5) categorías. Las cinco categorías se describen a continuación:

- General: esta categoría incluye las características que describen los atributos generales del entorno de mejora.
- Proceso: esta categoría incluye las características que describen cómo se usa el entorno.
- Organización: esta categoría incluye las características que describen cómo es la relación entre las características relacionadas con los atributos de la organización y el entorno en el que se utiliza.
- Calidad: esta categoría incluye las características relacionadas con la dimensión de calidad que indica: aspectos para la medición de calidad, qué perspectiva de calidad se usa y qué significa calidad en términos de indicadores de calidad.
- Resultado: esta categoría incluye las características que describen los resultados del uso del entorno, los costos de lograr los resultados y los métodos utilizados para su validación.

La Figura 2-6 muestra las categorías y características de la taxonomía original de Halvorsen y Conradi (Halvorsen & Conradi, 2001), diseñadas para comparar entornos de mejora de procesos. Esta taxonomía fue adaptada para ser aplicada en la comparación de los modelos de madurez de capacidad de ciberseguridad. Para la taxonomía adaptada, las categorías de calidad y resultado fueron rechazadas porque las características de estas categorías están presentes en todos los modelos y no permitieron la comparación de los modelos de madurez de capacidad de ciberseguridad. Además, todos los modelos tienen en común la capacidad de:

- Tratar procesos de evaluación y mejora, enfocarse en la mejora continua y proporcionar resultados que permitan la toma de decisiones.
- Tener características similares tanto en calidad como en el tipo de resultados obtenidos.
- Tener procesos similares.

Se redefinieron las características de las categorías General, Proceso y Organización. En la categoría General, se definieron las siguientes características:

- Orientada a la seguridad cibernética: si el modelo de madurez está diseñado para la ciberseguridad. Esta característica es fundamental para considerar qué modelos fueron diseñados para la ciberseguridad y cuáles no.
- Año de la última revisión: última revisión del modelo. Este punto puede proporcionar información sobre la evolución actual del modelo debido al constante cambio que existe en la ciberseguridad.
- Entorno organizacional: si el modelo de madurez de la capacidad de ciberseguridad se centra en toda la organización o no. Este punto proporciona información sobre si el modelo se generó para una necesidad específica de ciberseguridad o para todos los entornos organizacionales.
- Compatibilidad con el marco NIST: si el modelo de madurez de la capacidad de ciberseguridad tiene un marco de seguridad asociado. Con base en la revisión sistemática (Rea-Guaman et al., 2017), seleccionamos el marco NIST porque es el más utilizado con los modelos de madurez de la capacidad de ciberseguridad.
- Mide la gestión de riesgos (amenazas y vulnerabilidades de ciberseguridad): si el modelo de madurez mide la gestión de riesgos de forma específica o general.

Figura 2-6. Taxonomía para comparar entornos de mejora de procesos (Fuente: Halvorsen & Conradi, 2001).

En relación con la categoría Proceso, se han tenido en cuenta las siguientes características:

- Área de mejora: el área de implementación del modelo que es útil para comprender los objetivos del modelo.

- Profundidad: depende de la complejidad de la validación utilizada. Este punto nos ayuda a diferenciar entre los modelos que tienen un mayor detalle en los respectivos niveles de madurez y los que son simples en este aspecto.

En relación con la categoría Organizacional, se han tenido en cuenta las siguientes características:

- Definición de roles y responsabilidades: si el modelo de madurez de la capacidad de ciberseguridad tiene roles y funciones bien definidos. Esto nos ayuda a saber qué modelo tiene una mejor estructura de qué persona debe hacer cada actividad.
- Nivel de documentación para la implementación: si hay alguna documentación para apoyar y ayudar en la implementación del modelo. De esta manera, podemos saber en qué nivel de detalle hay información para la implementación del modelo.

Cada característica se ha evaluado de la siguiente manera:

- Orientada a la seguridad cibernética. Esta característica se evalúa con un "SÍ", si se trata de un modelo orientado a la ciberseguridad, y con un "NO", en caso contrario.
- Año de la última revisión. En esta función, se evalúa el último año de la revisión, cuanto más reciente es, mejor.
- Ambiente organizacional. Si el modelo se enfoca en toda la organización, se evalúa con "SÍ". En el caso de que esté enfocado en un área específica de la organización, se evalúa con "NO".
- Compatibilidad con el marco NIST. En caso de que el modelo sea compatible con el marco NIST, se evalúa con "SÍ", y en el caso opuesto, con "NO".
- Áreas de mejora: esta característica se representa con el nombre del área a la que se dirigió el modelo desde su creación.
- Profundidad. Esta característica se evalúa como "GENERAL" si solo hay una evaluación de primer nivel dentro de los niveles de madurez. También se considera como "ESPECÍFICO" si el modelo tiene un segundo nivel de evaluación en los niveles de madurez.
- Mide la gestión de riesgos (amenazas y vulnerabilidades de ciberseguridad). Esta característica se considera como "GENERAL" si no se realiza una evaluación de riesgo directa. En el caso de evaluación de riesgo directa, se evalúa como "ESPECÍFICO".
- Definición de roles y responsabilidades. Si hay roles y perfiles bien definidos en el modelo, se evalúa con "SÍ", de lo contrario con "NO".
- Nivel de documentación para implementación. El nivel del documento se considera "ALTO" si tiene un documento técnico, una guía de implementación y documentos relacionados. El nivel de documentación se considera "MEDIO" si tiene una documentación y documentos relacionados. El nivel de documentación se considera "BAJO" si solo tiene documentos introductorios.

Resultados y análisis

Tomando las características que se han definido previamente para evaluar los modelos de madurez en ciberseguridad de acuerdo con la revisión sistemática (Rea-Guaman et al., 2017), se ha realizado una tabla que resume la comparación entre ellos. La

Tabla 2-7 muestra el resumen de las características de cada uno de los modelos (C2M2, NICE, CCSMM y SSE-CMM).

El estudio comparativo muestra que los modelos de madurez de capacidad de ciberseguridad tienen una similitud significativa. La principal diferencia que se identifica es el área en la que se centran y el nivel de profundidad de las mejores prácticas que se implementarán. Para analizar los modelos de madurez se ha buscado en los documentos originales el área en el que se centran los modelos, si fueron concebidos para la ciberseguridad o si fueron enfocados para otra área.

Tabla 2-7. Comparación entre los modelos de madurez de la capacidad de ciberseguridad

CATEGORIAS	CARACTERISTICAS	C2M2	NICE	CCSMM	SSE-CMM
General					
	Orientado a Ciberseguridad	SI	SI	SI	NO
	Año de la última revisión	2019	2014	2006	2008
	Entorno Organizacional	SI	NO	NO	S
	Compatibilidad con el marco del NIST	SI	NO	SI	NO
	Mide la gestión del riesgo (amenazas y vulnerabilidades)	ESPECÍFICO	GENERAL	GENERAL	ESPECÍFICO
Procesos					
	Sectores de aplicación	Energía y Combustibles	Personal	Comunidades	Ingeniería de Seguridad
	Profundidad	ESPECÍFICA	GENERAL	GENERAL	ESPECÍFICA
Organización					
	Definición Roles y Responsabilidades	SI	SI	NO	SI
	Nivel de documentación para la implementación	MEDIO	MEDIO	BAJO	ALTO

Los principales resultados encontrados en la comparación son los siguientes:

- Para los modelos analizados (CMU, 2003) (Christopher, 2014) (White, 2011) (US Department of Homeland Security, 2014), se buscó en los documentos oficiales así como documentos adicionales, las áreas en las que se centran los modelos, si se concibieron para la ciberseguridad o para otra área y si se adaptaron para su uso en ciberseguridad.
- Los modelos más generales (C2M2 y SSE-CMM) cubren todas las áreas de la organización, y cubren todos los atributos de seguridad (confidencialidad, integridad y disponibilidad) (Department of Energy, 2019) (White, 2011).
- En los modelos analizados (CMU, 2003) (Christopher, 2014) (White, 2011) (US Department of Homeland Security, 2014), hay modelos cuyas características de evaluación son muy generales (NICE, CCSMM) en comparación con otras (C2M2, SSE-CMM). Los modelos más específicos proporcionan más información para la clasificación y evaluación adecuada de sus prácticas y proporcionan directrices más detalladas para mejorar los niveles de indicadores de madurez.

Conclusiones de la comparativa de modelos de madurez en ciberseguridad

Todos los modelos se pueden adaptar a diferentes tipos de organizaciones, sin embargo, necesitan cierto nivel de personalización. Hay modelos, como C2M2 y CCSMM, que están diseñados para implementarse junto con el marco NIST.

No se han identificado actualizaciones recientes de los modelos NICE, CCSMM, SSE-CMM comparados en el presente trabajo en los últimos 3 años, el único modelo de madurez que ha

presentado una nueva versión es el modelo C2M2, que liberó la versión 2.0 en julio de 2019, fecha posterior al estudio comparativo.

El único modelo de madurez de la capacidad de ciberseguridad que se centra en la ciberseguridad, uno de los más actualizados y que se centra en toda la organización es el C2M2.

El modelo SSE-CMM es un modelo que ya tiene varios años en el mercado, pero no se enfoca directamente en la ciberseguridad, aunque se ha utilizado en esta área.

Además, se ha identificado que todos los modelos de madurez de capacidad de ciberseguridad necesitan un nivel de personalización para implementarse en una organización.

Todos los modelos de madurez de capacidad de ciberseguridad se basan en la gestión de riesgos de ciberseguridad, pero solo SSE-CMM y C2M2 miden la gestión de riesgos de una manera más específica.

2.1.4. Un Modelo de Madurez en Ciberseguridad

El Gobierno de los Estados Unidos, a través de la Subsecretaría de Defensa para la Adquisición y el Mantenimiento (OUSD (A&S), Office of the Under Secretary of Defense for Acquisition and Sustainment) ha desarrollado, y publicado en marzo de 2020, el marco de Certificación del Modelo de Madurez de Ciberseguridad (CMMC, Cybersecurity Maturity Model Certification) en acuerdo con el Departamento de Defensa, los Centros de Investigación Afiliados de la Universidad (UARC, University Affiliated Research Centers) (US Department of Defense, 2019).

El modelo CMMC mide la madurez de la ciberseguridad en cinco niveles y alinea un conjunto de procesos y prácticas con el tipo y la sensibilidad de la información a proteger y el rango asociado de amenazas. El modelo consta de procesos de madurez y mejores prácticas de ciberseguridad de múltiples estándares, marcos y otras referencias de ciberseguridad, así como también aportes de la comunidad en general. El marco CMMC agrega un elemento de certificación para verificar la implementación de procesos y prácticas asociadas con el logro de un nivel de madurez de ciberseguridad.

El marco del modelo (Figura 2-7) organiza estos procesos y prácticas en un conjunto de dominios y los asigna en cinco niveles. Para proporcionar una estructura adicional, el marco también alinea las prácticas con un conjunto de capacidades dentro de cada dominio.

Figura 2-7. Marco del modelo CMMC (vista jerárquica simplificada) (Fuente: US Department of Defense, 2019).

El modelo CMMC mide la madurez de ciberseguridad con cinco niveles. Cada uno de estos niveles, a su vez, consiste en un conjunto de procesos y prácticas como se describen en la Figura 2-8. Los procesos van desde "Realizado" en el Nivel 1 hasta "Optimizando" en el Nivel 5, y las prácticas van desde "Higiene Cibernética Básica" en el Nivel 1 hasta "Avanzado / Progresivo" en el Nivel 5.

Los niveles de CMMC y los conjuntos asociados de procesos y prácticas entre dominios son acumulativos. Más específicamente, para que una organización alcance un nivel CMMC específico, también debe demostrar el logro de los niveles anteriores. Los niveles de CMMC se caracterizan de la siguiente manera:

Figura 2-8. Niveles y descripciones de CMMC (Fuente: US Department of Defense, 2019).

- Nivel 1: salvaguardar la información del contrato federal (FCI, Federal Contract Information).
- Nivel 2: servir como paso de transición en la progresión de madurez de ciberseguridad para proteger CUI (Controlled Unclassified Information).
- Nivel 3: proteger la información no clasificada controlada (CUI, Controlled Unclassified Information)
- Niveles 4-5: proteger la CUI y reducir el riesgo de ciberseguridad de amenazas persistentes avanzadas (APT, Advanced Persistent Threat).

El logro de los niveles CMMC más altos mejora la capacidad de una organización para proteger CUI. Para los niveles 4-5, reduce el riesgo de APT (Figura 2-9). Un APT es un adversario que posee niveles sofisticados de experiencia y recursos significativos que le permiten crear oportunidades para lograr sus objetivos mediante el uso de múltiples vectores de ataque (por ejemplo, cibernético, físico y engaño).

Figura 2-9. Niveles de CMMC y enfoque asociado (Fuente: US Department of Defense, 2019).

El modelo CMMC consta de 17 dominios. La mayoría de estos dominios se originan en las áreas relacionadas con la seguridad. En estos 17 dominios se incluyen los dominios de Gestión de

activos (AM, Asset Management) y Gestión de Riesgos (RM, Risk Management). Estos dominios y sus abreviaturas se muestran en la Figura 2-10 a continuación.

Figura 2-10. Dominios CMMC (Fuente: US Department of Defense, 2019).

Como se ha indicado anteriormente (Figura 2-7), cada dominio consta de un conjunto de procesos y capacidades (y, a su vez, prácticas) en los cinco niveles. La Tabla 2-8 detalla las 43 capacidades asociadas con los 17 dominios en el modelo CMMC.

Tabla 2-8. Capacidades CMMC

DOMINIO	CAPACIDAD
Control de Acceso (AC)	<ul style="list-style-type: none"> • Establecer requisitos de acceso al sistema. • Controlar el acceso al sistema interno. • Controlar el acceso remoto al sistema. • Limitar el acceso a los datos a usuarios y procesos autorizados.
Gestión de Activos (AM)	<ul style="list-style-type: none"> • Identificar y documentar activos. • Administrar inventario de activos.
Auditoría y Responsabilidad (AU)	<ul style="list-style-type: none"> • Definir los requisitos de auditoría. • Realizar auditorías. • Identificar y proteger la información de auditoría. • Revisar y administrar registros de auditoría.
Conciencia y Entrenamiento (AT)	<ul style="list-style-type: none"> • Realizar actividades de sensibilización sobre seguridad. • Entrenamiento de la conducta.
Gestión de Configuración (CM)	<ul style="list-style-type: none"> • Establecer líneas bases de configuración. • Realizar la configuración y la gestión de cambios.
Identificación and Autenticación (IA)	<ul style="list-style-type: none"> • Conceder acceso a entidades autenticadas.
Respuesta a Incidentes (IR)	<ul style="list-style-type: none"> • Planificar respuesta a incidentes. • Detectar e informar de eventos. • Desarrollar e implementar una respuesta a un incidente declarado. • Realizar revisiones posteriores al incidente. • Prueba de respuesta a incidentes.
Mantenimiento (MA)	<ul style="list-style-type: none"> • Gestionar mantenimiento.

DOMINIO	CAPACIDAD
Protección de Medios (MP)	<ul style="list-style-type: none"> • Identificar y marcar medios. • Proteger y controlar los medios. • Desinfectar los medios. • Proteger los medios durante el transporte.
Personal de Seguridad (PS)	<ul style="list-style-type: none"> • Personal de pantalla. • Proteger el CUI durante las acciones del personal.
Protección Física (PE)	<ul style="list-style-type: none"> • Limitar el acceso físico.
Recuperación (RE)	<ul style="list-style-type: none"> • Administrar copias de seguridad. • Gestionar la continuidad de la seguridad de la información.
Gestión de Riesgos (RM)	<ul style="list-style-type: none"> • Identificar y evaluar el riesgo. • Gestionar riesgos. • Gestionar el riesgo de la cadena de suministro.
Evaluación de Seguridad (CA)	<ul style="list-style-type: none"> • Desarrollar y administrar un plan de seguridad del sistema. • Definir y administrar controles. • Realizar revisiones de código.
Conciencia Situacional (SA)	<ul style="list-style-type: none"> • Implementar monitoreo de amenazas.
Protección de Sistemas y Comunicaciones (SC)	<ul style="list-style-type: none"> • Definir requisitos de seguridad para sistemas y comunicaciones. • Controlar las comunicaciones en los límites del sistema.
Sistema e Integridad de la Información (SI)	<ul style="list-style-type: none"> • Identificar y gestionar fallas del sistema de información. • Identificar contenido malicioso • Realizar monitoreo de redes y sistemas • Implemente protección avanzada de correo electrónico

Dentro del contexto del modelo CMMC, la institucionalización del proceso proporciona garantías adicionales de que las prácticas asociadas con cada nivel se implementan de manera efectiva. El modelo CMMC consta de cinco niveles de madurez que abarcan los niveles de madurez (ML, Maturity Level) 2-5 y se aplican a todos los dominios (Tabla 2-9).

Tabla 2-9. Procesos CMMC

NIVEL DE MADUREZ (ML)	DESCRIPCION DEL NIVEL DE MADUREZ	PROCESOS
ML 1	Realizados	No hay procesos de madurez evaluados en el Nivel de madurez 1. Una organización realiza prácticas de Nivel 1 pero no tiene requisitos de institucionalización de procesos
ML2	Documentados	Establezca una política que incluya [NOMBRE DE DOMINIO]
		Documente las prácticas de CMMC para implementar la política del [NOMBRE DE DOMINIO]
ML3	Gestionados	Establezca, mantenga y ofrezca un plan que incluya [NOMBRE DE DOMINIO]

<i>NIVEL DE MADUREZ (ML)</i>	<i>DESCRIPCION DEL NIVEL DE MADUREZ</i>	<i>PROCESOS</i>
ML4	Revisados	Revise y mida las actividades de [NOMBRE DE DOMINIO] para determinar su efectividad
ML5	Optimizando	Estandarice y optimice un enfoque documentado para [NOMBRE DE DOMINIO] en todas las unidades organizativas aplicables

Los procesos de madurez de CMMC institucionalizan las actividades de seguridad cibernética para garantizar que sean consistentes, repetibles y de alta calidad. Las prácticas de CMMC proporcionan un rango de mitigación en todos los niveles, comenzando con la protección básica en el Nivel 1, pasando a la protección amplia de Información Controlada No Clasificada (CUI) en el Nivel 3, y culminando con la reducción del riesgo de Amenazas Persistentes Avanzadas (APT) en Niveles 4 y 5. El marco CMMC se combina con un programa de certificación para verificar la implementación de procesos y prácticas.

2.1.5. Consideraciones Finales de Modelos de Madurez en Ciberseguridad

En esta sección se ha realizado una revisión sistemática de los modelos de madurez en ciberseguridad, analizando qué modelos de madurez (de los obtenidos en la revisión sistemática) son los más nombrados en los estudios científicos en la actualidad. Además, se han descrito los cuatro modelos de madurez más nombrados, analizando el enfoque, aplicación y estructura de cada modelo de madurez. Posteriormente, se ha realizado un estudio comparativo de los cuatro modelos de madurez descritos y analizados, para poder establecer las características comunes y diferencias notables de los mismos.

De lo descrito anteriormente, los aspectos más importantes encontrados son los siguientes:

- Los modelos más nombrados en los estudios científicos y que se pueden utilizar en ciberseguridad son: SSE-CMM, C2M2, CCSMM, NICE-CMM.
- El modelo de madurez de la capacidad de ciberseguridad, C2M2, es el único que se enfoca en la ciberseguridad, se actualiza de forma continua y permite abarcar a toda la organización.
- Todos los modelos de madurez más nombrados en los artículos científicos se basan en la gestión de riesgos de ciberseguridad en el nivel inicial de madurez.
- También se ha descrito un nuevo Modelo de Madurez de Ciberseguridad (CMMC), que ha sido publicado en marzo del 2020, y que dentro de sus procesos considera a la Gestión de Riesgos.

Por ello, se ha considerado realizar una segunda revisión sistemática sobre riesgos en ciberseguridad.

2.2. Riesgos en Ciberseguridad

En la sección anterior se ha realizado un estudio comparativo de los modelos de madurez a partir de los resultados de la revisión sistemática anterior (Rea-Guaman et al., 2017), en la cual uno de los resultados más importante fue: “Todos los modelos de madurez más nombrados en los artículos científicos se basan en la gestión de riesgos de ciberseguridad en el nivel inicial de madurez”.

Por lo mencionado, en esta sección se ha realizado una revisión de los principales conceptos de riesgos en ciberseguridad, en los que se incluyen las consideraciones de vulnerabilidades, amenazas y riesgos en ciberseguridad, así como el análisis y mitigación de riesgos en ciberseguridad. También se describen los resultados de la revisión sistemática que se ha realizado respecto a taxonomías de riesgos en ciberseguridad. Además, también se describen algunos

modelos conceptuales de riesgos en ciberseguridad analizados. Finalmente, se han realizado revisiones sistemáticas adicionales sobre taxonomías de activos, y de vulnerabilidades y de amenazas en ciberseguridad.

2.2.1. Principales Conceptos de Riesgos en Ciberseguridad

Una definición de riesgo de acuerdo con ISACA (Information Systems Audit and Control Association) es: "la combinación de la probabilidad de un evento y su consecuencia" (ISACA, 2016). Ésta es una definición que se aplica a cualquier campo, ya sea un riesgo ambiental, un riesgo de trabajo o un riesgo en el campo de las tecnologías de la información.

Independientemente de los desafíos de ciberseguridad, hay elementos fundamentales en los que toda la literatura principal está de acuerdo (Donaldson, Siegel, Williams, & Abdul, 2015). El elemento fundamental es el proceso de gestión de riesgos. Hay libros enteros dedicados a la gestión de riesgos, aunque el enfoque en ciberseguridad es aún incipiente. A continuación, se presenta un resumen de los puntos clave del proceso de gestión de riesgos. El proceso simplificado de gestión de riesgos puede actuar como punto de partida y puede adaptarse a las necesidades empresariales específicas, aunque el proceso esté orientado a un proceso de riesgos en toda la organización puede ser utilizado para el enfoque de ciberseguridad.

El proceso de gestión de riesgos implica un análisis sistemático para determinar dónde una empresa puede tener comprometidos sus elementos, las consecuencias de estos comprometimientos y la estimación del grado de exposición a que una amenaza materialice las vulnerabilidades de uno o más activos causando daños o perjuicios a la organización, y las maneras de reducir la probabilidad o la gravedad de esas consecuencias. Como se muestra en la Figura 2-11, el proceso de gestión de riesgos se representa, a continuación, simplemente y puede adaptarse a necesidades empresariales específicas.

Figura 2-11. Proceso simplificado de gestión de riesgos

- La gestión de riesgos comienza con los "activos", que son las cosas que la empresa quiere proteger. Generalmente (Donaldson et al., 2015), hay cuatro tipos de activos de interés: *personal*, *instalaciones*, *procesos* e *información*. El personal es la gente en la organización, y sus conocimientos y habilidades. Las instalaciones son los lugares donde las personas trabajan, y las herramientas y equipos que hay en esos lugares. Los procesos son los procedimientos por los cuales la organización opera y los sistemas que utiliza para lograr sus objetivos. La información son los datos de la empresa, ya sean propietarios, clientes o datos empresariales. Todos estos activos deben ser protegidos.
- El siguiente paso de la gestión de riesgos es considerar las "vulnerabilidades", que son las diferentes formas en las que los activos pueden verse comprometidos. Por ejemplo, una vulnerabilidad es que la instalación de la organización esté adyacente a un edificio abandonado. Una vulnerabilidad para un proceso de negocio puede ser que se base en un sistema de TI que sea extremadamente poco fiable. Las vulnerabilidades de los sistemas informáticos pueden caracterizarse además en términos de la "CIA" (Confidencialidad, Integridad y Disponibilidad) de la ciberseguridad:
 - Confidencialidad, que significa proteger el secreto de los datos.
 - Integridad, que significa proteger los datos de cambios no autorizados.
 - Disponibilidad, es decir, la disponibilidad de sistemas informáticos y de los datos que los sistemas alojan a aquellos que necesitan los datos cuando se necesitan.
- El siguiente paso de la gestión de riesgos es considerar las "amenazas", que son maneras en que las vulnerabilidades pueden ser explotadas para causar daño al activo. Las

amenazas pueden ser naturales o provocadas por el hombre, accidentales o deliberadas, aleatorias o deterministas.

Considerar las amenazas es uno de los pasos más creativos en el proceso de gestión de riesgos. Considerar amenazas implica un montón de "pensamiento de la ley de Murphy" (¿Qué puede salir mal?) Y pensar como atacantes (¿Qué vulnerabilidades pueden ser explotadas?). Es útil pensar en amenazas en cuanto a cómo afectarían a la confidencialidad, integridad y disponibilidad de los sistemas de información e información de la empresa.

- El siguiente paso de la gestión de riesgos es identificar y evaluar los riesgos. Combinando amenazas con vulnerabilidades, los riesgos pueden ser identificados. Una amenaza contra un área bien protegida generalmente produce un bajo nivel de riesgo, mientras que una amenaza contra un área donde la empresa no está bien protegida, produce un riesgo que debe ser considerado.

Desafortunadamente, identificar y evaluar los riesgos es fundamentalmente una decisión. Hay dos desafíos aquí: primero, subestimar el riesgo porque la vulnerabilidad es subestimada y, segundo, perder un riesgo porque no se considera un escenario de amenaza particular.

- Una vez que se han evaluado los riesgos, el siguiente paso es abordar el "tratamiento del riesgo". Existen varias maneras de manejar el riesgo, además de tratar de evitar que suceda lo malo:
- La primera manera de manejar el riesgo es "evitar" el riesgo, eliminando la vulnerabilidad o la amenaza.
- La segunda forma de manejar el riesgo es "mitigar" el riesgo, reduciendo la probabilidad de que ocurra o el impacto cuando ocurre.
- La tercera forma de manejar el riesgo es "compartir" el riesgo, mediante la introducción de un tercero -como una compañía de seguros- que compensará a la empresa en caso de que ocurra el riesgo.
- La cuarta manera de manejar el riesgo es "retener" el riesgo, donde la empresa simplemente acepta la posibilidad de que el riesgo pueda ocurrir y se ocupe de las consecuencias cuando sucedan; el auto-seguro es un buen ejemplo de este enfoque.
- El próximo paso de la gestión de riesgos, especialmente si la empresa elige reducir el riesgo, es aplicar "controles" de seguridad. Los controles de seguridad pueden hacer cuatro cosas.
- En primer lugar, los controles pueden reducir la probabilidad de que el riesgo se produzca o dificultar que los atacantes ejecuten el riesgo.
- En segundo lugar, los controles pueden reducir el impacto cuando ocurre el riesgo, tal vez limitando la cantidad de daño que ocurre.
- En tercer lugar, los controles pueden detectar la ocurrencia del riesgo que ocurre, permitiendo respuestas activas para contener el daño y reducir la exposición potencial.
- En cuarto lugar, los controles pueden recopilar evidencia que se usa para mostrar el funcionamiento de los controles de seguridad, para detectar fallos de los controles, o para apoyar las investigaciones después de que se haya producido un incidente.

2.2.1.1 Consideración de vulnerabilidades, amenazas y riesgos de ciberseguridad

La Figura 2-12 presenta el siguiente nivel de detalle del proceso de gestión de riesgos que se ha mostrado en la Figura 2-11.

Es necesario tener en cuenta que los factores de confidencialidad, integridad y disponibilidad (CIA) son considerados en las evaluaciones de vulnerabilidades, amenazas y riesgos. También hay que tener en cuenta que los activos se pueden clasificar como *personal*, *instalaciones*,

procesos e información. Con respecto a los activos de información, la empresa debe considerar las vulnerabilidades, amenazas y riesgos en términos de los factores de CIA, en lugar de considerarlos por separado.

Figura 2-12. Proceso detallado de gestión de riesgos

Primero, hay que considerar la confidencialidad. La confidencialidad es la protección de los datos que deben ser controlados por el acceso y no ser ampliamente difundidos. Para la confidencialidad, la empresa debe considerar qué vulnerabilidades hay: ¿Cómo se puede violar la confidencialidad? ¿Cuál sería la pérdida de datos resultante? A continuación, considerar las amenazas, ya sea accidental o deliberada, que podrían causar la pérdida de datos. Por último, la combinación de las vulnerabilidades y las amenazas, determinan el riesgo con respecto a la confidencialidad.

Luego, considerar la integridad. La integridad implica que los datos sean consistentes desde cuando se ingresa en un sistema hasta cuando se recupera posteriormente. La integridad no suena muy interesante, excepto cuando los datos que se modifican son de dinero o una transacción que implica dinero. Una vez que el dinero está involucrado, la integridad adquiere una importancia crítica. El análisis del riesgo que rodea a la integridad tiene que ver, en parte, con la identificación de la integridad, las consecuencias de una violación de la integridad y las amenazas que podrían dar lugar a esas consecuencias. A menudo, algunas personas no miran a la integridad con mucha preocupación, sin embargo, la integridad debe ser parte integral de la mentalidad de seguridad cibernética empresarial.

Finalmente, considerar la disponibilidad. La disponibilidad implica la disponibilidad de sistemas de información e información cuando se necesitan. Las amenazas a la disponibilidad pueden variar desde sistemas que están temporalmente indisponibles, pero que de otro modo no están alterados, hasta sistemas que están completamente destruidos o corrompidos más allá de la recuperación. En general, los niveles de preocupación por la disponibilidad son impulsados por consideraciones empresariales de impactos financieros negativos versus los costos de mantener o recuperar esa disponibilidad frente a la adversidad.

2.2.1.2 Análisis y Mitigación de Riesgos

Una vez que se han identificado los riesgos asociados a la confidencialidad, integridad y disponibilidad, y es probable que no sean los mismos niveles de riesgo para cada factor, se puede considerar la mitigación del riesgo. La mitigación de riesgos es sólo uno de los posibles tratamientos, pero es el que más atención recibe en el proceso de ciberseguridad.

Se necesita un análisis de riesgos antes de implementar la mitigación del riesgo. El análisis de riesgos caracteriza el riesgo en términos de su magnitud: alta, media o baja. Sin embargo, el riesgo podría dividirse en más gradaciones o en una escala numérica. El riesgo puede entonces ser pensado en términos de su probabilidad de ocurrir y del impacto si ocurre. La Figura 2-13 ilustra el primer paso para evaluar el riesgo en términos de su probabilidad e impacto. Si la probabilidad y el impacto son ambos altos, el nivel de riesgo general probablemente también será "alto". Si la probabilidad y el impacto son bajos, el riesgo general es probablemente también "bajo". Si la probabilidad de un riesgo es baja, pero el impacto es alto, el nivel de riesgo general es más

probable que sea "medio". De manera similar, si la probabilidad es alta, pero el impacto es bajo, el riesgo general es más probable que sea "medio".

Figura 2-13. Matriz de riesgo simplificado

Con este marco como contexto, se puede ver que la mitigación del riesgo tiene el efecto de reducir la probabilidad de un incidente o el impacto del incidente. La mitigación que reduce la probabilidad y el impacto es la más efectiva. ¿Por qué? Tal mitigación puede tomar un "alto" riesgo y moverlo a un "bajo" riesgo. Sin embargo, las mitigaciones del riesgo que afectan solamente a la probabilidad o al impacto pueden todavía ser eficaces. Si bien el análisis de riesgos puede realizarse en cualquier nivel -utilizando más o menos niveles de detalle- este marco general de "alto", "medio" y "bajo" es robusto y suficientemente bueno para muchos propósitos, como priorizar las mitigaciones.

2.2.1.3 Controles de Ciberseguridad

El siguiente componente del proceso de gestión de riesgos es la identificación de controles de ciberseguridad para ayudar a mitigar los riesgos empresariales. Existen cuatro formas en que estos controles reducen la confidencialidad, la integridad o los riesgos de disponibilidad. Los controles pueden: (1) reducir la probabilidad del riesgo, (2) reducir el impacto del riesgo, (3) detectar incidentes relacionados con el riesgo, y (4) recopilar evidencia para respaldar las evaluaciones de seguridad y las investigaciones de incidentes relacionados con el riesgo. Los tipos de control de ciberseguridad para mitigar los riesgos de las organizaciones incluyen los siguientes:

- Controles preventivos, que bloquean la amenaza y evitan que ocurran incidentes en conjunto.
- Controles de detección, que detecta cuándo se ha transmitido el riesgo y genera alertas que luego pueden ser implementadas.
- Controles forenses, que recopilan registros de actividades relacionadas con el riesgo y se pueden usar para producir artefactos para respaldar la operación de controles de detección, investigaciones de incidentes y auditorías de controles para verificar su operación y efectividad.
- Controles de auditoría, que investigan la presencia del riesgo, los incidentes asociados con el riesgo y la operación de controles que mitigan el riesgo.

En la Figura 2-14 se muestra cómo operan estos cuatro controles.

Figura 2-14 Interacción entre los riesgos y los diferentes tipos de controles

Es importante considerar cómo los cuatro tipos de control de seguridad cibernética interactúan entre sí y cómo los cuatro tipos sirven para propósitos útiles individualmente. Con frecuencia, se descuidan los controles de auditoría, a pesar de que una simple auditoría a menudo puede detectar actividades maliciosas que de otro modo se perderían.

La Figura 2-15 representa estos cuatro tipos de control en términos de varias características diferentes. Esta figura resalta algunos resultados interesantes con respecto a las fortalezas y debilidades de cada tipo de control.

	Preventivo	Detective	Forense	Auditoría
Ataques de Bloqueo?	Bueno	Medio	Pobre	Pobre
Detectar Ataques?	Pobre	Bueno	Pobre	Medio
Impacto Operacional	Alto	Bajo	Bajo	Bajo
Investigar Ataques?	Pobre	Medio	Bueno	Bueno
Costo para implementar	Alto	Medio	Medio	Bajo
Costo para operar	Medio	Alto	Bajo	Medio
Flexibilidad	Pobre	Pobre	Medio	Bueno

Figura 2-15 Algunas características de los tipos de control

Los controles preventivos de seguridad cibernética generalmente captan gran parte de la atención porque bloquean los ataques e incidentes, evitando así un ciberataque exitoso. Sin embargo, los controles preventivos tienen una serie de deficiencias. A menos que los controles preventivos se hayan configurado junto con los controles de detección correspondientes, generalmente no son buenos para detectar ataques. Los controles preventivos tienen un alto impacto operativo porque también pueden evitar que los usuarios legítimos hagan su trabajo. Otro inconveniente del control preventivo es que, aunque en general son económicos de operar una vez que están operativos, su implementación puede ser muy costosa debido a su complejidad. Finalmente, los controles preventivos pueden ser difíciles de modificar en respuesta a situaciones que cambian rápidamente.

El siguiente tipo de control de ciberseguridad son los controles de detección. Por lo general, estos controles no se modifican. Lo que es interesante con los controles de detección es que, a diferencia de los controles preventivos, son baratos de implementar y tienen poco impacto operacional en la empresa. Si bien el control en sí mismo puede ser costoso de operar, porque las alertas deben ser investigadas, el costo total de los controles de detección puede ser significativamente menor que la pérdida de productividad de los controles preventivos agresivos.

A continuación, están los controles forenses, que no son muy buenos para detectar o bloquear activamente los ataques, pero son absolutamente críticos para investigar los ataques con éxito después de que hayan ocurrido. Los controles forenses son relativamente baratos de operar una vez que están en su lugar y proporcionan una forma económica de implementar partes de los elementos de seguridad sin inversiones significativas.

Finalmente están los controles de auditoría, que son casi exactamente lo opuesto a los controles preventivos. Cuando los controles preventivos son efectivos para detener ataques, aunque con un impacto operacional considerable, los controles de auditoría casi no tienen impacto operativo, pero tampoco detienen mucho el camino de los ataques. Sin embargo, los controles de auditoría son de bajo costo, discretos y ágiles. Con frecuencia, los controles de auditoría son la única forma de encontrar ataques que han derrotado los controles preventivos de la empresa. Entonces, aunque los controles de auditoría no son llamativos, estos controles de ciberseguridad merecen respeto y consideración en la arquitectura de seguridad de una empresa. Una auditoría simple a menudo puede encontrar problemas que han estado acechando durante meses o años, a pesar de todos los otros controles.

Idealmente, los cuatro tipos de control están diseñados y operados en paralelo, apoyándose mutuamente. Cuando se analizan las tecnologías de seguridad, es útil evaluarlas en términos de qué tipos de funciones de control proporcionan principalmente. Para conocer los riesgos

potenciales que pueden presentarse en una organización, y poder catalogarlos, en la siguiente subsección se ha realizado una revisión sistemática de taxonomías de riesgos en ciberseguridad.

2.2.2. RS de Taxonomías de Riesgos en Ciberseguridad

“Riesgo es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicio a la Organización” (Ministerio de Administraciones Públicas, 2006). Este concepto es muy amplio, pues abarca todos los riesgos que afecten a los activos de la organización.

Según la definición anterior, sabemos que un riesgo de ciberseguridad es parte de los otros tipos de riesgos y, a su vez, los riesgos en ciberseguridad son muy variables. Por lo tanto, es importante contar con una taxonomía que ayude a identificar y clasificar los riesgos inherentes a la ciberseguridad.

En esta revisión sistemática, se pretende responder a través de la revisión sistemática de literatura a la siguiente pregunta: ¿existe alguna taxonomía de riesgo relacionada con la ciberseguridad publicada?

2.2.2.1 Identificación de las Necesidades

Se ha requerido una revisión sistemática para identificar las diferentes taxonomías de riesgos de ciberseguridad que se han publicado.

2.2.2.2 Protocolo de Revisión

En este punto se definen: la formulación de las preguntas a realizar, las fuentes de la base de datos para la búsqueda, la elaboración de las cadenas de búsqueda según los criterios definidos, y la búsqueda en las fuentes, para ubicar y seleccionar los estudios.

- **Pregunta:** la pregunta planteada ha sido: ¿qué taxonomías de riesgo se han propuesto para la ciberseguridad?
- **Fuentes seleccionadas:** IEEE Computer, Science Direct, ACM Digital Library y Web of Knowledge.
- **Las cadenas de búsqueda** fueron las siguientes:
 - "Taxonomía del riesgo de ciberseguridad".
 - "Riesgo de ciberseguridad".
 - "Taxonomía de riesgos".
 - "Taxonomía de riesgos cibernéticos".
- **Palabras Claves:** “Ciberseguridad”, “Riesgos”, “Taxonomía”.

2.2.2.3 Revisión

En este punto, se muestra la búsqueda de los documentos en las bases de datos seleccionadas con las cadenas de búsqueda predefinidas. La revisión se realiza en tres fases. Los criterios de inclusión y exclusión establecidos a continuación, se aplicaron a los resultados de búsqueda.

Criterios para seleccionar estudios, y procedimientos para inclusión y exclusión:

De los resultados encontrados, la Tabla 2-10 enumera los criterios de inclusión y exclusión que se aplicaron a los resultados de la búsqueda inicial. La selección de estudios se ha centrado en aquellos relacionados con las taxonomías de riesgo en ciberseguridad publicadas.

Tabla 2-10. Criterios de inclusión y exclusión (RS Riesgos de Ciberseguridad – RS RC)

<i>Inclusión (I)</i>	<i>Exclusión (E)</i>
I1. Estudios empíricos de taxonomías de riesgo de seguridad cibernética que en su contenido muestran alguna clasificación de riesgo que se aplica a la ciberseguridad	E1. Documentos que se basan solo en una opinión particular que no aborda la ciberseguridad.

<i>Inclusión (I)</i>	<i>Exclusión (E)</i>
12. Documentos que analizan taxonomías o clasificaciones de riesgos de ciberseguridad.	E2. Estudios que no son relevantes para la pregunta de investigación o no están relacionados con el estudio particular.
13. Artículos que usan las palabras claves de la búsqueda.	E3. Estudios que no son claros o ambiguos.
14. Artículos cuyo título, resumen o contenido están relacionados con el tema.	E5. Publicaciones duplicadas.
15 Documentos de acceso gratuito.	E6 Estudios previos a 1990 debido a la actualización constante en el área.

- En una primera fase de la revisión, haciendo uso de los motores de búsqueda de las bases de datos identificadas y poniendo la cadena de búsqueda elaborada en la tarea "la cadena de búsqueda" de la actividad "protocolo de revisión", se han encontrado un total de 132 estudios.
- En la segunda fase de la revisión, cada estudio se ha revisado teniendo en cuenta los criterios de inclusión y exclusión anteriores, obteniendo un total de 14 estudios relevantes. Para seleccionar los estudios pertinentes, se tomaron los siguientes pasos: leer el título, leer el resumen, leer las conclusiones y completar la plantilla creada; si proporcionan suficiente información, el estudio se selecciona y se guarda. De lo contrario, se elimina.
- En la tercera fase de la revisión, se obtuvieron cinco estudios primarios que respondían a las preguntas formuladas inicialmente. La Tabla 2-11 muestra las fuentes, el número total de trabajos y el número de trabajos primarios seleccionados por fuente.

Tabla 2-11. Distribución de estudios por fuente (RS RC)

<i>Fuente</i>	<i>Total</i>	<i>Relevantes</i>	<i>Primarios</i>
IEEE Explore	11	3	2
Science Direct	6	0	0
ACM Digital Library	8	0	0
Web of Knowledge	107	11	3
Total	132	14	5

Evaluación de la calidad de los estudios:

Para evaluar la calidad de los estudios, se realizaron las siguientes preguntas:

- ¿Es el estudio primario relevante para la investigación que se está realizando?
- ¿Los estudios primarios proveen la suficiente información como para que los resultados se beneficien de la revisión sistemática?
- ¿Los estudios revisados dan un valor agregado a la investigación que se está realizando?

De la evaluación de calidad de los estudios se pudo ratificar que los 5 estudios primarios seleccionados son relevantes, proveen la información adecuada y aportan un valor agregado a la revisión sistemática que se ha realizado.

2.2.2.4 Análisis, Interpretación e Informe de los Resultados

Al final de la revisión sistemática, se ha analizado el contexto de cada documento. Para los documentos que proponían una taxonomía en ciberseguridad, se ha analizado la clasificación de riesgo propuesta, y su enfoque y alcance.

De acuerdo con su contexto, los documentos se han clasificado en:

- Marcos de trabajo relacionados con riesgo.
- Conceptos sobre cómo realizar una taxonomía.
- Taxonomía enfocada en un área específica.

De los cinco (5) artículos primarios, uno es relativo a un marco de gestión de riesgos empresariales (Enterprise Risk Management, ERM), otro artículo menciona los conceptos sobre cómo realizar una taxonomía de riesgos de seguridad de la información y otros tres artículos hacen referencia a taxonomías centradas en: ingeniería social, proveedores de software y riesgo de seguridad de la información.

Los resultados de la revisión sistemática se presentan a continuación. Los elementos principales encontrados se describen en la Tabla 2-12 para un análisis más detallado.

Tabla 2-12. Estudios primarios (RS RC)

<i>Artículo</i>	<i>Contexto</i>	<i>Referencia</i>
Tres factores clave para la gestión exitosa del riesgo empresarial	Gestión del riesgo	(von Känel, Cope, Deleris, Nayak, & Torok, 2010)
Taxonomía de la evaluación de riesgos de seguridad de la información (ISRA, Information Security Risk Assessment)	Riesgo de seguridad de la información	(Shameli-Sendi, Aghababaei-Barzegar, & Cheriet, 2016)
Comprender la taxonomía de los riesgos cibernéticos de la industria financiera en la nube	Realizar una taxonomía de los riesgos para la seguridad de la información	(Elnagdy, Qiu, & Gai, 2016)
Análisis de amenazas internas no intencionales derivadas de vulnerabilidades de ingeniería social	Taxonomía enfocada en ingeniería social	(Greitzer et al., 2014)
Taxonomía de procesos y riesgos para proveedores de soluciones de mediano tamaño	Taxonomía centrada en proveedores de software	(Herzfeldt, Hausen, Briggs, & Krcmar, 2012)

Para obtener estudios complementarios, se ha aplicado la técnica de bola de nieve. Esto ha permitido obtener dos estudios adicionales de (Elnagdy et al., 2016) y un estudio adicional a partir de (Greitzer et al., 2014). Además, una búsqueda en Google Scholar proporcionó dos taxonomías complementarias.

Estos estudios complementarios se muestran en la Tabla 2-13.

Tabla 2-13. Estudios primarios adicionales (RS RC)

<i>Artículo</i>	<i>Contexto</i>	<i>Referencia</i>
Una taxonomía de los riesgos operacionales de ciberseguridad	Empresa	(Cebula & Young, 2010)
La estructura de un riesgo cibernético - un enfoque basado en escenarios en la evaluación del riesgo cibernético	Empresa	(Delmee, 2016)
Asegurar la red inteligente: ciberataques, contramedidas y desafíos	Red inteligente	(Xu Li et al., 2012)
Clasificación y análisis de tendencias de los orígenes de las amenazas a la seguridad de los sistemas de energía	Sistemas de Energía	(Bompard, Huang, Wu, & Cremenescu, 2013)
Desarrollo de la taxonomía metodológica de ingeniería social	Ingeniería Social	(Laribbe, 2006)

Una vez que se ha seleccionado y analizado cada uno de los estudios primarios (incluidos los adicionales), se han identificado las taxonomías de riesgo de ciberseguridad publicadas y se ha

determinado el área y el enfoque, así como los marcos y los modelos de gestión de riesgos en ciberseguridad, tal como se muestra a continuación:

- El documento de von Käne (von Känel et al., 2010) aborda una taxonomía de riesgos que incluye riesgos de ciberseguridad y riesgos financieros en organizaciones basadas en el marco de COSO (Comité de Organizaciones Patrocinadoras de la Comisión Treadway).
- En el documento de Elnagdy (Elnagdy et al., 2016), se descubre una taxonomía de ciberataques básicos en la red inteligente y una clasificación de amenazas maliciosas.
- El documento de Greitzer (Greitzer et al., 2014) presenta una taxonomía de los riesgos centrados en la ingeniería social.
- Identificamos que el autor Herzfeldt (Herzfeldt et al., 2012) presenta una taxonomía de riesgos ocultos y proveedores de sistemas de TI, que clasifica los riesgos desde la identificación de la necesidad hasta la implementación y el mantenimiento del sistema.
- El documento de Cebula (Cebula & Young, 2010) presenta una Taxonomía de Riesgos Operacionales de Ciberseguridad que menciona una taxonomía adecuada de riesgos en ciberseguridad. Esto se divide en cuatro clases: acciones de personas, sistemas y fallos tecnológicos, procesos internos fallidos, y eventos externos.
- El documento de Delmee (Delmee, 2016) crea una taxonomía de riesgos cibernéticos basada en un enfoque de riesgo basado en escenarios. Los escenarios se elaboran con información contextual sobre la víctima y el agente de la amenaza, para identificar todos los conceptos relevantes dentro del escenario.
- Identificamos que el autor Xu, Li (Xu Li et al., 2012) presenta una taxonomía de ciberataques básicos en la comunicación de la red inteligente. En esta taxonomía, hay cuatro tipos de ataques: ataque de dispositivo, ataque de datos, ataque de privacidad y ataque de disponibilidad de red. Tienen diferentes objetivos y son a menudo los componentes básicos de ataques más sofisticados.
- En el documento de Bompard (Bompard et al., 2013), debido al creciente reconocimiento de la importancia de los sistemas de energía en la sociedad actual, se presenta una clasificación de amenazas maliciosas. Existen tres amenazas maliciosas: amenaza física, amenaza humana y amenaza cibernética.
- Identificamos que el autor Laribee (Laribee, 2006) presenta en su estudio una taxonomía para codificar ataques de ingeniería social, y propone cuatro dimensiones principales de interés para determinar el tipo y la gravedad de un ataque de ingeniería social. La primera categoría es el objetivo, la segunda categoría es el tipo de engaño, la tercera categoría es el recurso particular o la información del objetivo, y la cuarta categoría es la estratagema de empuje.

Para analizar los resultados, se ha ampliado la clasificación de la perspectiva de las taxonomías. Para ello, se tomaron los datos de la clasificación de perspectiva de taxonomía obtenidos de Shameli-Sendi (Shameli-Sendi et al., 2016). La clasificación de Shameli-Sendi tiene tres niveles de abstracciones, de abajo hacia arriba, que son: activos, servicios y negocios. Aunque la mayoría de las taxonomías se basan en el nivel de activos, los nuevos estudios están cambiando el enfoque y avanzando hacia el nivel de servicio y negocios. Hemos incluido los ataques fuente y los eventos externos como dos categorías complementarias. Hemos agregado estas dos nuevas categorías, debido a la dificultad de igualar los elementos de clasificación de las taxonomías encontradas y a que son difíciles de encajar en las categorías propuestas por Shameli-Sendi (Shameli-Sendi et al., 2016). Cada elemento de las taxonomías analizadas se ha mapeado a una de las cinco categorías, y los resultados de este mapeo se muestran en la Tabla 2-14.

Tabla 2-14. Resumen de taxonomías (RS TC)

<i>Autor</i>	<i>Dominio</i>	<i>Perspectiva</i>	<i>Artículos de Taxonomías</i>
(von Känel et al., 2010)	Empresa	Activo + Servicio + Negocio + Externo	Fuentes y eventos

<i>Autor</i>	<i>Dominio</i>	<i>Perspectiva</i>	<i>Artículos de Taxonomías</i>
			Objetos comerciales y modelos dinámicos Impactos del riesgo
(Xu Li et al., 2012)	Red Inteligente	Activo + Ataque + Negocio	Dispositivo de ataque Ataque de datos Ataque de privacidad Ataque de disponibilidad de red
(Bompard et al., 2013)	Sistemas de Energía	Ataque + Negocio + Externo	Ataque Físico Amenaza humana Amenaza cibernética
(Greitzer et al., 2014)	Ingeniería Social	Activo +Ataque	Interacción personal Sin interacción personal
(Laribbe, 2006)	Ataques de Ingeniería Social	Activo + Ataque	Objetivo Tipo de engaño Información del recurso u objetivo Estrategia de confianza
(Herzfeldt et al., 2012)	Soluciones de Tecnología de la Información	Servicios + Negocio + Externo	Ambiente Riesgo del proveedor Solución de TI Riesgo Riesgo del cliente
(Cebula & Young, 2010)	Empresa	Activo + Servicio + Negocio + Externo	Acciones de personas Sistemas y fallas tecnológicas Procesos internos fallidos Eventos externos
(Delmee, 2016)	Empresa	Activo + Servicio + Ataque+ Negocio	Información general Organización (víctima) Agente de amenaza Activo Evento de amenaza Impacto de negocios Vulnerabilidades Controles

El análisis indica que todas las taxonomías toman en cuenta el nivel de Activos y Negocios, con la excepción de las taxonomías especializadas en ingeniería social. Esto se debe a que se centran en aspectos de la interacción humana. Es digno de mención que la taxonomía especializada de redes inteligentes se centra únicamente en aspectos de posibles formas de ataque.

Es común que, en todas las demás taxonomías, además del aspecto comercial, tomen en cuenta aspectos de los activos, servicios y eventos externos. Esto se debe a la necesidad de identificar amenazas, tanto para los recursos como para las actividades comerciales. Los eventos externos deben tenerse en cuenta, ya que deben ser monitoreados.

La taxonomía más moderna, (Delmee, 2016), combina los tres niveles de abstracción con la categoría de fuentes de ataque. Esto podría indicar que las taxonomías de riesgo podrían estar cambiando el enfoque del nivel de activos a los niveles de abstracción de servicios y negocios.

2.2.2.5 Conclusiones de la Revisión Sistemática de Riesgos en Ciberseguridad

Se han revisado los documentos de taxonomía de seguridad cibernética publicados en conferencias y publicaciones periódicas para comprender el progreso en las taxonomías de riesgos de ciberseguridad. El objetivo ha sido identificar los estudios con respecto a las taxonomías de riesgo que se han propuesto para la ciberseguridad.

Hay diferentes tipos de taxonomías de riesgo. Cada una de estas taxonomías se ha desarrollado para satisfacer una necesidad particular, y para cada una de dichas taxonomías se ha proporcionado una visión general y su estructura. Además, hemos desarrollado una nueva clasificación de tipos de taxonomía basada en la de Shameli-Sendi (Shameli-Sendi et al., 2016). Con base en esta nueva clasificación, hemos analizado las taxonomías encontradas e identificado que la mayoría de ellas son de aplicación particular y no se pueden aplicar en otros dominios.

Las taxonomías identificadas solo derogaron riesgos específicos, tales como riesgos de ingeniería social, riesgos financieros, riesgos operacionales, amenazas maliciosas y taxonomía de riesgos basados en ciertos escenarios específicos.

El artículo de Elnagdy (Elnagdy et al., 2016) no presenta una taxonomía, sino que indica los conceptos necesarios para poder definir una taxonomía de riesgos que pueda aplicarse en la seguridad cibernética en la nube.

La taxonomía más moderna de los riesgos de seguridad cibernética es el estudio Delmee (Delmee, 2016), basado en un enfoque de riesgo basado en escenarios, y se distribuye en ocho conceptos diferentes, y cincuenta y una (51) características.

Una vez que se ha descrito el concepto de riesgos en ciberseguridad, se ha definido que es el proceso de gestión de riesgo y se ha realizado una revisión sistemática de taxonomías de riesgos en ciberseguridad, es importante determinar qué elementos participan en el análisis y evaluación de los riesgos en ciberseguridad. Inicialmente, se han identificado como procesos importantes, la gestión a los activos, y a las amenazas y vulnerabilidades de ciberseguridad. Por ello, en la siguiente sección se va a realizar un análisis de los elementos de la gestión de riesgos en ciberseguridad y sus relaciones.

2.2.3. Modelo Conceptual de Riesgos en Ciberseguridad

De la revisión sistemática de taxonomía de riesgos en ciberseguridad, se identificaron algunos artículos que nombran a estándares internacionales como referencias para la gestión de riesgos, como es el caso de Instituto Nacional de Estándares y Tecnología (NIST) (Shameli-Sendi et al., 2016), (Delmee, 2016), (Cebula & Young, 2010), en los cuales se identifican los elementos que participan en la gestión de riesgos. Estos elementos son similares a los que se definen en los modelos conceptuales enfocados en necesidades y enfoques particulares definidos en otros artículos.

A continuación, se van a mostrar algunas relaciones encontradas y los elementos de gestión de riesgos identificados.

En el artículo (Singh, 2014), se muestra una relación de seguridad, que es tomada de la publicación especial 800-12 del Instituto Nacional de Estándares y Tecnología (NIST), en el cual existe una relación directa de las amenazas con los activos. Sin embargo, la relación debería ser a través de las vulnerabilidades, característica propia de los activos. Las relaciones conceptualizadas de alto nivel entre las entidades se muestran en la Figura 2-16.

Figura 2-16. Modelo Conceptual de Riesgos de NIST (Fuente: Singh, 2014)

En los artículos (Singhal & Wijesekera, 2010) y (Singhal & Singapogu, n.d.), se describe un modelo de datos para la seguridad a nivel empresarial en términos de entidades y las relaciones entre ellas. Este modelo de datos se puede usar para medir y comprender la efectividad de los mecanismos de seguridad actuales y los beneficios que brindan, pensando en la seguridad en términos de amenazas, riesgos y pérdidas. Para ello, se ha definido una ontología que permite saber qué amenazas ponen en peligro qué activos y qué contramedidas pueden reducir la probabilidad de que se produzca un ataque. En la Figura 2-17 se muestran los elementos identificados, sin embargo no se puede identificar las contramedidas que deben ser aplicadas a las vulnerabilidades de los activos.

Figura 2-17. Entidades y Relaciones de Riesgos empresariales (Fuente: Singhal & Wijesekera, 2010)

En el artículo (NIST, 2012), publicación especial 800-30, se describe una guía para realizar evaluaciones de riesgos de los sistemas de información y organizaciones federales o del gobierno. Además, se proporciona una guía para llevar a cabo cada uno de los pasos del proceso de evaluación de riesgos (es decir, prepararse para la evaluación, realizar la evaluación, comunicar los resultados de la evaluación y mantener la evaluación) y cómo las evaluaciones de riesgos y otros procesos de gestión de riesgos organizacionales se complementan e informan entre sí. Para ello, la Figura 2-18 ilustra un ejemplo de un modelo de riesgos que incluye los principales elementos de riesgo y la relación entre los elementos.

Figura 2-18. Modelo de riesgos genérico con elementos clave de riesgo de NIST (Fuente: NIST, 2012)

En el artículo (Goodwin et al., 2015), se menciona que un marco para el intercambio de información sobre ciberseguridad y la reducción de riesgos debe ser una guía relevante y oportuna para cualquier persona responsable de desarrollar nuevas ideas y soluciones para el intercambio de información. Por ello, se plantea un esquema de relación entre los elementos participantes para ayudar a crear un ecosistema en línea más seguro, como se muestra en la Figura 2-19.

Figura 2-19. Tipos de Información de Ciberseguridad (Fuente: Goodwin et al., 2015)

2.2.4. Consideraciones Finales de Riesgos en Ciberseguridad

En este apartado se ha realizado una revisión de los conceptos de la gestión de riesgos en ciberseguridad, también se ha realizado una revisión sistemática de taxonomías de riesgos en ciberseguridad, y luego se han analizado los modelos conceptuales de gestión de riesgos en ciberseguridad.

Del análisis realizado, se han identificado las siguientes particularidades:

- Los elementos críticos que deben considerarse en la gestión de riesgos en ciberseguridad son: los activos de la organización, las vulnerabilidades de ciberseguridad de los activos y las amenazas de ciberseguridad que materializan las vulnerabilidades de ciberseguridad, generando el riesgo en ciberseguridad.
- Existen contramedidas que ayudan a mitigar el impacto de los riesgos, algunas lo hacen contra las amenazas. y otras, contra las vulnerabilidades.
- Los modelos conceptuales tienen enfoques diferentes según las necesidades puntuales, aunque describen los elementos de la gestión de riesgos en ciberseguridad.
- No se muestra la participación de las dimensiones de seguridad (confidencialidad, integridad, disponibilidad) como parte de los elementos de riesgos en ciberseguridad.
- No se muestra que se llegue a medir las dimensiones de seguridad en las vulnerabilidades de ciberseguridad de los activos.
- Los buenos modelos proporcionan un fundamento para las mediciones y estos modelos de datos se pueden actualizar y calibrar a medida que se disponga de nuevos datos.

Luego de las revisiones realizadas, se ha determinado que se debe identificar si existen taxonomías de los elementos de riesgos en ciberseguridad como: activos, y vulnerabilidades y amenazas de ciberseguridad.

2.3. Otras Revisiones Sistemáticas

2.3.1. RS de Taxonomías de Activos en Ciberseguridad

Un activo es un componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos (71504 UNE, 2008). Se pretende a través de una revisión sistemática de la literatura responder a la siguiente pregunta:

¿Cuáles son las principales taxonomías de activos en ciberseguridad que han sido publicadas en artículos científicos?

2.3.1.1 Identificación de las Necesidades

Se ha requerido realizar la revisión sistemática que permita: (1) identificar las diferentes taxonomías de activos en ciberseguridad que han sido publicadas, (2) identificar las taxonomías más nombradas por los estudios realizados.

2.3.1.2 Protocolo de Revisión

En este punto se han definido: las preguntas a realizar, las fuentes de bases de datos que deben usarse para realizar la búsqueda, la elaboración de las cadenas de búsqueda según los criterios definidos, y la búsqueda en las fuentes, para localizar y seleccionar los estudios.

- **Preguntas:** se ha planteado la problemática y las preguntas que están relacionadas con las necesidades y objetivos de la revisión. ¿Cuáles son las taxonomías de activos en ciberseguridad publicadas en artículos científicos? ¿Cuáles son las principales taxonomías que se utilizan en los estudios de investigación?

- **Fuentes seleccionadas:** entre las fuentes seleccionadas están las bases de datos especializadas como: IEEE Computer, Science Direct, ACM (Association for Computing Machinery), Institute for Scientific Information (ISI) web of knowledge.
- **Las cadenas de búsqueda** definidas han sido las siguientes:
 - “Cyber assets“ and “Taxonomy”.
 - “Cyber assets“ and “Classification”.
 - “Organizational Assets” and “Taxonomy”.
 - “Organizational Assets” and “Classification”.
- **Palabras Claves:** “Cyber assets”, “Taxonomy”, “Classification”, “Organizational Assets”.

2.3.1.3 Revisión

En este punto se muestra la búsqueda realizada de los artículos en las bases de datos seleccionadas con las cadenas de búsquedas predefinidas. Al resultado de las búsquedas se les han aplicado los criterios de inclusión y exclusión establecidos a continuación.

Criterios de selección de estudios, y procedimientos para inclusión y exclusión:

En la Tabla 2-15 se presentan los criterios de inclusión y exclusión que se han aplicado a los resultados de la búsqueda inicial. La selección de estudios se ha centrado en aquellos relacionados con las taxonomías de activos en ciberseguridad y las más utilizadas en los estudios de investigación.

Tabla 2-15. Criterios de inclusión y exclusión de estudios (RS Taxonomía de Activos de Ciberseguridad – RS TAct)

<i>Inclusión (I)</i>	<i>Exclusión (E)</i>
I1. Estudios empíricos de taxonomías de activos. Artículos que tratan sobre los factores que condicionan las taxonomías de activos en las organizaciones. I2. Artículos que hablan sobre las taxonomías de activos. I3. Artículos que contiene las cadenas de búsqueda. I4. Artículos cuyo título, resumen o contenido está relacionado con el tema.	E1. Artículos que están basados sólo en una opinión particular y que no abordan taxonomías de activos en ciberseguridad. E2. Artículos cortos. E3. Estudios que no son relevantes para las preguntas de investigación o no están relacionados con el estudio en particular. E4. Estudios que no son claros o presentan ambigüedad. E5. Publicaciones duplicadas. E6 Estudios anteriores a 2000 debido a la constante actualización en el área.

- En una primera fase de la revisión sistemática, haciendo uso de los motores de búsqueda de las bases de datos identificadas y poniendo las cadenas de búsqueda elaboradas en el protocolo de revisión, se han encontrado un total de 255 estudios.
- En una segunda fase, se revisaron cada uno de los estudios tomando en consideración los criterios de inclusión y exclusión anteriores, obteniendo un total de 10 estudios relevantes.
- En una tercera fase, se obtuvieron 2 estudios primarios que respondían a las preguntas formuladas inicialmente. La Tabla 2-16 muestra en primera instancia las fuentes, el número total de artículos y el número de artículos relevantes y primarios seleccionados por fuente.

Tabla 2-16. Distribución de los estudios por fuente (RS TAct)

<i>Fuente</i>	<i>Total</i>	<i>Relevantes</i>	<i>Primarios</i>
IEEE Explore	166	7	2
Science Direct	52	2	0
ACM	34	1	0
ISI WoK	3	0	0
Total	255	10	2

Evaluación de la calidad de los estudios:

Para poder evaluar la calidad de los estudios, se realizaron las siguientes preguntas:

- ¿Es el estudio primario relevante para la investigación que se está realizando?
- ¿Los estudios primarios proveen la suficiente información como para que los resultados se beneficien de la revisión sistemática?
- ¿Los estudios revisados dan un valor agregado a la investigación que se está realizando?

De las preguntas anteriores, se ha podido comprobar que los 2 estudios primarios seleccionados son relevantes, proveen suficiente información y dan un valor agregado a la revisión sistemática.

2.3.1.4 Análisis, Interpretación e Informe de los Resultados

Al concluir la ejecución de la revisión sistemática, los resultados se han resumido y analizado. En el análisis, se usan herramientas para determinar la frecuencia del nombrado de las taxonomías de activos en ciberseguridad. Para realizar el resumen, los estudios fueron clasificados en estudios relacionados con taxonomías que cubran la organización o un área en particular, como se muestra en la Tabla 2-17.

Tabla 2-17. Taxonomías de activos en ciberseguridad

<i>Referencia</i>	<i>Área</i>
(Shamala & Ahmad, 2014)(Shamala & Ahmad, 2014)	Organización
(Yazid, Faizal, Rabiah, Shahrin, & Solahuddin, 2012)	Teléfonos Móviles

Se encontraron únicamente dos taxonomías:

- Taxonomía propuesta de activos para la evaluación de riesgos de seguridad de la información (ISRA) (Information Security Risk Assessment) (Shamala & Ahmad, 2014)(Shamala & Ahmad, 2014).
- Taxonomía que describe una categoría de dispositivos móviles (Yazid et al., 2012).

2.3.1.5 Conclusiones de la Revisión Sistemática de Activos en Ciberseguridad

Una vez seleccionados y analizados cada uno de los estudios primarios, se ha identificado que no existe un gran número de publicaciones de taxonomías de activos en ciberseguridad en artículos científicos, y se ha observado que:

- La taxonomía de ISRA es muy básica y contempla pocos activos.
- La categorización que se hace de dispositivos móviles se hace en función de la funcionalidad de los dispositivos.

No existen muchas taxonomías de activos en ciberseguridad que estén publicadas en artículos científicos. Por ello, se debe analizar las taxonomías de activos en la empresa privada y en organizaciones gubernamentales, así como en los organismos que se encargan de establecer los estándares de la industria. No obstante, existen esfuerzos aislados de empresas, por encargo, que realizan taxonomías para las organizaciones.

2.3.2. RS de Taxonomías de Vulnerabilidades en Ciberseguridad

Vulnerabilidad es un defecto o debilidad en el diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza. Son propiedades intrínsecas de que algo se produzca como resultado de una sensibilidad a una fuente de riesgo que puede conducir a un suceso con una consecuencia (IN, 2010).

Se denomina vulnerabilidad a toda debilidad que puede ser aprovechada por una amenaza, o más detalladamente a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial. Por lo tanto, son vulnerabilidades todas las ausencias o ineficacias de las salvaguardas pertinentes para salvaguardar el valor propio o acumulado sobre un activo.

En esta revisión sistemática, se pretende responder a través de la revisión sistemática de literatura a la siguiente pregunta: ¿existe alguna taxonomía de vulnerabilidades en ciberseguridad publicada?

2.3.2.1 Identificación de las Necesidades

Se ha requerido la revisión sistemática para identificar las diferentes taxonomías de vulnerabilidades en ciberseguridad que se han publicado.

2.3.2.2 Protocolo de Revisión

En este punto se definen: la formulación de las preguntas a realizar, las fuentes de la base de datos para la búsqueda, la elaboración de las cadenas de búsqueda según los criterios definidos, y la búsqueda en las fuentes, para ubicar y seleccionar los estudios.

- **Formulación de la pregunta:** la pregunta planteada es: ¿qué taxonomías de vulnerabilidades se han propuesto para la ciberseguridad?
- **Las bases de datos seleccionadas fueron:** IEEE Computer, Science Direct, ACM Digital Library y Web of Knowledge.
- **Las cadenas de búsqueda** fueron las siguientes:
 - ("Cyber Vulnerability" or "Cyber Vulnerabilities") and "Taxonomy".
 - ("Cyber Vulnerability" or "Cyber Vulnerabilities") and "Classification".
 - "Taxonomy of Vulnerability" or "Taxonomy of Vulnerabilities".
 - "Classification of Vulnerability" or "Classification of Vulnerabilities".
- **Palabras Claves:** "Cyber Vulnerability", "Taxonomy", "Classification".

2.3.2.3 Revisión

En este punto, se muestra la búsqueda de los documentos en las bases de datos seleccionadas con las cadenas de búsqueda predefinidas. La revisión se realiza en tres fases. Los criterios de inclusión y exclusión establecidos a continuación se han aplicado a los resultados de búsqueda.

Criterios para seleccionar estudios, y procedimientos para inclusión y exclusión

De los resultados encontrados, la Tabla 2-18 enumera los criterios de inclusión y exclusión que se han aplicado a los resultados de la búsqueda inicial. La selección de estudios se ha centrado en aquellos relacionados con las taxonomías de vulnerabilidades en ciberseguridad publicadas.

Tabla 2-18. Criterios de inclusión y exclusión de los estudios (RS Taxonomía de Vulnerabilidades de Ciberseguridad – RS TV)

<i>Inclusión (I)</i>	<i>Exclusión (E)</i>
I1. Estudios empíricos de ciberseguridad que muestren una clasificación de vulnerabilidades en ciberseguridad.	E1. Documentos que se basan solo en una opinión particular y que no aborden las vulnerabilidades en ciberseguridad.
I2. Documentos que analizan taxonomías o clasificaciones de vulnerabilidades en ciberseguridad.	E2. Estudios que no son relevantes para la pregunta de investigación o no están relacionados con el estudio particular.
I3. Artículos que contienen las cadenas de búsqueda.	E3. Estudios que no son claros o ambiguos.
I4. Artículos cuyo título, resumen o contenido están relacionados con el tema.	E5. Publicaciones duplicadas.
I5 Documentos de acceso gratuito.	E6 Estudios previos a 1990 debido a la actualización constante en el área.

- En una primera fase de la revisión, haciendo uso de los motores de búsqueda de las bases de datos identificadas y poniendo la cadena de búsqueda elaborada en la tarea "cadenas de búsqueda", se encontraron un total de 298 estudios.
- En la segunda fase de la revisión, cada estudio se revisó teniendo en cuenta los criterios de inclusión y exclusión anteriores, obteniendo un total de 36 estudios relevantes. Para seleccionar los estudios pertinentes, se tomaron los siguientes pasos: leer el título, leer el resumen, leer las conclusiones y completar la plantilla creada; si proporcionan suficiente información, el estudio se selecciona y se guarda. De lo contrario, se elimina.
- En la tercera fase de la revisión, se obtuvieron 23 estudios primarios que respondían a las preguntas formuladas inicialmente. La Tabla 2-19 muestra las fuentes, el número total de trabajos, y el número de trabajos relevantes y primarios seleccionados por fuente.

Tabla 2-19. Distribución de estudios por fuente (RS TV)

<i>Fuente</i>	<i>Total</i>	<i>Relevantes</i>	<i>Primarios</i>
IEEE Explore	168	26	2
Science Direct	75	4	3
ACM Digital Library	35	4	0
Web of Knowledge	20	2	3
Total	298	36	23

Evaluación de la calidad de los estudios:

Para poder evaluar la calidad de los estudios, se realizaron las siguientes preguntas:

- ¿Es el estudio primario relevante para la investigación que se está realizando?
- ¿Los estudios primarios proveen la suficiente información como para que los resultados se beneficien de la revisión sistemática?
- ¿Los estudios revisados dan un valor agregado a la investigación que se está realizando?

Una vez realizadas las preguntas correspondientes se determinó que los 23 estudios primarios seleccionados son lo suficientemente relevantes para la investigación, y proveen suficiente información para la revisión sistemática y dan un valor agregado a la revisión sistemática.

Para cada documento seleccionado, después de leer el texto completo, la información recopilada ha permitido el posterior análisis de los resultados.

2.3.2.4 Análisis, Interpretación e Informe de los Resultados

Al final de la revisión sistemática, se ha analizado el contexto de cada documento. Para los documentos que proponían una taxonomía de vulnerabilidades en ciberseguridad, se ha analizado la clasificación de vulnerabilidades propuestas, y su enfoque y alcance. De la revisión inicial de los 23 estudios primarios, se ha encontrado que:

- 10 artículos presentan taxonomías.
- 13 artículos no presentan taxonomías, sino que describen la importancia de la taxonomía de vulnerabilidades, realizan un mapeo con las ontologías y evolución de las mismas.

De los artículos que presentan taxonomías de acuerdo a su contexto, se clasificaron en:

- Vulnerabilidades de Aplicaciones de Software.
- Vulnerabilidades de Redes de Datos.
- Vulnerabilidades de Dispositivos móviles.
- Vulnerabilidades de la Organización.

De los 10 artículos que presentan taxonomías, se describen en la Tabla 2-20 los principales elementos encontrados.

Tabla 2-20. Estudios primarios que presentan taxonomías de vulnerabilidades de ciberseguridad

	<i>Artículo</i>	<i>Enfoque</i>	<i>Criterio</i>	<i>Referencia</i>
1	(Kamesh & Sakthi Priya, 2014)	Redes de Datos	Las amenazas potenciales y las medidas de protección; los componentes y características; y las actividades.	CVSS
2	(Xiaodan Li, Chang, Board, & Trivedi, 2017)	Aplicaciones de Software	Complejidad de identificar, solucionar y explotar vulnerabilidades. Similar a la utilizada para clasificar errores de software.	
3	(Bazaz & Arthur, 2007)	Aplicaciones de Software	Modelo de Proceso / Objeto de Computación, relación entre las vulnerabilidades, las aplicaciones de software y los recursos del sistema informático.	
4	(Miloslavskaya, Tolstoy, & Zapechnikov, 2016a)	Organización	Ataques que se ejecutan todos los días contra diferentes objetivos de la organización.	CVSS, NVD, NIST
5	(Zhao & Dai, 2012)	Organización	Confidencialidad, integridad, disponibilidad, controlabilidad y confiabilidad.	OSVDB
6	(Li, Z., Shahidehpour, M., and Aminifar, 2017)	Redes de Datos	Las que son utilizadas en el dominio de Tecnología de la Información.	
7	(Linares-Vasquez, Bavota, & Escobar-Velasquez, 2017)	Dispositivos Móviles	Sistema Operativo (Android).	CVE, NVD, CWE
8	(Bazaz, Arthur, & Tront, 2006)	Aplicaciones de Software	Modelo de Proceso / Objeto de Computación, relación entre las vulnerabilidades, las aplicaciones de software y los recursos del sistema informático.	
9	(Lai & Hsia, 2007)	Redes de Datos	Efectos de las vulnerabilidades.	CVE, NVD, TWCERT/CC
10	(Gupta, Rees, Chaturvedi, & Chi, 2006)	Organización	Sistemas de información de la organización y sus infraestructuras de soporte.	NIST

Las taxonomías que hacen referencia a la *organización* están alineadas y estructuradas según los estándares establecidos y gestionados por el NIST (National Institute of Standards and Technology), en la NVD (National Vulnerability Database), la cual se mantiene actualizada con los informes de los CERTs (Computer Emergency Response Team) asociados. Para medir el impacto de las vulnerabilidades, se utiliza el CVSS (Common Vulnerability Scoring System), que es un marco de trabajo abierto y universalmente utilizado que establece unas métricas para la comunicación de las características, impacto y severidad de vulnerabilidades que afectan a elementos del entorno de seguridad.

Las taxonomías que hacen referencia a las *redes de datos* están estructuradas según los elementos de tecnología de la información de la organización y por el efecto que puedan producir las vulnerabilidades.

Las taxonomías de *software* se estructuran según la complejidad de identificar, solucionar y explotar las vulnerabilidades. Por ejemplo, cómo se hace la clasificación de los errores de software, la taxonomía de (Bazaz & Arthur, 2007) establece la estructura según el modelo de procesos y los elementos de la organización. Las taxonomías de la NVD, que alimentan los CERTs, en su gran mayoría hacen relación a las vulnerabilidades de las aplicaciones de software.

Existe una taxonomía de vulnerabilidades de dispositivos móviles que establece la taxonomía en función de las funcionalidades del sistema operativo y, en este caso particular, para Android.

Del resto de estudios primarios, lo que se ha podido identificar es lo siguiente:

- Para aplicaciones web de código abierto, se utiliza la base de datos OSVDB (Open Sourced Vulnerability Database) y la lista Bugtraq.
- El artículo (Tripathi & Singh, 2010) muestra una lista de propiedades que debe tener una buena taxonomía.
- El artículo (Tripathi & Singh, 2012) muestra una lista de taxonomías de vulnerabilidades de base de datos y su esquema de clasificación.

2.3.2.5 Conclusiones de la Revisión Sistemática de Vulnerabilidades en Ciberseguridad

Una vez que se ha seleccionado y analizado cada uno de los estudios primarios, se identificaron las taxonomías de vulnerabilidades en ciberseguridad publicadas y se determinaron el área y el enfoque, así como información relevante sobre taxonomías de vulnerabilidades.

- Existe un gran esfuerzo por gestionar las vulnerabilidades de aplicaciones de software. Por ello, la NIST es la encargada de gestionar la NVD, la cual se mantiene actualizada con todos los reportes constantes de los CERTs asociados.
- Para poder medir el impacto de las vulnerabilidades, se ha creado el CVSS, sistema de gran ayuda y de continua actualización.
- De las taxonomías analizadas, se han encontrado tres taxonomías para: Aplicaciones de Software, Redes de Datos y Organización, la otra taxonomía existente es de dispositivos móviles.
- El enfoque de las taxonomías es diverso, desde el enfoque de procesos hasta por la funcionalidad que entrega.

El análisis indica que todas las taxonomías se basan en un enfoque específico para realizar su clasificación, que toman en cuenta un concepto de clasificación que se realiza según la necesidad de la organización, y el enfoque que requiera la organización y las necesidades de la misma.

Es común en todas las demás taxonomías que tomen en cuenta el impacto en los activos de la organización.

2.3.3. RS de Taxonomías de Amenazas en Ciberseguridad

Una amenaza es una causa potencial de un incidente que puede causar daños a un sistema de información o a una organización (UNE 71504, 2008). Algunos ejemplos son cuestiones aún por entender, con implicaciones potencialmente serias; indicadores de compromiso, como archivos maliciosos, direcciones de correo electrónico robadas, direcciones IP impactadas o muestras de malware; o información sobre los actores de amenazas. La información sobre amenazas puede ayudar a los operadores a detectar o evitar incidentes, aprender de los ataques y crear soluciones que puedan proteger mejor sus propios sistemas y generar información que pueda ser utilizada por el resto de personas.

En esta revisión sistemática, se pretende responder a través de una revisión sistemática de la literatura a la siguiente pregunta: ¿existe alguna taxonomía de amenazas en ciberseguridad publicada?

2.3.3.1 Identificación de las Necesidades

Se ha requerido una revisión sistemática para identificar las diferentes taxonomías de vulnerabilidades en ciberseguridad que se han publicado.

2.3.3.2 Protocolo de Revisión

En este punto se definen: la formulación de las preguntas a realizar, las fuentes de la base de datos para la búsqueda, la elaboración de las cadenas de búsqueda según los criterios definidos, y la búsqueda en las fuentes, para ubicar y seleccionar los estudios.

- **Formulación de la pregunta:** la pregunta planteada es: ¿qué taxonomías de amenazas se han propuesto para la ciberseguridad?
- **Las bases de datos seleccionadas fueron:** IEEE Computer, Science Direct, ACM Digital Library y Web of Knowledge.
- **Las cadenas de búsqueda** fueron las siguientes:
 - "Cyber Threats" and "Taxonomy".
 - "Cyber Threats" and "Classification".
 - "Taxonomy of Threats".
 - "Classification of Threats".
- **Palabras Claves:** "Cyber Threats". "Taxonomy", "Classification".

2.3.3.3 Revisión

En este punto, se muestra la búsqueda de los documentos en las bases de datos seleccionadas con las cadenas de búsqueda predefinidas. La revisión se realiza en tres fases. Los criterios de inclusión y exclusión establecidos a continuación se han aplicado a los resultados de búsqueda.

Criterios para seleccionar estudios, y procedimientos para inclusión y exclusión

De los resultados encontrados, la Tabla 2-21 enumera los criterios de inclusión y exclusión que se aplicaron a los resultados de la búsqueda inicial. La selección de estudios se ha centrado en aquellos relacionados con las taxonomías de amenazas en ciberseguridad publicadas.

Tabla 2-21. Criterios de Inclusión y exclusión de los estudios (RS Taxonomías de Amenazas de Ciberseguridad, RS TAm)

<i>Inclusión (I)</i>	<i>Exclusión (E)</i>
I1. Estudios empíricos de ciberseguridad que muestren una clasificación de amenazas en ciberseguridad.	E1. Documentos que se basan solo en una opinión particular que no aborda las amenazas en ciberseguridad.
I2. Documentos que analizan taxonomías o clasificaciones de amenazas en ciberseguridad.	E2. Estudios que no son relevantes para la pregunta de investigación o no están relacionados con el estudio particular.

<i>Inclusión (I)</i>	<i>Exclusión (E)</i>
I3. Artículos que incluyen en su contenido las cadenas de búsqueda.	E3. Estudios que no son claros o ambiguos.
I4. Artículos cuyo título, resumen o contenido están relacionados con el tema.	E5. Publicaciones duplicadas.
I5 Documentos de acceso gratuito.	E6 Estudios previos a 1990 debido a la actualización constante en el área.

- En una primera fase de la revisión, haciendo uso de los motores de búsqueda de las bases de datos identificadas y poniendo la cadena de búsqueda elaborada en la tarea "cadenas de búsqueda" de la actividad "Protocolo de Revisión", se encontraron un total de 955 estudios.
- En la segunda fase de la revisión, cada estudio se revisó teniendo en cuenta los criterios de inclusión y exclusión anteriores, obteniendo un total de 29 estudios relevantes. Para seleccionar los estudios pertinentes, se tomaron los siguientes pasos: leer el título, leer el resumen, leer las conclusiones y completar la plantilla creada; si proporcionan suficiente información, el estudio se selecciona y se guarda. De lo contrario, se elimina.
- En la tercera fase de la revisión, se obtuvieron 18 estudios primarios que respondían a las preguntas formuladas inicialmente. La Tabla 2-22 muestra las fuentes, el número total de trabajos y el número de trabajos relevantes y primarios seleccionados por fuente.

Tabla 2-22. Distribución de estudios por fuente (RS TAm)

<i>Fuente</i>	<i>Total</i>	<i>Relevantes</i>	<i>Primarios</i>
IEEE Explore	701	25	17
Science Direct	216	3	1
ACM Digital Library	5	1	0
Web of Knowledge	33	0	0
Total	955	29	18

Evaluación de la calidad de los estudios:

Para la evaluación de la calidad de los estudios, se realizaron las siguientes preguntas:

- ¿Es el estudio primario relevante para la investigación que se está realizando?
- ¿Los estudios primarios proveen la suficiente información como para que los resultados se beneficien de la revisión sistemática?
- ¿Los estudios revisados dan un valor agregado a la investigación que se está realizando?

Realizadas las preguntas anteriormente definidas, se pudo comprobar que los 18 estudios primarios seleccionados son relevantes, proveen suficiente información y dan un valor agregado a la revisión sistemática.

Para cada documento seleccionado, después de leer el texto completo, la información ha permitido el posterior análisis de los resultados.

2.3.3.4 Análisis, Interpretación e Informe de los Resultados

Al final de la revisión sistemática, se ha analizado el contexto de cada documento. Para los documentos que proponían una taxonomía de amenazas en ciberseguridad, se ha analizado la clasificación de amenazas propuestas, y su enfoque y alcance. De la revisión inicial de los 18 estudios primarios, se ha encontrado lo siguiente:

- 9 artículos presentan Taxonomías.

- 9 artículos no presentan taxonomías, sino que describen la importancia de la taxonomía de amenazas en ciberseguridad.

De los artículos que presentan taxonomías de acuerdo a su contexto, se clasificaron en:

- Amenazas de Organización.
- Amenazas de Redes de Datos.
- Amenazas de Web.
- Amenazas de Nube.
- Amenazas de VoIP.

De los 9 artículos que presentan taxonomías, se describen en la Tabla 2-23 los principales elementos encontrados.

Tabla 2-23. Estudios primarios que presentan taxonomías de amenazas

	<i>Artículo</i>	<i>Enfoque</i>	<i>Criterio</i>	<i>Referencia</i>
1	(Rot & Sobinska, 2013)	Organización	Según la estructura de la organización.	CERT
2	(Yu, Thomborson, Wang, Fu, & Wang, 2009)	VoIP	De alto nivel (abuso de servicios).	VOIPSA
3	(Miloslavskaya, Tolstoy, & Zapechnikov, 2016b)	Organización	Tipos de amenazas (integridad física, estructura lógica, contenido, confidencialidad, derechos de propiedad, disponibilidad, privacidad, etc.), naturaleza del origen de la amenaza, fuentes de amenaza y requisitos previos.	
4	(Liu, De Vel, Han, Zhang, & Xiang, 2018)	Organización	Impacto en: confidencialidad, integridad y disponibilidad, e infraestructura de la organización.	CERT
5	(Silva et al., 2016)	Web	Servicio, servicios de consumo, ingeniería social.	
6	(Yahya, Walters, & Wills, 2015)	Nube	Servicios y exposiciones.	
7	(Farooq, Kakakhel, Virtanen, & Isoaho, 2016)	Redes	Compartir información y servicios.	Encuesta
8	(Pitropakis, Darra, Vrakas, & Lambrinoudakis, 2013)	Nube	Servicios y exposiciones (Servicios, Infraestructura, Genérico).	CRAMM OCTAVE
9	(Kishor S. Trivedi, Dong Seong Kim, 2004)	Organización	Servicios y exposición (fallos y errores).	

Las taxonomías enfocadas en la organización, (Rot & Sobinska, 2013), (Miloslavskaya et al., 2016b), (Liu et al., 2018) y (Kishor S. Trivedi, Dong Seong Kim, 2004), presentan una clasificación basada en la estructura de la organización, los servicios que presta y los posibles fallos que pueda presentar.

Las taxonomías orientadas a la nube, (Yahya et al., 2015) y (Pitropakis et al., 2013), están estructuradas según el servicio y la exposición que puede presentar su disponibilidad.

La taxonomía de (Yu et al., 2009) plantea una clasificación de la taxonomía de VoIP desde un alto nivel enfocado en los abusos que se suelen presentar en el servicio de VoIP.

La taxonomía de Web que presenta (Silva et al., 2016) se realiza en función de los servicios que brinda la plataforma.

La taxonomía de redes (Farooq et al., 2016) estructura la taxonomía en base a una encuesta a estudiantes de los servicios de red de una Institución Educativa.

2.3.3.5 Conclusiones de la Revisión Sistemática de Amenazas en Ciberseguridad

Una vez que se ha seleccionado y analizado cada uno de los estudios primarios, se han identificado las taxonomías publicadas de amenazas en ciberseguridad y se ha identificado el área y el enfoque de cada una de ellas, así como información relevante sobre taxonomías de amenazas en ciberseguridad.

- Las taxonomías de amenazas presentadas son de investigaciones muy particulares, no cubren todas las necesidades de una organización y no existe una política de actualización continua.
- Los trabajos revisados muestran que es un trabajo bastante difícil el proponer una taxonomía que sea de utilidad general y que cumpla con las expectativas de la industria.
- En los trabajos revisados, se menciona que como líneas futuras de trabajo se deben establecer mecanismos oportunos para mantener una taxonomía adecuada de amenazas que sea estándar en la industria y que pueda ser actualizada de forma continua.

El análisis indica que todas las taxonomías se basan en un enfoque específico para realizar su clasificación, que toman en cuenta un concepto de clasificación que se realiza según la necesidad de la organización, y el enfoque que requiera la organización y las necesidades de la misma.

Para poder identificar taxonomías de amenazas no generalistas, auspiciadas por entidades de reconocimiento internacional y que sean referentes para establecer estándares en la industria, se debe realizar un análisis de estas taxonomías en entidades gubernamentales y en organismos que lideran las buenas prácticas en la industria.

2.4. Consideraciones Finales

En este capítulo se hace referencia a la revisión de la literatura de los diferentes artículos científicos y no científicos relacionados con la madurez en la identificación y evaluación de riesgos en ciberseguridad, considerando los elementos más importantes que deben ser analizados.

Los principales resultados que podemos destacar de este capítulo son los siguientes:

- La primera revisión sistemática realizada se ha enfocado en los modelos de madurez de seguridad de la información, en donde se ha podido observar que no existen modelos de madurez enfocados específicamente en ciberseguridad, sino que muchos de ellos se han adaptado a este enfoque.
- Luego de la revisión sistemática de modelos de madurez, la industria publicó un modelo de madurez específico para ciberseguridad publicado en marzo de 2020, mostrando la importancia que tiene la ciberseguridad para la industria.
- Al realizar una comparativa de los modelos de madurez revisados, se ha identificado que la base fundamental de su estructura son la evaluación y análisis de riesgos en ciberseguridad.
- La revisión sistemática de taxonomías de riesgos en ciberseguridad ha determinado que existen pocas taxonomías de riesgos, pues la mayoría son esfuerzos propios de las organizaciones, donde para poder gestionar los riesgos en una organización es importante identificar los activos de la organización, las vulnerabilidades de ciberseguridad asociadas a los mismos, y las amenazas en ciberseguridad que se aprovechan de las vulnerabilidades en ciberseguridad de los activos de la organización.

- No existe un marco conceptual común para la ciberseguridad, ya que los modelos conceptuales identificados se basan en enfoques particulares y usan diferentes semánticas para las relaciones de los principales elementos de los riesgos de ciberseguridad (activos, vulnerabilidades, amenazas y riesgos).
- Los activos en ciberseguridad de las organizaciones son muy particulares de cada una de ellas, y dependen de su naturaleza y fin. Por ello, tener una taxonomía de activos en ciberseguridad es una tarea bastante compleja, pues existen muchos tipos de organizaciones y lo único que se ha tratado es de generar taxonomías muy generales y a un nivel muy alto de especificación.
- De las taxonomías de vulnerabilidades de ciberseguridad publicadas, las de aplicaciones de software están continuamente actualizadas por parte de NIST, que gestiona la NVD, e inclusive existe el CVSS (Common Vulnerability Scoring System) que permite medir el impacto de las mismas. Además, la mayoría de las vulnerabilidades de ciberseguridad que se informan están enfocadas en los sistemas de software.
- No existe un número amplio de taxonomías de amenazas en ciberseguridad, sin embargo, existen taxonomías de organizaciones que administran y mantienen actualizadas continuamente estas taxonomías y gestionan las buenas prácticas de la industria como, por ejemplo, la taxonomía publicada por ENISA (European Union Agency for Network and Information Security).

3. PLATEAMIENTO DEL PROBLEMA E HIPÓTESIS DEL TRABAJO

En este capítulo se hace un repaso sobre la problemática de la gestión de riesgos en ciberseguridad, tema a investigar en esta tesis doctoral, y se analizan los trabajos previos realizados que, hasta la fecha, aportan alguna solución a la identificación y evaluación de riesgos en ciberseguridad, y que hay que tener en cuenta en la definición de un marco de trabajo. Posteriormente, se plantean las hipótesis de esta tesis doctoral, las cuales serán validadas al final del trabajo de investigación, y, finalmente, se presenta una breve descripción de cómo se va enfrentar la problemática identificada.

3.1. *Visión general del problema*

En el capítulo 1 se ha mostrado que el termino Ciberseguridad es ampliamente utilizado para hablar de la seguridad de los sistemas y los datos, y que su interés está en aumento (Enterprise Cybersecurity, 2015), debido a que estamos cada vez más interconectados y en línea. Además, el daño de las amenazas cibernéticas está aumentando dramáticamente, día a día, y en los últimos años, los costos por los delitos cibernéticos son significativos, según el estudio “The Cost of Cybercrime” (Accenture and Ponemon Institute, 2019) del año 2019.

En el contexto que nos ocupa, se han descrito algunas amenazas de ciberseguridad, las formas de ataques y quienes lo realizan. También se han descrito las características de algunos marcos de trabajo de ciberseguridad, y se identificaron algunas características en común:

- Los marcos dividen la empresa y su protección en varias áreas funcionales, que permiten la organización lógica y la gestión de un programa general de defensa cibernética.
- Casi todos los marcos principales aprovechan la metodología de gestión de riesgos como punto de partida.
- Todos estos marcos hablan de controles de seguridad.
- Estos marcos proporcionan un mecanismo para auditar, evaluar y validar la presencia o ausencia de los controles descritos en el marco.

Sobre la segunda característica común, de aprovechar la metodología de gestión de riesgos, es importante que exista un marco de trabajo de gestión de riesgos en ciberseguridad. Todos buscan objetivar el análisis de riesgos y medir su impacto en las organizaciones y, por ello, es necesario elaborar un marco de trabajo de gestión de riesgos en ciberseguridad.

El capítulo 2 aporta una revisión sistemática de los modelos de madurez en ciberseguridad, analizando el enfoque, aplicación y estructura de cada modelo de madurez. Posteriormente, se ha realizado un estudio comparativo de los modelos de madurez descritos y analizados, para poder establecer las características comunes y diferencias notables de los mismos, siendo lo mas sobresaliente, que todos los modelos de madurez más nombrados en los artículos científicos se basan en la gestión de riesgos de ciberseguridad en el nivel inicial de madurez.

También se ha realizado una revisión de los principales conceptos de riesgos en ciberseguridad, en los que se incluyen vulnerabilidades, amenazas y riesgos en ciberseguridad. Se describen los resultados de la revisión sistemática de taxonomías de riesgos en ciberseguridad. Además, se describen algunos modelos conceptuales de riesgos en ciberseguridad analizados. Finalmente, se han realizado revisiones sistemáticas adicionales sobre taxonomías de activos, y de vulnerabilidades y de amenazas en ciberseguridad.

Concluidos los trabajos de la revisión de la literatura de los diferentes artículos científicos y no científicos relacionados con la madurez en la identificación y evaluación de riesgos en ciberseguridad, y considerando los elementos más importantes que deben ser analizados, se ha podido observar que hay un vacío en relación con el tema de la tesis doctoral motivado porque:

- No existen modelos de madurez enfocados específicamente en ciberseguridad, sino que muchos de ellos se han adaptado a este enfoque, pero su estructura incluye la evaluación y análisis de riesgos en ciberseguridad.
- Existen pocas taxonomías de riesgos de ciberseguridad, y las que hay son esfuerzos propios de las organizaciones, enfocadas en la naturaleza de su negocio y muy particulares.
- Las taxonomías de vulnerabilidades y amenazas de ciberseguridad son muy particulares según el enfoque propio del negocio, sin embargo, se puede tomar de estándares internacionales como ISO 27005 y las publicadas por ENISA.
- Los modelos conceptuales tienen enfoques diferentes según las necesidades puntuales, sin embargo, describen los elementos de la gestión de riesgos en ciberseguridad. Los modelos revisados se basan en las amenazas de ciberseguridad y no, en las vulnerabilidades de ciberseguridad de los activos de ciberseguridad. Además, no dimensionan el daño de las vulnerabilidades de ciberseguridad en las dimensiones de seguridad, y tampoco se calcula el costo del daño de la vulnerabilidad en el activo de la organización, lo que afectaría directamente al impacto de las amenazas y al costo asociado al cálculo del riesgo en ciberseguridad.

Con todo ello, el trabajo realizado en el Capítulo 2 de esta tesis aporta un conjunto de relaciones de riesgos en ciberseguridad, que determinan los elementos que componen un marco de trabajo de riesgos en ciberseguridad. Esta estructura de relaciones de riesgos en ciberseguridad sirve de punto de partida para la aproximación a la solución del problema que se plantea en el apartado siguiente y para la definición de las hipótesis de esta tesis doctoral.

3.2. Aproximación a la solución

En esta tesis doctoral se propone una solución al problema a través de la elaboración de un marco de trabajo para la gestión de riesgos en ciberseguridad que: 1) sea aplicable en la identificación y evaluación de riesgos en ciberseguridad, 2) establezca la base para la elaboración de una metodología para la gestión de riesgos en ciberseguridad, y 3) integre los elementos más importantes y las buenas prácticas de un marco de trabajo.

Por lo tanto, el trabajo de investigación realizado en esta tesis doctoral y las actividades que nos aproximan a la solución del problema deseada se pueden secuenciar como sigue:

1. Analizar la importancia de ciberseguridad, describir las amenazas más comunes, las formas de ataques y quienes lo realizan, así como también describir los marcos de ciberseguridad involucrados.
2. Analizar los distintos modelos de madurez en ciberseguridad, su estructura, procesos, estándares y su enfoque en la gestión de la seguridad de TI en las organizaciones. Para ello, se establecerán las bases para realizar un análisis comparativo de los modelos de madurez en ciberseguridad, indicando los criterios más relevantes e importantes y, posteriormente, se realizará el análisis comparativo de los principales modelos definidos.
3. Realizar una revisión sistemática de taxonomías de riesgos en ciberseguridad con objeto de identificar las taxonomías definidas, para poder identificar los modelos conceptuales descritos, e identificar los elementos utilizados y sus relaciones.
4. Analizar los diferentes modelos conceptuales para la gestión de riesgos en ciberseguridad, identificando los elementos principales (activos, y vulnerabilidades y amenazas de ciberseguridad) y las relaciones entre ellos.
5. Realizar una revisión sistemática de taxonomías de los activos, y vulnerabilidades y amenazas de ciberseguridad, con objeto de completar este estudio e identificar las taxonomías definidas, para poder utilizarlas como punto de partida en las organizaciones.
6. Crear un marco de trabajo de gestión de riesgos en ciberseguridad que identifique los elementos que participan y sus relaciones, y la descripción de las actividades a ser implementadas, para medir el impacto de los riesgos en ciberseguridad en la organización.

7. Validar el marco de trabajo propuesto a través de su aplicación en un prototipo, para ser aplicado en una organización, ya sea pública o privada.

Los puntos del 1 al 5 han sido desarrollados en los Capítulos 1 y 2. En el Capítulo 4 se desarrolla el punto 6. Este capítulo define el marco de trabajo para la gestión de riesgos en ciberseguridad, en el que se incluyen los elementos que participan, las relaciones entre los elementos y la descripción de las actividades a ser realizadas. En el Capítulo 5 se desarrolla el punto 7, validando el marco de trabajo de gestión de riesgos en ciberseguridad propuesto, a través de la experimentación en distintas empresas en Ecuador, tanto públicas como privadas y que tengan la infraestructura necesaria para ser analizada.

Por lo tanto, el marco propuesto pretende “facilitar a las empresas la identificación y evaluación de riesgos en ciberseguridad, definiendo detalladamente los elementos a ser considerados, las relaciones que deben tener y las actividades a ser realizadas”.

Finalmente, se debe considerar que el marco propuesto tiene que:

- Permitir la cuantificación del costo de impacto para cada vulnerabilidad de los activos identificados.
- Posibilitar que cada riesgo de ciberseguridad tenga asociado un valor de impacto total según las vulnerabilidades que tengan los activos de la organización.

3.3. Hipótesis del trabajo

Un marco de trabajo es un conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática particular que sirve como referencia, para enfrentar y resolver nuevos problemas de índole similar, y que facilita el cumplimiento de los objetivos propuestos. Además, establece una guía para que pueda repetirse y que ayude a mejorar los resultados de las acciones, reduciendo los errores más comunes. El marco que se propone pretende:

- Tener un modelo conceptual que incluya los elementos identificados y sus relaciones, así como las actividades a realizar.
- A través del modelo, ayudar en la mejora de la identificación y evaluación de riesgos en ciberseguridad.

Así, en este apartado se plantean la siguiente hipótesis general, y sus hipótesis derivadas, del trabajo de investigación.

HIPOTESIS GENERAL. Si una empresa, sea cual sea su sector de negocio, se apoya en un marco de trabajo que le facilite un modelo para identificar y evaluar los riesgos de ciberseguridad, conseguirá mejorar la evaluación de riesgos en la implementación de los conceptos de ciberseguridad en la empresa.

HIPÓTESIS DERIVADA 1. Si una empresa define una clasificación de los tipos de activos de ciberseguridad, para identificar y catalogar los activos de ciberseguridad según su naturaleza, entonces permitirá clasificarlos, para facilitar la identificación de características y vulnerabilidades comunes.

HIPÓTESIS DERIVADA 2. Si una empresa define las taxonomías de vulnerabilidades y amenazas de ciberseguridad, para implementarlas y gestionarlas según las necesidades de la empresa, inclusive incluir nuevos elementos, entonces la identificación y evaluación de estos elementos será única sin posibilidad de ambigüedades o diferencias de sintaxis, que faciliten la gestión de vulnerabilidades y amenazas de ciberseguridad.

HIPOTESIS DERIVADA 3. Si una empresa en la identificación y evaluación de riesgos de los activos de ciberseguridad, asocia las vulnerabilidades a las dimensiones de seguridad y mide cada una de ellas como valor del daño de la vulnerabilidad, entonces el promedio del valor del daño de las vulnerabilidades en cada dimensión de seguridad, generará un valor del daño más representativo y justificado de cada vulnerabilidad.

HIPOTESIS DERIVADA 4. Si una empresa al realizar una identificación y evaluación de riesgos de sus activos de ciberseguridad, puede medir el costo del daño de cada vulnerabilidad, entonces la materialización de cada vulnerabilidad genera un costo de daño que puede acumularse y asociarse a la amenaza que lo materializa.

HIPÓTESIS DERIVADA 5. Si una empresa genera una matriz de gestión de riesgos en ciberseguridad que incluya además de las amenazas, daño, probabilidad de ocurrencia, medida de riesgo asociado y el costo total de cada amenaza, entonces podrá ser una herramienta que ayude a identificar los costos relacionados a cada amenaza, permitiendo a las autoridades tomar una decisión, para priorizar los riesgos a ser gestionados.

HIPÓTESIS DERIVADA 6. Si una empresa al identificar las contramedidas de los riesgos de ciberseguridad identificados, lo hace para cada una de las vulnerabilidades analizadas, entonces podrá generar contramedidas para cada vulnerabilidad que esté presente en muchos activos y mejorar la mitigación de los riesgos en ciberseguridad, con menor cantidad de contramedidas.

4. RESOLUCION DEL PROBLEMA

Una vez realizada la revisión de la literatura relativa a modelos de madurez en ciberseguridad y taxonomías de los diferentes elementos que participan para identificar y evaluar los riesgos de ciberseguridad, así como se refleja en el capítulo 2, hemos encontrado que no existe una postura común que identifique las relaciones que tienen los elementos de riesgo en ciberseguridad (activos, y vulnerabilidades y amenazas de ciberseguridad). También algunas herramientas que existen en el mercado para la gestión de riesgos (M. Rea-Guaman, J. A. Calvo-Manzano, 2018)(M. Rea-Guaman, J. A. Calvo-Manzano, 2018), no contemplan los elementos mencionados y, además, cada una de ellas se basa en su visión muy particular, como por ejemplo en amenazas, dejando de lado las vulnerabilidades de los activos.

Por tal razón, es necesario establecer un modelo conceptual del dominio que establezca las relaciones de los elementos encontrados en la gestión de riesgos en ciberseguridad. Para ello, se empezará realizando un modelo conceptual del dominio, luego se describirá la metodología para poder identificar y evaluar los riesgos de ciberseguridad y, por último, se realizará un prototipo/herramienta para validar el modelo conceptual siguiendo la metodología descrita previamente.

En lo referente a las taxonomías de activos, y vulnerabilidades y amenazas de ciberseguridad, se ha elaborado una taxonomía de cada uno de estos conceptos, en donde se recopila la información encontrada en las revisiones sistemáticas para que puedan ser utilizadas en lo posterior por la organización, definiéndose de esta manera una taxonomía única de estos elementos de ciberseguridad en la organización. Las mencionadas taxonomías están descritas en el Anexo II de este documento.

A continuación, se describe el conjunto de actividades realizadas para establecer el modelo conceptual del dominio, el marco de trabajo definido de identificación y evaluación de riesgos en ciberseguridad, y el prototipo/herramienta realizado.

4.1. Modelo Conceptual del Dominio

De la revisión de la literatura existente sobre la gestión de riesgos en ciberseguridad, se analizaron los diferentes elementos que participan en la gestión de riesgos y, específicamente, en la identificación y evaluación de riesgos en ciberseguridad. En el capítulo 2 de estado de la cuestión, sección 2.2.3, se ha analizado el modelo conceptual de riesgos en ciberseguridad, revisando algunos diagramas de elementos y relaciones de los mismos. A continuación, se presentan los elementos y relaciones que participan en este tema.

De la revisión sistemática de taxonomía de riesgos en ciberseguridad capítulo 2, sección 2.2, se han clasificado los artículos según el enfoque del mismo, y se han determinado los elementos principales del modelo conceptual y sus relaciones. Esta información ha servido de base para el diseño del modelo conceptual propuesto. Los documentos que se han tenido en cuenta han sido:

- (Singh, 2014), enfocado en relación de términos, ontologías de seguridad.
- (Singhal & Wijesekera, 2010), enfocado en entidades y relaciones.
- (Singhal & Singapogu, n.d.), enfocado en entidades y relaciones.
- (NIST, 2012), enfocado en los principales factores de riesgo.
- (Goodwin et al., 2015), enfocado en información de ciberseguridad.

Asimismo, se han tomado en cuenta para esta propuesta, algunos documentos de ontologías y taxonomías, que son los siguientes:

- (Buchanan, Larkin, & D'Amico, 2012), enfocado en ontologías de activos por usuario.
- (Shamala & Ahmad, 2014), enfocado en taxonomía de activos.
- (Wielki, 2006), enfocado en taxonomía de impactos en los activos.

- (Yazid, Faizal, Rabiah, Shahrin, & Solahuddin, 2012), enfocado en taxonomía de activos de móviles.
- (Farooq, Kakakhel, Virtanen, & Isoaho, 2016), enfocado en taxonomía de amenazas.
- (Yu, Thomborson, Wang, Fu, & Wang, 2009), enfocado en taxonomía de amenazas de voz sobre IP.
- (Razzaq, Anwar, Ahmad, Latif, & Munir, 2014), enfocado en ontología de ataques.
- (Shameli-Sendi, Aghababaei-Barzegar, & Cheriet, 2016), enfocado en taxonomía de ataques.
- (Bazaz & Arthur, 2007), enfocado en taxonomía de vulnerabilidades.
- (Zhao & Dai, 2012), enfocado en taxonomía de vulnerabilidades basada en atributos de información.
- (Shahriar & Zulkernine, 2011), enfocado en taxonomía de vulnerabilidades.
- (Igre & Williams, 2008), enfocado en taxonomía de vulnerabilidades.

4.1.1. Elementos y relaciones en el modelo conceptual del dominio

Los elementos y relaciones identificadas se han diagramado considerando la importancia que tienen las vulnerabilidades de ciberseguridad de los activos de la organización, y su efecto posterior en la gestión de amenazas, riesgos y contramedidas de ciberseguridad.

En esta sección se describen los elementos y relaciones identificadas en la revisión sistemática de taxonomía de riesgos en ciberseguridad del capítulo 2, sección 2.2.2, los mismos que han definido el modelo conceptual del dominio.

Activo. Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos (UNE:71504, 2008).

Los activos esenciales son la información y los servicios prestados; pero estos activos dependen de otros activos más prosaicos, como pueden ser los equipos, las comunicaciones, las instalaciones y las personas que trabajan con aquellos. Los activos son lo que queremos proteger (Ministerio de Administraciones Públicas, 2006).

Tipo de Activo. Es la clasificación que puede tener un activo según sus características o funcionalidades que pueda tener, así como en función del objetivo del mismo que tenga en la organización. La clasificación es dada por la organización según su necesidad y política interna.

Unidad Organizacional. Los activos deben ser asignados a un área de la organización y tener una persona/unidad responsable del mismo.

Vulnerabilidad. Defecto o debilidad en el diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza. Propiedades intrínsecas que pueden llegar a presentarse como resultado de una sensibilidad a una fuente de riesgo que puede conducir a un suceso con una consecuencia (UNE-ISO GUIA 73, 2010).

Se denomina vulnerabilidad a toda debilidad que puede ser aprovechada por una amenaza o, más detalladamente, a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial (Ministerio de Administraciones Públicas, 2006). Podemos decir que la vulnerabilidad es un factor intrínseco a los activos.

En la Figura 4-1, se muestran las relaciones de los elementos antes mencionados.

Figura 4-1. Relación Activo y Vulnerabilidad

A continuación, en la Tabla 4-1, se detallan las dependencias de los elementos mostrados en la Figura 4-1:

Tabla 4-1. Relación entre entidades de Activos

NOMBRE	DESCRIPCIÓN
1. Activo – Vulnerabilidad PRESENTA	Un activo puede tener muchas vulnerabilidades, y una vulnerabilidad se puede presentar en muchos activos.
2. Activo – Tipo de Activo TIENE	Un activo puede pertenecer a un tipo de activo según sus características, y un tipo de activo tendrá muchos activos asociados a su naturaleza.
3. Activo – Unidad Organizacional ES RESPONSABLE DE	El activo siempre pertenecerá a alguna unidad organizacional de la empresa, y la unidad organizacional podrá tener muchos activos.
4. Activo – Activo CONTIENE	Un activo puede ser el contenedor de otros activos formando un solo componente.
5. Activo – Activo DEPENDE	Un activo puede ser parte de un activo que contiene a él y muchos más.

Otro concepto importante que se ha encontrado es la relación Activo – Vulnerabilidad y su Valoración del impacto asociado a la vulnerabilidad (que puede afectar al valor del activo), en función de las dimensiones de confidencialidad, integridad y disponibilidad.

Dimensión Valoración. Las dimensiones son las características o atributos que hacen valioso un activo. Una dimensión es una faceta o aspecto de un activo, independiente de otras facetas. Puede hacerse un análisis de riesgos enfocado en una sola faceta independiente de lo que pueda ocurrir con las otras facetas.

Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión (Ministerio de Administraciones Públicas, 2006).

Para cada activo, se identifican las dimensiones siguientes:

- Confidencialidad: ¿qué daño causaría si lo conociera quien no debe? Esta valoración es típica de datos.
- Integridad: ¿qué perjuicio causaría si estuviera dañado o corrupto? Esta valoración es típica de datos, que pueden estar manipulados, ser total o parcialmente falsos o, incluso, faltar datos.
- Disponibilidad: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios.

Una vez determinadas qué dimensiones interesan de un activo, hay que valorarlas.

Valoración del Impacto. La valoración del impacto es la determinación del coste de una incidencia que afectara al activo.

La valoración del impacto se puede ver desde diferentes perspectivas. Una de estas perspectivas es la ‘necesidad de proteger’, es decir, cuanto más valioso es una dimensión de un activo, mayor nivel de protección se requerirá en la dimensión (o dimensiones) que sean pertinentes.

Se denomina impacto a la medida del daño sobre el activo, derivado de la materialización de una amenaza.

El impacto se valora en términos del coste derivado del valor de los activos afectados. El impacto se suele estimar en porcentaje de degradación que afecta al valor del activo así, por ejemplo, el 100% sería la pérdida total del activo.

Tipo de Valoración. La valoración puede ser cualitativa o cuantitativa. La selección del tipo de valoración dependerá de las características del activo.

Teniendo en cuenta los conceptos anteriores y estos nuevos elementos, en la Figura 4-2, se añaden las nuevas relaciones y elementos.

Figura 4-2. Relación Activo, Vulnerabilidad y Dimensión_Valoración

A continuación, en la Tabla 4-2, se detallan las dependencias de los elementos agregados al modelo conceptual mostrados en la Figura 4-2 :

Tabla 4-2. Relación de entidades de Vulnerabilidad

<i>NOMBRE</i>	<i>DESCRIPCIÓN</i>
1. Activo – Vulnerabilidad – Dimensión Vulnerabilidad – Tipo Valoración VALORACION IMPACTO	El activo podría hacer una valoración de impacto, por cada vulnerabilidad en una o varias dimensiones de valoración, tomando en cuenta el tipo de valoración.

Una vez que se encuentran valorados los impactos en los activos, hay que catalogar las amenazas que pueden afectar a los activos. A continuación, se describen estos conceptos complementarios.

Amenaza. Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización (UNE:71504, 2008). Algunos ejemplos de amenazas pueden ser archivos maliciosos, direcciones de correo electrónico robadas, direcciones IP impactadas o muestras de malware.

La información sobre amenazas puede ayudar a los operadores a detectar o evitar incidentes, aprender de los ataques y crear soluciones que puedan proteger mejor sus propios sistemas y los de los demás.

Fuentes. Una fuente es el origen identificado de una amenaza.

Tipo de Fuentes. El tipo de fuente de amenazas ayuda a clasificar las amenazas para poder identificar de mejor manera las evaluaciones de riesgo. Entre los tipos de fuentes que pueden ser considerados, se pueden mencionar los siguientes: Competidor, Accidental, Estructural, Ambiental. Durante las evaluaciones de riesgo, las organizaciones determinan qué tipos de fuentes de amenazas se deben considerar. Para ello, deben poner en marcha el proceso utilizado para identificar amenazas y cualquier suposición relacionada con el proceso de identificación de las mismas.

Riesgo (dato secundario). Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. Efecto de la incertidumbre sobre la consecución de los objetivos (UNE-ISO GUIA 73, 2010).

Al riesgo se le conoce como la probabilidad de que se produzca un incidente de seguridad, llegando a materializarse una amenaza, causando pérdidas y daños. El riesgo depende, por tanto, de los siguientes factores:

- la probabilidad de la amenaza, y
- el daño (impacto) que produce la ejecución de esta amenaza.

El producto de estos factores representa el riesgo.

$$\text{Riesgo} = \text{Impacto} \times \text{Probabilidad de Ocurrencia (amenaza)}$$

En la Figura 4-3 se muestran estos nuevos elementos y relaciones.

Figura 4-3. Relación Activo, Vulnerabilidad y Dimensión_Valoración, Amenaza

A continuación, en la Tabla 4-3, se detallan las dependencias de los elementos agregados al modelo conceptual mostrados en la Figura 4-3:

Tabla 4-3. Relación de entidades de Amenaza

NOMBRE	DESCRIPCIÓN
1. Vulnerabilidad – Amenaza APROVECHA (EXPLOTA)	Una amenaza puede explotar las vulnerabilidades de los activos, y una vulnerabilidad puede estar presente en muchas amenazas.
2. Amenaza – Fuente TIENE	Una amenaza debe tener al menos una fuente, y las fuentes pueden estar en varias amenazas
3. Fuente – Tipo_Fuente ES	Las fuentes de amenaza deben ser de un tipo, y el tipo puede estar en varias amenazas.

Control. Un control es un mecanismo que está diseñado para evitar que las amenazas sucedan o, en su defecto, para mitigar su impacto cuando lo hacen. Por ello, es importante tener una medida de la efectividad y eficiencia de las **contramedidas** disponibles. Por esto, es importante conocer la precisión de la contramedida.

Incidente. Suceso (inesperado o no deseado) con consecuencias en detrimento de la seguridad del sistema de información (UNE:71504, 2008).

También se puede definir como evento de seguridad de la información: aparición identificada de un sistema, servicio o estado de la red que indica una posible infracción de la política de seguridad de la información o fallo de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad (ISO/IEC 27000, 2014).

El diagrama con los nuevos conceptos y relaciones de las entidades identificadas se muestra en la Figura 4-4.

Figura 4-4. Modelo conceptual de identificación y evaluación de riesgos

A continuación, en la Tabla 4-4, se detallan las dependencias de los elementos agregados al modelo conceptual mostrados en la Figura 4-4:

Tabla 4-4. Relación de entidades de Incidente y Contramedida

NOMBRE	DESCRIPCIÓN
1. Vulnerabilidad – Contramedida REDUCE	Una contramedida puede reducir el efecto negativo que pueda tener una vulnerabilidad, y una contramedida puede ayudar a muchas vulnerabilidades.
2. Control – Contramedida POSEE	Un control puede poseer o no algunas contramedidas, y una contramedida siempre ayudará a un control.
3. Amenaza – Incidente IMPLEMENTA	Una amenaza puede ser implementada por un incidente o no, y el incidente se aprovecha de una o varias amenazas.

4.2. Marco de trabajo para la Identificación y Evaluación de riesgos en Ciberseguridad

Una vez definido el modelo conceptual del dominio, se va a definir el marco de trabajo para la identificación y evaluación de riesgos en ciberseguridad, que incluya las actividades y tareas a realizar.

Como complemento al modelo conceptual del dominio definido, en este punto se describe el marco de trabajo a establecer, utilizando el modelo definido previamente. Para la descripción de las actividades y tareas a considerar, se ha establecido un pequeño ejemplo demostrativo que explique de mejor manera el marco de trabajo definido.

Para explicarlo de mejor manera, se ha elaborado un diagrama de flujo del marco de trabajo que ayude a entender las actividades y tareas a realizar. El diagrama se muestra en la Figura 4-5.

Figura 4-5. Diagrama de Flujo del Marco de Trabajo

Aquí, se van a describir las actividades y tareas del marco de trabajo elaborado, y que hemos denominado **AVARCIBER** (Activos – Vulnerabilidades – Amenazas – Riesgos CIBERseguridad).

Para validar el modelo conceptual del dominio, se aplica a un ejemplo que permita visualizar las actividades y tareas descritas, así como los cálculos que deben realizarse. A continuación, se describen estas actividades y tareas que se deben realizar en el marco de trabajo definido.

Actividad 1: Lanzamiento

Como actividad inicial, es importante tener un catálogo de los elementos que participan en el modelo conceptual. Para ello, se han definido las taxonomías de estos elementos, las cuales son el resultado de las revisiones sistemáticas realizadas en el capítulo 2. Las taxonomías definidas se describen en las siguientes tareas:

Tarea 1: se define la taxonomía de tipos de activos de la organización enfocados en ciberseguridad en base al estándar ISO 27005 (ISO/IEC 27000, 2018).

Tarea 2: se determina la taxonomía de Vulnerabilidades en ciberseguridad en base al estándar ISO 27005 (ISO/IEC 27000, 2018).

Tarea 3: se establece la taxonomía de Amenazas en ciberseguridad en base al estándar ENISA 2016 (Marinos, 2016).

Estas taxonomías, una vez definidas, deberán ser actualizadas continuamente, debido al avance de la tecnología y las necesidades de la industria, que generará la aparición de nuevas amenazas y vulnerabilidades de ciberseguridad, así como de tipos de activos en ciberseguridad.

Actividad 2: Identificar y evaluar Activos

Esta actividad se refiere al proceso inicial que toda organización debe realizar para comenzar con la concienciación de la ciberseguridad por parte de todo el personal de la organización. Una de

las preguntas iniciales que se debe hacer es: ¿qué queremos proteger? Para ello, se hace un análisis de los elementos que son más importantes para la organización, tomando en consideración las siguientes cuestiones:

- ¿Qué actividad realizamos?
- ¿Qué es lo más importante para la organización?
- ¿Cuáles son los objetivos institucionales?
- ¿Qué servicios proporciono?

A continuación, se muestran las tareas necesarias para esta actividad.

Tarea 1: se toman los tipos de activos de ciberseguridad de la taxonomía previamente establecida, en la Actividad 1 – Tarea 1. Aquí, se identifican los activos de ciberseguridad y se asigna el tipo al que corresponde, como se puede ver en la Tabla 4-5.

Tabla 4-5. Activos y tipos de activos

<i>Tipo Activo</i>	<i>Activo</i>
Hardware	Servidor
Hardware	Almacenamiento
Software.	Sistema de monitoreo
Red	Firewall

Tarea 2: se identifican las dimensiones de seguridad (comúnmente, confidencialidad, integridad y disponibilidad) para los activos de ciberseguridad, y se mide el impacto de las dimensiones en cada activo de ciberseguridad basándose en el estándar ISO 27005. El impacto tomará los valores de la Tabla 4-6.

Tabla 4-6. Valoración del impacto para un activo

<i>RANGO</i>	<i>Valor Superior</i>	<i>Valor Inferior</i>
Alto	10	8
Medio	7	5
Bajo	4	2
Nulo	1	0

Para poder establecer los valores, se debe considerar para cada dimensión los siguientes criterios de valoración, según muestra la Tabla 4-7.

Tabla 4-7. Criterios de valoración dimensiones de Seguridad

<i>Criterio de valoración CONFIDENCIALIDAD</i>	
¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?	
Alta (A)	Información que puede ser conocida y utilizada por un grupo muy reducido de agentes, cuya divulgación podría ocasionar un perjuicio a la organización
Media (M)	Información que solo puede ser conocida y utilizada por un grupo de agentes, que la necesiten para realizar su trabajo.
Baja (B)	Información que puede ser conocida y utilizada por todos los agentes de la organización.
Nula (N)	Información que puede ser conocida y utilizada sin autorización por cualquier persona, dentro o fuera de la organización.

Criterio de valoración INTEGRIDAD	
¿Qué importancia tendría que los datos fueran modificados fuera de control?	
Alta (A)	Información cuya modificación no autorizada no podría repararse, impidiendo la realización de las actividades de la organización.
Media (M)	Información cuya modificación no autorizada es de difícil reparación y podría ocasionar un perjuicio significativo para la organización o terceros.
Baja (B)	Información cuya modificación no autorizada puede repararse, aunque podría ocasionar un perjuicio para la organización o terceros.
Nula (N)	Información cuya modificación no autorizada puede repararse fácilmente, o que no afecta a las actividades de la organización.
Criterio de valoración DISPONIBILIDAD	
¿Qué importancia tendría que el activo no estuviera disponible?	
Alta (A)	Información cuya inaccesibilidad permanente durante una hora podría impedir la ejecución de las actividades de la organización.
Media (M)	Información cuya inaccesibilidad permanente durante la jornada laboral podría impedir la ejecución de las actividades de la organización.
Baja (B)	Información cuya inaccesibilidad permanente durante una semana podría ocasionar un perjuicio significativo para la organización.
Nula (N)	Información cuya inaccesibilidad no afecta la actividad normal de la organización.

Para el ejemplo que vamos a seguir, los valores de las dimensiones de seguridad quedarían como se muestran en la Tabla 4-8.

Tabla 4-8. Valoración del impacto del Activo

Tipo Activo	Activo	Dimensión		
		Confidencialidad	Integridad	Disponibilidad
Hardware	Servidor	5	6	8
Hardware	Almacenamiento	9	7	5

Tarea 3: se añade la criticidad del activo como una nueva dimensión de seguridad, que será calculada como el valor más alto del resto de dimensiones de seguridad. En el caso del ejemplo, sería:

- Servidor: máximo de 5, 6 y 8, luego el valor de la criticidad sería 8.
- Almacenamiento: máximo de 9, 7 y 5, luego el valor de la criticidad sería 9.

El valor de la criticidad del activo será en lo posterior el valor de la dimensión de **Criticidad** para todas las vulnerabilidades que se lleguen a identificar al activo de ciberseguridad en cuestión.

Tarea 4: se le asigna el costo monetario que la organización calcula a cada activo. Dicho costo monetario se calcula en función de lo que supondría la pérdida o daño del activo analizado, así como el costo actual del activo. El valor monetario es determinado por el criterio experto del dueño del activo. En el caso del ejemplo, en la columna *Costo del Activo* de la Tabla 4-9 se muestra dicho valor.

Tabla 4-9. Valoración del Costo del Activo

<i>Tipo de Activo</i>	<i>Activo</i>	<i>Costo del Activo</i>	<i>Dimensión</i>			
			Confidencialidad	Integridad	Disponibilidad	Criticidad
Hardware	Servidor	10.000,00	5	6	8	8
Hardware	Almacenamiento	2.000,00	9	7	5	9

Actividad 3: Evaluar el nivel de daño para las tuplas Vulnerabilidad – Activo (dimensión)

En esta actividad se debe determinar cuál es el daño que van a producir las vulnerabilidades en cada uno de los activos de la organización previamente identificados. La valoración del daño de la vulnerabilidad se hará en base a los valores de la Tabla 4-10 (o su equivalente, establecida por la organización). La organización debe determinar el valor del daño de la vulnerabilidad en cada una de las dimensiones (confidencialidad, integridad, disponibilidad y criticidad) del activo. El costo del daño de la vulnerabilidad se calcula determinando el impacto, la importancia y la repercusión que puede tener el daño en el activo de la organización.

Tabla 4-10. Valoración del daño de las vulnerabilidades

<i>RANGO</i>	<i>Valor Superior</i>	<i>Valor Inferior</i>
Daño Extremo	10	10
Muy Alto	9	9
Alto	8	6
Medio	5	3
Bajo	2	1
Despreciable	0	0

Para el cálculo del valor del daño de las vulnerabilidades, se hace tomando la media aritmética, ya que identifica el punto de equilibrio de los valores considerados (Fuentes A., 2020), además, viene expresada en las mismas unidades que la variable, y en su cálculo intervienen todos los valores de la distribución (Inga & Paz, 2007).

A continuación, se muestran las tareas necesarias para esta actividad.

Tarea 1: se identifican las vulnerabilidades que afectan a cada activo, como se muestra en la Tabla 4-11. Estas vulnerabilidades podrían tomarse de la taxonomía previamente establecida, en la Actividad 1 – Tarea 2.

Tabla 4-11. Tuplas Vulnerabilidad - Activo

<i>Vulnerabilidad</i>	<i>Activo</i>
Falta de soporte preventivo y correctivo	Servidor
Ubicación en un área susceptible a inundaciones	Servidor
Susceptible a incendios y altas temperaturas	Servidor
Falta de soporte preventivo y correctivo	Almacenamiento
Ubicación en un área susceptible a inundaciones	Almacenamiento

<i>Vulnerabilidad</i>	<i>Activo</i>
Falta de planes de contingencia	Almacenamiento

Tarea 2: se evalúa el daño de la vulnerabilidad en el activo para cada una de las dimensiones de seguridad, incluyendo la criticidad. El daño en la criticidad se ha calculado previamente en la Actividad 2 – Tarea 3, correspondiente al valor del impacto del activo, y que será un valor único para todas las vulnerabilidades del activo de ciberseguridad. Para evaluar las dimensiones se deben tomar en consideración los rangos definidos en la Tabla 4-10. Así, por ejemplo, para el caso de la vulnerabilidad “Falta de soporte preventivo y correctivo” y activo “Servidor”, queda definido el valor del daño de la vulnerabilidad en el activo por cada dimensión de seguridad como se muestra en la Tabla 4-12.

Tabla 4-12. Valoración del daño de la vulnerabilidad

<i>Vulnerabilidad</i>	<i>Activo</i>	<i>Dimensiones</i>			
		<i>Daño Confiabilidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Criticidad</i>
Falta de soporte preventivo y correctivo	Servidor	2	3	8	8
Ubicación en un área susceptible a inundaciones.	Servidor	5	4	3	8
Susceptible a incendios y altas temperaturas	Servidor	6	7	8	8
Falta de soporte preventivo y correctivo	Almacenamiento	5	8	2	9
Ubicación en un área susceptible a inundaciones.	Almacenamiento	7	4	1	9
Falta de planes de contingencia	Almacenamiento	6	5	3	9

Tarea 3: se realiza la suma de los valores del daño de la vulnerabilidad de cada tupla vulnerabilidad – activo. En el ejemplo, el valor del daño de la vulnerabilidad de la tupla vulnerabilidad “falta de soporte preventivo y correctivo” y el activo “servidor” sería igual a 21 ($2 + 3 + 8 + 8$).

Tarea 4: se calcula el valor promedio del valor del daño de la vulnerabilidad de cada tupla vulnerabilidad – activo, dividiendo el valor del daño anterior entre el número de dimensiones consideradas (en este caso, cuatro dimensiones). En el ejemplo, el valor promedio del valor del daño de la vulnerabilidad para la tupla vulnerabilidad “falta de soporte preventivo y correctivo” y el activo “servidor” sería: $21/4 = 5,25$

Tarea 5: se repiten las tareas 2, 3 y 4 para cada una de las tuplas vulnerabilidad – activo de la organización.

Tarea 6: se realiza la asignación de un valor monetario a cada una de las vulnerabilidades que están afectando a los activos de la organización (tupla vulnerabilidad – activo). El valor monetario asignado se realiza según el criterio experto del dueño del activo, tomando información del valor actual y el daño que pudiera sufrir por la materialización de la vulnerabilidad. En el caso del ejemplo, en la columna Costo del Daño de la Vulnerabilidad de la Tabla 4-13 se muestra dicho valor.

Como se observa en la Tabla 4-13, podría darse el caso de que la suma de los costes del daño de la vulnerabilidad para un activo ($3.500 + 5000 + 6000 = 14,500$) podría ser mayor que el costo del propio activo (10.000 €). Sin embargo, hay que tener en cuenta que seguramente esos costos de los daños de las vulnerabilidades vienen provocados por diferentes amenazas, por lo que, si

estas vulnerabilidades son materializadas por la misma amenaza, el costo del daño de la amenaza puede ser mayor que el costo del activo como se puede ver en la Tabla 4-15.

Tabla 4-13. Tuplas de vulnerabilidades – activos, con valor y costo del daño, y costo del activo de las vulnerabilidades.

<i>Vulnerabilidad</i>	<i>Activo</i>	<i>Costo del Activo</i>	<i>Dimensiones</i>				<i>Valor del Daño de la Vulnerabilidad</i>	<i>Costo del Daño de la Vulnerabilidad</i>
			<i>Daño Confidencialidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Criticidad</i>		
Falta de soporte preventivo y correctivo	Servidor	10.000	2	3	8	8	5,25	3.500
Ubicación en un área susceptible a inundaciones.	Servidor		5	4	3	8	5,00	5.000
Susceptible a incendios y altas temperaturas	Servidor		6	7	8	8	4,25	6.000
Falta de soporte preventivo y correctivo	Almacenamiento	2.000	5	8	2	9	6,00	300
Ubicación en un área susceptible a inundaciones.	Almacenamiento		7	4	1	9	5,25	600
Falta de planes de contingencia	Almacenamiento		6	5	3	9	5,75	1.200

Actividad 4: Identificación de Amenazas de Ciberseguridad

En esta actividad se identifican las amenazas de ciberseguridad que pueden afectar a la organización y que puedan materializar las vulnerabilidades existentes en los activos. Para ello, se deben relacionar las amenazas de ciberseguridad con las vulnerabilidades existentes, y calcular, para cada amenaza, el valor del daño de la amenaza, así como el costo del daño de la amenaza.

A continuación, se muestran las tareas necesarias para esta actividad.

Tarea 1: se identifican las amenazas que puedan materializar las vulnerabilidades existentes. Las amenazas de ciberseguridad se podrían tomar de la taxonomía previamente establecida en la Actividad 1 – Tarea 3.

Tarea 2: se determina la amenaza que puede materializar cada vulnerabilidad de los activos de ciberseguridad de la organización, quedando estructurada las duplas Amenazas – Vulnerabilidades, y las triplas Amenazas – Vulnerabilidades – Activos, por la asociación de relaciones previamente definidas como se muestra en la Tabla 4-14 .

Tabla 4-14. Tripletas Amenazas – Vulnerabilidades – Activos

<i>Amenaza</i>	<i>Vulnerabilidad</i>	<i>Activo</i>
Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	Servidor
Agua	Ubicación en un área susceptible a inundaciones.	Servidor
Fuego	Susceptible a incendios y altas temperaturas	Servidor

<i>Amenaza</i>	<i>Vulnerabilidad</i>	<i>Activo</i>
Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	Almacenamiento
Condiciones climáticas desfavorables	Ubicación en un área susceptible a inundaciones.	Almacenamiento
Fallo de dispositivos o sistemas	Falta de planes de contingencia	Almacenamiento

Tarea 3: se recupera de la Actividad 2 – Tarea 4 el costo del activo, así como de la actividad anterior los valores calculados de valor del daño de la vulnerabilidad y costo del daño de la vulnerabilidad, de todas las vulnerabilidades identificadas, y se les asigna a las tripletas Amenazas – Vulnerabilidades – Activos, como se muestra en la Tabla 4-15 para el ejemplo que se sigue.

Tabla 4-15. Tripletas Amenazas – Vulnerabilidades – Activo con los valores y costo del daño de las amenazas

<i>Amenaza</i>	<i>Vulnerabilidad</i>	<i>Activo</i>	<i>Costo del Activo</i>	<i>Valor del Daño de la Vulnerabilidad</i>	<i>Costo del Daño de la Vulnerabilidad</i>
Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	Servidor	10.000,00	5,25	3.500
Agua	Ubicación en un área susceptible a inundaciones.	Servidor		5,00	5.000
Fuego	Susceptible a incendios y altas temperaturas	Servidor		4,25	6.000
Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	Almacenamiento	2.000,00	6,00	300
Condiciones climáticas desfavorables	Ubicación en un área susceptible a inundaciones.	Almacenamiento		5,25	600
Fallo de dispositivos o sistemas	Falta de planes de contingencia	Almacenamiento		5,75	1.200

Tarea 4: se agrupan las amenazas y vulnerabilidades en pares amenaza – vulnerabilidad, con el propósito de identificar todas las vulnerabilidades que podrían materializarse en caso de ocurrir la amenaza. Se calcula el valor del daño promedio de la vulnerabilidad, mediante el promedio de los valores del daño de las vulnerabilidades que están relacionadas con la amenaza en cuestión. De igual forma, se calcula el costo del daño total de la vulnerabilidad como la suma de los valores del coste del daño de las vulnerabilidades relacionadas con dicha amenaza. La Tabla 4-16 muestra estos valores.

En el ejemplo para la dupla “Condiciones climáticas desfavorables” – “Falta de soporte preventivo y correctivo” de la Tabla 4-15, el valor del daño promedio de la vulnerabilidad es igual al promedio de 5,25 y 6,00 $((5,25 + 6,00)/2)$ que es igual a 5,62; y el costo del daño de la amenaza es igual a la suma de 3.500 y 600, que es igual a 3.800.

Tabla 4-16. Duplas Amenazas – Vulnerabilidades con los valores y costo del daño de las vulnerabilidades

<i>Amenaza</i>	<i>Vulnerabilidad</i>	<i>Valor del Daño Promedio de la Vulnerabilidad</i>	<i>Costo del Daño Total de la Vulnerabilidad</i>
Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	5,62	3.800
Condiciones climáticas desfavorables	Ubicación en un área susceptible a inundaciones.	5,25	600
Agua	Ubicación en un área susceptible a inundaciones.	5,00	5.000
Fuego	Susceptible a incendios y altas temperaturas	4,25	6.000
Fallo de dispositivos o sistemas	Falta de planes de contingencia	5,75	1.200

Tarea 5: se agrupan las amenazas, y se calcula el valor del daño de la amenaza y el costo del daño de la amenaza. El valor del daño de cada amenaza se calcula con el promedio de los valores del daño de las vulnerabilidades que están relacionadas con la amenaza en cuestión. Y para el costo del daño de la amenaza se suman los valores del costo del daño de las vulnerabilidades relacionadas con dicha amenaza, como se muestra en la Tabla 4-17.

Tabla 4-17. Amenazas con valores totales de daño y costo del daño

<i>Amenaza</i>	<i>Valor del Daño de la Amenaza</i>	<i>Costo del Daño de la Amenaza</i>
Condiciones climáticas desfavorables	5,43	4.400
Agua	5,00	5.000
Fuego	4,25	6.000
Fallo de dispositivos o sistemas	5,75	1.200

En el ejemplo que se está siguiendo y para la amenaza “Condiciones climáticas desfavorables”, el valor del daño de la amenaza es igual al promedio de 5,62 y 5,25 $((5,62 + 5,25)/2)$ que es igual a 5,43; y el costo del daño de la amenaza es igual a la suma de 3.800 y 600, que es igual a 4.400.

Actividad 5: Medición del Riesgo

En esta actividad se calcula el riesgo de cada amenaza en función de las vulnerabilidades identificadas a los activos de la organización. Para ello, la organización debe establecer previamente la probabilidad de ocurrencia de las amenazas. Un ejemplo se muestra en la Tabla 4-18, tomando como referencia la norma ISO 27005 (ISO/IEC 27000, 2018), y agregando dos nuevos rangos: "muy alto" y "muy bajo" para identificar probabilidades muy inminentes y también insignificantes de ocurrencia.

Tabla 4-18. Probabilidad de ocurrencia de la amenaza

<i>RANGO</i>	<i>PROBABILIDAD</i>	<i>DESCRIPCION</i>	<i>FRECUENCIA</i>
MA (Muy Alto)	100	muy frecuente	a diario
A (Alto)	10	frecuente	mensualmente
M (Medio)	1	normal	una vez al año

RANGO	PROBABILIDAD	DESCRIPCION	FRECUENCIA
B (Bajo)	1/10	poco frecuente	cada varios años
MB (Muy Bajo)	1/100	muy poco frecuente	siglos

El riesgo asociado es el impacto potencial (I, impacto) multiplicado por la probabilidad de ocurrencia de la amenaza (F, frecuencia). El impacto potencial es el valor del daño de la amenaza calculado previamente (valor redondeado). La organización debe establecer la probabilidad de ocurrencia de las amenazas, según lo determine, por ejemplo, tomando en cuenta valores históricos de estas amenazas.

Un ejemplo de la medición del riesgo (R, riesgo), dada por el producto de la probabilidad de la ocurrencia de la amenaza (F, frecuencia) por el impacto (I, impacto), se muestra en la Tabla 4-19.

Tabla 4-19. Valoración del Riesgo

Tabla de Valoración del Riesgo														
I	F	R	I	F	R	I	F	R	I	F	R	I	F	R
0	MB	0	0	B	0	0	M	0	0	A	0	0	MA	0
1	MB	0	1	B	0	1	M	1	1	A	0	1	MA	1
2	MB	0	2	B	0	2	M	1	2	A	0	2	MA	4
3	MB	0	3	B	0	3	M	1	3	A	4	3	MA	4
4	MB	0	4	B	5	4	M	5	4	A	5	4	MA	8
5	MB	0	5	B	5	5	M	5	5	A	5	5	MA	8
6	MB	0	6	B	5	6	M	5	6	A	5	6	MA	9
7	MB	0	7	B	5	7	M	6	7	A	8	7	MA	9
8	MB	0	8	B	5	8	M	6	8	A	8	8	MA	9
9	MB	0	9	B	5	9	M	6	9	A	9	9	MA	10
10	MB	0	10	B	5	10	M	6	10	A	10	10	MA	10

Así, la organización podría establecer:

- Riesgo bajo, se considera de 0 a 3 (por ejemplo, color verde).
- Riesgo medio, de 4 a 6, (por ejemplo, color amarillo).
- Riesgo alto, de 7 a 8 (por ejemplo, color naranja).
- Riesgo extremo, de 9 a 10 (por ejemplo, color rojo).

Lo cual, ayudaría a la organización a la toma de decisiones (por ejemplo, enfocarse en los riesgos de color rojo y naranja).

A continuación, se muestran las tareas necesarias para esta actividad.

Tarea 1: se recuperan el valor del daño de la amenaza (impacto) y el valor del costo del daño de la amenaza. Estos valores fueron calculados previamente en la actividad anterior Actividad 4 – Tarea 5. El valor del daño de la amenaza debe ser redondeado.

Tarea 2: se asigna la probabilidad de ocurrencia de cada amenaza. Para esto, se toman como referencia casos similares que han ocurrido en la empresa y la experiencia del personal a cargo. De esta manera, la frecuencia de ocurrencia se define para cada amenaza tomando como referencia los valores de la Tabla 4-18.

Tarea 3: se realiza el cálculo del riesgo de ciberseguridad ($\text{Riesgo} = \text{Impacto} \times \text{Frecuencia}$), según como está definido en la Tabla 4-19. En la Tabla 4-20 se muestra dicho cálculo para el ejemplo que se está mostrando.

Tabla 4-20. Cálculo del Riesgo

<i>Amenazas</i>	<i>Frecuencia</i>	<i>Valor del Daño de la Amenaza (valor redondeado)</i>	<i>Riesgo</i>	<i>Costo del Daño de la Amenaza</i>
Condiciones climáticas desfavorables	(MA) Alto	5	8	4.400
Agua	(B) Bajo	5	5	5.000
Fuego	(MB) Muy Bajo	4	0	6.000
Fallo de dispositivos o sistemas	(MA) Muy Alto	6	9	1.200

Actividad 6: Contramedidas

La organización establecerá, como política de organización, qué riesgos atacar en base a la información disponible. Para ello, deberá analizar cada uno de los riesgos que puedan tener mayor factibilidad de ejecutarse, tomando la lectura de la medición de riesgo y el impacto de la organización, así como los costos en los que podría incurrir la organización. Para ello, deberá tomar las acciones correctivas necesarias y realizar las siguientes tareas.

Tarea 1: se identifica una contramedida para que pueda mitigar o eliminar un riesgo potencial. Estas contramedidas serán enfocadas a las vulnerabilidades (las contramedidas pueden contrarrestar a una o varias vulnerabilidades).

Tarea 2: se generan los controles para que permitan verificar si las contramedidas han llegado a contrarrestar el riesgo aparente de una amenaza por la materialización de las vulnerabilidades de los activos (los controles permiten controlar a una o varias contramedidas).

4.3. Prototipo del Modelo Conceptual

Como paso siguiente, se ha realizado un prototipo con el propósito de servir de base a la herramienta que permita valorar los riesgos de ciberseguridad de una organización (pequeña, aunque podrá ser utilizada por organizaciones de cualquier tamaño). Para ello, es necesario que la herramienta pueda gestionar una serie de requerimientos. A continuación, se presentan estos requerimientos que han sido identificados, así como un primer prototipo realizado en una hoja de cálculo y con una herramienta de dibujo de pantallas.

Para ello, se va a utilizar el marco de trabajo AVARCIBER, siguiendo las actividades, tareas y datos definidos en la sección anterior, y tomando como ejemplo los activos de ciberseguridad del Instituto Ecuatoriano de Seguridad Social (IESS), específicamente la plataforma del sistema legacy llamado Plataforma Host – IESS.

4.3.1. Actividad 1: Lanzamiento

En esta actividad se ha definido la taxonomía de Tipos de Activos de la organización basándose en el estándar ISO 27005 (ISO/IEC 27000, 2018). La Figura 4-6 muestra los tipos de activos a ser utilizados.

Codigo

5

Nombre

Red

Descripción

Componentes de Red

Añadir

Limpiar

☐	Codigo	Nombre	Descripción
☐	1	Procesos y actividades de negocios	Referente a procesos y actividades de negocios
☐	2	Información	Información de datos
☐	3	Hardware	Componentes de Hardware
☐	4	Software	Componentes de Software

Guardar

Cancelar

Figura 4-6. Taxonomía de Tipos de Activos

También se ha definido la taxonomía de Vulnerabilidades de ciberseguridad, basándose en el estándar ISO 27005 (ISO/IEC 27000, 2018). La Figura 4-7 muestra las vulnerabilidades de ciberseguridad a ser consideradas.

Codigo

5

Tipo

Software

Nombre

Falta de pista de auditoría

Añadir

Limpiar

☐	Codigo	Tipo	Descripción
☐	1	Hardware	No posee mecanismo de respaldo
☐	2	Hardware	No posee alta disponibilidad
☐	3	Software	Pruebas de software inexistentes o insuficientes
☐	4	Software	Errores conocidos en el software

Guardar

Cancelar

Figura 4-7. Taxonomía de Vulnerabilidades

Y finalmente se ha establecido la taxonomía de Amenazas de ciberseguridad, basándose en el estándar ENISA 2016 (Marinos, 2016). La Figura 4-8 muestra las amenazas definidas.

Código
 Tipo
 Nombre

☐	Código	Tipo	Nombre
☐	1	Ataque Físico	Fraude
☐	2	Ataque Físico	Sabotaje
☐	3	Daños involuntarios	Daños causados por un tercero
☐	4	Daños involuntarios	Daños resultantes de las pruebas de penetración

Figura 4-8. Taxonomía de Amenazas

4.3.2. Actividad 2: Identificar y evaluar Activos

Se han identificado los activos de ciberseguridad de la organización, y se les ha asignado al tipo de activo al que pertenecen.

También se ha calculado el impacto del activo para cada una de las dimensiones de seguridad (confidencialidad, integridad, disponibilidad), y se ha incluido una nueva dimensión de seguridad (criticidad), cuyo impacto se ha calculado tomando el valor más alto de las dimensiones de seguridad previas. Por ejemplo: Activo: Main-Frame Z10BC (Confidencialidad Media -7, Integridad Media - 6, Confidencialidad Alta -10), para el valor de Criticidad se toma el mayor valor de (7, 6, 10), entonces el valor de Criticidad sería Alta - 10.

Finalmente, a cada activo se le ha asignado el costo monetario del activo, el cual es el valor monetario que representa para la organización la pérdida o daño del mismo.

Las tareas realizadas en esta actividad, se pueden identificar en la Figura 4-9.

Código Nivel Seguridad
 Tipo Activo Valor Impacto
 Nombre Activo Valor Activo

☐	Código	Tipo Activo	Activo	Costo del Activo	Confidencialidad	Integridad	Disponibilidad	Criticidad
☐	1	Hardware	Main-Frame Z10BC	300.000,00	Media	Media	Alta	Alta
☐	2	Hardware	UNIDAD DE CARTUCHOS	10.000,00	Media	Media	Media	Media
☐	3	Hardware	ALMACENAMIENTO	500.000,00	Media	Media	Alta	Alta
☐	4	Software	Aplicativos alojados en el sistema HOST	100.000,00	Media	Baja	Alta	Alta

Figura 4-9. Valoración del Impacto del Activo de la Organización

4.3.3. Actividad 3: Evaluar el nivel de daño para las tuplas Vulnerabilidad – Activo (dimensión)

En esta actividad, una vez que se han identificado los activos que se van a gestionar, se han asignado las vulnerabilidades de ciberseguridad que están presentes en cada uno de los diferentes activos de la organización.

Además, se ha determinado el daño (valor del daño de la vulnerabilidad) que van a tener las vulnerabilidades en cada uno de ellos y para cada una de las dimensiones de seguridad definidas previamente (confidencialidad, integridad y disponibilidad). Para la dimensión de criticidad, se ha tomado el valor calculado en la actividad anterior. Es decir, se han considerado los datos e información definidos en la actividad anterior (4.3.2).

Luego, se ha calculado el valor promedio del daño de la vulnerabilidad para cada tupla vulnerabilidad – activo. Por ejemplo, para el activo Main-Frame Z10BC, se han sumado los valores de los daños de las dimensiones de seguridad, incluido la criticidad (10+5+2+10), siendo igual 6,75.

La medición del valor del daño de la vulnerabilidad se ha realizado para todos los activos en todas las dimensiones de seguridad definidas, incluido la criticidad. Y se ha asignado el valor monetario a cada una de las vulnerabilidades que están afectando a los activos de la organización (tupla vulnerabilidad – activo), denominado costo del daño de la vulnerabilidad.

La Figura 4-10 muestra el prototipo relativo a la valoración del valor del daño de la vulnerabilidad para cada par vulnerabilidad de ciberseguridad – activo de la organización, en cada una de las dimensiones de seguridad consideradas incluido la criticidad.

	Numero	Vulnerabilidad	Activo	Costo del Activo	Daño-Confidencialidad	Daño-Integridad	Daño-Disponibilidad	Daño-Criticidad	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
☐	1	Susceptible a incendios y altas temperaturas	Main-Frame Z10BC	300.000,00	10	5	2	10	6,75	300.000,00
☐	2	Ubicación en un área susceptible a inundaciones	Main-Frame Z10BC		10	5	2	10	6,75	300.000,00
☐	3	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	Main-Frame Z10BC		10	10	2	10	8,00	300.000,00
☐	4	Falta de soporte preventivo y correctivo	Main-Frame Z10BC		5	5	5	10	6,25	120.000,00

Figura 4-10. Valor y Costo del daño de la vulnerabilidad para la tupla Vulnerabilidad – Activo

4.3.4. Actividad 4: Identificación de Amenazas de Ciberseguridad

En esta actividad, se han identificado las amenazas de ciberseguridad que presentan los activos de la organización. Para ello, se han relacionado las amenazas de ciberseguridad con las vulnerabilidades de ciberseguridad existentes (véase Figura 4-11).

Código

Vulnerabilidad

Activo

Amenaza

☐	Número	Amenaza	Vulnerabilidad	Activo	Costo del Activo	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
☐	1	Fuego	Susceptible a incendios y altas temperaturas	Main-Frame Z10BC	300.000,00	6,75	300.000,00
☐	2	Agua	Ubicación en un área susceptible a inundaciones	Main-Frame Z10BC		6,75	300.000,00
☐	3	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	Main-Frame Z10BC		8,00	300.000,00
☐	4	Fallo o interrupción del suministro principal	Falta de soporte preventivo y correctivo	Main-Frame Z10BC		6,25	120.000,00

Figura 4-11. Asignación de amenazas a las vulnerabilidades de ciberseguridad - activos

Se han agrupado las amenazas y vulnerabilidades en las duplas amenaza – vulnerabilidad para identificar la ocurrencia de vulnerabilidades por amenaza como se muestra en la Figura 4-12.

El valor del daño promedio de la vulnerabilidad se ha obtenido mediante el promedio de los valores del daño de las vulnerabilidades que están relacionadas con la amenaza en cuestión.

Y el costo del daño total de la vulnerabilidad se ha obtenido sumando el coste del daño de las vulnerabilidades relacionadas con dicha amenaza.

Plataforma HOST - IESS

☐	Número	Amenaza	Vulnerabilidad	Valor del Daño Promedio de la Vulnerabilidad	Costo del Daño Total de la Vulnerabilidad
☐	1	Actividades no autorizadas	Falta de política formal de cambio de credenciales	6,25	3.000,00
☐	2	Actividades no autorizadas	Mala gestión de contraseñas	6,83	4.000,00
☐	3	Actividades no autorizadas	Mala gestión de contraseñas	6,83	4.000,00
☐	4	Agua	Ubicación en un área susceptible a inundaciones.	6,66	892.000,00
☐	5	Condiciones climáticas desfavorables	Fallo de los componentes	7,38	16.500,00
☐	6	Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	6,19	279.500,00
☐	7	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	7,25	892.000,00
☐	8	Diseño y planificación inadecuados o adaptación inadecuada	No posee mecanismo de respaldo	7,25	20.000,

Figura 4-12. Dupla Amenaza – Vulnerabilidad con valor y el costo del daño de la vulnerabilidad

También se han agrupado las amenazas, y se ha calculado el valor y el costo del daño de la amenaza. En el primer caso, se ha calculado el valor promedio de los valores del daño de las vulnerabilidades que están relacionadas con la amenaza en cuestión, y en el segundo caso, se ha realizado la sumatoria de los valores del costo del daño de las vulnerabilidades relacionadas con dicha amenaza.

Los valores promedio y sumatoria, calculados previamente, representan el valor del daño de la amenaza y el costo del daño de la amenaza respectivamente como se muestra en la Figura 4-13.

Plataforma HOST - IESS

[Consultar](#)

☐	Número	Amenaza	Valor del Daño de la Amenaza	Costo del Daño de la Amenaza
☐	1	Actividades no autorizadas	6,64	11.000,00
☐	2	Agua	6,66	892.000,00
☐	3	Condiciones climáticas desfavorables	6,78	296.000,00
☐	4	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	7,25	892.000,00
☐	5	Diseño y planificación inadecuados o adaptación inadecuada	7,25	20.000,00
☐	6	Fallo de dispositivos o sistemas	7,77	1.505.000,00
☐	7	Fallo de software /aplicaciones o servicio	6,00	400,00
☐	8	Fallo o interrupción del suministro principal	6,75	134.300,00
☐	9	Fuego	7,30	892.000,00
☐	10	Pérdida de recursos	6,30	237.600,00
☐	11	Robo (dispositivos, medios de almacenamiento y documentos)	7,79	525.000,00
☐	12	Uso erróneo o administración de dispositivos y sistemas	6,23	684.400,00

[Cancelar](#)

Figura 4-13. Amenazas de ciberseguridad con Valores del daño y Costo del daño de la Amenaza.

4.3.5. Actividad 5: Medición del Riesgo

Una vez que se ha agrupado las amenazas, y se ha calculado el valor del daño de la amenaza y el costo del daño de la amenaza, se ha procedido a asignar la frecuencia de ocurrencia de la amenaza de ciberseguridad según la experiencia de la organización o tomando valores que son publicados por la industria. En la Tabla 4-18 se muestra un ejemplo que puede ayudar a la organización a introducir el rango de frecuencia. Por ejemplo, si la amenaza de ciberseguridad es algo que ocurre mensualmente, su rango de frecuencia es Alto (A), también cabe mencionar que el valor del daño de la amenaza para esta actividad se ha redondeado, por ejemplo, si el valor es 6,65, se debe asignar el valor de 7.

En el caso del prototipo, y teniendo en cuenta la escala de cuantificación mostrada en la Tabla 4-18 se asigna el rango de frecuencia a la amenaza de ciberseguridad (véase Figura 4-14).

A continuación, se ha calculado de forma automática el riesgo de que ocurra la amenaza de ciberseguridad. El riesgo se calcula mediante el producto de la probabilidad de la ocurrencia de la amenaza de ciberseguridad (Rango de Frecuencia) por valor del daño de la amenaza (impacto). La Tabla 4-19 muestra cómo se calcula el riesgo y, por ejemplo, para una frecuencia Alta y un valor de daño de la vulnerabilidad (impacto) de 8, el valor del riesgo es igual a 8 y corresponde a un color naranja, indicando que el riesgo es medio.

La Figura 4-14 muestra el cálculo de los riesgos para las amenazas identificadas.

Código
 Amenaza
 Frecuencia
 Costo del Daño

Valor del Daño
 Riesgo

☐	Numer	Amenaza	Valor del daño	Frecuencia	Riesgo	Costo del Daño
☐	1	Actividades no autorizadas	7	M	5	11.000,00
☐	2	Agua	7	B	3	892.000,00
☐	3	Condiciones climáticas desfavorables	7	B	3	296.000,00
☐	4	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	7	B	3	892.000,00
☐	5	Diseño y planificación inadecuados o adaptación inadecuada	7	MA	9	20.000,00

Figura 4-14. Riesgo de las amenazas de ciberseguridad

4.3.6. Actividad 6: Contramedidas

En esta actividad se ha identificado todas las vulnerabilidades de ciberseguridad que fueron identificadas a los activos de la organización, y para cada una de ellas hay que determinar una contramedida que pueda contrarrestar la materialización de la vulnerabilidad, en caso de que la amenaza de ciberseguridad asociada llegue a ocurrir. En la Figura 4-15 se muestran las contramedidas identificadas.

Código
 Vulnerabilidad
 Contramedida

☐	Numer	Vulnerabilidad	Contramedida
☐	1	Errores conocidos en el software.	Control de calidad de los sistemas de software
☐	2	Fallo de los componentes	Contratos de soporte y mantenimiento en vigencia
☐	3	Falta de capacitación en la administración del activo	Capacitación continua en la administración del activo
☐	4	Falta de garantía técnica de los equipos	Contrato de garantía en vigencia
☐	5	Falta de mantenimiento y/o actualizaciones	Contratos de mantenimiento y actualizaciones vigente
☐	6	Falta de planes de contingencia	Generar plan de contingencia por activo
☐	7	Falta de política formal de cambio de credenciales	Política de gestión de credenciales
☐	8	Falta de precaución en las conexiones físicas	Mejora de las conexiones físicas de los activos
☐	9	Falta de soporte preventivo y correctivo	Contratos de soporte y mantenimiento en vigencia

Figura 4-15. Contramedidas a las vulnerabilidades identificadas

4.3.7. Resumen del prototipo

El prototipo construido es una primera implementación del modelo conceptual definido, siguiendo la metodología de identificación y evaluación AVARCIBER. El prototipo ha permitido implementar las definiciones de:

- Activos de la organización en cuanto a ciberseguridad.
- Vulnerabilidades de ciberseguridad.
- Amenazas de ciberseguridad.
- Riesgos de ciberseguridad.

Además, ha permitido valorar los conceptos definidos y recopilados para la elaboración del modelo conceptual, así como la aplicación de la metodología de identificación y evaluación AVARCIBER, validando las siguientes características:

- Completitud del modelo conceptual (elementos y conceptos).
- Factibilidad de la solución, con los elementos descritos.
- Usabilidad y rendimiento del sistema planteado.
- Validez de la metodología AVARCIBER.

4.3.8. Conclusiones

Se ha presentado un prototipo elaborado con las actividades y tareas necesarias a seguir, como una alternativa para la identificación y evaluación de riesgos en ciberseguridad para las organizaciones.

Un elemento importante que identifica a este prototipo es la identificación y evaluación del riesgo a partir de las vulnerabilidades de ciberseguridad, pues éstas se asocian a los activos y a las amenazas de ciberseguridad identificadas en la organización.

Un punto que hay que tener en cuenta es la necesidad de que la organización determine la valoración del impacto del activo, el costo del activo, el valor del daño de la vulnerabilidad, y el costo del daño de la vulnerabilidad según sus necesidades y objetivos estratégicos. Sin embargo, en el futuro esta valoración puede ser implementada con un proceso de aprendizaje y asignación automática.

El prototipo se ha desarrollado en una hoja Excel y en un entorno web, y se ha buscado que fuera muy sencillo en su uso. Se contemplan desarrollar versiones periódicas para mejorar y mantener la aplicación.

4.4. Aportaciones realizadas

En la revisión de los modelos de madurez en ciberseguridad y taxonomías de los elementos para identificar y evaluar los riesgos de ciberseguridad, se ha identificado que no existe una postura común que describa las relaciones de los elementos de riesgo en ciberseguridad (activos, y vulnerabilidades y amenazas de ciberseguridad). Por lo que se ha decidido elaborar un modelo conceptual de dominio que establezca las relaciones de los elementos de riesgos en ciberseguridad.

En la elaboración del modelo conceptual, como complemento a los elementos identificados en la revisión de la literatura, y a la identificación de las relaciones de estos elementos, se incluyeron algunos elementos diferenciadores como:

- El elemento dimensión de valoración que ayuda a medir el impacto del activo según las dimensiones de seguridad como, por ejemplo: confidencialidad, integridad, disponibilidad y criticidad.
- La vulnerabilidad de ciberseguridad es el elemento primordial para medir el daño de una amenaza de ciberseguridad en los activos de la organización.
- La valoración del daño de las vulnerabilidades del activo para cada dimensión de seguridad es medida.
- Para cada vulnerabilidad de ciberseguridad se incluye el costo del daño de afectación en el activo asociado.
- Las contramedidas están ligadas a las vulnerabilidades, para eliminar o reducir el daño en caso de llegar a materializarse.

En la metodología de identificación y evaluación, se han identificado actividades muy particulares como son:

- Identificación de las vulnerabilidades de ciberseguridad para cada activo de la organización.
- Medición de la valoración del daño de las vulnerabilidades por cada dimensión de seguridad definida.
- La valoración del daño final de cada vulnerabilidad se calcula con el promedio de la valoración del daño de las dimensiones de seguridad de cada vulnerabilidad.
- El valor del costo total del daño de la vulnerabilidad se calcula sumando el costo del daño de la vulnerabilidad por cada activo en cual está presente.

Todos los elementos identificados y descritos anteriormente han sido incluidos en el prototipo definido, con la finalidad de: 1) validar los elementos del modelo conceptual, 2) verificar la viabilidad de la metodología definida, y 3) establecer un modelo conceptual que responda a las necesidades de la organización, en la identificación y evaluación de riesgos en ciberseguridad.

El prototipo también utiliza una metodología que complementa al modelo conceptual, y que contempla los requerimientos funcionales que debe tener un producto de software que gestione la identificación y evaluación de riesgos en ciberseguridad.

5. EXPERIMENTACIÓN

En este capítulo se presenta el trabajo de experimentación realizado con el fin de validar las hipótesis de trabajo planteadas en el capítulo 3 de esta tesis. La contrastación de las hipótesis se realizará mediante técnicas de diseño de experimentos para la ingeniería de software. Es por ello que, en la siguiente sección, se presenta el método seguido para su posterior aplicación. Posteriormente, se desarrollan los casos de estudio que permitan validar las hipótesis, para generar una línea base.

Se procederá a aplicar la metodología definida siguiendo cada uno de sus actividades y tareas propuestas, para recopilar la información generada.

Al final, se analizará toda la información obtenida comparando con la información de la línea base inicial y se valorará la utilidad del modelo conceptual definido, la metodología utilizada y demás artefactos elaborados.

5.1. Método de diseño de experimentos de ingeniería del software

El único modo para contrastar las creencias y las opiniones para convertirlas en hechos es la experimentación. El fin de la experimentación es identificar las causas por las que se producen determinados resultados. Según (Wohlin, Runeson, Höst, Ohlsson, & Reg, 2000), la ingeniería de software (IS) debe tratarse como una ciencia y considerar la experimentación como una parte importante del conocimiento científico (Juristo & Moreno, 2001) y una de las formas de validación de las propuestas. La IS hará posible la comprensión e identificación de las variables que entran en juego en la construcción de software y las conexiones que existen entre ellas. Las estrategias empíricas existentes para el desarrollo de experimentos en ingeniería de software incluyen encuestas, estudios de caso y experimentos (Wohlin, Höst, & Henningsson, 2003).

La Figura 5-1 muestra las características de los estudios de caso como método de investigación según se propone en (Wohlin, Höst, & Henningsson, 2003).

Figura 5-1. Características de los estudios de caso. (Fuente: Wohlin, Höst, & Henningsson, 2003)

Según estos autores, hay tres formas de plantear los estudios de casos:

- Comparar los resultados entre una línea base y la nueva propuesta.
- Desarrollar dos proyectos simultáneamente tomando uno de ellos como base.
- Aplicar la nueva propuesta sobre unos determinados componentes y comparar los resultados obtenidos con los de aquellos componentes sobre los que no se haya aplicado la nueva propuesta.

En esta tesis se ha optado por la primera forma. Para establecer la línea base (inicial) se ha procedido a obtener la matriz de riesgos según la metodología definida actualmente en la organización. Después de implantar el modelo conceptual y el marco de trabajo definido, los resultados obtenidos constituirán la línea base (final) frente a que comparar la nueva propuesta.

Después de definir la línea base inicial se ha implementado el marco de trabajo de identificación y evaluación de riesgos definido en el capítulo 4, tomando como referencia el modelo conceptual y ejecutando las actividades y tareas propuestas. Luego de la ejecución de las actividades y tareas definidas, se han generado los entregables definidos hasta llegar a conseguir la matriz de riesgos, de ciberseguridad, y la valoración de los activos y de las amenazas.

5.2. Caso de estudio

El Instituto Ecuatoriano de Seguridad Social (IESS) es una entidad cuya organización y funcionamiento se fundamenta en los principios de solidaridad, obligatoriedad, universalidad, equidad, eficiencia, subsidiariedad y suficiencia. Se encarga de aplicar el Sistema del Seguro General Obligatorio que forma parte del Sistema Nacional de Seguridad Social de Ecuador.

El gobierno del doctor Isidro Ayora Cueva, mediante Decreto N° 018, del 8 de marzo de 1928, creó la Caja de Jubilaciones y Montepío Civil, Retiro y Montepío Militares, Ahorro y Cooperativa, institución de crédito con personería jurídica, organizada de conformidad con la Ley se denominó Caja de Pensiones.

Mediante Decreto Supremo N° 40 del 25 de julio de 1970 y publicado en el Registro Oficial N° 15 del 10 de julio de 1970, se transformó la Caja Nacional del Seguro Social en el Instituto Ecuatoriano de Seguridad Social.

La Asamblea Nacional, reunida en 1998 para reformar la Constitución Política de la República, consagró la permanencia del IESS como única institución autónoma, responsable de la aplicación del Seguro General Obligatorio.

El IESS, según lo determina la vigente Ley del Seguro Social Obligatorio, se mantiene como entidad autónoma, con personería jurídica, recursos propios y distintos de los del Fisco.

El IESS se encuentra en una etapa de transformación, el plan estratégico que se está aplicando, sustentado en la Ley de Seguridad Social vigente, convertirá a esta institución en una aseguradora moderna, técnica, con personal capacitado que atenderá con eficiencia, oportunidad y amabilidad a toda persona que solicite los servicios y prestaciones que ofrece.

El IESS cuenta con 30.000 empleados, y cuenta con 7 direcciones que son los procesos sustantivos de la organización, y dentro de los procesos de apoyo está conformado por 3 direcciones, en donde se encuentra la Dirección Nacional de Tecnologías de la Información (DNTI), cuya misión es la de: generar y administrar servicios de tecnología de la información, que permitan garantizar el control y seguridad informática en la gestión de la institución, de una manera eficiente, alineados a la misión institucional y al marco regulatorio vigente. La Dirección está conformada por las siguientes subdirecciones:

- Subdirección Nacional de Infraestructura de Tecnologías de la Información (SNTI). Se encarga de gestionar la instalación, configuración e implementación de infraestructura de

servicios tecnológicos, de acuerdo a las necesidades institucionales a fin de mejorar la disponibilidad de los servicios tecnológicos.

- Subdirección Nacional de Desarrollo Informático (SNDI). Se encarga de dirigir los procesos de construcción y mantenimiento de los sistemas de información, bajo políticas de calidad y seguridad de la información y metodologías en base a la normativa legal y necesidades institucionales, apoyando al fortalecimiento de los procesos tecnológicos.
- Subdirección Nacional de Arquitectura y Soluciones (SNAS). Se encarga de dirigir procesos de investigación, análisis y recomendaciones para la adopción de nuevas plataformas y/o soluciones tecnológicas basadas en las necesidades de la institución.
- Subdirección Nacional de Seguridad Informática (SNDISI). Preservar la confidencialidad, integridad y seguridad de la infraestructura tecnológica y de la información que se procesa, almacena y transmite a través de diferentes sistemas informáticos institucionales.

En la SNTI se encuentra la infraestructura tecnológica donde se ha realizado el levantamiento de los activos de organización, para la identificación y evaluación de los riesgos de ciberseguridad.

5.3. Línea base inicial de los activos de la organización

La DNTI, en el año 2017, inició el levantamiento de los activos de la organización de su infraestructura tecnológica. El alcance inicial cubrió los siguientes componentes tecnológicos:

- Unidad de datos de protocolo (PDU).
- Sistema de Energía Ininterrumpida (UPS).
- Aire Acondicionados, Sistema Contra Incendios y Equipo de Seguridad.
- Sistema de prevención de intrusos (IPS).
- Plataforma Host – IESS.
- Aires de Precisión Liebert.
- Plataforma AS400 – IESS.
- Sistema de Climatización – Eléctrico – Contra Incendios.
- Correo Electrónico – IESS.
- Plataforma Firewall – IESS.
- Plataforma Oracle – IESS.
- Tivoli Storage Manager – IESS.
- UPS – TTIPP – LITE.
- Telefonía IP.

El análisis de la Gestión de Riesgos incluyó: identificar, controlar y eliminar o minimizar eventos inciertos que puedan afectar los recursos de TI. Para realizar estas actividades, se tomó como referencia lo definido por la norma ISO/IEC 27005, la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT y la Metodología de gestión de riesgos RISK IT de ISACA.

Para poder establecer la línea base inicial y siguiendo la metodología referencial definida, se ha definido tomar tres componentes de la infraestructura tecnológica definida en el alcance inicial, e incluir un componente adicional que por su criticidad será un factor importante en el momento de evaluar la línea base. Los componentes que se han definido son los siguientes:

- Del alcance inicial:
 - Plataforma Host – IESS.
 - Plataforma Oracle – IESS.
 - Plataforma Firewall – IESS.
- Componente adicional:
 - Plataforma AS400 – IESS – (Hospital Carlos Andrade Marín - HCAM).

De los componentes definidos, en esta sección se describe únicamente la actividades realizadas a plataforma Host - IESS, y en el Anexo III de este documento se incluye el detalle de las

actividades de las plataformas descritas, para ello inicialmente se describen las actividades realizadas, así como los parámetros utilizados para la identificación y evaluación de riesgos en los activos de la DNTI.

Las actividades que se han llevado a cabo para la identificación y evaluación de riesgos han sido las siguientes, y se describen a continuación:

- Identificación de los equipos de la plataforma Host y sus equipos dependientes.
 - Dependencia de Activos.
 - Identificación de Activos.
- Valoración de activos considerando tres dimensiones: disponibilidad, integridad y confidencialidad.
- Identificación y valoración de las amenazas y vulnerabilidades sobre dichos equipos.
- Evaluación del impacto y frecuencia de los escenarios de riesgos identificados.
- Cálculo del riesgo total.
- Valoración Riesgo.
- Gráficos de Mapa de calor de Riesgos.
- Mapa de Radar de Riesgos.
- Propuesta de controles o salvaguardas.

Dependencias de Activos

Para cada activo, se identifican las dependencias de otros activos, diagramando de ser posible el activo principal y sus activos dependientes.

Identificación de activos

Para cada activo identificado, se indica su nombre, la descripción y la finalidad de uso del mismo, con objeto de identificar las actividades que realiza el activo, y poder analizarlo en ese contexto.

Valoración de Activos

La valoración de los activos identificados se debe realizar considerando las tres dimensiones de seguridad informática que son: Confidencialidad, Integridad y Disponibilidad.

- **Confidencialidad:** que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.
- **Integridad:** mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una organización.
- **Disponibilidad:** disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

Además, se incluye otro criterio calculado que se describe a continuación:

- **Críticidad:** determina la importancia que tiene el activo en la organización y describe el cuidado que se debe tener sobre el mismo. El valor asignado es el valor máximo de las tres características Disponibilidad /Integridad/Confidencialidad, como se explica en la Tabla 5-1.

Las escalas utilizadas para la valoración se detallan a continuación (Tabla 5-1):

Tabla 5-1. Criterios de valoración Confidencialidad, Integridad, Disponibilidad y Criticidad

Criterio de valoración DISPONIBILIDAD		
¿Qué importancia tendría que el activo no estuviera disponible?		
Alta (A)	3	Información cuya inaccesibilidad permanente durante una hora podría impedir la ejecución de las actividades del IESS.
Media (M)	2	Información cuya inaccesibilidad permanente durante la jornada laboral podría impedir la ejecución de las actividades del IESS.
Baja (B)	1	Información cuya inaccesibilidad permanente durante una semana podría ocasionar un perjuicio significativo para el IESS.
Nula (N)	0	Información cuya inaccesibilidad no afecta la actividad normal del IESS.

Criterio de valoración INTEGRIDAD		
¿Qué importancia tendría que los datos fueran modificados fuera de control?		
Alta (A)	3	Información cuya modificación no autorizada no podría repararse, impidiendo la realización de las actividades del IESS.
Media (M)	2	Información cuya modificación no autorizada es de difícil reparación y podría ocasionar un perjuicio significativo para el IESS o terceros.
Baja (B)	1	Información cuya modificación no autorizada puede repararse, aunque podría ocasionar un perjuicio para el IESS o terceros.
Nula (N)	0	Información cuya modificación no autorizada puede repararse fácilmente, o que no afecta a las actividades del IESS.

Criterio de valoración CONFIDENCIALIDAD		
¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?		
Alta (A)	3	Información que puede ser conocida y utilizada por un grupo muy reducido de agentes, cuya divulgación podría ocasionar un perjuicio al IESS o terceros.
Media (M)	2	Información que solo puede ser conocida y utilizada por un grupo de agentes, que la necesiten para realizar su trabajo.
Baja (B)	1	Información que puede ser conocida y utilizada por todos los agentes del IESS.
Nula (N)	0	Información que puede ser conocida y utilizada sin autorización por cualquier persona, dentro o fuera del IESS.

Criterio de valoración CRITICIDAD		
Valor máximo de las tres características Disponibilidad /Integridad/Confidencialidad		
Alta (A)	3	Si el máximo es 3
Media (M)	2	Si el máximo es 2
Baja (B)	1	Si el máximo es 1
Nula (N)	0	Si todos son 0

Identificación y valoración de amenazas

En este punto, se identifican las vulnerabilidades y las amenazas para cada activo, también se incluye el valor de la criticidad del activo, calculado en la actividad anterior, lo que permite tener elementos adicionales para identificar las vulnerabilidades y amenazas.

Valoración del impacto

Para cada activo y amenaza se estima la degradación, es decir el porcentaje en que la amenaza daña al activo en estudio, estableciendo un valor entre 0% (no lo daña) y el 100% (lo daña absolutamente) para cada una de las características de confidencialidad, integridad y disponibilidad.

- **Degradación (Confidencialidad):** la confidencialidad hace referencia a la protección de la información contra la divulgación no autorizada. El impacto producido por un evento de estas características, sea en forma no autorizada, intencional o inadvertida, puede variar entre la pérdida de confianza en la institución hasta la posibilidad de acciones legales contra la misma.
- **Degradación (Integridad):** se refiere al requerimiento de que el activo o la información sea protegido contra la modificación no autorizada. Se pierde integridad si se realizan cambios no autorizados en los sistemas o se pierde parte de los datos almacenados, sea por un evento accidental o intencionado.
- **Degradación (Disponibilidad):** el hecho de que la información o un sistema no esté disponible para sus usuarios, ya sea por la pérdida de datos o la destrucción de elementos necesarios, puede afectar a la efectividad operacional y, consecuentemente, al cumplimiento de la misión de una organización.

El impacto se calcula en base al máximo valor de degradación que la amenaza produce sobre un activo, multiplicado por el valor del impacto calculado previamente, un ejemplo se muestra en la Tabla 5-2.

Tabla 5-2 Ejemplo de valoración de impacto

IDENTIFICACIÓN DE ACTIVOS		AMENAZAS	DEGRADACIÓN			IMPACTO
Activo	Criticidad	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL
Activo x	3	Daños ocasionados por fuego	100%	50%	20%	3x100%=3

Valoración Riesgo

En la valoración del riesgo se establece el nivel de riesgo que cada amenaza ocasiona sobre el activo. Para ello, se debe establecer la frecuencia de ocurrencia de la amenaza, y el impacto (pérdidas y daños) que el evento produce sobre los activos.

Los criterios utilizados para la calificación de la frecuencia son descritos en la Tabla 5-3.

Tabla 5-3. Criterios de valoración frecuencia

Criterio de valoración FRECUENCIA		
Frecuencia con la que ocurre o puede ocurrir dicho evento		
Alta (A)	3	A diario
Media (M)	2	Mensualmente
Baja (B)	1	1 vez al año
Nula (N)	0.1	Cada varios años

En la Tabla 5-4 se muestra un ejemplo de la valoración del riesgo. El cálculo del riesgo se realiza multiplicando la Frecuencia por el Impacto: **Riesgo = Frecuencia x Impacto**.

Tabla 5-4 Ejemplo de valoración del riesgo

IDENTIFICACIÓN DE ACTIVOS	AMENAZAS	CÁLCULOS		
		FRECUENCIA	IMPACTO	RIESGO
Activo x	Daños ocasionados por fuego	0.1	3.00	$0.1 \times 3 = 0.30$

Una vez realizado el cálculo del riesgo para cada amenaza de los activos, se elabora un mapa de calor con los valores del riesgo, impacto y frecuencia, con la finalidad de identificar los riesgos críticos, los cuales se ubicarán en el cuadrante rojo, según las siguientes definiciones:

- **Cuadrante Rojo:** alto impacto - alta frecuencia.
- **Cuadrantes Amarillos:** alto impacto - baja frecuencia, o bajo impacto – alta frecuencia.
- **Cuadrante Verde:** baja frecuencia – bajo impacto.

Un ejemplo de lo mencionado se puede visualizar en el Figura 5-2.

Figura 5-2. Ejemplo de riesgo en función del impacto y la frecuencia

Gráfica de radar de los riesgos por activo

Con los riesgos identificados de cada activo, se determina el riesgo total de cada activo. Para ello, se debe calcular el valor promedio de los riesgos identificados, y con este valor promedio se deben calcular los siguientes valores adicionales para cada activo:

- Valor actual: promedio del riesgo.
- Valor esperado: 50% del promedio del riesgo.
- Valor límite: riesgo máximo permitido.

Finalmente, con estos valores se genera un gráfico de radar con todos los activos analizados para identificar los activos más expuestos a los riesgos y que deben ser considerados para la identificación de contramedidas.

Controles o salvaguardas sugeridas

De la actividad “Gráfica de Radar de los riesgos por activo”, se identifican los activos más expuestos a los riesgos identificados. De los mapas de calor identificados en la actividad “Valoración de Riesgo”, se analizan los riesgos de cada activo que están en el cuadrante rojo, los mismos que serán considerados como riesgos críticos, e identificar contramedidas apropiadas.

Con la información generada previamente, se procede a elaborar las contramedidas para cada una de las tripletas activo – vulnerabilidad – amenaza. Estas tripletas se construyen tomando los valores de los activos más expuestos a los riesgos, y los riesgos de estos activos que se encuentran en el cuadrante rojo.

Para elaborar las actividades descritas, se utilizan como referencias las siguientes siglas:

- D: Disponibilidad.
- I: Integridad.
- C: Confidencialidad.
- Cr: Criticidad.
- IM: Impacto.
- Tot: Total.
- FR: Frecuencia.

A continuación, se detalla el informe con el resumen de las actividades que se han ejecutado para la **Plataforma Host – IESS**. Los informes adicionales para el resto de las plataformas que conforman la línea base inicial se adjuntan en el Anexo III, de la presente tesis doctoral.

5.3.1. Análisis de Riesgos de la Plataforma Host – IESS

Los equipos de la plataforma Host – IESS son activos críticos e importante para la organización, ya que en dichos equipos se ejecutan transacciones que aún no se han migrado al sistema de Historia Laboral, por lo que es sumamente importante que exista alta disponibilidad de dicha plataforma en virtud de que los aplicativos de Historia Laboral (datos históricos de los afiliados) requieren información de dicha plataforma para proporcionar las prestaciones y servicios a los asegurados.

A continuación, se describan las actividades ejecutadas.

5.3.1.1 Dependencias de activos.

Para cada activo se han identificado las dependencias de otros activos, diagramando de ser posible el activo principal y sus activos dependientes (véase Figura 5-3), en el caso de la plataforma Host el activo principal es el activo Main-Frame Z10BC, como se puede apreciar en la Figura 5-3.

Figura 5-3. Diagrama de dependencia de equipos de la Plataforma Host-IESS

5.3.1.2 Identificación de activos

Los activos de la plataforma Host-IESS se han identificado, y para cada uno de ellos, se ha colocado su descripción y la finalidad de uso. En el caso del activo “Unidad de Cartuchos”, se ha colocado en dos líneas debido a que existen dos unidades muy particulares que se desea analizar por separado.

Tabla 5-5. Identificación de Activos de la Plataforma Host-IESS

Identificación de Activos			
#	Activo	Descripción del hardware	Finalidad de uso
1	Main-Frame Z10BC	Main-Frame Z10BC	SERVIDOR MAINFRAME PLATAFORMA Z10, COFIGURADO POR 4 LPAR'S(ZVSEUIO, ZVSEGYE,ZVSEDESA Y ZVM)
2	UNIDAD DE CARTUCHOS	UNIDAD DE CARTUCHOS	UNIDAD DE CINTAS(CARTUCHOS)
3	UNIDAD DE CARTUCHOS	UNIDAD DE CARTUCHOS	UNIDAD DE CINTAS(CARTUCHOS)
4	ALMACENAMIENTO (STORAGE)	REPOSITORIO	ARREGLO DE DISCOS RESIDENTE DE ARCHIVOS VSAM Y CONFIGURACIÓN LPAR'S DEL Z10 Y S.O
5	SERVIDOR HMC	SERVIDOR	SERVIDOR DEL Z10
6	AIRE DE PRECISION	AIRE DE PRECISION	AIRE ACONDICIONADO DE PRECISION
7	AIRE TIPO MOCHILA	AIRE TIPO MOCHILA	AIRE ACONDICIONADO DE CONTIGENCIA
8	UPS	UPS	EQUIPO DE PROTECCION ELECTRICA
9	SERVIDOR UNIX	SERVIDOR UNIX	PLATAFORMA MICROS, DATAFLEX
10	SERVER VTAPE	SERVER VTAPE	REPOSITORIO LOCAL DATA VTAPE, ALMACENAMIENTO BACKUP'S VSAM
11	SWITCH DE PASO	SWITCH DE PASO	SWITH DE PASO RED Z10 (172.16.8.XX
12	APLICATIVOS; SISTEMA OPERATIVO	Aplicativos alojados en el sistema Host	APLICATIVSO QUE CORREN EN LA PLATAFORMA HOST -IESS

5.3.1.3 Valoración de activos

La valoración de los equipos de la plataforma Host se ha realizado considerando las tres dimensiones de seguridad informática que son: Disponibilidad, Integridad y Confidencialidad.

Las escalas utilizadas para la valoración se detallan en la Tabla 5-1. La valoración de los activos se realizó con personal técnico de la plataforma Host, Ing. Paúl Galarraga, Tecnólogo Marco García y Tecnólogo Alberto Andrade.

Desde el activo 1 al número 11 son activos de Hardware, el activo 12 es un activo de software que estaba agrupando varios activos con el nombre de “Aplicativos, sistema operativo”, como se muestra en la Tabla 5-6.

Tabla 5-6. Valoración de activos en disponibilidad, integridad, confidencialidad y criticidad

IDENTIFICACIÓN DE ACTIVOS		VALORACIÓN DE ACTIVOS						
#	Activo	Disponibilidad	Valor	Integridad	Valor	Confidencialidad	Valor	Criticidad
1	Main-Frame Z10BC	Alta (A)	3	Media (M)	2	Media (M)	2	3
2	UNIDAD DE CARTUCHOS	Media (M)	2	Media (M)	2	Media (M)	2	2
3	UNIDAD DE CARTUCHOS	Media (M)	2	Media (M)	2	Media (M)	2	2
4	ALMACENAMIENTO (STORAGE)	Alta (A)	3	Media (M)	2	Media (M)	2	3
5	SERVIDOR HMC	Media (M)	2	Media (M)	2	Media (M)	2	1
6	AIRE DE PRESICION	Alta (A)	3	Media (M)	2	Media (M)	2	3
7	AIRE TIPO MOCHILA	Baja (B)	1	Media (M)	2	Media (M)	2	2
8	UPS	Alta (A)	3	Media (M)	2	Media (M)	2	3
9	SERVIDOR UNIX	Alta (A)	3	Media (M)	2	Media (M)	2	3
10	SERVER VTape	Media (M)	2	Media (M)	2	Media (M)	2	2
11	SWITCH DE PASO	Alta (A)	3	Media (M)	2	Media (M)	2	3
12	Aplicativos alojados en el sistema Host	Alta (A)	3	Baja (B)	1	Media (M)	2	3

5.3.1.4 Identificación y valoración de amenazas

Para cada uno de los activos, se han identificado las Vulnerabilidades y Amenazas de ciberseguridad, como se muestra en la Tabla 5-7. En relación con el activo “Unidad de Cartucho”, que en la actividad anterior se trató como dos activos por existir dos unidades con diferente utilidad, en esta actividad y en las posteriores se los considerara como un solo activo por no haber generado información diferente el momento de la valoración de activos.

Tabla 5-7. Identificación de vulnerabilidades y amenazas de ciberseguridad de cada activo

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS
Activo	Criticidad	Descripción	Descripción
Main-Frame Z10BC	3	Posibilidad de incendios	Daños ocasionados por fuego
		Falta de protección contra inundaciones	Daños ocasionados por agua
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres naturales (Terremotos)
		UPS sin soporte técnico	Daños ocasionados por corte de suministro eléctrico
		Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad
		Falta de capacitación (personal de administración)	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo
		Imposibilidad de brindar servicio por cortes en los enlaces de datos	Posibilidad de tener interrupción de servicios de enlaces de datos
		No tener soporte y garantía del fabricante	Falta de soporte y garantía del fabricante sobre el hardware en el que está instalada la solución
		No tener al momento soporte del fabricante del equipo	Falta de soporte y actualización del equipo
		Falla del equipo	Perdida de servicio de conectividad con elementos periféricos de la plataforma
		Falta de servicio	No contar con un sistema de alimentación eléctrica externa (grupo electrógeno)
UNIDAD DE CARTUCHOS	2	Falta de garantía del fabricante (no se resuelvan los problemas graves)	Posibilidad de tener cortes en la continuidad del servicio (disponibilidad)
		Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad
		Falta de protección contra inundaciones	Daños ocasionados por agua
		Posibilidad de incendios	Daños ocasionados por fuego
		Funcionamiento inadecuado de UPS (sin soporte)	Daños ocasionados por corte de suministro eléctrico
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres naturales (Terremotos)
		Falta de capacitación (personal de administración)	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)
		Control de acceso de entrada y salida	Robo

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS
Activo	Criticidad	Descripción	Descripción
		Falta de planes de contingencia y políticas formalizados	Falta y actualización de planes de contingencia y políticas de uso formalizado
		Robo de clave o ingreso a máquinas de administración	Acceso indebido de personas no autorizadas (lógico)
		Problemas con actualizaciones y mantenimientos por vigencia tecnológica vencida	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo
ALMACENAMIENTO (STORAGE)	3	Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad
		Falta de protección contra inundaciones	Daños ocasionados por agua
		Posibilidad de incendios	Daños ocasionados por fuego
		Funcionamiento inadecuado de UPS (sin soporte)	Daños ocasionados por corte de suministro eléctrico
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres naturales (Terremotos)
		Crecimiento no planificado de personal, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo
		Falta de capacitación (personal de administración)	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)
		Control de acceso de entrada y salida	Robo
		Falta de planes de contingencia y políticas formalizados	Falta y actualización de planes de contingencia y políticas de uso formalizado
		Robo de clave o ingreso a máquinas de administración	Acceso indebido de personas no autorizadas (lógico)
		Capacidad y disponibilidad de almacenamiento	No contar con capacidad para almacenamiento
		Falla del equipo	Pérdida de información de los aplicativos vigentes en Host, afectando la continuidad de la operación y servicios
		Problemas con actualizaciones y mantenimientos por vigencia tecnológica vencida	Daños ocasionados por falta de mantenimiento (físico y lógico), actualización de sistema operativo
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo
		No contar con el equipo de almacenamiento	No continuidad con el proyecto de cierre de host

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS
Activo	Criticidad	Descripción	Descripción
SERVIDOR HMC	1	Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad
		Falta de protección contra inundaciones	Daños ocasionados por agua
		Posibilidad de incendios	Daños ocasionados por fuego
		Funcionamiento inadecuado de UPS (sin soporte)	Daños ocasionados por corte de suministro eléctrico
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres naturales (Terremotos)
		Crecimiento no planificado de entidades externas, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo
		Falta de capacitación (personal de administración)	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)
		Control de acceso de entrada y salida	Robo
		Falta de planes de contingencia y políticas formalizados	Falta y actualización de planes de contingencia y políticas de uso formalizado
		Robo de clave o ingreso a máquinas de administración	Acceso indebido de personas no autorizadas (lógico)
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo
		No existe una política formal de cambio de credenciales	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores
AIRE DE PRESICION	3	Falla del equipo	Daños ocasionados por condiciones inadecuadas de temperatura y humedad
		Falta de protección contra inundaciones	Daños ocasionados por agua
		Posibilidad de incendios	Daños ocasionados por fuego
		Funcionamiento inadecuado de UPS (sin soporte)	Daños ocasionados por corte de suministro eléctrico
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres naturales (Terremotos)
		Falta de capacitación (personal de administración)	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS
Activo	Criticidad	Descripción	Descripción
		Control de acceso de entrada y salida	Robo
		Falta de planes de contingencia y políticas formalizados	Falta y actualización de planes de contingencia y políticas de uso formalizado
		Robo de clave o ingreso a máquinas de administración	Acceso indebido de personas no autorizadas (lógico)
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo
		No existe una política formal de cambio de credenciales	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores
AIRE MOCHILA	TIPO 2	Falla del equipo	Daños ocasionados por condiciones inadecuadas de temperatura y humedad
		Falta de protección contra inundaciones	Daños ocasionados por agua
		Posibilidad de incendios	Daños ocasionados por fuego
		Funcionamiento inadecuado de UPS (sin soporte)	Daños ocasionados por corte de suministro eléctrico
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres naturales (Terremotos)
		Falta de capacitación (personal de administración)	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)
		Control de acceso de entrada y salida	Robo
		Falta de planes de contingencia y políticas formalizados	Falta y actualización de planes de contingencia y políticas de uso formalizado
		Robo de clave o ingreso a máquinas de administración	Acceso indebido de personas no autorizadas (lógico)
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo
		No existe una política formal de cambio de credenciales	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores
UPS	3	Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS
Activo	Criticidad	Descripción	Descripción
		Falta de protección contra inundaciones	Daños ocasionados por agua
		Posibilidad de incendios	Daños ocasionados por fuego
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres naturales (Terremotos)
		Crecimiento no planificado de entidades externas, aplicativos y transaccionalidad	Degradación por saturación de carga eléctrica
		Falta de capacitación (personal de administración)	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)
		Control de acceso de entrada y salida	Robo
		Falta de planes de contingencia y políticas formalizados	Falta y actualización de planes de contingencia y políticas de uso formalizado
		Robo de clave o ingreso a máquinas de administración	Acceso indebido de personas no autorizadas (lógico)
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo
		No existe una política formal de cambio de credenciales	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores
SERVIDOR UNIX	3	Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad
		Falta de protección contra inundaciones	Daños ocasionados por agua
		Posibilidad de incendios	Daños ocasionados por fuego
		Funcionamiento inadecuado de UPS (sin soporte)	Daños ocasionados por corte de suministro eléctrico
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres naturales (Terremotos)
		Crecimiento no planificado de entidades externas, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo
		Falta de capacitación (personal de administración)	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)
		Control de acceso de entrada y salida	Robo

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS
Activo	Criticidad	Descripción	Descripción
		Falta de planes de contingencia y políticas formalizados	Falta y actualización de planes de contingencia y políticas de uso formalizado
		Robo de clave o ingreso a máquinas de administración	Acceso indebido de personas no autorizadas (lógico)
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo
		No existe una política formal de cambio de credenciales	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores
SERVER VTAPE	2	Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad
		Falta de protección contra inundaciones	Daños ocasionados por agua
		Posibilidad de incendios	Daños ocasionados por fuego
		Funcionamiento inadecuado de UPS (sin soporte)	Daños ocasionados por corte de suministro eléctrico
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres naturales (Terremotos)
		Crecimiento no planificado de entidades externas, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo
		Falta de capacitación (personal de administración)	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)
		Control de acceso de entrada y salida	Robo
		Falta de planes de contingencia y políticas formalizados	Falta y actualización de planes de contingencia y políticas de uso formalizado
		Robo de clave o ingreso a máquinas de administración	Acceso indebido de personas no autorizadas (lógico)
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo
		No existe una política formal de cambio de credenciales	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS
Activo	Criticidad	Descripción	Descripción
SWITCH DE PASO	3	Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad
		Falta de protección contra inundaciones	Daños ocasionados por agua
		Posibilidad de incendios	Daños ocasionados por fuego
		Funcionamiento inadecuado de UPS (sin soporte)	Daños ocasionados por corte de suministro eléctrico
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres naturales (Terremotos)
		Crecimiento no planificado de entidades externas, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo
		Falta de capacitación (personal de administración)	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)
		Control de acceso de entrada y salida	Robo
		Falta de planes de contingencia y políticas formalizados	Falta y actualización de planes de contingencia y políticas de uso formalizado
		Robo de clave o ingreso a máquinas de administración	Acceso indebido de personas no autorizadas (lógico)
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo
		No existe una política formal de cambio de credenciales	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores
Aplicativos alojados en el sistema HOST	3	Aplicación de cambios sin pruebas	No contar con las pruebas unitarias necesarias para cambio
		Falta de capacitación (personal de administración)	Inadecuado manejo de mantenimiento de los aplicativos
		Imposibilidad de recuperar los aplicativos	Falta y actualización de planes de contingencia
		Robo de clave o ingreso a máquinas de administración	Acceso indebido de personas no autorizadas (lógico)
		Pisar los cambios recientes de los aplicativos	No tener versionado el código fuente de los aplicativos
		Mal funcionamiento de los aplicativos	No tener un ambiente de desarrollo y pruebas

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS
Activo	Criticidad	Descripción	Descripción
		No proporcionar servicios	No contar con alta disponibilidad
		Accesos no controlados a los aplicativos	No contar con módulo autenticación
		Mal uso de las cuentas de usuario	Las claves no siguen las buenas prácticas de construcción
		No existe una política formal de cambio de credenciales	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores

5.3.1.5 Valoración del impacto

Para cada activo y amenaza se ha estimado la degradación, es decir el porcentaje en que la amenaza daña al activo en estudio, estableciendo un valor entre 0% (no lo daña) y el 100% (lo daña absolutamente) para cada una de las características de disponibilidad, integridad y confidencialidad.

A continuación, se muestra la degradación que se ha aplicado a los activos que se están analizando en la Tabla 5-8.

Tabla 5-8 Valoración de degradación e impacto

IDENTIFICACIÓN DE ACTIVOS		AMENAZAS	DEGRADACIÓN			IMPACTO
Activo	Criticidad	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL
Main-Frame Z10BC	3	Daños ocasionados por fuego	100%	50%	20%	3
		Daños ocasionados por agua	100%	50%	20%	3
		Daños ocasionados por desastres naturales (Terremotos)	100%	100%	20%	3
		Daños ocasionados por corte de suministro eléctrico	50%	50%	50%	1,5
		Daños ocasionados por condiciones inadecuadas de temperatura y humedad	50%	50%	20%	1,5
		Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	50%	50%	50%	1,5
		Posibilidad de tener interrupción de servicios de enlaces de datos	100%	50%	50%	3

IDENTIFICACIÓN DE ACTIVOS		AMENAZAS	DEGRADACIÓN			IMPACTO
Activo	Criticidad	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL
		Falta de soporte y garantía del fabricante sobre el hardware en el que está instalada la solución	100%	100%	50%	3
		Falta de soporte y actualización del equipo	50%	50%	20%	1,5
		Perdida de servicio de conectividad con elementos periféricos de la plataforma	100%	50%	50%	3
		No contar con un sistema de alimentación eléctrica externa (grupo electrógeno)	50%	100%	100%	3
		Posibilidad de tener cortes en la continuidad del servicio (disponibilidad)	100%	100%	10%	3
UNIDAD DE CARTUCHOS	2	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	50%	50%	20%	1,5
		Daños ocasionados por agua	50%	50%	20%	1,5
		Daños ocasionados por fuego	100%	100%	10%	3
		Daños ocasionados por corte de suministro eléctrico	100%	100%	20%	3
		Daños ocasionados por desastres naturales (Terremotos)	100%	100%	10%	3
		Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	50%	50%	20%	1,5
		Robo	100%	100%	50%	3
		Falta y actualización de planes de contingencia y políticas de uso formalizado	100%	100%	50%	3
		Acceso indebido de personas no autorizadas (lógico)	100%	100%	50%	3
		Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	100%	100%	50%	3
		Desconexión deliberada o accidental del equipo	100%	100%	20%	3
ALMACENAMIENTO (STORAGE)	3	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	100%	20%	3
		Daños ocasionados por agua	100%	100%	20%	3
		Daños ocasionados por fuego	100%	100%	20%	3
		Daños ocasionados por corte de suministro eléctrico	100%	50%	20%	3

IDENTIFICACIÓN DE ACTIVOS		AMENAZAS	DEGRADACIÓN			IMPACTO
Activo	Criticidad	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL
		Daños ocasionados por desastres naturales (Terremotos)	100%	100%	10%	3
		Degradación por saturación de recursos del equipo	50%	50%	50%	1,5
		Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	100%	50%	50%	3
		Robo	100%	100%	20%	3
		Falta y actualización de planes de contingencia y políticas de uso formalizado		50%	50%	1,5
		Acceso indebido de personas no autorizadas (lógico)	100%	50%	20%	3
		No contar con capacidad para almacenamiento	100%	50%	20%	3
		Pérdida de información de los aplicativos vigentes en Host, afectando la continuidad de la operación y servicios	100%	100%	50%	3
		Daños ocasionados por falta de mantenimiento (físico y lógico), actualización de sistema operativo	100%	100%	50%	3
		Desconexión deliberada o accidental del equipo	100%	50%	20%	3
		No continuidad con el proyecto de cierre de host	100%	100%	50%	3
SERVIDOR HMC	1	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	30%	30%	10%	0,9
		Daños ocasionados por agua	100%	50%	10%	3
		Daños ocasionados por fuego	100%	100%	10%	3
		Daños ocasionados por corte de suministro eléctrico	100%	100%	10%	3
		Daños ocasionados por desastres naturales (Terremotos)	100%	100%	10%	3
		Degradación por saturación de recursos del equipo	30%	30%	10%	0,9
		Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	100%	50%	20%	3
		Robo	100%	100%	50%	3

IDENTIFICACIÓN DE ACTIVOS		AMENAZAS	DEGRADACIÓN			IMPACTO
Activo	Criticidad	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL
		Falta y actualización de planes de contingencia y políticas de uso formalizado	50%	50%	20%	1,5
		Acceso indebido de personas no autorizadas (lógico)	50%	50%	10%	1,5
		Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	50%	50%	20%	1,5
		Desconexión deliberada o accidental del equipo	50%	50%	20%	1,5
		Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	50%	50%	20%	1,5
AIRE DE PRESICION	3	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	100%	20%	3
		Daños ocasionados por agua	100%	100%	20%	3
		Daños ocasionados por fuego	100%	100%	20%	3
		Daños ocasionados por corte de suministro eléctrico	100%	100%	20%	3
		Daños ocasionados por desastres naturales (Terremotos)	100%	100%	10%	3
		Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	50%	50%	20%	1,5
		Robo	100%	100%	20%	3
		Falta y actualización de planes de contingencia y políticas de uso formalizado	100%	50%	20%	3
		Acceso indebido de personas no autorizadas (lógico)	100%	50%	50%	3
		Daños ocasionados por falta de mantenimiento	100%	50%	20%	3
		Desconexión deliberada o accidental del equipo	100%	50%	20%	3
		Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	100%	50%	20%	3
AIRE MOCHILA	TIPO 2	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	100%	20%	3
		Daños ocasionados por agua	100%	100%	20%	3

IDENTIFICACIÓN DE ACTIVOS		AMENAZAS	DEGRADACIÓN			IMPACTO
Activo	Criticidad	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL
		Daños ocasionados por fuego	100%	100%	20%	3
		Daños ocasionados por corte de suministro eléctrico	100%	100%	20%	3
		Daños ocasionados por desastres naturales (Terremotos)	100%	100%	10%	3
		Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	50%	50%	20%	1,5
		Robo	100%	100%	20%	3
		Falta y actualización de planes de contingencia y políticas de uso formalizado	100%	50%	20%	3
		Acceso indebido de personas no autorizadas (lógico)	100%	50%	50%	3
		Daños ocasionados por falta de mantenimiento	100%	50%	20%	3
		Desconexión deliberada o accidental del equipo	100%	50%	20%	3
		Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	100%	50%	20%	3
UPS	3	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	100%	20%	3
		Daños ocasionados por agua	100%	50%	20%	3
		Daños ocasionados por fuego	100%	100%	20%	3
		Daños ocasionados por desastres naturales (Terremotos)	100%	100%	10%	3
		Degradación por saturación de carga eléctrica	50%	50%	20%	1,5
		Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	100%	100%	20%	3
		Robo	100%	100%	20%	3
		Falta y actualización de planes de contingencia y políticas de uso formalizado	50%	50%	10%	1,5
		Acceso indebido de personas no autorizadas (lógico)	100%	50%	20%	3
		Daños ocasionados por falta de mantenimiento	100%	100%	20%	3

IDENTIFICACIÓN DE ACTIVOS		AMENAZAS	DEGRADACIÓN			IMPACTO
Activo	Criticidad	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL
		Desconexión deliberada o accidental del equipo	100%	50%	20%	3
		Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	50%	50%	20%	1,5
SERVIDOR UNIX	3	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	100%	20%	3
		Daños ocasionados por agua	100%	100%	20%	3
		Daños ocasionados por fuego	100%	100%	20%	3
		Daños ocasionados por corte de suministro eléctrico	100%	100%	10%	3
		Daños ocasionados por desastres naturales (Terremotos)	100%	100%	10%	3
		Degradación por saturación de recursos del equipo	50%	50%	20%	1,5
		Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	100%	50%	20%	3
		Robo	100%	100%	20%	3
		Falta y actualización de planes de contingencia y políticas de uso formalizado	50%	50%	20%	1,5
		Acceso indebido de personas no autorizadas (lógico)	100%	50%	10%	3
		Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	100%	100%	20%	3
		Desconexión deliberada o accidental del equipo	100%	50%	20%	3
		Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	100%	50%	20%	3
SERVER VTAPE	2	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	50%	20%	3
		Daños ocasionados por agua	100%	100%	20%	3
		Daños ocasionados por fuego	100%	100%	20%	3
		Daños ocasionados por corte de suministro eléctrico	100%	100%	20%	3

IDENTIFICACIÓN DE ACTIVOS		AMENAZAS	DEGRADACIÓN			IMPACTO
Activo	Criticidad	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL
		Daños ocasionados por desastres naturales (Terremotos)	100%	100%	10%	3
		Degradación por saturación de recursos del equipo	100%	50%	20%	3
		Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	100%	50%	20%	3
		Robo	100%	100%	20%	3
		Falta y actualización de planes de contingencia y políticas de uso formalizado	50%	50%	20%	1,5
		Acceso indebido de personas no autorizadas (lógico)	100%	50%	20%	3
		Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	100%	100%	20%	3
		Desconexión deliberada o accidental del equipo	100%	50%	20%	3
		Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	100%	50%	20%	3
SWITCH DE PASO	3	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	100%	20%	3
		Daños ocasionados por agua	100%	100%	20%	3
		Daños ocasionados por fuego	100%	100%	20%	3
		Daños ocasionados por corte de suministro eléctrico	100%	100%	20%	3
		Daños ocasionados por desastres naturales (Terremotos)	100%	100%	10%	3
		Degradación por saturación de recursos del equipo	50%	50%	20%	1,5
		Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	100%	50%	20%	3
		Robo	100%	100%	20%	3
		Falta y actualización de planes de contingencia y políticas de uso formalizado	100%	50%	20%	3
		Acceso indebido de personas no autorizadas (lógico)	100%	50%	20%	3

IDENTIFICACIÓN DE ACTIVOS		AMENAZAS	DEGRADACIÓN			IMPACTO
Activo	Criticidad	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL
		Daños ocasionados por falta de mantenimiento	100%	100%	20%	3
		Desconexión deliberada o accidental del equipo	100%	50%	20%	3
		Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	100%	50%	20%	3
Aplicativos alojados en el sistema HOST	3	No contar con las pruebas unitarias necesarias para cambio	50%	50%	20%	1,5
		Inadecuado manejo de mantenimiento de los aplicativos	100%	100%	20%	3
		Falta y actualización de planes de contingencia	100%	100%	20%	3
		Acceso indebido de personas no autorizadas (lógico)	50%	100%	100%	3
		No tener versionado el código fuente de los aplicativos	50%	100%	50%	3
		No tener un ambiente de desarrollo y pruebas	25%	100%	50%	3
		No contar con alta disponibilidad	100%	50%	50%	3
		No contar con módulo autenticación	25%	100%	100%	3
		Las claves no siguen las buenas prácticas de construcción	25%	100%	100%	3
		Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	25%	100%	100%	3

5.3.1.6 Valoración Riesgo

En la valoración del riesgo se establece el nivel de riesgo que cada amenaza ocasiona sobre el activo, y se establece mediante la identificación de la frecuencia de que ocurra el evento y el impacto (pérdidas y daños) que el evento produce sobre los activos.

Los criterios utilizados para la calificación de la frecuencia se muestran en la Tabla 5-3:

El cálculo del riesgo se obtiene multiplicando la frecuencia por el impacto, como se puede ver en la Tabla 5-9, y el cálculos posteriores:

Tabla 5-9 Tabla resumen de valoración del riesgo

IDENTIFICACIÓN DE ACTIVOS		AMENAZAS			CÁLCULOS		
<i>Activo</i>	<i>Descripción</i>	<i>FRECUENCIA</i>	<i>IMPACTO</i>	<i>RIESGO</i>			
Main-Frame Z10BC	Daños ocasionados por fuego	0,1	3,00	0,30			
	Daños ocasionados por agua	0,1	3,00	0,30			
	Daños ocasionados por desastres naturales (Terremotos)	0,1	3,00	0,30			
	Daños ocasionados por corte de suministro eléctrico	0,1	1,50	0,15			
	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	1	1,50	1,50			
	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	0,1	1,50	0,15			
	Posibilidad de tener interrupción de servicios de enlaces de datos	0,1	3,00	0,30			
	Falta de soporte y garantía del fabricante sobre el hardware en el que está instalada la solución	2	3,00	6,00			
	Falta de soporte y actualización del equipo	2	1,50	3,00			
	Perdida de servicio de conectividad con elementos periféricos de la plataforma	1	3,00	3,00			
	No contar con un sistema de alimentación eléctrica externa (grupo electrógeno)	0,1	3,00	0,30			
	Posibilidad de tener cortes en la continuidad del servicio (disponibilidad)	0,1	3,00	0,30			
UNIDAD CARTUCHOS DE	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	2	1,50	3,00			
	Daños ocasionados por agua	0,1	1,50	0,15			
	Daños ocasionados por fuego	0,1	3,00	0,30			
	Daños ocasionados por corte de suministro eléctrico	1	3,00	3,00			
	Daños ocasionados por desastres naturales (Terremotos)	0,1	3,00	0,30			
	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	0,1	1,50	0,15			
	Robo	0,1	3,00	0,30			
	Falta y actualización de planes de contingencia y políticas de uso formalizado	0,1	3,00	0,30			
	Acceso indebido de personas no autorizadas (lógico)	0,1	3,00	0,30			

IDENTIFICACIÓN DE ACTIVOS	AMENAZAS	CÁLCULOS		
<i>Activo</i>	<i>Descripción</i>	<i>FRECUENCIA</i>	<i>IMPACTO</i>	<i>RIESGO</i>
	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	3	3,00	9,00
	Desconexión deliberada o accidental del equipo	0,1	3,00	0,30
	No continuidad con el proyecto de cierre de host	3	3,00	9,00
ALMACENAMIENTO (STORAGE)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	1	3,00	3,00
	Daños ocasionados por agua	0,1	3,00	0,30
	Daños ocasionados por fuego	0,1	3,00	0,30
	Daños ocasionados por corte de suministro eléctrico	0,1	3,00	0,30
	Daños ocasionados por desastres naturales (Terremotos)	0,1	3,00	0,30
	Degradación por saturación de recursos del equipo	1	1,50	1,50
	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	0,1	3,00	0,30
	Robo	0,1	3,00	
	Falta y actualización de planes de contingencia y políticas de uso formalizado	0,1	1,50	0,15
	Acceso indebido de personas no autorizadas (lógico)	0,1	3,00	0,30
	No contar con capacidad para almacenamiento	1	3,00	3,00
	Pérdida de información de los aplicativos vigentes en Host, afectando la continuidad de la operación y servicios	1	3,00	3,00
	Daños ocasionados por falta de mantenimiento (físico y lógico), actualización de sistema operativo	3	3,00	9,00
	Desconexión deliberada o accidental del equipo	0,1	3,00	0,30
	No continuidad con el proyecto de cierre de host	0,1	3,00	0,30
SERVIDOR HMC	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	0,1	0,90	0,09
	Daños ocasionados por agua	0,1	3,00	0,30
	Daños ocasionados por fuego	0,1	3,00	0,30
	Daños ocasionados por corte de suministro eléctrico	0,1	3,00	0,30

IDENTIFICACIÓN DE ACTIVOS	AMENAZAS	CÁLCULOS		
<i>Activo</i>	<i>Descripción</i>	<i>FRECUENCIA</i>	<i>IMPACTO</i>	<i>RIESGO</i>
	Daños ocasionados por desastres naturales (Terremotos)	0,1	3,00	0,30
	Degradación por saturación de recursos del equipo	0,1	0,90	0,09
	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	0,1	3,00	0,30
	Robo	0,1	3,00	0,30
	Falta y actualización de planes de contingencia y políticas de uso formalizado	0,1	1,50	0,15
	Acceso indebido de personas no autorizadas (lógico)	0,1	1,50	0,15
	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	0,1	1,50	0,15
	Desconexión deliberada o accidental del equipo	0,1	1,50	0,15
	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	0,1	1,50	0,15
AIRE DE PRESICION	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	0,1	3,00	0,30
	Daños ocasionados por agua	0,1	3,00	0,30
	Daños ocasionados por fuego	0,1	3,00	0,30
	Daños ocasionados por corte de suministro eléctrico	0,1	3,00	0,30
	Daños ocasionados por desastres naturales (Terremotos)	0,1	3,00	0,30
	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	0,1	3,00	0,30
	Robo	0,1	3,00	0,30
	Falta y actualización de planes de contingencia y políticas de uso formalizado	0,1	3,00	0,30
	Acceso indebido de personas no autorizadas (lógico)	0,1	3,00	0,30
	Daños ocasionados por falta de mantenimiento	0,1	3,00	0,30
	Desconexión deliberada o accidental del equipo	0,1	3,00	0,30
	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	0,1	3,00	0,30

IDENTIFICACIÓN DE ACTIVOS		CÁLCULOS		
Activo	AMENAZAS	FRECUENCIA	IMPACTO	RIESGO
AIRE MOCHILA	TIPO			
	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	0,1	3,00	0,30
	Daños ocasionados por agua	0,1	3,00	0,30
	Daños ocasionados por fuego	0,1	3,00	0,30
	Daños ocasionados por corte de suministro eléctrico	0,1	3,00	0,30
	Daños ocasionados por desastres naturales (Terremotos)	0,1	3,00	0,30
	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	0,1	1,50	0,15
	Robo	0,1	3,00	0,30
	Falta y actualización de planes de contingencia y políticas de uso formalizado	0,1	3,00	0,30
	Acceso indebido de personas no autorizadas (lógico)	0,1	3,00	0,30
	Daños ocasionados por falta de mantenimiento	0,1	3,00	0,30
	Desconexión deliberada o accidental del equipo	0,1	3,00	0,30
	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	0,1	3,00	0,30
UPS				
	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	0,1	3,00	0,30
	Daños ocasionados por agua	0,1	3,00	0,30
	Daños ocasionados por fuego	0,1	3,00	0,30
	Daños ocasionados por desastres naturales (Terremotos)	0,1	3,00	0,30
	Degradación por saturación de carga eléctrica	0,1	1,50	0,15
	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	0,1	3,00	0,30
	Robo	0,1	3,00	0,30
	Falta y actualización de planes de contingencia y políticas de uso formalizado	0,1	1,50	0,15
	Acceso indebido de personas no autorizadas (lógico)	0,1	3,00	0,30
	Daños ocasionados por falta de mantenimiento	3	3,00	9,00
	Desconexión deliberada o accidental del equipo	0,1	3,00	0,30

IDENTIFICACIÓN DE ACTIVOS	AMENAZAS	CÁLCULOS		
<i>Activo</i>	<i>Descripción</i>	<i>FRECUENCIA</i>	<i>IMPACTO</i>	<i>RIESGO</i>
	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	0,1	1,50	0,15
SERVIDOR UNIX	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	0,1	3,00	0,30
	Daños ocasionados por agua	0,1	3,00	0,30
	Daños ocasionados por fuego	0,1	3,00	0,30
	Daños ocasionados por corte de suministro eléctrico	0,1	3,00	0,30
	Daños ocasionados por desastres naturales (Terremotos)	0,1	3,00	0,30
	Degradación por saturación de recursos del equipo	0,1	1,50	0,15
	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	0,1	3,00	0,30
	Robo	0,1	3,00	0,30
	Falta y actualización de planes de contingencia y políticas de uso formalizado	0,1	1,50	0,15
	Acceso indebido de personas no autorizadas (lógico)	0,1	3,00	0,30
	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	3	3,00	9,00
	Desconexión deliberada o accidental del equipo	0,1	3,00	0,30
SERVER VTAPE	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	0,1	3,00	0,30
	Daños ocasionados por agua	0,1	3,00	0,30
	Daños ocasionados por fuego	0,1	3,00	0,30
	Daños ocasionados por corte de suministro eléctrico	0,1	3,00	0,30
	Daños ocasionados por desastres naturales (Terremotos)	0,1	3,00	0,30
	Degradación por saturación de recursos del equipo	0,1	3,00	0,30
	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	0,1	3,00	0,30
	Robo	0,1	3,00	0,30

IDENTIFICACIÓN DE ACTIVOS	AMENAZAS	CÁLCULOS		
<i>Activo</i>	<i>Descripción</i>	<i>FRECUENCIA</i>	<i>IMPACTO</i>	<i>RIESGO</i>
	Falta y actualización de planes de contingencia y políticas de uso formalizado	0,1	1,50	0,15
	Acceso indebido de personas no autorizadas (lógico)	0,1	3,00	0,30
	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	3	3,00	9,00
	Desconexión deliberada o accidental del equipo	0,1	3,00	0,30
	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	0,1	3,00	0,30
SWITCH DE PASO	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	0,1	3,00	0,30
	Daños ocasionados por agua	0,1	3,00	0,30
	Daños ocasionados por fuego	0,1	3,00	0,30
	Daños ocasionados por corte de suministro eléctrico	0,1	3,00	0,30
	Daños ocasionados por desastres naturales (Terremotos)	0,1	3,00	0,30
	Degradación por saturación de recursos del equipo	0,1	1,50	0,15
	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	0,1	3,00	0,30
	Robo	0,1	3,00	0,30
	Falta y actualización de planes de contingencia y políticas de uso formalizado	0,1	3,00	0,30
	Acceso indebido de personas no autorizadas (lógico)	0,1	3,00	0,30
	Daños ocasionados por falta de mantenimiento	3	3,00	9,00
	Desconexión deliberada o accidental del equipo	0,1	3,00	0,30
	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	0,1	3,00	0,30
Aplicativos alojados en el sistema HOST - IESS	No contar con las pruebas unitarias necesarias para cambio	0,1	1,50	0,15
	Inadecuado manejo de mantenimiento de los aplicativos	0,1	3,00	0,30
	Falta y actualización de planes de contingencia	1	3,00	3,00

IDENTIFICACIÓN DE ACTIVOS		AMENAZAS			CÁLCULOS		
<i>Activo</i>		<i>Descripción</i>		<i>FRECUENCIA</i>	<i>IMPACTO</i>	<i>RIESGO</i>	
		Acceso indebido de personas no autorizadas (lógico)		0,1	3,00	0,30	
		No tener versionado el código fuente de los aplicativos		1	3,00	3,00	
		No tener un ambiente de desarrollo y pruebas		0,1	3,00	0,30	
		No contar con alta disponibilidad		3	3,00	9,00	
		No contar con módulo autenticación		0,1	3,00	0,30	
		Las claves no siguen las buenas prácticas de construcción		1	3,00	3,00	
		Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores		1	3,00	3,00	

Una vez que se han realizado los cálculos definidos, a la amenaza se le considera como el riesgo identificado, y se generan las gráficas de los mapas de calor con los valores del impacto y de la frecuencia. Los riesgos que sean críticos se deben analizar para identificar las contramedidas necesarias.

- Gráfica de riesgo sobre el equipo Main-frameZ10BC

En la Figura 5-4 se establece la relación frecuencia e impacto de cada uno de los activos como se muestra en la Tabla 5-10.

Tabla 5-10 Listado de riesgos de Main-FrameZ10BC

RIESGOS		Impacto	Frecuencia
R1	Daños ocasionados por fuego	3,00	0,10
R2	Daños ocasionados por agua	3,00	0,10
R3	Daños ocasionados por desastres naturales (Terremotos)	3,00	0,10
R4	Daños ocasionados por corte de suministro eléctrico	1,50	0,10
R5	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	1,50	1,00
R6	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	1,50	0,10
R7	Posibilidad de tener interrupción de servicios de enlaces de datos	3,00	0,10
R8	Falta de soporte y garantía del fabricante sobre el hardware en el que está instalada la solución	3,00	2,00
R9	Falta de soporte y actualización del equipo	1,50	2,00
R10	Perdida de servicio de conectividad con elementos periféricos de la plataforma	3,00	1,00
R11	No contar con un sistema de alimentación eléctrica externa (grupo electrógeno)	3,00	0,10

RIESGOS		Impacto	Frecuencia
R12	Posibilidad de tener cortes en la continuidad del servicio (disponibilidad)	3,00	0,10

Figura 5-4 Mapa de calor “Main-Frame Z10BC”

Resultados

Los riesgos en color verde son los que se encuentran controlados, los riesgos en amarillo son los que deben ser monitoreados en especial los que están más propensos a pasar al cuadrante rojo (R8, R10)

- Gráfica de riesgos de la Unidad de cartuchos

En la Figura 5-5 se establece la relación frecuencia e impacto de cada uno de los activos como se muestra en la Tabla 5-11.

Tabla 5-11. Listado de riesgos de la Unidad de cartuchos

RIESGOS		Impacto	Frecuencia
R1	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	1,50	2,00
R2	Daños ocasionados por agua	1,50	0,10
R3	Daños ocasionados por fuego	3,00	0,10
R4	Daños ocasionados por corte de suministro eléctrico	3,00	1,00
R5	Daños ocasionados por desastres naturales (Terremotos)	3,00	0,10
R6	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	1,50	0,10
R7	Robo	3,00	0,10
R8	Falta y actualización de planes de contingencia y políticas de uso formalizado	3,00	0,10
R9	Acceso indebido de personas no autorizadas (lógico)	3,00	0,10

RIESGOS		Impacto	Frecuencia
R10	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	3,00	3,00
R11	Desconexión deliberada o accidental del equipo	3,00	0,10
R12	No continuidad con el proyecto de cierre de host	3,00	3,00

Figura 5-5. Mapa de calor “Unidad de cartuchos”

Resultados

Los riesgos en color verde son los que se encuentran controlados (R6, R2), los riesgos que están en amarillo son los que deben ser monitoreados, en especial los que están más propensos a pasar al cuadrante rojo (R4), y los de color rojo son los riesgos descontrolados en los que debemos enfocarnos prioritariamente R10 y R12.

- Gráfica de los riesgos del Storage

En la Figura 5-6 se establece la relación frecuencia e impacto de cada uno de los activos como se muestra en la Tabla 5-12.

Tabla 5-12 Detalle de riesgos del Storage

RIESGOS		Impacto	Frecuencia
R1	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	3,00	1,00
R2	Daños ocasionados por agua	3,00	0,10
R3	Daños ocasionados por fuego	3,00	0,10
R4	Daños ocasionados por corte de suministro eléctrico	3,00	0,10
R5	Daños ocasionados por desastres naturales (Terremotos)	3,00	0,10
R6	Degradación por saturación de recursos del equipo	1,50	1,00

RIESGOS		Impacto	Frecuencia
R7	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	3,00	0,10
R8	Robo	3,00	0,10
R9	Falta y actualización de planes de contingencia y políticas de uso formalizado	1,50	0,10
R10	Acceso indebido de personas no autorizadas (lógico)	3,00	0,10
R11	No contar con capacidad para almacenamiento	3,00	1,00
R12	Pérdida de información de los aplicativos vigentes en Host , afectando la continuidad de la operación y servicios	3,00	1,00
R13	Daños ocasionados por falta de mantenimiento (físico y lógico) , actualización de sistema operativo	3,00	3,00
R14	Desconexión deliberada o accidental del equipo	3,00	0,10
R15	No continuidad con el proyecto de cierre de host	3,00	0,10

Figura 5-6 Mapa de calor "Storage"

Resultados

Los riesgos en color verde son los que se encuentran controlados R9, los riesgos que están en amarillo son los que deben ser monitoreados, en especial los que están más propensos a pasar al cuadrante rojo (R1, R11, R12), y los de color rojo son los riesgos descontrolados en los que debemos enfocarnos prioritariamente R13.

- Gráfica de riesgo Servidor HMC

En la Figura 5-7 se establece la relación frecuencia e impacto de cada uno de los activos como se muestra en la Tabla 5-13.

Tabla 5-13 Detalle de riesgos del Servidor HMC

RIESGOS		Impacto	Frecuencia
R1	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	0,90	0,10
R2	Daños ocasionados por agua	3,00	0,10
R3	Daños ocasionados por fuego	3,00	0,10
R4	Daños ocasionados por corte de suministro eléctrico	3,00	0,10
R5	Daños ocasionados por desastres naturales (Terremotos)	3,00	0,10
R6	Degradación por saturación de recursos del equipo	0,90	0,10
R7	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	3,00	0,10
R8	Robo	3,00	0,10
R9	Falta y actualización de planes de contingencia y políticas de uso formalizado	1,50	0,10
R10	Acceso indebido de personas no autorizadas (lógico)	1,50	0,10
R11	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	1,50	0,10
R12	Desconexión deliberada o accidental del equipo	1,50	0,10
R13	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	1,50	0,10

Figura 5-7 Mapa de calor “servidor HMC”

Resultados

Los riesgos en color verde son los que se encuentran controlados, los riesgos que están en amarillo son los que deben ser monitoreados, en especial los que están más propensos a pasar al cuadrante rojo (R2, R3, R4, R5, R7, R8), y no hay riesgos descontrolados.

- Gráfica de riesgo de equipo de Aires de Precisión

En la Figura 5-8 se establece la relación frecuencia e impacto de cada uno de los activos como se muestra en la Tabla 5-14.

Tabla 5-14 Detalle de riesgos de Aires de Precisión

RIESGOS		Impacto	Frecuencia
R1	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	3,00	0,10
R2	Daños ocasionados por agua	3,00	0,10
R3	Daños ocasionados por fuego	3,00	0,10
R4	Daños ocasionados por corte de suministro eléctrico	3,00	0,10
R5	Daños ocasionados por desastres naturales (Terremotos)	3,00	0,10
R6	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	3,00	0,10
R7	Robo	3,00	0,10
R8	Falta y actualización de planes de contingencia y políticas de uso formalizado	3,00	0,10
R9	Acceso indebido de personas no autorizadas (lógico)	3,00	0,10
R10	Daños ocasionados por falta de mantenimiento	3,00	0,10
R11	Desconexión deliberada o accidental del equipo	3,00	0,10
R12	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	3,00	0,10

Figura 5-8 Mapa de calor “Aires de Precisión”

Resultados

Los riesgos en color verde son los que se encuentran controlados, los riesgos que están en amarillo son los que deben ser monitoreados, en caso que estén propensos a pasar al cuadrante rojo, en este caso particular, los riesgo del cuadrante amarillo están muy abajo para pasar al cuadrante rojo.

- Gráfica de riesgo de equipo de Aires tipo mochila

En la Figura 5-9 se establece la relación frecuencia e impacto de cada uno de los activos como se muestra en la Tabla 5-15.

Tabla 5-15 Detalle de riesgos de Aires tipo Mochila

RIESGOS		Impacto	Frecuencia
R1	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	3,00	0,10
R2	Daños ocasionados por agua	3,00	0,10
R3	Daños ocasionados por fuego	3,00	0,10
R4	Daños ocasionados por corte de suministro eléctrico	3,00	0,10
R5	Daños ocasionados por desastres naturales (Terremotos)	3,00	0,10
R6	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	1,50	0,10
R7	Robo	3,00	0,10
R8	Falta y actualización de planes de contingencia y políticas de uso formalizado	3,00	0,10
R9	Acceso indebido de personas no autorizadas (lógico)	3,00	0,10
R10	Daños ocasionados por falta de mantenimiento	3,00	0,10
R11	Desconexión deliberada o accidental del equipo	3,00	0,10
R12	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	3,00	0,10

Figura 5-9 Mapa de calor “Aires tipo Mochila”

Resultados

Los riesgos en color verde son los que se encuentran controlados, los riesgos que están en amarillo son los que deben ser monitoreados, en caso que estén propensos a pasar al cuadrante rojo, en este caso particular, los riesgo del cuadrante amarillo están muy abajo para pasar al cuadrante rojo.

- Gráfica de riesgo de equipo UPS

En la Figura 5-10 se establece la relación frecuencia e impacto de cada uno de los activos como se muestra en la Tabla 5-16.

Tabla 5-16 Detalle de riesgos de equipo UPS

RIESGOS		Impacto	Frecuencia
R1	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	3,00	0,10
R2	Daños ocasionados por agua	3,00	0,10
R3	Daños ocasionados por fuego	3,00	0,10
R4	Daños ocasionados por desastres naturales (Terremotos)	3,00	0,10
R5	Degradación por saturación de carga eléctrica	1,50	0,10
R6	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	3,00	0,10
R7	Robo	3,00	0,10
R8	Falta y actualización de planes de contingencia y políticas de uso formalizado	1,50	0,10
R9	Acceso indebido de personas no autorizadas (lógico)	3,00	0,10
R10	Daños ocasionados por falta de mantenimiento	3,00	3,00
R11	Desconexión deliberada o accidental del equipo	3,00	0,10
R12	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	1,50	0,10

Figura 5-10 Mapa de calor “UPS”

Resultados

Los riesgos en color verde son los que se encuentran controlados, los riesgos que están en amarillo son los que deben ser monitoreados, en especial los que están más propensos a pasar al cuadrante en rojo, y el riesgo descontrolado es R10, en el cual hay que poner énfasis en mecanismos de mitigación

- Gráfica de riesgo de equipo servidor Unix (Micros)

En la Figura 5-11 se establece la relación frecuencia e impacto de cada uno de los activos como se muestra en la Tabla 5-17.

Tabla 5-17 Detalle de riesgos servidor Unix (Micros)

RIESGOS		Impacto	Frecuencia
R1	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	3,00	0,10
R2	Daños ocasionados por agua	3,00	0,10
R3	Daños ocasionados por fuego	3,00	0,10
R4	Daños ocasionados por corte de suministro eléctrico	3,00	0,10
R5	Daños ocasionados por desastres naturales (Terremotos)	3,00	0,10
R6	Degradación por saturación de recursos del equipo	1,50	0,10
R7	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	3,00	0,10
R8	Robo	3,00	0,10
R9	Falta y actualización de planes de contingencia y políticas de uso formalizado	1,50	0,10
R10	Acceso indebido de personas no autorizadas (lógico)	3,00	0,10

RIESGOS		Impacto	Frecuencia
R11	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	3,00	3,00
R12	Desconexión deliberada o accidental del equipo	3,00	0,10
R13	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	3,00	0,10

Figura 5-11 Mapa de calor “servidor Unix Micros”

Resultados

Los riesgos en color verde son los que se encuentran controlados (R6, R9), los riesgos que están en amarillo son los que deben ser monitoreados, en especial los que están más propensos a pasar al cuadrante en rojo, y el riesgo descontrolado es R11, en el cual hay que poner énfasis en mecanismos de mitigación.

- Gráfica de riesgo de equipo servidor vtape

En la Figura 5-12 se establece la relación frecuencia e impacto de cada uno de los activos como se muestra en la Tabla 5-18 .

Tabla 5-18 Detalle de riesgos servidor vtape

RIESGOS		Impacto	Frecuencia
R1	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	3,00	0,10
R2	Daños ocasionados por agua	3,00	0,10
R3	Daños ocasionados por fuego	3,00	0,10
R4	Daños ocasionados por corte de suministro eléctrico	3,00	0,10
R5	Daños ocasionados por desastres naturales (Terremotos)	3,00	0,10
R6	Degradación por saturación de recursos del equipo	3,00	0,10

RIESGOS		Impacto	Frecuencia
R7	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	3,00	0,10
R8	Robo	3,00	0,10
R9	Falta y actualización de planes de contingencia y políticas de uso formalizado	1,50	0,10
R10	Acceso indebido de personas no autorizadas (lógico)	3,00	0,10
R11	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	3,00	3,00
R12	Desconexión deliberada o accidental del equipo	3,00	0,10
R13	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	3,00	0,10

Figura 5-12 Mapa de calor “servidor vtape”

Resultados

Los riesgos en color verde son los que se encuentran controlados (R9), los riesgos en amarillo son los que deben ser monitoreados, en especial los que están más propensos a pasar al cuadrante en rojo, y el riesgo descontrolado es R11, en el cual hay que poner énfasis en mecanismos de mitigación.

- Gráfica de riesgo de equipo switch de paso

En la Figura 5-13Figura 5-8 se establece la relación frecuencia e impacto de cada uno de los activos como se muestra en la Tabla 5-19.

Tabla 5-19 Detalle de riesgos switch de paso

RIESGOS		Impacto	Frecuencia
R1	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	3,00	0,10
R2	Daños ocasionados por agua	3,00	0,10
R3	Daños ocasionados por fuego	3,00	0,10
R4	Daños ocasionados por corte de suministro eléctrico	3,00	0,10
R5	Daños ocasionados por desastres naturales (Terremotos)	3,00	0,10
R6	Degradación por saturación de recursos del equipo	1,50	0,10
R7	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	3,00	0,10
R8	Robo	3,00	0,10
R9	Falta y actualización de planes de contingencia y políticas de uso formalizado	3,00	0,10
R10	Acceso indebido de personas no autorizadas (lógico)	3,00	0,10
R11	Daños ocasionados por falta de mantenimiento	3,00	3,00
R12	Desconexión deliberada o accidental del equipo	3,00	0,10
R13	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	3,00	0,10

Figura 5-13 Mapa de calor “switch de paso”

Resultados

Los riesgos en color verde son los que se encuentran controlados (R6), los riesgos que están en amarillo son los que deben ser monitoreados, en especial los que están más propensos a pasar al cuadrante en rojo, y el riesgo descontrolado es R11, en el cual hay que poner énfasis en mecanismos de mitigación.

- Gráfica de riesgo de aplicativos alojados en el sistema HOST-IESS

En la Figura 5-14Figura 5-8 se establece la relación frecuencia e impacto de cada uno de los activos como se muestra en la Tabla 5-20.

Tabla 5-20 Detalle de riesgos “aplicativos alojados en el sistema Host-IESS”

RIESGOS		Impacto	Frecuencia
R1	No contar con las pruebas unitarias necesarias para cambio	1,50	0,10
R2	Inadecuado manejo de mantenimiento de los aplicativos	3,00	0,10
R3	Falta y actualización de planes de contingencia	3,00	1,00
R4	Acceso indebido de personas no autorizadas (lógico)	3,00	0,10
R5	No tener versionado el código fuente de los aplicativos	3,00	1,00
R6	No tener un ambiente de desarrollo y pruebas	3,00	0,10
R7	No contar con alta disponibilidad	3,00	3,00
R8	No contar con módulo autenticación	3,00	0,10
R9	Las claves no siguen las buenas prácticas de construcción	3,00	1,00
R10	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	3,00	1,00

Figura 5-14 Mapa de calor “aplicativos alojados en el sistema Host-IESS”

Resultados

Los riesgos en color verde son los que se encuentran controlados (R1), los riesgos que están en amarillo son los que deben ser monitoreados, en especial los que están más propensos a pasar al cuadrante en rojo (R3, R5, R9, R10), y el riesgo descontrolado es R7, en el cual hay que poner énfasis en mecanismos de mitigación.

- Gráfica de radar de los riesgos por activo

Se recupera la información calculada de los riesgos de los activos, se calcula el promedio de todos los riesgos identificados y se determinan los siguientes valores:

- Valor actual: promedio de todos los riesgos.
- Valor objetivo: recomendación de la SDNSI de reducción de riesgo (al menos el 50%).
- Valor límite: valor dado por condiciones gráficas, al que nunca se debería llegar el riesgo de los activos.

Los valores calculados se describen en la Tabla 5-21 y Figura 5-15.

Tabla 5-21 Tabla de valores de Riesgos de plataforma Host - IESS por activo

ACTIVO	ACTUAL	OBJETIVO	LIMITE	OBSERVACIÓN
Main-Frame Z10BC	1,30	0,65	3	Se recomienda para todos los identificados una reducción en el 50 %.
UNIDAD DE CARTUCHOS	2,18	1,09	3	
ALMACENAMIENTO (STORAGE)	1,58	0,79	3	
SERVIDOR HMC	0,21	0,11	3	
AIRE DE PRESICION	0,30	0,15	3	
AIRE TIPO MOCHILA	0,29	0,14	3	
UPS	0,99	0,49	3	
SERVIDOR UNIX (MICROS)	0,95	0,47	3	
SERVER VTAPE	0,96	0,48	3	
SWITCH DE PASO	0,96	0,48	3	
Aplicativos alojados en el sistema HOST	2,24	1,12	3

Figura 5-15 Reporte de riesgos plataforma Host – IESS por activo

- Controles o salvaguardas sugeridas

Con la información generada previamente, se procede a elaborar las contramedidas para cada una de las triplete activo – vulnerabilidad – amenaza, que se construye tomando los valores de los

activos más expuestos a los riesgos, y los riesgos de estos activos que se encuentran en el cuadrante rojo.

Tabla 5-22. Contramedidas para la Plataforma Host - IESS

Activo	Vulnerabilidad	Amenazas	Salvaguarda
Main-Frame Z10BC	No tener soporte y garantía del fabricante	Falta de soporte y garantía del fabricante sobre el hardware en el que está instalada la solución	Revisar y validar la factibilidad de arreglar los daños existentes y/o gestionar soporte técnico y mantenimiento
UNIDAD DE CARTUCHOS	Problemas con actualizaciones y mantenimientos por vigencia tecnológica vencida	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	Implementar una solución de gestión de respaldo(servicio) que permitan el uso de cartuchos y gestionar soporte técnico y mantenimiento periódico sobre dicho equipo
	No contar con medios de respaldos	No continuidad con el proyecto de cierre de host	
ALMACENAMIENTO (STORAGE)	Problemas con actualizaciones y mantenimientos por vigencia tecnológica vencida	Daños ocasionados por falta de mantenimiento (físico y lógico) , actualización de sistema operativo	Contar con soporte técnico y mantenimiento periódico que garantice el actual almacenamiento de los aplicativos de Host, data y sistema operativo.
UPS	Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento	Habilitar la carga en el ups EATON (sin carga) instalado en el data center para tener un equipo de contingencia
SERVIDOR UNIX (MICROS)	Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	Contar con la documentación de instalación del SERVIDOR UNIX (MICROS) y realizar un piloto de clonación del sistema en otro equipo
SERVER VTAPE	Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	Gestionar soporte técnico y mantenimiento periódico en dicho equipo para la gestión de respaldos
SWITCH DE PASO	Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento	Tener mecanismo de contingencia de dicho equipo
Aplicativos alojados en el sistema HOST	No proporcionar servicios	No contar con alta disponibilidad	Migrar los aplicativos, data y sistema operativo del Host a un Storage que permita garantizar alta disponibilidad con vigencia tecnológica.

5.3.1.7 Conclusiones

Los siguientes puntos resumen las conclusiones de la línea base del caso de estudio:

- Mediante el presente análisis y evaluación de riesgos, se concluye que el equipo Main-Frame Z10BC no tiene mantenimiento correctivo ni garantía del fabricante, siendo un activo crítico de la infraestructura informática del IESS.

- El equipo de almacenamiento Storage tiene una vulnerabilidad crítica debido a problemas con actualizaciones y mantenimientos por vigencia tecnológica vencida, lo cual al presentarse un problema puede desembocar en pérdida del equipo y de disponibilidad de los aplicativos alojados en el mismo.
- El equipo UPS EATON debe conectarse a la carga del Data Center, como equipo de contingencia al banco de UPS del Edificio Matriz, donde se encuentra instalada la Plataforma Z10, a fin de que no se afecte la operación.
- El equipo Servidor Vtape puede sufrir daños y, al no contar con soporte y mantenimiento, puede ocasionar que se afecte al proyecto de salvaguarda, migración, a servicio de procesos batch y no se tenga forma de generar respaldos de información.
- El equipo Switch de paso puede sufrir daños y, al no contar con soporte y mantenimiento, puede ocasionar que se afecte la operación del Main-Frame Z10BC.
- El equipo Unidad de Cartuchos puede sufrir daños y, al no contar con soporte y mantenimiento, puede ocasionar que se afecte la operación, el proyecto de salvaguarda, migración para el cierre del host, servicio de procesos batch y no se tenga forma de generar respaldos físicos de la información.

Resultado del presente análisis, los riesgos localizados en los cuadrantes de alto impacto y media frecuencia, así como los de medio impacto y alta frecuencia de los mapas de riesgos, deben ser monitoreados con periodicidad para cada uno de los activos, en la actividad “Valoración de Riesgos”.

5.3.1.8 Resumen de la Línea Base Inicial

En esta subsección se han plasmado las actividades realizadas en la elaboración de la matriz de riesgos utilizando los conceptos, parámetros y metodología definida en la SDNSI, de lo cual podemos identificar lo siguiente:

- El modelo conceptual para la gestión de riesgos de ciberseguridad está basado en la gestión de amenazas de ciberseguridad y no en vulnerabilidades de ciberseguridad.
- Los parámetros cualitativos son de rangos muy cortos, impidiendo determinar un impacto más puntual y no tan objetivo.
- No existen taxonomías y catálogos de las vulnerabilidades y amenazas utilizadas, generando duplicidad de las mismas por errores de sintaxis.
- No se validan los costos de los activos ni se valoran las vulnerabilidades de cada activo.
- Los riesgos son identificados para cada activo y no se tiene la trazabilidad de una amenaza presente en varios activos, así como las vulnerabilidades comunes que presentan los activos de la organización.
- Las contramedidas son presentadas por activo, y no permite analizar las vulnerabilidades y amenazas de ciberseguridad comunes que pueden ser atendidas por la misma contramedida.
- No utilizan ninguna herramienta informática para la gestión de riesgos en ciberseguridad.

Como conclusión podemos indicar que la gestión de riesgos de la DNTI se está realizando enfocándose en amenazas de ciberseguridad, dejando de lado el impacto de las vulnerabilidades de los activos de la organización.

5.3.2. Actividades del Marco de Trabajo AVARCIBER (Activos–Vulnerabilidades – Amenazas – Riesgos – CIBERseguridad)

En esta sección se describe como se ha implementado el marco de trabajo AVARCIBER, que es parte de la resolución del problema, en la empresa objeto del estudio experimental, que en este caso particular es el Instituto Ecuatoriano de Seguridad Social (IESS).

Para poder aplicar el marco de trabajo referencial definido, y poder comparar con la línea base elaborada, se han tomado las plataformas de la infraestructura tecnológica consideradas en el alcance de la línea base inicia. Las plataformas son las siguientes:

- Plataforma Host – IESS.
- Plataforma Oracle – IESS.
- Plataforma Firewall – IESS.
- Plataforma AS400 – IESS – (Hospital Carlos Andrade Marín - HCAM).

A continuación, se describen las actividades a desarrollar en el marco de trabajo AVARCIBER descrito en el capítulo 4. También, se indica como se ha realizado la implementación de las diferentes actividades definidas en el marco de trabajo.

Únicamente se han descrito las actividades ejecutadas para la **Plataforma Host – IESS**, los informes adicionales para el resto de las plataformas, utilizando el marco de trabajo AVARCIBER, se adjuntan en el Anexo IV de la presente tesis doctoral.

5.3.2.1 Identificar criterios de valoración

En esta actividad se determinan los criterios de valoración con los que se va a realizar la experimentación. En este caso particular, se ha determinado lo siguiente:

- Parámetros para medir el impacto de las dimensiones de seguridad (confidencialidad, integridad, disponibilidad, – CID), indicando los valores cualitativos y valores cuantitativos asociados, como se muestra en la Tabla 5-23.

Tabla 5-23. Parámetros para medir las dimensiones de seguridad AVARCIBER.

Criterio de valoración CONFIDENCIALIDAD (C)		
¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?		
Alta (A)	3	Información que puede ser conocida y utilizada por un grupo muy reducido de agentes, cuya divulgación podría ocasionar un perjuicio al IESS o terceros.
Media (M)	2	Información que solo puede ser conocida y utilizada por un grupo de agentes, que la necesiten para realizar su trabajo.
Baja (B)	1	Información que puede ser conocida y utilizada por todos los agentes del IESS.
Nula (N)	0	Información que puede ser conocida y utilizada sin autorización por cualquier persona, dentro o fuera del IESS.
Criterio de valoración INTEGRIDAD (I)		
¿Qué importancia tendría que los datos fueran modificados fuera de control?		
Alta (A)	3	Información cuya modificación no autorizada no podría repararse, impidiendo la realización de las actividades del IESS.
Media (M)	2	Información cuya modificación no autorizada es de difícil reparación y podría ocasionar un perjuicio significativo para el IESS o terceros.
Baja (B)	1	Información cuya modificación no autorizada puede repararse, aunque podría ocasionar un perjuicio para el IESS o terceros.
Nula (N)	0	Información cuya modificación no autorizada puede repararse fácilmente, o que no afecta a las actividades del IESS.
Criterio de valoración DISPONIBILIDAD (D)		

¿Qué importancia tendría que el activo no estuviera disponible?		
Alta (A)	3	Información cuya inaccesibilidad permanente durante una hora podría impedir la ejecución de las actividades del IESS.
Media (M)	2	Información cuya inaccesibilidad permanente durante la jornada laboral podría impedir la ejecución de las actividades del IESS.
Baja (B)	1	Información cuya inaccesibilidad permanente durante una semana podría ocasionar un perjuicio significativo para el IESS.
Nula (N)	0	Información cuya inaccesibilidad no afecta la actividad normal del IESS.

- Parámetro para determinar la criticidad del activo, en base a las dimensiones de seguridad que se describan para el activo, como se muestra en la Tabla 5-24.

Tabla 5-24. Parámetros para medir la criticidad en los activos de ciberseguridad AVARCIBER

Criterio de valoración CRITICIDAD		
Valor máximo de las tres características C.I.D.		
Alta (A)	3	Si el máximo es 3
Media (M)	2	Si el máximo es 2
Baja (B)	1	Si el máximo es 1
Nula (N)	0	Si todos son 0

- Daño que pueda presentarse en el activo (degradación del activo), que toma un valor de 0 a 10, dependiendo del impacto que vaya a representar según la Tabla 5-25.

Tabla 5-25. Parámetros para medir el impacto de degradación en los activos de ciberseguridad AVARCIBER

RANGO	Valor Superior	Valor Inferior
Daño Extremo	10	10
Muy Alto	9	9
Alto	8	6
Medio	5	3
Bajo	2	1
Despreciable	0	0

- Para medir la probabilidad de ocurrencia de una amenaza, se ha utilizado la siguiente relación de valores, que se muestra en la Tabla 5-26.

Tabla 5-26. Parámetros para medir la criticidad en los activos de ciberseguridad AVARCIBER

PROBABILIDAD				
RANGO	VALOR	PROBABILIDAD	DESCRIPCION	FRECUENCIA
MA (Muy Alto)	MA	100 %	muy frecuente	a diario

A (Alto)	A	10 %	frecuente	mensualmente
M (Medio)	M	1 %	normal	una vez al año
B (Bajo)	B	(1 / 10) %	poco frecuente	cada varios años
MB (Muy Bajo)	MB	(1/100) %	muy poco frecuente	siglos

- Para el calcular el riesgo de un activo, se ha utilizado la relación que se muestra en la Tabla 5-27.

Tabla 5-27. Valoración del Riesgo AVARCIBER

Tabla de Valoración del Riesgo														
I	F	R	I	F	R	I	F	R	I	F	R	I	F	R
0	MB	0	0	B	0	0	M	0	0	A	0	0	MA	0
1	MB	0	1	B	0	1	M	1	1	A	0	1	MA	1
2	MB	0	2	B	0	2	M	1	2	A	0	2	MA	4
3	MB	0	3	B	0	3	M	1	3	A	4	3	MA	4
4	MB	0	4	B	5	4	M	5	4	A	5	4	MA	8
5	MB	0	5	B	5	5	M	5	5	A	5	5	MA	8
6	MB	0	6	B	5	6	M	5	6	A	5	6	MA	9
7	MB	0	7	B	5	7	M	6	7	A	8	7	MA	9
8	MB	0	8	B	5	8	M	6	8	A	8	8	MA	9
9	MB	0	9	B	5	9	M	6	9	A	9	9	MA	10
10	MB	0	10	B	5	10	M	6	10	A	10	10	MA	10

- Se han personalizado las taxonomías de tipos de Activos, Vulnerabilidades de Ciberseguridad, Amenazas de Ciberseguridad, en base a estándares internacionales. Además, se incluyeron nuevos elementos según lo requería la organización. De esta forma, se han establecido taxonomías propias para la organización en donde se está experimentando (IESS). Los estándares tenidos en cuenta han sido:
- Para los Tipos de Activos, se ha utilizado ISO 27005.
- Para las Vulnerabilidades de ciberseguridad, se ha utilizado ISO 27005.
- Para Amenazas de ciberseguridad, se ha utilizado ENISA (European Union Agency for Network and Information Security).
- Para las Contramedidas, se han establecido de forma particular para el IESS.

5.3.2.2 Actividad 1: Lanzamiento

En esta actividad se han definido las taxonomías de los elementos del modelo conceptual, que fueron identificadas en el capítulo 2. Las taxonomías definidas fueron las siguientes:

Tarea 1: se establece la taxonomía de tipos de activos de la organización enfocados en ciberseguridad, basada en el estándar ISO 27005 (ISO/IEC 27000, 2018), tal como se muestra en la Tabla 5-28.

Tabla 5-28. Tipos de activos de ciberseguridad AVARCIBER

TIPO DE ACTIVO
Procesos y actividades de negocios

Información
Hardware
Software
Red
Personal
Sitio
Estructura de la organización

Tarea 2: se establece la taxonomía de Vulnerabilidades en ciberseguridad, basada en el estándar ISO 27005 (ISO/IEC 27000, 2018), tal como se muestra en la Tabla 5-29. Las vulnerabilidades están divididas para una mejor comprensión por tipos de activos, como por ejemplo hardware, software.

Tabla 5-29. Vulnerabilidades de ciberseguridad

VULNERABILIDADES (ISO 27005)
***** HARDWARE *****
Mantenimiento insuficiente / instalación defectuosa de medios de almacenamiento
Falta de esquemas de reemplazo periódicos
Susceptibilidad a la humedad, polvo, suciedad
Sensibilidad a la radiación electromagnética
Falta de control de cambio de configuración eficiente
Susceptibilidad a las variaciones de tensión
Susceptibilidad a las variaciones de temperatura
Almacenamiento no protegido
Falta de cuidados en la eliminación desechos
Copia incontrolada
No posee mecanismo de respaldo
No posee alta disponibilidad
Falta de mecanismo de redundancia
Mantenimiento insuficiente / instalación defectuosa
Falta de precaución en las conexiones físicas
Falta de esquema de ampliar capacidad
Falla de equipos dependientes
Fallo de los componentes
***** SOFTWARE *****
Pruebas de software inexistentes o insuficientes
Errores conocidos en el software

VULNERABILIDADES (ISO 27005)
No 'logout' al salir de la estación de trabajo
Eliminación o reutilización de medios de almacenamiento sin el correcto borrado
Falta de pista de auditoria
Asignación errónea de derechos de acceso
Software de amplia distribución (libre)
Aplicando programas de aplicación a los datos incorrectos en términos de tiempo
Interfaz de usuario de difícil comprensión
Falta de documentación técnica
Configuración incorrecta de parámetros
Fechas sin validación (incorrectas)
Falta de mecanismos de identificación y autenticación como la autenticación de usuarios
Tablas de contraseñas no protegidas
Mala gestión de contraseñas
Servicios innecesarios habilitados
Software inmaduro o nuevo
Especificaciones poco claras o incompletas para desarrolladores
Falta de control efectivo del cambio
Descarga incontrolada y uso de software
Falta de copias de respaldo
Falta de protección física del edificio, puertas y ventanas
No se producen informes de gestión
No posee un procedimiento de respaldo
Obsolescencia del software
Presenta errores lógicos el software
Inexistente entorno de pruebas
No cuenta con mecanismos contra ataques informáticos

Tarea 3: se establece la taxonomía de Amenazas en ciberseguridad, basada en el estándar ENISA 2016 (Marinos, 2016), tal como se muestra en la Tabla 5-30. Las amenazas están divididas para una mejor comprensión como, por ejemplo, ataque físico (deliberado /intencional) y daños involuntarios / pérdida de información o activos de TI.

Tabla 5-30. Amenazas de Ciberseguridad

AMENAZAS (ENISA)
*****ATAQUE FÍSICO (DELIBERADO / INTENCIONAL) *****
Fraude

AMENAZAS (ENISA)
Sabotaje
Vandalismo
Robo (dispositivos, medios de almacenamiento y documentos)
Fuga de información / intercambio
Acceso físico no autorizado / Entrada no autorizada a las instalaciones
Coerción, extorsión o corrupción
Daños de la guerra
Ataque terrorista
***** DAÑOS INVOLUNTARIOS / PÉRDIDA DE INFORMACIÓN O ACTIVOS DE TI *****
Fuga de información / intercambio debido a un error humano
Uso erróneo o administración de dispositivos y sistemas
Usando información de una fuente no confiable
Cambio involuntario de datos en un sistema de información
Diseño y planificación inadecuados o adaptación inadecuada
Daños causados por un tercero
Daños resultantes de las pruebas de penetración
Pérdida de información en la nube
Pérdida de (integridad de) información sensible
Pérdida de dispositivos, medios de almacenamiento y documentos
Destrucción de registros

El listado de las taxonomías de vulnerabilidades y amenazas de ciberseguridad son una muestra de la taxonomía general, el listado total se encuentra descrito en el Anexo II de esta tesis doctoral.

5.3.2.3 Actividad 2: Identificar y evaluar Activos

En esta actividad se ha realizado el proceso inicial, donde se ha determinado qué activos queremos proteger. Para ello, se ha realizado un análisis de los elementos que son más importantes para la organización de la plataforma Host – IESS.

A continuación, se muestran las tareas necesarias para esta actividad.

Tarea 1: los tipos de activos se toman de las taxonomías previamente establecidas en la Tabla 5-28. Los activos que la organización ha identificado se muestran en la columna “activo” (con su respectivo tipo) en la Tabla 5-32.

Tarea 2: se identifican las dimensiones de seguridad (confidencialidad, integridad, y disponibilidad) para los activos de ciberseguridad, y se mide el impacto de estas dimensiones en los activos de la organización, basados en el estándar ISO 27005, como se muestra en la Tabla 5-31.

Tabla 5-31. Valoración del impacto para un activo AVARCIBER

RANGO	Valor Superior	Valor Inferior
--------------	-----------------------	-----------------------

Alto	10	8
Medio	7	5
Bajo	4	2
Nulo	1	0

Para poder establecer la valoración, se deben considerar para cada dimensión los criterios de valoración descritos en la sección 4.2, Actividad 2 – Tarea 2 del capítulo 4 de la presente tesis doctoral, como se muestra en la Tabla 5-32.

Tarea 3: se calcula la criticidad del activo. Para calcular la criticidad del activo, se ha tomado el valor más alto de las dimensiones de seguridad de confidencialidad, integridad y disponibilidad.

El resultado de estas tres tareas se muestra en la Tabla 5-32.

Tabla 5-32. Dimensiones de seguridad de los Activos de la Plataforma HOST-IESS AVARCIBER

IDENTIFICACIÓN DE ACTIVOS										
#	Tipo de Activo	Activo	Confidencialidad		Integridad		Disponibilidad		Criticidad	
1	Hardware	Main-Frame Z10BC	7	Media	6	Media	10	Alta	10	Alta
2	Hardware	UNIDAD DE CARTUCHOS	7	Media	7	Media	6	Media	7	Media
3	Hardware	UNIDAD DE CARTUCHOS 1	5	Media	7	Media	6	Media	7	Media
4	Hardware	ALMACENAMIENTO	6	Media	7	Media	10	Alta	10	Alta
5	Hardware	SERVIDOR HMC	7	Media	6	Media	6	Media	7	Media
6	Hardware	AIRE DE PRECISION	6	Media	6	Media	9	Alta	9	Alta
7	Hardware	AIRE TIPO MOCHILA	5	Media	6	Media	3	Baja	6	Media
8	Hardware	UPS	7	Media	6	Media	8	Alta	8	Alta
9	Hardware	SERVIDOR UNIX	6	Media	7	Media	8	Alta	8	Alta
10	Hardware	SERVER VTAPE	5	Media	7	Media	2	Baja	7	Media
11	Hardware	SWITCH DE PASO	5	Media	7	Media	8	Alta	8	Alta
12	Software	Aplicativos alojados en el sistema HOST	6	Media	2	Baja	9	Alta	9	Alta

Tarea 4: La organización tendrá que determinar un valor (costo del activo) para los activos definidos.

Se determina el valor para cada activo de la organización, en función del precio de adquisición y el valor actual del mercado como se muestra en la Tabla 5-33.

Tabla 5-33. Costo del activo HOS - IESS AVARCIBER

IDENTIFICACIÓN DE ACTIVOS			
#	Tipo	Activo	Costo del Activo
1	Hardware	Main-Frame Z10BC	\$ 300.000,00
2	Hardware	UNIDAD DE CARTUCHOS	\$ 10.000,00

IDENTIFICACIÓN DE ACTIVOS			
3	Hardware	UNIDAD DE CARTUCHOS 1	\$ 10.000,00
4	Hardware	ALMACENAMIENTO	\$ 500.000,00
5	Hardware	SERVIDOR HMC	\$ 2.000,00
6	Hardware	AIRE DE PRESION	\$ 25.000,00
7	Hardware	AIRE TIPO MOCHILA	\$ 8.000,00
8	Hardware	UPS	\$ 30.000,00
9	Hardware	SERVIDOR UNIX	\$ 4.000,00
10	Hardware	SERVER VTAPE	\$ 2.000,00
11	Hardware	SWITCH DE PASO	\$ 1.000,00
12	Software	Aplicativos alojados en la plataforma HOST - IESS	\$ 100.000,00

5.3.2.4 Actividad 3: Evaluar el nivel de daño para las tuplas Vulnerabilidad – Activo (dimensión)

En esta actividad se ha determinado el daño de las vulnerabilidades en cada uno de los activos de la organización previamente identificados. La organización ha determinado el valor del daño de la vulnerabilidad en cada una de las dimensiones (disponibilidad, integridad y confidencialidad) del activo. La valoración del daño se ha definido según la importancia y repercusión que puede tener en la organización el daño irreparable del activo. Para la medición se ha tomado como referencia la Tabla 5-34.

Tabla 5-34. Valoración del daño de las vulnerabilidades AVARCIBER

RANGO	Valor Superior	Valor Inferior
Daño Extremo	10	10
Muy Alto	9	9
Alto	8	6
Medio	5	3
Bajo	2	1
Despreciable	0	0

A continuación, se muestran las tareas necesarias para esta actividad.

Tarea 1: se ha identificado / seleccionado para cada activo, las vulnerabilidades definidas en la taxonomía de la Actividad 1 – Tarea 2. Las tuplas Vulnerabilidad – Activo quedan definidas como se muestra en la Tabla 5-35.

Tabla 5-35. Tuplas Vulnerabilidad – Activo de la plataforma HOST -IESS

	VULNERABILIDADES	ACTIVOS
1	Susceptible a incendios y altas temperaturas	Main-Frame Z10BC
2	Ubicación en un área susceptible a inundaciones.	Main-Frame Z10BC

	VULNERABILIDADES	ACTIVOS
3	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	Main-Frame Z10BC
4	Falta de soporte preventivo y correctivo	Main-Frame Z10BC
5	Falta de capacitación en la administración del activo	Main-Frame Z10BC
6	Falta de garantía técnica de los equipos	Main-Frame Z10BC
7	Fallo de los componentes	Main-Frame Z10BC
8	Falta de soporte preventivo y correctivo	UNIDAD DE CARTUCHOS
9	Ubicación en un área susceptible a inundaciones.	UNIDAD DE CARTUCHOS
10	Susceptible a incendios y altas temperaturas	UNIDAD DE CARTUCHOS
11	Fallo de los componentes	UNIDAD DE CARTUCHOS
12	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	UNIDAD DE CARTUCHOS
13	Falta de capacitación en la administración del activo	UNIDAD DE CARTUCHOS
14	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	UNIDAD DE CARTUCHOS
15	Falta de planes de contingencia	UNIDAD DE CARTUCHOS
16	Falta de mantenimiento y/o actualizaciones	UNIDAD DE CARTUCHOS
17	Falta de precaución en las conexiones físicas	UNIDAD DE CARTUCHOS
18	No posee mecanismo de respaldo	UNIDAD DE CARTUCHOS
19	Falta de soporte preventivo y correctivo	UNIDAD DE CARTUCHOS 1
20	Ubicación en un área susceptible a inundaciones.	UNIDAD DE CARTUCHOS 1
21	Susceptible a incendios y altas temperaturas	UNIDAD DE CARTUCHOS 1
22	Fallo de los componentes	UNIDAD DE CARTUCHOS 1
23	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	UNIDAD DE CARTUCHOS 1
24	Falta de capacitación en la administración del activo	UNIDAD DE CARTUCHOS 1
25	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	UNIDAD DE CARTUCHOS 1
26	Falta de planes de contingencia	UNIDAD DE CARTUCHOS 1
27	Falta de mantenimiento y/o actualizaciones	UNIDAD DE CARTUCHOS 1
28	Falta de precaución en las conexiones físicas	UNIDAD DE CARTUCHOS 1
29	No posee mecanismo de respaldo	UNIDAD DE CARTUCHOS 1
30	Falta de soporte preventivo y correctivo	ALMACENAMIENTO
31	Ubicación en un área susceptible a inundaciones.	ALMACENAMIENTO
32	Susceptible a incendios y altas temperaturas	ALMACENAMIENTO
33	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	ALMACENAMIENTO

	VULNERABILIDADES	ACTIVOS
34	Falta de capacitación en la administración del activo	ALMACENAMIENTO
35	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	ALMACENAMIENTO
36	Falta de planes de contingencia	ALMACENAMIENTO
37	Fallo de los componentes	ALMACENAMIENTO
38	Falta de mantenimiento y/o actualizaciones	ALMACENAMIENTO
39	Falta de precaución en las conexiones físicas	ALMACENAMIENTO
40	Falta de soporte preventivo y correctivo	SERVIDOR HMC
41	Ubicación en un área susceptible a inundaciones.	SERVIDOR HMC
42	Susceptible a incendios y altas temperaturas	SERVIDOR HMC
43	Fallo de los componentes	SERVIDOR HMC
44	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	SERVIDOR HMC
45	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	SERVIDOR HMC
46	Falta de precaución en las conexiones físicas	SERVIDOR HMC
47	Fallo de los componentes	AIRE DE PRESICION
48	Ubicación en un área susceptible a inundaciones.	AIRE DE PRESICION
49	Susceptible a incendios y altas temperaturas	AIRE DE PRESICION
50	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	AIRE DE PRESICION
51	Falta de capacitación en la administración del activo	AIRE DE PRESICION
52	Falta de precaución en las conexiones físicas	AIRE DE PRESICION
53	Fallo de los componentes	AIRE TIPO MOCHILA
54	Ubicación en un área susceptible a inundaciones.	AIRE TIPO MOCHILA
55	Susceptible a incendios y altas temperaturas	AIRE TIPO MOCHILA
56	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	AIRE TIPO MOCHILA
57	Falta de mantenimiento y/o actualizaciones	AIRE TIPO MOCHILA
58	Falta de precaución en las conexiones físicas	AIRE TIPO MOCHILA
59	Falta de soporte preventivo y correctivo	UPS
60	Ubicación en un área susceptible a inundaciones.	UPS
61	Susceptible a incendios y altas temperaturas	UPS
62	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	UPS
63	Falta de capacitación en la administración del activo	UPS

	VULNERABILIDADES	ACTIVOS
64	Falta de mantenimiento y/o actualizaciones	UPS
65	Falta de precaución en las conexiones físicas	UPS
66	Falta de soporte preventivo y correctivo	SERVIDOR UNIX
67	Ubicación en un área susceptible a inundaciones.	SERVIDOR UNIX
68	Susceptible a incendios y altas temperaturas	SERVIDOR UNIX
69	Fallo de los componentes	SERVIDOR UNIX
70	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	SERVIDOR UNIX
71	Falta de capacitación en la administración del activo	SERVIDOR UNIX
72	Falta de planes de contingencia	SERVIDOR UNIX
73	Mala gestión de contraseñas	SERVIDOR UNIX
74	Falta de mantenimiento y/o actualizaciones	SERVIDOR UNIX
75	Falta de precaución en las conexiones físicas	SERVIDOR UNIX
76	Falta de política formal de cambio de credenciales	SERVIDOR UNIX
77	Falta de soporte preventivo y correctivo	SERVER VTAPE
78	Ubicación en un área susceptible a inundaciones.	SERVER VTAPE
79	Susceptible a incendios y altas temperaturas	SERVER VTAPE
80	Fallo de los componentes	SERVER VTAPE
81	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	SERVER VTAPE
82	Falta de capacitación en la administración del activo	SERVER VTAPE
83	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	SERVER VTAPE
84	Falta de planes de contingencia	SERVER VTAPE
85	Mala gestión de contraseñas	SERVER VTAPE
86	Falta de mantenimiento y/o actualizaciones	SERVER VTAPE
87	Falta de precaución en las conexiones físicas	SERVER VTAPE
88	Falta de soporte preventivo y correctivo	SWITCH DE PASO
89	Ubicación en un área susceptible a inundaciones.	SWITCH DE PASO
90	Susceptible a incendios y altas temperaturas	SWITCH DE PASO
91	Fallo de los componentes	SWITCH DE PASO
92	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	SWITCH DE PASO
93	Falta de capacitación en la administración del activo	SWITCH DE PASO
94	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	SWITCH DE PASO

	<i>VULNERABILIDADES</i>	<i>ACTIVOS</i>
95	Falta de precaución en las conexiones físicas	SWITCH DE PASO
96	Inexistente ambiente de pruebas	Aplicativos alojados en el sistema HOST - IESS
97	Falta de capacitación en la administración del activo	Aplicativos alojados en el sistema HOST - IESS
98	Mala gestión de contraseñas	Aplicativos alojados en el sistema HOST - IESS
99	Errores conocidos en el software.	Aplicativos alojados en el sistema HOST - IESS

Tarea 2: a partir de las duplas de Activo – Vulnerabilidad de ciberseguridad se ha determinado el daño de las vulnerabilidades en cada uno de los activos, en base a los valores previamente definidos en la Tabla 5-34, para cada una de las dimensiones de seguridad (Confidencialidad, Integridad, Disponibilidad) del activo. El valor del daño de la vulnerabilidad para la dimensión de criticidad se toma de la Actividad 2 – Tarea 2 que fue previamente calculado.

Tarea 3: se han sumado los valores de los daños de la vulnerabilidad de cada tupla Vulnerabilidad – Activo.

Tarea 4: se ha calculado el valor promedio del valor del daño de la vulnerabilidad de cada tupla Vulnerabilidad – Activo.

Tarea 5: se han repetido las tareas 2, 3 y 4 para cada una de las tuplas Vulnerabilidad – Activo.

Tarea 6: se ha asignado un valor monetario a cada una de las vulnerabilidades que están afectando a los activos de la organización (tupla vulnerabilidad – activo), como se muestra en la columna Costo del Daño en la Tabla 5-36.

Tabla 5-36. Vulnerabilidades con activos, valor y costo del daño HOST – IESS AVARCIBER

	VULNERABILIDADES	ACTIVOS	COSTO DEL ACTIVO	Dimensiones				Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
				<i>Daño Disponibilidad</i>	<i>Daño Integridad</i>	<i>Daño Confidencialidad</i>	<i>Daño Criticidad</i>		
1	Susceptible a incendios y altas temperaturas	Main-Frame Z10BC	300.000,00	10	5	2	10	6,75	300.000,00
2	Ubicación en un área susceptible a inundaciones.	Main-Frame Z10BC		10	5	2	10	6,75	300.000,00
3	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	Main-Frame Z10BC		10	10	2	10	8,00	300.000,00
4	Falta de soporte preventivo y correctivo	Main-Frame Z10BC		5	5	5	10	6,25	120.000,00
5	Falta de capacitación en la administración del activo	Main-Frame Z10BC		5	5	5	10	6,25	150.000,00
6	Falta de garantía técnica de los equipos	Main-Frame Z10BC		10	10	5	10	8,75	150.000,00
7	Fallo de los componentes	Main-Frame Z10BC		10	5	5	10	7,50	90.000,00
8	Falta de soporte preventivo y correctivo	UNIDAD DE CARTUCHOS	10.000,00	5	5	2	7	4,75	5.000,00
9	Ubicación en un área susceptible a inundaciones.	UNIDAD DE CARTUCHOS		5	5	2	7	4,75	10.000,00
10	Susceptible a incendios y altas temperaturas	UNIDAD DE CARTUCHOS		10	10	1	7	7,00	10.000,00
11	Fallo de los componentes	UNIDAD DE CARTUCHOS		10	10	2	7	7,25	5.000,00
12	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	UNIDAD DE CARTUCHOS		10	10	1	7	7,00	10.000,00

13	Falta de capacitación en la administración del activo	UNIDAD DE CARTUCHOS		5	5	2	7	4,75	3.000,00
14	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	UNIDAD DE CARTUCHOS		10	10	5	7	8,00	10.000,00
15	Falta de planes de contingencia	UNIDAD DE CARTUCHOS		10	10	5	7	8,00	10.000,00
16	Falta de mantenimiento y/o actualizaciones	UNIDAD DE CARTUCHOS		10	10	5	7	8,00	10.000,00
17	Falta de precaución en las conexiones físicas	UNIDAD DE CARTUCHOS		10	10	2	7	7,25	4.000,00
18	No posee mecanismo de respaldo	UNIDAD DE CARTUCHOS		10	10	2	7	7,25	10.000,00
19	Falta de soporte preventivo y correctivo	UNIDAD DE CARTUCHOS 1	10.000,00	5	5	2	7	4,75	5.000,00
20	Ubicación en un área susceptible a inundaciones.	UNIDAD DE CARTUCHOS 1		5	5	2	7	4,75	10.000,00
21	Susceptible a incendios y altas temperaturas	UNIDAD DE CARTUCHOS 1		10	10	1	7	7,00	10.000,00
22	Fallo de los componentes	UNIDAD DE CARTUCHOS 1		10	10	2	7	7,25	5.000,00
23	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	UNIDAD DE CARTUCHOS 1		10	10	1	7	7,00	10.000,00
24	Falta de capacitación en la administración del activo	UNIDAD DE CARTUCHOS 1		5	5	2	7	4,75	3.000,00
25	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	UNIDAD DE CARTUCHOS 1		10	10	5	7	8,00	10.000,00
26	Falta de planes de contingencia	UNIDAD DE CARTUCHOS 1		10	10	5	7	8,00	10.000,00
27	Falta de mantenimiento y/o actualizaciones	UNIDAD DE CARTUCHOS 1		10	10	5	7	8,00	10.000,00
28	Falta de precaución en las conexiones físicas	UNIDAD DE CARTUCHOS 1		10	10	2	7	7,25	4.000,00
29	No posee mecanismo de respaldo	UNIDAD DE CARTUCHOS 1		10	10	2	7	7,25	10.000,00
30	Falta de soporte preventivo y correctivo	ALMACENAMIENTO	500.000,00	10	10	2	10	8,00	250.000,00

31	Ubicación en un área susceptible a inundaciones.	ALMACENAMIENTO		10	10	2	10	8,00	500.000,00
32	Susceptible a incendios y altas temperaturas	ALMACENAMIENTO		10	10	2	10	8,00	500.000,00
33	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	ALMACENAMIENTO		10	10	1	10	7,75	500.000,00
34	Falta de capacitación en la administración del activo	ALMACENAMIENTO		10	5	5	10	7,50	500.000,00
35	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	ALMACENAMIENTO		10	10	2	10	8,00	500.000,00
36	Falta de planes de contingencia	ALMACENAMIENTO		10	5	5	10	7,50	500.000,00
37	Fallo de los componentes	ALMACENAMIENTO		10	10	5	10	8,75	200.000,00
38	Falta de mantenimiento y/o actualizaciones	ALMACENAMIENTO		10	10	5	10	8,75	500.000,00
39	Falta de precaución en las conexiones físicas	ALMACENAMIENTO		10	5	2	10	6,75	200.000,00
40	Falta de soporte preventivo y correctivo	SERVIDOR HMC	2.000,00	3	3	1	7	3,50	1.000,00
41	Ubicación en un área susceptible a inundaciones.	SERVIDOR HMC		10	5	1	7	5,75	2.000,00
42	Susceptible a incendios y altas temperaturas	SERVIDOR HMC		10	10	1	7	7,00	2.000,00
43	Fallo de los componentes	SERVIDOR HMC		10	10	1	7	7,00	800,00
44	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	SERVIDOR HMC		10	10	1	7	7,00	2.000,00
45	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	SERVIDOR HMC		10	10	5	7	8,00	2.000,00
46	Falta de precaución en las conexiones físicas	SERVIDOR HMC		5	5	2	7	4,75	800,00
47	Fallo de los componentes	AIRE DE PRESION	25.000,00	10	10	2	9	7,75	12.500,00
48	Ubicación en un área susceptible a inundaciones.	AIRE DE PRESION		10	10	2	9	7,75	25.000,00

49	Susceptible a incendios y altas temperaturas	AIRE DE PRESICION		10	10	2	9	7,75	25.000,00
50	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	AIRE DE PRESICION		10	10	1	9	7,50	25.000,00
51	Falta de capacitación en la administración del activo	AIRE DE PRESICION		5	5	2	9	5,25	10.000,00
52	Falta de precaución en las conexiones físicas	AIRE DE PRESICION		10	5	2	9	6,50	10.000,00
53	Fallo de los componentes	AIRE TIPO MOCHILA	8.000,00	10	10	2	6	7,00	4.000,00
54	Ubicación en un área susceptible a inundaciones.	AIRE TIPO MOCHILA		10	10	2	6	7,00	8.000,00
55	Susceptible a incendios y altas temperaturas	AIRE TIPO MOCHILA		10	10	2	6	7,00	8.000,00
56	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	AIRE TIPO MOCHILA		10	10	1	6	6,75	8.000,00
57	Falta de mantenimiento y/o actualizaciones	AIRE TIPO MOCHILA		10	5	2	6	5,75	4.000,00
58	Falta de precaución en las conexiones físicas	AIRE TIPO MOCHILA		10	5	2	6	5,75	3.200,00
59	Falta de soporte preventivo y correctivo	UPS	30.000,00	10	10	2	8	7,50	15.000,00
60	Ubicación en un área susceptible a inundaciones.	UPS		10	5	2	8	6,25	30.000,00
61	Susceptible a incendios y altas temperaturas	UPS		10	10	2	8	7,50	30.000,00
62	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	UPS		10	10	1	8	7,25	30.000,00
63	Falta de capacitación en la administración del activo	UPS		10	10	2	8	7,50	12.000,00
64	Falta de mantenimiento y/o actualizaciones	UPS		10	10	2	8	7,50	15.000,00
65	Falta de precaución en las conexiones físicas	UPS		10	5	2	8	6,25	12.000,00
66	Falta de soporte preventivo y correctivo	SERVIDOR UNIX	4.000,00	10	10	2	8	7,50	2.000,00

67	Ubicación en un área susceptible a inundaciones.	SERVIDOR UNIX		10	10	2	8	7,50	4.000,00
68	Susceptible a incendios y altas temperaturas	SERVIDOR UNIX		10	10	2	8	7,50	4.000,00
69	Fallo de los componentes	SERVIDOR UNIX		10	10	1	8	7,25	2.000,00
70	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	SERVIDOR UNIX		10	10	1	8	7,25	4.000,00
71	Falta de capacitación en la administración del activo	SERVIDOR UNIX		10	5	2	8	6,25	2.000,00
72	Falta de planes de contingencia	SERVIDOR UNIX		5	5	2	8	5,00	2.000,00
73	Mala gestión de contraseñas	SERVIDOR UNIX		10	5	1	8	6,00	2.000,00
74	Falta de mantenimiento y/o actualizaciones	SERVIDOR UNIX		10	10	2	8	7,50	2.000,00
75	Falta de precaución en las conexiones físicas	SERVIDOR UNIX		10	5	2	8	6,25	1.600,00
76	Falta de política formal de cambio de credenciales	SERVIDOR UNIX		10	5	2	8	6,25	3.000,00
77	Falta de soporte preventivo y correctivo	SERVER VTAPE	2.000,00	10	5	2	7	6,00	1.000,00
78	Ubicación en un área susceptible a inundaciones.	SERVER VTAPE		10	10	2	7	7,25	2.000,00
79	Susceptible a incendios y altas temperaturas	SERVER VTAPE		10	10	2	7	7,25	2.000,00
80	Fallo de los componentes	SERVER VTAPE		10	10	2	7	7,25	1.000,00
81	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	SERVER VTAPE		10	10	1	7	7,00	2.000,00
82	Falta de capacitación en la administración del activo	SERVER VTAPE		10	5	2	7	6,00	2.000,00
83	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	SERVER VTAPE		10	10	2	7	7,25	2.000,00
84	Falta de planes de contingencia	SERVER VTAPE		5	5	2	7	4,75	1.000,00
85	Mala gestión de contraseñas	SERVER VTAPE		10	5	2	7	6,00	1.000,00

86	Falta de mantenimiento y/o actualizaciones	SERVER VTAPE		10	10	2	7	7,25	1.000,00
87	Falta de precaución en las conexiones físicas	SERVER VTAPE		10	5	2	7	6,00	1.000,00
88	Falta de soporte preventivo y correctivo	SWITCH DE PASO	1.000,00	10	10	2	8	7,50	500,00
89	Ubicación en un área susceptible a inundaciones.	SWITCH DE PASO		10	10	2	8	7,50	1.000,00
90	Susceptible a incendios y altas temperaturas	SWITCH DE PASO		10	10	2	8	7,50	1.000,00
91	Fallo de los componentes	SWITCH DE PASO		10	10	2	8	7,50	500,00
92	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	SWITCH DE PASO		10	10	1	8	7,25	1.000,00
93	Falta de capacitación en la administración del activo	SWITCH DE PASO		10	5	2	8	6,25	200,00
94	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	SWITCH DE PASO		10	10	2	8	7,50	1.000,00
95	Falta de precaución en las conexiones físicas	SWITCH DE PASO		10	5	2	8	6,25	1.000,00
96	Inexistente ambiente de pruebas	Aplicativos alojados en el sistema HOST	10.000,00	5	5	2	9	5,25	200,00
97	Falta de capacitación en la administración del activo	Aplicativos alojados en el sistema HOST		10	10	2	9	7,75	2.200,00
98	Mala gestión de contraseñas	Aplicativos alojados en el sistema HOST		5	10	10	9	8,50	1.000,00
99	Errores conocidos en el software.	Aplicativos alojados en el sistema HOST		3	10	5	9	6,75	200,00

Actividad 4: Identificación de Amenazas de ciberseguridad

A partir de la medición del daño de las vulnerabilidades y su costo, se ha procedido a identificar las amenazas de ciberseguridad que podrían materializar las vulnerabilidades existentes en los activos y establecer las duplas Amenazas – Vulnerabilidades y las tripletas Amenazas-Vulnerabilidades – Activos. Posteriormente, se ha recuperado de la actividad anterior, los valores calculados de: valor del daño y costo del daño de todas las vulnerabilidades identificadas y se les asigna a las tripletas Amenazas – Vulnerabilidades – Activos.

A continuación, se muestran las tareas necesarias para esta actividad.

Tarea 1: las amenazas de ciberseguridad se han tomado de la taxonomía previamente establecida en la Actividad 1 – Tarea 3.

Tarea 2: se ha determinado qué amenaza puede materializar cada una de las vulnerabilidades de los activos de ciberseguridad, quedando establecida la dupla Amenaza – Vulnerabilidad y la Tripletas Amenaza – Vulnerabilidad – Activo, por la asociación de relaciones previamente definidas, como se muestra en la Tabla 5-37.

Tarea 3: se ha recuperado de la Actividad2 – Tarea 4 el costo del activo, así como de la actividad anterior los valores calculados de: valor del daño de la vulnerabilidad y costo del daño de la vulnerabilidad, de todas las vulnerabilidades identificadas, y se asignaron a las tripletas Amenazas – Vulnerabilidades – Activos, como se muestra en la Tabla 5-37.

Tabla 5-37. Tripletas Amenazas – Vulnerabilidades – Activos con los valores y costo del daño de las vulnerabilidades para HOST - IESS AVARCIBER

	AMENAZAS	VULNERABILIDAD	ACTIVOS	COSTO DEL ACTIVO	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
1	Fuego	Susceptible a incendios y altas temperaturas	Main-Frame Z10BC	300.000,00	6,75	300.000,00
2	Agua	Ubicación en un área susceptible a inundaciones.	Main-Frame Z10BC		6,75	300.000,00
3	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	Main-Frame Z10BC		8,00	300.000,00
4	Fallo o interrupción del suministro principal	Falta de soporte preventivo y correctivo	Main-Frame Z10BC		6,25	120.000,00
5	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Main-Frame Z10BC		6,25	150.000,00
6	Fallo de dispositivos o sistemas	Falta de garantía técnica de los equipos	Main-Frame Z10BC		8,75	150.000,00
7	Fallo de dispositivos o sistemas	Fallo de los componentes	Main-Frame Z10BC		7,50	90.000,00
8	Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	UNIDAD DE CARTUCHOS	10.000,00	4,75	5.000,00
9	Agua	Ubicación en un área susceptible a inundaciones.	UNIDAD DE CARTUCHOS		4,75	10.000,00
10	Fuego	Susceptible a incendios y altas temperaturas	UNIDAD DE CARTUCHOS		7,00	10.000,00
11	Fallo o interrupción del suministro principal	Fallo de los componentes	UNIDAD DE CARTUCHOS		7,25	5.000,00
12	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	UNIDAD DE CARTUCHOS		7,00	10.000,00
13	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	UNIDAD DE CARTUCHOS		4,75	3.000,00

14	Robo (dispositivos, medios de almacenamiento y documentos)	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	UNIDAD DE CARTUCHOS		8,00	10.000,00
15	Fallo de dispositivos o sistemas	Falta de planes de contingencia	UNIDAD DE CARTUCHOS		8,00	10.000,00
16	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	UNIDAD DE CARTUCHOS		8,00	10.000,00
17	Pérdida de recursos	Falta de precaución en las conexiones físicas	UNIDAD DE CARTUCHOS		7,25	4.000,00
18	Diseño y planificación inadecuados o adaptación inadecuada	No posee mecanismo de respaldo	UNIDAD DE CARTUCHOS		7,25	10.000,00
19	Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	UNIDAD DE CARTUCHOS 1	10.000,00	4,75	5.000,00
20	Agua	Ubicación en un área susceptible a inundaciones.	UNIDAD DE CARTUCHOS 1		4,75	10.000,00
21	Fuego	Susceptible a incendios y altas temperaturas	UNIDAD DE CARTUCHOS 1		7,00	10.000,00
22	Fallo o interrupción del suministro principal	Fallo de los componentes	UNIDAD DE CARTUCHOS 1		7,25	5.000,00
23	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	UNIDAD DE CARTUCHOS 1		7,00	10.000,00
24	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	UNIDAD DE CARTUCHOS 1		4,75	3.000,00
25	Robo (dispositivos, medios de almacenamiento y documentos)	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	UNIDAD DE CARTUCHOS 1		8,00	10.000,00
26	Fallo de dispositivos o sistemas	Falta de planes de contingencia	UNIDAD DE CARTUCHOS 1		8,00	10.000,00
27	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	UNIDAD DE CARTUCHOS 1		8,00	10.000,00
28	Pérdida de recursos	Falta de precaución en las conexiones físicas	UNIDAD DE CARTUCHOS 1		7,25	4.000,00
29	Diseño y planificación inadecuados o adaptación inadecuada	No posee mecanismo de respaldo	UNIDAD DE CARTUCHOS 1		7,25	10.000,00

30	Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	ALMACENAMIENTO	500.000,00	8,00	250.000,00
31	Agua	Ubicación en un área susceptible a inundaciones.	ALMACENAMIENTO		8,00	500.000,00
32	Fuego	Susceptible a incendios y altas temperaturas	ALMACENAMIENTO		8,00	500.000,00
33	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	ALMACENAMIENTO		7,75	500.000,00
34	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	ALMACENAMIENTO		7,50	500.000,00
35	Robo (dispositivos, medios de almacenamiento y documentos)	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	ALMACENAMIENTO		8,00	500.000,00
36	Fallo de dispositivos o sistemas	Falta de planes de contingencia	ALMACENAMIENTO		7,50	500.000,00
37	Fallo de dispositivos o sistemas	Fallo de los componentes	ALMACENAMIENTO		8,75	200.000,00
38	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	ALMACENAMIENTO		8,75	500.000,00
39	Pérdida de recursos	Falta de precaución en las conexiones físicas	ALMACENAMIENTO		6,75	200.000,00
40	Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	SERVIDOR HMC	2.000,00	3,50	1.000,00
41	Agua	Ubicación en un área susceptible a inundaciones.	SERVIDOR HMC		5,75	2.000,00
42	Fuego	Susceptible a incendios y altas temperaturas	SERVIDOR HMC		7,00	2.000,00
43	Fallo o interrupción del suministro principal	Fallo de los componentes	SERVIDOR HMC		7,00	800,00
44	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	SERVIDOR HMC		7,00	2.000,00

45	Robo (dispositivos, medios de almacenamiento y documentos)	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	SERVIDOR HMC		8,00	2.000,00
46	Pérdida de recursos	Falta de precaución en las conexiones físicas	SERVIDOR HMC		4,75	800,00
47	Condiciones climáticas desfavorables	Fallo de los componentes	AIRE DE PRESICION	25.000,00	7,75	12.500,00
48	Agua	Ubicación en un área susceptible a inundaciones.	AIRE DE PRESICION		7,75	25.000,00
49	Fuego	Susceptible a incendios y altas temperaturas	AIRE DE PRESICION		7,75	25.000,00
50	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	AIRE DE PRESICION		7,50	25.000,00
51	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	AIRE DE PRESICION		5,25	10.000,00
52	Pérdida de recursos	Falta de precaución en las conexiones físicas	AIRE DE PRESICION		6,50	10.000,00
53	Condiciones climáticas desfavorables	Fallo de los componentes	AIRE TIPO MOCHILA	8.000,00	7,00	4.000,00
54	Agua	Ubicación en un área susceptible a inundaciones.	AIRE TIPO MOCHILA		7,00	8.000,00
55	Fuego	Susceptible a incendios y altas temperaturas	AIRE TIPO MOCHILA		7,00	8.000,00
56	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	AIRE TIPO MOCHILA		6,75	8.000,00
57	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	AIRE TIPO MOCHILA		5,75	4.000,00
58	Pérdida de recursos	Falta de precaución en las conexiones físicas	AIRE TIPO MOCHILA		5,75	3.200,00
59	Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	UPS	30.000,00	7,50	15.000,00
60	Agua	Ubicación en un área susceptible a inundaciones.	UPS		6,25	30.000,00
61	Fuego	Susceptible a incendios y altas temperaturas	UPS		7,50	30.000,00

62	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	UPS		7,25	30.000,00
63	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	UPS		7,50	12.000,00
64	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	UPS		7,50	15.000,00
65	Pérdida de recursos	Falta de precaución en las conexiones físicas	UPS		6,25	12.000,00
66	Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	SERVIDOR UNIX	4.000,00	7,50	2.000,00
67	Agua	Ubicación en un área susceptible a inundaciones.	SERVIDOR UNIX		7,50	4.000,00
68	Fuego	Susceptible a incendios y altas temperaturas	SERVIDOR UNIX		7,50	4.000,00
69	Fallo o interrupción del suministro principal	Fallo de los componentes	SERVIDOR UNIX		7,25	2.000,00
70	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	SERVIDOR UNIX		7,25	4.000,00
71	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	SERVIDOR UNIX		6,25	2.000,00
72	Fallo de dispositivos o sistemas	Falta de planes de contingencia	SERVIDOR UNIX		5,00	2.000,00
73	Actividades no autorizadas	Mala gestión de contraseñas	SERVIDOR UNIX		6,00	2.000,00
74	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	SERVIDOR UNIX		7,50	2.000,00
75	Pérdida de recursos	Falta de precaución en las conexiones físicas	SERVIDOR UNIX		6,25	1.600,00
76	Actividades no autorizadas	Falta de política formal de cambio de credenciales	SERVIDOR UNIX		6,25	3.000,00
77	Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	SERVER VTAPE	2.000,00	6,00	1.000,00

78	Agua	Ubicación en un área susceptible a inundaciones.	SERVER VTAPE		7,25	2.000,00
79	Fuego	Susceptible a incendios y altas temperaturas	SERVER VTAPE		7,25	2.000,00
80	Fallo o interrupción del suministro principal	Fallo de los componentes	SERVER VTAPE		7,25	1.000,00
81	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	SERVER VTAPE		7,00	2.000,00
82	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	SERVER VTAPE		6,00	2.000,00
83	Robo (dispositivos, medios de almacenamiento y documentos)	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	SERVER VTAPE		7,25	2.000,00
84	Fallo de dispositivos o sistemas	Falta de planes de contingencia	SERVER VTAPE		4,75	1.000,00
85	Actividades no autorizadas	Mala gestión de contraseñas	SERVER VTAPE		6,00	1.000,00
86	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	SERVER VTAPE		7,25	1.000,00
87	Pérdida de recursos	Falta de precaución en las conexiones físicas	SERVER VTAPE		6,00	1.000,00
88	Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	SWITCH DE PASO	1.000,00	7,50	500,00
89	Agua	Ubicación en un área susceptible a inundaciones.	SWITCH DE PASO		7,50	1.000,00
90	Fuego	Susceptible a incendios y altas temperaturas	SWITCH DE PASO		7,50	1.000,00
91	Fallo o interrupción del suministro principal	Fallo de los componentes	SWITCH DE PASO		7,50	500,00
92	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	SWITCH DE PASO		7,25	1.000,00
93	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	SWITCH DE PASO		6,25	200,00

94	Robo (dispositivos, medios de almacenamiento y documentos)	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	SWITCH DE PASO		7,50	1.000,00
95	Pérdida de recursos	Falta de precaución en las conexiones físicas	SWITCH DE PASO		6,25	1.000,00
96	Fallo de software /aplicaciones o servicio	Inexistente ambiente de pruebas	Aplicativos alojados en el sistema HOST	10.000,00	5,25	200,00
97	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Aplicativos alojados en el sistema HOST		7,75	2.200,00
98	Actividades no autorizadas	Mala gestión de contraseñas	Aplicativos alojados en el sistema HOST		8,50	1.000,00
99	Fallo de software /aplicaciones o servicio	Errores conocidos en el software.	Aplicativos alojados en el sistema HOST		6,75	200,00

Tarea 4: las amenazas y vulnerabilidades se han agrupado en pares amenaza – vulnerabilidad. Se calcula el valor del daño promedio de la vulnerabilidad, mediante el promedio de los valores del daño de las vulnerabilidades que están relacionadas con la amenaza en cuestión. De igual forma, se calcula el costo del daño total de la vulnerabilidad como la suma de los valores del coste del daño de las vulnerabilidades relacionadas con dicha amenaza. La Tabla 5-38 muestra dichos valores.

Tabla 5-38. Duplas Amenazas – Vulnerabilidades con los valores y costo del daño de las vulnerabilidades AVARCIBER

<i>AMENAZA</i>	<i>VULNERABILIDAD</i>	<i>Valor del Daño Promedio de la Vulnerabilidad</i>	<i>Costo del Daño Total de la Vulnerabilidad</i>
Actividades no autorizadas	Falta de política formal de cambio de credenciales	6,25	\$ 3.000,00
Actividades no autorizadas	Mala gestión de contraseñas	6,83	\$ 4.000,00
Actividades no autorizadas	Mala gestión de contraseñas	6,83	\$ 4.000,00
Agua	Ubicación en un área susceptible a inundaciones.	6,66	\$ 892.000,00
Condiciones climáticas desfavorables	Fallo de los componentes	7,38	\$ 16.500,00
Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	6,19	\$ 279.500,00
Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	7,25	\$ 892.000,00
Diseño y planificación inadecuados o adaptación inadecuada	No posee mecanismo de respaldo	7,25	\$ 20.000,00
Fallo de dispositivos o sistemas	Fallo de los componentes	8,13	\$ 290.000,00
Fallo de dispositivos o sistemas	Falta de garantía técnica de los equipos	8,75	\$ 150.000,00
Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	7,54	\$ 542.000,00
Fallo de dispositivos o sistemas	Falta de planes de contingencia	6,65	\$ 523.000,00
Fallo de software /aplicaciones o servicio	Errores conocidos en el software.	6,63	\$ 200,00
Fallo de software /aplicaciones o servicio	Inexistente ambiente de pruebas	5,25	\$ 200,00
Fallo o interrupción del suministro principal	Fallo de los componentes	7,25	\$ 14.300,00
Fallo o interrupción del suministro principal	Falta de soporte preventivo y correctivo	6,25	\$ 120.000,00
Fuego	Susceptible a incendios y altas temperaturas	7,30	\$ 892.000,00
Pérdida de recursos	Falta de precaución en las conexiones físicas	6,30	\$ 237.600,00

Robo (dispositivos, medios de almacenamiento y documentos)	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	7,79	\$ 525.000,00
Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	6,23	\$ 684.400,00

Tarea 5: las amenazas se han agrupado, y se calcula el valor y costo del daño de la amenaza. El valor del daño de cada amenaza se calcula con el promedio de los valores del daño de las vulnerabilidades que están relacionadas con la amenaza en cuestión. Y para el costo del daño de la amenaza se suman los valores del costo del daño de las vulnerabilidades relacionadas con dicha amenaza, como se muestra en la Tabla 5-39.

Tabla 5-39. Amenazas con totales del valor del daño y costo del daño HOST – IESS AVARCIBER

<i>AMENAZA</i>	<i>VALOR DEL DAÑO DE LA AMENAZA</i>	<i>COSTO DEL DAÑO DE LA AMENAZA</i>
Actividades no autorizadas	6,64	\$ 11.000,00
Agua	6,66	\$ 892.000,00
Condiciones climáticas desfavorables	6,78	\$ 296.000,00
Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	7,25	\$ 892.000,00
Diseño y planificación inadecuados o adaptación inadecuada	7,25	\$ 20.000,00
Fallo de dispositivos o sistemas	7,77	\$ 1.505.000,00
Fallo de software /aplicaciones o servicio	6,00	\$ 400,00
Fallo o interrupción del suministro principal	6,75	\$ 134.300,00
Fuego	7,30	\$ 892.000,00
Pérdida de recursos	6,30	\$ 237.600,00
Robo (dispositivos, medios de almacenamiento y documentos)	7,79	\$ 525.000,00
Uso erróneo o administración de dispositivos y sistemas	6,23	\$ 684.400,00

5.3.2.5 Actividad 5: Medición del Riesgo

En esta actividad se ha calculado el riesgo de cada amenaza que materializaran las vulnerabilidades identificadas a los activos de ciberseguridad de la plataforma HOST-IESS. Para ello, la organización debe establecer previamente la probabilidad de ocurrencia de las amenazas.

A continuación, se muestran las tareas necesarias para esta actividad.

Tarea 1: se ha recuperado el valor del Daño de la Amenaza (impacto) y el valor del costo del daño de cada amenaza, valores que fue calculado previamente en la actividad anterior Actividad 4 - Tarea 5. El valor del daño de la amenaza debe ser redondeado.

Tarea 2: se ha asignado la probabilidad de ocurrencia de la amenaza. Para esto, se toman como referencia casos similares que han ocurrido en la empresa y la experiencia del personal a cargo, tomando los criterios definidos en la Tabla 5-40.

Tabla 5-40. Probabilidad de ocurrencia de la amenaza AVARCIBER

RANGO	PROBABILIDAD	DESCRIPCION	FRECUENCIA
MA (Muy Alto)	100 %	muy frecuente	a diario
A (Alto)	10 %	frecuente	mensualmente
M (Medio)	1 %	normal	una vez al año
B (Bajo)	1/10 %	poco frecuente	cada varios años
MB (Muy Bajo)	1/100 %	muy poco frecuente	siglos

Para definir la probabilidad de ocurrencia de las amenazas, se ha tomado como referencia la norma ISO 27005 (ISO/IEC 27000, 2018), y agregando dos nuevos rangos: "muy alto" y "muy bajo" para identificar probabilidades muy inminentes y también insignificantes de ocurrencia.

Tarea3: se ha realizado el cálculo del riesgo de ciberseguridad ($\text{Riesgo} = \text{Impacto} \times \text{Frecuencia}$), según los criterios definidos en la Tabla 5-41.

El riesgo asociado es el impacto potencial (I, impacto) multiplicado por la probabilidad de ocurrencia de la amenaza (F, frecuencia). El impacto potencial es el valor del daño de la amenaza (valor redondeado). La frecuencia se ha tomado de la Tabla 5-40, según el criterio experto del personal de la organización. La valoración del riesgo se ha hecho en base a los criterios definidos en la Tabla 5-41.

Tabla 5-41. Valoración del Riesgo HOST – IESS AVARCIBER

Tabla de Valoración del Riesgo														
I	F	R	I	F	R	I	F	R	I	F	R	I	F	R
0	MB	0	0	B	0	0	M	0	0	A	0	0	MA	0
1	MB	0	1	B	0	1	M	1	1	A	0	1	MA	1
2	MB	0	2	B	0	2	M	1	2	A	0	2	MA	4
3	MB	0	3	B	0	3	M	1	3	A	4	3	MA	4
4	MB	0	4	B	5	4	M	5	4	A	5	4	MA	8
5	MB	0	5	B	5	5	M	5	5	A	5	5	MA	8
6	MB	0	6	B	5	6	M	5	6	A	5	6	MA	9
7	MB	0	7	B	5	7	M	6	7	A	8	7	MA	9
8	MB	0	8	B	5	8	M	6	8	A	8	8	MA	9
9	MB	0	9	B	5	9	M	6	9	A	9	9	MA	10
10	MB	0	10	B	5	10	M	6	10	A	10	10	MA	10

Así, la organización ha podido establecer:

- Riesgo bajo, se considera de 0 a 3 (por ejemplo, color verde).
- Riesgo medio, de 4 a 6, (por ejemplo, color amarillo).
- Riesgo alto, de 7 a 8 (por ejemplo, color naranja).
- Riesgo extremo, de 9 a 10 (por ejemplo, color rojo).

La matriz de riesgos para la plataforma HOST IESS ha quedado definida como se muestra en la Tabla 5-42.

Tabla 5-42. Matriz de Riesgo de la Plataforma HOST - IESS

AMENAZA	VALOR DEL DAÑO	FRECUENCIA	RIESGO	COSTO DEL DAÑO
Actividades no autorizadas	7	M	5	\$ 11.000,00
Agua	7	B	3	\$ 892.000,00
Condiciones climáticas desfavorables	7	B	3	\$ 296.000,00
Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	7	B	3	\$ 892.000,00
Diseño y planificación inadecuados o adaptación inadecuada	7	MA	9	\$ 20.000,00
Fallo de dispositivos o sistemas	8	A	8	\$ 1.505.000,00
Fallo de software /aplicaciones o servicio	6	B	3	\$ 400,00
Fallo o interrupción del suministro principal	7	M	5	\$ 134.300,00
Fuego	7	B	3	\$ 892.000,00
Pérdida de recursos	6	B	3	\$ 237.600,00
Robo (dispositivos, medios de almacenamiento y documentos)	8	B	5	\$ 525.000,00
Uso erróneo o administración de dispositivos y sistemas	6	B	3	\$ 684.400,00

5.3.2.6 Actividad 6: Contramedidas

En base a la matriz de riesgo, la organización ha podido establecer el riesgo a ser considerado, tomando en cuenta la factibilidad de ocurrencia y el costo del daño. Por ello, la organización ha establecido tomar los correctivos necesarios y realizar las siguientes tareas.

Tarea 1: se han definido las contramedidas que pueda mitigar o eliminar el riesgo potencial. Estas contramedidas han sido enfocadas a las vulnerabilidades (las contramedidas pueden contrarrestar a una o varias vulnerabilidades). Para ello, se identificaron las vulnerabilidades de los activos de la organización como se muestra en la Tabla 5-43 (para estructurar esta tabla se han tomado los valores de la Tabla 5-38).

Tabla 5-43. Contramedidas para HOST - IESS

VULNERABILIDAD	CONTRAMEDIDA
Errores conocidos en el software	Control de calidad de los sistemas de software
Fallo de los componentes	Contratos de soporte y mantenimiento en vigencia
Falta de capacitación en la administración del activo	Capacitación continua en la administración del activo
Falta de garantía técnica de los equipos	Contrato de garantía en vigencia

<i>VULNERABILIDAD</i>	<i>CONTRAMEDIDA</i>
Falta de mantenimiento y/o actualizaciones	Contratos de mantenimiento y actualizaciones vigente
Falta de planes de contingencia	Generar plan de contingencia por activo
Falta de política formal de cambio de credenciales	Política de gestión de credenciales
Falta de precaución en las conexiones físicas	Mejora de las conexiones físicas de los activos
Falta de soporte preventivo y correctivo	Contratos de soporte y mantenimiento en vigencia
Inexistente ambiente de pruebas	Implementar ambiente de pruebas para los aplicativos de Software
Mala gestión de contraseñas	Proceso adecuado de gestión de contraseñas
No posee mecanismo de respaldo	Disponer de un dispositivo de respaldo para el activo
Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	Instalaciones sismo-resistentes
Susceptible a incendios y altas temperaturas	Sistema contra incendios y ventilación adecuada
Ubicación en un área susceptible a inundaciones.	Mejora física de las instalaciones, drenajes adecuados
Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Mejora en los accesos físicos al edificio y habitación

Tarea 2: los controles que permitan verificar si las contramedidas han llegado a contrarrestar el riesgo aparente de una amenaza, no se han sido considerados en este análisis.

5.3.3. Comparación resultados línea base inicial y marco de trabajo AVARCIBER (línea base final)

La Figura 5-16 muestra la combinación de los resultados de las líneas base inicial y final (AVARCIBER), ofreciendo una visión global de los puntos fuertes y débiles de la identificación y evaluación de riesgos en ciberseguridad para los elementos de gestión de riesgos en ciberseguridad, asociación de los elementos, y resultados obtenidos.

	Línea Base	Avarciber
Activo - Vulnerabilidad	X	X
Activo - Amenaza	X	X
Activo - Contramedida	X	
Vulnerabilidad - Amenaza	X	X
Vulnerabilidad - Contramedida	X	X
Amenaza - Contramedida	X	

	Línea Base	Avarciber
Vulnerabilidad por Dimensiones		X
Costo de Vulnerabilidad		X
Matriz de Riesgo	X	X
Costo del Riesgo		X
Contramedida	X	X

Figura 5-16. Comparativa de elementos, asociaciones y resultados de línea base inicial y final (AVARCIBER)

La revisión de los resultados entre las líneas base inicial y final (AVARCIBER) se describen a continuación:

- Los elementos de riesgos de ciberseguridad (vulnerabilidades, amenazas, contramedidas) identificados con AVARCIBER, fueron más visibles debido a que se utilizaron las taxonomías de vulnerabilidades y amenazas, lo que ha permitido una identificación más apropiada debida a la estructura jerárquica de las taxonomías. En el caso de las contramedidas, al estar relacionadas con cada vulnerabilidad, nos ha permitido identificar las contramedidas necesarias para cubrir con mayor certeza los riesgos asociados.
- Las relaciones de los elementos de riesgo en ciberseguridad con el marco de trabajo AVARCIBER fueron depuradas, para que exista una relación coherente y adecuada entre los elementos participantes para optimizar la identificación y evaluación de riesgos en ciberseguridad.
- En la identificación de vulnerabilidades de los activos de ciberseguridad, la relación de las dimensiones de seguridad para cada vulnerabilidad utilizadas en el marco de trabajo AVARCIBER ha permitido medir el valor del daño de las vulnerabilidades con mayor coherencia y exactitud.
- Al elaborar la matriz de riesgo de los activos de ciberseguridad, el costo del daño de las vulnerabilidades identificadas en el marco de trabajo AVARCIBER, y que fueron totalizadas por cada amenaza de ciberseguridad identificada, permite brindar un elemento adicional de información para la gestión de los riesgos de ciberseguridad identificados, en función de la criticidad, impacto y costo del riesgo identificado.

5.3.4. Conclusiones

En este capítulo se han presentado los requisitos y el proceso del prototipo elaborado, como una alternativa para la identificación y evaluación de riesgos en ciberseguridad para las organizaciones.

Un elemento importante que identifica a este prototipo es la identificación y medición del riesgo a partir de las vulnerabilidades de ciberseguridad, pues éstas se asocian a los activos y a las amenazas de ciberseguridad identificadas de la organización.

Un punto que hay que tener en cuenta es la necesidad de que la organización determine la valoración del impacto según sus necesidades y objetivos estratégicos. Sin embargo, en el futuro esta valoración puede ser implementada con un proceso de aprendizaje y asignación automática.

El prototipo se ha desarrollado en una hoja Excel y en un entorno web, y se ha buscado que fuera muy sencillo en su uso. Se contemplan desarrollar versiones periódicas para mejorar y mantener la aplicación.

5.4. Validación de las Hipótesis de Trabajo

Un marco de trabajo no es una herramienta que asegure el éxito de aquella actividad a la que se aplique, sino una guía de ayuda para mejorar los resultados y reducir la dependencia del criterio experto de las personas. El marco de trabajo propuesto en esta tesis no pretende resolver todos los problemas a los que se enfrenta la organización para la identificación y evaluación de riesgos en ciberseguridad, sino guiarle desde las actividades más tempranas en la identificación de activos, asignación de vulnerabilidades, medición del daño de las vulnerabilidades, medición del costo del daño de las vulnerabilidades y asociarlas con las amenazas, para que mejore la **medición de los riesgos en ciberseguridad basados en la medición del daño de las vulnerabilidades y del costo del daño de las mismas**. Si se logra este cometido, es factible mencionar que el marco de trabajo es aplicable y ha cumplido las expectativas planteadas. Y verificar, si las hipótesis que se plantearon han sido validadas.

Después de haber realizado las evaluaciones de las líneas base inicial y final (marco de trabajo AVARCIBER), y comparar los resultados obtenidos, se puede concluir que se han cumplido los objetivos esperados y se pueden validar las hipótesis del trabajo.

PARA LA HIPÓTESIS GENERAL:

- “Si una empresa, sea cual sea su sector de negocio, se apoya en un marco de trabajo que le facilite un modelo para identificar y evaluar los riesgos de ciberseguridad, conseguirá mejorar la evaluación de riesgos en la implementación de los conceptos de ciberseguridad en la empresa”.

Esta hipótesis queda validada con la identificación de los elementos y relaciones del modelo conceptual de dominio definido. **Véase sección 4.1.1 Elementos y relaciones en el modelo conceptual de dominio**. Así mismo la Figura 5-17, y la Tabla 5-44 muestra las relaciones de cada uno de los elementos identificados del modelo conceptual y que se describen en el marco de trabajo AVARCIBER, que puede ser utilizado por las empresas independiente del sector al cual pertenece. En el proceso de la línea base no se consideraba la influencia de las vulnerabilidades en la evaluación del riesgo, y no se evaluaba el daño y costo de las vulnerabilidades en cada activo, así como tampoco se utilizaba taxonomías de vulnerabilidades y amenazas, generando incremento inadecuado de elementos por errores de sintaxis.

Figura 5-17. Relación entre los elementos del modelo conceptual AVARCIBER.

Tabla 5-44. Relación entre elementos del modelo conceptual AVARCIBER

NOMBRE	DESCRIPCIÓN
1. Activo – Vulnerabilidad PRESENTA	Un activo puede tener muchas vulnerabilidades, y una vulnerabilidad se puede presentar en muchos activos.
2. Activo – Tipo de Activo TIENE	Un activo puede pertenecer a un tipo de activo según sus características, y un tipo de activo tendrá muchos activos asociados a su naturaleza.
3. Activo – Unidad Organizacional ES RESPONSABLE DE	El activo siempre pertenecerá a alguna unidad organizacional de la empresa, y la unidad organizacional podrá tener muchos activos.
4. Activo – Activo CONTIENE	Un activo puede ser el contenedor de otros activos formando un solo componente.
5. Activo – Activo DEPENDE	Un activo puede ser parte de un activo que contiene a él y muchos más.
6. Activo – Vulnerabilidad – Dimensión Vulnerabilidad – Tipo Valoración VALORACION IMPACTO	El activo podría hacer una valoración de impacto, por cada vulnerabilidad en una o varias dimensiones de valoración, tomando en cuenta el tipo de valoración.
7. Vulnerabilidad – Amenaza APROVECHA (EXPLOTA)	Una amenaza puede explotar las vulnerabilidades de los activos, y una vulnerabilidad puede estar presente en muchas amenazas.
8. Amenaza – Fuente TIENE	Una amenaza debe tener al menos una fuente, y las fuentes pueden estar en varias amenazas
9. Fuente – Tipo_Fuente ES	Las fuentes de amenaza deben ser de un tipo, y el tipo puede estar en varias amenazas.
10. Vulnerabilidad – Contramedida REDUCE	Una contramedida puede reducir el efecto negativo que pueda tener una vulnerabilidad, y una contramedida puede ayudar a muchas vulnerabilidades.
11. Control – Contramedida POSEE	Un control puede poseer o no algunas contramedidas, y una contramedida siempre ayudará a un control.

12. Amenaza – Incidente IMPLEMENTA	Una amenaza puede ser implementada por un incidente o no, y el incidente se aprovecha de una o varias amenazas.
---------------------------------------	---

PARA LA HIPÓTESIS DERIVADA 1.

- Si una empresa define una clasificación de los tipos de activos de ciberseguridad, para identificar y catalogar los activos de ciberseguridad según su naturaleza, entonces permitirá clasificarlos, para facilitar la identificación de características y vulnerabilidades comunes.

Esta hipótesis queda validada con la definición de una taxonomía de tipos de activos basados en estándares internacionales como la ISO 27005. Para ello, véase sección 5.3.2 Actividades del Marco de Trabajo AVARCIBER, subsección 5.3.2.2 Actividad 1: Lanzamiento. Así mismo en la Tabla 5-28 y Tabla 5-45 se muestran los tipos de activos utilizados en el caso de estudio. En el proceso de la línea base no existía la clasificación de tipos de activos generando confusión en la identificación y clasificación de los activos.

Tabla 5-45. Tipo de activos de ciberseguridad utilizados en AVARCIBER

TIPO ACTIVO
Procesos y actividades de negocios
Información
Hardware
Software
Red
Personal
Sitio
Estructura de la organización

HIPÓTESIS DERIVADA 2.

- Si una empresa define las taxonomías de vulnerabilidades y amenazas de ciberseguridad para implementarlas y gestionarlas según las necesidades de la empresa, inclusive incluir nuevos elementos, entonces la identificación y evaluación de estos elementos será única sin posibilidad de ambigüedades o diferencias de sintaxis, que faciliten la gestión de vulnerabilidades y amenazas de ciberseguridad.

Esta hipótesis queda validada con el establecimiento de las taxonomías de las vulnerabilidades, basada en el estándar ISO 27005 y la taxonomía de las amenazas basada en el estándar ENISA 2016. Para ello, véase la sección 5.3.2 Actividades del Marco de Trabajo AVARCIBER, subsección 5.3.2.2 Actividad 1: Lanzamiento. Así mismo, en la Tabla 5-29 y Tabla 5-30 se muestran las taxonomías definidas. En el proceso de la línea base no se utilizaron taxonomías definidas previamente.

La utilización de las taxonomías nos ha permitido asignar las vulnerabilidades a los activos, y las amenazas a las vulnerabilidades, desde una lista de valores válidos. De esta forma, se ha impedido el ingreso manual de los datos, permitiendo tener valores sin ambigüedades, o diferencias de sintaxis, y facilitando esta actividad.

HIPOTESIS DERIVADA 3.

- Si una empresa en la identificación y evaluación de riesgos de los activos de ciberseguridad asocia las vulnerabilidades a las dimensiones de seguridad y mide cada una de ellas como valor del daño de la vulnerabilidad, entonces el promedio del valor del daño de las vulnerabilidades en cada dimensión de seguridad generará un valor del daño más representativo y justificado de cada vulnerabilidad.

Esta hipótesis queda validada con la descripción del marco de trabajo donde se describe la medición de las vulnerabilidades en cada una de las dimensiones de seguridad para definir el valor del daño de cada vulnerabilidad en los activos de ciberseguridad. Para ello, véase sección 4.2 *Marco de Trabajo AVARCIBER, Actividad 3. Evaluar el nivel de daño para las tuplas Vulnerabilidad – Activo (dimensión), Tareas 2, 3 y 4*. Así mismo en la Tabla 5-46 se muestran los resultados de las relaciones entre vulnerabilidades, activos, dimensiones de seguridad y valor del daño. Estas actividades no son consideradas en la línea base.

Calcular el daño que produce la vulnerabilidad en cada una de las dimensiones de seguridad definidas, permite tener una mejor percepción del daño que puede producir una vulnerabilidad en el activo, el costo del daño nos permite medir el impacto económico que sufriría la empresa en caso de materializarse la vulnerabilidad.

Tabla 5-46. Vulnerabilidades, activos, valor y costo del daño HOST – IESS AVARCIBER

<i>Vulnerabilidad</i>	<i>Activo</i>	<i>Costo del Activo</i>	<i>Dimensiones</i>				<i>Vulnerabilidad</i>	
			<i>Daño Confidencialidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Criticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
Falta de soporte preventivo y correctivo	Servidor	10.000,00	2	3	8	8	5,25	3.500
Ubicación en un área susceptible a inundaciones.	Servidor		5	4	3	8	5,00	5.000
Susceptible a incendios y altas temperaturas	Servidor		6	7	8	8	4,25	6.000
Falta de soporte preventivo y correctivo	Almacenamiento	2.000,00	5	8	2	9	6,00	300
Ubicación en un área susceptible a inundaciones.	Almacenamiento		7	4	1	9	5,25	600
Falta de planes de contingencia	Almacenamiento		6	5	3	9	5,75	1.200

HIPOTESIS DERIVADA 4.

- Si una empresa al realizar una identificación y evaluación de riesgos de sus activos de ciberseguridad puede medir el costo del daño de cada vulnerabilidad, entonces la materialización de cada vulnerabilidad genera un costo de daño que puede acumularse y asociarse a la amenaza que lo materializa.

Esta hipótesis queda validada con la descripción del marco de trabajo donde se describe el costo del daño de cada vulnerabilidad en los activos de ciberseguridad. Para ello, véase la sección 4.2 *Marco de Trabajo AVARCIBER, Actividad 3. Evaluar el nivel de daño para las tuplas Vulnerabilidad – Activo (dimensión), Tarea 6*. Así mismo, en la Tabla 5-46 se muestran los resultados de las relaciones entre vulnerabilidades, activos, dimensiones de seguridad y el costo del daño. En el proceso de la línea base estas actividades no existen.

La valoración del daño de las vulnerabilidades asociadas a los activos, permite identificar la magnitud económica del daño que podría tener el activo cuando una amenaza materialice la vulnerabilidad, estos valores serán sumados si la vulnerabilidad está presente en varios activos, lo que genera una información adecuada del impacto económico que sufrirá la empresa.

HIPÓTESIS DERIVADA 5.

- Si una empresa genera una matriz de gestión de riesgos en ciberseguridad que incluya además de las amenazas, el daño, la probabilidad de ocurrencia, la medida de riesgo asociado y el costo total de cada amenaza, entonces podrá ser una herramienta que ayude a identificar los costos relacionados a cada amenaza, permitiendo a las autoridades de la organización tomar una decisión para priorizar los riesgos a ser gestionados.

Esta hipótesis queda validada con la descripción del marco de trabajo donde se describe la matriz de riesgo, identificando para cada amenaza el valor del daño de la amenaza, el costo del daño de la amenaza y el riesgo asociado, lo cual permitirá a los responsables de la organización tomar una decisión adecuada para gestionar el riesgo, no solo por su valor sino también por el costo asociado. Para ello, véase la sección 4.2 *Marco de Trabajo AVARCIBER, Actividad 5. Medición del Riesgo*. Así mismo, la Tabla 5-47 muestra la matriz de riesgo referida. En el proceso de la línea base no se considera el costo del daño de la amenaza.

El tener un costo de daño asociada a cada amenaza, es un valor cuantitativo que facilita la toma de decisiones el momento de identificar los riesgos a ser considerados para el tratamiento de los mismos.

Tabla 5-47. Matriz de Riesgo AVARCIBER

<i>Amenaza</i>	<i>Frecuencia</i>	<i>Valor de Daño de la amenaza (valor redondeado)</i>	<i>Riesgo</i>	<i>Costo del Daño de la amenaza</i>
Condiciones climáticas desfavorables	(MA) Alto	6	9	3.800
Agua	(B) Bajo	5	5	5.600
Fuego	(MB) Muy Bajo	4	0	6.000
Fallo de dispositivos o sistemas	(MA) Muy Alto	6	9	1.200

HIPÓTESIS DERIVADA 6.

- Si una empresa al identificar las contramedidas de los riesgos de ciberseguridad identificados, lo hace para cada una de las vulnerabilidades analizadas, entonces podrá generar contramedidas para cada vulnerabilidad que esté presente en muchos activos y mejorar la mitigación de los riesgos en ciberseguridad, con menor cantidad de contramedidas.

Esta hipótesis queda validada con el establecimiento de las contramedidas, para contrarrestar los riesgos identificados, y que además van asociadas a las vulnerabilidades identificadas a los activos de ciberseguridad. Para ello, véase sección 5.3.2 Actividades del Marco de Trabajo AVARCIBER, subsección 5.3.2.6 Actividad 5: Contramedidas. Así mismo, en la Tabla 5-46 y Tabla 5-48 se muestran las contramedidas establecidas. En el proceso de la línea base las contramedidas son asignadas para cada amenaza, dejando de lado muchas vulnerabilidades sin gestión adecuada.

El poder generar contramedidas para cada vulnerabilidad permite abarcar de mejor manera el tratamiento de los riesgos y proteger a los activos de las amenazas identificadas.

Tabla 5-48. Contramedidas por vulnerabilidades HOST – IESS AVARCIBER

VULNERABILIDAD	CONTRAMEDIDA
Errores conocidos en el software.	Control de calidad de los sistemas de software
Fallo de los componentes	Contratos de soporte y mantenimiento en vigencia
Falta de capacitación en la administración del activo	Capacitación continua en la administración del activo
Falta de garantía técnica de los equipos	Contrato de garantía en vigencia
Falta de mantenimiento y/o actualizaciones	Contratos de mantenimiento y actualizaciones vigente
Falta de planes de contingencia	Generar plan de contingencia por activo
Falta de política formal de cambio de credenciales	Política de gestión de credenciales
Falta de precaución en las conexiones físicas	Mejora de las conexiones físicas de los activos
Falta de soporte preventivo y correctivo	Contratos de soporte y mantenimiento en vigencia
Inexistente ambiente de pruebas	Implementar ambiente de pruebas para los aplicativos de Software
Mala gestión de contraseñas	Proceso adecuado de gestión de contraseñas
No posee mecanismo de respaldo	Disponer de un dispositivo de respaldo para el activo
Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	Instalaciones sismo-resistentes
Susceptible a incendios y altas temperaturas	Sistema contra incendios y ventilación adecuada
Ubicación en un área susceptible a inundaciones.	Mejora física de las instalaciones, drenajes adecuados
Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Mejora en los accesos físicos al edificio y habitación

6. APORTACIONES, CONCLUSIONES Y LÍNEAS FUTURAS

En este capítulo se presentan los resultados de la investigación realizada. Para ello, lo hemos dividido en tres apartados. En el primero, se exponen las aportaciones realizadas en esta tesis doctoral. En el segundo, se presentan las conclusiones finales, recopiladas de la elaboración, descripción y validación del marco de trabajo AVARCIBER para la identificación y evaluación de los riesgos en ciberseguridad. Finalmente, en el tercero, se presentan algunos temas de interés que han sido identificados y que no han sido analizados por estar fuera del contexto de la investigación, pero que pueden ser el punto de partida para investigaciones futuras y continuación de este trabajo de investigación.

6.1. Principales aportaciones

Las principales aportaciones de la investigación realizada para esta tesis doctoral se fueron identificando en los capítulos de estudio del estado de la cuestión, y resolución del problema, acerca de un marco de trabajo para la identificación y evaluación de riesgos en ciberseguridad AVARCIBER. A continuación, se enumeran dichas aportaciones:

- Del capítulo II, del estado de la cuestión, se desprenden las siguientes aportaciones:
 - Se ha realizado una **revisión sistemática (RS) de los modelos de madurez más nombrados (y utilizados) en ciberseguridad**, determinando que en la actualidad existe una deficiencia de modelos de madurez que sean totalmente enfocados en ciberseguridad, de fácil implementación y adaptables a diferentes tipos de organizaciones.
 - Se ha realizado un **estudio comparativo de los modelos de madurez de ciberseguridad** más nombrados en los artículos científicos según la RS (Rea-Guaman et al., 2017), determinando: a) que existe una deficiencia de modelos de madurez que estén totalmente enfocados en ciberseguridad, y b) que todos los modelos de madurez de capacidad de ciberseguridad se basan en la gestión de riesgos de ciberseguridad, pero solo los modelos SSE-CMM y C2M2 miden la gestión de riesgos de una manera más específica.
 - Se ha realizado una **revisión sistemática de taxonomías de riesgos en ciberseguridad**, donde se ha identificado que dichas taxonomías están enfocadas en riesgos específicos como, por ejemplo, riesgos de ingeniería social, riesgos financieros, riesgos operacionales, amenazas maliciosas y basadas en ciertos escenarios específicos.
 - De la revisión sistemática de taxonomía de riesgos en ciberseguridad, se identificaron algunos artículos que muestran **modelos conceptuales donde se describen los elementos que participan en la gestión de riesgos**. Estos modelos conceptuales describen relaciones particulares entre los elementos de gestión de riesgos, enfocados en necesidades particulares.
 - También se han realizado una **revisión sistemática de taxonomías de activos en ciberseguridad**, identificando que no existen muchas taxonomías de activos en ciberseguridad que estén publicadas en artículos científicos. No obstante, existen esfuerzos aislados de empresas, por encargo, que realizan taxonomías para las organizaciones.
 - Se ha realizado una **revisión sistemática de taxonomías de vulnerabilidades y otra revisión sistemática de amenazas en ciberseguridad**, analizando que todas las taxonomías se basan en un enfoque específico según el enfoque que requiera la organización y las necesidades de la misma.

- Del capítulo 4, de la resolución del problema planteado, se pueden identificar las siguientes aportaciones:
 - Se ha desarrollado un **modelo conceptual de dominio**, en donde se han descrito las relaciones que se pueden establecer entre los elementos importantes de los riesgos en ciberseguridad como son: activos, vulnerabilidades de ciberseguridad y amenazas de ciberseguridad. También se han establecido **relaciones entre las vulnerabilidades de ciberseguridad y las dimensiones de seguridad** (Disponibilidad, Integridad y Confiabilidad).
 - El modelo conceptual de dominio desarrollado incluye algunos elementos diferenciadores como:
 - El elemento **dimensión de valoración** ayuda a medir el impacto de la vulnerabilidad según las dimensiones de seguridad como, por ejemplo: confidencialidad, integridad, disponibilidad y criticidad.
 - La **vulnerabilidad de ciberseguridad es el elemento primordial** para medir el impacto de una amenaza de ciberseguridad en los activos de la organización.
 - Las **contramedidas están ligadas a las vulnerabilidades**, para eliminar o reducir el impacto en caso de llegar a materializarse.
 - Se ha desarrollado el **marco de trabajo AVARCIBER para la identificación y evaluación de riesgos de ciberseguridad**, tomando en cuenta el modelo conceptual de dominio definido previamente.
 - El marco de trabajo desarrollado también describe la inclusión de una **nueva dimensión de seguridad, que es la criticidad del activo de ciberseguridad**, que se calcula tomando el mayor valor de las dimensiones de seguridad previamente evaluadas.
 - En el marco de trabajo desarrollado, también se ha incluido la **evaluación de las vulnerabilidades de los activos de ciberseguridad, en cada una de las dimensiones de seguridad** (Disponibilidad, Integridad Confiabilidad y Criticidad), que permite calcular **el valor promedio del valor del daño que puede tener cada una de las vulnerabilidades de ciberseguridad**.
 - Otro elemento importante que se ha incluido en el marco de trabajo desarrollado ha sido la inclusión del **costo del daño que se asocia a cada vulnerabilidad de los activos de ciberseguridad**, que luego son totalizados por cada amenaza, para incluirlos en la matriz de riesgos y sea información que ayude en la **toma de decisiones para la priorización** de la gestión de los **riesgos de ciberseguridad identificados**.
 - Se ha elaborado un **prototipo para validar el modelo conceptual de dominio y el marco de trabajo** establecido para la identificación y evaluación de riesgos en ciberseguridad, e identificar los requerimientos funcionales definitivos para elaborar un producto de software que gestione la identificación y análisis de gestión de riesgos en ciberseguridad.

6.2. Conclusiones

Del análisis realizado a los conceptos de ciberseguridad, a los modelos de madurez en ciberseguridad y a las taxonomías de activos de la organización, y riesgos, vulnerabilidades y amenazas de ciberseguridad, se puede concluir lo siguiente:

- Que casi todos los marcos de ciberseguridad utilizan la metodología de gestión de riesgos.
- Que no existen modelos de madurez enfocados específicamente en ciberseguridad, sino que muchos de ellos se han adaptado a este enfoque.
- La comparativa de ciertos modelos de madurez indica que la base fundamental de su estructura es la identificación y evaluación de riesgos en ciberseguridad.

- Los activos en ciberseguridad de las organizaciones son muy particulares, pues existen muchos tipos de organizaciones y lo único que se ha tratado es de generar taxonomías muy generales y a un nivel muy alto de especificación.
- De las taxonomías de vulnerabilidades de ciberseguridad publicadas, la mayoría de ellas están enfocadas en los sistemas de software.
- Existen taxonomías de amenazas en ciberseguridad, de organizaciones que administran y mantienen actualizadas continuamente estas taxonomías y gestionan las buenas prácticas de la industria, como por ejemplo la taxonomía publicada por ENISA (European Union Agency for Network and Information Security).

Los modelos conceptuales que describen la gestión de riesgos tienen una variedad de elementos, asociaciones y descripciones, que describen casos puntuales y focalizados según el área de aplicación, que no están especificados para ciberseguridad.

En la actualidad no hay publicados un marco de trabajo para la identificación y evaluación de riesgos en ciberseguridad, ni taxonomías definidas para los activos de la organización, y vulnerabilidades y amenazas de ciberseguridad que estén catalogadas como estándares internacionales para la industria, sino trabajos puntuales y focalizados según el tipo del negocio de la organización, lo que no ha permitido una estandarización de las taxonomías.

No se ha identificado un marco de trabajo que determine los elementos básicos y necesarios poder establecer un proceso que permita identificar y valorar los riesgos en ciberseguridad, basados en un modelo conceptual orientado a ciberseguridad.

La valoración de cada una de las vulnerabilidades de los activos de ciberseguridad en las dimensiones de seguridad, y su cálculo promedio, ha permitido identificar el valor del daño de cada vulnerabilidad con mayor precisión por los cálculos previos, que afectará directamente en el daño que puede generar la amenaza de un riesgo de ciberseguridad.

La medición del costo de cada una de las vulnerabilidades de los activos de ciberseguridad ha permitido calcular el costo del daño, que luego de totalizarlo, ha sido un elemento importante en la matriz de riesgo, pudiendo mostrar los riesgos de ciberseguridad no solo con valores cualitativos sino cuantitativos, permitiendo la toma de decisiones por parte de los responsables de la organización.

El prototipo elaborado analiza y evalúa la gestión de riesgos en ciberseguridad a partir de las vulnerabilidades de ciberseguridad, pues éstas se asocian a los activos y a las amenazas de ciberseguridad identificadas de la organización.

De la validación del prototipo, se establecerán las observaciones que se puedan hacer al modelo conceptual de dominio y sus relaciones, así como la validación del proceso de medición de riesgos en ciberseguridad elaborado para el efecto.

Es necesario generar un aplicativo de software para la identificación y evaluación de riesgos en ciberseguridad que permita la gestión de los activos de la organización a partir de las vulnerabilidades de ciberseguridad, por lo cual se debe desarrollar un aplicativo que contemple el modelo conceptual definido, el marco de trabajo desarrollado y utilizar las taxonomías identificadas.

6.3. Líneas futuras de investigación

Tras la realización de esta tesis, se han identificado algunas vías con las que continuar investigando:

- Identificar nuevos elementos para ser considerados en el modelo conceptual, de forma que se incluyan nuevos paradigmas de los estándares de la industria y las tendencias tecnológicas.

- Ampliar el marco de trabajo AVARCIBER, incluyendo nuevos elementos del modelo conceptual para poder ampliar la gestión de riesgos en ciberseguridad, y para el control de los mismos.
- Desarrollar una herramienta que amplíe las funcionalidades para la gestión de riesgos en ciberseguridad, de acuerdo con el modelo conceptual y con el marco de trabajo AVARCIBER.
- Definir un plan de formación continua para el personal de la empresa para socializar y evangelizar los conceptos de ciberseguridad en la empresa, destinado tanto a usuarios como a los distintos perfiles de TI. Para estos últimos, se debería definir el conjunto de competencias y formación necesaria para el desempeño de cada rol.
- Definir un proceso de revisión sistemática del marco de trabajo que permita adaptar las actividades mejorando el marco de trabajo.
- Identificar un mecanismo que permita calcular el costo del daño de las vulnerabilidades en las dimensiones de seguridad, basados en el riesgo operativo.

7. BIBLIOGRAFÍA

- 71504, U. (2008). *Metodología de análisis y gestión de riesgos para los sistemas de información*.
- Accenture and Ponemon Institute. (2019). The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study. *NINTH ANNUAL COST OF CYBERCRIME STUDY*, 18. Retrieved from https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50
- Adler, R. M. (2013). A dynamic capability maturity model for improving cyber security. *2013 IEEE International Conference on Technologies for Homeland Security (HST)*, 230–235. <https://doi.org/10.1109/THS.2013.6699005>
- Amutio Gómez, M. A. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. 75. Retrieved from http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html
- AVTEST (IT-Security Institute). (2019). *SECURITY REPORT 2018/19*.
- Barclay, C. (2014). Sustainable security advantage in a changing environment: The cybersecurity capability maturity model (CM2). *Proceedings of the 2014 ITU Kaleidoscope Academic Conference: Living in a Converged World - Impossible Without Standards?*, K 2014, 275–282. <https://doi.org/10.1109/Kaleidoscope.2014.6858466>
- Barnes, B., & Cieply, M. (The N. Y. T. (2014). Intrusion on Sony Unit Prompts a Shutdown of Messaging Systems. Retrieved March 29, 2020, from The New York Times website: <https://www.nytimes.com/2014/11/30/business/media/intrusion-on-sony-unit-prompts-a-shutdown-of-messaging-systems.html>
- Bazaz, A., & Arthur, J. D. (2007). Towards a taxonomy of vulnerabilities. *Proceedings of the Annual Hawaii International Conference on System Sciences*, (c), 1–10. <https://doi.org/10.1109/HICSS.2007.566>
- Bazaz, A., Arthur, J. D., & Tront, J. G. (2006). Modeling security vulnerabilities: A constraints and assumptions perspective. *Proceedings - 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, DASC 2006*, (c), 95–102. <https://doi.org/10.1109/DASC.2006.35>
- Bergmann, F. B., & Silveira, M. S. (2014). “My life doesn’t have to be an open book”: A model to help designers to enhance privacy controls on social network sites. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8533 LNCS, 387–399. https://doi.org/10.1007/978-3-319-07620-1_34
- Berkley Research Group. (2016). *Estudio comparativo de los niveles de madurez en ciberseguridad*. 1–45.
- Bishop, M., Miloslavskaya, N., & Theocharidou, M. (2015). Information Security Education Across the Curriculum: 9th IFIP WG 11.8 World Conference, WISE9 Hamburg, Germany, May 26-28, 2015 Proceedings. *IFIP Advances in Information and Communication Technology*, 453, 53–63. <https://doi.org/10.1007/978-3-319-18500-2>
- Bompard, E., Huang, T., Wu, Y., & Cremenescu, M. (2013). Classification and trend analysis of threats origins to the security of power systems. *International Journal of Electrical Power and Energy Systems*, 50(1), 50–64. <https://doi.org/10.1016/j.ijepes.2013.02.008>
- Brian, D. (Kaspersky D. (2014). Malware POS y raspadores de RAM. Retrieved March 29, 2020, from Kaspersky Daily website: <https://www.kaspersky.es/blog/malware-pos-y-raspadores->

de-ram/2304/

- Buchanan, L., Larkin, M., & D'Amico, A. (2012). Mission assurance proof-of-concept: Mapping dependencies among cyber assets, missions, and users. *2012 IEEE International Conference on Technologies for Homeland Security, HST 2012*, 298–304. <https://doi.org/10.1109/THS.2012.6459865>
- Cebula, J. J., & Young, L. R. (2010). A Taxonomy of Operational Cyber Security Risks. *Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst*, (December), 1–47. <https://doi.org/10.1007/978-1-4419-7133-3>
- Christopher, J. D. (2014). Cybersecurity Capability Maturity Model (C2M2). *Department of Homeland Security*, (February). Retrieved from <https://energy.gov/oe/cybersecurity-critical-energy-infrastructure/cybersecurity-capability-maturity-model-c2m2-program>
- CMU. (2003). System Security Engineering Capability Maturity Model (SSE-CMM). *Proceedings of the 19th International Conference on Software Engineering ICSE 97*, 35, 566–567. <https://doi.org/10.1145/253228.253454>
- Cohen, F., Lowrie, J., & Preston, C. (n.d.). Chapter 1 THE STATE OF THE SCIENCE OF DIGITAL EVIDENCE EXAMINATION. *Ifip International Federation For Information Processing*, 3–21.
- Delmee, F. (2016). *the Structure of a Cyber Risk a Scenario Based Approach in Cyber Risk*.
- Department of Energy, U. (2019). *CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2)*. (June).
- Donaldson, S. E., Siegel, S. G., & Williams, C. K. (2019). *Understanding Security Issues* (p. 175). p. 175. Boston/Berlin: Walter de Gruyter Inc.
- Donaldson, S. E., Siegel, S. G., Williams, C. K., & Abdul, A. (2015). *Enterprise Cybersecurity*. Apress.
- Donaldson, S. E., Siegel, S. G., Williams, C. K., & Abdul, A. (2018). *Enterprise Cybersecurity Study Guide How to Build a Successful Cyberdefense*.
- Elnagdy, S. A., Qiu, M., & Gai, K. (2016). Understanding Taxonomy of Cyber Risks for Cybersecurity Insurance of Financial Industry in Cloud Computing. *Proceedings - 3rd IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2016 and 2nd IEEE International Conference of Scalable and Smart Cloud, SSC 2016*, 295–300. <https://doi.org/10.1109/CSCloud.2016.46>
- Farooq, A., Kakakhel, S. R. U., Virtanen, S., & Isoaho, J. (2016). A taxonomy of perceived information security and privacy threats among IT security students. *2015 10th International Conference for Internet Technology and Secured Transactions, ICITST 2015*, 280–286. <https://doi.org/10.1109/ICITST.2015.7412106>
- Fuentes A., M. (2020). Una analogía entre la Estadística y la Física : la media aritmética y un sistema de palanca. *Épsilon Revista de Educación Matemática*, (104), 75–81. Retrieved from <https://thales.cica.es/epsilon/?q=node/4839>
- Goksen, Y., Cevik, E., & Avunduk, H. (2015). A Case Analysis on the Focus on the Maturity Models and Information Technologies. *Procedia Economics and Finance*, 19(15), 208–216. [https://doi.org/10.1016/S2212-5671\(15\)00022-2](https://doi.org/10.1016/S2212-5671(15)00022-2)
- Goodwin, C., Nicholas, J. P., Bryant, J., Ciglic, K., Kleiner, A., Kutterer, C., ... Sullivan, K. (2015). *A framework for cybersecurity information sharing and risk reduction*. 1–24. Retrieved from http://download.microsoft.com/download/8/0/1/801358EC-2A0A-4675-A2E7-96C2E7B93E73/Framework_for_Cybersecurity_Info_Sharing.pdf
- Greitzer, F. L., Strozer, J. R., Cohen, S., Moore, A. P., Mundie, D., & Cowley, J. (2014). Analysis

- of unintentional insider threats deriving from social engineering exploits. *Proceedings - IEEE Symposium on Security and Privacy*, 2014-Janua, 236–250. <https://doi.org/10.1109/SPW.2014.39>
- Gupta, M., Rees, J., Chaturvedi, A., & Chi, J. (2006). Matching information security vulnerabilities to organizational security profiles: A genetic algorithm approach. *Decision Support Systems*, 41(3), 592–603. <https://doi.org/10.1016/j.dss.2004.06.004>
- Halvorsen, C. P., & Conradi, R. (2001). A Taxonomy to Compare SPI Frameworks. *Software Process Technology*, 2077(0212), 217–235. https://doi.org/10.1007/3-540-45752-6_17
- Hern, Alex; Gibbs, S. (The G. (2017). What is WannaCry ransomware and why is it attacking global computers? Retrieved from The Guardian News website: <https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20>
- Herzfeldt, A., Hausen, M., Briggs, R. O., & Krcmar, H. (2012). Developing a Risk Management Process and Risk Taxonomy for Medium-Sized It Solution Providers. *Ecis*, (2012), Paper 165.
- Hohan, A. I., Olaru, M., & Pirnea, I. C. (2015). Assessment and Continuous Improvement of Information Security Based on TQM and Business Excellence Principles. *Procedia Economics and Finance*, 32(15), 352–359. [https://doi.org/10.1016/S2212-5671\(15\)01404-5](https://doi.org/10.1016/S2212-5671(15)01404-5)
- Igure, V. M., & Williams, R. D. (2008). Taxonomies of attacks and vulnerabilities in computer systems. *IEEE Communications Surveys and Tutorials*, 10(1), 6–19. <https://doi.org/10.1109/COMST.2008.4483667>
- IN, U.-I. G. 73:2010. (2010). *Gestión del riesgo. Vocabulario*.
- Inga, P., & Paz, K. (2007). *MEDIA ARITMÉTICA SIMPLE*. (07), 1–13.
- ISACA. (2016). Glossary (2016). Retrieved from <https://www.isaca.org/Pages/Glossary.aspx?tid=1784&char=R>
- ISO/IEC 27000. (2014). ISO/IEC 27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary. *October*, 3, 38. Retrieved from http://www.iso.org/iso/catalogue_detail?csnumber=42103
- ISO/IEC 27000. (2018). International Standard ISO / IEC Information technology — Security techniques. *ACM Workshop on Formal Methods in Security Engineering. Washington, DC, USA*, 34(19), 45–55. <https://doi.org/10.1016/j.im.2003.02.002>
- Javier, A., Concha, M., Altamirano, A., Rica, C., Morales, D., Rica, C., ... Rica, C. (2015). *ISACA ® Glossary of Terms*.
- Kamesh, & Sakthi Priya, N. (2014). Security enhancement of authenticated RFID generation. *International Journal of Applied Engineering Research*, 9(22), 5968–5974. <https://doi.org/10.1002/sec>
- Kamra, S., & Scott, J. (2017). *Title : Impact of Data Breaches to Organizations and Individuals*. 1–10.
- Kaspersky, E. (Kapersk L. (2020). ¿Que es la ciberseguridad? Retrieved from KAPERSKY website: <https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security>
- Kishor S. Trivedi, Dong Seong Kim, A. R. (2004). *Dependability and Security*. 1–10.
- Kitchenham, B. A., & Jorgensen, T. D. M. (2004). Evidence-based Software Engineering. *Proceedings of the 26th International Conference on Software Engineering*. <https://doi.org/10.1109/ICSE.2004.1317449>
- Kitchenham, B., & Charters, S. (2007). Guidelines for performing Systematic Literature reviews

- in Software Engineering Version 2.3. *Engineering*, 45(4ve), 1051. <https://doi.org/10.1145/1134285.1134500>
- Lai, Y. P., & Hsia, P. L. (2007). Using the vulnerability information of computer systems to improve the network security. *Computer Communications*, 30(9), 2032–2047. <https://doi.org/10.1016/j.comcom.2007.03.007>
- Laribbe, L. (2006). *NAVAL POSTGRADUATE* by. Naval Postgraduate School.
- Le, N. T. (2016). *Can maturity models support cyber security ?*
- Lee, S., Chung, T., & Choi, M. (2006). An empirical study of quality and cost based security engineering. *Information Security Practice and Experience*, 379–389. Retrieved from http://link.springer.com/chapter/10.1007/11689522_35
- Li, Z., Shahidehpour, M., and Aminifar, F. (2017). Cybersecurity in Distributed Power Systems. *Proceedings of the IEEE, PP(99)*, 1–22. <https://doi.org/10.1109/JPROC.2017.2687865>
- Li, Xiaodan, Chang, X., Board, J. A., & Trivedi, K. S. (2017). A novel approach for software vulnerability classification. *Proceedings - Annual Reliability and Maintainability Symposium*. <https://doi.org/10.1109/RAM.2017.7889792>
- Li, Xu, Liang, X., Lu, R., Shen, X., Lin, X., & Zhu, H. (2012). Securing smart grid: Cyber attacks, countermeasures, and challenges. *IEEE Communications Magazine*, 50(8), 38–45. <https://doi.org/10.1109/MCOM.2012.6257525>
- Linares-Vasquez, M., Bavota, G., & Escobar-Velasquez, C. (2017). An empirical study on android-related vulnerabilities. *IEEE International Working Conference on Mining Software Repositories*, (i), 2–13. <https://doi.org/10.1109/MSR.2017.60>
- Liu, L., De Vel, O., Han, Q.-L., Zhang, J., & Xiang, Y. (2018). Detecting and Preventing Cyber Insider Threats: A Survey. *IEEE Communications Surveys & Tutorials*, (c), 1–1. <https://doi.org/10.1109/COMST.2018.2800740>
- Lugo, D. (2002). FRENTE A LOS FRAUDES CONTABLES (LEY SARBANES-OXLEY – Julio 30, 2002). Retrieved from Auditoria Forense website: <http://interamerican-usa.com/articulos/Leyes/Ley-Sar-Oxley.htm>
- MEP, N. N. (2019). *MANUFACTURERS GUIDE TO CIBERSECURITY*. 24.
- Miloslavskaya, N., Tolstoy, A., & Zapechnikov, S. (2016a). Taxonomy for unsecure big data processing in security operations centers. *Proceedings - 2016 4th International Conference on Future Internet of Things and Cloud Workshops, W-FiCloud 2016*, 154–159. <https://doi.org/10.1109/W-FiCloud.2016.42>
- M. Rea-Guaman, J. A. Calvo-Manzano, T. S. F. (2018). Prototipo para Gestionar la Ciberseguridad en Pequeñas Empresas A Prototype to Manage Cybersecurity in Small Companies. *2018 13th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–6.
- Marinos, L. (2016). *Threat taxonomy: A tool for structuring threat information. Initial report*. (January), 1–24. Retrieved from <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information>
- Miloslavskaya, N., Tolstoy, A., & Zapechnikov, S. (2016b). Taxonomy for unsecure digital information processing. *2016 3rd International Conference on Digital Information Processing, Data Mining, and Wireless Communications, DIPDMWC 2016*, 81–86. <https://doi.org/10.1109/DIPDMWC.2016.7529368>
- Ministerio de Administraciones Públicas. (2006). *MAGERIT.v.2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. 3 - Guías de Técnicas*. 3, 72.

- Nakashima, E. (The W. P. (2015). Security firm finds link between China and Anthem hack. Retrieved from The Washington Post website: <https://www.washingtonpost.com/news/the-switch/wp/2015/02/27/security-firm-finds-link-between-china-and-anthem-hack/>
- Nicola, Stefan; Donahue, P. (The S. M. G. (2019). Hackers dump data on Merkel, hundreds of German politicians. Retrieved March 29, 2020, from The Star Media Group website: <https://www.thestar.com.my/tech/tech-news/2019/01/04/hackers-dump-personal-data-of-hundreds-of-german-politicians>
- NIST. (2012). Guide for Conducting Risk Assessments. *Special Publication (NIST SP) - 800-30 Rev 1*, (September), 95. <https://doi.org/10.6028/NIST.SP.800-30r1>
- Ouedraogo, M., Mouratidis, H., Dubois, E., & Khadraoui, D. (2010). Information systems security criticality and assurance evaluation. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 6059 LNCS, 38–54. https://doi.org/10.1007/978-3-642-13577-4_4
- Payette, J., Anegbe, E., Caceres, E., & Muegge, S. (2015). Secure by Design: Cybersecurity Extensions to Project Management Maturity Models for Critical Infrastructure Projects. *Technology Innovation Management Review*, 5(6), 26. Retrieved from <http://proxy1.ncu.edu/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=108596380&site=eds-live>
- Petersen, K., Feldt, R., Mujtaba, S., & Mattsson, M. (2008). Systematic Mapping Studies in Software Engineering. *12Th International Conference on Evaluation and Assessment in Software Engineering*, 17, 10. <https://doi.org/10.1142/S0218194007003112>
- Pitropakis, N., Darra, E., Vrakas, N., & Lambrinoudakis, C. (2013). It's all in the cloud: Reviewing cloud security. *Proceedings - IEEE 10th International Conference on Ubiquitous Intelligence and Computing, UIC 2013 and IEEE 10th International Conference on Autonomic and Trusted Computing, ATC 2013*, (1), 355–362. <https://doi.org/10.1109/UIC-ATC.2013.13>
- Razzaq, A., Anwar, Z., Ahmad, H. F., Latif, K., & Munir, F. (2014). Ontology for attack detection: An intelligent approach to web application security. *Computers & Security*, 45, 124–146. <https://doi.org/10.1016/j.cose.2014.05.005>
- Rea-Guaman, A. M., Sanchez-Garcia, I. D., Feliu, T. S., & Calvo-Manzano, J. A. (2017). Modelos de Madurez en Ciberseguridad: una revisión sistemática. *Iberian Conference on Information Systems and Technologies, CISTI*. <https://doi.org/10.23919/CISTI.2017.7975865>
- Redacción, B. (BBC M. (2016). Cómo fue el “hacking” de piratas informáticos de Rusia durante las elecciones de Estados Unidos. Retrieved from BBC News website: <https://www.bbc.com/mundo/noticias-internacional-38350244>
- Richmond, R. (The N. Y. T. (2011). The RSA Hack: How They Did It. Retrieved March 29, 2020, from The New York Times website: <https://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/>
- Rot, a, & Sobinska, M. (2013). IT security threats in cloud computing sourcing model. *2013 Federated Conference on Computer Science and Information Systems, FedCSIS 2013*, 1153–1156. Retrieved from <http://www.scopus.com/inward/record.url?eid=2-s2.0-84892536420&partnerID=40&md5=5ed58482479a8c1e0dc64e972e727d01>
- Shahriar, H., & Zulkernine, M. (2011). Taxonomy and classification of automatic monitoring of program security vulnerability exploitations. *Journal of Systems and Software*, 84(2), 250–269. <https://doi.org/10.1016/j.jss.2010.09.020>
- Shamala, P., & Ahmad, R. (2014). A proposed taxonomy of assets for information security risk assessment (ISRA). *2014 4th World Congress on Information and Communication*

- Technologies, WICT 2014*, 29–33. <https://doi.org/10.1109/WICT.2014.7077297>
- Shameli-Sendi, A., Aghababaei-Barzegar, R., & Cheriet, M. (2016). Taxonomy of information security risk assessment (ISRA). *Computers & Security*, 57, 14–30. <https://doi.org/10.1016/j.cose.2015.11.001>
- Silva, C., Batista, R., Queiroz, R., Garcia, V., Silva, J., Gatti, D., ... Miranda, P. (2016). Towards a taxonomy for security threats on the web ecosystem. *Proceedings of the NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium*, (Noms), 584–590. <https://doi.org/10.1109/NOMS.2016.7502862>
- Singh, V. (2014). Revisiting Security Ontologies. *IJCSI International Journal of Computer Science Issues*, 11(6), 150–159. Retrieved from www.IJCSI.org
- Singhal, A., & Singapogu, S. (n.d.). *Security Ontologies for Modeling Enterprise Level Risk Assessment*.
- Singhal, A., & Wijesekera, D. (2010). Ontologies for modeling enterprise level security metrics. *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research - CSIRW '10*, 1. <https://doi.org/10.1145/1852666.1852731>
- Siponen, M. T. (2002). MATURITY CRITERIA FOR DEVELOPING SECURE IS AND SW. *Proceedings of the IFIP TC11 17th International Conference on Information Security. Visions and Perspectives*, 1–18. <https://doi.org/10.1007/978-0-387-3558>
- Technology, E., & News, B. (2014). Hack attack causes “massive damage” at steel works. Retrieved from BBC News website: <https://www.bbc.com/news/technology-30575104>
- Tripathi, A., & Singh, U. K. (2010). Towards standardization of vulnerability taxonomy. *ICCTD 2010 - 2010 2nd International Conference on Computer Technology and Development, Proceedings*, (ICCTD), 379–384. <https://doi.org/10.1109/ICCTD.2010.5645826>
- Tripathi, A., & Singh, U. K. (2012). Taxonomic Analysis of Classification Schemes in Vulnerability Databases. *2011 6Th International Conference on Computer Sciences and Convergence Information Technology (Iccit)*, 686–691.
- UNE-ISO GUIA 73, U.-I. G. 73:2010. (2010). *Gestión del riesgo. Vocabulario*. UNE:71504. (2008). *española*.
- US Department of Defense. (2019). *Cybersecurity Maturity Model Certification*. (Cmmc).
- US Department of Homeland Security. (2014). *Department of Homeland Security Cybersecurity Capability Maturity Model White Paper*. Retrieved from [file:///C:/Users/Marcelo/Downloads/Capability Maturity Model White Paper.pdf](file:///C:/Users/Marcelo/Downloads/Capability%20Maturity%20Model%20White%20Paper.pdf)
- von Känel, J., Cope, E. W., Deleris, L. A., Nayak, N., & Torok, R. G. (2010). Three key enablers to successful enterprise risk management. *IBM Journal of Research and Development*, 54(3), 231–245. <https://doi.org/10.1147/JRD.2010.2043973>
- Von Solms, S. H. B. (2015). A maturity model for part of the African Union Convention on Cyber Security. *Proceedings of the 2015 Science and Information Conference, SAI 2015*, 1316–1320. <https://doi.org/10.1109/SAI.2015.7237313>
- White, G. B. (2011). The community cyber security maturity model. *2011 IEEE International Conference on Technologies for Homeland Security, HST 2011*, 173–178. <https://doi.org/10.1109/THS.2011.6107866>
- Wielki, J. (2006). *A Framework of the Impact of Cyberspace on Contemporary Organizations*.
- Yahya, F., Walters, R. J., & Wills, G. B. (2015). Analysing threats in cloud storage. *2015 World Congress on Internet Security, WorldCIS 2015*, 44–48. <https://doi.org/10.1109/WorldCIS.2015.7359411>

- Yazid, A. I. S., Faizal, M. A., Rabiah, A., Shahrin, S., & Solahuddin, S. (2012). Enhancement of Asset value classification for Mobile devices. *Proceedings 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic, CyberSec 2012*, 106–110. <https://doi.org/10.1109/CyberSec.2012.6246097>
- Yu, Z., Thomborson, C., Wang, C., Fu, J., & Wang, J. (2009). A security model for VoIP steganography. *1st International Conference on Multimedia Information Networking and Security, MINES 2009, 1*, 35–40. <https://doi.org/10.1109/MINES.2009.227>
- Zhao, Z., & Dai, Y. (2012). A New Method of Vulnerability Taxonomy Based on Information Security Attributes. *2012 IEEE 12th International Conference on Computer and Information Technology*, 739–741. <https://doi.org/10.1109/CIT.2012.152>

ANEXOS

I. Procedimiento para realizar las revisiones sistemáticas

I.1. Introducción

El objetivo de este anexo es describir la guía para revisiones sistemáticas, esta guía está basada en las definiciones de (Kitchenham, 2004) (Kitchenham & Charters, 2007), la misma que se ha utilizado en las revisiones sistemáticas de esta tesis doctoral.

Una revisión sistemática es un medio de evaluar e interpretar toda la investigación disponible relevante para una pregunta de investigación particular, área temática o fenómeno de interés. Las revisiones sistemáticas tienen como objetivo presentar una evaluación justa de un tema de investigación mediante el uso de una metodología confiable, rigurosa y auditable.

La estructura de la guía es la siguiente:

- La sección 2 proporciona una introducción a las revisiones sistemáticas como un método de investigación significativo.
- La sección 3 especifica las etapas en una revisión sistemática.
- La sección 4 las observaciones finales.

I.2. Revisiones sistemáticas

Una revisión sistemática de la literatura es un medio para identificar, evaluar e interpretar toda la investigación disponible relevante para una pregunta de investigación en particular, un área temática o un fenómeno de interés. Los estudios individuales que contribuyen a una revisión sistemática se denominan estudios primarios.

I.2.1. Razones para realizar revisiones sistemáticas

Hay muchas razones para emprender una revisión sistemática. Las razones más comunes son:

- Para resumir la evidencia existente sobre un tratamiento o tecnología, por ejemplo, para resumir la evidencia empírica de los beneficios y limitaciones de un método ágil específico.
- Identificar las lagunas en la investigación actual para sugerir áreas para futuras investigaciones.
- Proporcionar un marco / antecedentes para posicionar adecuadamente nuevas actividades de investigación.

Sin embargo, también se pueden realizar revisiones sistemáticas para examinar en qué medida la evidencia empírica respalda / contradice las hipótesis teóricas, o incluso para ayudar a la generación de nuevas hipótesis.

I.2.2. La importancia de las revisiones sistemáticas

Una revisión sistemática sintetiza el trabajo existente de manera adecuada. Por ejemplo, las revisiones sistemáticas deben realizarse de acuerdo con una estrategia de búsqueda predefinida. La estrategia de búsqueda debe permitir evaluar la integridad de la búsqueda.

Su principal ventaja es que proporcionan información sobre los efectos de algún fenómeno en una amplia gama de entornos y métodos empíricos. Si los estudios dan resultados consistentes, las revisiones sistemáticas proporcionan evidencia de que el fenómeno es robusto y transferible. Si los estudios dan resultados inconsistentes, se pueden estudiar las fuentes de variación.

Una segunda ventaja, en el caso de los estudios cuantitativos, es que es posible combinar datos utilizando técnicas meta analíticas. Esto aumenta la probabilidad de detectar efectos reales que los estudios individuales más pequeños no pueden detectar. Sin embargo, el aumento de potencia también puede ser una desventaja, ya que es posible detectar pequeños sesgos y efectos reales.

1.3. El proceso de revisión

Una revisión sistemática involucra varias actividades discretas. Las pautas existentes para las revisiones sistemáticas tienen diferentes sugerencias sobre el número y el orden de las actividades. Este documento resume las actividades de una revisión sistemática de la siguiente manera:

- Identificación las necesidades para realizar la revisión sistemática.
- Proponer un protocolo de revisión.
- Llevar a cabo la revisión.
- Analizar e interpretar los resultados.
- Informar de los resultados.

A continuación, se describen las actividades identificadas.

1.3.1. La necesidad de una revisión sistemática

La necesidad de una revisión sistemática surge del requisito de los investigadores de resumir toda la información existente sobre algún fenómeno de manera exhaustiva e imparcial. Esto puede ser para sacar una conclusión más general sobre algún fenómeno de lo que es posible a partir de estudios individuales, o como un prelude para futuras actividades de investigación.

Antes de emprender una revisión sistemática, hay que asegurarse de que sea necesaria una revisión sistemática. Se deben identificar y revisar cualquier revisión sistemática existente del fenómeno de interés contra los criterios de evaluación apropiados. Se sugiere la siguiente lista de verificación:

- ¿Cuáles son los objetivos de la revisión?
- ¿Qué fuentes se buscaron para identificar estudios primarios? ¿Hubo alguna restricción?
- ¿Cuáles fueron los criterios de inclusión / exclusión y cómo se aplicaron?
- ¿Qué criterios se usaron para evaluar la calidad de los estudios primarios y cómo se aplicaron?
- ¿Cómo se extrajeron los datos de los estudios primarios?
- ¿Cómo se sintetizaron los datos? ¿Cómo se investigaron las diferencias entre los estudios? ¿Cómo se combinaron los datos? ¿Fue razonable combinar los estudios? ¿Las conclusiones fluyen de la evidencia?

En este apartado se debe describir las razones que nos lleva a realizar la revisión sistemática, indicando lo que se quiere desea conseguir.

1.3.2. Desarrollo de un protocolo de revisión

Un protocolo de revisión especifica los métodos que se utilizarán para llevar a cabo una revisión sistemática específica. Es necesario un protocolo predefinido para reducir la posibilidad de sesgo del investigador. Los componentes de un protocolo incluyen todos los elementos de la revisión, más información adicional de planificación.

En esta etapa se definen las normas que seguirá la investigación respecto del proceso de búsqueda en las fuentes de información definidas en el punto anterior. Deben ser definidos en el protocolo de búsqueda los términos que se buscarán, las combinaciones de éstos, la estrategia de búsqueda empleada según cada fuente y cómo se registrarán los resultados de cada búsqueda. Es recomendable registrar los resultados de las búsquedas. El protocolo puede ser mejorado en la

medida que se avanza con la revisión. Por ej., se pueden incorporar otros términos de búsqueda o realizar otras combinaciones de los términos usados.

A continuación, se describen los elementos del protocolo definido.

1.3.2.1 Formulación de la pregunta

Se plantea la problemática y las preguntas que están relacionadas con las necesidades y objetivos de la revisión.

1.3.2.1.1 Problema

Se plantea la problemática existente y la razón para elaborar la revisión sistemática. Se realiza una descripción de lo que se desea conseguir con la investigación planteada, para determinar las diferentes necesidades a ser cubiertas.

1.3.2.1.2 Preguntas

La actividad más importante durante el protocolo es formular la pregunta de investigación. El tema crítico en cualquier revisión sistemática es hacer la pregunta correcta. En este contexto, la pregunta correcta suele ser una que:

- Es significativa e importante tanto para los profesionales como para los investigadores.
- Conducirá a cambios en la práctica actual de ingeniería de software o a una mayor confianza en el valor de la práctica actual.
- Identifica las discrepancias entre las creencias comunes y la realidad.

Una pregunta debe considerar tres puntos de vista:

- La población, es decir, las personas afectadas por la intervención.
- Las intervenciones suelen ser una comparación entre dos o más tratamientos alternativos.
- Los resultados, es decir, los factores clínicos y económicos que se utilizarán para comparar las intervenciones.

Se describen las preguntas a responder en la revisión sistemática.

1.3.2.1.3 Población

Se determina el ámbito sobre el cual se va a realizar la búsqueda de los temas que están siendo analizados en la revisión sistemática. Una pregunta puede referirse a las publicaciones relacionadas con los modelos de madurez en ciberseguridad, gestión de seguridad en sistemas de información, y aplicaciones en las organizaciones. En ingeniería de software, se realizan estudios mucho menos primarios, por lo tanto, es posible que debamos evitar cualquier restricción en la población hasta que lleguemos a considerar las implicaciones prácticas de la revisión sistemática.

1.3.2.1.4 Intervención

La intervención hace referencia a la relación que tiene el tema de la revisión sistemática con el entorno en el cual es analizado. Por ejemplo, identificar los diferentes modelos de madurez en ciberseguridad y los principales utilizados en los estudios de investigación.

1.3.2.1.5 Efecto

La implicación que puede tener el tema a investigar en el área de análisis determinado, que incluye la incidencia y el impacto de lo que se está analizando. Por ejemplo, modelos de madurez en ciberseguridad y los principales utilizados en los estudios de investigación.

1.3.2.1.6 Medida del Resultado

Los resultados deben relacionarse con factores de importancia para los profesionales, como una mayor confiabilidad, manejo de frecuencia de utilización, menores costos de producción y menor tiempo de comercialización. Se deben especificar todos los resultados relevantes. Por ejemplo,

frecuencia de nombrado de los modelos de madurez en ciberseguridad en publicaciones por año de publicación.

Un problema particular para los experimentos de ingeniería de software es el uso de medidas sustitutas, por ejemplo, defectos encontrados durante las pruebas del sistema como un sustituto de la calidad o medidas de acoplamiento para la calidad del diseño. Los estudios que utilizan medidas sustitutivas pueden ser engañosos y las conclusiones basadas en tales estudios pueden ser menos sólidas.

I.3.2.1.7 Aplicación

Se debe determinar el área donde tiene aplicación el tema de investigación, determinando tendencias o áreas comunes de aplicación. Por ejemplo, conocer las investigaciones que hacen mención a los diferentes modelos de madurez en ciberseguridad y qué modelos son los más utilizados en los estudios de investigación, así como identificar las tendencias actuales de uso de dichos modelos.

I.3.2.2 Criterios para la selección de fuentes

Se deben establecer los criterios para la identificación y selección de las fuentes bibliográficas, y las bases de datos especializadas en las que se va a llevar a cabo la búsqueda de los estudios.

Los criterios para la selección se deben analizar de las siguientes fuentes:

- Bases de datos que incluyan revistas y artículos enfocados en modelos de madurez en ciberseguridad, sistemas de gestión de seguridad de la información, y la aplicación de los modelos de madurez en ciberseguridad en las organizaciones.
- Bases de datos que cuenten con mecanismos de búsqueda avanzada, haciendo uso de los términos y sinónimos usados en las preguntas de búsqueda.
- Disponibilidad del texto completo de los artículos.
- Artículos disponibles en la Web de forma gratuita.
- Revistas especializadas disponibles en la biblioteca de la Escuela Técnica Superior de Ingenieros Informáticos de la Universidad Politécnica de Madrid.
- Artículos en inglés o español.

I.3.2.3 Identificación de las fuentes

Del punto anterior se avalúan cuáles serían las fuentes de datos a ser consideradas y se los lista según lo definido. Las bases de datos deben ser seleccionadas tomando en consideración los términos que identifican las áreas de investigación.

Entre las fuentes seleccionadas se pueden considerar las bases de datos especializadas, un ejemplo puede ser: IEEE Computer, Science Direct, SpringerLink, Institute for Scientific Information (ISI) web of knowledge.

I.3.2.4 4) Cadena de búsqueda

Es necesario determinar y seguir una estrategia de búsqueda. Las estrategias de búsqueda suelen ser iterativas y se benefician de:

- Las búsquedas preliminares tenían como objetivo identificar las revisiones sistemáticas existentes y evaluar el volumen de estudios potencialmente relevantes.
- Buscadores de prueba que utilizan varias combinaciones de términos de búsqueda derivados de la pregunta de investigación.
- Revisiones de resultados de investigaciones.
- Consultas con expertos en la materia.

Un enfoque general es dividir la pregunta en facetas individuales, es decir, población, intervención, resultados, diseños de estudio. Luego elabore una lista de sinónimos, abreviaturas y ortografías alternativas. Las cadenas de búsqueda sofisticadas se pueden construir utilizando los conectores booleanos AND y OR.

Las búsquedas iniciales de estudios primarios se realizan sobre las fuentes identificadas anteriormente, pero si no es suficiente, también se deben buscar otras fuentes de evidencia (a veces manualmente) que incluyen:

- Listas de referencias de estudios primarios relevantes y artículos de revisión.
- Revistas (incluidas revistas de la empresa especializadas), literatura gris (es decir, informes técnicos, trabajos en curso) y actas de congresos.
- Registros de investigación.
- Internet.

Los términos en la revisión sistemática deben ser construidos utilizando los criterios que permitan responder a las preguntas elaboradas. Por ejemplo, construidos usando los siguientes criterios: (1) “capability maturity model for cybersecurity”, deduciendo los principales términos o palabras claves de las preguntas para identificar la población, intervención y resultados esperados, (2) “capability maturity model for information security management system” identificando las palabras alternativas y sinónimos de los términos principales y también (3) “capability maturity model for cybersecurity applied in organizations”. Estas palabras claves combinadas con los operadores lógicos AND (para enlazar términos de población, intervención y efecto) y OR (para incorporar palabras alternativas y sinónimos), así como el operador NOT para refinar la búsqueda, se utilizaron en los motores de búsquedas de las bases de datos especializadas.

Las palabras usadas en la cadena de búsqueda, por ejemplo, incluyen: “maturity model”, “cybersecurity”, “capability”, “information security management system”, “organizations”.

1.3.2.5 Búsqueda en las fuentes

Se realiza la búsqueda en las fuentes determinadas usando los criterios definidos para su selección. Se incluyen todas las fuentes de bases de datos identificadas. Se aplican las cadenas de búsqueda en las bases de datos electrónicas y en las otras fuentes (revistas y conferencias). En caso de requerirlo de debe contar con la participación de expertos en el tema y área de investigación, para evaluar la lista de fuentes obtenidas.

También pueden existir el sesgo de publicación, el cual se refiere al problema de que es más probable que se publiquen resultados positivos que resultados negativos. El concepto de resultados positivos o negativos a veces depende del punto de vista del investigador. Sin embargo, el sesgo de publicación sigue siendo un problema, particularmente para los experimentos formales, donde el hecho de no rechazar la hipótesis nula se considera menos interesante que un experimento que puede rechazar la hipótesis nula.

El sesgo de publicación puede conducir a un sesgo sistemático en las revisiones sistemáticas a menos que se realicen esfuerzos especiales para abordar este problema. Muchas de las estrategias de búsqueda estándar identificadas anteriormente se utilizan para abordar este problema, incluyendo:

- Escaneando la literatura gris.
- Escaneo de actas de congresos.
- Contactando a expertos e investigadores que trabajan en el área y preguntándoles si conocen algún resultado no publicado.

Además, se pueden usar técnicas de análisis estadístico para identificar la importancia potencial del sesgo de publicación.

I.3.3. Revisión

En este punto se muestra la búsqueda realizada de los artículos en las bases de datos seleccionadas con las cadenas de búsquedas predefinidas. Al resultado de las búsquedas se debe aplicar los criterios de inclusión y exclusión. Por ejemplo, como los definidos en la Tabla I-1.

El objetivo de una revisión sistemática es encontrar tantos estudios primarios relacionados con la pregunta de investigación como sea posible utilizando una estrategia de búsqueda imparcial. Por ejemplo, es necesario evitar el sesgo del idioma. El rigor del proceso de búsqueda es un factor que distingue las revisiones sistemáticas de las revisiones tradicionales.

El proceso de realizar una revisión sistemática debe ser transparente y replicable:

- La revisión debe documentarse con suficiente detalle para que los lectores puedan evaluar la minuciosidad de la búsqueda.
- La búsqueda debe documentarse a medida que ocurre y los cambios anotados y justificados.
- Los resultados de búsqueda sin filtrar deben guardarse y conservarse para un posible nuevo análisis.

Una vez que se han obtenido los estudios primarios potencialmente relevantes, deben evaluarse para determinar su relevancia real.

I.3.3.1 Criterios de selección de estudios

Los criterios de selección de estudios están destinados a identificar aquellos estudios primarios que proporcionan evidencia directa sobre la pregunta de investigación. Para reducir la probabilidad de sesgo, los criterios de selección deben decidirse durante la definición del protocolo según Tabla I-1.

Los criterios de inclusión y exclusión deben basarse en la pregunta de investigación. Deben ponerse a prueba para garantizar que puedan ser interpretados de manera confiable y que clasifiquen los estudios correctamente.

En una primera fase de la revisión sistemática, haciendo uso de los motores de búsqueda de las bases de datos identificadas y poniendo la cadena de búsqueda elaborada en el protocolo de revisión se identifican los estudios que cumplen con las condiciones definidas, algunas cuestiones a considerar son:

- Es importante evitar, en la medida de lo posible, las exclusiones basadas en el lenguaje del estudio primario.
- Es posible que las decisiones de inclusión se vean afectadas por el conocimiento de los autores, las instituciones, las revistas o el año de publicación.

Tabla I-1. Criterios de Inclusión y Exclusión

<i>Inclusión (I)</i>	<i>Exclusión (E)</i>
I1. Estudios empíricos. I2. Artículos que hablan sobre el tema a investigar y elementos afines. I3. Artículos que utilizan las palabras claves. I4. Artículos cuyo título, resumen o contenido está relacionado con el tema.	E1. Artículos que están basados sólo en una opinión particular que no aborde el tema de investigación. E2. Artículos cortos. E3. Estudios que no son relevantes para las preguntas de investigación o no están relacionados con el estudio en particular. E4. Estudios que no son claros o presentan ambigüedad. E5. Publicaciones duplicadas. E6 Estudios anteriores a determinado año, según la actualización del tema.

En una segunda fase, se revisan cada uno de los estudios tomando en consideración los criterios de inclusión y exclusión anteriormente definidos, obteniendo el total de estudios relevantes. Para seleccionar los estudios relevantes, se deben seguir los siguientes pasos:

- Paso 1. Leer el título. Si éste proporciona suficiente información, el estudio es seleccionado y guardado. Si no proporciona suficiente información, se realiza el paso 2.
- Paso 2. Leer el resumen del artículo. Si éste proporciona suficiente información, el estudio es seleccionado y guardado. Si no proporciona información o existe la evidencia de que no pueda estar relacionado con el tema, se realiza el paso 3.
- Paso 3. Leer las conclusiones. Si éstas proporcionan suficiente información, el estudio es seleccionado y guardado. En caso contrario se elimina.

En una tercera fase, se obtienen los estudios primarios que respondan a las preguntas formuladas inicialmente. La Tabla I-2 muestra en primera instancia las fuentes, el número total de artículos y el número de artículos primarios seleccionados por fuente.

Las decisiones finales de inclusión / exclusión deben tomarse después de que se hayan recuperado los textos completos. Es útil mantener una lista de estudios excluidos que identifiquen el motivo de la exclusión.

Tabla I-2. Distribución de los estudios por fuente.

<i>Fuente</i>	<i>Total</i>	<i>Primarios</i>
Fuente 1	86	6
Fuente 2	75	8

1.3.3.2 Estudio de evaluación de calidad

Además, para los criterios generales de inclusión y exclusión, generalmente se considera importante evaluar la "calidad" de los estudios primarios, para evaluar la calidad de los estudios, se deben realizar las siguientes preguntas:

- ¿Es el estudio primario relevante para la investigación que se está realizando?
- ¿Los estudios primarios proveen la suficiente información como para que los resultados se beneficien de la revisión sistemática?
- ¿Los estudios revisados dan un valor agregado a la investigación que se está realizando?

Una dificultad inicial es que no existe una definición acordada de "calidad" del estudio. Sin embargo, se sugiere que la calidad se relaciona con la medida en que el estudio minimiza el sesgo y maximiza la validez interna y externa según lo determina la Tabla I-3.

Tabla I-3. Definiciones del concepto de calidad

<i>Término</i>	<i>Sinónimos</i>	<i>Definición</i>
Parcialidad	Error sistemático	Una tendencia a producir resultados que parten sistemáticamente de los resultados "verdaderos". Los resultados imparciales son válidos internamente
Validez interna	Validez	Es probable que el diseño y la realización del estudio eviten errores sistemáticos. La validez interna es un prerrequisito para la validez externa.
Validez externa	Generalización, Aplicabilidad	La medida en que los efectos observados en el estudio son aplicables fuera del estudio.

1.3.3 Extracción de datos y síntesis

El objetivo de esta etapa es diseñar formularios de extracción de datos para registrar con precisión la información que los investigadores obtienen de los estudios primarios. Para reducir la posibilidad de sesgo, los formularios de extracción de datos deben definirse y ponerse a prueba cuando se define el protocolo del estudio.

Los formularios de extracción de datos deben estar diseñados para recopilar toda la información necesaria para abordar las preguntas de revisión y los criterios de calidad del estudio. También deben recopilar todos los elementos de datos especificados en la sección de estrategia de síntesis de revisión del protocolo.

Para extraer la información importante de cada artículo, se debe llenar en el formulario diseñado. El formulario contiene los siguientes campos: (1) identificación del artículo, (2) bibliografía (título, autor, año), (3) tipo de artículo (caso de estudio, encuesta, experimento, investigación), (4) objetivo del estudio, (5) contexto en que se desarrolla el estudio, (6) tipo de estudio (mejora, despliegue o ambos), (7) nivel de profundidad del análisis (alto, medio, bajo), (8) tema analizado en la revisión sistemática, (9) frecuencia de nombrado, y (10) conclusiones.

Por cada artículo seleccionado, después de leerse el texto completo, se debe registrar la información en el formulario, el cual permite realizar un análisis posterior a los resultados. Los campos 8 y 9 resumen los aspectos que responden a la pregunta planteada y las conclusiones que presenta el estudio.

1.3.4. Analizar e interpretar los resultados

El análisis de datos implica recopilar y resumir los resultados de los estudios primarios incluidos. La síntesis puede ser descriptiva (no cuantitativa). Sin embargo, a veces es posible complementar una síntesis descriptiva con un resumen cuantitativo. El uso de técnicas estadísticas para obtener una síntesis cuantitativa se denomina metaanálisis.

La información extraída sobre los estudios (es decir, intervención, población, contexto, tamaños de muestra, resultados, calidad del estudio) debe tabularse de manera coherente con la pregunta de revisión. Las tablas deben estructurarse para resaltar las similitudes y diferencias entre los resultados del estudio.

Los resultados se deben resumir y analizar. En el análisis, se usan herramientas estadísticas para determinar valores cuantitativos. Para realizar el resumen, los estudios deben ser clasificados en estudios relacionados con los criterios tomados de la cadena de búsqueda. También se puede presentar los artículos que contienen casos de estudio, experimentos, encuestas, presentados a continuación y clasificados de acuerdo a los criterios definidos por (Petersen, Feldt, Mujtaba, & Mattsson, 2008), y la clasificación se puede realizar como se muestra en la Tabla I-4.

Tabla I-4. Estudios Clasificados en base a la categorización de Petersen

<i>Clasificación</i>	<i>Referencia</i>
Propuestas de solución	[6], [8], [12]
Búsquedas de evaluación	[7], [9], [10], [15]
Artículos de opinión	[11], [16], [17]
Artículos de experiencia	[13]
Artículos filosóficos	[14]

I.3.5. Informar la revisión

Es importante comunicar los resultados de una revisión sistemática de manera efectiva. Por lo general, las revisiones sistemáticas se informarán en al menos dos formatos:

- En un informe técnico o en una sección de una tesis doctoral.
- En un diario o documento de conferencia.

Un diario o documento de conferencia normalmente tendrá una restricción de tamaño. Con el fin de garantizar que los lectores puedan evaluar adecuadamente el rigor y la validez de una revisión sistemática, los artículos de revistas deben hacer referencia a un informe técnico o tesis que contenga todos los detalles.

Además, las revisiones sistemáticas con resultados prácticos importantes pueden resumirse en artículos no técnicos en revistas profesionales, en comunicados de prensa y en páginas web. Por ejemplo, del análisis realizado de los modelos de madurez en ciberseguridad para implementarlos en la industria, se observó lo siguiente:

- “C2M2” Cybersecurity Capability Maturity Model. Es un modelo que está enfocado a ciberseguridad y que debido a su importancia se crearon dos variantes, una para el sector energético [6], [7], [8], y otra para el sector de gas y combustibles [7] de los Estados Unidos de Norteamérica [17].

Como se observa en el ejemplo previo, al informar los resultados de la revisión sistemática, se coloca los resultados encontrados para ser utilizados posteriormente como referencias de información.

I.4. Observaciones finales

En esta guía se ha presentado un conjunto de pautas para planificar la realización y el informe de una revisión sistemática. Las pautas se basan en pautas utilizadas en la investigación médica. Sin embargo, es importante reconocer que la investigación en ingeniería de software no es lo mismo que la investigación médica. Esta guía ha sido utilizada en todas las revisiones sistemáticas realizadas en esta tesis doctoral.

Finalmente, estas pautas están destinadas a ayudar en la realización de las revisiones sistemáticas de esta tesis doctoral. Sin embargo, muchos de los pasos en una revisión sistemática suponen que será realizada por un gran grupo de investigadores. En el caso de una sola investigación (como un estudiante de doctorado), se definió que los pasos más importantes a seguir son:

- Desarrollando un protocolo.
- Definiendo la pregunta de investigación.
- Especificando qué se hará para abordar el problema de un solo investigador que aplica criterios de inclusión / exclusión y realiza toda la extracción de datos.
- Definiendo la estrategia de búsqueda.
- Definir los datos que se extraerán de cada estudio primario, incluidos los datos de calidad.
- Mantener listas de estudios incluidos y excluidos.
- Utilizando las pautas de síntesis de datos.
- Usando las pautas de informes.

II. Taxonomías de Elementos de Ciberseguridad

II.1. Introducción

El objetivo de este anexo es describir los catálogos de los elementos que participan en el modelo conceptual. Para ello, se han definido las taxonomías de estos elementos, que fueron descritos en el capítulo 2 de esta tesis doctoral, se define la taxonomía de tipos de activos de la organización enfocados en ciberseguridad en base al estándar ISO 27005 (ISO/IEC 27000, 2018), la taxonomía de Vulnerabilidades en ciberseguridad en base al estándar ISO 27005 y se establece la taxonomía de Amenazas en ciberseguridad en base al estándar ENISA 2016 (Marinos, 2016).

II.2. Definición

Etimológicamente hablando, *taxonomía* procede de los términos griegos “*taxis*”, ordenación, y “*nomos*”, norma. Los principios que proporcionaban una guía rigurosa para la construcción de taxonomías eran la base lógica, la observación empírica, la estructura jerárquica basada en la herencia de propiedades, la historia evolutiva y la utilidad pragmática. Las fuentes terminológicas de la lengua general todavía recogen el significado especialmente orientado al entorno de las ciencias experimentales.

Aplicando el principio etimológico, la taxonomía se ha definido como la ciencia que trata de los principios, métodos y fines de la clasificación, y procura la organización jerarquizada y sistemática, dando nombres a grupos de elementos y a los elementos mismos.

II.3. Taxonomías descritas

Se han definido las taxonomías de estos elementos, las cuales son el resultado de las revisiones sistemáticas realizadas en el capítulo 2. Las taxonomías definidas se describen a continuación:

- Se define la taxonomía de tipos de activos de la organización enfocados en ciberseguridad en base al estándar ISO 27005.
- Se determina la taxonomía de Vulnerabilidades en ciberseguridad en base al estándar ISO 27005.
- Se establece la taxonomía de Amenazas en ciberseguridad en base al estándar ENISA 2016.

A continuación, se describen las taxonomías utilizadas.

II.3.1. Tipos de Activos

Basada en el estándar ISO 27005.

Tabla II-1. Tipos de Activos

TIPO DE ACTIVO
Procesos y actividades de negocios
Información
Hardware
Software
Red
Personal

<i>TIPO DE ACTIVO</i>
Sitio
Estructura de la organización

II.3.2. Vulnerabilidades

Basada en el estándar ISO 27005.

Tabla II-2. Taxonomía de Vulnerabilidades

<i>VULNERABILIDADES (ISO 27005)</i>
***** Hardware *****
Mantenimiento insuficiente / instalación defectuosa de medios de almacenamiento
Falta de esquemas de reemplazo periódicos.
Susceptibilidad a la humedad, polvo, suciedad.
Sensibilidad a la radiación electromagnética.
Falta de control de cambio de configuración eficiente
Susceptibilidad a las variaciones de tensión.
Susceptibilidad a las variaciones de temperatura.
Almacenamiento no protegido
Falta de cuidados a eliminación desechos
Copia incontrolada
No posee mecanismo de respaldo
No posee alta disponibilidad
Falta de mecanismo de redundancia
Mantenimiento insuficiente / instalación defectuosa
Falta de precaución en las conexiones físicas
Falta de esquema de ampliar capacidad
Falla de equipos dependientes
Fallo de los componentes
Obsolescencia del Hardware
***** Software *****
Pruebas de software inexistentes o insuficientes
Errores conocidos en el software.
No 'logout' al salir de la estación de trabajo
Eliminación o reutilización de medios de almacenamiento sin el correcto borrado

<i>VULNERABILIDADES (ISO 27005)</i>
Falta de pista de auditoria
Asignación errónea de derechos de acceso
Software de amplia distribución
Aplicando programas de aplicación a los datos incorrectos en términos de tiempo.
Interfaz de usuario complicada
Falta de documentación técnica
Configuración incorrecta de parámetros
Fechas incorrectas
Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.
Tablas de contraseñas no protegidas
Mala gestión de contraseñas
Servicios innecesarios habilitados
Software inmaduro o nuevo
Especificaciones poco claras o incompletas para desarrolladores
Falta de control efectivo del cambio
Descarga incontrolada y uso de software.
Falta de copias de respaldo
Falta de protección física del edificio, puertas y ventanas.
No se producen informes de gestión
No posee un procedimiento de respaldo
Obsolescencia del Software
Presenta errores lógicos el software
Inexistente ambiente de pruebas
No cuenta con mecanismos contra ataques informáticos
***** Red *****
Falta de comprobante de envío o recepción de un mensaje.
Líneas de comunicación desprotegidas.
Tráfico sensible no protegido
Presenta cableado deficiente
Punto único de fallo
Falta de identificación y autenticación del remitente y receptor.
Arquitectura de red insegura
Transferencia de contraseñas en claro

<i>VULNERABILIDADES (ISO 27005)</i>
Gestión inadecuada de la red (resistencia de enrutamiento)
Conexiones de red pública sin protección.
Gestión inadecuado del accesos a Internet en las unidades de gestión
Intermitencia en el tráfico de la red
Falla de enlaces externos-terceros
***** Personal *****
Ausencia de personal
Procedimientos de reclutamiento inadecuados.
Capacitación de seguridad insuficiente
Uso incorrecto de software y hardware
Falta de conciencia de seguridad
Falta de mecanismos de seguimiento.
Trabajo no supervisado por personal externo o de limpieza.
Falta de políticas para el uso correcto de los medios de comunicación y mensajería de telecomunicaciones.
Falta de capacitación en la administración del activo
No existe la divulgación adecuada del expertise adquirido
***** Sitio *****
Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones
Ubicación en un área susceptible a inundaciones.
Red eléctrica inestable
Falta de protección física del edificio, puertas y ventanas.
Susceptible a incendios y altas temperaturas
Espacio físico designado no reúne condiciones técnicas
Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio
***** Organización *****
Falta de trámite formal de registro de uso y anulación de registro.
Falta de proceso formal para la revisión de los derechos de acceso (supervisión)
Falta o insuficiente de las disposiciones (relativas a la seguridad) en los contratos con clientes y / o terceros
Falta de procedimiento de monitoreo de las instalaciones de procesamiento de información.
Falta de auditorías regulares (supervisión)
Falta de procedimientos de identificación y evaluación de riesgos.
Informes de falta de fallas registrados por el administrador y los registros del operador
Servicio inadecuado respuesta de mantenimiento

<i>VULNERABILIDADES (ISO 27005)</i>
Falta o falta de acuerdo de nivel de servicio
Falta de procedimiento de control de cambios.
Falta de procedimiento formal para el control de la documentación del SGSI.
Falta de procedimiento formal para la supervisión del registro del SGSI.
Falta de un proceso formal para la autorización de la información pública disponible.
Falta de asignación adecuada de las responsabilidades de seguridad de la información.
Falta de planes de continuidad.
Falta de política de uso del correo electrónico
Falta de procedimientos para introducir software en sistemas operativos.
Falta de registros en los registros de administrador y operador.
Falta de procedimientos para el manejo de información clasificada.
Falta de responsabilidades de seguridad de la información en las descripciones de los puestos.
Falta o insuficiencia de disposiciones (en materia de seguridad) seguridad de la información) en contratos con empleados
Falta de proceso disciplinario definido en caso de incidente de seguridad de la información.
Falta de política formal sobre el uso de computadoras móviles
Falta de control de los activos fuera de las instalaciones
Falta o insuficiente política de 'limpiar escritorio y pantalla'
Falta de autorización para el procesamiento de la información.
Falta de mecanismos de monitoreo establecidos para violaciones de seguridad.
La falta de revisiones de gestión regulares
Falta de procedimientos para reportar debilidades de seguridad.
Falta de procedimientos de cumplimiento de los derechos de propiedad intelectual.
Falta socialización de políticas internas y externas
Falta de política formal de cambio de credenciales
Falta de gestión en la disponibilidad de repuestos de equipos críticos
Falta de políticas internas de gestión y cumplimiento
Falta de garantía técnica de los equipos
Falta de licenciamiento vigente
Falta de planes de recuperación
Falta de planes de contingencia
Falta de soporte preventivo y correctivo
Falta de mantenimiento y/o actualizaciones

<i>VULNERABILIDADES (ISO 27005)</i>
Falta de planes de crecimiento y expansión de servicios de TI

II.3.3. Amenazas

Basada en el estándar ENISA 2016.

Tabla II-3. Taxonomía de Amenazas

<i>AMENAZAS (ENISA)</i>
*****Ataque físico (deliberado / intencional) *****
Fraude extorsión
Sabotaje
Vandalismo
Robo (dispositivos, medios de almacenamiento y documentos)
Fuga de información / intercambio
Acceso físico no autorizado / Entrada no autorizada a las instalaciones
Coerción, o corrupción
Daños de la guerra
Ataque terrorista
***** Daños involuntarios / pérdida de información o activos de TI *****
Fuga de información / intercambio debido a un error humano
Uso erróneo o administración de dispositivos y sistemas
Usando información de una fuente no confiable
Cambio involuntario de datos en un sistema de información
Diseño y planificación inadecuados o adaptación inadecuada
Daños causados por un tercero
Daños resultantes de las pruebas de penetración
Pérdida de información en la nube
Pérdida de (integridad de) información sensible
Pérdida de dispositivos, medios de almacenamiento y documentos
Destrucción de registros
***** Desastres (naturales, ambientales) *****
Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)
Fuego
Contaminación, polvo, corrosión

AMENAZAS (ENISA)
Golpe de trueno
Agua
Explosión
Fuga de radiación peligrosa
Condiciones climáticas desfavorables
Grandes eventos en el medio ambiente
Amenazas desde el espacio / Tormenta electromagnética
Fauna silvestre
***** Fallos / Mal funcionamiento *****
Fallo de dispositivos o sistemas
Fallo o interrupción de los enlaces de comunicación (redes de comunicación)
Fallo o interrupción del suministro principal
Fallo o interrupción de los proveedores de servicios (cadena de suministro)
Mal funcionamiento de los equipos (dispositivos o sistemas)
<i>Fallo de software /aplicaciones o servicio</i>
***** Cortes de Luz *****
Pérdida de recursos
Ausencia de personal
Huelga
Pérdida de servicios de apoyo
Corte de internet
Caída de la red
***** Escuchas / Interceptación / Secuestro *****
Conducción de guerra
Interceptando emisiones comprometedoras
Intercepción de la información
Radiación interferente
Repetición de mensajes
Reconocimiento de redes, manipulación de tráfico de redes y recopilación de información
Hombre en el medio / secuestro de sesión
***** Actividad/Abuso nefasto *****
Robo de identidad (Fraude de identidad / Cuenta)
Recepción de correos electrónicos no solicitados

<i>AMENAZAS (ENISA)</i>
Negación de servicio
Código malicioso / software / actividad
Ingeniería social
Abuso de la fuga de información
Generación y uso de certificados deshonestos
Manipulación de hardware y software
Manipulación de la información
Mal uso de las herramientas de auditoría
Uso indebido de los sistemas de información / información (incluidas las aplicaciones móviles)
Actividades no autorizadas
Instalación no autorizada de software
Comprometiendo información confidencial (violaciones de datos)
Farsa
Actividad remota (ejecución)
Ataques dirigidos (APTs, etc.)
Fallo de proceso de negocio
Fuerza bruta
Abuso de autorizaciones
***** <i>legal</i> *****
Violación de leyes o reglamentos / incumplimiento de la legislación
Incumplimiento de los requisitos contractuales
Uso no autorizado de recursos protegidos por derechos de propiedad intelectual
Abuso de datos personales
Decisiones judiciales / órdenes judiciales

II.4. Observaciones finales

En esta guía se ha presentado las taxonomías utilizadas en el capítulo 5 de experimentación, estas taxonomías, han sido tomadas como base y han sido utilizadas en la en la etapa de experimentación, también se han incluido nuevos elementos a la taxonomía según las necesidades de la empresa donde se ha realizado al experimentación, lo que permite tener unas taxonomías con mayor cobertura, lo que ratifica que se irán actualizando continuamente, debido al avance de la tecnología y las necesidades de la industria.

III. Línea Base Inicial de Análisis de Riesgos de la Dirección Nacional de Tecnología de la Información - IESS

III.1. Introducción

En el presente informe se presentan los resultados del análisis y evaluación de riesgos de los activos de ciberseguridad del Instituto Ecuatoriano de Seguridad Social (IESS), que son administrados por la Dirección Nacional de Tecnología de la Información (DNTI), los mismos que serán la línea base del trabajo experimental de esta tesis doctoral, para ello se ha seguido las directrices existentes en la institución que están basadas en la norma (ISO/IEC 27000, 2018) y la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT (Amutio Gómez, 2012).

El análisis, evaluación y gestión de riesgos consiste en un proceso continuo para identificar, controlar y eliminar o minimizar eventos inciertos que puedan afectar los recursos de la tecnología de la información (TI), pues la información de una organización, aplicaciones y redes que la respaldan son activos importantes. La confidencialidad, integridad y disponibilidad de los activos pueden ser esenciales para mantener la ventaja competitiva, rentabilidad, cumplimiento legal e imagen del IESS.

III.2. Objetivo

Determinar los riesgos sobre los equipos de la plataforma AS400-IESS, Host-IESS, Oracle-IESS y Firewall-IESS que operan en el Instituto Ecuatoriano de Seguridad Social, mediante la identificación y valoración de sus activos, amenazas y vulnerabilidades, para determinar el nivel de riesgos de dichos activos.

III.3. Justificación

Considerando que el análisis y evaluación de riesgos es competencia de la Subdirección Nacional de Seguridad Informática según la Resolución C.D: 535, se hace necesario contar con una línea base de riesgos que permita identificar, evaluar y responder a los riesgos de los activos críticos, tomando en cuenta las siguientes consideraciones:

- Los equipos de la plataforma AS400 – IESS son un activo crítico e importante para la organización, ya que en dichos equipos se lleva el Sistema Médico del HCAM (Hospital Carlos Andrade Marín), por lo que es sumamente importante que exista alta disponibilidad de dicha plataforma en virtud de que los aplicativos de Historia Laboral requieren información de dicha plataforma para proporcionar varias prestaciones y servicios a los asegurados.
- Los equipos de la plataforma Host – IESS son un activo crítico e importante para la organización, ya que en dichos equipos se ejecutan transacciones que aún no se han migrado al sistema de Historia Laboral, por lo que es sumamente importante que exista alta disponibilidad de dicha plataforma en virtud de que los aplicativos de Historia Laboral requieren información de dicha plataforma para proporcionar las prestaciones y servicios a los asegurados.
- El hardware y software de la plataforma Oracle – IESS son un activo crítico e importante para la organización, ya que permite brindar servicios de base de datos a los sistemas especializados del IESS, y la disponibilidad necesaria para proporcionar las prestaciones y servicios a los asegurados.

- Los equipos de la plataforma Firewall – IESS son un activo crítico e importante para la organización, ya que permite proteger las redes del IESS mediante el monitoreo y la aplicación de políticas de seguridad, determinando qué servicios de la red pueden estar disponibles y quienes pueden utilizar estos recursos, manteniendo al margen a los usuarios no autorizados y en caso de un ataque genera alarmas de seguridad.

Por consiguiente, se realiza un análisis de riesgos donde se sugieran salvaguardas para minimizar los riesgos de dichos activos.

III.4. Alcance

Las plataformas de la DNTI que han sido consideradas para el análisis y evaluación de riesgos de los activos de ciberseguridad son las siguientes:

- La plataforma AS400 – IESS del Hospital Carlos Andrade Marín (HCAM) y sus activos directamente dependientes.
- La plataforma Host – IESS.
- La Plataforma Oracle – IESS.
- Plataforma Firewall – IESS y sus activos directamente dependientes.

Se han analizado los riesgos de los equipos de las plataformas definidas anteriormente y sus dependientes mediante:

- Identificación de los equipos de la plataforma definida y sus equipos dependientes.
- Valoración de activos considerando tres dimensiones: disponibilidad, integridad y confidencialidad.
- Identificación y valoración de las amenazas y vulnerabilidades sobre dichos equipos.
- Evaluación del impacto y frecuencia de los escenarios de riesgos identificados.
- Cálculo del riesgo total.
- Propuesta de controles o salvaguardas.

También se tuvo como referencia las normas y metodologías definidas por la DNTI para estas actividades, que son las siguientes:

- Metodología de gestión de riesgos de MAGERIT v3.0.
- Metodología de gestión de riesgos RISK IT de ISACA.
- Normas de control interno de la Contraloría General del Estado (300, Evaluación del Riesgo).

III.5. Actividades realizadas

En esta sección se describen las actividades que se han realizado para cada una de las plataformas definidas, así como se describe los parámetros utilizados para el análisis y evaluación de riesgos de los activos de ciberseguridad de las plataformas gestionadas por la DNTI.

III.5.1. Valoración de los Activos

La valoración de los activos se ha realizado considerando las tres dimensiones de seguridad informática que son: Confidencialidad, Integridad y Disponibilidad, según los lineamientos definidos.

- **Confidencialidad:** que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es

diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.

- **Integridad:** mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una organización.
- **Disponibilidad:** disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

Además, se incluye otro criterio calculado que se describe a continuación:

- **Críticidad:** determina la importancia que tiene el activo en la organización y describe el cuidado que se debe tener sobre el mismo.

Las escalas utilizadas para la valoración se detallan a continuación (Tabla III-1):

Tabla III-1. Criterios de valoración Confidencialidad, Integridad, Disponibilidad y Criticidad

Criterio de valoración CONFIDENCIALIDAD		
¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?		
Alta (A)	3	Información que puede ser conocida y utilizada por un grupo muy reducido de agentes, cuya divulgación podría ocasionar un perjuicio al IESS o terceros.
Media (M)	2	Información que solo puede ser conocida y utilizada por un grupo de agentes, que la necesiten para realizar su trabajo.
Baja (B)	1	Información que puede ser conocida y utilizada por todos los agentes del IESS.
Nula (N)	0	Información que puede ser conocida y utilizada sin autorización por cualquier persona, dentro o fuera del IESS.
Criterio de valoración INTEGRIDAD		
¿Qué importancia tendría que los datos fueran modificados fuera de control?		
Alta (A)	3	Información cuya modificación no autorizada no podría repararse, impidiendo la realización de las actividades.
Media (M)	2	Información cuya modificación no autorizada es de difícil reparación y podría ocasionar un perjuicio significativo para el IESS o terceros.
Baja (B)	1	Información cuya modificación no autorizada puede repararse, aunque podría ocasionar un perjuicio para el IESS o terceros.
Nula (N)	0	Información cuya modificación no autorizada puede repararse fácilmente, o no afecta a las actividades del IESS.
Criterio de valoración DISPONIBILIDAD		
¿Qué importancia tendría que el activo no estuviera disponible?		
Alta (A)	3	Información cuya inaccesibilidad permanente durante una hora podría impedir la ejecución de las actividades del IESS.
Media (M)	2	Información cuya inaccesibilidad permanente durante la jornada laboral podría impedir la ejecución de las actividades del IESS.

Baja (B)	1	Información cuya inaccesibilidad permanente durante una semana podría ocasionar un perjuicio significativo para el IESS.
Nula (N)	0	Información cuya inaccesibilidad no afecta la actividad normal del IESS.
Criterio de valoración CRITICIDAD		
Valor máximo de las tres características D.I.C.		
Alta (A)	3	Si el máximo es 3.
Media (M)	2	Si el máximo es 2.
Baja (B)	1	Si el máximo es 1.
Nula (N)	0	Si todos son 0.

III.5.2. Valoración del Impacto

Para cada activo y amenaza es necesario estimar la degradación, es decir el porcentaje en que la amenaza daña al activo en estudio, estableciendo un valor entre 0% (no lo daña) y el 100% (lo daña absolutamente) para cada una de las características de confidencialidad, integridad y disponibilidad.

- **Degradación (Confidencialidad):** la confidencialidad hace referencia a la protección de la información contra la divulgación no autorizada. El impacto producido por un evento de estas características, sea en forma no autorizada, intencional o inadvertida, puede variar entre la pérdida de confianza en la institución hasta la posibilidad de acciones legales contra la misma.
- **Degradación (Integridad):** se refiere al requerimiento de que el activo o la información sea protegido contra la modificación no autorizada. Se pierde integridad si se realizan cambios no autorizados en los sistemas o se pierde parte de los datos almacenados, sea por un evento accidental o intencionado.
- **Degradación (Disponibilidad):** el hecho de que la información o un sistema no esté disponible para sus usuarios, ya sea por la pérdida de datos o la destrucción de elementos necesarios, puede afectar a la efectividad operacional y, consecuentemente, al cumplimiento de la misión de una organización.

El **impacto** se calcula en base al máximo valor de degradación que la amenaza produce sobre un activo definido anteriormente. Si un activo tiene una degradación alta en cualquier dimensión de seguridad, su criticidad también será alta.

III.5.3. Valoración del Riesgo

En la valoración del riesgo se establece el nivel de riesgo que cada amenaza ocasiona sobre el activo, y se establece mediante la identificación de la frecuencia de que ocurra el evento y el impacto (pérdidas y daños), que el evento produce sobre los activos.

Los criterios utilizados para la calificación de la frecuencia son los descritos en la Tabla III-2:

Tabla III-2. Criterios de valoración frecuencia

Criterio de valoración FRECUENCIA		
Frecuencia con la que ocurre o puede ocurrir dicho evento		
Alta (A)	3	A diario

Criterio de valoración FRECUENCIA		
Frecuencia con la que ocurre o puede ocurrir dicho evento		
Media (M)	2	Mensualmente
Baja (B)	1	1 vez al año
Nula (N)	0,1	Cada varios años

El cálculo del riesgo se realiza multiplicando la Frecuencia por el Impacto:

Riesgo = Frecuencia x Impacto, y se puede ver gráficamente más adelante en las Tablas: Tabla III-4, Tabla III-8, Tabla III-12, Tabla III-16.

- **Cuadrante Rojo:** alto impacto - alta frecuencia.
- **Cuadrantes Amarillos:** alto impacto - baja frecuencia, o bajo impacto – alta frecuencia.
- **Cuadrante Verde:** baja frecuencia – bajo impacto.

Figura III-1. Ejemplo de riesgo en función del impacto y la frecuencia

III.6. Análisis de Riesgos de la Plataforma AS400 – IESS

En esta sección se describen las actividades definidas en el punto III.5, para la plataforma AS400 – IESS, que han sido ejecutadas para el análisis y evaluación de riesgos de los activos de la plataforma y sus dependientes.

III.6.1. Dependencias de activos

La Figura III-2 muestra como está estructurada la plataforma AS400 – IESS, con los componentes y sus dependencias.

Figura III-2. Diagrama de dependencia de equipos AS400 – IESS

III.6.2. Identificación y valoración de activos

La valoración de los activos (véase Tabla III-3) se ha realizado con personal técnico de la plataforma AS400 – IESS, Ing. Iván Reinoso, funcionario del HCAM-Infraestructura, con la participación del Ing. Rodney Castro, Coordinador General de tecnología del HCAM. Los activos que no están asignados a una persona o área en particular son de responsabilidad de TICS (Área de Tecnología de la Información y Comunicación).

Tabla III-3. Valoración de activos en disponibilidad, integridad, confidencialidad y criticidad AS400 – IESS.

IDENTIFICACIÓN DE ACTIVOS			VALORACIÓN DE ACTIVOS						
#	Activo	Dueño de Activo	Disponibilidad	Valor	Integridad	Valor	Confidencialidad	Valor	Criticidad
1	Servidor Producción	TICS	Alta (A)	3	Media (M)	2	Media (M)	2	3
2	Servidor Preproducción aplicativos	TICS	Baja (B)	1	Media (M)	2	Media (M)	2	2
3	Servidor preproducción BD	TICS	Baja (B)	1	Media (M)	2	Media (M)	2	2
4	Servidor web app	TICS	Media (M)	2	Baja (B)	1	Media (M)	2	2
5	Servidor Backup red	TICS	Media (M)	2	Media (M)	2	Alta (A)	3	3
6	Servidor principal red	TICS	Alta (A)	3	Media (M)	2	Alta (A)	3	3

IDENTIFICACIÓN DE ACTIVOS			VALORACIÓN DE ACTIVOS						
#	Activo	Dueño de Activo	Disponibilidad	Valor	Integridad	Valor	Confiabledad	Valor	Criticidad
7	Servidor de desarrollo	TICS	Baja (B)	1	Media (M)	2	Media (M)	2	2
8	Stack core 1	TICS	Alta (A)	3	Media (M)	2	Alta (A)	3	3
9	Stack core 2	TICS	Alta (A)	3	Media (M)	2	Alta (A)	3	3
10	Stack acceso 1	TICS	Alta (A)	3	Media (M)	2	Alta (A)	3	3
11	Stack acceso 2	TICS	Alta (A)	3	Media (M)	2	Alta (A)	3	3
12	Stack acceso 3	TICS	Alta (A)	3	Media (M)	2	Alta (A)	3	3
13	AS400 Producción	TICS	Alta (A)	3	Media (M)	2	Alta (A)	3	3
14	AS400 GYE	TICS	Alta (A)	3	Media (M)	2	Alta (A)	3	3
15	AS400 Desarrollo	TICS	Alta (A)	3	Media (M)	2	Alta (A)	3	3
16	Controladora wireless	TICS	Alta (A)	3	Baja (B)	1	Baja (B)	1	3
17	Central Telefónica IP	MANTENIMIENTO	Alta (A)	3	Media (M)	2	Media (M)	2	3
18	Optimizador Wan	TICS	Media (M)	2	Baja (B)	1	Baja (B)	1	2
19	Aires Acondicionados	MANTENIMIENTO	Media (M)	2	Baja (B)	1	Nula (N)	0	2
20	UPS	TICS	Alta (A)	3	Baja (B)	1	Nula (N)	0	3
21	Switch piso	TICS	Alta (A)	3	Media (M)	2	Alta (A)	3	3
22	MIS AS400	Director (a) Nacional de Seguro de Salud Individual y Familiar	Alta (A)	3	Media (M)	2	Alta (A)	3	3
23	QlikView	Gerencia General HCAM	Alta (A)	3	Alta (A)	3	Alta (A)	3	3
24	Aplicativos Web Producción	Coordinación General TICs - HCAM	Alta (A)	3	Alta (A)	3	Alta (A)	3	3
25	Página Web	Jefatura Comunicación Social - HCAM	Baja (B)	1	Baja (B)	1	Baja (B)	1	1
26	Firewall	Coordinación General TICs - HCAM	Alta (A)	3	Media (M)	2	Media (M)	2	3
27	Alfresco	Coordinación General TICs - HCAM	Media (M)	2	Baja (B)	1	Media (M)	2	2

IDENTIFICACIÓN DE ACTIVOS			VALORACIÓN DE ACTIVOS						
#	Activo	Dueño de Activo	Disponibilidad	Valor	Integridad	Valor	Confidencialidad	Valor	Criticidad
28	Biblioteca Virtual	Coordinación General Docencia - HCAM	Baja (B)	1	Baja (B)	1	Baja (B)	1	1
29	EVCAM	Coordinación General TICs - HCAM	Baja (B)	1	Baja (B)	1	Baja (B)	1	1
30	Facturación	Coordinación General TICs	Media (M)	2	Alta (A)	3	Alta (A)	3	3
31	Control de Asistencia	Talento Humano	Alta (A)	3	Media (M)	2	Alta (A)	3	3
32	Base de datos postgres	Coordinación General TICs	Alta (A)	3	Alta (A)	3	Alta (A)	3	3

III.6.3. Identificación y valoración de las vulnerabilidades y amenazas

En la Tabla III-4 se muestra las vulnerabilidades y amenazas de los activos de la plataforma AS400 – IESS que han sido identificadas, así como el impacto de las amenazas en los activos según su degradación medida en las dimensiones de seguridad como: Confidencialidad, Integridad y Disponibilidad, así como la asignación de la frecuencia de ocurrencia de la amenaza para el cálculo del riesgo expuesto.

Tabla III-4. Impacto de las amenazas en los activos según su degradación AS400 – IESS

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confiability	TOTAL	FRECUENCIA	RIESGO
Servidor Producción	3	Posibilidad de incendios	Daños ocasionados por fuego	100%	60%	20%	3	0,1	0,3
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	60%	20%	3	1	3
		Falla en UPS	Daños ocasionados por corte de suministro eléctrico	100%	5%	5%	3	1	3
		Mal funcionamiento de equipos de climatización	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	50%	20%	3	1	3
		Error en la administración del equipo	Posibilidad de errores de usuario en la administración, configuración del equipo	60%	90%	20%	2,7	2	5,4
		No contar con garantía técnica en los equipos	Falta de actualizaciones de versión de sistema operativo	30%	20%	20%	0,9	1	0,9
		No cuentan con políticas internas	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	70%	20%	20%	2,1	2	4,2
		Crecimiento no planificado de personal, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo	50%	60%	20%	1,8	3	5,4

		Falta de planes de contingencia	Imposibilidad de recuperar el equipo por falta de planes de contingencia	100%	100%	100%	3	3	9
		Ingreso no autorizado a máquinas de administración que pueden posibilitar Acceso sin autorización a los equipos de clave	Acceso indebido de personas no autorizadas (lógico)	60%	80%	80%	2,4	0,1	0,24
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	40%	20%	3	0,1	0,3
		No existe una política formal de cambio de credenciales	Posibilidad de vulnerabilidad del equipo por no existir una política formal de cambio de credenciales	20%	80%	80%	2,4	0,1	0,24
		Falta de seguridad acceso al data center	Acceso sin autorización al equipo	100%	100%	100%	3	0,1	0,3
		Falla en la tarjeta de red	No se tenga acceso a la navegación interna	100%	20%	20%	3	0,1	0,3
		No contar con soporte y mantenimiento del equipo	Daño en el equipo por falta de mantenimiento	100%	10%	10%	3	1	3
		Falla de recursos físicos (hardware)	Deja de funcionar el equipo	100%	20%	20%	3	2	6
Servidor de preproducción de aplicativos, Servidor de preproducción BDD, Servidor web app	2	Posibilidad de incendios	Daños ocasionados por fuego	60%	10%	10%	1,8	0,1	0,18
		Falta de protección contra inundaciones	Daños ocasionados por agua	60%	10%	10%	1,8	1	1,8
		Falla en UPS	Daños ocasionados por corte de suministro eléctrico	60%	10%	10%	1,8	1	1,8

		Mal funcionamiento de equipos de climatización	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	60%	10%	10%	1,8	1	1,8
		Error en la administración del equipo	Posibilidad de errores de usuario en la administración, configuración del equipo	60%	60%	60%	1,8	0,1	0,18
		No contar con garantía técnica en los equipos	Falta de actualizaciones de versión de sistema operativo	80%	20%	20%	2,4	0,1	0,24
		No cuentan con políticas internas	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	60%	20%	20%	1,8	2	3,6
		Crecimiento no planificado de personal, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo	60%	20%	20%	1,8	0,1	0,18
		Falta de planes de contingencia	Imposibilidad de recuperar el equipo por falta de planes de contingencia	80%	20%	20%	2,4	2	4,8
		Ingreso no autorizado a máquinas de administración que pueden posibilitar Acceso sin autorización a los equipos de clave	Acceso indebido de personas no autorizadas (lógico)	100%	20%	20%	3	0,1	0,3
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	60%	20%	20%	1,8	0,1	0,18
		No existe una política formal de cambio de credenciales	Posibilidad de vulnerabilidad del equipo por no existir una política formal de cambio de credenciales	60%	20%	20%	1,8	1	1,8
		Falta de seguridad acceso al data center	Acceso sin autorización al equipo	100%	100%	100%	3	0,1	0,3

		Falla en la tarjeta de red	No se tenga acceso a la navegación interna	60%	20%	20%	1,8	0,1	0,18
		Falla de recursos físicos (hardware)	Deje de funcionar el equipo	20%	20%	20%	0,6	2	1,2
Servidor principal de red Servidor backup de red	3	Posibilidad de incendios	Daños ocasionados por fuego	50%	20%	20%	1,5	0,1	0,15
		Falta de protección contra inundaciones	Daños ocasionados por agua	50%	20%	20%	1,5	1	1,5
		Falla en UPS	Daños ocasionados por corte de suministro eléctrico	50%	20%	20%	1,5	1	1,5
		Mal funcionamiento de equipos de climatización	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	50%	20%	20%	1,5	1	1,5
		Error en la administración del equipo	Posibilidad de errores de usuario en la administración, configuración del equipo	60%	80%	20%	2,4	0,1	0,24
		No contar con garantía técnica en los equipos	Falta de actualizaciones de versión de sistema operativo	60%	80%	20%	2,4	0,1	0,24
		No cuentan con políticas internas	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	20%	20%	20%	0,6	2	1,2
		Crecimiento no planificado de personal, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo	20%	20%	20%	0,6	0,1	0,06
		Falta de planes de contingencia	Imposibilidad de recuperar el equipo por falta de planes de contingencia	60%	20%	20%	1,8	2	3,6

		Ingreso no autorizado a máquinas de administración que pueden posibilitar Acceso sin autorización a los equipos de clave	Acceso indebido de personas no autorizadas (lógico)	40%	20%	20%	1,2	0,1	0,12
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	40%	20%	20%	1,2	0,1	0,12
		No existe una política formal de cambio de credenciales	Posibilidad de vulnerabilidad del equipo por no existir una política formal de cambio de credenciales	60%	20%	20%	1,8	1	1,8
		Falta de seguridad acceso al data center	Acceso sin autorización al equipo	20%	20%	20%	0,6	0,1	0,06
		Falla en la tarjeta de red	No se tenga acceso a la navegación interna	10%	10%	10%	0,3	0,1	0,03
		Falla de recursos físicos (hardware)	Deje de funcionar el equipo	20%	20%	20%	0,6	3	1,8
Servidor de desarrollo	2	Posibilidad de incendios	Daños ocasionados por fuego	80%	30%	30%	2,4	0,1	0,24
		Falta de protección contra inundaciones	Daños ocasionados por agua	80%	30%	30%	2,4	1	2,4
		Falla en UPS	Daños ocasionados por corte de suministro eléctrico	80%	30%	30%	2,4	1	2,4
		Mal funcionamiento de equipos de climatización	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	80%	30%	30%	2,4	1	2,4
		Error en la administración del equipo	Posibilidad de errores de usuario en la administración, configuración del equipo	60%	60%	60%	1,8	0,1	0,18

	No contar con garantía técnica en los equipos	Falta de actualizaciones de versión de sistema operativo	80%	20%	20%	2,4	0,1	0,24
	No cuentan con políticas internas	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	60%	20%	20%	1,8	2	3,6
	Crecimiento no planificado de personal, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo	60%	20%	20%	1,8	1	1,8
	Falta de planes de contingencia	Imposibilidad de recuperar el equipo por falta de planes de contingencia	100%	20%	20%	3	2	6
	Ingreso no autorizado a máquinas de administración que pueden posibilitar Acceso sin autorización a los equipos de clave	Acceso indebido de personas no autorizadas (lógico)	100%	20%	20%	3	0,1	0,3
	Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	60%	20%	20%	1,8	0,1	0,18
	No existe una política formal de cambio de credenciales	Posibilidad de vulnerabilidad del equipo por no existir una política formal de cambio de credenciales	60%	20%	20%	1,8	1	1,8
	Falta de seguridad acceso al data center	Acceso sin autorización al equipo	100%	100%	100%	3	0,1	0,3
	Falla en la tarjeta de red	No se tenga acceso a la navegación interna	20%	20%	20%	0,6	0,1	0,06
	Falla de recursos físicos (hardware)	Deje de funcionar el equipo	20%	20%	20%	0,6	2	1,2

Stack core 1 Stack core 2	3	Mal funcionamiento de equipos de climatización	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	10%	10%	3	1	3
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	10%	10%	3	1	3
		Posibilidad de incendios	Daños ocasionados por fuego	100%	10%	10%	3	0,1	0,3
		Funcionamiento inadecuado de UPS	Daños ocasionados por corte de suministro eléctrico	100%	10%	10%	3	1	3
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	100%	10%	10%	3	2	6
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	0%	0%	3	0,1	0,3
		No existe una política formal de cambio de credenciales	Posibilidad de vulnerabilidad del equipo por no existir una política formal de cambio de credenciales	100%	100%	100%	3	0,1	0,3
		No cuentan con políticas internas	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	100%	20%	20%	3	2	6
		Crecimiento no planificado de personal, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo	100%	10%	10%	3	0,1	0,3
		Error humano en la administración	Funcionamiento erróneo del equipo	100%	10%	10%	3	0,1	0,3
		Falla de recursos físicos (hardware)	Deje de funcionar el equipo por falta de recursos	100%	10%	10%	3	2	6

		Debilidad en el control de acceso de entrada y salida	Acceso sin autorización al equipo	100%	80%	80%	3	0,1	0,3
		Falta de planes de contingencia	Imposibilidad de recuperar el equipo por falta de planes de contingencia	100%	80%	80%	3	3	9
		Ingreso no autorizado a máquinas de administración que pueden posibilitar Acceso sin autorización a los equipos de clave	Acceso indebido de personas no autorizadas (lógico)	100%	100%	100%	3	0,1	0,3
Stack acceso 1 Stack acceso 2 Stack acceso 3	3	Mal funcionamiento de equipos de climatización	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	10%	10%	3	1	3
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	10%	10%	3	1	3
		Posibilidad de incendios	Daños ocasionados por fuego	100%	10%	10%	3	0,1	0,3
		Funcionamiento inadecuado de UPS	Daños ocasionados por corte de suministro eléctrico	100%	10%	10%	3	1	3
		Falta de planes de contingencia	Imposibilidad de recuperar el equipo por falta de planes de contingencia	100%	10%	10%	3	2	6
		Ingreso no autorizado a máquinas de administración que pueden posibilitar Acceso sin autorización a los equipos de clave	Acceso indebido de personas no autorizadas (lógico)	100%	100%	100%	3	0,1	0,3
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	100%	100%	100%	3	2	6

		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	20%	20%	3	0,1	0,3
		No existe una política formal de cambio de credenciales	Posibilidad de vulnerabilidad del equipo por no existir una política formal de cambio de credenciales	100%	10%	10%	3	0,1	0,3
		No cuentan con políticas internas	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	100%	10%	10%	3	2	6
		Crecimiento no planificado de personal, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo	100%	10%	10%	3	0,1	0,3
		Error humano en la administración	Funcionamiento erróneo del equipo	100%	80%	80%	3	0,1	0,3
		Falla de recursos físicos (hardware)	Deje de funcionar el equipo	100%	80%	80%	3	2	6
		Debilidad en el control de acceso de entrada y salida	Acceso sin autorización al equipo	100%	100%	100%	3	0,1	0,3
Equipo AS400 Producción	3	Ataque de denegación de servicios	No contar con el servicio del sistema médico	100%	100%	100%	3	2	6
		Mal funcionamiento de equipos de climatización	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	60%	60%	3	1	3
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	60%	60%	3	1	3
		Posibilidad de incendios	Daños ocasionados por fuego	100%	60%	60%	3	0,1	0,3
		Funcionamiento inadecuado de UPS	Daños ocasionados por corte de suministro eléctrico	100%	60%	60%	3	1	3

	Falla en enlaces externos	Que se queden sin el sistema	100%	30%	30%	3	0,1	0,3
	Falta de planes de contingencia	Imposibilidad de recuperar el equipo por falta de planes de contingencia	100%	100%	100%	3	3	9
	Ingreso no autorizado a máquinas de administración que pueden posibilitar Acceso sin autorización a los equipos de clave	Acceso indebido de personas no autorizadas (lógico)	100%	100%	100%	3	0,1	0,3
	Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	100%	40%	40%	3	1	3
	Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	30%	30%	3	0,1	0,3
	No existe una política formal de cambio de credenciales	Posibilidad de vulnerabilidad del equipo por no existir una política formal de cambio de credenciales	100%	100%	100%	3	0,1	0,3
	No cuentan con políticas internas	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	80%	60%	60%	2,4	2	4,8
	Error humano en la administración	Funcionamiento erróneo del equipo	100%	60%	60%	3	0,1	0,3
	Falla de recursos físicos (hardware)	Deje de funcionar el equipo por saturación de recursos	100%	20%	20%	3	3	9
	Debilidad en el control de acceso de entrada y salida	Acceso sin autorización al equipo	100%	100%	100%	3	0,1	0,3

Equipo AS400 GYE	3	Ataque de denegación de servicios	No contar con el servicio del sistema médico	100%	100%	100%	3	0,1	0,3
		Mal funcionamiento de equipos de climatización	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	60%	60%	3	1	3
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	60%	60%	3	1	3
		Posibilidad de incendios	Daños ocasionados por fuego	100%	60%	60%	3	0,1	0,3
		Funcionamiento inadecuado de UPS	Daños ocasionados por corte de suministro eléctrico	100%	60%	60%	3	1	3
		Falla en enlaces externos	Que se queden sin el sistema	100%	30%	30%	3	0,1	0,3
		Falta de planes de contingencia	Imposibilidad de recuperar el equipo por falta de planes de contingencia	100%	100%	100%	3	2	6
		Ingreso no autorizado a máquinas de administración que pueden posibilitar Acceso sin autorización a los equipos de clave	Acceso indebido de personas no autorizadas (lógico)	100%	100%	100%	3	0,1	0,3
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	100%	40%	40%	3	0,1	0,3
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	30%	30%	3	0,1	0,3
		No existe una política formal de cambio de credenciales	Posibilidad de vulnerabilidad del equipo por no existir una política formal de cambio de credenciales	100%	100%	100%	3	0,1	0,3

		No cuentan con políticas internas	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	80%	60%	60%	2,4	2	4,8
		Error humano en la administración	Funcionamiento erróneo del equipo	100%	60%	60%	3	0,1	0,3
		Falla de recursos físicos (hardware)	Deje de funcionar el equipo por saturación de recursos	100%	20%	20%	3	2	6
		Debilidad en el control de acceso de entrada y salida	Acceso sin autorización al equipo	100%	100%	100%	3	0,1	0,3
Equipo AS400 Desarrollo	3	Ataque de denegación de servicios	No contar con el servicio del sistema médico	100%	30%	30%	3	0,1	0,3
		Mal funcionamiento de equipos de climatización	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	80%	30%	30%	2,4	1	2,4
		Falta de protección contra inundaciones	Daños ocasionados por agua	80%	30%	30%	2,4	1	2,4
		Posibilidad de incendios	Daños ocasionados por fuego	80%	30%	30%	2,4	0,1	0,24
		Funcionamiento inadecuado de UPS	Daños ocasionados por corte de suministro eléctrico	60%	60%	60%	1,8	0,1	0,18
		Falla en enlaces externos	Que se queden sin el sistema	80%	20%	20%	2,4	0,1	0,24
		Falta de planes de contingencia	Imposibilidad de recuperar el equipo por falta de planes de contingencia	60%	20%	20%	1,8	1	1,8
		Ingreso no autorizado a máquinas de administración que pueden posibilitar Acceso sin autorización a los equipos de clave	Acceso indebido de personas no autorizadas (lógico)	60%	20%	20%	1,8	0,1	0,18

		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	100%	20%	20%	3	1	3
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	20%	20%	3	0,1	0,3
		No existe una política formal de cambio de credenciales	Posibilidad de vulnerabilidad del equipo por no existir una política formal de cambio de credenciales	60%	20%	20%	1,8	0,1	0,18
		No cuentan con políticas internas	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	60%	20%	20%	1,8	2	3,6
		Error humano en la administración	Funcionamiento erróneo del equipo	100%	100%	100%	3	0,1	0,3
		Falla de recursos físicos (hardware)	Deje de funcionar el equipo	20%	20%	20%	0,6	0,1	0,06
		Debilidad en el control de acceso de entrada y salida	Acceso sin autorización al equipo	20%	20%	20%	0,6	0,1	0,06
Controladora wireless	3	Posibilidad de incendios	Daños ocasionados por fuego	100%	20%	20%	3	0,1	0,3
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	20%	20%	3	1	3
		Falla en UPS	Daños ocasionados por corte de suministro eléctrico	100%	20%	20%	3	1	3
		Mal funcionamiento de equipos de climatización	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	20%	20%	3	1	3

		Error en la administración del equipo	Posibilidad de errores de usuario en la administración, configuración del equipo	100%	20%	20%	3	0,1	0,3
		No contar con garantía técnica en los equipos	Falta de actualizaciones de versión de sistema operativo	100%	10%	10%	3	1	3
		No cuentan con políticas internas	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	60%	20%	20%	1,8	2	3,6
		Falta de planes de contingencia	Imposibilidad de recuperar el equipo por falta de planes de contingencia	100%	100%	100%	3	2	6
		Ingreso no autorizado a máquinas de administración que pueden posibilitar Acceso sin autorización a los equipos de clave	Acceso indebido de personas no autorizadas (lógico)	100%	80%	80%	3	0,1	0,3
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	20%	20%	3	0,1	0,3
		No existe una política formal de cambio de credenciales	Posibilidad de vulnerabilidad del equipo por no existir una política formal de cambio de credenciales	100%	80%	80%	3	0,1	0,3
		NO existe equipo de backups	Se queda sin servicio de red inalámbrica el HCAM	100%	20%	20%	3	3	9
		Falta de seguridad acceso al data center	Acceso sin autorización al equipo	100%	100%	100%	3	0,1	0,3
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	100%	10%	10%	3	2	6

		Falla de recursos físicos (hardware)	Deje de funcionar el equipo por saturación de recursos	100%	20%	20%	3	3	9
Central Telefónica IP	3	Posibilidad de incendios	Daños ocasionados por fuego	100%	20%	20%	3	0,1	0,3
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	20%	20%	3	1	3
		Falla en UPS	Daños ocasionados por corte de suministro eléctrico	100%	20%	20%	3	1	3
		Mal funcionamiento de equipos de climatización	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	20%	20%	3	1	3
		Error en la administración del equipo	Posibilidad de errores de usuario en la administración, configuración del equipo	100%	10%	10%	3	1	3
		No contar con garantía técnica en los equipos	Falta de actualizaciones de versión de sistema operativo	80%	10%	10%	0,3	2	0,6
		No cuentan con políticas internas	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	80%	10%	10%	2,4	2	4,8
		Error humano en la administración	Funcionamiento erróneo del equipo	100%	20%	20%	3	0,1	0,3
		Falta de planes de contingencia	Imposibilidad de recuperar el equipo por falta de planes de contingencia	100%	10%	10%	3	2	6
		Ingreso no autorizado a máquinas de administración que pueden posibilitar Acceso sin autorización al equipo de clave	Acceso indebido de personas no autorizadas (lógico)	100%	100%	100%	3	0,1	0,3

		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	20%	20%	3	0,1	0,3
		No existe una política formal de cambio de credenciales	Posibilidad de vulnerabilidad del equipo por no existir una política formal de cambio de credenciales	100%	100%	100%	3	1	3
		NO existe equipo de backups	Se queda sin servicio de telefonía por no contar con equipo de backup	100%	10%	10%	3	3	9
		Falta de seguridad acceso al data center	Acceso sin autorización al equipo	100%	100%	100%	3	0,1	0,3
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	100%	60%	10%	3	3	9
		Falla de recursos físicos (hardware)	Deje de funcionar el equipo por desconexión de la red	100%	10%	10%	3	2	6
		Crecimiento no planificado de personal, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo	100%	10%	10%	3	3	9
Optimizador Wan	2	Posibilidad de incendios	Daños ocasionados por fuego	100%	10%	10%	3	0,1	0,3
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	10%	10%	3	0,1	0,3
		Falla en UPS	Daños ocasionados por corte de suministro eléctrico	100%	10%	10%	3	1	3
		Mal funcionamiento de equipos de climatización	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	10%	10%	3	1	3

		Error humano en la administración	Funcionamiento erróneo del equipo	100%	20%	20%	3	0,1	0,3
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	20%	20%	3	0,1	0,3
		Falta de seguridad acceso al data center	Acceso sin autorización al equipo	100%	100%	100%	3	0,1	0,3
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	100%	10%	10%	3	2	6
		Falla de recursos físicos (hardware)	Deje de funcionar el equipo por falta de recursos	100%	10%	10%	3	2	6
Aires Acondicionados	2	Posibilidad de incendios	Daños ocasionados por fuego	100%	10%	10%	3	0,1	0,3
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	10%	10%	3	1	3
		Falla en UPS	Daños ocasionados por corte de suministro eléctrico	100%	10%	10%	3	1	3
		Los equipos se encuentran con componentes defectuosos	Daño de componentes del equipo	100%	10%	10%	3	2	6
		Falta de capacitación (personal de administración)	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	100%	10%	10%	3	0,1	0,3
		No disponer de repuestos de partes críticas de los equipos	No garantizar disponibilidad del equipo	100%	0%	0%	3	2	6
		Falta de procedimientos de contingencia y políticas formalizadas	Imposibilidad de recuperar el equipo por falta de planes de contingencia	100%	10%	10%	3	2	6

		No tener soporte técnico y mantenimiento por lo que puede ocurrir problemas graves que no se puedan solventar en cortos tiempos	Falta de soporte técnico y mantenimientos	100%	10%	10%	3	1	3
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	10%	10%	3	0,1	0,3
UPS	3	Posibilidad de incendios	Daños ocasionados por fuego	100%	10%	10%	3	0,1	0,3
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	10%	10%	3	1	3
		Falla en el sistema de batería en UPS	Daños ocasionados por corte de suministro eléctrico	100%	10%	10%	3	1	3
		Los equipos se encuentran con componentes defectuosos	Daño de componentes del equipo	100%	10%	10%	3	1	3
		Falta de capacitación (personal de administración)	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	100%	10%	10%	3	0,1	0,3
		No disponer de repuestos de partes críticas de los equipos	No garantizar disponibilidad del equipo	100%	0%	0%	3	2	6
		Falta de procedimientos de contingencia y políticas formalizadas	Imposibilidad de recuperar el equipo por falta de planes de contingencia	100%	10%	10%	3	2	6
		No tener soporte técnico y mantenimiento por lo que puede ocurrir problemas graves que no se puedan solventar en cortos tiempos	Falta de soporte técnico y mantenimientos	100%	10%	10%	3	3	9
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	10%	10%	3	0,1	0,3

Switch piso	3	Mal funcionamiento de equipos de climatización	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	10%	10%	3	1	3
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	10%	10%	3	0,1	0,3
		Posibilidad de incendios	Daños ocasionados por fuego	100%	10%	10%	3	0,1	0,3
		Funcionamiento inadecuado de UPS	Daños ocasionados por corte de suministro eléctrico	100%	10%	10%	3	2	6
		Falta de planes de contingencia	Imposibilidad de recuperar el equipo por falta de planes de contingencia	100%	10%	10%	3	2	6
		Ingreso no autorizado a máquinas de administración que pueden posibilitar Acceso sin autorización al equipo de clave	Acceso indebido de personas no autorizadas (lógico)	100%	100%	100%	3	0,1	0,3
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	100%	20%	20%	3	2	6
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	20%	20%	3	0,1	0,3
		No existe una política formal de cambio de credenciales	Posibilidad de vulnerabilidad del equipo por no existir una política formal de cambio de credenciales	100%	10%	10%	3	0,1	0,3
		No cuentan con políticas internas	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	100%	10%	10%	3	2	6

		Crecimiento no planificado de personal, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo	100%	10%	10%	3	0,1	0,3
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres Naturales (Terremotos)	100%	0%	0%	3	0,1	0,3
		Error humano en la administración	Funcionamiento erróneo del equipo	100%	80%	80%	3	0,1	0,3
		Espacio físico inadecuado para rack de piso	Espacios reducidos y están al alcance de personal no autorizado	100%	100%	100%	3	3	9
		Degradación de patchcord de fibra	Perdida de enlace entre switches	100%	10%	10%	3	1	3
		Falla de recursos físicos (hardware)	Deje de funcionar el equipo por falla de recursos físicos	100%	10%	10%	3	2	6
		Debilidad en el control de acceso de entrada y salida	Acceso sin autorización al equipo	100%	100%	100%	3	0,1	0,3
Sistema Médico AS400	3	No contar con las pruebas unitarias necesarias para cambio	Aplicación de cambios sin pruebas	100%	10%	10%	3	2	6
		Falta de capacitación (personal de administración)	Inadecuado manejo de mantenimiento de los aplicativos	100%	20%	20%	3	1	3
		Falta y actualización de planes de contingencia	Imposibilidad de recuperar los aplicativos	100%	80%	80%	3	3	9
		Ingreso no autorizado a máquinas de administración que pueden posibilitar Acceso sin autorización al equipo de clave	Acceso indebido de personas no autorizadas (lógico)	100%	100%	100%	3	0,1	0,3

		No tener versionado el código fuente de los aplicativos	Pisar los cambios recientes de los aplicativos	80%	20%	20%	2,4	1	2,4
		No tener un ambiente de desarrollo y pruebas	Mal funcionamiento de los aplicativos	20%	20%	20%	0,6	0,1	0,06
		No contar con alta disponibilidad	No proporcionar servicios	100%	100%	100%	3	1	3
		No contar con modulo autenticación	Accesos no controlados a los aplicativos	60%	100%	100%	3	0,1	0,3
		Las claves no siguen las buenas prácticas de construcción	Mal uso de las cuentas de usuario	60%	80%	80%	2,4	0,1	0,24
		No existe una política formal de cambio de credenciales	Posibilidad de vulnerabilidad del equipo por no existir una política formal de cambio de credenciales	60%	100%	100%	3	0,1	0,3
		Ataque de denegación de servicios	No contar con el servicio del sistema médico por ataques o falta de recursos del equipo	100%	10%	10%	3	1	3
		No cuenta con documentación técnica de implementación de los aplicativos	Problemas al momento de delegar la administración de los aplicativos	80%	20%	20%	0,6	1	0,6
		No cuenta con políticas de respaldos	Pérdida de información del sistema médico	100%	60%	60%	3	0,1	0,3
QlikView	3	No tiene redundancia	Problemas de disponibilidad del aplicativo	60%	20%	20%	1,8	1	1,8
		No cuenta con soporte técnico	Que no se puede actualizar las versiones del aplicativo base	60%	10%	10%	1,8	1	1,8
		No cuenta con normas de seguridad	Uso indebido de credenciales de acceso por funcionarios no autorizados	100%	100%	100%	3	0,1	0,3

		No cuenta con versionamiento	Inflexibilidad al momento de hacer cambios en el software y problemas de seguimiento a la trazabilidad (estado)	100%	10%	10%	3	1	3
		Falta de antivirus	Posible acceso indebido al servidor remotamente	100%	100%	100%	3	2	6
		No cuenta con sistema de respaldos	Pérdida de información alojada en el servidor (plantillas de aplicativos)	100%	10%	10%	3	0,1	0,3
Aplicativos Web Producción	3	No contar con las pruebas unitarias necesarias para cambio	Aplicación de cambios sin pruebas	100%	10%	10%	3	1	3
		Falta de capacitación (personal de administración)	Inadecuado manejo de mantenimiento de los aplicativos	100%	20%	20%	3	1	3
		Falta y actualización de planes de contingencia	Imposibilidad de recuperar los aplicativos	100%	100%	100%	3	2	6
		Ingreso no autorizado a máquinas de administración que pueden posibilitar Acceso sin autorización al equipo de claves	Acceso indebido de personas no autorizadas (lógico)	100%	100%	100%	3	0,1	0,3
		No tener versionado el código fuente de los aplicativos	Pisar los cambios recientes de los aplicativos	100%	20%	20%	3	0,1	0,3
		No tener un ambiente de desarrollo y pruebas	Mal funcionamiento de los aplicativos	100%	80%	80%	3	0,1	0,3
		No contar con alta disponibilidad	No proporcionar servicios	100%	20%	30%	3	2	6
		No contar con modulo autenticación	Accesos no controlados a los aplicativos	100%	100%	100%	3	0,1	0,3

		Las claves no siguen las buenas prácticas de construcción	Mal uso de las cuentas de usuario	100%	80%	80%	3	1	3
		No existe una política formal de cambio de credenciales	Posibilidad de vulnerabilidad del equipo por no existir una política formal de cambio de credenciales	100%	80%	80%	3	0,1	0,3
		Ataque de denegación de servicios	No contar con el servicio de los aplicativos	100%	20%	30%	3	1	3
		No cuenta con documentación técnica de implementación de los aplicativos	Problemas al momento de delegar la administración de los aplicativos	100%	100%	100%	3	2	6
		No cuenta con políticas de respaldos	Pérdida de información de las fuentes de los aplicativos	100%	20%	20%	3	0,1	0,3
Página Web	1	Utiliza un gestor de contenidos en software libre y vulnerable	Que se realice acciones mal intencionadas en el sitio web	100%	80%	80%	3	1	3
		No tiene antivirus	Difusión de software dañino	80%	10%	10%	2,4	0,1	0,24
		No posee soporte	Errores de actualización y mantenimiento	100%	20%	20%	3	0,1	0,3
		No se cuenta con políticas de administración de credenciales	Manipulación de programas	100%	80%	80%	3	1	3
Software Firewall	3	Falta de capacitación (personal de administración)	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	100%	60%	60%	3	1	3
		No tener soporte y garantía del fabricante	Imposibilidad de realizar actualizaciones y probabilidad de infecciones en las máquinas de los usuarios.	100%	20%	20%	3	2	6

Alfresco, Biblioteca Virtual, EVCAM	2	Al momento no se tiene una solución de filtrado de contenido, antivirus, antiboot en las unidades	No poder atender el incremento de solicitudes de acceso hacia internet con los controles adecuados	100%	20%	20%	3	3	9
		Al momento no se tiene controles de URL Filtering, Antivirus y Antiboot perimetral	Falta de protección en la red, con probabilidad de ataques e infección en las máquinas de los usuarios.	100%	100%	100%	3	2	6
		No existe el control de acceso a internet en algunas de las unidades, ni tampoco desde las unidades hacia la red del IESS.	Posibilidad de problemas de seguridad en la red por el acceso directo a internet y la falta de control en los accesos de las redes LAN	100%	100%	100%	3	2	6
	2	No tiene redundancia	Problemas de disponibilidad del aplicativo	60%	10%	10%	1,8	0,1	0,18
		No cuenta con soporte técnico	Imposibilidad de actualizar las versiones del aplicativo base	60%	10%	10%	1,8	1	1,8
		No cuenta con normas de seguridad	Uso indebido de credenciales de acceso por funcionarios no autorizados	100%	100%	100%	3	0,1	0,3
		No cuenta con versionamiento	Inflexibilidad al momento de hacer cambios en el software y problemas de seguimiento a la trazabilidad (estado)	60%	10%	10%	1,8	0,1	0,18
	2	Falta de antivirus	Posible acceso indebido al servidor remotamente	100%	100%	100%	3	3	9
		No cuenta con sistema de respaldos	Posibilidad de pérdida de información alojada en el servidor (plantillas de aplicativos)	100%	10%	10%	3	0,1	0,3

Aplicativo de Facturación	3	No contar con las pruebas unitarias necesarias para cambio	Aplicación de cambios sin pruebas	100%	20%	20%	3	0,1	0,3
		Falta de capacitación (personal de administración)	Inadecuado manejo de mantenimiento de los aplicativos	100%	20%	20%	3	0,1	0,3
		Falta y actualización de planes de contingencia	Imposibilidad de recuperar los aplicativos	100%	100%	100%	3	2	6
		Ingreso no autorizado a máquinas de administración que pueden posibilitar Acceso sin autorización al equipo de claves	Acceso indebido de personas no autorizadas (lógico)	100%	100%	100%	3	0,1	0,3
		No tener versionado el código fuente de los aplicativos	Pisar los cambios recientes de los aplicativos	100%	60%	60%	3	1	3
		No tener un ambiente de desarrollo y pruebas	Mal funcionamiento de los aplicativos	100%	50%	50%	3	0,1	0,3
		No contar con alta disponibilidad	No proporcionar servicios	100%	80%	80%	3	2	6
		No contar con modulo autenticación	Accesos no controlados a los aplicativos	100%	100%	100%	3	0,1	0,3
		Las claves no siguen las buenas prácticas de construcción	Mal uso de las cuentas de usuario	100%	100%	100%	3	0,1	0,3
		No existe una política formal de cambio de credenciales	Posibilidad de vulnerabilidad del equipo por no existir una política formal de cambio de credenciales	100%	100%	100%	3	0,1	0,3
		Ataque de denegación de servicios	No contar con el servicio de facturación	100%	20%	20%	3	1	3

		No cuenta con documentación técnica de implementación de los aplicativos	Problemas al momento de delegar la administración de los aplicativos	100%	20%	20%	3	1	3
		No cuenta con políticas de respaldos	Pérdida de información de la facturación	100%	20%	20%	3	0,1	0,3
Base de datos postgres	3	No tiene redundancia	Problemas de disponibilidad de la data	100%	20%	20%	3	0,1	0,3
		No cuenta con sistema de respaldos	Pérdida total o parcial de información alojada en la base de datos en casos contingentes	100%	60%	60%	3	0,1	0,3
		No dispone de los recursos necesarios (hardware)	Tiempos de respuesta muy elevados en horas pico	100%	20%	20%	3	1	3
		No dispone de soporte técnico especializado para implementación escalable	Uso no óptimo de las prestaciones de la herramienta	100%	20%	20%	3	1	3
		Desconocimiento de la estructura de la base de datos	No contar con un diccionario de datos que permita realizar cambios	100%	20%	20%	3	1	3
		No contar con personal capacitado en la administración de la base	Imposibilidad de cambio o mejoras en la administración	100%	50%	50%	3	0,1	0,3
		No contar con una arquitectura de base de datos	Imposibilidad de mejoras en la estructura de la base de datos	100%	20%	20%	3	0,1	0,3
		Falta de planes de capacidad de crecimiento de la base	Dificultad de crecimiento de la base de datos	100%	20%	20%	3	0,1	0,3
		Falta de planes de contingencia	Imposibilidad de proporcionar el servicio de base de datos	100%	100%	100%	3	2	6

III.6.4. Gráfica de radar de los riesgos por activo

La Tabla III-5 muestra los riesgos de la plataforma AS400 – IESS que han sido identificados, donde:

- Valor actual: Promedio de todos los riesgos.
- Valor objetivo: Recomendación de la SDNSI de reducción de riesgo (al menos el 50%).
- Valor límite: Valor dado por condiciones gráficas, al que nunca se debería llegar.

Tabla III-5. Tabla de Valores de Riesgos AS400 – IESS

ACTIVO	ACTUAL	OBJETIVO	LIMITE
Servidor Producción	2,79	1,39	7
Servidor de preproducción de aplicativos, Servidor de preproducción BDD, Servidor web app	1,24	0,62	7
Servidor principal de red Servidor backup de red	0,93	0,46	7
Servidor de desarrollo	1,54	0,77	7
Stack core 1 Stack core 2	2,72	1,36	7
Stack acceso 1 Stack acceso 2 Stack acceso 3	2,51	1,25	7
Equipo AS400 Producción	2,86	1,43	7
Equipo AS400 GYE	1,90	0,95	7
Equipo AS400 Desarrollo	1,02	0,51	7
Controladora wireless	3,16	1,58	7
Central Telefónica IP	3,58	1,79	7
Optimizador Wan	2,17	1,08	7
Aires Acondicionados	3,10	1,55	7
UPS	3,43	1,72	7
Switch piso	2,81	1,40	7
Sistema Médico AS400	2,19	1,10	7
QlikView	2,20	1,10	7
Aplicativos Web Producción	2,45	1,22	7
Página Web	1,64	0,82	7
Software Firewall	6,00	3,00	7
Alfresco, Biblioteca Virtual, EVCAM	1,96	0,98	7
Aplicativo de Facturación	1,80	0,90	7
Base de datos postgres	1,83	0,92	7

La Figura III-3 muestra un reporte de los riesgos de la plataforma AS400 – IESS, que indica el riesgo actual, objetivo y el límite aceptable.

Figura III-3. Reporte de riesgos plataforma AS400 – IESS

III.6.5. Controles o salvaguardas sugeridas

La Tabla III-6. Salvaguardas sugeridas AS400 – IESS muestra las salvaguardas que han sido identificadas para cada tripleta activo – vulnerabilidad – amenaza.

Tabla III-6. Salvaguardas sugeridas AS400 – IESS

IDENTIFICACIÓN DE ACTIVOS	VULNERABILIDADES	AMENAZAS	SALVAGUARDAS
Servidor Producción	Falta de planes de contingencia	No existe planes de contingencia	Establecer planes y procedimientos de contingencia Contar con infraestructura tecnológica en otra localidad Generar un piloto de plan de contingencia
Servidor de preproducción de aplicativos, Servidor de preproducción BDD, Servidor web app	No cuentan con políticas internas	Falta de normativas o políticas internas de la institución	Proponer normativas y procedimientos técnicos para retroalimentación y aprobación de DNTI
	Falta de planes de contingencia	No existe planes de contingencia	Establecer planes y procedimientos de contingencia Generar un piloto de plan de contingencia

IDENTIFICACIÓN DE ACTIVOS	VULNERABILIDADES	AMENAZAS	SALVAGUARDAS
Servidor principal de red Servidor backup de red	Falta de planes de contingencia	No existe planes de contingencia	Establecer planes y procedimientos de contingencia Generar un piloto de plan de contingencia
Servidor de desarrollo	No cuentan con políticas internas	Falta de normativas o políticas internas de la institución	Proponer normativas y procedimientos técnicos para retroalimentación y aprobación de DNTI
	Falta de planes de contingencia	No existe planes de contingencia	Establecer planes y procedimientos de contingencia Generar un piloto de plan de contingencia
Stack core 1 Stack core 2	Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	Contar con soporte y mantenimientos periódicos en los equipos
	No cuentan con políticas internas	Falta de normativas o políticas internas de la institución	Proponer normativas y procedimientos técnicos para retroalimentación y aprobación de DNTI
	Falla de recursos físicos (hardware)	Deje de funcionar el equipo por falta de recursos	Actualización de firmware para corrección de errores, repotenciación o cambio de equipo
	Falta de planes de contingencia	Falta de planes de contingencia	Establecer planes y procedimientos de contingencia Generar un piloto de plan de contingencia
Stack acceso 1 Stack acceso 2 Stack acceso 3	Falta de planes de contingencia	Falta de planes de contingencia	Establecer planes y procedimientos de contingencia Generar un piloto de plan de contingencia
	Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	Contar con soporte y mantenimientos periódicos en los equipos
	No cuentan con políticas internas	Falta de normativas o políticas internas de la institución	Proponer normativas y procedimientos técnicos para retroalimentación y aprobación de DNTI
	Falla de recursos físicos (hardware)	Deje de funcionar el equipo	Actualización de firmware para corrección de errores, repotenciación o cambio de equipo
Equipo AS400 Producción	Ataque de denegación de servicios	No contar con el servicio del sistema médico	Proteger el servidor con firewall de frontera

IDENTIFICACIÓN DE ACTIVOS	VULNERABILIDADES	AMENAZAS	SALVAGUARDAS
	Falta de planes de contingencia	Falta de planes de contingencia	Establecer planes y procedimientos de contingencia Generar un piloto de plan de contingencia
	No cuentan con políticas internas	Falta de normativas o políticas internas de la institución	Proponer normativas y procedimientos técnicos para retroalimentación y aprobación de DNTI
	Falla de recursos físicos (hardware)	Deje de funcionar el equipo por saturación de recursos	Realizar una gestión de la capacidad que permita estimar los recursos físicos (memoria, procesador, discos) del servidor
Equipo AS400 GYE	Falta de planes de contingencia	Falta de planes de contingencia	Establecer planes y procedimientos de contingencia Generar un piloto de plan de contingencia
	No cuentan con políticas internas	Falta de normativas o políticas internas de la institución	Proponer normativas y procedimientos técnicos para retroalimentación y aprobación de DNTI
	Falla de recursos físicos (hardware)	Deje de funcionar el equipo por saturación de recursos	Realizar una gestión de la capacidad que permita estimar los recursos físicos (memoria, procesador, discos) del servidor
Equipo AS400 Desarrollo	No cuentan con políticas internas	Falta de normativas o políticas internas de la institución	Proponer normativas y procedimientos técnicos para retroalimentación y aprobación de DNTI
Controladora wireless	No cuentan con políticas internas	Falta de normativas o políticas internas de la institución	Proponer normativas y procedimientos técnicos para retroalimentación y aprobación de DNTI
	Falta de planes de contingencia	No existe planes de contingencia	Establecer planes y procedimientos de contingencia Generar un piloto de plan de contingencia
	NO existe equipo de backups	Se queda sin servicio de red inalámbrica el HCAM	Contar con equipos de backup de red inalámbrica para el HCAM
	Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	Contar con soporte y mantenimientos periódicos en los equipos
	Falla de recursos físicos (hardware)	Deje de funcionar el equipo por saturación de recursos	Realizar una gestión de la capacidad que permita estimar los recursos físicos (memoria, procesador, discos) del servidor

IDENTIFICACIÓN DE ACTIVOS	VULNERABILIDADES	AMENAZAS	SALVAGUARDAS
Central Telefónica IP	No cuentan con políticas internas	Falta de normativas o políticas internas de la institución	Proponer normativas y procedimientos técnicos para retroalimentación y aprobación de DNTI
	Falta de planes de contingencia	No existe planes de contingencia	Establecer planes y procedimientos de contingencia Generar un piloto de plan de contingencia
	NO existe equipo de backups	Se queda sin servicio de telefonía por no contar con equipo de backup	Contar con equipos de backup de servicio de telefonía para el HCAM
	Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	Contar con soporte y mantenimientos periódicos en los equipos
	Falla de recursos físicos (hardware)	Deje de funcionar el equipo por desconexión de la red	Realizar una gestión de la capacidad que permita estimar los recursos físicos (memoria, procesador, discos) del servidor
	Crecimiento no planificado de personal, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo	Repotenciación de equipamiento de la plataforma de telefonía
Optimizador Wan	Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	Contar con soporte y mantenimientos periódicos en los equipos
	Falla de recursos físicos (hardware)	Deje de funcionar el equipo por falta de recursos	Realizar una gestión de la capacidad que permita estimar los recursos físicos (memoria, procesador, discos) del servidor
Aires Acondicionados	Los equipos se encuentran con componentes defectuosos	Daño de componentes del equipo	Contar con soporte y mantenimientos periódicos en los equipos
	No disponer de repuestos de partes críticas de los equipos	Falla del equipo afectando su disponibilidad	Repotenciar los equipos de aires acondicionados
	Falta de procedimientos de contingencia y políticas formalizadas	Falta de procedimientos de contingencia	Establecer planes y procedimientos de contingencia Generar un piloto de plan de contingencia
UPS	No disponer de repuestos de partes críticas de los equipos	Falla del equipo afectando su disponibilidad	Repotenciar los equipos ups

IDENTIFICACIÓN DE ACTIVOS	VULNERABILIDADES	AMENAZAS	SALVAGUARDAS
	Falta de procedimientos de contingencia y políticas formalizadas	Falta de procedimientos de contingencia	Establecer planes y procedimientos de contingencia Generar un piloto de plan de contingencia
	No tener soporte técnico y mantenimiento por lo que puede ocurrir problemas graves que no se puedan solventar en cortos tiempos	Falta de soporte técnico y mantenimientos	Contar con soporte y mantenimientos periódicos en los equipos
Switch piso	Funcionamiento inadecuado de UPS	Daños ocasionados por corte de suministro eléctrico	Disponer de una planta eléctrica de contingencia
	Falta de planes de contingencia	Falta de planes de contingencia	Establecer planes y procedimientos de contingencia Generar un piloto de plan de contingencia
	Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	Contar con soporte y mantenimientos periódicos en los equipos
	No cuentan con políticas internas	Falta de normativas o políticas internas de la institución	Proponer normativas y procedimientos técnicos para retroalimentación y aprobación de DNTI
	Espacio físico inadecuado para rack de piso	Espacios reducidos y están al alcance de personal no autorizado	Establecer nueva localización de espacio físico para rack de piso
	Falla de recursos físicos (hardware)	Deje de funcionar el equipo por falla de recursos físicos	Realizar una gestión de la capacidad que permita estimar los recursos físicos (memoria, procesador, discos) del servidor
Sistema Médico AS400	Aplicación de cambios sin pruebas	No contar con las pruebas unitarias necesarias para cambio	Establecer un proceso de control de cambios debidamente formalizado
	Imposibilidad de recuperar los aplicativos	Falta y actualización de planes de contingencia	Establecer planes y procedimientos de contingencia Generar un piloto de plan de contingencia
QlikView	No cuenta con sistema de respaldos	perdida de información alojada en el servidor (plantillas de aplicativos)	Contar con un backup de la data en un repositorio específico
Aplicativos Web Producción	Imposibilidad de recuperar los aplicativos	Falta y actualización de planes de contingencia	Establecer planes y procedimientos de contingencia Generar un piloto de plan de contingencia

IDENTIFICACIÓN DE ACTIVOS	VULNERABILIDADES	AMENAZAS	SALVAGUARDAS
	No proporcionar servicios	No contar con alta disponibilidad	Contar con una solución tecnológica de balanceador de carga
	No cuenta con documentación técnica de implementación de los aplicativos	Problemas al momento de delegar la administración de los aplicativos	Documentar técnicamente la implementación de los aplicativos web para evitar problemas de delegación de administración
Software Firewall	No tener soporte y garantía del fabricante	Falta de soporte y garantía del fabricante sobre el hardware en el que está instalada la solución	Solicitar recomendaciones técnicas de soluciones tecnológicas de Firewall a la DNTI
	Al momento no se tiene una solución de filtrado de contenido, antivirus, antiboot en las unidades	No poder atender el incremento de solicitudes de acceso hacia internet con los controles adecuados	Posibilitar la implementación de equipos de una solución de firewall con URLFiltering, Antivirus y Antiboot perimetral con aprobación de la DNTI
	Al momento no se tiene controles de URLFiltering, Antivirus y Antiboot perimetral	Falta de controles URLFiltering, Antivirus y Antiboot perimetral	
	No existe el control de acceso a internet en algunas de las unidades, ni tampoco desde las unidades hacia la red del IESS.	Posibilidad de problemas de seguridad en la red por el acceso directo a internet y la falta de control en los accesos de las redes LAN	Solicitar recomendaciones técnicas a la DNTI, para minimizar la exposición de equipos a internet
Alfresco, Biblioteca Virtual, EVCAM	Falta de antivirus	Posible acceso indebido al servidor remotamente	Implementar una solución antivirus, antimalware, así como la adopción de controles de seguridad (ej. usuarios autenticados), con la finalidad de evitar la ocurrencia de accesos remotos no autorizados
Aplicativo de Facturación	Imposibilidad de recuperar los aplicativos	Falta y actualización de planes de contingencia	Establecer planes y procedimientos de contingencia Generar un piloto de plan de contingencia
	No proporcionar servicios	No contar con alta disponibilidad	Contar con una solución tecnológica de balanceador de carga
Base de datos postgres	Imposibilidad de proporcionar el servicio de base de datos	Falta de planes de contingencia	Establecer planes y procedimientos de contingencia Generar un piloto de plan de contingencia

III.6.6. Conclusiones

- Mediante el presente análisis y evaluación de riesgos se concluye que la plataforma tecnológica AS400 – IESS que corresponde del Sistema Médico del Hospital Carlos Andrade Marín (HCAM) no cuenta con planes de contingencia implantados, siendo un riesgo crítico para la continuidad de las operaciones del IESS.

- Varios equipos de la plataforma tecnológica del HCAM, no cuentan con soporte y mantenimiento, lo que pone en riesgo otros equipos dependientes y el Sistema Médico del IESS.
- Varios equipos de la plataforma tecnológica del HCAM, podrían dejar de funcionar por saturación de recursos (memoria RAM, procesador, discos).
- Resultado del presente análisis, los riesgos localizados en los cuadrantes de alto impacto y bajo frecuencia, y bajo impacto y alta frecuencia de los mapas de riesgos, deben ser monitoreados con periodicidad.

III.7. Análisis de Riesgos de la Plataforma Host – IESS

En esta sección se describen las actividades definidas en el punto III.5, para la plataforma Host – IESS, y se han analizado los riesgos de los equipos de la plataforma y sus dependientes mediante:

- Identificación de los equipos de la plataforma definida y sus equipos dependientes.
- Valoración de activos considerando tres dimensiones: disponibilidad, integridad y confidencialidad.
- Identificación y valoración de las amenazas y vulnerabilidades sobre dichos equipos.
- Evaluación del impacto y frecuencia de los escenarios de riesgos identificados.
- Cálculo del riesgo total.
- Propuesta de controles o salvaguardas.

III.7.1. Dependencias de activos

La Figura III-4 muestra como está estructurada la plataforma Host – IESS, con los componentes y sus dependencias.

Figura III-4. Diagrama de dependencias de equipos Host

III.7.2. Identificación y valoración de activos

La valoración de los activos (véase Tabla III-7) se ha realizado con personal técnico de la plataforma Host – IESS, Ing. Paúl Galarraga, Tecnólogo. Marco García y Tecnólogo Alberto Andrade, quienes han colaborado en la identificación de los activos y el desarrollo de las actividades definidas.

Tabla III-7. Valoración de activos en disponibilidad, integridad, confidencialidad y criticidad Host – IESS

IDENTIFICACIÓN DE ACTIVOS			VALORACIÓN DE ACTIVOS						
#	Activo	Dueño de Activo	Disponibilidad	Valor	Integridad	Valor	Confidencialidad	Valor	Criticidad
1	Main-Frame Z10BC	HOST	Alta (A)	3	Media (M)	2	Media (M)	2	3
2	UNIDAD DE CARTUCHOS 1	HOST	Media (M)	2	Media (M)	2	Media (M)	2	2
3	UNIDAD DE CARTUCHOS 2	HOST	Media (M)	2	Media (M)	2	Media (M)	2	2
4	ALMACENAMIENTO (STORAGE)	HOST	Alta (A)	3	Media (M)	2	Media (M)	2	3
5	SERVIDOR HMC	HOST	Media (M)	2	Media (M)	2	Media (M)	2	1
6	AIRE DE PRESICION	HOST	Alta (A)	3	Media (M)	2	Media (M)	2	3
7	AIRE TIPO MOCHILA	HOST	Baja (B)	1	Media (M)	2	Media (M)	2	2
8	UPS	HOST	Alta (A)	3	Media (M)	2	Media (M)	2	3
9	SERVIDOR UNIX	HOST	Alta (A)	3	Media (M)	2	Media (M)	2	3
10	SERVER VTAPE	HOST	Media (M)	2	Media (M)	2	Media (M)	2	2
11	SWITCH DE PASO	HOST	Alta (A)	3	Media (M)	2	Media (M)	2	3
12	Consulta de Información de Empresas	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
13	Ingreso de glosas (“auditoria” en la contabilidad fiscal)	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
14	Liquidación de Glosas y Títulos de Crédito	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
15	Notificación de Glosas	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
16	Consulta de Glosas y Títulos de Crédito	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
17	Modificación de Aportes y descuentos en Glosas	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
18	Ingreso del Comprobante de pago de Abonos	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
19	Emisión de Títulos de Crédito	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
20	Consulta de plan de cuentas	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
21	Ingreso de cargos empleados del IESS	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
22	Consulta de cuentas auxiliares	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
23	Consulta histórica de prestamos	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3

IDENTIFICACIÓN DE ACTIVOS			VALORACIÓN DE ACTIVOS						
#	Activo	Dueño de Activo	Disponibilidad	Valor	Integridad	Valor	Confiablez	Valor	Criticidad
24	Consulta de cuenta corriente patronal de prestamos	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
25	Consulta de cuenta de planillas de prestamos	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
26	Liquidación de prestamos	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
27	Consulta histórica de liquidaciones de prestamos	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
28	Justificación de Abonos	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
29	Control de tramites de levantamientos de hipoteca	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
30	Calificación estado de préstamo	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
31	Emisión de Planillas de descuentos	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
32	Recaudación de prestamos	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
33	Consulta de comprobantes contabilizados	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
34	Control de Cajeros	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
35	Consulta de recaudación a nivel nacional	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
36	Impresos	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
37	Consulta de recaudación a nivel nacional	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
38	Descarga de Egresos	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
39	Consulta histórica de egresos del IESS	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
40	Ingreso de tramites	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
41	Ingreso de Beneficiarios:	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
42	Calificación de derechos de los beneficiarios de montepío	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
43	Liquidación de montepío	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
44	Registrar boletines de egreso de montepío	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
45	Pago de Retenciones Judiciales	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3

IDENTIFICACIÓN DE ACTIVOS			VALORACIÓN DE ACTIVOS						
#	Activo	Dueño de Activo	Disponibilidad	Valor	Integridad	Valor	Confidencialidad	Valor	Criticidad
46	Consulta de tramites de prestaciones	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
47	Pago de Montepío a Beneficiarios	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
48	Liquidación de Viáticos	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
49	Consulta histórica de nómina de empleados del IESS	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
50	Ingreso de planillas de FR por pago de glosas y títulos	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
51	Liquidación de Boletines de Cesantía de afiliados fallecidos	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
52	Control de Operadores	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3
53	Consulta Registro Civil	HOST	Alta (A)	3	Baja (B)	1	Media (M)	2	3

III.7.3. Identificación y valoración de las vulnerabilidades y amenazas

En la Tabla III-8 se muestran las vulnerabilidades y amenazas de los activos de la plataforma Host – IESS, así como el impacto de las amenazas en los activos según su degradación, medidas en las dimensiones de seguridad como: Confidencialidad, Integridad y Disponibilidad, así como la asignación de la frecuencia de ocurrencia de la amenaza para el cálculo del riesgo expuesto, que han sido identificadas.

Tabla III-8. Impacto de las amenazas en los activos según su degradación Host – IESS

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confiableidad	TOTAL	FRECUENCIA	RIESGO
Main-Frame Z10BC	3	Posibilidad de incendios	Daños ocasionados por fuego	100%	50%	20%	3	0,1	0,3
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	50%	20%	3	0,1	0,3
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres Naturales (Terremotos)	100%	100%	20%	3	0,1	0,3
		UPS sin soporte técnico	Daños ocasionados por corte de suministro eléctrico	50%	50%	50%	1,5	0,1	0,15
		Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	50%	50%	20%	1,5	1	1,5
		Falta de capacitación (personal de administración)	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	50%	50%	50%	1,5	0,1	0,15
		Imposibilidad de brindar servicio por cortes en los enlaces de datos	Posibilidad de tener interrupción de servicios de enlaces de datos	100%	50%	50%	3	0,1	0,3
		No tener soporte y garantía del fabricante	Falta de soporte y garantía del fabricante sobre el hardware en el que está instalada la solución	100%	100%	50%	3	2	6

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confiableidad	TOTAL	FRECUENCIA	RIESGO
		No tener al momento soporte del fabricante del equipo	Falta de soporte y actualización del equipo	50%	50%	20%	1,5	2	3
		Falla del equipo	Perdida de servicio de conectividad con elementos periféricos de la plataforma	100%	50%	50%	3	1	3
		Falta de servicio	No contar con un sistema de alimentación eléctrica externa (grupo electrógeno)	50%	100%	100%	3	0,1	0,3
		Falta de garantía del fabricante (no se resuelvan los problemas graves)	Posibilidad de tener cortes en la continuidad del servicio (disponibilidad)	100%	100%	10%	3	0,1	0,3
UNIDAD DE CARTUCHOS	2	Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	50%	50%	20%	1,5	2	3
		Falta de protección contra inundaciones	Daños ocasionados por agua	50%	50%	20%	1,5	0,1	0,15
		Posibilidad de incendios	Daños ocasionados por fuego	100%	100%	10%	3	0,1	0,3
		Funcionamiento inadecuado de UPS (sin soporte)	Daños ocasionados por corte de suministro eléctrico	100%	100%	20%	3	1	3
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres Naturales (Terremotos)	100%	100%	10%	3	0,1	0,3

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL	FRECUENCIA	RIESGO
		Falta de capacitación (personal de administración)	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	50%	50%	20%	1,5	0,1	0,15
		Control de acceso de entrada y salida	Robo	100%	100%	50%	3	0,1	0,3
		Falta de planes de contingencia y políticas formalizados	Falta y actualización de planes de contingencia y políticas de uso formalizado	100%	100%	50%	3	0,1	0,3
		Robo de clave o ingreso a máquinas de administración	Acceso indebido de personas no autorizadas (lógico)	100%	100%	50%	3	0,1	0,3
		Problemas con actualizaciones y mantenimientos por vigencia tecnológica vencida	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	100%	100%	50%	3	3	9
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	100%	20%	3	0,1	0,3
		No contar con medios de respaldos	No continuidad con el proyecto de cierre de host	100%	100%	20%	3	3	9
ALMACENAMIENTO (STORAGE)	3	Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	100%	20%	3	1	3
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	100%	20%	3	0,1	0,3

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confiableidad	TOTAL	FRECUENCIA	RIESGO
		Posibilidad de incendios	Daños ocasionados por fuego	100%	100%	20%	3	0,1	0,3
		Funcionamiento inadecuado de UPS (sin soporte)	Daños ocasionados por corte de suministro eléctrico	100%	50%	20%	3	0,1	0,3
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres Naturales (Terremotos)	100%	100%	10%	3	0,1	0,3
		Crecimiento no planificado de personal, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo	50%	50%	50%	1,5	1	1,5
		Falta de capacitación (personal de administración)	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	100%	50%	50%	3	0,1	0,3
		Control de acceso de entrada y salida	Robo	100%	100%	20%	3	0,1	0,3
		Falta de planes de contingencia y políticas formalizados	Falta y actualización de planes de contingencia y políticas de uso formalizado		50%	50%	1,5	0,1	0,15
		Robo de clave o ingreso a máquinas de administración	Acceso indebido de personas no autorizadas (lógico)	100%	50%	20%	3	0,1	0,3
		Capacidad y disponibilidad de almacenamiento	No contar con capacidad para almacenamiento	100%	50%	20%	3	1	3
		Falla del equipo	Pérdida de información de los aplicativos vigentes en Host,	100%	100%	50%	3	1	3

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confiableidad	TOTAL	FRECUENCIA	RIESGO
			afectando la continuidad de la operación y servicios						
		Problemas con actualizaciones y mantenimientos por vigencia tecnológica vencida	Daños ocasionados por falta de mantenimiento (físico y lógico), actualización de sistema operativo	100%	100%	50%	3	3	9
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	50%	20%	3	0,1	0,3
		No contar con el equipo de almacenamiento	No continuidad con el proyecto de cierre de host	100%	100%	50%	3	0,1	0,3
SERVIDOR HMC	1	Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	30%	30%	10%	0,9	0,1	0,09
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	50%	10%	3	0,1	0,3
		Posibilidad de incendios	Daños ocasionados por fuego	100%	100%	10%	3	0,1	0,3
		Funcionamiento inadecuado de UPS (sin soporte)	Daños ocasionados por corte de suministro eléctrico	100%	100%	10%	3	0,1	0,3
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres Naturales (Terremotos)	100%	100%	10%	3	0,1	0,3
		Crecimiento no planificado de entidades externas, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo	30%	30%	10%	0,9	0,1	0,09

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confiableidad	TOTAL	FRECUENCIA	RIESGO
		Falta de capacitación (personal de administración)	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	100%	50%	20%	3	0,1	0,3
		Control de acceso de entrada y salida	Robo	100%	100%	50%	3	0,1	0,3
		Falta de planes de contingencia y políticas formalizados	Falta y actualización de planes de contingencia y políticas de uso formalizado	50%	50%	20%	1,5	0,1	0,15
		Robo de clave o ingreso a máquinas de administración	Acceso indebido de personas no autorizadas (lógico)	50%	50%	10%	1,5	0,1	0,15
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	50%	50%	20%	1,5	0,1	0,15
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	50%	50%	20%	1,5	0,1	0,15
		No existe una política formal de cambio de credenciales	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	50%	50%	20%	1,5	0,1	0,15
AIRE DE PRESICION	3	Falla del equipo	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	100%	20%	3	0,1	0,3
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	100%	20%	3	0,1	0,3

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL	FRECUENCIA	RIESGO
		Posibilidad de incendios	Daños ocasionados por fuego	100%	100%	20%	3	0,1	0,3
		Funcionamiento inadecuado de UPS (sin soporte)	Daños ocasionados por corte de suministro eléctrico	100%	100%	20%	3	0,1	0,3
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres Naturales (Terremotos)	100%	100%	10%	3	0,1	0,3
		Falta de capacitación (personal de administración)	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	50%	50%	20%	1,5	0,1	0,15
		Control de acceso de entrada y salida	Robo	100%	100%	20%	3	0,1	0,3
		Falta de planes de contingencia y políticas formalizados	Falta y actualización de planes de contingencia y políticas de uso formalizado	100%	50%	20%	3	0,1	0,3
		Robo de clave o ingreso a máquinas de administración	Acceso indebido de personas no autorizadas (lógico)	100%	50%	50%	3	0,1	0,3
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento	100%	50%	20%	3	0,1	0,3
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	50%	20%	3	0,1	0,3
		No existe una política formal de cambio de credenciales	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	100%	50%	20%	3	0,1	0,3

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL	FRECUENCIA	RIESGO
AIRE TIPO MOCHILA	2	Falla del equipo	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	100%	20%	3	0,1	0,3
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	100%	20%	3	0,1	0,3
		Posibilidad de incendios	Daños ocasionados por fuego	100%	100%	20%	3	0,1	0,3
		Funcionamiento inadecuado de UPS (sin soporte)	Daños ocasionados por corte de suministro eléctrico	100%	100%	20%	3	0,1	0,3
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres Naturales (Terremotos)	100%	100%	10%	3	0,1	0,3
		Falta de capacitación (personal de administración)	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	50%	50%	20%	1,5	0,1	0,15
		Control de acceso de entrada y salida	Robo	100%	100%	20%	3	0,1	0,3
		Falta de planes de contingencia y políticas formalizados	Falta y actualización de planes de contingencia y políticas de uso formalizado	100%	50%	20%	3	0,1	0,3
		Robo de clave o ingreso a máquinas de administración	Acceso indebido de personas no autorizadas (lógico)	100%	50%	50%	3	0,1	0,3
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento	100%	50%	20%	3	0,1	0,3

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL	FRECUENCIA	RIESGO
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	50%	20%	3	0,1	0,3
		No existe una política formal de cambio de credenciales	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	100%	50%	20%	3	0,1	0,3
UPS	3	Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	100%	20%	3	0,1	0,3
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	50%	20%	3	0,1	0,3
		Posibilidad de incendios	Daños ocasionados por fuego	100%	100%	20%	3	0,1	0,3
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres Naturales (Terremotos)	100%	100%	10%	3	0,1	0,3
		Crecimiento no planificado de entidades externas, aplicativos y transaccionalidad	Degradación por saturación de carga eléctrica	50%	50%	20%	1,5	0,1	0,15
		Falta de capacitación (personal de administración)	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	100%	100%	20%	3	0,1	0,3
		Control de acceso de entrada y salida	Robo	100%	100%	20%	3	0,1	0,3

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confiablez	TOTAL	FRECUENCIA	RIESGO
		Falta de planes de contingencia y políticas formalizados	Falta y actualización de planes de contingencia y políticas de uso formalizado	50%	50%	10%	1,5	0,1	0,15
		Robo de clave o ingreso a máquinas de administración	Acceso indebido de personas no autorizadas (lógico)	100%	50%	20%	3	0,1	0,3
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento	100%	100%	20%	3	3	9
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	50%	20%	3	0,1	0,3
		No existe una política formal de cambio de credenciales	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	50%	50%	20%	1,5	0,1	0,15
SERVIDOR UNIX (MICROS)	3	Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	100%	20%	3	0,1	0,3
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	100%	20%	3	0,1	0,3
		Posibilidad de incendios	Daños ocasionados por fuego	100%	100%	20%	3	0,1	0,3
		Funcionamiento inadecuado de UPS (sin soporte)	Daños ocasionados por corte de suministro eléctrico	100%	100%	10%	3	0,1	0,3
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres Naturales (Terremotos)	100%	100%	10%	3	0,1	0,3

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL	FRECUENCIA	RIESGO
		Crecimiento no planificado de entidades externas, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo	50%	50%	20%	1,5	0,1	0,15
		Falta de capacitación (personal de administración)	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	100%	50%	20%	3	0,1	0,3
		Control de acceso de entrada y salida	Robo	100%	100%	20%	3	0,1	0,3
		Falta de planes de contingencia y políticas formalizados	Falta y actualización de planes de contingencia y políticas de uso formalizado	50%	50%	20%	1,5	0,1	0,15
		Robo de clave o ingreso a máquinas de administración	Acceso indebido de personas no autorizadas (lógico)	100%	50%	10%	3	0,1	0,3
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	100%	100%	20%	3	3	9
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	50%	20%	3	0,1	0,3
		No existe una política formal de cambio de credenciales	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	100%	50%	20%	3	0,1	0,3

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confiableidad	TOTAL	FRECUENCIA	RIESGO
SERVER VTAPE	2	Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	50%	20%	3	0,1	0,3
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	100%	20%	3	0,1	0,3
		Posibilidad de incendios	Daños ocasionados por fuego	100%	100%	20%	3	0,1	0,3
		Funcionamiento inadecuado de UPS (sin soporte)	Daños ocasionados por corte de suministro eléctrico	100%	100%	20%	3	0,1	0,3
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres Naturales (Terremotos)	100%	100%	10%	3	0,1	0,3
		Crecimiento no planificado de entidades externas, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo	100%	50%	20%	3	0,1	0,3
		Falta de capacitación (personal de administración)	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	100%	50%	20%	3	0,1	0,3
		Control de acceso de entrada y salida	Robo	100%	100%	20%	3	0,1	0,3
		Falta de planes de contingencia y políticas formalizados	Falta y actualización de planes de contingencia y políticas de uso formalizado	50%	50%	20%	1,5	0,1	0,15

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confiableidad	TOTAL	FRECUENCIA	RIESGO
		Robo de clave o ingreso a máquinas de administración	Acceso indebido de personas no autorizadas (lógico)	100%	50%	20%	3	0,1	0,3
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	100%	100%	20%	3	3	9
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	50%	20%	3	0,1	0,3
		No existe una política formal de cambio de credenciales	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	100%	50%	20%	3	0,1	0,3
SWITCH DE PASO	3	Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	100%	20%	3	0,1	0,3
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	100%	20%	3	0,1	0,3
		Posibilidad de incendios	Daños ocasionados por fuego	100%	100%	20%	3	0,1	0,3
		Funcionamiento inadecuado de UPS (sin soporte)	Daños ocasionados por corte de suministro eléctrico	100%	100%	20%	3	0,1	0,3
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres Naturales (Terremotos)	100%	100%	10%	3	0,1	0,3

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL	FRECUENCIA	RIESGO
		Crecimiento no planificado de entidades externas, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo	50%	50%	20%	1,5	0,1	0,15
		Falta de capacitación (personal de administración)	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	100%	50%	20%	3	0,1	0,3
		Control de acceso de entrada y salida	Robo	100%	100%	20%	3	0,1	0,3
		Falta de planes de contingencia y políticas formalizados	Falta y actualización de planes de contingencia y políticas de uso formalizado	100%	50%	20%	3	0,1	0,3
		Robo de clave o ingreso a máquinas de administración	Acceso indebido de personas no autorizadas (lógico)	100%	50%	20%	3	0,1	0,3
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento	100%	100%	20%	3	3	9
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	50%	20%	3	0,1	0,3
		No existe una política formal de cambio de credenciales	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	100%	50%	20%	3	0,1	0,3

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL	FRECUENCIA	RIESGO
Aplicativos alojados en el sistema HOST	3	Aplicación de cambios sin pruebas	No contar con las pruebas unitarias necesarias para cambio	50%	50%	20%	1,5	0,1	0,15
		Falta de capacitación (personal de administración)	Inadecuado manejo de mantenimiento de los aplicativos	100%	100%	20%	3	0,1	0,3
		Imposibilidad de recuperar los aplicativos	Falta y actualización de planes de contingencia	100%	100%	20%	3	1	3
		Robo de clave o ingreso a máquinas de administración	Acceso indebido de personas no autorizadas (lógico)	50%	100%	100%	3	0,1	0,3
		Pisar los cambios recientes de los aplicativos	No tener versionado el código fuente de los aplicativos	50%	100%	50%	3	1	3
		Mal funcionamiento de los aplicativos	No tener un ambiente de desarrollo y pruebas	25%	100%	50%	3	0,1	0,3
		No proporcionar servicios	No contar con alta disponibilidad	100%	50%	50%	3	3	9
		Accesos no controlados a los aplicativos	No contar con modulo autenticación	25%	100%	100%	3	0,1	0,3
		Mal uso de las cuentas de usuario	Las claves no siguen las buenas prácticas de construcción	25%	100%	100%	3	1	3
		No existe una política formal de cambio de credenciales	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	25%	100%	100%	3	1	3

III.7.4. Gráfica de radar de los riesgos por activo

La Tabla III-9 muestra los riesgos de la plataforma Host – IESS que han sido identificados con la siguiente información:

- Valor actual: Promedio de todos los riesgos.
- Valor objetivo: Recomendación de la SDNSI de reducción de riesgo (al menos el 50%).
- Valor límite: Valor dado por condiciones gráficas, al que nunca se debería llegar.

Tabla III-9. Tabla de valores de riesgos Host – IESS

ACTIVO	ACTUAL	OBJETIVO	LIMITE
Main-Frame Z10BC	1,30	0,65	3
UNIDAD DE CARTUCHOS	2,18	1,09	3
ALMACENAMIENTO (STORAGE)	1,58	0,79	3
SERVIDOR HMC	0,21	0,11	3
AIRE DE PRESICION	0,30	0,15	3
AIRE TIPO MOCHILA	0,29	0,14	3
UPS	0,99	0,49	3
SERVIDOR UNIX (MICROS)	0,95	0,47	3
SERVER VTAPE	0,96	0,48	3
SWITCH DE PASO	0,96	0,48	3
Aplicativos alojados en el sistema HOST	2,24	1,12	3

La Figura III-5 muestra un reporte de los riesgos de la plataforma Host – IESS, que indica el riesgo actual, objetivo y el límite aceptable.

Figura III-5. Reporte de riesgos plataforma Host – IESS

III.7.5. Controles o salvaguardas sugeridas

La Tabla III-10 muestra las salvaguardas que han sido identificadas para cada tripleta activo – vulnerabilidad – amenaza.

Tabla III-10. Salvaguardas por activo Host – IESS

Activo	Vulnerabilidad	Amenazas	Salvaguarda
Main-Frame Z10BC	No tener soporte y garantía del fabricante	Falta de soporte y garantía del fabricante sobre el hardware en el que está instalada la solución	Revisar y validar la factibilidad de arreglar los daños existentes y/o gestionar soporte técnico y mantenimiento
UNIDAD DE CARTUCHOS	Problemas con actualizaciones y mantenimientos por vigencia tecnológica vencida	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	Implementar una solución de gestión de respaldo(servicio) que permitan el uso de cartuchos y gestionar soporte técnico y mantenimiento periódico sobre dicho equipo
	No contar con medios de respaldos	No continuidad con el proyecto de cierre de host	
ALMACENAMIENTO (STORAGE)	Problemas con actualizaciones y mantenimientos por vigencia tecnológica vencida	Daños ocasionados por falta de mantenimiento (físico y lógico), actualización de sistema operativo	Contar con soporte técnico y mantenimiento periódico que garantice el actual almacenamiento de los aplicativos de Host, data y sistema operativo.
UPS	Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento	Habilitar la carga en el ups EATON (sin carga) instalado en el data center para tener un equipo de contingencia
SERVIDOR UNIX (MICROS)	Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	Contar con la documentación de instalación del SERVIDOR UNIX (MICROS) y realizar un piloto de clonación del sistema en otro equipo
SERVER VTAPE	Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	Gestionar soporte técnico y mantenimiento periódico en dicho equipo para la gestión de respaldos
SWITCH DE PASO	Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento	Tener mecanismo de contingencia de dicho equipo
Aplicativos alojados en el sistema HOST	No proporcionar servicios	No contar con alta disponibilidad	Migrar los aplicativos, data y sistema operativo del Host a un Storage que permita garantizar alta disponibilidad con vigencia tecnológica.

III.7.6. Conclusiones

- Mediante el presente análisis y evaluación de riesgos, se concluye que el equipo Main-Frame Z10BC no tiene mantenimiento correctivo ni garantía del fabricante, siendo un activo crítico de la Infraestructura informática del IESS.

- El equipo de almacenamiento Storage, tiene una vulnerabilidad crítica debido a problemas con actualizaciones y mantenimientos por vigencia tecnológica vencida, lo cual al presentarse un problema puede desembocar en pérdida del equipo y de disponibilidad de los aplicativos alojados en el mismo.
- El equipo UPS EATON debe conectarse a la carga del Data Center, para tener un equipo de contingencia en el sistema existente del banco de UPS del Edificio Matriz donde se encuentra instalada la Plataforma Z10, a fin de que no se afecte la operación.
- El equipo Servidor Vtape puede sufrir daños y al no contar con soporte y mantenimiento, puede ocasionar que se afecte al proyecto de salvaguarda, migración para el cierre del host, servicio de procesos batch y no se tenga forma de generar respaldos de información.
- El equipo Switch de paso puede sufrir daños y, al no contar con soporte y mantenimiento, puede ocasionar que se afecte la operación del Main-Frame Z10BC.
- El equipo Unidad de cartuchos puede sufrir daños y, al no contar con soporte y mantenimiento, puede ocasionar que se afecte la operación, el proyecto de salvaguarda, migración para el cierre del host, servicio de procesos batch y no se tenga forma de generar respaldos físicos de la información.
- Resultado del presente análisis, los riesgos localizados en los cuadrantes de alto impacto y bajo frecuencia, y bajo impacto y alta frecuencia de los mapas de riesgos, deben ser monitoreados con periodicidad.

III.8. Análisis y Gestión de Riesgos Plataforma Oracle – IESS

En esta sección se describen las actividades definidas en el punto III.5, para la plataforma Oracle – IESS, y se han analizado los riesgos de los activos de la plataforma y sus dependientes.

III.8.1. Dependencias de activos

La Figura III-6 muestra como está estructurada la plataforma Oracle – IESS, con los componentes y sus dependencias.

Figura III-6 Diagrama de dependencia de equipos de la Plataforma Oracle – IESS

La dependencia directa de los equipos de la Plataforma Oracle – IESS se establece con los equipos Power 770, Power 780 en los que se encuentran instaladas los diferentes hosts de la base de datos, tal y como se muestra en la Figura III-6.

III.8.2. Identificación y valoración de los activos

La valoración de los activos (véase Tabla III-11) se ha realizado con personal técnico de la Plataforma Oracle – IESS, Ingeniera Paulina Gallo encargada del licenciamiento de la base de datos Oracle y con el ingeniero Marcelo Vásquez encargado del área de Plataforma de Servidores.

Tabla III-11. Valoración de activos en disponibilidad, integridad, confidencialidad y criticidad Oracle – IESS

IDENTIFICACIÓN DE ACTIVOS			VALORACIÓN DE ACTIVOS						
#	Activo	Dueño de Activo	Disponibilidad	Valor	Integridad	Valor	Confiable	Valor	Criticidad
1	Power 770 (prosrviuorac1 BDD prosrviuorac2 BDD)	BASES DE DATOS	Alta (A)	3	Media (M)	2	Media (M)	2	3
2	Power 770 (prosrviuorac3 BDD prosrviuorac4 BDD)	BASES DE DATOS	Alta (A)	3	Media (M)	2	Media (M)	2	3
3	Power 770 (SrvuioBD05 BDD)	BASES DE DATOS	Alta (A)	3	Media (M)	2	Media (M)	2	3
4	Power 770 (Srvuiodbpen BDD)	BASES DE DATOS	Alta (A)	3	Media (M)	2	Media (M)	2	3
5	Power 780 (prosrviuorac1 prosrviuorac2)	BASES DE DATOS	Alta (A)	3	Media (M)	2	Media (M)	2	3
6	Power 780 (prosrviuorac3 prosrviuorac4)	BASES DE DATOS	Alta (A)	3	Media (M)	2	Media (M)	2	3
6	Hosts (prosrviuorac1 BDD prosrviuorac2 BDD prosrviuorac3 BDD prosrviuorac4 BDD prosrviuorac5 BDD)	BASES DE DATOS	Alta (A)	3	Alta (A)	3	Alta (A)	3	3
7	Host (BDD- Replica Guayaquil -1 BDD- Replica Guayaquil -2)	BASES DE DATOS	Alta (A)	3	Alta (A)	3	Alta (A)	3	3
8	Host Grid Control	BASES DE DATOS	Media (M)	2	Baja (B)	1	Baja (B)	1	2
9	Host Servidor del SOA	BASES DE DATOS	Media (M)	2	Media (M)	2	Media (M)	2	2
10	Host Serv. Base de datos unificadas	BASES DE DATOS	Alta (A)	3	Media (M)	2	Media (M)	2	3

IDENTIFICACIÓN DE ACTIVOS			VALORACIÓN DE ACTIVOS						
#	Activo	Dueño de Activo	Disponibilidad	Valor	Integridad	Valor	Confidencialidad	Valor	Criticidad
11	Host Base de Datos. Desarrollo y Calidad	BASES DE DATOS	Media (M)	2	Baja (B)	1	Media (M)	2	2

III.8.3. Identificación y valoración de las vulnerabilidades y amenazas

En la Tabla III-12 se muestra las vulnerabilidades y amenazas de los activos de la plataforma Oracle – IESS, así como el impacto de las amenazas en los activos según su degradación, medidas en las dimensiones de seguridad como: Confidencialidad, Integridad y Disponibilidad, así como la asignación de la frecuencia de ocurrencia de la amenaza para el cálculo del riesgo expuesto, que han sido definidas.

Tabla III-12. Impacto de las amenazas en los activos según su degradación Oracle – IESS

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confiableidad	TOTAL	FRECUENCIA	RIESGO
Power 770 (prosrviuorac1 BDD prosrviuorac2 BDD)	3	Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	50%	20%	3	0,1	0,3
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	50%	20%	3	0,1	0,3
		Posibilidad de incendios	Daños ocasionados por fuego	100%	100%	20%	3	0,1	0,3
		Funcionamiento inadecuado de UPS (sin soporte)	Daños ocasionados por corte de suministro eléctrico	50%	5%	5%	1,5	1	1,5
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres Naturales (Terremotos)	100%	100%	20%	3	0,1	0,3
		Crecimiento no planificado de personal, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo	60%	70%	20%	2,1	2	4,2
		Falta de capacitación (personal de administración)	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	50%	20%	20%	1,5	0,1	0,15
		Control de acceso de entrada y salida	Robo	100%	100%	20%	3	0,1	0,3

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL	FRECUENCIA	RIESGO
		Falta de planes de contingencia y políticas formalizados	Falta y actualización de planes de contingencia y políticas de uso formalizado	100%	50%	20%	3	3	9
		Robo de clave o ingreso a máquinas de administración	Acceso indebido de personas no autorizadas (lógico)	100%	70%	70%	3	0,1	0,3
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	50%	70%	20%	2,1	2	4,2
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	50%	20%	3	0,1	0,3
		No existe una política formal de cambio de credenciales	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	70%	20%	10%	2,1	1	2,1
Power 770 (prosrviuorac3 BDD prosrviuorac4 BDD)	3	Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	50%	20%	3	0,1	0,3
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	50%	20%	3	0,1	0,3
		Posibilidad de incendios	Daños ocasionados por fuego	100%	100%	20%	3	0,1	0,3

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL	FRECUENCIA	RIESGO
		Funcionamiento inadecuado de UPS (sin soporte)	Daños ocasionados por corte de suministro eléctrico	50%	5%	5%	1,5	1	1,5
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres Naturales (Terremotos)	100%	100%	20%	3	0,1	0,3
		Crecimiento no planificado de personal, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo	60%	70%	20%	2,1	2	4,2
		Falta de capacitación (personal de administración)	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	50%	20%	20%	1,5	0,1	0,15
		Control de acceso de entrada y salida	Robo	100%	100%	20%	3	0,1	0,3
		Falta de planes de contingencia y políticas formalizados	Falta y actualización de planes de contingencia y políticas de uso formalizado	100%	50%	20%	3	3	9
		Robo de clave o ingreso a máquinas de administración	Acceso indebido de personas no autorizadas (lógico)	100%	70%	70%	3	0,1	0,3
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y	50%	70%	20%	2,1	2	4,2

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confiableidad	TOTAL	FRECUENCIA	RIESGO
Power (SrvuioBD05 BDD)	770		actualización de sistema operativo						
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	50%	20%	3	0,1	0,3
		No existe una política formal de cambio de credenciales	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	70%	20%	10%	2,1	1	2,1
	3	Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	50%	20%	3	0,1	0,3
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	50%	20%	3	0,1	0,3
		Posibilidad de incendios	Daños ocasionados por fuego	100%	100%	20%	3	0,1	0,3
		Funcionamiento inadecuado de UPS (sin soporte)	Daños ocasionados por corte de suministro eléctrico	50%	5%	5%	1,5	1	1,5
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres Naturales (Terremotos)	100%	100%	20%	3	0,1	0,3
		Crecimiento no planificado de personal, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo	60%	70%	20%	2,1	2	4,2

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL	FRECUENCIA	RIESGO
		Falta de capacitación (personal de administración)	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	50%	20%	20%	1,5	0,1	0,15
		Control de acceso de entrada y salida	Robo	100%	100%	20%	3	0,1	0,3
		Falta de planes de contingencia y políticas formalizados	Falta y actualización de planes de contingencia y políticas de uso formalizado	100%	50%	20%	3	3	9
		Robo de clave o ingreso a máquinas de administración	Acceso indebido de personas no autorizadas (lógico)	100%	70%	70%	3	0,1	0,3
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	50%	70%	20%	2,1	2	4,2
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	50%	20%	3	0,1	0,3
		No existe una política formal de cambio de credenciales	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	70%	20%	10%	2,1	1	2,1

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL	FRECUENCIA	RIESGO
Power 770 (Srvuiodbpen BDD)	3	Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	50%	20%	3	0,1	0,3
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	50%	20%	3	0,1	0,3
		Posibilidad de incendios	Daños ocasionados por fuego	100%	100%	20%	3	0,1	0,3
		Funcionamiento inadecuado de UPS (sin soporte)	Daños ocasionados por corte de suministro eléctrico	50%	5%	5%	1,5	1	1,5
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres Naturales (Terremotos)	100%	100%	20%	3	0,1	0,3
		Crecimiento no planificado de personal, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo	60%	70%	20%	2,1	2	4,2
		Falta de capacitación (personal de administración)	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	50%	20%	20%	1,5	0,1	0,15
		Control de acceso de entrada y salida	Robo	100%	100%	20%	3	0,1	0,3

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL	FRECUENCIA	RIESGO
		Falta de planes de contingencia y políticas formalizados	Falta y actualización de planes de contingencia y políticas de uso formalizado	100%	50%	20%	3	3	9
		Robo de clave o ingreso a máquinas de administración	Acceso indebido de personas no autorizadas (lógico)	100%	70%	70%	3	0,1	0,3
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	50%	70%	20%	2,1	2	4,2
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	50%	20%	3	0,1	0,3
		No existe una política formal de cambio de credenciales	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	70%	20%	10%	2,1	1	2,1
Power (prosrviuorac1 prosrviuorac2)	780 3	Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	50%	20%	3	0,1	0,3
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	50%	20%	3	0,1	0,3
		Posibilidad de incendios	Daños ocasionados por fuego	100%	100%	20%	3	0,1	0,3

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL	FRECUENCIA	RIESGO
		Funcionamiento inadecuado de UPS (sin soporte)	Daños ocasionados por corte de suministro eléctrico	50%	5%	5%	1,5	1	1,5
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres Naturales (Terremotos)	100%	100%	20%	3	0,1	0,3
		Crecimiento no planificado de personal, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo	60%	70%	20%	2,1	2	4,2
		Falta de capacitación (personal de administración)	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	50%	20%	20%	1,5	0,1	0,15
		Control de acceso de entrada y salida	Robo	100%	100%	20%	3	0,1	0,3
		Falta de planes de contingencia y políticas formalizados	Falta y actualización de planes de contingencia y políticas de uso formalizado	100%	50%	20%	3	3	9
		Robo de clave o ingreso a máquinas de administración	Acceso indebido de personas no autorizadas (lógico)	100%	70%	70%	3	0,1	0,3
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y	50%	70%	20%	2,1	2	4,2

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO		
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confiability	TOTAL	FRECUENCIA	RIESGO	
			actualización de sistema operativo							
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	50%	20%	3	0,1	0,3	
		No existe una política formal de cambio de credenciales	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	70%	20%	10%	2,1	1	2,1	
Power (prosrviuorac3 prosrviuorac4)	780	3	Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	50%	20%	3	0,1	0,3
			Falta de protección contra inundaciones	Daños ocasionados por agua	100%	50%	20%	3	0,1	0,3
			Posibilidad de incendios	Daños ocasionados por fuego	100%	100%	20%	3	0,1	0,3
			Funcionamiento inadecuado de UPS (sin soporte)	Daños ocasionados por corte de suministro eléctrico	50%	5%	5%	1,5	1	1,5
			Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres Naturales (Terremotos)	100%	100%	20%	3	0,1	0,3
			Crecimiento no planificado de personal, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo	60%	70%	20%	2,1	2	4,2

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL	FRECUENCIA	RIESGO
		Falta de capacitación (personal de administración)	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	50%	20%	20%	1,5	0,1	0,15
		Control de acceso de entrada y salida	Robo	100%	100%	20%	3	0,1	0,3
		Falta de planes de contingencia y políticas formalizados	Falta y actualización de planes de contingencia y políticas de uso formalizado	100%	50%	20%	3	3	9
		Robo de clave o ingreso a máquinas de administración	Acceso indebido de personas no autorizadas (lógico)	100%	70%	70%	3	0,1	0,3
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico), actualización de sistema operativo y suscripción de vacunas digitales	50%	70%	20%	2,1	2	4,2
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	50%	20%	3	0,1	0,3
		No existe una política formal de cambio de credenciales	Credenciales de acceso genéricas/ por defecto y cambios periódicos de claves de administradores	70%	20%	10%	2,1	1	2,1

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL	FRECUENCIA	RIESGO
Hosts (prosrvuiorac1 BDD prosrvuiorac2 BDD prosrvuiorac3 BDD prosrvuiorac4 BDD prosrvuiorac5 BDD)	3	No se encuentren cubiertos bugs y vulnerabilidades conocidas	No contar con una versión de software de base de datos actualizada	100%	100%	100%	3	1	3
		Imposibilidad de resolución urgente de incidentes de la base de datos	No tener con soporte y mantenimiento del fabricante	100%	100%	100%	3	3	9
		Problemas legales con el fabricante del software	No tener un licenciamiento legalizado y otorgado por el fabricante	100%	100%	100%	3	3	9
		Falla crítica del motor de base de datos	Pérdida de disponibilidad del servicio de base de datos para los aplicativos tanto del Banco del BIESS, Historia Laboral, Recaudación, Fondos de Reserva, Riesgos del trabajo, Pensiones, Sistema de Salud entre otros.	100%	100%	100%	3	1	3
		No cuenta con sistema de respaldos	Pérdida total o parcial de información alojada en la base de datos en casos contingentes	100%	100%	100%	3	1	3
		No dispone de los recursos necesarios (hardware)	Tiempos de respuesta muy elevados en horas pico	100%	100%	100%	3	1	3

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL	FRECUENCIA	RIESGO
		No dispone de soporte técnico especializado para implementación escalable	Uso no óptimo de las prestaciones de la herramienta	100%	100%	100%	3	1	3
		Desconocimiento de la estructura de la base de datos	No contar con un diccionario de datos	50%	50%	50%	1,5	1	1,5
		Imposibilidad de cambio o mejoras en la administración	No contar con suficiente personal capacitado en la administración de la base	20%	30%	30%	0,9	2	1,8
		Imposibilita de mejoras en la estructura de la base de datos	No contar con una arquitectura de base de datos	100%	100%	100%	3	1	3
		Dificultad de crecimiento de la base de datos	Falta de planes de capacidad de crecimiento de la base	100%	100%	100%	3	1	3
		Imposibilidad de proporcionar servicios de base de datos en el sitio principal	No contar con switch over con una base de datos en un sitio de datos alternativo	100%	100%	100%	3	1	3
		Imposibilidad de proporcionar el servicio de base de datos	Falta de planes de contingencia	100%	100%	100%	3	3	9
Host (BDD- Replica Guayaquil -1	3	Imposibilidad de recuperación de la base de datos desde una base de datos replicada	No contar una versión actualizada de la una base de datos replicada correctamente	100%	100%	100%	3	1	3

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL	FRECUENCIA	RIESGO
BDD- Replica Guayaquil - 2)		Imposibilidad de resolución urgente de incidentes de la base de datos	No tener con soporte y mantenimiento del fabricante	100%	100%	100%	3	3	9
		Problemas legales con el fabricante del software	No tener con licenciamiento legalizado y otorgado por el fabricante	100%	100%	100%	3	3	9
		Imposibilidad de recuperación de la base de datos desde una base de datos replicada	Pérdida total o parcial de información de la réplica de base de datos por no contar con un sistema de respaldos	100%	100%	100%	3	1	3
		No dispone de los recursos necesarios (hardware, software, comunicaciones)	Tiempos de respuesta muy elevado para la gestión de un replica de base de datos	80%	100%	100%	3	0,8	2,4
		No dispone de soporte técnico especializado para implementación escalable	Uso no óptimo de las prestaciones de la herramienta	100%	100%	100%	3	1	3
		Imposibilidad de cambio o mejoras en la administración	No contar con personal capacitado en la administración de la base	10%	100%	100%	3	1	3
		Imposibilidad de proporcionar el servicio de base de datos	Falta de planes de contingencia	100%	100%	100%	3	1	3

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confiableidad	TOTAL	FRECUENCIA	RIESGO
Host Grid Control	2	No se encuentren cubiertos bugs y vulnerabilidades conocidas	No contar con control, monitoreo y administración de la base de datos	100%	50%	50%	3	1	3
		Imposibilidad de resolución urgente de incidentes de la base de datos	No contar con soporte y mantenimiento del fabricante	100%	50%	50%	3	1	3
		No dispone de los recursos necesarios (hardware)	Tiempos de respuesta muy elevados en horas pico	100%	50%	50%	3	1	3
		No dispone de soporte técnico especializado para implementación escalable	Uso no óptimo de las prestaciones de la herramienta	100%	50%	50%	3	1	3
		Desconocimiento de la estructura de la base de datos	No contar con un diccionario de datos	100%	50%	50%	3	1	3
		Imposibilidad de cambio o mejoras en la administración	No contar con personal capacitado en la administración de la base	100%	50%	50%	3	1	3
		Imposibilita de mejoras en la estructura de la base de datos	No contar con una arquitectura de base de datos	100%	50%	50%	3	1	3
		Imposibilidad de proporcionar el servicio de base de datos	Falta de planes de contingencia	100%	50%	50%	3	1	3
Host Servidor del SOA	2	Imposibilidad de resolución urgente de incidentes de la base de datos	No se cuente con soporte y mantenimiento del fabricante	100%	100%	100%	3	1	3

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL	FRECUENCIA	RIESGO
		Problemas legales con el fabricante del software	No contar con licenciamiento legalizado y otorgado por el fabricante	100%	100%	100%	3	1	3
		No dispone de soporte técnico especializado para implementación escalable	Uso no óptimo de las prestaciones de la herramienta	100%	100%	100%	3	1	3
		Imposibilidad de cambio o mejoras en la administración	No contar con suficiente personal capacitado en la administración de servidor SOA	100%	100%	100%	3	1	3
		Imposibilita de mejoras en la estructura de la base de datos	No contar con una arquitectura de base de datos	100%	100%	100%	3	1	3
Host Servidor. Base de datos unificadas	3	No se encuentren cubiertos bugs y vulnerabilidades conocidas	No contar con una versión actualizada del software de la base de datos actualizada	100%	100%	100%	3	2	6
		Imposibilidad de resolución urgente de incidentes de la base de datos	No contar con soporte y mantenimiento del fabricante	100%	100%	100%	3	1	3
		Problemas legales con el fabricante del software	No contar con licenciamiento legalizado y otorgado por el fabricante	100%	100%	100%	3	1	3
		Falla crítica del motor de base de datos	Pérdida de disponibilidad del servicio de base de datos para los aplicativos tanto del Banco del	100%	100%	100%	3	1	3

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confiableidad	TOTAL	FRECUENCIA	RIESGO
			BIESS, Historia Laboral, Recaudación, Fondos de Reserva, Riesgos del trabajo, Pensiones, Sistema de Salud entre otros.						
		No cuenta con sistema de respaldos	Pérdida total o parcial de información alojada en la base de datos en casos contingentes	10%	10%	10%	0,3	1	0,3
		No dispone de los recursos necesarios (hardware)	Tiempos de respuesta muy elevados en horas pico	10%	10%	10%	0,3	1	0,3
		Imposibilidad de cambio o mejoras en la administración	No contar con suficiente personal capacitado en la administración de la base	50%	50%	50%	1,5	1	1,5
		Dificultad de crecimiento de la base de datos	Falta de planes de capacidad de crecimiento de la base	10%	10%	10%	0,3	1	0,3
		Imposibilidad de proporcionar el servicio de base de datos	Falta de planes de contingencia	10%	10%	10%	0,3	1	0,3
Host Base de datos. Desarrollo y Calidad	2	No se encuentren cubiertos bugs y vulnerabilidades conocidas	No contar con una versión de software de base de datos actualizada	10%	0%	10%	0,3	1	0,3
		Imposibilidad de resolución urgente de incidentes de la base de datos	No se cuente con soporte y mantenimiento del fabricante	10%	0%	10%	0,3	1	0,3

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL	FRECUENCIA	RIESGO
		Problemas legales con el fabricante del software	No contar con licenciamiento legalizado y otorgado por el fabricante	10%	0%	10%	0,3	1	0,3
		Falla crítica del motor de base de datos	Pérdida de disponibilidad del servicio de base de datos para los aplicativos tanto del Banco del BIESS, Historia Laboral, Recaudación, Fondos de Reserva, Riesgos del trabajo, Pensiones, Sistema de Salud entre otros.	10%	0%	10%	0,3	1	0,3
		No cuenta con sistema de respaldos	Pérdida total o parcial de información alojada en la base de datos en casos contingentes	10%	0%	10%	0,3	1	0,3
		No dispone de los recursos necesarios (hardware)	Tiempos de respuesta muy elevados en horas pico	10%	0%	10%	0,3	1	0,3
		No dispone de soporte técnico especializado para implementación escalable	Uso no óptimo de las prestaciones de la herramienta	10%	0%	10%	0,3	1	0,3
		Desconocimiento de la estructura de la base de datos	No contar con un diccionario de datos	10%	0%	10%	0,3	1	0,3

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confiableidad	TOTAL	FRECUENCIA	RIESGO
		Imposibilidad de cambio o mejoras en la administración	No contar con personal capacitado en la administración de la base	10%	0%	10%	0,3	1	0,3
		Imposibilita de mejoras en la estructura de la base de datos	No contar con una arquitectura de base de datos	10%	0%	10%	0,3	1	0,3
		Dificultad de crecimiento de la base de datos	Falta de planes de capacidad de crecimiento de la base	10%	0%	10%	0,3	1	0,3
		Imposibilidad de proporcionar servicios de base de datos en el sitio principal	No contar con switch over con una base de datos en un sitio de datos alternativo	10%	0%	10%	0,3	1	0,3
		Imposibilidad de proporcionar el servicio de base de datos	Falta de planes de contingencia	10%	0%	10%	0,3	1	0,3

III.8.4. Gráfica de radar de los riesgos por activo

La Tabla III-13 muestra los riesgos que han sido identificados de la plataforma Oracle – IESS, donde:

- Valor actual: Promedio de todos los riesgos.
- Valor objetivo: Recomendación de la SDNSI de reducción de riesgo (al menos el 50%).
- Valor límite: Valor dado por condiciones gráficas, al que nunca se debería llegar.

Tabla III-13 Tabla de Valores de Riesgos Oracle – IESS

ACTIVO	ACTUAL	OBJETIVO	LIMITE
Power 770 (prosrvuiorac1 BDD, prosrvuiorac2 BDD)	1,79	0,89	6
Power 770 (prosrvuiorac3 BDD, prosrvuiorac4 BDD)	1,79	0,89	6
Power 770 (SrvuiobD05 BDD)	1,79	0,89	6
Power 770 (Srvuiodbpén BDD)	1,79	0,89	6
Power 780 (prosrvuiorac1, prosrvuiorac2)	1,79	0,89	6
Power 780 (prosrvuiorac3, prosrvuiorac4)	1,79	0,89	6
Hosts (prosrvuiorac1 BDD, prosrvuiorac2 BDD, prosrvuiorac3 BDD, prosrvuiorac4 BDD, prosrvuiorac5 BDD)	4,40	2,20	6
Host (BDD- Replica Guayaquil -1 BDD- Replica Guayaquil -2)	4,43	2,21	6
Host Grid Control	3,00	1,50	6
Host Servidor del SOA	3,00	1,50	6
Host Serv. Base de datos unificadas	1,55	0,78	6
Host Base de datos. Desarrollo y Calidad	0,28	0,14	6
Power 770 (prosrvuiorac1 BDD, prosrvuiorac2 BDD)	1,79	0,89	6

La Figura III-7 muestra un reporte de los riesgos que han sido identificados de la plataforma Oracle – IESS, que indica el riesgo actual, objetivo y el límite aceptable.

Figura III-7 Reporte de riesgos Plataforma Oracle – IESS

III.8.5. Controles o salvaguardas sugeridas

La Tabla III-14 muestra las salvaguardas que se han identificado para cada triplete activo – vulnerabilidad – amenaza.

Tabla III-14. Salvaguardas sugeridas Oracle – IESS

ACTIVO	VULNERABILIDADES	AMENAZAS	SALVAGUARDAS
"Power 770 (prosrviuorac1 BDD, prosrviuorac2 BDD)"	Crecimiento no planificado de personal, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo	Contar con un plan de capacidad de crecimiento de los equipos considerando HW, SW y comunicaciones
"Power 770 (prosrviuorac3 BDD, prosrviuorac4 BDD)"	Falta de planes de contingencia y políticas formalizados	Falta y actualización de planes de contingencia y políticas de uso formalizado	Levantar y gestionar un plan de contingencia para el Sitio alterno de datos en conjunto con la SDNSI.
"Power 770 (SrvuiobD05 BDD)"			
"Power 770 (Srvuiodbpén BDD)"			
"Power 780 (prosrviuorac1, prosrviuorac2)"			
"Power 780 (prosrviuorac3, prosrviuorac4)"	Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	Tener soporte y mantenimiento físico y lógico de los equipos

ACTIVO	VULNERABILIDADES	AMENAZAS	SALVAGUARDAS
Hosts (prosrvuiorac1 BDD prosrvuiorac2 BDD prosrvuiorac3 BDD prosrvuiorac4 BDD prosrvuiorac5 BDD)	Imposibilidad de resolución urgente de incidentes de la base de datos	No se cuenta con soporte y mantenimiento del fabricante	Tener el soporte técnico de licencias perpetuas de base de datos Oracle
	Problemas legales con el fabricante del software	No contar con licenciamiento legalizado y otorgado por el fabricante	Disponer de licencias de base de datos Oracle de acuerdo al número de cores utilizados
	Imposibilidad de proporcionar el servicio de base de datos	Falta de planes de contingencia	Tener implementado un plan de contingencia debidamente aprobado
Host (BDD- Replica Guayaquil -1 BDD- Replica Guayaquil -2)	Imposibilidad de resolución urgente de incidentes de la base de datos	No se cuenta con soporte y mantenimiento del fabricante	Tener el soporte técnico de licencias perpetuas de base de datos Oracle
	Problemas legales con el fabricante del software	No contar con licenciamiento legalizado y otorgado por el fabricante	Disponer de licencias de base de datos Oracle de acuerdo al número de cores utilizados
Host Servidor. Base de datos unificadas	No se encuentren cubiertos bugs y vulnerabilidades conocidas	No contar con la una versión de software de base de datos actualizada	Tener el soporte técnico de licencias perpetuas de base de datos Oracle Disponer de licencias de base de datos Oracle de acuerdo al número de cores utilizados

III.8.6. Conclusiones

- Mediante el presente análisis y evaluación de riesgos se concluye que el hardware y software de la plataforma Oracle – IESS son activos críticos de la Infraestructura informática del IESS.
- El hardware y software de la plataforma Oracle – IESS tiene varias amenazas, entre las más severas, se pueden mencionar:
 - No contar con soporte y mantenimiento del fabricante,
 - No contar con licenciamiento legalizado y otorgado por el fabricante,
 - Falta de planes de contingencia.
 - Degradación por saturación de recursos del equipo
- Resultado del presente análisis, los riesgos localizados en los cuadrantes de alto impacto y bajo frecuencia, y bajo impacto y alta frecuencia de los mapas de riesgos, deben ser monitoreados con periodicidad

III.9. Análisis de Riesgos Plataforma Firewall – IESS

En esta sección se describen las actividades definidas en el punto III.5, para la plataforma Firewall – IESS, y se han analizado los riesgos de los activos de la plataforma y sus dependientes.

III.9.1. Dependencias de activos

La Figura III-8 muestra como está estructurada la plataforma Firewall – IESS, con los componentes y sus dependencias.

Figura III-8 Diagrama de dependencia de equipos con Firewall – IESS

III.9.2. Identificación y valoración de activos

La valoración de los activos (véase Tabla III-15) se ha realizado con personal técnico a cargo de la plataforma Firewall – IESS, Ingeniera Silvia Duque encargada de la administración y el stack switch core, ips y stack switch extranet con el ingeniero Fernando Erraez, del Área de redes.

Tabla III-15 Valoración de activos en disponibilidad, integridad, confidencialidad y criticidad Firewall – IESS.

IDENTIFICACIÓN DE ACTIVOS				VALORACIÓN DE ACTIVOS					
	Activo	Dueño de Activo	Disponibilidad	Valor	Integridad	Valor	Confidencialidad	Valor	Criticidad
1	FIREWALL INTERNET	REDES	Alta (A)	3	Media (M)	2	Media (M)	2	3
2	FIREWALL INTERNET	REDES	Alta (A)	3	Media (M)	2	Media (M)	2	3
3	FIREWALL INTRANET	REDES	Alta (A)	3	Media (M)	2	Media (M)	2	3
4	FIREWALL INTRANET	REDES	Alta (A)	3	Media (M)	2	Media (M)	2	3
5	STACK SWITCH CORE	REDES	Alta (A)	3	Baja (B)	1	Media (M)	2	3
6	IPS	REDES	Baja (B)	1	Baja (B)	1	Media (M)	2	2
7	STACK SWITCH EXTRANET	REDES	Alta (A)	3	Baja (B)	1	Media (M)	2	3

III.9.3. Identificación y valoración de vulnerabilidades y amenazas

En la Tabla III-16 se muestra las vulnerabilidades y amenazas de los activos de la plataforma Firewall – IESS, así como el impacto de las amenazas en los activos según su degradación, medidas en las dimensiones de seguridad como: Confidencialidad, Integridad y Disponibilidad, así como la asignación de la frecuencia de ocurrencia de la amenaza para el cálculo del riesgo expuesto, cálculos que han sido analizados con los responsables de los activos, siguiendo los lineamientos definidos.

Tabla III-16. Impacto de las amenazas en los activos según su degradación Firewall – IESS

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confiability	TOTAL	FRECUENCIA	RIESGO
FIREWALL INTERNET (1) FIREWALL INTERNET (2) FIREWALL INTRANET (1) FIREWALL INTRANET (2)	3	Posibilidad de incendios	Daños ocasionados por fuego	100%	50%	20%	3	0,1	0,3
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	50%	20%	3	2	6
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres Naturales (Terremotos)	100%	50%	20%	3	0,1	0,3
		UPS sin soporte técnico	Daños ocasionados por corte de suministro eléctrico	50%	5%	5%	1,5	1	1,5
		Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	80%	50%	20%	2,4	2	4,8
		Falta de capacitación (personal de administración)	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	60%	70%	20%	2,1	2	4,2
		Problemas con actualizaciones de suscripciones y sistema operativo	Falta de actualizaciones de firmas de los módulos con suscripciones y de sistema operativo	30%	20%	20%	0,9	2	1,8
		Falta de socialización de políticas internas y externas	Posibilidad de errores de usuario en la administración, configuración y monitorización del equipo	70%	70%	20%	2,1	2	4,2
		Falta de políticas de acceso para usuarios internos y externos	Acceso indebido de personas no autorizadas al Área de Infraestructura	10%	60%	20%	1,8	0,1	0,18

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL	FRECUENCIA	RIESGO
		Posibilidad de cortes en los enlaces de datos	Posibilidad de tener interrupción de servicios de enlaces de datos	50%	40%	20%	1,5	2	3
		No tener soporte y garantía del fabricante	Posibilidad de daño del equipo	70%	70%	20%	2,1	2	4,2
		No se puede monitorear las reglas instaladas en los equipos locales de las unidades	Falta de acceso para administración local en cada Unidad (Agencias, Unidades Médicas)	10%	10%	80%	2,4	2	4,8
		No se está centralizando el tráfico de las unidades que cuentan con firewall para ser analizado en línea	Falta de visibilidad de la red, a través de un análisis de tráfico en línea	10%	60%	80%	2,4	2	4,8
		No tener soporte del fabricante en la solución firewall	No contar con la disponibilidad del servicio por problemas que no puedan ser superados por falta de soporte y actualización.	80%	20%	20%	2,4	1	2,4
		No se tiene una solución de filtrado de contenido, antivirus, antiboot en las unidades	No poder atender el incremento de solicitudes de acceso hacia internet con los controles adecuados	10%	80%	80%	2,4	2	4,8
		Probabilidad de falla de configuraciones o de accesos	Posibilidad de falla a la protección de los servidores del core del IESS	10%	85%	80%	2,55	3	7,65
		No se tiene controles de URLFiltering, Antivirus y Antiboot perimetral	Posibilidad de virus, ataques, malware	50%	100%	100%	3	3	9
		No se cuenta con soporte del fabricante por lo que pueden ocurrir problemas	No tener buenos tiempos de respuesta ante incidentes ocurridos	80%	20%	20%	2,4	1	2,4

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confiableidad	TOTAL	FRECUENCIA	RIESGO
		graves que no se puedan solventar en cortos tiempos							
		Falta de garantía del fabricante (no se resuelvan los problemas graves)	Posibilidad de tener cortes en la continuidad del servicio (disponibilidad)	90%	20%	10%	2,7	1	2,7
		No existe el control de acceso a internet en algunas de las unidades, ni tampoco desde las unidades hacia la red del IESS.	Posibilidad de problemas de seguridad en la red por el acceso directo a internet y la falta de control en los accesos de las redes LAN	50%	90%	80%	2,7	3	8,1
		No se puede verificar las reglas instaladas en las unidades donde al momento existen firewall	Posibilidad de virus, ataques, malware	10%	80%	80%	2,4	2	4,8
		No se centralizan los logs de las unidades que tienen firewall a fin de ser analizadas y correlacionadas	No conocer de las vulnerabilidades existentes para mitigación	10%	60%	60%	1,8	2	3,6
		Algunas funcionalidades deshabilitadas debido a término de vigencia del soporte	Indisponibilidad del servicio, y posibilidad de que se infecte la red	80%	80%	80%	2,4	2	4,8
		Al momento los firewalls son administrados localmente y en forma separada sin poder verificarse si cumplen las normativas	Falta de seguridad en la red	10%	60%	60%	1,8	2	3,6

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL	FRECUENCIA	RIESGO
		Posibilidad de tener puntos de falla que no puedan ser superados por falta de soporte técnico (errores avanzados)	Falta de seguridad en la red	100%	20%	20%	3	3	9
		Al momento hay unidades que no tiene firewalls o son soluciones básicas	Falta de seguridad en la red	60%	85%	80%	2,55	3	7,65
		No existe un sistema de verificación y autorización de las reglas que se vayan a instalar en las unidades	Red institucional desprotegida sin reglas de configuración definidas	10%	50%	50%	1,5	2	3
STACK SWITCH CORE	3	Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	0%	0%	3	2	6
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	0%	0%	3	2	6
		Posibilidad de incendios	Daños ocasionados por fuego	100%	0%	0%	3	0,1	0,3
		Funcionamiento inadecuado de UPS (sin soporte)	daños ocasionados por corte de suministro eléctrico	100%	50%	0%	3	1	3
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres Naturales (Terremotos)	100%	0%	0%	3	0,1	0,3
		Crecimiento no planificado de personal, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo	80%	0%	0%	2,4	0,1	0,24
		Falta de capacitación (personal de administración)	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	100%	100%	50%	3	0,1	0,3

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confiableidad	TOTAL	FRECUENCIA	RIESGO
		Debilidad en el Control de acceso de entrada y salida	Acceso de personal no autorizado que puede ocasionar daño, des configuración robo, etc.	100%	100%	100%	3	0,1	0,3
		Falta de planes de contingencia y políticas formalizados	Imposibilidad de recuperar el equipo por falta de planes de contingencia	10%	10%	50%	1,5	1	1,5
		Controles de acceso débiles de ingreso a máquinas de administración	Posibilidad de robo de clave	80%	100%	100%	3	0,1	0,3
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	100%	0%	0%	3	2	6
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	0%	0%	3	0,1	0,3
		No existe una política formal de cambio de credenciales	Posibilidad de vulnerabilidad del equipo por no existir una política formal de cambio de credenciales	10%	10%	50%	1,5	2	3
IPS	2	Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	0%	0%	3	2	6
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	0%	0%	3	2	6
		Posibilidad de incendios	Daños ocasionados por fuego	100%	0%	0%	3	0,1	0,3
		Funcionamiento inadecuado de UPS (sin soporte)	daños ocasionados por corte de suministro eléctrico	100%	40%	0%	3	1	3

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL	FRECUENCIA	RIESGO
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres Naturales (Terremotos)	100%	0%	0%	3	0,1	0,3
		Crecimiento no planificado de personal, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo	90%	0%	0%	2,7	0,1	0,27
		Falta de capacitación (personal de administración)	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	100%	100%	50%	3	0,1	0,3
		Debilidad en el Control de acceso de entrada y salida	Acceso de personal no autorizado que puede ocasionar daño, des configuración robo, etc.	100%	100%	100%	3	0,1	0,3
		Falta de planes de contingencia y políticas formalizados	Posibilidad de vulnerabilidad del equipo por no existir una política formal de cambio de credenciales	10%	10%	50%	1,5	1	1,5
		Controles de acceso débiles de ingreso a máquinas de administración	Posibilidad de robo de clave)	80%	100%	100%	3	0,1	0,3
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico), actualización de sistema operativo y suscripción de vacunas digitales	100%	50%	0%	3	2	6
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	0%	0%	3	0,1	0,3

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confiable	TOTAL	FRECUENCIA	RIESGO
		No existe una política formal de cambio de credenciales	Posibilidad de vulnerabilidad del equipo por no existir una política formal de cambio de credenciales	10%	10%	50%	1,5	2	3
STACK SWITCH EXTRANET	3	Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	100%	0%	0%	3	2	6
		Falta de protección contra inundaciones	Daños ocasionados por agua	100%	0%	0%	3	3	9
		Posibilidad de incendios	Daños ocasionados por fuego	100%	0%	0%	3	0,1	0,3
		Funcionamiento inadecuado de UPS (sin soporte)	daños ocasionados por corte de suministro eléctrico	100%	50%	0%	3	1	3
		Problemas de origen estructural donde se encuentra el activo	Daños ocasionados por desastres Naturales (Terremotos)	100%	0%	0%	3	0,1	0,3
		Crecimiento no planificado de entidades externas, aplicativos y transaccionalidad	Degradación por saturación de recursos del equipo	80%	0%	0%	2,4	0,1	0,24
		Falta de capacitación (personal de administración)	Mal funcionamiento por inadecuado manejo de sus configuraciones (administradores)	100%	100%	50%	3	0,1	0,3
		Debilidad en el control de acceso de entrada y salida	Acceso de personal no autorizado que puede ocasionar daño, des configuración robo, etc.	100%	100%	100%	3	0,1	0,3

IDENTIFICACIÓN DE ACTIVOS		VULNERABILIDADES	AMENAZAS	DEGRADACIÓN			IMPACTO	RIESGO	
Activo	Criticidad	Descripción	Descripción	Disponibilidad	Integridad	Confidencialidad	TOTAL	FRECUENCIA	RIESGO
		Falta de planes de contingencia y políticas formalizados	Posibilidad de vulnerabilidad del equipo por no existir una política formal de cambio de credenciales	10%	10%	50%	1,5	1	1,5
		Controles de acceso débiles de ingreso a máquinas de administración	Posibilidad de robo de clave	80%	100%	100%	3	0,1	0,3
		Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	100%	0%	0%	3	2	6
		Falta de precaución en las conexiones físicas	Desconexión deliberada o accidental del equipo	100%	0%	0%	3	0,1	0,3
		No existe una política formal de cambio de credenciales	Posibilidad de vulnerabilidad del equipo por no existir una política formal de cambio de credenciales	10%	10%	50%	1,5	2	3

III.9.4. Gráfica de radar de los riesgos por activo

La Tabla III-17 muestra los riesgos que se han identificado a la plataforma Firewall – IESS, donde:

- Valor actual: Promedio de todos los riesgos.
- Valor objetivo: Recomendación de la SDNSI de reducción de riesgo (al menos el 50%).
- Valor límite: Valor dado por condiciones gráficas, al que nunca se debería llegar.

Tabla III-17 Tabla de valores de riesgos Firewall – IESS

ACTIVO	ACTUAL	OBJETIVO	LIMITE
FIREWALL INTERNET (1)	4.21	2.10	7
FIREWALL INTERNET (2)	4.21	2.10	7
FIREWALL INTRANET (1)	4.21	2.10	7
FIREWALL INTRANET (2)	4.21	2.10	7
STACK SWITCH CORE	2.12	1.59	7
IPS	2.12	1.59	7
STACK SWITCH EXTRANET	2.35	1.76	7

La Figura III-9 muestra un reporte de los riesgos que se han identificado a la plataforma Firewall – IESS, que indica el riesgo actual, objetivo y el límite aceptable.

Figura III-9 Reporte de riesgos Firewall – IESS

III.9.5. Controles o salvaguardas sugeridas

La Tabla III-18 muestra las salvaguardas que se han identificado para cada tripleta activo-vulnerabilidad-amenaza.

Tabla III-18. Salvaguardas sugeridas Firewall – IESS

Activo	RIESGO	Vulnerabilidad	Amenazas	Salvaguarda
FIREWALL INTERNET (1) FIREWALL INTERNET (2) FIREWALL INTRANET (1) FIREWALL INTRANET (2)	R17	No se tiene controles de URLFiltering, Antivirus y Antiboot perimetral	Posibilidad de virus, ataques, malware	Se sugiere implementar las funcionalidades de URL filtering, antivirus, antiboot
	R20	No existe el control de acceso a internet en algunas de las unidades, ni tampoco desde las unidades hacia la red del IESS.	Posibilidad de problemas de seguridad en la red por el acceso directo a internet y la falta de control en los accesos de las redes LAN	Se sugiere contar con una solución de protección perimetral en cada unidad que tenga acceso a internet
	R25	Posibilidad de tener puntos de falla que no puedan ser superados por falta de soporte técnico (errores avanzados)	Falta de seguridad en la red	Se sugiere que la solución de firewall posea soporte técnico, garantía técnica y manteneamientos periódicos.
	R16	Probabilidad de falla de configuraciones o de accesos	Posibilidad de falla a la protección de los servidores del core del IESS	Se sugiere repotenciar la arquitectura de los equipos dedicados a la protección del core
	R26	Al momento hay unidades que no tiene firewalls o son soluciones básicas	Falta de seguridad en la red	Se sugiere contar con una solución de protección perimetral en cada unidad que tenga acceso a internet
STACK SWITCH CORE	R1	Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	Se sugiere contar con el soporte técnico y los mantenimientos periódicos sobre el equipo s de climatización
	R2	Falta de protección contra inundaciones	Daños ocasionados por agua	Se sugiere realizar los trabajos de impermeabilización en el centro de datos del segundo piso (se dañaría todo el sistema eléctrico)
	R11	Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	Se sugiere contar con el soporte técnico y los mantenimientos periódicos
IPS	R11	Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) , actualización de sistema operativo y suscripción de vacunas digitales	Se sugiere contar con el soporte técnico y los mantenimientos periódicos
	R2	Falta de protección contra inundaciones	Daños ocasionados por agua	Se sugiere realizar los trabajos de impermeabilización en el centro de datos del

Activo	RIESGO	Vulnerabilidad	Amenazas	Salvaguarda
				segundo piso (se dañaría todo el sistema eléctrico)
	R1	Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	Se sugiere contar con el soporte técnico y los mantenimientos periódicos sobre el equipo s de climatización
STACK SWITCH EXTRANET	R11	Problemas con actualizaciones y mantenimientos	Daños ocasionados por falta de mantenimiento (físico y lógico) y actualización de sistema operativo	Se sugiere contar con el soporte técnico y los mantenimientos periódicos
	R2	Falta de protección contra inundaciones	Daños ocasionados por agua	Se sugiere realizar los trabajos de impermeabilización en el centro de datos del segundo piso (se dañaría todo el sistema eléctrico)
	R1	Mal funcionamiento de equipos de climatización (sin soporte)	Daños ocasionados por condiciones inadecuadas de temperatura y humedad	Se sugiere contar con el soporte técnico y los mantenimientos periódicos sobre el equipo s de climatización

III.9.6. Conclusiones

- El equipo firewall tiene 5 amenazas en el cuadrante de alto impacto y alta frecuencia del mapa de riesgos, entre las cuales se pueden mencionar que dichos equipos: no cuentan con controles de URLFiltering, antivirus y antiboot perimetral; adicionalmente no existe control de acceso a internet en algunas de las unidades; tampoco existe control desde las unidades hacia la red del IESS; además se ha evidenciado la falta de soporte técnico; tampoco existe control de acceso hacia los servidores; y existen algunas unidades que tienen soluciones básicas de protección.
- Los equipos (Stack switch core, ips, stack switch extranet) que tienen dependencia con la solución de firewall, no cuentan con servicio de mantenimiento preventivo y correctivo, además el datacenter del piso 2 tiene riesgos de inundación y podría dañar todo el sistema eléctrico.
- Resultado del presente análisis, los riesgos localizados en los cuadrantes de alto impacto y bajo frecuencia, y bajo impacto y alta frecuencia de los mapas de riesgos, deben ser monitoreados con periodicidad.
- Existen riesgos controlados en los equipos de firewall, Stack switch core, ips, stack switch extranet, que deben ser monitoreados para identificar cambio de cuadrante para su gestión.

III.10. Resumen del Anexo III

En este anexo se ha plasmado las actividades realizadas en la elaboración de la matriz de riesgos utilizando los conceptos, parámetros y metodología definida en la SDNSI, de lo cual podemos identificar lo siguiente:

- El modelo conceptual para la gestión de riesgos de ciberseguridad está basado en la gestión de amenazas y no en vulnerabilidades.

- Los parámetros cualitativos son de rangos muy cortos impidiendo determinar un impacto más puntual y no tan subjetivo.
- No existe taxonomías y catálogos de las vulnerabilidades y amenazas utilizadas, generando duplicidad de los mismos por errores de sintaxis.
- No se validan los costos de los activos ni se valoran las vulnerabilidades de cada activo.
- Los riesgos son identificados para cada activo y no se tiene la trazabilidad de una amenaza presente en varios activos, así como las vulnerabilidades comunes que presentan los activos de ciberseguridad.
- Las contramedidas son presentadas por activo, y no permite analizar las vulnerabilidades y amenazas comunes que pueden ser atendidas por la misma contramedida.
- No utilizan ninguna herramienta informática para la gestión de riesgos en ciberseguridad.

Como conclusión final, podemos indicar que el análisis y evaluación gestión de riesgos de la DNTI se está realizando enfocándose en amenazas de ciberseguridad, dejando de lado el impacto de las vulnerabilidades de los activos de ciberseguridad.

IV. Línea base final de Identificación y Evaluación de Riesgos de la Dirección Nacional de Tecnología de la Información - IESS

IV.1. Introducción

En septiembre de 2018, se ha empezado a evaluar los riesgos de ciberseguridad de la DNTI (Dirección Nacional de Tecnología de la Información). Los activos fueron evaluados según el impacto de las vulnerabilidades de cada uno de ellos, se identificaron las amenazas, se calcularon los riesgos y se determinaron las contramedidas. Para poder realizar estas actividades, se elaborarán taxonomías de activos, vulnerabilidades y amenazas, que estén basadas en ontologías y estándares que ofrezca la industria.

La evaluación de riesgos se ha realizado utilizando el nuevo modelo conceptual de dominio, que está descrito en el marco de trabajo de gestión de riesgos de ciberseguridad AVARCIBER, descrito en los capítulo 4 de esta tesis doctoral.

IV.2. Objetivo

Determinar los riesgos sobre los equipos de las plataformas definidas por la DNTI, mediante la identificación y valoración de activos, vulnerabilidades y amenazas, así como la valoración de las vulnerabilidades y consecuente impacto en las amenazas una vez materializadas.

Para poder conseguir el objetivo planteado, se han planteado objetivos secundarios, que se describen a continuación:

- Revisar y analizar los activos, vulnerabilidades y amenazas de los activos definidos previamente.
- Elaborar la taxonomía de activos de la Institución.
- Elaborar la taxonomía de las vulnerabilidades de la institución.
- Elaborar la taxonomía de las amenazas de la Institución.
- Valorar los activos y el impacto de las vulnerabilidades por activo.
- Identificar las amenazas que materializan las vulnerabilidades, medir su frecuencia y calcular el riesgo.

IV.3. Justificación

Se ha validado el modelo conceptual definido en el capítulo 4 de la presente tesis doctoral, y se han realizado las actividades definidas en el marco de trabajo AVARCIBER para la identificación y evaluación de riesgos de ciberseguridad. Esto nos ha permitido valorar los activos y las vulnerabilidades de cada uno de ellos.

La valoración de las vulnerabilidades nos ha ayudado a determinar el costo de recuperación de los activos, la valoración del impacto se ha realizado sobre las dimensiones de seguridad (confidencialidad, integridad, disponibilidad), también se incluyó a la criticidad.

Todos los valores calculados o asignados al final serán valores referenciales y conductivos que permitan a los ejecutivos de la Dirección tomar decisiones en el momento de decidir qué riesgos hay que tratar. Para ello, se definirán las contramedidas que sean oportunas, según los objetivos estratégicos de la DNTI.

Los activos considerados fueron los mismos que se tuvieron en cuenta en la línea base inicial, para poder tener elementos de referencia y elaborar el comparativo necesario.

IV.4.Alcance

En el presente Anexo se presentan los resultados de la identificación y evaluación de riesgos de los activos del Instituto Ecuatoriano de Seguridad Social (IESS), que son administrados por la Dirección Nacional de Tecnología de la Información (DNTI), para poder analizar el estudio comparativo con la línea base final en:

- Plataforma AS400-IESS del Hospital Carlos Andrade Marín (HCAM).
- Plataforma Host-IESS.
- Plataforma Oracle-IESS.
- Plataforma Firewall-IESS.

Se ha analizado el identificación y evaluación de riesgos de los activos de las plataformas definidas anteriormente según el Marco de Trabajo a metodología AVARCIBER.

IV.5.Marco de trabajo para la Identificación y Evaluación de riesgos en Ciberseguridad AVARCIBER

Para explicarlo de mejor manera, se ha elaborado un diagrama de flujo del marco de trabajo que ayude a entender las actividades y tareas a realizar. El diagrama se muestra en la [Figura IV-1](#).

Figura IV-1. Diagrama de Flujo del Marco de Trabajo

Aquí, se van a describir las actividades y tareas del marco de trabajo elaborado, denominado **AVARCIBER** (Activos – Vulnerabilidades – Amenazas – Riesgos **CIBER**seguridad).

A continuación, se describen estas actividades y tareas que se deben realizar en el marco de trabajo definido.

Actividad 1: Lanzamiento

Como actividad inicial, es importante tener un catálogo de los elementos que participan en el modelo conceptual. Para ello, se han definido las taxonomías de estos elementos, las cuales son el resultado de las revisiones sistemáticas realizadas en el capítulo 2. Las taxonomías definidas se describen en las siguientes tareas:

Tarea 1: se define la taxonomía de tipos de activos de la organización enfocados en ciberseguridad en base al estándar ISO 27005.

Tarea 2: se determina la taxonomía de Vulnerabilidades en ciberseguridad en base al estándar ISO 27005.

Tarea 3: se establece la taxonomía de Amenazas en ciberseguridad en base al estándar ENISA 2016.

Estas taxonomías, una vez definidas, deberán ser actualizadas continuamente, debido al avance de la tecnología y las necesidades de la industria, que generará la aparición de nuevas amenazas y vulnerabilidades de ciberseguridad, así como de tipos de activos en ciberseguridad.

Actividad 2: Identificar y evaluar Activos

Esta actividad se refiere al proceso inicial que toda organización debe realizar para comenzar con la concienciación de la ciberseguridad por parte de todo el personal de la organización. Una de las preguntas iniciales que se debe hacer es: ¿qué queremos proteger? Para ello, se hace un análisis de los elementos que son más importantes para la organización, tomando en consideración las siguientes cuestiones:

- ¿Qué actividad realizamos?
- ¿Qué es lo más importante para la organización?
- ¿Cuáles son los objetivos institucionales?
- ¿Qué servicios proporciono?

A continuación, se muestran las tareas necesarias para esta actividad.

Tarea 1: se toman los tipos de activos de ciberseguridad de la taxonomía previamente establecida, en la Actividad 1 – Tarea 1. Aquí, se identifican los activos de ciberseguridad y se asigna el tipo al que corresponde, como se puede ver en la Tabla IV-1.

Tabla IV-1. Activos y tipos de activos

<i>Tipo Activo</i>	<i>Activo</i>
Hardware	Servidor
Hardware	Almacenamiento
Software.	Sistema de monitoreo
Red	Firewall

Tarea 2: se identifican las dimensiones de seguridad (comúnmente, confidencialidad, integridad y disponibilidad) para los activos de ciberseguridad, y se mide el impacto de las dimensiones en cada activo de ciberseguridad basándose en el estándar ISO 27005. El impacto tomará los valores de la Tabla IV-2.

Tabla IV-2. Valoración del impacto para un activo

<i>RANGO</i>	<i>Valor Superior</i>	<i>Valor Inferior</i>
Alto	10	8

RANGO	Valor Superior	Valor Inferior
Medio	7	5
Bajo	4	2
Nulo	1	0

Para poder establecer los valores, se debe considerar para cada dimensión los siguientes criterios de valoración, según muestra la Tabla IV-3.

Tabla IV-3. Criterios de valoración dimensiones de Seguridad

Criterio de valoración CONFIDENCIALIDAD	
¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?	
Alta (A)	Información que puede ser conocida y utilizada por un grupo muy reducido de agentes, cuya divulgación podría ocasionar un perjuicio a la organización
Media (M)	Información que solo puede ser conocida y utilizada por un grupo de agentes, que la necesiten para realizar su trabajo.
Baja (B)	Información que puede ser conocida y utilizada por todos los agentes de la organización.
Nula (N)	Información que puede ser conocida y utilizada sin autorización por cualquier persona, dentro o fuera de la organización.
Criterio de valoración INTEGRIDAD	
¿Qué importancia tendría que los datos fueran modificados fuera de control?	
Alta (A)	Información cuya modificación no autorizada no podría repararse, impidiendo la realización de las actividades de la organización.
Media (M)	Información cuya modificación no autorizada es de difícil reparación y podría ocasionar un perjuicio significativo para la organización o terceros.
Baja (B)	Información cuya modificación no autorizada puede repararse, aunque podría ocasionar un perjuicio para la organización o terceros.
Nula (N)	Información cuya modificación no autorizada puede repararse fácilmente, o que no afecta a las actividades de la organización.
Criterio de valoración DISPONIBILIDAD	
¿Qué importancia tendría que el activo no estuviera disponible?	
Alta (A)	Información cuya inaccesibilidad permanente durante una hora podría impedir la ejecución de las actividades de la organización.
Media (M)	Información cuya inaccesibilidad permanente durante la jornada laboral podría impedir la ejecución de las actividades de la organización.
Baja (B)	Información cuya inaccesibilidad permanente durante una semana podría ocasionar un perjuicio significativo para la organización.
Nula (N)	Información cuya inaccesibilidad no afecta la actividad normal de la organización.

Para el ejemplo que vamos a seguir, los valores de las dimensiones de seguridad quedarían como se muestran en la Tabla IV-4.

Tabla IV-4. Valoración del impacto del Activo

		Dimensión
--	--	------------------

<i>Tipo Activo</i>	<i>Activo</i>	Confidencialidad	Integridad	Disponibilidad
Hardware	Servidor	5	6	8
Hardware	Almacenamiento	9	7	5

Tarea 3: se añade la criticidad del activo como una nueva dimensión de seguridad, que será calculada como el valor más alto del resto de dimensiones de seguridad. En el caso del ejemplo, sería:

- Servidor: máximo de 5, 6 y 8, luego el valor de la criticidad sería 8.
- Almacenamiento: máximo de 9, 7 y 5, luego el valor de la criticidad sería 9.

El valor de la criticidad del activo será en lo posterior el valor de la dimensión de **Criticidad** para todas las vulnerabilidades que se lleguen a identificar al activo de ciberseguridad en cuestión.

Tarea 4: se le asigna el costo monetario que la organización calcula a cada activo. Dicho costo monetario se calcula en función de lo que supondría la pérdida o daño del activo analizado, así como el costo actual del activo. El valor monetario es determinado por el criterio experto del dueño del activo. En el caso del ejemplo, en la columna *Costo del Activo* de la Tabla IV-5 se muestra dicho valor.

Tabla IV-5. Valoración del Costo del Activo

<i>Tipo de Activo</i>	<i>Activo</i>	<i>Costo del Activo</i>	<i>Dimensión</i>			
			Confidencialidad	Integridad	Disponibilidad	Criticidad
Hardware	Servidor	10.000,00	5	6	8	8
Hardware	Almacenamiento	2.000,00	9	7	5	9

Actividad 3: Evaluar el nivel de daño para las tuplas Vulnerabilidad – Activo (dimensión)

En esta actividad se debe determinar cuál es el daño que van a producir las vulnerabilidades en cada uno de los activos de la organización previamente identificados. La valoración del daño de la vulnerabilidad se hará en base a los valores de la Tabla IV-6 (o su equivalente, establecida por la organización). La organización debe determinar el valor del daño de la vulnerabilidad en cada una de las dimensiones (confidencialidad, integridad, disponibilidad y criticidad) del activo. El costo del daño de la vulnerabilidad se calcula determinando el impacto, la importancia y la repercusión que puede tener el daño en el activo de la organización.

Tabla IV-6. Valoración del daño de las vulnerabilidades

<i>RANGO</i>	<i>Valor Superior</i>	<i>Valor Inferior</i>
Daño Extremo	10	10
Muy Alto	9	9
Alto	8	6
Medio	5	3
Bajo	2	1
Despreciable	0	0

A continuación, se muestran las tareas necesarias para esta actividad.

Tarea 1: se identifican las vulnerabilidades que afectan a cada activo, como se muestra en la Tabla IV-7. Estas vulnerabilidades podrían tomarse de la taxonomía previamente establecida, en la Actividad 1 – Tarea 2.

Tabla IV-7. Tuplas Vulnerabilidad – Activo

<i>Vulnerabilidad</i>	<i>Activo</i>
Falta de soporte preventivo y correctivo	Servidor
Ubicación en un área susceptible a inundaciones	Servidor
Susceptible a incendios y altas temperaturas	Servidor
Falta de soporte preventivo y correctivo	Almacenamiento
Ubicación en un área susceptible a inundaciones	Almacenamiento
Falta de planes de contingencia	Almacenamiento

Tarea 2: se evalúa el daño de la vulnerabilidad en el activo para cada una de las dimensiones de seguridad, incluyendo la criticidad. El daño en la criticidad se ha calculado previamente en la Actividad 2 – Tarea 3, correspondiente al valor del impacto del activo, y que será un valor único para todas las vulnerabilidades del activo de ciberseguridad. Para evaluar las dimensiones se deben tomar en consideración los rangos definidos en la Tabla IV-6. Así, por ejemplo, para el caso de la vulnerabilidad “Falta de soporte preventivo y correctivo” y activo “Servidor”, queda definido el valor del daño de la vulnerabilidad en el activo por cada dimensión de seguridad como se muestra en la Tabla IV-8.

Tabla IV-8. Valoración del daño de la vulnerabilidad

<i>Vulnerabilidad</i>	<i>Activo</i>	<i>Dimensiones</i>			
		<i>Daño Confidencialidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Criticidad</i>
Falta de soporte preventivo y correctivo	Servidor	2	3	8	8
Ubicación en un área susceptible a inundaciones.	Servidor	5	4	3	8
Susceptible a incendios y altas temperaturas	Servidor	6	7	8	8
Falta de soporte preventivo y correctivo	Almacenamiento	5	8	2	9
Ubicación en un área susceptible a inundaciones.	Almacenamiento	7	4	1	9
Falta de planes de contingencia	Almacenamiento	6	5	3	9

Tarea 3: se realiza la suma de los valores del daño de la vulnerabilidad de cada tupla vulnerabilidad – activo. En el ejemplo, el valor del daño de la vulnerabilidad de la tupla vulnerabilidad “falta de soporte preventivo y correctivo” y el activo “servidor” sería igual a 21 ($2 + 3 + 8 + 8$).

Tarea 4: se calcula el valor promedio del valor del daño de la vulnerabilidad de cada tupla vulnerabilidad – activo, dividiendo el valor del daño anterior entre el número de dimensiones

consideradas (en este caso, cuatro dimensiones). En el ejemplo, el valor promedio del valor del daño de la vulnerabilidad para la tupla vulnerabilidad “falta de soporte preventivo y correctivo” y el activo “servidor” sería: $21/4 = 5,25$

Tarea 5: se repiten las tareas 2, 3 y 4 para cada una de las tuplas vulnerabilidad – activo de la organización.

Tarea 6: se realiza la asignación de un valor monetario a cada una de las vulnerabilidades que están afectando a los activos de la organización (tupla vulnerabilidad – activo). El valor monetario asignado se realiza según el criterio experto del dueño del activo, tomando información del valor actual y el daño que pudiera sufrir por la materialización de la vulnerabilidad. En el caso del ejemplo, en la columna Costo del Daño de la Vulnerabilidad de la Tabla IV-9 se muestra dicho valor.

Como se observa en la Tabla IV-9, podría darse el caso de que la suma de los costes del daño de la vulnerabilidad para un activo ($3.500 + 5000 + 6000 = 14,500$) podría ser mayor que el costo del propio activo (10.000 \$). Sin embargo, hay que tener en cuenta que seguramente esos costos de los daños de las vulnerabilidades vienen provocados por diferentes amenazas, por lo que, si estas vulnerabilidades son materializadas por la misma amenaza, el costo del daño de la amenaza puede ser mayor que el coste del activo como se puede ver en la Tabla IV-11.

Tabla IV-9. Tuplas de Vulnerabilidades – Activos, con valor y costo del daño de las vulnerabilidades, costo del activo.

<i>Vulnerabilidad</i>	<i>Activo</i>	<i>Costo del Activo</i>	<i>Dimensiones</i>				<i>Valor del Daño de la Vulnerabilidad</i>	<i>Costo del Daño de la Vulnerabilidad</i>
			<i>Daño Confidencial</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Criticidad</i>		
Falta de soporte preventivo y correctivo	Servidor	10.000	2	3	8	8	5,25	3.500
Ubicación en un área susceptible a inundaciones.	Servidor		5	4	3	8	5,00	5.000
Susceptible a incendios y altas temperaturas	Servidor		6	7	8	8	4,25	6.000
Falta de soporte preventivo y correctivo	Almacenamiento	2.000	5	8	2	9	6,00	300
Ubicación en un área susceptible a inundaciones.	Almacenamiento		7	4	1	9	5,25	600
Falta de planes de contingencia	Almacenamiento		6	5	3	9	5,75	1.200

Actividad 4: Identificación de Amenazas de Ciberseguridad

En esta actividad se identifican las amenazas de ciberseguridad que pueden afectar a la organización y que puedan materializar las vulnerabilidades existentes en los activos. Para ello, se deben relacionar las amenazas de ciberseguridad con las vulnerabilidades existentes, y calcular, para cada amenaza, el valor del daño de la amenaza, así como el costo del daño de la amenaza.

A continuación, se muestran las tareas necesarias para esta actividad.

Tarea 1: se identifican las amenazas que puedan materializar las vulnerabilidades existentes. Las amenazas de ciberseguridad se podrían tomar de la taxonomía previamente establecida en la Actividad 1 – Tarea 3.

Tarea 2: se determina la amenaza que puede materializar cada vulnerabilidad de los activos de ciberseguridad de la organización, quedando estructurada las duplas Amenazas – Vulnerabilidades, y las tripletas Amenazas – Vulnerabilidades – Activos, por la asociación de relaciones previamente definidas como se muestra en la Tabla IV-10.

Tabla IV-10. Tripletas Amenazas – Vulnerabilidades – Activos

<i>Amenaza</i>	<i>Vulnerabilidad</i>	<i>Activo</i>
Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	Servidor
Agua	Ubicación en un área susceptible a inundaciones.	Servidor
Fuego	Susceptible a incendios y altas temperaturas	Servidor
Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	Almacenamiento
Condiciones climáticas desfavorables	Ubicación en un área susceptible a inundaciones.	Almacenamiento
Fallo de dispositivos o sistemas	Falta de planes de contingencia	Almacenamiento

Tarea 3: se recupera de la Actividad 2 – Tarea 4 el costo del activo, así como de la actividad anterior los valores calculados de valor del daño de la vulnerabilidad y costo del daño de la vulnerabilidad, de todas las vulnerabilidades identificadas, y se les asigna a las tripletas Amenazas – Vulnerabilidades – Activos, como se muestra en la Tabla IV-11 para el ejemplo que se sigue.

Tabla IV-11. Tripletas Amenazas – Vulnerabilidades – Activo con los valores y costo del daño de las amenazas

<i>Amenaza</i>	<i>Vulnerabilidad</i>	<i>Activo</i>	<i>Costo del Activo</i>	<i>Valor del Daño de la Vulnerabilidad</i>	<i>Costo del Daño de la Vulnerabilidad</i>
Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	Servidor	10.000,00	5,25	3.500
Agua	Ubicación en un área susceptible a inundaciones.	Servidor		5,00	5.000
Fuego	Susceptible a incendios y altas temperaturas	Servidor		4,25	6.000
Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	Almacenamiento	2.000,00	6,00	300
Condiciones climáticas desfavorables	Ubicación en un área susceptible a inundaciones.	Almacenamiento		5,25	600
Fallo de dispositivos o sistemas	Falta de planes de contingencia	Almacenamiento		5,75	1.200

Tarea 4: se agrupan las amenazas y vulnerabilidades en pares amenaza – vulnerabilidad, con el propósito de identificar todas las vulnerabilidades que podrían materializarse en caso de ocurrir la amenaza. Se calcula el valor del daño promedio de la vulnerabilidad, mediante el promedio de los valores del daño de las vulnerabilidades que están relacionadas con la amenaza en cuestión. De igual forma, se calcula el costo del daño total de la vulnerabilidad como la suma de los valores del costo del daño de las vulnerabilidades relacionadas con dicha amenaza. La Tabla IV-12 muestra estos valores.

En el ejemplo para la dupla “Condiciones climáticas desfavorables” – “Falta de soporte preventivo y correctivo” de la Tabla IV-11, el valor del daño promedio de la vulnerabilidad es igual al promedio de 5,25 y 6,00 $((5,25 + 6,00)/2)$ que es igual a 5,62; y el costo del daño de la amenaza es igual a la suma de 3.500 y 600, que es igual a 3.800.

Tabla IV-12. Duplas Amenazas – Vulnerabilidades con los valores y costo del daño de las vulnerabilidades

<i>Amenaza</i>	<i>Vulnerabilidad</i>	<i>Valor del Daño Promedio de la Vulnerabilidad</i>	<i>Costo del Daño Total de la Vulnerabilidad</i>
Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	5,62	3.800
Condiciones climáticas desfavorables	Ubicación en un área susceptible a inundaciones.	5,25	600
Agua	Ubicación en un área susceptible a inundaciones.	5,00	5.000
Fuego	Susceptible a incendios y altas temperaturas	4,25	6.000
Fallo de dispositivos o sistemas	Falta de planes de contingencia	5,75	1.200

Tarea 5: se agrupan las amenazas, y se calcula el valor del daño de la amenaza y el costo del daño de la amenaza. El valor del daño de cada amenaza se calcula con el promedio de los valores del daño de las vulnerabilidades que están relacionadas con la amenaza en cuestión. Y para el costo del daño de la amenaza se suman los valores del costo del daño de las vulnerabilidades relacionadas con dicha amenaza, como se muestra en la Tabla IV-13.

Tabla IV-13. Amenazas con valores totales de daño y costo del daño

<i>Amenaza</i>	<i>Valor del Daño de la Amenaza</i>	<i>Costo del Daño de la Amenaza</i>
Condiciones climáticas desfavorables	5,43	4.400
Agua	5,00	5.000
Fuego	4,25	6.000
Fallo de dispositivos o sistemas	5,75	1.200

En el ejemplo que se está siguiendo y para la amenaza “Condiciones climáticas desfavorables”, el valor del daño de la amenaza es igual al promedio de 5,62 y 5,25 $((5,62 + 5,25)/2)$ que es igual a 5,43; y el costo del daño de la amenaza es igual a la suma de 3.800 y 600, que es igual a 4.400.

Actividad 5: Medición del Riesgo

En esta actividad se calcula el riesgo de cada amenaza en función de las vulnerabilidades identificadas a los activos de la organización. Para ello, la organización debe establecer previamente la probabilidad de ocurrencia de las amenazas. Un ejemplo se muestra en la Tabla IV-14, tomando como referencia la norma ISO 27005, y agregando dos nuevos rangos: "muy alto" y "muy bajo" para identificar probabilidades muy inminentes y también insignificantes de ocurrencia.

Tabla IV-14. Probabilidad de ocurrencia de la amenaza

RANGO	PROBABILIDAD	DESCRIPCION	FRECUENCIA
MA (Muy Alto)	100	muy frecuente	a diario
A (Alto)	10	frecuente	mensualmente
M (Medio)	1	normal	una vez al año
B (Bajo)	1/10	poco frecuente	cada varios años
MB (Muy Bajo)	1/100	muy poco frecuente	siglos

El riesgo asociado es el impacto potencial (I, impacto) multiplicado por la probabilidad de ocurrencia de la amenaza (F, frecuencia). El impacto potencial es el valor del daño de la amenaza calculado previamente (valor redondeado). La organización debe establecer la probabilidad de ocurrencia de las amenazas, según lo determine, por ejemplo, tomando en cuenta valores históricos de estas amenazas.

Un ejemplo de la medición del riesgo (R, riesgo), dada por el producto de la probabilidad de la ocurrencia de la amenaza (F, frecuencia) por el impacto (I, impacto), se muestra en la Tabla IV-15.

Tabla IV-15. Valoración del Riesgo

Tabla de Valoración del Riesgo														
I	F	R	I	F	R	I	F	R	I	F	R	I	F	R
0	MB	0	0	B	0	0	M	0	0	A	0	0	MA	0
1	MB	0	1	B	0	1	M	1	1	A	0	1	MA	1
2	MB	0	2	B	0	2	M	1	2	A	0	2	MA	4
3	MB	0	3	B	0	3	M	1	3	A	4	3	MA	4
4	MB	0	4	B	5	4	M	5	4	A	5	4	MA	8
5	MB	0	5	B	5	5	M	5	5	A	5	5	MA	8
6	MB	0	6	B	5	6	M	5	6	A	5	6	MA	9
7	MB	0	7	B	5	7	M	6	7	A	8	7	MA	9
8	MB	0	8	B	5	8	M	6	8	A	8	8	MA	9
9	MB	0	9	B	5	9	M	6	9	A	9	9	MA	10
10	MB	0	10	B	5	10	M	6	10	A	10	10	MA	10

Así, la organización podría establecer:

- Riesgo bajo, se considera de 0 a 3 (por ejemplo, color verde).
- Riesgo medio, de 4 a 6, (por ejemplo, color amarillo).
- Riesgo alto, de 7 a 8 (por ejemplo, color naranja).
- Riesgo extremo, de 9 a 10 (por ejemplo, color rojo).

Lo cual, ayudaría a la organización a la toma de decisiones (por ejemplo, enfocarse en los riesgos de color rojo y naranja).

A continuación, se muestran las tareas necesarias para esta actividad.

Tarea 1: se recuperan el valor del daño de la amenaza (impacto) y el valor del costo del daño de la amenaza. Estos valores fueron calculados previamente en la actividad anterior Actividad 4 – Tarea 5. El valor del daño de la amenaza debe ser redondeado.

Tarea 2: se asigna la probabilidad de ocurrencia de cada amenaza. Para esto, se toman como referencia casos similares que han ocurrido en la empresa y la experiencia del personal a cargo. De esta manera, la frecuencia de ocurrencia se define para cada amenaza tomando como referencia los valores de la Tabla IV-14.

Tarea 3: se realiza el cálculo del riesgo de ciberseguridad ($\text{Riesgo} = \text{Impacto} \times \text{Frecuencia}$), según como está definido en la Tabla IV-15. En la Tabla IV-16 se muestra dicho cálculo para el ejemplo que se está mostrando.

Tabla IV-16. Cálculo del Riesgo

<i>Amenazas</i>	<i>Frecuencia</i>	<i>Valor del Daño de la Amenaza (valor redondeado)</i>	<i>Riesgo</i>	<i>Costo del Daño de la Amenaza</i>
Condiciones climáticas desfavorables	(MA) Alto	5	8	4.400
Agua	(B) Bajo	5	5	5.000
Fuego	(MB) Muy Bajo	4	0	6.000
Fallo de dispositivos o sistemas	(MA) Muy Alto	6	9	1.200

Actividad 6: Contramedidas

La organización establecerá, como política de organización, qué riesgos atacar en base a la información disponible. Para ello, deberá analizar cada uno de los riesgos que puedan tener mayor factibilidad de ejecutarse, tomando la lectura de la medición de riesgo y el impacto de la organización, así como los costos en los que podría incurrir la organización. Para ello, deberá tomar las acciones correctivas necesarias y realizar las siguientes tareas.

Tarea 1: se identifica una contramedida para que pueda mitigar o eliminar un riesgo potencial. Estas contramedidas serán enfocadas a las vulnerabilidades (las contramedidas pueden contrarrestar a una o varias vulnerabilidades).

Tarea 2: se generan los controles para que permitan verificar si las contramedidas han llegado a contrarrestar el riesgo aparente de una amenaza por la materialización de las vulnerabilidades de los activos (los controles permiten controlar a una o varias contramedidas).

IV.6. Análisis de Riesgos de la Plataforma AS400 – IESS

La valoración de los activos se ha realizado con personal técnico de la plataforma AS400, Ingeniero. Iván Reinoso, funcionario del Hospital Carlos Andrade Marín (HCAM)-Infraestructura, también se contó con la participación del Ing. Rodney Castro, Coordinador General de tecnología del HCAM.

La dependencia de los activos de la plataforma AS400 – IESS se muestra en la Figura IV-2.

Figura IV-2. Diagrama de dependencias de equipos AS400 – IESS

IV.6.1. Actividad 1: Lanzamiento

En esta actividad se define un catálogo de los elementos que participan en el modelo conceptual. Para ello, se han definido las taxonomías de estos elementos, que fueron descritos en el capítulo 2 de esta tesis doctoral, se define la taxonomía de tipos de activos de la organización enfocados en ciberseguridad en base al estándar ISO 27005, la taxonomía de Vulnerabilidades en ciberseguridad en base al estándar ISO 27005 y se establece la taxonomía de Amenazas en ciberseguridad en base al estándar ENISA 2016.

IV.6.2. Actividad 2: Identificar y evaluar Activos

En esta actividad se identifica los activos de ciberseguridad, determinar el costo del activo y la medición del impacto que tiene el activo en cada una de las dimensiones de seguridad. La Tabla IV-17 muestra el costo y dimensiones de seguridad de los activos de la plataforma AS400-IESS.

Tabla IV-17. Costo e impacto en las dimensiones de seguridad de los activos de la plataforma AS400-IESS

IDENTIFICACIÓN DE ACTIVOS										
#	Tipo Activo	Activo	Costo del Activo	Confidencialidad		Integridad		Confiabilidad		Criticidad
1	Hardware	Servidor Producción	\$ 15.000,00	7	Media	6	Media	9	Alta	9
2	Hardware	Servidor Preproducción aplicativos	\$ 20.000,00	5	Media	7	Media	2	Baja	7
3	Hardware	Servidor preproducción BD	\$ 20.000,00	7	Media	6	Media	3	Baja	7
4	Hardware	Servidor web app	\$ 20.000,00	6	Media	3	Baja	7	Media	7

IDENTIFICACIÓN DE ACTIVOS										
#	Tipo Activo	Activo	Costo del Activo	Confidencialidad		Integridad		Confiability		Criticidad
5	Hardware	Servidor Backup red	\$ 15.000,00	8	Alta	7	Media	6	Media	8
6	Hardware	Servidor principal red	\$ 15.000,00	9	Alta	6	Media	9	Alta	9
7	Hardware	Servidor de desarrollo	\$ 20.000,00	7	Media	7	Media	4	Baja	7
8	Hardware	Stack core 1	\$ 15.000,00	10	Alta	6	Media	9	Alta	10
9	Hardware	Stack core 2	\$ 15.000,00	10	Alta	6	Media	8	Alta	10
10	Hardware	Stack acceso 1	\$ 12.000,00	9	Alta	6	Media	9	Alta	9
11	Hardware	Stack acceso 2	\$ 12.000,00	9	Alta	7	Media	9	Alta	9
12	Hardware	Stack acceso 3	\$ 12.000,00	9	Alta	5	Media	9	Alta	9
13	Hardware	Equipo AS400 Producción	\$ 80.000,00	8	Alta	5	Media	10	Alta	10
14	Hardware	Equipo AS400 GYE	\$ 800.000,00	9	Alta	7	Media	8	Alta	9
15	Hardware	Equipo AS400 Desarrollo	\$ 500.000,00	10	Alta	7	Media	10	Alta	10
16	Hardware	Controladora wireless	\$ 60.000,00	3	Baja	4	Baja	10	Alta	10
17	Hardware	Optimizador Wan	\$ 30.000,00	4	Baja	4	Baja	7	Media	7
18	Hardware	Aires Acondicionados	\$ 40.000,00	1	Nula (N)	3	Baja	6	Media	6
19	Hardware	UPS	\$ 20.000,00	1	Nula (N)	3	Baja	9	Alta	9
20	Hardware	Switch piso	\$ 10.000,00	10	Alta	6	Media	10	Alta	10
21	Software	Sistema Médico AS400	\$ 3.000.000,00	10	Alta	7	Media	8	Alta	10
22	Software	QlikView	\$ 30.000,00	8	Alta	9	Alta	9	Alta	9
23	Software	Aplicativos Web Producción	\$ 500.000,00	9	Alta	10	Alta	8	Alta	10
24	Software	Página Web	\$ 10.000,00	4	Baja	2	Baja	4	Baja	4
25	Software	Software Firewall	\$ 15.000,00	6	Media	6	Media	9	Alta	9
26	Software	Alfresco	\$ 10.000,00	7	Media	3	Baja	7	Media	7
27	Software	Biblioteca Virtual	\$ 10.000,00	4	Baja	3	Baja	3	Baja	4
28	Software	EVCAM	\$ 10.000,00	3	Baja	4	Baja	4	Baja	4
29	Software	Aplicativo de Facturación	\$ 15.000,00	10	Alta	10	Alta	7	Media	10
30	Software	Base de datos postgres	\$ 10.000,00	9	Alta	9	Alta	10	Alta	10

IV.6.3. Actividad 3: Evaluar el nivel del daño para las tuplas Vulnerabilidad -Activo (dimensión)

En esta actividad se ha determinado el daño de las vulnerabilidades en cada uno de los activos de la organización previamente identificados. La organización ha determinado el valor del daño de la vulnerabilidad en cada una de las dimensiones (confidencialidad, integridad, , disponibilidad y criticidad) del activo, para ello hay que identificar las vulnerabilidades de los activos de la plataforma AS400-IESS. La Tabla IV-18 muestra el impacto de las vulnerabilidades en los activos según su degradación en las dimensiones de seguridad de la información de la plataforma AS400 – IESS.

Tabla IV-18. Tuplas Vulnerabilidades - Activos, valor y costo del daño de las vulnerabilidades de la plataforma AS400-IESS

				DIMENSION				VULNERABILIDAD	
	VULNERABILIDAD	ACTIVO	Costo del Activo	Daño Confiabilidad	Daño Integridad	Daño Disponibilidad	Daño Criticidad	Valor del Daño	Costo del Daño
1	Susceptible a incendios y altas temperaturas	Servidor Producción	\$ 15.000,00	10	6	2	9	6,75	\$ 15.000,00
2	Ubicación en un área susceptible a inundaciones.	Servidor Producción		10	6	2	9	6,75	\$ 15.000,00
3	Falla de equipos dependientes	Servidor Producción		10	1	1	9	5,00	\$ 8.000,00
4	Fallo de los componentes	Servidor Producción		10	5	2	9	6,50	\$ 5.000,00
5	Falta de capacitación en la administración del activo	Servidor Producción		6	9	2	9	6,50	\$ 2.000,00
6	Falta de garantía técnica de los equipos	Servidor Producción		3	2	2	9	4,00	\$ 15.000,00
7	Falta de políticas internas de gestión y cumplimiento	Servidor Producción		7	2	2	9	5,00	\$ 2.000,00
8	Falta de planes de crecimiento y expansión de servicios de TI	Servidor Producción		5	6	2	9	5,50	\$ 2.000,00
9	Falta de planes de recuperación	Servidor Producción		10	10	10	9	9,75	\$ 5.000,00
10	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Servidor Producción		6	8	8	9	7,75	\$ 2.000,00
11	Falta de precaución en las conexiones físicas	Servidor Producción		10	4	2	9	6,25	\$ 5.000,00
12	Falta de política formal de cambio de credenciales	Servidor Producción		2	8	8	9	6,75	\$ 2.000,00

				DIMENSION				VULNERABILIDAD	
	VULNERABILIDAD	ACTIVO	Costo del Activo	Daño Confiabilidad	Daño Integridad	Daño Disponibilidad	Daño Criticidad	Valor del Daño	Costo del Daño
13	Uso inadecuado o descuido del control de acceso físico a edificios y habitaciones	Servidor Producción		10	10	10	9	9,75	\$ 2.000,00
14	Fallo de los componentes	Servidor Producción		10	2	2	9	5,75	\$ 1.000,00
15	Falta de soporte preventivo y correctivo	Servidor Producción		10	1	1	9	5,25	\$ 8.000,00
16	Fallo de los componentes	Servidor Producción		10	2	2	9	5,75	\$ 5.000,00
17	Susceptible a incendios y altas temperaturas	Servidor Preproducción aplicativos	\$ 20.000,00	6	1	1	7	3,75	\$ 20.000,00
18	Ubicación en un área susceptible a inundaciones.	Servidor Preproducción aplicativos		6	1	1	7	3,75	\$ 20.000,00
19	Falla de equipos dependientes	Servidor Preproducción aplicativos		6	1	1	7	3,75	\$ 10.000,00
20	Fallo de los componentes	Servidor Preproducción aplicativos		6	1	1	7	3,75	\$ 7.000,00
21	Falta de capacitación en la administración del activo	Servidor Preproducción aplicativos		6	6	6	7	6,25	\$ 2.000,00
22	Falta de garantía técnica de los equipos	Servidor Preproducción aplicativos		8	2	2	7	4,75	\$ 20.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confiabilidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Críticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
23	Falta de políticas internas de gestión y cumplimiento	Servidor Preproducción aplicativos		6	2	2	7	4,25	\$ 2.000,00
24	Falta de planes de crecimiento y expansión de servicios de TI	Servidor Preproducción aplicativos		6	2	2	7	4,25	\$ 2.000,00
25	Falta de planes de recuperación	Servidor Preproducción aplicativos		8	2	2	7	4,75	\$ 8.000,00
26	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Servidor Preproducción aplicativos		10	2	2	7	5,25	\$ 2.000,00
27	Falta de precaución en las conexiones físicas	Servidor Preproducción aplicativos		6	2	2	7	4,25	\$ 20.000,00
28	Falta de política formal de cambio de credenciales	Servidor Preproducción aplicativos		6	2	2	7	4,25	\$ 2.000,00
29	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Servidor Preproducción aplicativos		10	10	10	7	9,25	\$ 2.000,00
30	Fallo de los componentes	Servidor Preproducción aplicativos		2	2	2	7	3,25	\$ 7.000,00
31	Susceptible a incendios y altas temperaturas	Servidor preproducción BD	\$ 20.000,00	6	1	1	7	3,75	\$ 20.000,00

				DIMENSION				VULNERABILIDAD	
	VULNERABILIDAD	ACTIVO	Costo del Activo	Daño Confiabilidad	Daño Integridad	Daño Disponibilidad	Daño Críticidad	Valor del Daño	Costo del Daño
32	Ubicación en un área susceptible a inundaciones.	Servidor preproducción BD		6	1	1	7	3,75	\$ 20.000,00
33	Falla de equipos dependientes	Servidor preproducción BD		6	1	1	7	3,75	\$ 10.000,00
34	Fallo de los componentes	Servidor preproducción BD		6	1	1	7	3,75	\$ 7.000,00
35	Falta de capacitación en la administración del activo	Servidor preproducción BD		6	6	6	7	6,25	\$ 2.000,00
36	Falta de garantía técnica de los equipos	Servidor preproducción BD		8	2	2	7	4,75	\$ 20.000,00
37	Falta de políticas internas de gestión y cumplimiento	Servidor preproducción BD		6	2	2	7	4,25	\$ 2.000,00
38	Falta de planes de crecimiento y expansión de servicios de TI	Servidor preproducción BD		6	2	2	7	4,25	\$ 2.000,00
39	Falta de planes de recuperación	Servidor preproducción BD		8	2	2	7	4,75	\$ 8.000,00
40	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Servidor preproducción BD		10	2	2	7	5,25	\$ 2.000,00
41	Falta de precaución en las conexiones físicas	Servidor preproducción BD		6	2	2	7	4,25	\$ 20.000,00
42	Falta de política formal de cambio de credenciales	Servidor preproducción BD		6	2	2	7	4,25	\$ 2.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confiabilidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Criticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
43	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Servidor preproducción BD		10	10	10	7	9,25	\$ 2.000,00
44	Fallo de los componentes	Servidor preproducción BD		2	2	2	7	3,25	\$ 7.000,00
45	Susceptible a incendios y altas temperaturas	Servidor web app	\$ 20.000,00	6	1	1	7	3,75	\$ 20.000,00
46	Ubicación en un área susceptible a inundaciones.	Servidor web app		6	1	1	7	3,75	\$ 20.000,00
47	Falla de equipos dependientes	Servidor web app		6	1	1	7	3,75	\$ 10.000,00
48	Fallo de los componentes	Servidor web app		6	1	1	7	3,75	\$ 7.000,00
49	Falta de capacitación en la administración del activo	Servidor web app		6	6	6	7	6,25	\$ 2.000,00
50	Falta de garantía técnica de los equipos	Servidor web app		8	2	2	7	4,75	\$ 20.000,00
51	Falta de políticas internas de gestión y cumplimiento	Servidor web app		6	2	2	7	4,25	\$ 2.000,00
52	Falta de planes de crecimiento y expansión de servicios de TI	Servidor web app		6	2	2	7	4,25	\$ 2.000,00
53	Falta de planes de recuperación	Servidor web app		8	2	2	7	4,75	\$ 8.000,00
54	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Servidor web app		10	2	2	7	5,25	\$ 2.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confiabilidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Criticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
55	Falta de precaución en las conexiones físicas	Servidor web app		6	2	2	7	4,25	\$ 20.000,00
56	Falta de política formal de cambio de credenciales	Servidor web app		6	2	2	7	4,25	\$ 2.000,00
57	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Servidor web app		10	10	10	7	9,25	\$ 2.000,00
58	Fallo de los componentes	Servidor web app		2	2	2	7	3,25	\$ 7.000,00
59	Susceptible a incendios y altas temperaturas	Servidor Backup red	\$ 15.000,00	5	2	2	8	4,25	\$ 15.000,00
60	Ubicación en un área susceptible a inundaciones.	Servidor Backup red		5	2	2	8	4,25	\$ 15.000,00
61	Falla de equipos dependientes	Servidor Backup red		5	2	2	8	4,25	\$ 8.000,00
62	Fallo de los componentes	Servidor Backup red		5	2	2	8	4,25	\$ 5.000,00
63	Falta de capacitación en la administración del activo	Servidor Backup red		6	8	2	8	6,00	\$ 2.000,00
64	Falta de garantía técnica de los equipos	Servidor Backup red		6	8	2	8	6,00	\$ 15.000,00
65	Falta de políticas internas de gestión y cumplimiento	Servidor Backup red		2	2	2	8	3,50	\$ 2.000,00
66	Falta de planes de crecimiento y expansión de servicios de TI	Servidor Backup red		2	2	2	8	3,50	\$ 2.000,00
67	Falta de planes de recuperación	Servidor Backup red		6	2	2	8	4,50	\$ 5.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confiabilidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Criticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
68	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Servidor Backup red		4	2	2	8	4,00	\$ 2.000,00
69	Falta de precaución en las conexiones físicas	Servidor Backup red		4	2	2	8	4,00	\$ 5.000,00
70	Falta de política formal de cambio de credenciales	Servidor Backup red		6	2	2	8	4,50	\$ 2.000,00
71	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Servidor Backup red		2	2	2	8	3,50	\$ 2.000,00
72	Fallo de los componentes	Servidor Backup red		2	2	2	8	3,50	\$ 5.000,00
73	Susceptible a incendios y altas temperaturas	Servidor principal red	\$ 15.000,00	5	2	2	9	4,50	\$ 15.000,00
74	Ubicación en un área susceptible a inundaciones.	Servidor principal red		5	2	2	9	4,50	\$ 15.000,00
75	Falla de equipos dependientes	Servidor principal red		5	2	2	9	4,50	\$ 8.000,00
76	Fallo de los componentes	Servidor principal red		5	2	2	9	4,50	\$ 5.000,00
77	Falta de capacitación en la administración del activo	Servidor principal red		6	8	2	9	6,25	\$ 2.000,00
78	Falta de garantía técnica de los equipos	Servidor principal red		6	8	2	9	6,25	\$ 15.000,00
79	Falta de políticas internas de gestión y cumplimiento	Servidor principal red		2	2	2	9	3,75	\$ 2.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confiabilidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Críticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
80	Falta de planes de crecimiento y expansión de servicios de TI	Servidor principal red		2	2	2	9	3,75	\$ 2.000,00
81	Falta de planes de recuperación	Servidor principal red		6	2	2	9	4,75	\$ 5.000,00
82	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Servidor principal red		4	2	2	9	4,25	\$ 2.000,00
83	Falta de precaución en las conexiones físicas	Servidor principal red		4	2	2	9	4,25	\$ 5.000,00
84	Falta de política formal de cambio de credenciales	Servidor principal red		6	2	2	9	4,75	\$ 2.000,00
85	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Servidor principal red		2	2	2	9	3,75	\$ 2.000,00
86	Fallo de los componentes	Servidor principal red		2	2	2	9	3,75	\$ 5.000,00
87	Susceptible a incendios y altas temperaturas	Servidor de desarrollo	\$ 20.000,00	8	3	3	7	5,25	\$ 20.000,00
88	Ubicación en un área susceptible a inundaciones.	Servidor de desarrollo		8	3	3	7	5,25	\$ 20.000,00
89	Falla de equipos dependientes	Servidor de desarrollo		8	3	3	7	5,25	\$ 10.000,00
90	Fallo de los componentes	Servidor de desarrollo		8	3	3	7	5,25	\$ 10.000,00
91	Falta de capacitación en la administración del activo	Servidor de desarrollo		6	6	6	7	6,25	\$ 2.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confiabilidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Criticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
92	Falta de garantía técnica de los equipos	Servidor de desarrollo		8	2	2	7	4,75	\$ 20.000,00
93	Falta de políticas internas de gestión y cumplimiento	Servidor de desarrollo		6	2	2	7	4,25	\$ 2.000,00
94	Falta de planes de crecimiento y expansión de servicios de TI	Servidor de desarrollo		6	2	2	7	4,25	\$ 2.000,00
95	Falta de planes de recuperación	Servidor de desarrollo		10	2	2	7	5,25	\$ 5.000,00
96	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Servidor de desarrollo		10	2	2	7	5,25	\$ 2.000,00
97	Falta de precaución en las conexiones físicas	Servidor de desarrollo		6	2	2	7	4,25	\$ 5.000,00
98	Falta de política formal de cambio de credenciales	Servidor de desarrollo		6	2	2	7	4,25	\$ 2.000,00
99	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Servidor de desarrollo		10	10	10	7	9,25	\$ 2.000,00
100	Fallo de los componentes	Servidor de desarrollo		2	2	2	7	3,25	\$ 5.000,00
101	Fallo de los componentes	Stack core 1	\$ 15.000,00	10	1	1	10	5,50	\$ 8.000,00
102	Ubicación en un área susceptible a inundaciones.	Stack core 1		10	1	1	10	5,50	\$ 15.000,00
103	Susceptible a incendios y altas temperaturas	Stack core 1		10	1	1	10	5,50	\$ 15.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confiabilidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Críticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
104	Fallo de los componentes	Stack core 1		10	1	1	10	5,50	\$ 8.000,00
105	Falta de mantenimiento y/o actualizaciones	Stack core 1		10	1	1	10	5,50	\$ 2.000,00
106	Falta de precaución en las conexiones físicas	Stack core 1		10	-	-	10	5,00	\$ 7.000,00
107	Falta de política formal de cambio de credenciales	Stack core 1		10	10	10	10	10,00	\$ 2.000,00
108	Falta de políticas internas de gestión y cumplimiento	Stack core 1		10	2	2	10	6,00	\$ 2.000,00
109	Falta de planes de crecimiento y expansión de servicios de TI	Stack core 1		10	1	1	10	5,50	\$ 2.000,00
110	Falta de capacitación en la administración del activo	Stack core 1		10	1	1	10	5,50	\$ 2.000,00
111	Fallo de los componentes	Stack core 1		10	1	1	10	5,50	\$ 7.000,00
112	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Stack core 1		10	8	8	10	9,00	\$ 2.000,00
113	Falta de planes de recuperación	Stack core 1		10	8	8	10	9,00	\$ 5.000,00
114	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Stack core 1		10	10	10	10	10,00	\$ 2.000,00
115	Fallo de los componentes	Stack core 2	\$ 15.000,00	10	1	1	10	5,50	\$ 8.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confiabilidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Críticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
116	Ubicación en un área susceptible a inundaciones.	Stack core 2		10	1	1	10	5,50	\$ 15.000,00
117	Susceptible a incendios y altas temperaturas	Stack core 2		10	1	1	10	5,50	\$ 15.000,00
118	Fallo de los componentes	Stack core 2		10	1	1	10	5,50	\$ 8.000,00
119	Falta de mantenimiento y/o actualizaciones	Stack core 2		10	1	1	10	5,50	\$ 2.000,00
120	Falta de precaución en las conexiones físicas	Stack core 2		10	-	-	10	5,00	\$ 7.000,00
121	Falta de política formal de cambio de credenciales	Stack core 2		10	10	10	10	10,00	\$ 2.000,00
122	Falta de políticas internas de gestión y cumplimiento	Stack core 2		10	2	2	10	6,00	\$ 2.000,00
123	Falta de planes de crecimiento y expansión de servicios de TI	Stack core 2		10	1	1	10	5,50	\$ 2.000,00
124	Falta de capacitación en la administración del activo	Stack core 2		10	1	1	10	5,50	\$ 2.000,00
125	Fallo de los componentes	Stack core 2		10	1	1	10	5,50	\$ 7.000,00
126	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Stack core 2		10	8	8	10	9,00	\$ 2.000,00
127	Falta de planes de recuperación	Stack core 2		10	8	8	10	9,00	\$ 5.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confiabilidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Criticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
128	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Stack core 2		10	10	10	10	10,00	\$ 2.000,00
129	Fallo de los componentes	Stack acceso 1	\$ 12.000,00	10	1	1	9	5,25	\$ 7.000,00
130	Ubicación en un área susceptible a inundaciones.	Stack acceso 1		10	1	1	9	5,25	\$ 12.000,00
131	Susceptible a incendios y altas temperaturas	Stack acceso 1		10	1	1	9	5,25	\$ 12.000,00
132	Fallo de los componentes	Stack acceso 1		10	1	1	9	5,25	\$ 7.000,00
133	Falta de planes de recuperación	Stack acceso 1		10	1	1	9	5,25	\$ 5.000,00
134	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Stack acceso 1		10	10	10	9	9,75	\$ 2.000,00
135	Falta de mantenimiento y/o actualizaciones	Stack acceso 1		10	10	10	9	9,75	\$ 2.000,00
136	Falta de precaución en las conexiones físicas	Stack acceso 1		10	2	2	9	5,75	\$ 7.000,00
137	Falta de política formal de cambio de credenciales	Stack acceso 1		10	1	1	9	5,25	\$ 2.000,00
138	Falta de políticas internas de gestión y cumplimiento	Stack acceso 1		10	1	1	9	5,25	\$ 2.000,00
139	Falta de planes de crecimiento y expansión de servicios de TI	Stack acceso 1		10	1	1	9	5,25	\$ 2.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confiabilidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Críticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
140	Falta de capacitación en la administración del activo	Stack acceso 1		10	8	8	9	8,75	\$ 2.000,00
141	Fallo de los componentes	Stack acceso 1		10	8	8	9	8,75	\$ 7.000,00
142	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Stack acceso 1		10	10	10	9	9,75	\$ 2.000,00
143	Fallo de los componentes	Stack acceso 2	\$ 12.000,00	10	1	1	9	5,25	\$ 7.000,00
144	Ubicación en un área susceptible a inundaciones.	Stack acceso 2		10	1	1	9	5,25	\$ 12.000,00
145	Susceptible a incendios y altas temperaturas	Stack acceso 2		10	1	1	9	5,25	\$ 12.000,00
146	Fallo de los componentes	Stack acceso 2		10	1	1	9	5,25	\$ 7.000,00
147	Falta de planes de recuperación	Stack acceso 2		10	1	1	9	5,25	\$ 5.000,00
148	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Stack acceso 2		10	10	10	9	9,75	\$ 2.000,00
149	Falta de mantenimiento y/o actualizaciones	Stack acceso 2		10	10	10	9	9,75	\$ 2.000,00
150	Falta de precaución en las conexiones físicas	Stack acceso 2		10	2	2	9	5,75	\$ 7.000,00
151	Falta de política formal de cambio de credenciales	Stack acceso 2		10	1	1	9	5,25	\$ 2.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confiabilidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Críticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
152	Falta de políticas internas de gestión y cumplimiento	Stack acceso 2		10	1	1	9	5,25	\$ 2.000,00
153	Falta de planes de crecimiento y expansión de servicios de TI	Stack acceso 2		10	1	1	9	5,25	\$ 2.000,00
154	Falta de capacitación en la administración del activo	Stack acceso 2		10	8	8	9	8,75	\$ 2.000,00
155	Fallo de los componentes	Stack acceso 2		10	8	8	9	8,75	\$ 7.000,00
156	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Stack acceso 2		10	10	10	9	9,75	\$ 2.000,00
157	Fallo de los componentes	Stack acceso 3	\$ 12.000,00	10	1	1	9	5,25	\$ 7.000,00
158	Ubicación en un área susceptible a inundaciones.	Stack acceso 3		10	1	1	9	5,25	\$ 12.000,00
159	Susceptible a incendios y altas temperaturas	Stack acceso 3		10	1	1	9	5,25	\$ 12.000,00
160	Fallo de los componentes	Stack acceso 3		10	1	1	9	5,25	\$ 7.000,00
161	Falta de planes de recuperación	Stack acceso 3		10	1	1	9	5,25	\$ 5.000,00
162	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Stack acceso 3		10	10	10	9	9,75	\$ 2.000,00
163	Falta de mantenimiento y/o actualizaciones	Stack acceso 3		10	10	10	9	9,75	\$ 2.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confiabilidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Criticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
164	Falta de precaución en las conexiones físicas	Stack acceso 3		10	2	2	9	5,75	\$ 7.000,00
165	Falta de política formal de cambio de credenciales	Stack acceso 3		10	1	1	9	5,25	\$ 2.000,00
166	Falta de políticas internas de gestión y cumplimiento	Stack acceso 3		10	1	1	9	5,25	\$ 2.000,00
167	Falta de planes de crecimiento y expansión de servicios de TI	Stack acceso 3		10	1	1	9	5,25	\$ 2.000,00
168	Falta de capacitación en la administración del activo	Stack acceso 3		10	8	8	9	8,75	\$ 2.000,00
169	Fallo de los componentes	Stack acceso 3		10	8	8	9	8,75	\$ 7.000,00
170	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Stack acceso 3		10	10	10	9	9,75	\$ 2.000,00
171	No cuenta con mecanismos contra ataques informáticos	Equipo Producción AS400	\$ 800.000,00	10	10	10	10	10,00	\$ 120.000,00
172	Fallo de los componentes	Equipo Producción AS400		10	6	6	10	8,00	\$ 10.000,00
173	Ubicación en un área susceptible a inundaciones.	Equipo Producción AS400		10	6	6	10	8,00	\$ 800.000,00
174	Susceptible a incendios y altas temperaturas	Equipo Producción AS400		10	6	6	10	8,00	\$ 800.000,00
175	Fallo de los componentes	Equipo Producción AS400		10	6	6	10	8,00	\$ 10.000,00

				DIMENSION				VULNERABILIDAD	
	VULNERABILIDAD	ACTIVO	Costo del Activo	Daño Confiabilidad	Daño Integridad	Daño Disponibilidad	Daño Críticidad	Valor del Daño	Costo del Daño
176	Falla de enlaces externos-terceros	Equipo AS400 Producción		10	3	3	10	6,50	\$ 10.000,00
177	Falta de planes de recuperación	Equipo AS400 Producción		10	10	10	10	10,00	\$ 100.000,00
178	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Equipo AS400 Producción		10	10	10	10	10,00	\$ 10.000,00
179	Falta de mantenimiento y/o actualizaciones	Equipo AS400 Producción		10	4	4	10	7,00	\$ 40.000,00
180	Falta de precaución en las conexiones físicas	Equipo AS400 Producción		10	3	3	10	6,50	\$ 10.000,00
181	Falta de política formal de cambio de credenciales	Equipo AS400 Producción		10	10	10	10	10,00	\$ 10.000,00
182	Falta de políticas internas de gestión y cumplimiento	Equipo AS400 Producción		8	6	6	10	7,50	\$ 10.000,00
183	Falta de capacitación en la administración del activo	Equipo AS400 Producción		10	6	6	10	8,00	\$ 10.000,00
184	Fallo de los componentes	Equipo AS400 Producción		10	2	2	10	6,00	\$ 120.000,00
185	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Equipo AS400 Producción		10	10	10	10	10,00	\$ 10.000,00
186	No cuenta con mecanismos contra ataques informáticos	Equipo AS400 GYE	\$ 800.000,00	10	10	10	9	9,75	\$ 120.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confiabilidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Críticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
187	Fallo de los componentes	Equipo AS400 GYE		10	6	6	9	7,75	\$ 10.000,00
188	Ubicación en un área susceptible a inundaciones.	Equipo AS400 GYE		10	6	6	9	7,75	\$ 800.000,00
189	Susceptible a incendios y altas temperaturas	Equipo AS400 GYE		10	6	6	9	7,75	\$ 800.000,00
190	Fallo de los componentes	Equipo AS400 GYE		10	6	6	9	7,75	\$ 10.000,00
191	Falla de enlaces externos-terceros	Equipo AS400 GYE		10	3	3	9	6,25	\$ 10.000,00
192	Falta de planes de recuperación	Equipo AS400 GYE		10	10	10	9	9,75	\$ 100.000,00
193	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Equipo AS400 GYE		10	10	10	9	9,75	\$ 10.000,00
194	Falta de mantenimiento y/o actualizaciones	Equipo AS400 GYE		10	4	4	9	6,75	\$ 40.000,00
195	Falta de precaución en las conexiones físicas	Equipo AS400 GYE		10	3	3	9	6,25	\$ 10.000,00
196	Falta de política formal de cambio de credenciales	Equipo AS400 GYE		10	10	10	9	9,75	\$ 10.000,00
197	Falta de políticas internas de gestión y cumplimiento	Equipo AS400 GYE		8	6	6	9	7,25	\$ 10.000,00
198	Falta de capacitación en la administración del activo	Equipo AS400 GYE		10	6	6	9	7,75	\$ 10.000,00
199	Fallo de los componentes	Equipo AS400 GYE		10	2	2	9	5,75	\$ 120.000,00

				DIMENSION				VULNERABILIDAD	
	VULNERABILIDAD	ACTIVO	Costo del Activo	Daño Confiabilidad	Daño Integridad	Daño Disponibilidad	Daño Criticidad	Valor del Daño	Costo del Daño
200	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Equipo AS400 GYE		10	10	10	9	9,75	\$ 10.000,00
201	No cuenta con mecanismos contra ataques informáticos	Equipo AS400 Desarrollo	\$ 500.000,00	10	3	3	10	6,50	\$ 80.000,00
202	Fallo de los componentes	Equipo AS400 Desarrollo		8	3	3	10	6,00	\$ 10.000,00
203	Ubicación en un área susceptible a inundaciones.	Equipo AS400 Desarrollo		8	3	3	10	6,00	\$ 500.000,00
204	Susceptible a incendios y altas temperaturas	Equipo AS400 Desarrollo		8	3	3	10	6,00	\$ 500.000,00
205	Fallo de los componentes	Equipo AS400 Desarrollo		6	6	6	10	7,00	\$ 10.000,00
206	Falla de enlaces externos-terceros	Equipo AS400 Desarrollo		8	2	2	10	5,50	\$ 8.000,00
207	Falta de planes de recuperación	Equipo AS400 Desarrollo		6	2	2	10	5,00	\$ 80.000,00
208	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Equipo AS400 Desarrollo		6	2	2	10	5,00	\$ 10.000,00
209	Falta de mantenimiento y/o actualizaciones	Equipo AS400 Desarrollo		10	2	2	10	6,00	\$ 30.000,00
210	Falta de precaución en las conexiones físicas	Equipo AS400 Desarrollo		10	2	2	10	6,00	\$ 8.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confiabilidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Criticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
211	Falta de política formal de cambio de credenciales	Equipo Desarrollo AS400		6	2	2	10	5,00	\$ 8.000,00
212	Falta de políticas internas de gestión y cumplimiento	Equipo Desarrollo AS400		6	2	2	10	5,00	\$ 8.000,00
213	Falta de capacitación en la administración del activo	Equipo Desarrollo AS400		10	10	10	10	10,00	\$ 8.000,00
214	Fallo de los componentes	Equipo Desarrollo AS400		2	2	2	10	4,00	\$ 100.000,00
215	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Equipo Desarrollo AS400		2	2	2	10	4,00	\$ 8.000,00
216	Susceptible a incendios y altas temperaturas	Controladora wireless	\$ 60.000,00	10	2	2	10	6,00	\$ 60.000,00
217	Ubicación en un área susceptible a inundaciones.	Controladora wireless		10	2	2	10	6,00	\$ 60.000,00
218	Falla de equipos dependientes	Controladora wireless		10	2	2	10	6,00	\$ 5.000,00
219	Fallo de los componentes	Controladora wireless		10	2	2	10	6,00	\$ 2.000,00
220	Falta de capacitación en la administración del activo	Controladora wireless		10	2	2	10	6,00	\$ 2.000,00
221	Falta de garantía técnica de los equipos	Controladora wireless		10	1	1	10	5,50	\$ 60.000,00
222	Falta de políticas internas de gestión y cumplimiento	Controladora wireless		6	2	2	10	5,00	\$ 2.000,00

				DIMENSION				VULNERABILIDAD	
	VULNERABILIDAD	ACTIVO	Costo del Activo	Daño Confiabilidad	Daño Integridad	Daño Disponibilidad	Daño Críticidad	Valor del Daño	Costo del Daño
223	Falta de planes de recuperación	Controladora wireless		10	10	10	10	10,00	\$ 5.000,00
224	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Controladora wireless		10	8	8	10	9,00	\$ 2.000,00
225	Falta de precaución en las conexiones físicas	Controladora wireless		10	2	2	10	6,00	\$ 8.000,00
226	Falta de política formal de cambio de credenciales	Controladora wireless		10	8	8	10	9,00	\$ 2.000,00
227	Falta de planes de contingencia	Controladora wireless		10	2	2	10	6,00	\$ 5.000,00
228	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Controladora wireless		10	10	10	10	10,00	\$ 2.000,00
229	Falta de mantenimiento y/o actualizaciones	Controladora wireless		10	1	1	10	5,50	\$ 2.000,00
230	Fallo de los componentes	Controladora wireless		10	2	2	10	6,00	\$ 10.000,00
231	Susceptible a incendios y altas temperaturas	Optimizador Wan	\$ 30.000,00	10	1	1	7	4,75	\$ 30.000,00
232	Ubicación en un área susceptible a inundaciones.	Optimizador Wan		10	1	1	7	4,75	\$ 30.000,00
233	Falla de equipos dependientes	Optimizador Wan		10	1	1	7	4,75	\$ 5.000,00
234	Fallo de los componentes	Optimizador Wan		10	1	1	7	4,75	\$ 2.000,00
235	Falta de capacitación en la administración del activo	Optimizador Wan		10	2	2	7	5,25	\$ 2.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confiabilidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Criticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
236	Falta de precaución en las conexiones físicas	Optimizador Wan		10	2	2	7	5,25	\$ 5.000,00
237	Uso inadecuado o descuido del control de acceso físico a edificios y habitaciones	Optimizador Wan		10	10	10	7	9,25	\$ 2.000,00
238	Falta de mantenimiento y/o actualizaciones	Optimizador Wan		10	1	1	7	4,75	\$ 2.000,00
239	Fallo de los componentes	Optimizador Wan		10	1	1	7	4,75	\$ 15.000,00
240	Susceptible a incendios y altas temperaturas	Aires Acondicionados	\$ 40.000,00	10	1	1	6	4,50	\$ 40.000,00
241	Ubicación en un área susceptible a inundaciones.	Aires Acondicionados		10	1	1	6	4,50	\$ 40.000,00
242	Falla de equipos dependientes	Aires Acondicionados		10	1	1	6	4,50	\$ 5.000,00
243	Fallo de los componentes	Aires Acondicionados		10	1	1	6	4,50	\$ 15.000,00
244	Falta de capacitación en la administración del activo	Aires Acondicionados		10	1	1	6	4,50	\$ 3.000,00
245	Falta de gestión en la disponibilidad de repuestos de equipos críticos	Aires Acondicionados		10	-	-	6	4,00	\$ 10.000,00
246	Falta de planes de contingencia	Aires Acondicionados		10	1	1	6	4,50	\$ 5.000,00
247	Falta de soporte preventivo y correctivo	Aires Acondicionados		10	1	1	6	4,50	\$ 7.000,00
248	Falta de precaución en las conexiones físicas	Aires Acondicionados		10	1	1	6	4,50	\$ 7.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confiabilidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Criticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
249	Susceptible a incendios y altas temperaturas	UPS	\$ 20.000,00	10	1	1	9	5,25	\$ 20.000,00
250	Ubicación en un área susceptible a inundaciones.	UPS		10	1	1	9	5,25	\$ 20.000,00
251	Fallo de los componentes	UPS		10	1	1	9	5,25	\$ 7.000,00
252	Fallo de los componentes	UPS		10	1	1	9	5,25	\$ 5.000,00
253	Falta de capacitación en la administración del activo	UPS		10	1	1	9	5,25	\$ 3.000,00
254	Falta de gestión en la disponibilidad de repuestos de equipos críticos	UPS		10	-	-	9	4,75	\$ 7.000,00
255	Falta de planes de contingencia	UPS		10	1	1	9	5,25	\$ 5.000,00
256	Falta de soporte preventivo y correctivo	UPS		10	1	1	9	5,25	\$ 7.000,00
257	Falta de precaución en las conexiones físicas	UPS		10	1	1	9	5,25	\$ 5.000,00
258	Fallo de los componentes	Switch piso	\$ 10.000,00	10	1	1	10	5,50	\$ 8.000,00
259	Ubicación en un área susceptible a inundaciones.	Switch piso		10	1	1	10	5,50	\$ 10.000,00
260	Susceptible a incendios y altas temperaturas	Switch piso		10	1	1	10	5,50	\$ 10.000,00
261	Fallo de los componentes	Switch piso		10	1	1	10	5,50	\$ 5.000,00
262	Falta de planes de recuperación	Switch piso		10	1	1	10	5,50	\$ 2.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confiabilidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Criticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
263	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Switch piso		10	10	10	10	10,00	\$ 2.000,00
264	Falta de mantenimiento y/o actualizaciones	Switch piso		10	2	2	10	6,00	\$ 2.000,00
265	Falta de precaución en las conexiones físicas	Switch piso		10	2	2	10	6,00	\$ 5.000,00
266	Falta de política formal de cambio de credenciales	Switch piso		10	1	1	10	5,50	\$ 2.000,00
267	Falta de políticas internas de gestión y cumplimiento	Switch piso		10	1	1	10	5,50	\$ 2.000,00
268	Falta de planes de crecimiento y expansión de servicios de TI	Switch piso		10	1	1	10	5,50	\$ 5.000,00
269	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	Switch piso		10	-	-	10	5,00	\$ 10.000,00
270	Falta de capacitación en la administración del activo	Switch piso		10	8	8	10	9,00	\$ 2.000,00
271	Espacio físico designado no reúne condiciones técnicas	Switch piso		10	10	10	10	10,00	\$ 5.000,00
272	Fallo de los componentes	Switch piso		10	1	1	10	5,50	\$ 2.000,00
273	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Switch piso		10	10	10	10	10,00	\$ 2.000,00

				DIMENSION				VULNERABILIDAD	
	VULNERABILIDAD	ACTIVO	Costo del Activo	Daño Confiabilidad	Daño Integridad	Daño Disponibilidad	Daño Criticidad	Valor del Daño	Costo del Daño
274	Falta de capacitación en la administración del activo	Sistema AS400 Médico	\$ 3.000.000,00	10	2	2	10	6,00	\$ 25.000,00
275	Falta de planes de contingencia	Sistema AS400 Médico		10	8	8	10	9,00	\$ 1.000.000,00
276	No posee alta disponibilidad	Sistema AS400 Médico		10	10	10	10	10,00	\$ 1.000.000,00
277	No cuenta con mecanismos contra ataques informáticos	Sistema AS400 Médico		10	1	1	10	5,50	\$ 100.000,00
278	Falta de documentación técnica	Sistema AS400 Médico		8	2	2	10	5,50	\$ 200.000,00
279	No posee un procedimiento de respaldo	Sistema AS400 Médico		10	6	6	10	8,00	\$ 200.000,00
280	Falta de soporte preventivo y correctivo	QlikView	\$ 30.000,00	6	1	1	9	4,25	\$ 15.000,00
281	No posee un procedimiento de respaldo	QlikView		10	1	1	9	5,25	\$ 10.000,00
282	Falta de planes de contingencia	Aplicativos Producción Web	\$ 500.000,00	10	10	10	10	10,00	\$ 100.000,00
283	No posee alta disponibilidad	Aplicativos Producción Web		10	2	3	10	6,25	\$ 200.000,00
284	Mala gestión de contraseñas	Aplicativos Producción Web		10	8	8	10	9,00	\$ 10.000,00
285	Falta de política formal de cambio de credenciales	Aplicativos Producción Web		10	8	8	10	9,00	\$ 10.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confiabilidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Criticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
286	No cuenta con mecanismos contra ataques informáticos	Página Web	\$ 10.000,00	8	1	1	4	3,50	\$ 5.000,00
287	Falta de política formal de cambio de credenciales	Página Web		10	8	8	4	7,50	\$ 5.000,00
288	Falta de capacitación en la administración del activo	Software Firewall	\$ 15.000,00	10	6	6	9	7,75	\$ 7.000,00
289	Falta de garantía técnica de los equipos	Software Firewall		10	2	2	9	5,75	\$ 8.000,00
290	Falta de planes de contingencia	Alfresco	\$ 10.000,00	6	1	1	7	3,75	\$ 10.000,00
291	Falta de soporte preventivo y correctivo	Alfresco		6	1	1	7	3,75	\$ 5.000,00
292	Falta de control efectivo del cambio	Alfresco		6	1	1	7	3,75	\$ 5.000,00
293	Falta de planes de contingencia	Biblioteca Virtual	\$ 10.000,00	6	1	1	4	3,00	\$ 10.000,00
294	Falta de soporte preventivo y correctivo	Biblioteca Virtual		6	1	1	4	3,00	\$ 5.000,00
295	Falta de control efectivo del cambio	Biblioteca Virtual		6	1	1	4	3,00	\$ 5.000,00
296	Falta de planes de contingencia	EVCAM	\$ 10.000,00	6	1	1	4	3,00	\$ 10.000,00
297	Falta de soporte preventivo y correctivo	EVCAM		6	1	1	4	3,00	\$ 5.000,00
298	Falta de control efectivo del cambio	EVCAM		6	1	1	4	3,00	\$ 5.000,00
299	Falta de planes de contingencia	Aplicativo de Facturación	\$ 15.000,00	10	10	10	10	10,00	\$ 10.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confiabilidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Críticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
300	No posee alta disponibilidad	Aplicativo de Facturación		10	8	8	10	9,00	\$ 10.000,00
301	Falta de política formal de cambio de credenciales	Aplicativo de Facturación		10	10	10	10	10,00	\$ 5.000,00
302	Falta de planes de contingencia	Base de datos postgres	\$ 10.000,00	10	2	2	10	6,00	\$ 10.000,00
303	Falta de planes de crecimiento y expansión de servicios de TI	Base de datos postgres		10	2	2	10	6,00	\$ 20.000,00
304	Falta de planes de recuperación	Base de datos postgres		10	10	10	10	10,00	\$ 10.000,00

IV.6.4. Actividad 4: Identificación de Amenazas de ciberseguridad

En esta actividad se identifican las amenazas para cada una de las vulnerabilidades asociadas a los activos de ciberseguridad, como se muestra en la Tabla IV-19.

Tabla IV-19. Triplete Amenazas – Vulnerabilidades -Activos con el valor y costo del daño de la Amenaza para plataforma AS400-IESS

	AMENAZA	VULNERABILIDAD	ACTIVO	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
1	Fuego	Susceptible a incendios y altas temperaturas	Servidor Producción	6,75	\$ 15.000,00
2	Agua	Ubicación en un área susceptible a inundaciones.	Servidor Producción	6,75	\$ 15.000,00
3	Fallo o interrupción del suministro principal	Falla de equipos dependientes	Servidor Producción	5,00	\$ 8.000,00
4	Condiciones climáticas desfavorables	Fallo de los componentes	Servidor Producción	6,00	\$ 11.000,00
5	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Servidor Producción	6,50	\$ 2.000,00
6	Mal funcionamiento de los equipos (dispositivos o sistemas)	Falta de garantía técnica de los equipos	Servidor Producción	4,00	\$ 15.000,00
7	Uso erróneo o administración de dispositivos y sistemas	Falta de políticas internas de gestión y cumplimiento	Servidor Producción	5,00	\$ 2.000,00
8	Fallo de software /aplicaciones o servicio	Falta de planes de crecimiento y expansión de servicios de TI	Servidor Producción	5,50	\$ 2.000,00
9	Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de recuperación	Servidor Producción	9,75	\$ 5.000,00
10	Actividades no autorizadas	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Servidor Producción	7,75	\$ 2.000,00
11	Pérdida de recursos	Falta de precaución en las conexiones físicas	Servidor Producción	6,25	\$ 5.000,00
12	Robo de identidad (Fraude de identidad / Cuenta)	Falta de política formal de cambio de credenciales	Servidor Producción	6,75	\$ 2.000,00

	AMENAZA	VULNERABILIDAD	ACTIVO	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
13	Manipulación de hardware y software	Uso inadecuado o descuido del control de acceso físico a edificios y habitaciones	Servidor Producción	9,75	\$ 2.000,00
14	Fallo de dispositivos o sistemas	Fallo de los componentes	Servidor Producción	6,00	\$ 11.000,00
15	Fallo de dispositivos o sistemas	Falta de soporte preventivo y correctivo	Servidor Producción	5,25	\$ 8.000,00
16	Fallo de dispositivos o sistemas	Fallo de los componentes	Servidor Producción	6,00	\$ 11.000,00
17	Fuego	Susceptible a incendios y altas temperaturas	Servidor Preproducción aplicativos	3,75	\$ 20.000,00
18	Agua	Ubicación en un área susceptible a inundaciones.	Servidor Preproducción aplicativos	3,75	\$ 20.000,00
19	Fallo o interrupción del suministro principal	Falla de equipos dependientes	Servidor Preproducción aplicativos	3,75	\$ 10.000,00
20	Condiciones climáticas desfavorables	Fallo de los componentes	Servidor Preproducción aplicativos	3,50	\$ 14.000,00
21	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Servidor Preproducción aplicativos	6,25	\$ 2.000,00
22	Mal funcionamiento de los equipos (dispositivos o sistemas)	Falta de garantía técnica de los equipos	Servidor Preproducción aplicativos	4,75	\$ 20.000,00
23	Uso erróneo o administración de dispositivos y sistemas	Falta de políticas internas de gestión y cumplimiento	Servidor Preproducción aplicativos	4,25	\$ 2.000,00
24	Fallo de software /aplicaciones o servicio	Falta de planes de crecimiento y expansión de servicios de TI	Servidor Preproducción aplicativos	4,25	\$ 2.000,00
25	Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de recuperación	Servidor Preproducción aplicativos	4,75	\$ 8.000,00
26	Actividades no autorizadas	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Servidor Preproducción aplicativos	5,25	\$ 2.000,00

	AMENAZA	VULNERABILIDAD	ACTIVO	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
27	Pérdida de recursos	Falta de precaución en las conexiones físicas	Servidor Preproducción aplicativos	4,25	\$ 20.000,00
28	Robo de identidad (Fraude de identidad / Cuenta)	Falta de política formal de cambio de credenciales	Servidor Preproducción aplicativos	4,25	\$ 2.000,00
29	Manipulación de hardware y software	Uso inadecuado o descuido del control de acceso físico a edificios y habitaciones	Servidor Preproducción aplicativos	9,25	\$ 2.000,00
30	Fallo de dispositivos o sistemas	Fallo de los componentes	Servidor Preproducción aplicativos	3,50	\$ 14.000,00
31	Fuego	Susceptible a incendios y altas temperaturas	Servidor preproducción BD	3,75	\$ 20.000,00
32	Agua	Ubicación en un área susceptible a inundaciones.	Servidor preproducción BD	3,75	\$ 20.000,00
33	Fallo o interrupción del suministro principal	Falla de equipos dependientes	Servidor preproducción BD	3,75	\$ 10.000,00
34	Condiciones climáticas desfavorables	Fallo de los componentes	Servidor preproducción BD	3,50	\$ 14.000,00
35	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Servidor preproducción BD	6,25	\$ 2.000,00
36	Mal funcionamiento de los equipos (dispositivos o sistemas)	Falta de garantía técnica de los equipos	Servidor preproducción BD	4,75	\$ 20.000,00
37	Uso erróneo o administración de dispositivos y sistemas	Falta de políticas internas de gestión y cumplimiento	Servidor preproducción BD	4,25	\$ 2.000,00
38	Fallo de software /aplicaciones o servicio	Falta de planes de crecimiento y expansión de servicios de TI	Servidor preproducción BD	4,25	\$ 2.000,00
39	Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de recuperación	Servidor preproducción BD	4,75	\$ 8.000,00
40	Actividades no autorizadas	Falta de mecanismos de identificación y autenticación como la	Servidor preproducción BD	5,25	\$ 2.000,00

	AMENAZA	VULNERABILIDAD	ACTIVO	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
		autenticación de usuarios.			
41	Pérdida de recursos	Falta de precaución en las conexiones físicas	Servidor preproducción BD	4,25	\$ 20.000,00
42	Robo de identidad (Fraude de identidad / Cuenta)	Falta de política formal de cambio de credenciales	Servidor preproducción BD	4,25	\$ 2.000,00
43	Manipulación de hardware y software	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Servidor preproducción BD	9,25	\$ 2.000,00
44	Fallo de dispositivos o sistemas	Fallo de los componentes	Servidor preproducción BD	3,50	\$ 14.000,00
45	Fuego	Susceptible a incendios y altas temperaturas	Servidor web app	3,75	\$ 20.000,00
46	Agua	Ubicación en un área susceptible a inundaciones.	Servidor web app	3,75	\$ 20.000,00
47	Fallo o interrupción del suministro principal	Falla de equipos dependientes	Servidor web app	3,75	\$ 10.000,00
48	Condiciones climáticas desfavorables	Fallo de los componentes	Servidor web app	3,50	\$ 14.000,00
49	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Servidor web app	6,25	\$ 2.000,00
50	Mal funcionamiento de los equipos (dispositivos o sistemas)	Falta de garantía técnica de los equipos	Servidor web app	4,75	\$ 20.000,00
51	Uso erróneo o administración de dispositivos y sistemas	Falta de políticas internas de gestión y cumplimiento	Servidor web app	4,25	\$ 2.000,00
52	Fallo de software /aplicaciones o servicio	Falta de planes de crecimiento y expansión de servicios de TI	Servidor web app	4,25	\$ 2.000,00
53	Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de recuperación	Servidor web app	4,75	\$ 8.000,00
54	Actividades no autorizadas	Falta de mecanismos de identificación y autenticación como la	Servidor web app	5,25	\$ 2.000,00

	AMENAZA	VULNERABILIDAD	ACTIVO	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
		autenticación de usuarios.			
55	Pérdida de recursos	Falta de precaución en las conexiones físicas	Servidor web app	4,25	\$ 20.000,00
56	Robo de identidad (Fraude de identidad / Cuenta)	Falta de política formal de cambio de credenciales	Servidor web app	4,25	\$ 2.000,00
57	Manipulación de hardware y software	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Servidor web app	9,25	\$ 2.000,00
58	Fallo de dispositivos o sistemas	Fallo de los componentes	Servidor web app	3,50	\$ 14.000,00
59	Fuego	Susceptible a incendios y altas temperaturas	Servidor Backup red	4,25	\$ 15.000,00
60	Agua	Ubicación en un área susceptible a inundaciones.	Servidor Backup red	4,25	\$ 15.000,00
61	Fallo o interrupción del suministro principal	Falla de equipos dependientes	Servidor Backup red	4,25	\$ 8.000,00
62	Condiciones climáticas desfavorables	Fallo de los componentes	Servidor Backup red	3,88	\$ 10.000,00
63	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Servidor Backup red	6,00	\$ 2.000,00
64	Mal funcionamiento de los equipos (dispositivos o sistemas)	Falta de garantía técnica de los equipos	Servidor Backup red	6,00	\$ 15.000,00
65	Uso erróneo o administración de dispositivos y sistemas	Falta de políticas internas de gestión y cumplimiento	Servidor Backup red	3,50	\$ 2.000,00
66	Fallo de software /aplicaciones o servicio	Falta de planes de crecimiento y expansión de servicios de TI	Servidor Backup red	3,50	\$ 2.000,00
67	Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de recuperación	Servidor Backup red	4,50	\$ 5.000,00
68	Actividades no autorizadas	Falta de mecanismos de identificación y autenticación como la	Servidor Backup red	4,00	\$ 2.000,00

	AMENAZA	VULNERABILIDAD	ACTIVO	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
		autenticación de usuarios.			
69	Pérdida de recursos	Falta de precaución en las conexiones físicas	Servidor Backup red	4,00	\$ 5.000,00
70	Robo de identidad (Fraude de identidad / Cuenta)	Falta de política formal de cambio de credenciales	Servidor Backup red	4,50	\$ 2.000,00
71	Manipulación de hardware y software	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Servidor Backup red	3,50	\$ 2.000,00
72	Fallo de dispositivos o sistemas	Fallo de los componentes	Servidor Backup red	3,88	\$ 10.000,00
73	Fuego	Susceptible a incendios y altas temperaturas	Servidor principal red	4,50	\$ 15.000,00
74	Agua	Ubicación en un área susceptible a inundaciones.	Servidor principal red	4,50	\$ 15.000,00
75	Fallo o interrupción del suministro principal	Falla de equipos dependientes	Servidor principal red	4,50	\$ 8.000,00
76	Condiciones climáticas desfavorables	Fallo de los componentes	Servidor principal red	4,13	\$ 10.000,00
77	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Servidor principal red	6,25	\$ 2.000,00
78	Mal funcionamiento de los equipos (dispositivos o sistemas)	Falta de garantía técnica de los equipos	Servidor principal red	6,25	\$ 15.000,00
79	Uso erróneo o administración de dispositivos y sistemas	Falta de políticas internas de gestión y cumplimiento	Servidor principal red	3,75	\$ 2.000,00
80	Fallo de software /aplicaciones o servicio	Falta de planes de crecimiento y expansión de servicios de TI	Servidor principal red	3,75	\$ 2.000,00
81	Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de recuperación	Servidor principal red	4,75	\$ 5.000,00
82	Actividades no autorizadas	Falta de mecanismos de identificación y autenticación como la	Servidor principal red	4,25	\$ 2.000,00

	AMENAZA	VULNERABILIDAD	ACTIVO	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
		autenticación de usuarios.			
83	Pérdida de recursos	Falta de precaución en las conexiones físicas	Servidor principal red	4,25	\$ 5.000,00
84	Robo de identidad (Fraude de identidad / Cuenta)	Falta de política formal de cambio de credenciales	Servidor principal red	4,75	\$ 2.000,00
85	Manipulación de hardware y software	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Servidor principal red	3,75	\$ 2.000,00
86	Fallo de dispositivos o sistemas	Fallo de los componentes	Servidor principal red	4,13	\$ 10.000,00
87	Fuego	Susceptible a incendios y altas temperaturas	Servidor de desarrollo	5,25	\$ 20.000,00
88	Agua	Ubicación en un área susceptible a inundaciones.	Servidor de desarrollo	5,25	\$ 20.000,00
89	Fallo o interrupción del suministro principal	Falla de equipos dependientes	Servidor de desarrollo	5,25	\$ 10.000,00
90	Condiciones climáticas desfavorables	Fallo de los componentes	Servidor de desarrollo	4,25	\$ 15.000,00
91	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Servidor de desarrollo	6,25	\$ 2.000,00
92	Mal funcionamiento de los equipos (dispositivos o sistemas)	Falta de garantía técnica de los equipos	Servidor de desarrollo	4,75	\$ 20.000,00
93	Uso erróneo o administración de dispositivos y sistemas	Falta de políticas internas de gestión y cumplimiento	Servidor de desarrollo	4,25	\$ 2.000,00
94	Fallo de software /aplicaciones o servicio	Falta de planes de crecimiento y expansión de servicios de TI	Servidor de desarrollo	4,25	\$ 2.000,00
95	Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de recuperación	Servidor de desarrollo	5,25	\$ 5.000,00
96	Actividades no autorizadas	Falta de mecanismos de identificación y autenticación como la	Servidor de desarrollo	5,25	\$ 2.000,00

	AMENAZA	VULNERABILIDAD	ACTIVO	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
		autenticación de usuarios.			
97	Pérdida de recursos	Falta de precaución en las conexiones físicas	Servidor de desarrollo	4,25	\$ 5.000,00
98	Robo de identidad (Fraude de identidad / Cuenta)	Falta de política formal de cambio de credenciales	Servidor de desarrollo	4,25	\$ 2.000,00
99	Manipulación de hardware y software	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Servidor de desarrollo	9,25	\$ 2.000,00
100	Fallo de dispositivos o sistemas	Fallo de los componentes	Servidor de desarrollo	4,25	\$ 15.000,00
101	Condiciones climáticas desfavorables	Fallo de los componentes	Stack core 1	5,50	\$ 23.000,00
102	Agua	Ubicación en un área susceptible a inundaciones.	Stack core 1	5,50	\$ 15.000,00
103	Fuego	Susceptible a incendios y altas temperaturas	Stack core 1	5,50	\$ 15.000,00
104	Fallo o interrupción del suministro principal	Fallo de los componentes	Stack core 1	5,50	\$ 23.000,00
105	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	Stack core 1	5,50	\$ 2.000,00
106	Pérdida de recursos	Falta de precaución en las conexiones físicas	Stack core 1	5,00	\$ 7.000,00
107	Robo de identidad (Fraude de identidad / Cuenta)	Falta de política formal de cambio de credenciales	Stack core 1	10,00	\$ 2.000,00
108	Uso erróneo o administración de dispositivos y sistemas	Falta de políticas internas de gestión y cumplimiento	Stack core 1	6,00	\$ 2.000,00
109	Fallo de software /aplicaciones o servicio	Falta de planes de crecimiento y expansión de servicios de TI	Stack core 1	5,50	\$ 2.000,00
110	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Stack core 1	5,50	\$ 2.000,00
111	Fallo de dispositivos o sistemas	Fallo de los componentes	Stack core 1	5,50	\$ 23.000,00

	AMENAZA	VULNERABILIDAD	ACTIVO	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
112	Manipulación de hardware y software	Uso inadecuado o descuido del control de acceso físico a edificios y habitaciones	Stack core 1	9,00	\$ 2.000,00
113	Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de recuperación	Stack core 1	9,00	\$ 5.000,00
114	Actividades no autorizadas	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Stack core 1	10,00	\$ 2.000,00
115	Condiciones climáticas desfavorables	Fallo de los componentes	Stack core 2	5,50	\$ 23.000,00
116	Agua	Ubicación en un área susceptible a inundaciones.	Stack core 2	5,50	\$ 15.000,00
117	Fuego	Susceptible a incendios y altas temperaturas	Stack core 2	5,50	\$ 15.000,00
118	Fallo o interrupción del suministro principal	Fallo de los componentes	Stack core 2	5,50	\$ 23.000,00
119	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	Stack core 2	5,50	\$ 2.000,00
120	Pérdida de recursos	Falta de precaución en las conexiones físicas	Stack core 2	5,00	\$ 7.000,00
121	Robo de identidad (Fraude de identidad / Cuenta)	Falta de política formal de cambio de credenciales	Stack core 2	10,00	\$ 2.000,00
122	Uso erróneo o administración de dispositivos y sistemas	Falta de políticas internas de gestión y cumplimiento	Stack core 2	6,00	\$ 2.000,00
123	Fallo de software /aplicaciones o servicio	Falta de planes de crecimiento y expansión de servicios de TI	Stack core 2	5,50	\$ 2.000,00
124	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Stack core 2	5,50	\$ 2.000,00
125	Fallo de dispositivos o sistemas	Fallo de los componentes	Stack core 2	5,50	\$ 23.000,00

	AMENAZA	VULNERABILIDAD	ACTIVO	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
126	Manipulación de hardware y software	Uso inadecuado o descuido del control de acceso físico a edificios y habitaciones	Stack core 2	9,00	\$ 2.000,00
127	Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de recuperación	Stack core 2	9,00	\$ 5.000,00
128	Actividades no autorizadas	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Stack core 2	10,00	\$ 2.000,00
129	Condiciones climáticas desfavorables	Fallo de los componentes	Stack acceso 1	6,42	\$ 21.000,00
130	Agua	Ubicación en un área susceptible a inundaciones.	Stack acceso 1	5,25	\$ 12.000,00
131	Fuego	Susceptible a incendios y altas temperaturas	Stack acceso 1	5,25	\$ 12.000,00
132	Fallo o interrupción del suministro principal	Fallo de los componentes	Stack acceso 1	6,42	\$ 21.000,00
133	Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de recuperación	Stack acceso 1	5,25	\$ 5.000,00
134	Actividades no autorizadas	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Stack acceso 1	9,75	\$ 2.000,00
135	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	Stack acceso 1	9,75	\$ 2.000,00
136	Pérdida de recursos	Falta de precaución en las conexiones físicas	Stack acceso 1	5,75	\$ 7.000,00
137	Robo de identidad (Fraude de identidad / Cuenta)	Falta de política formal de cambio de credenciales	Stack acceso 1	5,25	\$ 2.000,00
138	Uso erróneo o administración de dispositivos y sistemas	Falta de políticas internas de gestión y cumplimiento	Stack acceso 1	5,25	\$ 2.000,00

	AMENAZA	VULNERABILIDAD	ACTIVO	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
139	Fallo de software /aplicaciones o servicio	Falta de planes de crecimiento y expansión de servicios de TI	Stack acceso 1	5,25	\$ 2.000,00
140	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Stack acceso 1	8,75	\$ 2.000,00
141	Fallo de dispositivos o sistemas	Fallo de los componentes	Stack acceso 1	6,42	\$ 21.000,00
142	Manipulación de hardware y software	Uso inadecuado o descuido del control de acceso físico a edificios y habitaciones	Stack acceso 1	9,75	\$ 2.000,00
143	Condiciones climáticas desfavorables	Fallo de los componentes	Stack acceso 2	6,42	\$ 21.000,00
144	Agua	Ubicación en un área susceptible a inundaciones.	Stack acceso 2	5,25	\$ 12.000,00
145	Fuego	Susceptible a incendios y altas temperaturas	Stack acceso 2	5,25	\$ 12.000,00
146	Fallo o interrupción del suministro principal	Fallo de los componentes	Stack acceso 2	6,42	\$ 21.000,00
147	Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de recuperación	Stack acceso 2	5,25	\$ 5.000,00
148	Actividades no autorizadas	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Stack acceso 2	9,75	\$ 2.000,00
149	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	Stack acceso 2	9,75	\$ 2.000,00
150	Pérdida de recursos	Falta de precaución en las conexiones físicas	Stack acceso 2	5,75	\$ 7.000,00
151	Robo de identidad (Fraude de identidad / Cuenta)	Falta de política formal de cambio de credenciales	Stack acceso 2	5,25	\$ 2.000,00
152	Uso erróneo o administración de dispositivos y sistemas	Falta de políticas internas de gestión y cumplimiento	Stack acceso 2	5,25	\$ 2.000,00

	AMENAZA	VULNERABILIDAD	ACTIVO	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
153	Fallo de software /aplicaciones o servicio	Falta de planes de crecimiento y expansión de servicios de TI	Stack acceso 2	5,25	\$ 2.000,00
154	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Stack acceso 2	8,75	\$ 2.000,00
155	Fallo de dispositivos o sistemas	Fallo de los componentes	Stack acceso 2	6,42	\$ 21.000,00
156	Manipulación de hardware y software	Uso inadecuado o descuido del control de acceso físico a edificios y habitaciones	Stack acceso 2	9,75	\$ 2.000,00
157	Condiciones climáticas desfavorables	Fallo de los componentes	Stack acceso 3	6,42	\$ 21.000,00
158	Agua	Ubicación en un área susceptible a inundaciones.	Stack acceso 3	5,25	\$ 12.000,00
159	Fuego	Susceptible a incendios y altas temperaturas	Stack acceso 3	5,25	\$ 12.000,00
160	Fallo o interrupción del suministro principal	Fallo de los componentes	Stack acceso 3	6,42	\$ 21.000,00
161	Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de recuperación	Stack acceso 3	5,25	\$ 5.000,00
162	Actividades no autorizadas	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Stack acceso 3	9,75	\$ 2.000,00
163	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	Stack acceso 3	9,75	\$ 2.000,00
164	Pérdida de recursos	Falta de precaución en las conexiones físicas	Stack acceso 3	5,75	\$ 7.000,00
165	Robo de identidad (Fraude de identidad / Cuenta)	Falta de política formal de cambio de credenciales	Stack acceso 3	5,25	\$ 2.000,00
166	Uso erróneo o administración de dispositivos y sistemas	Falta de políticas internas de gestión y cumplimiento	Stack acceso 3	5,25	\$ 2.000,00

	AMENAZA	VULNERABILIDAD	ACTIVO	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
167	Fallo de software /aplicaciones o servicio	Falta de planes de crecimiento y expansión de servicios de TI	Stack acceso 3	5,25	\$ 2.000,00
168	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Stack acceso 3	8,75	\$ 2.000,00
169	Fallo de dispositivos o sistemas	Fallo de los componentes	Stack acceso 3	6,42	\$ 21.000,00
170	Manipulación de hardware y software	Uso inadecuado o descuido del control de acceso físico a edificios y habitaciones	Stack acceso 3	9,75	\$ 2.000,00
171	Negación de servicio	No cuenta con mecanismos contra ataques informáticos	Equipo AS400 Producción	10,00	\$ 120.000,00
172	Condiciones climáticas desfavorables	Fallo de los componentes	Equipo AS400 Producción	7,33	\$ 140.000,00
173	Agua	Ubicación en un área susceptible a inundaciones.	Equipo AS400 Producción	8,00	\$ 800.000,00
174	Fuego	Susceptible a incendios y altas temperaturas	Equipo AS400 Producción	8,00	\$ 800.000,00
175	Fallo o interrupción del suministro principal	Fallo de los componentes	Equipo AS400 Producción	7,33	\$ 140.000,00
176	Daños causados por un tercero	Falla de enlaces externos-terceros	Equipo AS400 Producción	6,50	\$ 10.000,00
177	Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de recuperación	Equipo AS400 Producción	10,00	\$ 100.000,00
178	Actividades no autorizadas	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Equipo AS400 Producción	10,00	\$ 10.000,00
179	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	Equipo AS400 Producción	7,00	\$ 40.000,00
180	Pérdida de recursos	Falta de precaución en las conexiones físicas	Equipo AS400 Producción	6,50	\$ 10.000,00
181	Robo de identidad (Fraude de identidad / Cuenta)	Falta de política formal de cambio de credenciales	Equipo AS400 Producción	10,00	\$ 10.000,00

	AMENAZA	VULNERABILIDAD	ACTIVO	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
182	Uso erróneo o administración de dispositivos y sistemas	Falta de políticas internas de gestión y cumplimiento	Equipo AS400 Producción	7,50	\$ 10.000,00
183	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Equipo AS400 Producción	8,00	\$ 10.000,00
184	Fallo de dispositivos o sistemas	Fallo de los componentes	Equipo AS400 Producción	7,33	\$ 140.000,00
185	Manipulación de hardware y software	Uso inadecuado o descuido del control de acceso físico a edificios y habitaciones	Equipo AS400 Producción	10,00	\$ 10.000,00
186	Negación de servicio	No cuenta con mecanismos contra ataques informáticos	Equipo AS400 GYE	9,75	\$ 120.000,00
187	Condiciones climáticas desfavorables	Fallo de los componentes	Equipo AS400 GYE	7,08	\$ 140.000,00
188	Agua	Ubicación en un área susceptible a inundaciones.	Equipo AS400 GYE	7,75	\$ 800.000,00
189	Fuego	Susceptible a incendios y altas temperaturas	Equipo AS400 GYE	7,75	\$ 800.000,00
190	Fallo o interrupción del suministro principal	Fallo de los componentes	Equipo AS400 GYE	7,08	\$ 140.000,00
191	Daños causados por un tercero	Falla de enlaces externos-terceros	Equipo AS400 GYE	6,25	\$ 10.000,00
192	Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de recuperación	Equipo AS400 GYE	9,75	\$ 100.000,00
193	Actividades no autorizadas	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Equipo AS400 GYE	9,75	\$ 10.000,00
194	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	Equipo AS400 GYE	6,75	\$ 40.000,00
195	Pérdida de recursos	Falta de precaución en las conexiones físicas	Equipo AS400 GYE	6,25	\$ 10.000,00
196	Robo de identidad (Fraude de identidad / Cuenta)	Falta de política formal de cambio de credenciales	Equipo AS400 GYE	9,75	\$ 10.000,00

	AMENAZA	VULNERABILIDAD	ACTIVO	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
197	Uso erróneo o administración de dispositivos y sistemas	Falta de políticas internas de gestión y cumplimiento	Equipo AS400 GYE	7,25	\$ 10.000,00
198	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Equipo AS400 GYE	7,75	\$ 10.000,00
199	Fallo de dispositivos o sistemas	Fallo de los componentes	Equipo AS400 GYE	7,08	\$ 140.000,00
200	Manipulación de hardware y software	Uso inadecuado o descuido del control de acceso físico a edificios y habitaciones	Equipo AS400 GYE	9,75	\$ 10.000,00
201	Negación de servicio	No cuenta con mecanismos contra ataques informáticos	Equipo AS400 Desarrollo	6,50	\$ 80.000,00
202	Condiciones climáticas desfavorables	Fallo de los componentes	Equipo AS400 Desarrollo	5,67	\$ 120.000,00
203	Agua	Ubicación en un área susceptible a inundaciones.	Equipo AS400 Desarrollo	6,00	\$ 500.000,00
204	Fuego	Susceptible a incendios y altas temperaturas	Equipo AS400 Desarrollo	6,00	\$ 500.000,00
205	Fallo o interrupción del suministro principal	Fallo de los componentes	Equipo AS400 Desarrollo	5,67	\$ 120.000,00
206	Daños causados por un tercero	Falla de enlaces externos-terceros	Equipo AS400 Desarrollo	5,50	\$ 8.000,00
207	Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de recuperación	Equipo AS400 Desarrollo	5,00	\$ 80.000,00
208	Actividades no autorizadas	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Equipo AS400 Desarrollo	5,00	\$ 10.000,00
209	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	Equipo AS400 Desarrollo	6,00	\$ 30.000,00
210	Pérdida de recursos	Falta de precaución en las conexiones físicas	Equipo AS400 Desarrollo	6,00	\$ 8.000,00
211	Robo de identidad (Fraude de identidad / Cuenta)	Falta de política formal de cambio de credenciales	Equipo AS400 Desarrollo	5,00	\$ 8.000,00

	AMENAZA	VULNERABILIDAD	ACTIVO	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
212	Uso erróneo o administración de dispositivos y sistemas	Falta de políticas internas de gestión y cumplimiento	Equipo AS400 Desarrollo	5,00	\$ 8.000,00
213	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Equipo AS400 Desarrollo	10,00	\$ 8.000,00
214	Fallo de dispositivos o sistemas	Fallo de los componentes	Equipo AS400 Desarrollo	5,67	\$ 120.000,00
215	Manipulación de hardware y software	Uso inadecuado o descuido del control de acceso físico a edificios y habitaciones	Equipo AS400 Desarrollo	4,00	\$ 8.000,00
216	Fuego	Susceptible a incendios y altas temperaturas	Controladora wireless	6,00	\$ 60.000,00
217	Agua	Ubicación en un área susceptible a inundaciones.	Controladora wireless	6,00	\$ 60.000,00
218	Fallo o interrupción del suministro principal	Falla de equipos dependientes	Controladora wireless	6,00	\$ 5.000,00
219	Condiciones climáticas desfavorables	Fallo de los componentes	Controladora wireless	6,00	\$ 12.000,00
220	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Controladora wireless	6,00	\$ 2.000,00
221	Mal funcionamiento de los equipos (dispositivos o sistemas)	Falta de garantía técnica de los equipos	Controladora wireless	5,50	\$ 60.000,00
222	Uso erróneo o administración de dispositivos y sistemas	Falta de políticas internas de gestión y cumplimiento	Controladora wireless	5,00	\$ 2.000,00
223	Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de recuperación	Controladora wireless	10,00	\$ 5.000,00
224	Actividades no autorizadas	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Controladora wireless	9,00	\$ 2.000,00

	AMENAZA	VULNERABILIDAD	ACTIVO	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
225	Pérdida de recursos	Falta de precaución en las conexiones físicas	Controladora wireless	6,00	\$ 8.000,00
226	Robo de identidad (Fraude de identidad / Cuenta)	Falta de política formal de cambio de credenciales	Controladora wireless	9,00	\$ 2.000,00
227	Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de contingencia	Controladora wireless	6,00	\$ 5.000,00
228	Manipulación de hardware y software	Uso inadecuado o descuido del control de acceso físico a edificios y habitaciones	Controladora wireless	10,00	\$ 2.000,00
229	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	Controladora wireless	5,50	\$ 2.000,00
230	Fallo de dispositivos o sistemas	Fallo de los componentes	Controladora wireless	6,00	\$ 12.000,00
231	Fuego	Susceptible a incendios y altas temperaturas	Optimizador Wan	4,75	\$ 30.000,00
232	Agua	Ubicación en un área susceptible a inundaciones.	Optimizador Wan	4,75	\$ 30.000,00
233	Fallo o interrupción del suministro principal	Falla de equipos dependientes	Optimizador Wan	4,75	\$ 5.000,00
234	Condiciones climáticas desfavorables	Fallo de los componentes	Optimizador Wan	4,75	\$ 17.000,00
235	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Optimizador Wan	5,25	\$ 2.000,00
236	Pérdida de recursos	Falta de precaución en las conexiones físicas	Optimizador Wan	5,25	\$ 5.000,00
237	Manipulación de hardware y software	Uso inadecuado o descuido del control de acceso físico a edificios y habitaciones	Optimizador Wan	9,25	\$ 2.000,00
238	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	Optimizador Wan	4,75	\$ 2.000,00
239	Fallo de dispositivos o sistemas	Fallo de los componentes	Optimizador Wan	4,75	\$ 17.000,00
240	Fuego	Susceptible a incendios y altas temperaturas	Aires Acondicionados	4,50	\$ 40.000,00

	AMENAZA	VULNERABILIDAD	ACTIVO	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
241	Agua	Ubicación en un área susceptible a inundaciones.	Aires Acondicionados	4,50	\$ 40.000,00
242	Fallo o interrupción del suministro principal	Falla de equipos dependientes	Aires Acondicionados	4,50	\$ 5.000,00
243	Fallo de dispositivos o sistemas	Fallo de los componentes	Aires Acondicionados	4,50	\$ 15.000,00
244	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Aires Acondicionados	4,50	\$ 3.000,00
245	Fallo de dispositivos o sistemas	Falta de gestión en la disponibilidad de repuestos de equipos críticos	Aires Acondicionados	4,00	\$ 10.000,00
246	Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de contingencia	Aires Acondicionados	4,50	\$ 5.000,00
247	Fallo de dispositivos o sistemas	Falta de soporte preventivo y correctivo	Aires Acondicionados	4,50	\$ 7.000,00
248	Pérdida de recursos	Falta de precaución en las conexiones físicas	Aires Acondicionados	4,50	\$ 7.000,00
249	Fuego	Susceptible a incendios y altas temperaturas	UPS	5,25	\$ 20.000,00
250	Agua	Ubicación en un área susceptible a inundaciones.	UPS	5,25	\$ 20.000,00
251	Fallo o interrupción del suministro principal	Fallo de los componentes	UPS	5,25	\$ 12.000,00
252	Fallo de dispositivos o sistemas	Fallo de los componentes	UPS	5,25	\$ 12.000,00
253	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	UPS	5,25	\$ 3.000,00
254	Fallo de dispositivos o sistemas	Falta de gestión en la disponibilidad de repuestos de equipos críticos	UPS	4,75	\$ 7.000,00
255	Diseño y planificación inadecuados o	Falta de planes de contingencia	UPS	5,25	\$ 5.000,00

	AMENAZA	VULNERABILIDAD	ACTIVO	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
	adaptación inadecuada				
256	Fallo de dispositivos o sistemas	Falta de soporte preventivo y correctivo	UPS	5,25	\$ 7.000,00
257	Pérdida de recursos	Falta de precaución en las conexiones físicas	UPS	5,25	\$ 5.000,00
258	Condiciones climáticas desfavorables	Fallo de los componentes	Switch piso	5,50	\$ 15.000,00
259	Agua	Ubicación en un área susceptible a inundaciones.	Switch piso	5,50	\$ 10.000,00
260	Fuego	Susceptible a incendios y altas temperaturas	Switch piso	5,50	\$ 10.000,00
261	Fallo o interrupción del suministro principal	Fallo de los componentes	Switch piso	5,50	\$ 15.000,00
262	Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de recuperación	Switch piso	5,50	\$ 2.000,00
263	Actividades no autorizadas	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Switch piso	10,00	\$ 2.000,00
264	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	Switch piso	6,00	\$ 2.000,00
265	Pérdida de recursos	Falta de precaución en las conexiones físicas	Switch piso	6,00	\$ 5.000,00
266	Robo de identidad (Fraude de identidad / Cuenta)	Falta de política formal de cambio de credenciales	Switch piso	5,50	\$ 2.000,00
267	Uso erróneo o administración de dispositivos y sistemas	Falta de políticas internas de gestión y cumplimiento	Switch piso	5,50	\$ 2.000,00
268	Fallo de software /aplicaciones o servicio	Falta de planes de crecimiento y expansión de servicios de TI	Switch piso	5,50	\$ 5.000,00
269	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis,	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	Switch piso	5,00	\$ 10.000,00

	AMENAZA	VULNERABILIDAD	ACTIVO	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
	lluvias intensas, fuertes nevadas, vientos fuertes)				
270	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Switch piso	9,00	\$ 2.000,00
271	Acceso físico no autorizado / Entrada no autorizada a las instalaciones	Espacio físico designado no reúne condiciones técnicas	Switch piso	10,00	\$ 5.000,00
272	Fallo de dispositivos o sistemas	Fallo de los componentes	Switch piso	5,50	\$ 15.000,00
273	Manipulación de hardware y software	Uso inadecuado o descuido del control de acceso físico a edificios y habitaciones	Switch piso	10,00	\$ 2.000,00
274	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Sistema AS400 Médico	6,00	\$ 25.000,00
275	Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de contingencia	Sistema AS400 Médico	9,00	\$ 1.000.000,00
276	Diseño y planificación inadecuados o adaptación inadecuada	No posee alta disponibilidad	Sistema AS400 Médico	10,00	\$ 1.000.000,00
277	Negación de servicio	No cuenta con mecanismos contra ataques informáticos	Sistema AS400 Médico	5,50	\$ 100.000,00
278	Uso erróneo o administración de dispositivos y sistemas	Falta de documentación técnica	Sistema AS400 Médico	5,50	\$ 200.000,00
279	Mal funcionamiento de los equipos (dispositivos o sistemas)	No posee un procedimiento de respaldo	Sistema AS400 Médico	8,00	\$ 200.000,00
280	Fallo de software /aplicaciones o servicio	Falta de soporte preventivo y correctivo	QlikView	4,25	\$ 15.000,00
281	Diseño y planificación inadecuados o	No posee un procedimiento de respaldo	QlikView	5,25	\$ 10.000,00

	AMENAZA	VULNERABILIDAD	ACTIVO	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
	adaptación inadecuada				
282	Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de contingencia	Aplicativos Web Producción	10,00	\$ 100.000,00
283	Diseño y planificación inadecuados o adaptación inadecuada	No posee alta disponibilidad	Aplicativos Web Producción	6,25	\$ 200.000,00
284	Uso indebido de los sistemas de información / información (incluidas las aplicaciones móviles)	Mala gestión de contraseñas	Aplicativos Web Producción	9,00	\$ 10.000,00
285	Robo de identidad (Fraude de identidad / Cuenta)	Falta de política formal de cambio de credenciales	Aplicativos Web Producción	9,00	\$ 10.000,00
286	Código malicioso / software / actividad	No cuenta con mecanismos contra ataques informáticos	Página Web	3,50	\$ 5.000,00
287	Manipulación de hardware y software	Falta de política formal de cambio de credenciales	Página Web	7,50	\$ 5.000,00
288	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Software Firewall	7,75	\$ 7.000,00
289	Mal funcionamiento de los equipos (dispositivos o sistemas)	Falta de garantía técnica de los equipos	Software Firewall	5,75	\$ 8.000,00
290	Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de contingencia	Alfresco	3,75	\$ 10.000,00
291	Fallo de software /aplicaciones o servicio	Falta de soporte preventivo y correctivo	Alfresco	3,75	\$ 5.000,00
292	Diseño y planificación inadecuados o adaptación inadecuada	Falta de control efectivo del cambio	Alfresco	3,75	\$ 5.000,00

	AMENAZA	VULNERABILIDAD	ACTIVO	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
293	Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de contingencia	Biblioteca Virtual	3,00	\$ 10.000,00
294	Fallo de software /aplicaciones o servicio	Falta de soporte preventivo y correctivo	Biblioteca Virtual	3,00	\$ 5.000,00
295	Diseño y planificación inadecuados o adaptación inadecuada	Falta de control efectivo del cambio	Biblioteca Virtual	3,00	\$ 5.000,00
296	Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de contingencia	EVCAM	3,00	\$ 10.000,00
297	Fallo de software /aplicaciones o servicio	Falta de soporte preventivo y correctivo	EVCAM	3,00	\$ 5.000,00
298	Diseño y planificación inadecuados o adaptación inadecuada	Falta de control efectivo del cambio	EVCAM	3,00	\$ 5.000,00
299	Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de contingencia	Aplicativo de Facturación	10,00	\$ 10.000,00
300	Diseño y planificación inadecuados o adaptación inadecuada	No posee alta disponibilidad	Aplicativo de Facturación	9,00	\$ 10.000,00
301	Robo de identidad (Fraude de identidad / Cuenta)	Falta de política formal de cambio de credenciales	Aplicativo de Facturación	10,00	\$ 5.000,00
302	Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de contingencia	Base de datos postgres	6,00	\$ 10.000,00
303	Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de crecimiento y expansión de servicios de TI	Base de datos postgres	6,00	\$ 20.000,00

	AMENAZA	VULNERABILIDAD	ACTIVO	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
304	Mal funcionamiento de los equipos (dispositivos o sistemas)	Falta de planes de recuperación	Base de datos postgres	10,00	\$ 10.000,00

La Tabla IV-20 muestra las amenazas para cada una de las vulnerabilidades identificadas a los activos de la plataforma AS400 – IESS, que se han identificado y analizado en la las tareas de la actividad 4.

Tabla IV-20.- Tupla Amenazas – Vulnerabilidades con los valores y costo del daño de las vulnerabilidades para plataforma AS400-IESS

AMENAZA	VULNERABILIDAD	Valor del Daño Promedio de la Vulnerabilidad	Costo del Daño Total de la Vulnerabilidad
Acceso físico no autorizado / Entrada no autorizada a las instalaciones	Espacio físico designado no reúne condiciones técnicas	10,00	\$5.000,00
Actividades no autorizadas	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	7,65	\$ 58.000,00
Agua	Ubicación en un área susceptible a inundaciones.	5,33	\$ 2.451.000,00
Código malicioso / software / actividad	No cuenta con mecanismos contra ataques informáticos	3,50	\$ 5.000,00
Condiciones climáticas desfavorables	Fallo de los componentes	5,30	\$ 641.000,00
Daños causados por un tercero	Falla de enlaces externos-terceros	6,08	\$ 28.000,00
Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	5,00	\$ 10.000,00
Diseño y planificación inadecuados o adaptación inadecuada	Falta de control efectivo del cambio	3,25	\$ 15.000,00
Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de contingencia	6,05	\$ 1.165.000,00
Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de crecimiento y expansión de servicios de TI	6,00	\$ 20.000,00
Diseño y planificación inadecuados o adaptación inadecuada	Falta de planes de recuperación	6,62	\$ 356.000,00
Diseño y planificación inadecuados o adaptación inadecuada	No posee alta disponibilidad	8,42	\$ 1.210.000,00
Diseño y planificación inadecuados o adaptación inadecuada	No posee un procedimiento de respaldo	5,25	\$ 10.000,00

AMENAZA	VULNERABILIDAD	Valor del Daño Promedio de la Vulnerabilidad	Costo del Daño Total de la Vulnerabilidad
Fallo de dispositivos o sistemas	Fallo de los componentes	5,29	\$ 679.000,00
Fallo de dispositivos o sistemas	Falta de gestión en la disponibilidad de repuestos de equipos críticos	4,38	\$ 17.000,00
Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	6,93	\$ 126.000,00
Fallo de dispositivos o sistemas	Falta de soporte preventivo y correctivo	5,00	\$ 22.000,00
Fallo de software /aplicaciones o servicio	Falta de planes de crecimiento y expansión de servicios de TI	4,77	\$ 29.000,00
Fallo de software /aplicaciones o servicio	Falta de soporte preventivo y correctivo	3,50	\$ 30.000,00
Fallo o interrupción del suministro principal	Falla de equipos dependientes	4,55	\$ 79.000,00
Fallo o interrupción del suministro principal	Fallo de los componentes	6,11	\$ 536.000,00
Fuego	Susceptible a incendios y altas temperaturas	5,33	\$ 2.451.000,00
Mal funcionamiento de los equipos (dispositivos o sistemas)	Falta de garantía técnica de los equipos	5,17	\$ 193.000,00
Mal funcionamiento de los equipos (dispositivos o sistemas)	Falta de planes de recuperación	10,00	\$ 10.000,00
Mal funcionamiento de los equipos (dispositivos o sistemas)	No posee un procedimiento de respaldo	8,00	\$ 200.000,00
Manipulación de hardware y software	Falta de política formal de cambio de credenciales	7,50	\$ 5.000,00
Manipulación de hardware y software	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	8,57	\$ 58.000,00
Negación de servicio	No cuenta con mecanismos contra ataques informáticos	7,94	\$ 420.000,00
Pérdida de recursos	Falta de precaución en las conexiones físicas	5,23	\$ 173.000,00
Robo de identidad (Fraude de identidad / Cuenta)	Falta de política formal de cambio de credenciales	6,68	\$ 71.000,00
Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	6,84	\$ 96.000,00
Uso erróneo o administración de dispositivos y sistemas	Falta de documentación técnica	5,50	\$ 200.000,00
Uso erróneo o administración de dispositivos y sistemas	Falta de políticas internas de gestión y cumplimiento	5,13	\$ 56.000,00

AMENAZA	VULNERABILIDAD	Valor del Daño Promedio de la Vulnerabilidad	Costo del Daño Total de la Vulnerabilidad
Uso indebido de los sistemas de información / información (incluidas las aplicaciones móviles)	Mala gestión de contraseñas	9,00	\$ 10.000,00

La Tabla IV-21 muestra las amenazas identificadas que pueden afectar a los activos de la plataforma AS400-IESS.

Tabla IV-21.- Amenazas con los valores y costo del daño de la amenaza para plataforma AS400-IESS

AMENAZA	VALOR DEL DAÑO DE LA AMENAZA	COSTO DEL DAÑO DE LA AMENAZA
Acceso físico no autorizado / Entrada no autorizada a las instalaciones	10,00	\$ 5.000,00
Actividades no autorizadas	7,65	\$ 58.000,00
Agua	5,33	\$ 2.451.000,00
Código malicioso / software / actividad	3,50	\$ 5.000,00
Condiciones climáticas desfavorables	5,30	\$ 641.000,00
Daños causados por un tercero	6,08	\$ 28.000,00
Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	5,00	\$ 10.000,00
Diseño y planificación inadecuados o adaptación inadecuada	5,93	\$ 2.776.000,00
Fallo de dispositivos o sistemas	5,40	\$ 844.000,00
Fallo de software /aplicaciones o servicio	4,13	\$ 59.000,00
Fallo o interrupción del suministro principal	5,33	\$ 615.000,00
Fuego	5,33	\$ 2.451.000,00
Mal funcionamiento de los equipos (dispositivos o sistemas)	7,72	\$ 403.000,00
Manipulación de hardware y software	8,03	\$ 63.000,00
Negación de servicio	7,94	\$ 420.000,00
Pérdida de recursos	5,23	\$ 173.000,00
Robo de identidad (Fraude de identidad / Cuenta)	6,68	\$ 71.000,00
Uso erróneo o administración de dispositivos y sistemas	5,82	\$ 352.000,00
Uso indebido de los sistemas de información / información (incluidas las aplicaciones móviles)	9,00	\$ 10.000,00

IV.6.5. Actividad 5: Medición del Riesgo

La Figura IV-3 muestra la matriz de riesgos de la plataforma AS400-IESS, según los valores definidos en la Tabla IV-15.

AMENAZA	VALOR DEL DAÑO	FRECUENCIA	RIESGO	COSTO DEL DAÑO
Acceso físico no autorizado / Entrada no autorizada a las instalaciones	10	B	6	\$ 5.000,00
Actividades no autorizadas	8	B	5	\$ 58.000,00
Agua	5	M	3	\$ 2.451.000,00
Código malicioso / software / actividad	4	B	2	\$ 5.000,00
Condiciones climáticas desfavorables	5	M	3	\$ 641.000,00
Daños causados por un tercero	6	B	3	\$ 28.000,00
Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	5	B	2	\$ 10.000,00
Diseño y planificación inadecuados o adaptación inadecuada	6	MA	9	\$ 2.776.000,00
Fallo de dispositivos o sistemas	5	A	5	\$ 844.000,00
Fallo de software /aplicaciones o servicio	4	A	5	\$ 59.000,00
Fallo o interrupción del suministro principal	5	M	3	\$ 615.000,00
Fuego	5	B	2	\$ 2.451.000,00
Mal funcionamiento de los equipos (dispositivos o sistemas)	8	M	6	\$ 403.000,00
Manipulación de hardware y software	8	B	5	\$ 63.000,00
Negación de servicio	8	M	6	\$ 420.000,00
Pérdida de recursos	5	B	2	\$ 173.000,00
Robo de identidad (Fraude de identidad / Cuenta)	7	B	3	\$ 71.000,00
Uso erróneo o administración de dispositivos y sistemas	6	A	6	\$ 352.000,00
Uso indebido de los sistemas de información / información (incluidas las aplicaciones móviles)	9	M	7	\$ 10.000,00

Figura IV-3. Matriz de riesgos AS400-IESS

IV.6.6. Actividad 6: Contramedidas

La Tabla IV-22 muestra las contramedidas que han sido identificadas para las vulnerabilidades encontradas en los activos de la plataforma AS400 – IESS.

Tabla IV-22. Contramedidas para las vulnerabilidades AS400-IESS

VULNERABILIDAD	CONTRAMEDIDA
Espacio físico designado no reúne condiciones técnicas	Adecuación de espacios físicos según las necesidades tecnológicas de los activos
Falla de enlaces externos-terceros	Implementar enlaces externos alternos con terceros
Falla de equipos dependientes	Contratos de soporte y mantenimiento en vigencia
Fallo de los componentes	Contratos de soporte y mantenimiento en vigencia
Falta de capacitación en la administración del activo	Capacitación continua en la administración del activo
Falta de control efectivo del cambio	Implementar controles de calidad de los activos
Falta de documentación técnica	Establecer políticas de gestión de los documentos técnicos de los activos
Falta de garantía técnica de los equipos	Contrato de garantía en vigencia
Falta de gestión en la disponibilidad de repuestos de equipos críticos	Establecer convenios con los proveedores para provisión de repuestos críticos de los activos
Falta de mantenimiento y/o actualizaciones	Contratos de mantenimiento y actualizaciones vigente

VULNERABILIDAD	CONTRAMEDIDA
Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Establecer lineamientos de gestión de identificación y autenticación de usuarios para el acceso a los activos de la organización
Falta de planes de contingencia	Generar plan de contingencia por activo
Falta de planes de crecimiento y expansión de servicios de TI	Implementar una Arquitectura Empresarial
Falta de planes de recuperación	Implementar Plan de Recuperación por cada Sistema
Falta de política formal de cambio de credenciales	Política de gestión de credenciales
Falta de políticas internas de gestión y cumplimiento	Concientización de las políticas internas de la organización
Falta de precaución en las conexiones físicas	Mejora de las conexiones físicas de los activos
Falta de soporte preventivo y correctivo	Contratos de soporte y mantenimiento en vigencia
Mala gestión de contraseñas	Proceso adecuado de gestión de contraseñas
No cuenta con mecanismos contra ataques informáticos	Implementar medidas que repelan los ataques informáticos hacia los activos de la organización
No posee alta disponibilidad	Implementar sistemas alternos para garantizar la continuidad del funcionamiento de los activos
No posee un procedimiento de respaldo	Establecer lineamientos de respaldo de los activos
Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	Instalaciones sísmo resistentes (resistente a movimientos telúricos)
Susceptible a incendios y altas temperaturas	Sistema contra incendios y ventilación adecuada
Ubicación en un área susceptible a inundaciones.	Mejora física de las instalaciones, drenajes adecuados
Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Mejora en los accesos físicos al edificio y habitación

IV.6.6.1 Gráfica de radar de las amenazas por activo

En esta sección se muestra los valores de los riesgos de las amenazas identificadas, con los valores actuales, el valor objetivo que como organización se desea tener y el valor permisible y controlable de los mismos.

- Valor actual: promedio de todos los riesgos.
- Valor objetivo: recomendación de la SDNSI de reducción de riesgo (al menos el 50%).
- Valor límite: Valor dado por condiciones gráficas, al que nunca se debería llegar.

Tabla IV-23. Valores de riesgos de las amenazas AS400-IESS

AMENAZA	ACTUAL	OBJETIVO	LÍMITE
Acceso físico no autorizado / Entrada no autorizada a las instalaciones	6,00	3,00	7
Actividades no autorizadas	5,00	2,50	7
Agua	3,00	1,50	7
Código malicioso / software / actividad	1,00	0,50	7

<i>AMENAZA</i>	<i>ACTUAL</i>	<i>OBJETIVO</i>	<i>LIMITE</i>
Condiciones climáticas desfavorables	3,00	1,50	7
Daños causados por un tercero	3,00	1,50	7
Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	2,00	1,00	7
Diseño y planificación inadecuados o adaptación inadecuada	9,00	4,50	7
Fallo de dispositivos o sistemas	6,00	3,00	7
Fallo de software /aplicaciones o servicio	5,00	2,50	7
Fallo o interrupción del suministro principal	3,00	1,50	7
Fuego	2,00	1,00	7
Mal funcionamiento de los equipos (dispositivos o sistemas)	6,00	3,00	7
Manipulación de hardware y software	5,00	2,50	7
Negación de servicio	6,00	3,00	7
Pérdida de recursos	2,00	1,00	7
Robo de identidad (Fraude de identidad / Cuenta)	3,00	1,50	7
Uso erróneo o administración de dispositivos y sistemas	6,00	3,00	7
Uso indebido de los sistemas de información / información (incluidas las aplicaciones móviles)	7,00	3,50	7

La Figura IV-4 muestra los valores identificados de los riesgos actuales, valor del riesgo objetivo y los riesgos que la organización permite a una amenaza.

Figura IV-4. Riesgos por amenazas AS400-IESS

IV.7. Análisis de Riesgos de la Plataforma Host – IESS

La Figura IV-5 muestra el diagrama de dependencias de activos de la plataforma Host – IESS.

Figura IV-5. Diagrama de dependencia de equipos de HOST – IESS

La valoración de los activos se ha realizado con personal técnico de la plataforma Host, Ing. Paúl Galarraga, Tecnólogo. Marco García y Tecnólogo Alberto Andrade.

IV.7.1. Actividad 1: Lanzamiento

En esta actividad se define un catálogo de los elementos que participan en el modelo conceptual. Para ello, se han definido las taxonomías de estos elementos, se define la taxonomía de tipos de activos de la organización enfocados en ciberseguridad en base al estándar ISO 27005 (Standard, 2011), la taxonomía de Vulnerabilidades en ciberseguridad en base al estándar ISO 27005

(Standard, 2011), y se establece la taxonomía de Amenazas en ciberseguridad en base al estándar ENISA 2016 (Marinos, 2016) Actividad 1: Identificar Activos – Vulnerabilidades

IV.7.2. Actividad 2: Identificar y evaluar Activos

En esta actividad se identifica los activos de ciberseguridad, determinar el costo del activo y la medición del impacto que tiene el activo en cada una de las dimensiones de seguridad.

La Tabla IV-24 muestra la valoración de la criticidad de los activos de la plataforma Host-IESS, medidos a partir de las dimensiones de seguridad de la información.

Tabla IV-24. Costo e impacto en las dimensiones de seguridad de los activos de la plataforma Host-IESS.

IDENTIFICACIÓN DE ACTIVOS										
#	Tipo Activo	Activo	Costo del Activo	Confidencialidad		Integridad		Disponibilidad		Criticidad
1	Hardware	Main-Frame Z10BC	\$ 30.000,00	7	Media	6	Media	10	Alta	10
2	Hardware	UNIDAD DE CARTUCHOS	\$ 10.000,00	7	Media	7	Media	6	Media	7
3	Hardware	UNIDAD DE CARTUCHOS 1	\$ 10.000,00	5	Media	7	Media	6	Media	7
4	Hardware	ALMACENAMIENTO	\$ 500.000,00	6	Media	7	Media	10	Alta	10
5	Hardware	SERVIDOR HMC	\$ 2.000,00	7	Media	6	Media	6	Media	7
6	Hardware	AIRE DE PRESION	\$ 25.000,00	6	Media	6	Media	9	Alta	9
7	Hardware	AIRE TIPO MOCHILA	\$ 8.000,00	5	Media	6	Media	3	Baja	6
8	Hardware	UPS	\$ 30.000,00	7	Media	6	Media	8	Alta	8
9	Hardware	SERVIDOR UNIX	\$ 4.000,00	6	Media	7	Media	8	Alta	8
10	Hardware	SERVER VTAPE	\$ 2.000,00	5	Media	7	Media	2	Baja	7
11	Hardware	SWITCH DE PASO	\$ 1.000,00	5	Media	7	Media	8	Alta	8
12	Software	Aplicativos alojados en el sistema HOST	\$ 100.000,00	6	Media	2	Baja	9	Alta	9

IV.7.3. Actividad 3: Evaluar el nivel de daño para las tuplas Vulnerabilidad – Activo (dimensión)

En esta actividad se ha determinado el daño de las vulnerabilidades en cada uno de los activos de la organización previamente identificados. La organización ha determinado el valor del daño de la vulnerabilidad en cada una de las dimensiones (confidencialidad, integridad, disponibilidad y criticidad) del activo, para ello hay que identificar las vulnerabilidades de los activos de la plataforma Host -IESS.

La Tabla IV-25 muestra las vulnerabilidades que se han identificado a los activos de la plataforma Host-IESS. Incluye el valor del daño en las dimensiones de seguridad y costo del daño de las vulnerabilidades de la plataforma HOST – IESS.

Tabla IV-25. Tuplas Vulnerabilidades - Activos, valor y costo del daño de las vulnerabilidades de la plataforma Host-IESS

				DIMENSION				VULNERABILIDAD	
	VULNERABILIDAD	ACTIVO	Costo del Activo	Daño Confiabilidad	Daño Integridad	Daño Disponibilidad	Daño Criticidad	Valor del Daño	Costo del Daño
1	Susceptible a incendios y altas temperaturas	Main-Frame Z10BC	\$ 300.000,00	2	5	10	10	6,75	\$ 300.000,00
2	Ubicación en un área susceptible a inundaciones.	Main-Frame Z10BC		2	5	10	10	6,75	\$ 300.000,00
3	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	Main-Frame Z10BC		2	10	10	10	8,00	\$ 300.000,00
4	Falta de soporte preventivo y correctivo	Main-Frame Z10BC		5	5	5	10	6,25	\$ 120.000,00
5	Falta de capacitación en la administración del activo	Main-Frame Z10BC		5	5	5	10	6,25	\$ 150.000,00
6	Falta de garantía técnica de los equipos	Main-Frame Z10BC		5	10	10	10	8,75	\$ 150.000,00
7	Fallo de los componentes	Main-Frame Z10BC		5	5	10	10	7,50	\$ 90.000,00
8	Falta de soporte preventivo y correctivo	UNIDAD DE CARTUCHOS	\$ 10.000,00	2	5	5	7	4,75	\$ 5.000,00
9	Ubicación en un área susceptible a inundaciones.	UNIDAD DE CARTUCHOS		2	5	5	7	4,75	\$ 10.000,00
10	Susceptible a incendios y altas temperaturas	UNIDAD DE CARTUCHOS		1	10	10	7	7,00	\$ 10.000,00
11	Fallo de los componentes	UNIDAD DE CARTUCHOS		2	10	10	7	7,25	\$ 5.000,00
12	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	UNIDAD DE CARTUCHOS		1	10	10	7	7,00	\$ 10.000,00
13	Falta de capacitación en la administración del activo	UNIDAD DE CARTUCHOS		2	5	5	7	4,75	\$ 3.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confiabilidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Críticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
14	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	UNIDAD DE CARTUCHOS		5	10	10	7	8,00	\$ 10.000,00
15	Falta de planes de contingencia	UNIDAD DE CARTUCHOS		5	10	10	7	8,00	\$ 10.000,00
16	Falta de mantenimiento y/o actualizaciones	UNIDAD DE CARTUCHOS		5	10	10	7	8,00	\$ 10.000,00
17	Falta de precaución en las conexiones físicas	UNIDAD DE CARTUCHOS		2	10	10	7	7,25	\$ 4.000,00
18	No posee mecanismo de respaldo	UNIDAD DE CARTUCHOS		2	10	10	7	7,25	\$ 10.000,00
19	Falta de soporte preventivo y correctivo	UNIDAD DE CARTUCHOS 1	\$ 10.000,00	2	5	5	7	4,75	\$ 5.000,00
20	Ubicación en un área susceptible a inundaciones.	UNIDAD DE CARTUCHOS 1		2	5	5	7	4,75	\$ 10.000,00
21	Susceptible a incendios y altas temperaturas	UNIDAD DE CARTUCHOS 1		1	10	10	7	7,00	\$ 10.000,00
22	Fallo de los componentes	UNIDAD DE CARTUCHOS 1		2	10	10	7	7,25	\$ 5.000,00
23	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	UNIDAD DE CARTUCHOS 1		1	10	10	7	7,00	\$ 10.000,00
24	Falta de capacitación en la administración del activo	UNIDAD DE CARTUCHOS 1		2	5	5	7	4,75	\$ 3.000,00
25	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	UNIDAD DE CARTUCHOS 1		5	10	10	7	8,00	\$ 10.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confiabilidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Críticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
26	Falta de planes de contingencia	UNIDAD DE CARTUCHOS 1		5	10	10	7	8,00	\$ 10.000,00
27	Falta de mantenimiento y/o actualizaciones	UNIDAD DE CARTUCHOS 1		5	10	10	7	8,00	\$ 10.000,00
28	Falta de precaución en las conexiones físicas	UNIDAD DE CARTUCHOS 1		2	10	10	7	7,25	\$ 4.000,00
29	No posee mecanismo de respaldo	UNIDAD DE CARTUCHOS 1		2	10	10	7	7,25	\$ 10.000,00
30	Falta de soporte preventivo y correctivo	ALMACENAMIENTO	\$ 500.000,00	2	10	10	10	8,00	\$ 250.000,00
31	Ubicación en un área susceptible a inundaciones.	ALMACENAMIENTO		2	10	10	10	8,00	\$ 500.000,00
32	Susceptible a incendios y altas temperaturas	ALMACENAMIENTO		2	10	10	10	8,00	\$ 500.000,00
33	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	ALMACENAMIENTO		1	10	10	10	7,75	\$ 500.000,00
34	Falta de capacitación en la administración del activo	ALMACENAMIENTO		5	5	10	10	7,50	\$ 500.000,00
35	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	ALMACENAMIENTO		2	10	10	10	8,00	\$ 500.000,00
36	Falta de planes de contingencia	ALMACENAMIENTO		5	5	10	10	7,50	\$ 500.000,00
37	Fallo de los componentes	ALMACENAMIENTO		5	10	10	10	8,75	\$ 200.000,00
38	Falta de mantenimiento y/o actualizaciones	ALMACENAMIENTO		5	10	10	10	8,75	\$ 500.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confiabilidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Críticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
39	Falta de precaución en las conexiones físicas	ALMACENAMIENTO		2	5	10	10	6,75	\$ 200.000,00
40	Falta de soporte preventivo y correctivo	SERVIDOR HMC	\$ 2.000,00	1	3	3	7	3,50	\$ 1.000,00
41	Ubicación en un área susceptible a inundaciones.	SERVIDOR HMC		1	5	10	7	5,75	\$ 2.000,00
42	Susceptible a incendios y altas temperaturas	SERVIDOR HMC		1	10	10	7	7,00	\$ 2.000,00
43	Fallo de los componentes	SERVIDOR HMC		1	10	10	7	7,00	\$ 800,00
44	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	SERVIDOR HMC		1	10	10	7	7,00	\$ 2.000,00
45	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	SERVIDOR HMC		5	10	10	7	8,00	\$ 2.000,00
46	Falta de precaución en las conexiones físicas	SERVIDOR HMC		2	5	5	7	4,75	\$ 800,00
47	Fallo de los componentes	AIRE DE PRESICION	\$ 25.000,00	2	10	10	9	7,75	\$ 12.500,00
48	Ubicación en un área susceptible a inundaciones.	AIRE DE PRESICION		2	10	10	9	7,75	\$ 25.000,00
49	Susceptible a incendios y altas temperaturas	AIRE DE PRESICION		2	10	10	9	7,75	\$ 25.000,00
50	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	AIRE DE PRESICION		1	10	10	9	7,50	\$ 25.000,00
51	Falta de capacitación en la administración del activo	AIRE DE PRESICION		2	5	5	9	5,25	\$ 10.000,00
52	Falta de precaución en las conexiones físicas	AIRE DE PRESICION		2	5	10	9	6,50	\$ 10.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confiabilidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Críticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
53	Fallo de los componentes	AIRE TIPO MOCHILA	\$ 8.000,00	2	10	10	6	7,00	\$ 4.000,00
54	Ubicación en un área susceptible a inundaciones.	AIRE TIPO MOCHILA		2	10	10	6	7,00	\$ 8.000,00
55	Susceptible a incendios y altas temperaturas	AIRE TIPO MOCHILA		2	10	10	6	7,00	\$ 8.000,00
56	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	AIRE TIPO MOCHILA		1	10	10	6	6,75	\$ 8.000,00
57	Falta de mantenimiento y/o actualizaciones	AIRE TIPO MOCHILA		2	5	10	6	5,75	\$ 4.000,00
58	Falta de precaución en las conexiones físicas	AIRE TIPO MOCHILA		2	5	10	6	5,75	\$ 3.200,00
59	Falta de soporte preventivo y correctivo	UPS	\$ 30.000,00	2	10	10	8	7,50	\$ 15.000,00
60	Ubicación en un área susceptible a inundaciones.	UPS		2	5	10	8	6,25	\$ 30.000,00
61	Susceptible a incendios y altas temperaturas	UPS		2	10	10	8	7,50	\$ 30.000,00
62	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	UPS		1	10	10	8	7,25	\$ 30.000,00
63	Falta de capacitación en la administración del activo	UPS		2	10	10	8	7,50	\$ 12.000,00
64	Falta de mantenimiento y/o actualizaciones	UPS		2	10	10	8	7,50	\$ 15.000,00
65	Falta de precaución en las conexiones físicas	UPS		2	5	10	8	6,25	\$ 12.000,00
66	Falta de soporte preventivo y correctivo	SERVIDOR UNIX	\$ 4.000,00	2	10	10	8	7,50	\$ 2.000,00
67	Ubicación en un área susceptible a inundaciones.	SERVIDOR UNIX		2	10	10	8	7,50	\$ 4.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confiabilidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Críticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
68	Susceptible a incendios y altas temperaturas	SERVIDOR UNIX		2	10	10	8	7,50	\$ 4.000,00
69	Fallo de los componentes	SERVIDOR UNIX		1	10	10	8	7,25	\$ 2.000,00
70	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	SERVIDOR UNIX		1	10	10	8	7,25	\$ 4.000,00
71	Falta de capacitación en la administración del activo	SERVIDOR UNIX		2	5	10	8	6,25	\$ 2.000,00
72	Falta de planes de contingencia	SERVIDOR UNIX		2	5	5	8	5,00	\$ 2.000,00
73	Mala gestión de contraseñas	SERVIDOR UNIX		1	5	10	8	6,00	\$ 2.000,00
74	Falta de mantenimiento y/o actualizaciones	SERVIDOR UNIX		2	10	10	8	7,50	\$ 2.000,00
75	Falta de precaución en las conexiones físicas	SERVIDOR UNIX		2	5	10	8	6,25	\$ 1.600,00
76	Falta de política formal de cambio de credenciales	SERVIDOR UNIX		2	5	10	8	6,25	\$ 3.000,00
77	Falta de soporte preventivo y correctivo	SERVER VTAPE	\$ 2.000,00	2	5	10	7	6,00	\$ 1.000,00
78	Ubicación en un área susceptible a inundaciones.	SERVER VTAPE		2	10	10	7	7,25	\$ 2.000,00
79	Susceptible a incendios y altas temperaturas	SERVER VTAPE		2	10	10	7	7,25	\$ 2.000,00
80	Fallo de los componentes	SERVER VTAPE		2	10	10	7	7,25	\$ 1.000,00
81	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	SERVER VTAPE		1	10	10	7	7,00	\$ 2.000,00
82	Falta de capacitación en la administración del activo	SERVER VTAPE		2	5	10	7	6,00	\$ 2.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confiabilidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Críticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
83	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	SERVER VTAPE		2	10	10	7	7,25	\$ 2.000,00
84	Falta de planes de contingencia	SERVER VTAPE		2	5	5	7	4,75	\$ 1.000,00
85	Mala gestión de contraseñas	SERVER VTAPE		2	5	10	7	6,00	\$ 1.000,00
86	Falta de mantenimiento y/o actualizaciones	SERVER VTAPE		2	10	10	7	7,25	\$ 1.000,00
87	Falta de precaución en las conexiones físicas	SERVER VTAPE		2	5	10	7	6,00	\$ 1.000,00
88	Falta de soporte preventivo y correctivo	SWITCH DE PASO	\$ 1.000,00	2	10	10	8	7,50	\$ 500,00
89	Ubicación en un área susceptible a inundaciones.	SWITCH DE PASO		2	10	10	8	7,50	\$ 1.000,00
90	Susceptible a incendios y altas temperaturas	SWITCH DE PASO		2	10	10	8	7,50	\$ 1.000,00
91	Fallo de los componentes	SWITCH DE PASO		2	10	10	8	7,50	\$ 500,00
92	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	SWITCH DE PASO		1	10	10	8	7,25	\$ 1.000,00
93	Falta de capacitación en la administración del activo	SWITCH DE PASO		2	5	10	8	6,25	\$ 200,00
94	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	SWITCH DE PASO		2	10	10	8	7,50	\$ 1.000,00
95	Falta de precaución en las conexiones físicas	SWITCH DE PASO		2	5	10	8	6,25	\$ 1.000,00
96	Inexistente ambiente de pruebas	Aplicativos alojados en el sistema HOST	\$ 100.000,00	2	5	5	9	5,25	\$ 200,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confiabilidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Críticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
97	Falta de capacitación en la administración del activo	Aplicativos alojados en el sistema HOST		2	10	10	9	7,75	\$ 2.200,00
98	Mala gestión de contraseñas	Aplicativos alojados en el sistema HOST		10	10	5	9	8,50	\$ 1.000,00
99	Errores conocidos en el software.	Aplicativos alojados en el sistema HOST		5	10	3	9	6,75	\$ 200,00

IV.7.4. Actividad 4: Identificación de Amenazas de ciberseguridad

En esta actividad se identifican las amenazas para cada una de las vulnerabilidades asociadas a los activos de ciberseguridad, como se muestra en la Tabla IV-26.

Tabla IV-26 Tripleta Amenazas – Vulnerabilidades -Activos con el valor y costo del daño de la Amenaza de la plataforma Host - IESS

	AMENAZAS	VULNERABILIDAD	ACTIVOS	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
1	Fuego	Susceptible a incendios y altas temperaturas	Main-Frame Z10BC	6,75	\$ 300.000,00
2	Agua	Ubicación en un área susceptible a inundaciones.	Main-Frame Z10BC	6,75	\$ 300.000,00
3	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	Main-Frame Z10BC	8,00	\$ 300.000,00
4	Fallo o interrupción del suministro principal	Falta de soporte preventivo y correctivo	Main-Frame Z10BC	6,25	\$ 120.000,00
5	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Main-Frame Z10BC	6,25	\$ 150.000,00
6	Fallo de dispositivos o sistemas	Falta de garantía técnica de los equipos	Main-Frame Z10BC	8,75	\$ 150.000,00
7	Fallo de dispositivos o sistemas	Fallo de los componentes	Main-Frame Z10BC	7,50	\$ 90.000,00
8	Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	UNIDAD DE CARTUCHOS	4,75	\$ 5.000,00
9	Agua	Ubicación en un área susceptible a inundaciones.	UNIDAD DE CARTUCHOS	4,75	\$ 10.000,00
10	Fuego	Susceptible a incendios y altas temperaturas	UNIDAD DE CARTUCHOS	7,00	\$ 10.000,00
11	Fallo o interrupción del suministro principal	Fallo de los componentes	UNIDAD DE CARTUCHOS	7,25	\$ 5.000,00
12	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	UNIDAD DE CARTUCHOS	7,00	\$ 10.000,00

	AMENAZAS	VULNERABILIDAD	ACTIVOS	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
13	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	UNIDAD DE CARTUCHOS	4,75	\$ 3.000,00
14	Robo (dispositivos, medios de almacenamiento y documentos)	Uso inadecuado o descuido del control de acceso físico a edificios y habitaciones	UNIDAD DE CARTUCHOS	8,00	\$ 10.000,00
15	Fallo de dispositivos o sistemas	Falta de planes de contingencia	UNIDAD DE CARTUCHOS	8,00	\$ 10.000,00
16	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	UNIDAD DE CARTUCHOS	8,00	\$ 10.000,00
17	Pérdida de recursos	Falta de precaución en las conexiones físicas	UNIDAD DE CARTUCHOS	7,25	\$ 4.000,00
18	Diseño y planificación inadecuados o adaptación inadecuada	No posee mecanismo de respaldo	UNIDAD DE CARTUCHOS	7,25	\$ 10.000,00
19	Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	UNIDAD DE CARTUCHOS 1	4,75	\$ 5.000,00
20	Agua	Ubicación en un área susceptible a inundaciones.	UNIDAD DE CARTUCHOS 1	4,75	\$ 10.000,00
21	Fuego	Susceptible a incendios y altas temperaturas	UNIDAD DE CARTUCHOS 1	7,00	\$ 10.000,00
22	Fallo o interrupción del suministro principal	Fallo de los componentes	UNIDAD DE CARTUCHOS 1	7,25	\$ 5.000,00
23	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	UNIDAD DE CARTUCHOS 1	7,00	\$ 10.000,00
24	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	UNIDAD DE CARTUCHOS 1	4,75	\$ 3.000,00
25	Robo (dispositivos, medios de almacenamiento y documentos)	Uso inadecuado o descuido del control de acceso físico a edificios y habitaciones	UNIDAD DE CARTUCHOS 1	8,00	\$ 10.000,00
26	Fallo de dispositivos o sistemas	Falta de planes de contingencia	UNIDAD DE CARTUCHOS 1	8,00	\$ 10.000,00
27	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	UNIDAD DE CARTUCHOS 1	8,00	\$ 10.000,00

	AMENAZAS	VULNERABILIDAD	ACTIVOS	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
28	Pérdida de recursos	Falta de precaución en las conexiones físicas	UNIDAD DE CARTUCHOS 1	7,25	\$ 4.000,00
29	Diseño y planificación inadecuados o adaptación inadecuada	No posee mecanismo de respaldo	UNIDAD DE CARTUCHOS 1	7,25	\$ 10.000,00
30	Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	ALMACENAMIENT O	8,00	\$ 250.000,00
31	Agua	Ubicación en un área susceptible a inundaciones.	ALMACENAMIENT O	8,00	\$ 500.000,00
32	Fuego	Susceptible a incendios y altas temperaturas	ALMACENAMIENT O	8,00	\$ 500.000,00
33	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	ALMACENAMIENT O	7,75	\$ 500.000,00
34	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	ALMACENAMIENT O	7,50	\$ 500.000,00
35	Robo (dispositivos, medios de almacenamiento y documentos)	Uso inadecuado o descuido del control de acceso físico a edificios y habitaciones	ALMACENAMIENT O	8,00	\$ 500.000,00
36	Fallo de dispositivos o sistemas	Falta de planes de contingencia	ALMACENAMIENT O	7,50	\$ 500.000,00
37	Fallo de dispositivos o sistemas	Fallo de los componentes	ALMACENAMIENT O	8,75	\$ 200.000,00
38	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	ALMACENAMIENT O	8,75	\$ 500.000,00
39	Pérdida de recursos	Falta de precaución en las conexiones físicas	ALMACENAMIENT O	6,75	\$ 200.000,00
40	Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	SERVIDOR HMC	3,50	\$ 1.000,00
41	Agua	Ubicación en un área susceptible a inundaciones.	SERVIDOR HMC	5,75	\$ 2.000,00
42	Fuego	Susceptible a incendios y altas temperaturas	SERVIDOR HMC	7,00	\$ 2.000,00
43	Fallo o interrupción del suministro principal	Fallo de los componentes	SERVIDOR HMC	7,00	\$ 800,00

	AMENAZAS	VULNERABILIDAD	ACTIVOS	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
44	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	SERVIDOR HMC	7,00	\$ 2.000,00
45	Robo (dispositivos, medios de almacenamiento y documentos)	Uso inadecuado o descuido del control de acceso físico a edificios y habitaciones	SERVIDOR HMC	8,00	\$ 2.000,00
46	Pérdida de recursos	Falta de precaución en las conexiones físicas	SERVIDOR HMC	4,75	\$ 800,00
47	Condiciones climáticas desfavorables	Fallo de los componentes	AIRE DE PRESICION	7,75	\$ 12.500,00
48	Agua	Ubicación en un área susceptible a inundaciones.	AIRE DE PRESICION	7,75	\$ 25.000,00
49	Fuego	Susceptible a incendios y altas temperaturas	AIRE DE PRESICION	7,75	\$ 25.000,00
50	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	AIRE DE PRESICION	7,50	\$ 25.000,00
51	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	AIRE DE PRESICION	5,25	\$ 10.000,00
52	Pérdida de recursos	Falta de precaución en las conexiones físicas	AIRE DE PRESICION	6,50	\$ 10.000,00
53	Condiciones climáticas desfavorables	Fallo de los componentes	AIRE TIPO MOCHILA	7,00	\$ 4.000,00
54	Agua	Ubicación en un área susceptible a inundaciones.	AIRE TIPO MOCHILA	7,00	\$ 8.000,00
55	Fuego	Susceptible a incendios y altas temperaturas	AIRE TIPO MOCHILA	7,00	\$ 8.000,00
56	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	AIRE TIPO MOCHILA	6,75	\$ 8.000,00

	AMENAZAS	VULNERABILIDAD	ACTIVOS	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
57	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	AIRE TIPO MOCHILA	5,75	\$ 4.000,00
58	Pérdida de recursos	Falta de precaución en las conexiones físicas	AIRE TIPO MOCHILA	5,75	\$ 3.200,00
59	Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	UPS	7,50	\$ 15.000,00
60	Agua	Ubicación en un área susceptible a inundaciones.	UPS	6,25	\$ 30.000,00
61	Fuego	Susceptible a incendios y altas temperaturas	UPS	7,50	\$ 30.000,00
62	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	UPS	7,25	\$ 30.000,00
63	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	UPS	7,50	\$ 12.000,00
64	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	UPS	7,50	\$ 15.000,00
65	Pérdida de recursos	Falta de precaución en las conexiones físicas	UPS	6,25	\$ 12.000,00
66	Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	SERVIDOR UNIX	7,50	\$ 2.000,00
67	Agua	Ubicación en un área susceptible a inundaciones.	SERVIDOR UNIX	7,50	\$ 4.000,00
68	Fuego	Susceptible a incendios y altas temperaturas	SERVIDOR UNIX	7,50	\$ 4.000,00
69	Fallo o interrupción del suministro principal	Fallo de los componentes	SERVIDOR UNIX	7,25	\$ 2.000,00
70	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	SERVIDOR UNIX	7,25	\$ 4.000,00
71	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	SERVIDOR UNIX	6,25	\$ 2.000,00

	AMENAZAS	VULNERABILIDAD	ACTIVOS	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
72	Fallo de dispositivos o sistemas	Falta de planes de contingencia	SERVIDOR UNIX	5,00	\$ 2.000,00
73	Actividades no autorizadas	Mala gestión de contraseñas	SERVIDOR UNIX	6,00	\$ 2.000,00
74	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	SERVIDOR UNIX	7,50	\$ 2.000,00
75	Pérdida de recursos	Falta de precaución en las conexiones físicas	SERVIDOR UNIX	6,25	\$ 1.600,00
76	Actividades no autorizadas	Falta de política formal de cambio de credenciales	SERVIDOR UNIX	6,25	\$ 3.000,00
77	Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	SERVER VTAPE	6,00	\$ 1.000,00
78	Agua	Ubicación en un área susceptible a inundaciones.	SERVER VTAPE	7,25	\$ 2.000,00
79	Fuego	Susceptible a incendios y altas temperaturas	SERVER VTAPE	7,25	\$ 2.000,00
80	Fallo o interrupción del suministro principal	Fallo de los componentes	SERVER VTAPE	7,25	\$ 1.000,00
81	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	SERVER VTAPE	7,00	\$ 2.000,00
82	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	SERVER VTAPE	6,00	\$ 2.000,00
83	Robo (dispositivos, medios de almacenamiento y documentos)	Uso inadecuado o descuido del control de acceso físico a edificios y habitaciones	SERVER VTAPE	7,25	\$ 2.000,00
84	Fallo de dispositivos o sistemas	Falta de planes de contingencia	SERVER VTAPE	4,75	\$ 1.000,00
85	Actividades no autorizadas	Mala gestión de contraseñas	SERVER VTAPE	6,00	\$ 1.000,00
86	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	SERVER VTAPE	7,25	\$ 1.000,00
87	Pérdida de recursos	Falta de precaución en las conexiones físicas	SERVER VTAPE	6,00	\$ 1.000,00

	AMENAZAS	VULNERABILIDAD	ACTIVOS	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
88	Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	SWITCH DE PASO	7,50	\$ 500,00
89	Agua	Ubicación en un área susceptible a inundaciones.	SWITCH DE PASO	7,50	\$ 1.000,00
90	Fuego	Susceptible a incendios y altas temperaturas	SWITCH DE PASO	7,50	\$ 1.000,00
91	Fallo o interrupción del suministro principal	Fallo de los componentes	SWITCH DE PASO	7,50	\$ 500,00
92	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	SWITCH DE PASO	7,25	\$ 1.000,00
93	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	SWITCH DE PASO	6,25	\$ 200,00
94	Robo (dispositivos, medios de almacenamiento y documentos)	Uso inadecuado o descuido del control de acceso físico a edificios y habitaciones	SWITCH DE PASO	7,50	\$ 1.000,00
95	Pérdida de recursos	Falta de precaución en las conexiones físicas	SWITCH DE PASO	6,25	\$ 1.000,00
96	Fallo de software /aplicaciones o servicio	Inexistente ambiente de pruebas	Aplicativos alojados en el sistema HOST	5,25	\$ 200,00
97	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Aplicativos alojados en el sistema HOST	7,75	\$ 2.200,00
98	Actividades no autorizadas	Mala gestión de contraseñas	Aplicativos alojados en el sistema HOST	8,50	\$ 1.000,00
99	Fallo de software /aplicaciones o servicio	Errores conocidos en el software.	Aplicativos alojados en el sistema HOST	6,75	\$ 200,00

La Tabla IV-27 muestra las amenazas identificadas para cada una de las vulnerabilidades de los activos de la plataforma Host-IESS, que se han identificado y analizado en la las tareas de la actividad 4

Tabla IV-27. Tuplas Amenazas – Vulnerabilidades con los valores y costo del daño de las vulnerabilidades para la plataforma Host-IESS

AMENAZA	VULNERABILIDAD	Valor del Daño Promedio de la Vulnerabilidad	Costo del Daño Total de la Vulnerabilidad
Actividades no autorizadas	Falta de política formal de cambio de credenciales	6,25	\$ 3.000,00
Actividades no autorizadas	Mala gestión de contraseñas	6,83	\$ 4.000,00
Actividades no autorizadas	Mala gestión de contraseñas	6,83	\$ 4.000,00
Agua	Ubicación en un área susceptible a inundaciones.	6,66	\$ 892.000,00
Condiciones climáticas desfavorables	Fallo de los componentes	7,38	\$ 16.500,00
Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	6,19	\$ 279.500,00
Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	7,25	\$ 892.000,00
Diseño y planificación inadecuados o adaptación inadecuada	No posee mecanismo de respaldo	7,25	\$ 20.000,00
Fallo de dispositivos o sistemas	Fallo de los componentes	8,13	\$ 290.000,00
Fallo de dispositivos o sistemas	Falta de garantía técnica de los equipos	8,75	\$ 150.000,00
Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	7,54	\$ 542.000,00
Fallo de dispositivos o sistemas	Falta de planes de contingencia	6,65	\$ 523.000,00
Fallo de software /aplicaciones o servicio	Errores conocidos en el software.	6,75	\$ 200,00
Fallo de software /aplicaciones o servicio	Inexistente ambiente de pruebas	5,25	\$ 200,00
Fallo o interrupción del suministro principal	Fallo de los componentes	7,25	\$ 14.300,00
Fallo o interrupción del suministro principal	Falta de soporte preventivo y correctivo	6,25	\$ 120.000,00
Fuego	Susceptible a incendios y altas temperaturas	7,30	\$ 892.000,00
Pérdida de recursos	Falta de precaución en las conexiones físicas	6,30	\$ 237.600,00

AMENAZA	VULNERABILIDAD	Valor del Daño Promedio de la Vulnerabilidad	Costo del Daño Total de la Vulnerabilidad
Robo (dispositivos, medios de almacenamiento y documentos)	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	7,79	\$ 525.000,00
Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	6,23	\$ 684.400,00

La Tabla IV-28 muestra las amenazas identificadas que pueden afectar a los activos de la plataforma Host-IESS.

Tabla IV-28.- Amenazas con los valores y costo del daño de la amenaza para la plataforma Host -IESS

AMENAZA	VALOR DEL DAÑO DE LA AMENAZA	COSTO DEL DAÑO DE LA AMENAZA
Actividades no autorizadas	6,64	\$ 11.000,00
Agua	6,66	\$ 892.000,00
Condiciones climáticas desfavorables	6,78	\$ 296.000,00
Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	7,25	\$ 892.000,00
Diseño y planificación inadecuados o adaptación inadecuada	7,25	\$ 20.000,00
Fallo de dispositivos o sistemas	7,77	\$ 1.505.000,00
Fallo de software /aplicaciones o servicio	6,00	\$ 400,00
Fallo o interrupción del suministro principal	6,75	\$ 134.300,00
Fuego	7,30	\$ 892.000,00
Pérdida de recursos	6,30	\$ 237.600,00
Robo (dispositivos, medios de almacenamiento y documentos)	7,79	\$ 525.000,00
Uso erróneo o administración de dispositivos y sistemas	6,23	\$ 684.400,00

IV.7.5. Actividad 5: Medición del Riesgo

La Figura IV-6 muestra la matriz de riesgos identificada para la plataforma Host-IESS.

AMENAZA	VALOR DEL DAÑO	FRECUENCIA	RIESGO	COSTO DEL DAÑO
Actividades no autorizadas	7,00	M	5	\$ 11.000,00
Agua	7,00	B	3	\$ 892.000,00
Condiciones climáticas desfavorables	7,00	B	3	\$ 296.000,00
Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	7,00	B	3	\$ 892.000,00
Diseño y planificación inadecuados o adaptación inadecuada	7,00	MA	9	\$ 20.000,00
Fallo de dispositivos o sistemas	8,00	A	8	\$ 1.505.000,00
Fallo de software /aplicaciones o servicio	6,00	B	3	\$ 400,00
Fallo o interrupción del suministro principal	7,00	M	5	\$ 134.300,00
Fuego	7,00	B	3	\$ 892.000,00
Pérdida de recursos	6,00	B	3	\$ 237.600,00
Robo (dispositivos, medios de almacenamiento y documentos)	8,00	B	5	\$ 525.000,00
Uso erróneo o administración de dispositivos y sistemas	6,00	B	3	\$ 684.400,00

Figura IV-6. Matriz de riesgos Host-IESS

IV.7.6. Actividad 6: Contramedidas

La Tabla IV-29 muestra las contramedidas que se pueden aplicar a las vulnerabilidades presentes en los activos de la plataforma Host-IESS.

Tabla IV-29. Contramedidas para las vulnerabilidades plataforma Host-IESS

VULNERABILIDAD	CONTRAMEDIDA
Errores conocidos en el software.	Control de calidad de los sistemas de software
Fallo de los componentes	Contratos de soporte y mantenimiento en vigencia
Falta de capacitación en la administración del activo	Capacitación continua en la administración del activo
Falta de garantía técnica de los equipos	Contrato de garantía en vigencia
Falta de mantenimiento y/o actualizaciones	Contratos de mantenimiento y actualizaciones vigente
Falta de planes de contingencia	Generar plan de contingencia por activo
Falta de política formal de cambio de credenciales	Política de gestión de credenciales
Falta de precaución en las conexiones físicas	Mejora de las conexiones físicas de los activos
Falta de soporte preventivo y correctivo	Contratos de soporte y mantenimiento en vigencia
Inexistente ambiente de pruebas	Implementar ambiente de pruebas para los aplicativos de Software
Mala gestión de contraseñas	Proceso adecuado de gestión de contraseñas
No posee mecanismo de respaldo	Disponer de un dispositivo de respaldo para el activo
Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	Instalaciones sismo-resistentes
Susceptible a incendios y altas temperaturas	Sistema contra incendios y ventilación adecuada
Ubicación en un área susceptible a inundaciones.	Mejora física de las instalaciones, drenajes adecuados
Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Mejora en los accesos físicos al edificio y habitación

IV.7.6.1 Gráfica de radar de los riesgos por amenaza

En esta sección se muestra los valores de los riesgos de las amenazas identificadas, con los valores actuales, el valor objetivo que como organización se desea tener, y valor permisible y controlable de los mismos.

- Valor actual: promedio de todos los riesgos.
- Valor objetivo: recomendación de la SDNSI de reducción de riesgo (al menos el 50%).
- Valor límite: valor dado por condiciones gráficas, al que nunca se debería llegar.

Tabla IV-30 Valores de riesgos de las amenazas Host-IESS

AMENAZA	ACTUAL	OBJETIVO	LIMITE
Actividades no autorizadas	5	2,50	7
Agua	3	1,50	7
Condiciones climáticas desfavorables	3	1,50	7
Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	3	1,50	7
Diseño y planificación inadecuados o adaptación inadecuada	9	4,50	7
Fallo de dispositivos o sistemas	8	4,00	7
Fallo de software /aplicaciones o servicio	3	1,50	7
Fallo o interrupción del suministro principal	5	2,50	7
Fuego	3	1,50	7
Pérdida de recursos	3	1,50	7
Robo (dispositivos, medios de almacenamiento y documentos)	5	2,50	7
Uso erróneo o administración de dispositivos y sistemas	3	1,50	7

La Figura IV-7 muestra los riesgos identificados con los valores actuales, objetivos y permitidos por la organización.

Figura IV-7. Riesgos por amenazas Host-IESS

IV.8. Análisis y Gestión de Riesgos Plataforma Oracle - IESS

La Figura IV-8 muestra la dependencia de activos de la plataforma Oracle.

Figura IV-8. Diagrama de dependencia de equipos de la Plataforma Oracle-IESS

La dependencia directa de los equipos de la Plataforma Oracle se establece con los equipos Power 770, Power 780 en los que se encuentran instaladas los diferentes hosts de la base de datos, tal y como se muestra en la Figura II-7.

La valoración de los activos se ha realizado con personal técnico de la Plataforma Oracle, Ingeniera Paulina Gallo encargada del licenciamiento de la base de datos Oracle y con el ingeniero Marcelo Vásquez encargado del área de Plataforma de Servidores.

IV.8.1. Actividad 1: Lanzamiento

En esta actividad se define un catálogo de los elementos que participan en el modelo conceptual. Para ello, se han definido las taxonomías de estos elementos, que fueron descritos en el capítulo 2 de esta tesis doctoral, se define la taxonomía de tipos de activos de la organización enfocados en ciberseguridad en base al estándar ISO 27005, la taxonomía de Vulnerabilidades en ciberseguridad en base al estándar ISO 27005, y se establece la taxonomía de Amenazas en ciberseguridad en base al estándar ENISA 2016 Actividad 1: Identificar Activos – Vulnerabilidades.

IV.8.2. Actividad 2: Identificar y evaluar Activos

En esta actividad se identifica los activos de ciberseguridad, determinar el costo del activo y la medición del impacto que tiene el activo en cada una de las dimensiones de seguridad. La Tabla IV-31 muestra la criticidad de los activos de la plataforma Oracle-IESS.

Tabla IV-31. Costo e impacto en las dimensiones de seguridad de los activos de la plataforma Oracle-IESS

IDENTIFICACIÓN DE ACTIVOS										
#	Tipo Activo	Activo	Costo del Activo	Confidencialidad		Integridad		Disponibilidad		Criticidad
1	Hardware	Power 770 (prosrvuiorac1 BDD, prosrvuiorac2 BDD)	\$ 250.000,00	7	Media	7	Media	10	Alta	10
2	Hardware	Power 770 (prosrvuiorac3 BDD, prosrvuiorac4 BDD)	\$ 250.000,00	6	Media	7	Media	9	Alta	9
3	Hardware	Power 770 (prosrvuiorac BDD)	\$ 250.000,00	7	Media	6	Media	8	Alta	8
4	Hardware	Power 780 (Srvuiodbpen BDD, SOA, desarrollo, calidad)	\$ 300.000,00	6	Media	6	Media	9	Alta	9
5	Software	Licencias de oracle	\$ 300.000,00	10	Alta	10	Alta	10	Alta	10

IV.8.3. Actividad 3: Evaluar el nivel de daño para las tuplas Vulnerabilidad – Activo (dimensión)

En esta actividad se ha determinado el daño de las vulnerabilidades en cada uno de los activos de la organización previamente identificados. La organización ha determinado el valor del daño de la vulnerabilidad en cada una de las dimensiones (confidencialidad, integridad, disponibilidad y criticidad) del activo, para ello hay que identificar las vulnerabilidades de los activos de la plataforma Oracle.

La Tabla IV-32 muestra la valoración del impacto en los activos según el valor del daño en las dimensiones de seguridad de la información de la plataforma Oracle, así como el costo del daño de las vulnerabilidades identificadas al activo.

Tabla IV-32. Tuplas Vulnerabilidades - Activos, valor y costo del daño de las vulnerabilidades de la plataforma Oracle-IESS

			DIMENSION					VULNERABILIDAD	
			Costo del Activo	Daño Confidencialidad	Daño Integridad	Daño Disponibilidad	Daño Criticidad	Valor del Daño	Costo del Daño
1	Fallo de los componentes	Power 770 (prosrvuiorac1 BDD, prosrvuiorac2 BDD)	\$ 250.000,00	2	5	10	10	6,75	\$ 125.000,00
2	Ubicación en un área susceptible a inundaciones.	Power 770 (prosrvuiorac1 BDD, prosrvuiorac2 BDD)		2	5	10	10	6,75	\$ 250.000,00
3	Susceptible a incendios y altas temperaturas	Power 770 (prosrvuiorac1 BDD, prosrvuiorac2 BDD)		2	10	10	10	8,00	\$ 250.000,00
4	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	Power 770 (prosrvuiorac1 BDD, prosrvuiorac2 BDD)		2	10	10	10	8,00	\$ 125.000,00
5	Falta de capacitación en la administración del activo	Power 770 (prosrvuiorac1 BDD, prosrvuiorac2 BDD)		2	2	5	10	4,75	\$ 75.000,00
6	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Power 770 (prosrvuiorac1 BDD, prosrvuiorac2 BDD)		2	10	10	10	8,00	\$ 150.000,00
7	Falta de planes de contingencia	Power 770 (prosrvuiorac1 BDD, prosrvuiorac2 BDD)		2	5	10	10	6,75	\$ 150.000,00
8	Mala gestión de contraseñas	Power 770 (prosrvuiorac1 BDD, prosrvuiorac2 BDD)		7	7	10	10	8,50	\$ 75.000,00
9	Falta de mantenimiento y/o actualizaciones	Power 770 (prosrvuiorac1 BDD, prosrvuiorac2 BDD)		2	7	5	10	6,00	\$ 150.000,00
10	Falta de precaución en las conexiones físicas	Power 770 (prosrvuiorac1 BDD, prosrvuiorac2 BDD)		2	5	10	10	6,75	\$ 150.000,00
11	Falta de política formal de cambio de credenciales	Power 770 (prosrvuiorac1 BDD, prosrvuiorac2 BDD)		1	2	7	10	5,00	\$ 75.000,00

			<i>DIMENSION</i>					<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confidencialidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Criticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
12	Fallo de los componentes	Power 770 (prosrvuiorac3 BDD, prosrvuiorac4 BDD)	\$ 250.000,00	2	5	10	9	6,50	\$ 125.000,00
13	Ubicación en un área susceptible a inundaciones.	Power 770 (prosrvuiorac3 BDD, prosrvuiorac4 BDD)		2	5	10	9	6,50	\$ 250.000,00
14	Susceptible a incendios y altas temperaturas	Power 770 (prosrvuiorac3 BDD, prosrvuiorac4 BDD)		2	10	10	9	7,75	\$ 250.000,00
15	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	Power 770 (prosrvuiorac3 BDD, prosrvuiorac4 BDD)		2	10	10	9	7,75	\$ 125.000,00
16	Falta de capacitación en la administración del activo	Power 770 (prosrvuiorac3 BDD, prosrvuiorac4 BDD)		2	2	5	9	4,50	\$ 75.000,00
17	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Power 770 (prosrvuiorac3 BDD, prosrvuiorac4 BDD)		2	10	10	9	7,75	\$ 150.000,00
18	Falta de planes de contingencia	Power 770 (prosrvuiorac3 BDD, prosrvuiorac4 BDD)		2	5	10	9	6,50	\$ 150.000,00
19	Mala gestión de contraseñas	Power 770 (prosrvuiorac3 BDD, prosrvuiorac4 BDD)		7	7	10	9	8,25	\$ 75.000,00
20	Falta de mantenimiento y/o actualizaciones	Power 770 (prosrvuiorac3 BDD, prosrvuiorac4 BDD)		2	7	5	9	5,75	\$ 150.000,00
21	Falta de precaución en las conexiones físicas	Power 770 (prosrvuiorac3 BDD, prosrvuiorac4 BDD)		2	5	10	9	6,50	\$ 150.000,00
22	Falta de política formal de cambio de credenciales	Power 770 (prosrvuiorac3 BDD, prosrvuiorac4 BDD)		1	2	7	9	4,75	\$ 75.000,00

			<i>DIMENSION</i>					<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confidencialidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Criticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
23	Fallo de los componentes	Power 770 (prosrviuorac BDD)	\$ 250.000,00	2	5	10	8	6,25	\$ 125.000,00
24	Ubicación en un área susceptible a inundaciones.	Power 770 (prosrviuorac BDD)		2	5	10	8	6,25	\$ 250.000,00
25	Susceptible a incendios y altas temperaturas	Power 770 (prosrviuorac BDD)		2	10	10	8	7,50	\$ 250.000,00
26	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	Power 770 (prosrviuorac BDD)		2	10	10	8	7,50	\$ 125.000,00
27	Falta de capacitación en la administración del activo	Power 770 (prosrviuorac BDD)		2	2	5	8	4,25	\$ 75.000,00
28	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Power 770 (prosrviuorac BDD)		2	10	10	8	7,50	\$ 150.000,00
29	Falta de planes de contingencia	Power 770 (prosrviuorac BDD)		2	5	10	8	6,25	\$ 150.000,00
30	Mala gestión de contraseñas	Power 770 (prosrviuorac BDD)		7	7	10	8	8,00	\$ 75.000,00
31	Falta de mantenimiento y/o actualizaciones	Power 770 (prosrviuorac BDD)		2	7	5	8	5,50	\$ 150.000,00
32	Falta de precaución en las conexiones físicas	Power 770 (prosrviuorac BDD)		2	5	10	8	6,25	\$ 150.000,00
33	Falta de política formal de cambio de credenciales	Power 770 (prosrviuorac BDD)		1	2	7	8	4,50	\$ 75.000,00

			<i>DIMENSION</i>					<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confidencialidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Criticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
34	Fallo de los componentes	Power 780 (Srvuiodbpen BDD, SOA, desarrollo, calidad)	\$ 300.000,00	2	5	10	9	6,50	\$ 150.000,00
35	Ubicación en un área susceptible a inundaciones.	Power 780 (Srvuiodbpen BDD, SOA, desarrollo, calidad)		2	5	10	9	6,50	\$ 300.000,00
36	Susceptible a incendios y altas temperaturas	Power 780 (Srvuiodbpen BDD, SOA, desarrollo, calidad)		2	10	10	9	7,75	\$ 300.000,00
37	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	Power 780 (Srvuiodbpen BDD, SOA, desarrollo, calidad)		2	10	10	9	7,75	\$ 150.000,00
38	Falta de capacitación en la administración del activo	Power 780 (Srvuiodbpen BDD, SOA, desarrollo, calidad)		2	2	5	9	4,50	\$ 85.000,00
39	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Power 780 (Srvuiodbpen BDD, SOA, desarrollo, calidad)		2	10	10	9	7,75	\$ 180.000,00
40	Falta de planes de contingencia	Power 780 (Srvuiodbpen BDD, SOA, desarrollo, calidad)		2	5	10	9	6,50	\$ 180.000,00
41	Mala gestión de contraseñas	Power 780 (Srvuiodbpen BDD, SOA, desarrollo, calidad)		7	7	10	9	8,25	\$ 85.000,00

			DIMENSION					VULNERABILIDAD	
	VULNERABILIDAD	ACTIVO	Costo del Activo	Daño Confidencialidad	Daño Integridad	Daño Disponibilidad	Daño Criticidad	Valor del Daño	Costo del Daño
42	Falta de mantenimiento y/o actualizaciones	Power 780 (Srvuiodbpen BDD, SOA, desarrollo, calidad)		2	7	5	9	5,75	\$ 180.000,00
43	Falta de precaución en las conexiones físicas	Power 780 (Srvuiodbpen BDD, SOA, desarrollo, calidad)		2	5	10	9	6,50	\$ 180.000,00
44	Falta de política formal de cambio de credenciales	Power 780 (Srvuiodbpen BDD, SOA, desarrollo, calidad)		1	2	7	9	4,75	\$ 85.000,00
45	Falta de licenciamiento vigente	Licencias Oracle	\$ 300.000,00	1	3	10	10	6,00	\$ 300.000,00
46	Presenta errores lógicos el software	Licencias Oracle		2	3	4	10	4,75	\$ 100.000,00
47	Obsolescencia del Software	Licencias Oracle		1	3	6	10	5,00	\$ 200.000,00

IV.8.4. Actividad 4: Identificación de Amenazas de ciberseguridad

En esta actividad se identifican las amenazas para cada una de las vulnerabilidades asociadas a los activos de ciberseguridad, como se muestra en la Tabla IV-33.

Tabla IV-33. Tripleta Amenazas – Vulnerabilidades -Activos con el valor y costo del daño de la Amenaza para la plataforma Oracle-IESS

	AMENAZAS	VULNERABILIDAD	ACTIVOS	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
1	Condiciones climáticas desfavorables	Fallo de los componentes	Power 770 (prosrvuiorac1 BDD, prosrvuiorac2 BDD)	6,75	\$ 125.000,00
2	Agua	Ubicación en un área susceptible a inundaciones.	Power 770 (prosrvuiorac1 BDD, prosrvuiorac2 BDD)	6,75	\$ 250.000,00
3	Fuego	Susceptible a incendios y altas temperaturas	Power 770 (prosrvuiorac1 BDD, prosrvuiorac2 BDD)	8,00	\$ 250.000,00
4	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	Power 770 (prosrvuiorac1 BDD, prosrvuiorac2 BDD)	8,00	\$ 125.000,00
5	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Power 770 (prosrvuiorac1 BDD, prosrvuiorac2 BDD)	4,75	\$ 75.000,00
6	Robo (dispositivos, medios de almacenamiento y documentos)	Uso inadecuado o descuido del control de acceso físico a edificios y habitaciones	Power 770 (prosrvuiorac1 BDD, prosrvuiorac2 BDD)	8,00	\$ 150.000,00
7	Fallo de dispositivos o sistemas	Falta de planes de contingencia	Power 770 (prosrvuiorac1 BDD, prosrvuiorac2 BDD)	6,75	\$ 150.000,00
8	Actividades no autorizadas	Mala gestión de contraseñas	Power 770 (prosrvuiorac1 BDD, prosrvuiorac2 BDD)	8,50	\$ 75.000,00
9	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	Power 770 (prosrvuiorac1 BDD, prosrvuiorac2 BDD)	6,00	\$ 150.000,00
10	Pérdida de recursos	Falta de precaución en las conexiones físicas	Power 770 (prosrvuiorac1 BDD, prosrvuiorac2 BDD)	6,75	\$ 150.000,00
11	Actividades no autorizadas	Falta de política formal de cambio de credenciales	Power 770 (prosrvuiorac1 BDD, prosrvuiorac2 BDD)	5,00	\$ 75.000,00
12	Condiciones climáticas desfavorables	Fallo de los componentes	Power 770 (prosrvuiorac3 BDD, prosrvuiorac4 BDD)	6,50	\$ 125.000,00

	AMENAZAS	VULNERABILIDAD	ACTIVOS	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
13	Agua	Ubicación en un área susceptible a inundaciones.	Power 770 (prosrviuorac3 BDD, prosrviuorac4 BDD)	6,50	\$ 250.000,00
14	Fuego	Susceptible a incendios y altas temperaturas	Power 770 (prosrviuorac3 BDD, prosrviuorac4 BDD)	7,75	\$ 250.000,00
15	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	Power 770 (prosrviuorac3 BDD, prosrviuorac4 BDD)	7,75	\$ 125.000,00
16	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Power 770 (prosrviuorac3 BDD, prosrviuorac4 BDD)	4,50	\$ 75.000,00
17	Robo (dispositivos, medios de almacenamiento y documentos)	Uso inadecuado o descuido del control de acceso físico a edificios y habitaciones	Power 770 (prosrviuorac3 BDD, prosrviuorac4 BDD)	7,75	\$ 150.000,00
18	Fallo de dispositivos o sistemas	Falta de planes de contingencia	Power 770 (prosrviuorac3 BDD, prosrviuorac4 BDD)	6,50	\$ 150.000,00
19	Actividades no autorizadas	Mala gestión de contraseñas	Power 770 (prosrviuorac3 BDD, prosrviuorac4 BDD)	8,25	\$ 75.000,00
20	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	Power 770 (prosrviuorac3 BDD, prosrviuorac4 BDD)	5,75	\$ 150.000,00
21	Pérdida de recursos	Falta de precaución en las conexiones físicas	Power 770 (prosrviuorac3 BDD, prosrviuorac4 BDD)	6,50	\$ 150.000,00
22	Actividades no autorizadas	Falta de política formal de cambio de credenciales	Power 770 (prosrviuorac3 BDD, prosrviuorac4 BDD)	4,75	\$ 75.000,00
23	Condiciones climáticas desfavorables	Fallo de los componentes	Power 770 (prosrviuorac BDD)	6,25	\$ 125.000,00
24	Agua	Ubicación en un área susceptible a inundaciones.	Power 770 (prosrviuorac BDD)	6,25	\$ 250.000,00
25	Fuego	Susceptible a incendios y altas temperaturas	Power 770 (prosrviuorac BDD)	7,50	\$ 250.000,00
26	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	Power 770 (prosrviuorac BDD)	7,50	\$ 125.000,00

	AMENAZAS	VULNERABILIDAD	ACTIVOS	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
27	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Power 770 (prosrviuorac BDD)	4,25	\$ 75.000,00
28	Robo (dispositivos, medios de almacenamiento y documentos)	Uso inadecuado o descuido del control de acceso físico a edificios y habitaciones	Power 770 (prosrviuorac BDD)	7,50	\$ 150.000,00
29	Fallo de dispositivos o sistemas	Falta de planes de contingencia	Power 770 (prosrviuorac BDD)	6,25	\$ 150.000,00
30	Actividades no autorizadas	Mala gestión de contraseñas	Power 770 (prosrviuorac BDD)	8,00	\$ 75.000,00
31	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	Power 770 (prosrviuorac BDD)	5,50	\$ 150.000,00
32	Pérdida de recursos	Falta de precaución en las conexiones físicas	Power 770 (prosrviuorac BDD)	6,25	\$ 150.000,00
33	Actividades no autorizadas	Falta de política formal de cambio de credenciales	Power 770 (prosrviuorac BDD)	4,50	\$ 75.000,00
34	Condiciones climáticas desfavorables	Fallo de los componentes	Power 780 (Srvuiodbpen BDD, SOA, desarrollo, calidad)	6,50	\$ 150.000,00
35	Agua	Ubicación en un área susceptible a inundaciones.	Power 780 (Srvuiodbpen BDD, SOA, desarrollo, calidad)	6,50	\$ 300.000,00
36	Fuego	Susceptible a incendios y altas temperaturas	Power 780 (Srvuiodbpen BDD, SOA, desarrollo, calidad)	7,75	\$ 300.000,00
37	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	Power 780 (Srvuiodbpen BDD, SOA, desarrollo, calidad)	7,75	\$ 150.000,00
38	Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	Power 780 (Srvuiodbpen BDD, SOA, desarrollo, calidad)	4,50	\$ 85.000,00
39	Robo (dispositivos, medios de almacenamiento y documentos)	Uso inadecuado o descuido del control de acceso físico a edificios y habitaciones	Power 780 (Srvuiodbpen BDD, SOA, desarrollo, calidad)	7,75	\$ 180.000,00
40	Fallo de dispositivos o sistemas	Falta de planes de contingencia	Power 780 (Srvuiodbpen BDD, SOA, desarrollo, calidad)	6,50	\$ 180.000,00

	AMENAZAS	VULNERABILIDAD	ACTIVOS	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
41	Actividades no autorizadas	Mala gestión de contraseñas	Power 780 (Srvuiodbpén BDD, SOA, desarrollo, calidad)	8,25	\$ 85.000,00
42	Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	Power 780 (Srvuiodbpén BDD, SOA, desarrollo, calidad)	5,75	\$ 180.000,00
43	Pérdida de recursos	Falta de precaución en las conexiones físicas	Power 780 (Srvuiodbpén BDD, SOA, desarrollo, calidad)	6,50	\$ 180.000,00
44	Actividades no autorizadas	Falta de política formal de cambio de credenciales	Power 780 (Srvuiodbpén BDD, SOA, desarrollo, calidad)	4,75	\$ 85.000,00
45	Fallo de software /aplicaciones o servicio	Falta de licenciamiento vigente	Licencias Oracle	6,00	\$ 300.000,00
46	Fallo de software /aplicaciones o servicio	Presenta errores lógicos el software	Licencias Oracle	4,75	\$ 100.000,00
47	Fallo de software /aplicaciones o servicio	Obsolescencia del Software	Licencias Oracle	5,00	\$ 200.000,00

La Tabla IV-34 muestra las amenazas identificadas para cada vulnerabilidad de los activos de ciberseguridad, que se han identificado y analizado en la las tareas de la actividad 4

Tabla IV-34. Tupla Amenazas – Vulnerabilidades con los valores y costo del daño de las vulnerabilidades para plataforma Oracle-IESS

AMENAZA	VULNERABILIDAD	Valor del Daño Promedio de la Vulnerabilidad	Costo del Daño Total de la Vulnerabilidad
Actividades no autorizadas	Falta de política formal de cambio de credenciales	4,75	\$ 310.000,00
Actividades no autorizadas	Mala gestión de contraseñas	8,25	\$ 310.000,00
Agua	Ubicación en un área susceptible a inundaciones.	6,50	\$ 1.050.000,00
Condiciones climáticas desfavorables	Fallo de los componentes	6,50	\$ 525.000,00
Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	7,75	\$ 525.000,00
Fallo de dispositivos o sistemas	Falta de mantenimiento y/o actualizaciones	5,75	\$ 630.000,00
Fallo de dispositivos o sistemas	Falta de planes de contingencia	6,50	\$ 630.000,00

AMENAZA	VULNERABILIDAD	Valor del Daño Promedio de la Vulnerabilidad	Costo del Daño Total de la Vulnerabilidad
Fallo de software /aplicaciones o servicio	Falta de licenciamiento vigente	6,00	\$ 300.000,00
Fallo de software /aplicaciones o servicio	Obsolescencia del Software	5,00	\$ 200.000,00
Fallo de software /aplicaciones o servicio	Presenta errores lógicos el software	4,75	\$ 100.000,00
Fuego	Susceptible a incendios y altas temperaturas	7,75	\$ 1.050.000,00
Pérdida de recursos	Falta de precaución en las conexiones físicas	6,50	\$ 630.000,00
Robo (dispositivos, medios de almacenamiento y documentos)	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	7,75	\$ 630.000,00
Uso erróneo o administración de dispositivos y sistemas	Falta de capacitación en la administración del activo	4,50	\$ 310.000,00

La Tabla IV-35 muestra las amenazas identificadas que pueden afectar a los activos de la plataforma Oracle.

Tabla IV-35.- Amenazas con los valores y costo del daño de la amenaza para Oracle-IESS

AMENAZAS	VALOR DEL DAÑO DE LA AMENAZA	COSTO DEL DAÑO DE LA AMENAZA
Actividades no autorizadas	6,50	\$ 620.000,00
Agua	6,50	\$1.050.000,00
Condiciones climáticas desfavorables	6,50	\$ 525.000,00
Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	7,75	\$ 525.000,00
Fallo de dispositivos o sistemas	6,13	\$1.260.000,00
Fallo de software /aplicaciones o servicio	5,25	\$ 600.000,00
Fuego	7,75	\$1.050.000,00
Pérdida de recursos	6,50	\$ 630.000,00
Robo (dispositivos, medios de almacenamiento y documentos)	7,75	\$ 630.000,00
Uso erróneo o administración de dispositivos y sistemas	4,50	\$ 310.000,00

IV.8.5. Actividad 5: Medición del Riesgo

La Figura IV-9 muestra la matriz de riesgos de la plataforma Oracle.

AMENAZAS	VALOR DEL DAÑO	FRECUENCIA	RIESGO	COSTO DEL DAÑO
Actividades no autorizadas	7,00	M	5	\$ 620.000,00
Agua	7,00	B	3	\$ 1.050.000,00
Condiciones climáticas desfavorables	7,00	B	3	\$ 525.000,00
Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	8,00	B	5	\$ 525.000,00
Fallo de dispositivos o sistemas	6,00	A	6	\$ 1.260.000,00
Fallo de software /aplicaciones o servicio	5,00	A	5	\$ 600.000,00
Fuego	8,00	B	5	\$ 1.050.000,00
Pérdida de recursos	7,00	B	3	\$ 630.000,00
Robo (dispositivos, medios de almacenamiento y documentos)	8,00	B	5	\$ 630.000,00
Uso erróneo o administración de dispositivos y sistemas	5,00	B	2	\$ 310.000,00

Figura IV-9. Matriz de riesgos de la plataforma Oracle-IESS

IV.8.6. Actividad 6: Contramedidas

La Tabla IV-36 muestra las contramedidas que se han identificado a las vulnerabilidades presentes en los activos de ciberseguridad.

Tabla IV-36. Contramedidas para las vulnerabilidades de la plataforma Oracle-IESS

VULNERABILIDAD	CONTRAMEDIDA
Fallo de los componentes	Contratos de soporte y mantenimiento en vigencia
Falta de capacitación en la administración del activo	Capacitación continua en la administración del activo
Falta de licenciamiento vigente	Contratos de mantenimiento y actualizaciones vigente
Falta de mantenimiento y/o actualizaciones	Contratos de mantenimiento y actualizaciones vigente
Falta de planes de contingencia	Generar plan de contingencia por activo
Falta de política formal de cambio de credenciales	Política de gestión de credenciales
Falta de precaución en las conexiones físicas	Mejora de las conexiones físicas de los activos
Mala gestión de contraseñas	Proceso adecuado de gestión de contraseñas
Obsolescencia del Software	Implementar una Arquitectura Empresarial
Presenta errores lógicos el software	Contrato de garantía en vigencia
Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	Instalaciones sismo-resistentes
Susceptible a incendios y altas temperaturas	Sistema contra incendios y ventilación adecuada
Ubicación en un área susceptible a inundaciones.	Mejora física de las instalaciones, drenajes adecuados
Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	Mejora en los accesos físicos al edificio y habitación

IV.8.6.1 Gráfica de radar de los riesgos por amenaza

En esta sección se muestra los valores de los riesgos de las amenazas identificadas, con los valores actuales, el valor objetivo que como organización se desea tener, y valor permisible y controlable de los mismos.

- Valor actual: promedio de todos los riesgos.
- Valor objetivo: recomendación de la SDNSI de reducción de riesgo (al menos el 50%).
- Valor límite: valor dado por condiciones gráficas, al que nunca se debería llegar.

Tabla IV-37. Valores de riesgos de las amenazas de la plataforma Oracle-IESS

AMENAZA	ACTUAL	OBJETIVO	LIMITE
Actividades no autorizadas	5,00	2,50	7
Agua	3,00	1,50	7
Condiciones climáticas desfavorables	3,00	1,50	7
Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	5,00	2,50	7
Fallo de dispositivos o sistemas	6,00	3,00	7
Fallo de software /aplicaciones o servicio	5,00	2,50	7
Fuego	5,00	2,50	7
Pérdida de recursos	3,00	1,50	7
Robo (dispositivos, medios de almacenamiento y documentos)	5,00	2,50	7
Uso erróneo o administración de dispositivos y sistemas	2,00	1,00	7

La Figura IV-10 muestra los riesgos identificados en la plataforma Oracle-IESS, con los valores actuales, objetivos y permitidos por la organización.

Figura IV-10. Riesgos por amenazas de la plataforma Oracle

IV.9. Análisis de Riesgos de la plataforma Firewall - IESS

La Figura IV-11 muestra el diagrama de conexión de equipos de la plataforma Firewall-IESS.

Figura IV-11. Topología de la red de conexión de equipos de la plataforma Firewall

La Figura IV-11 indica el diagrama de conectividad actual de los equipos de la plataforma Firewall checkpoint, teniendo cuatro equipos físicamente, siendo dos un clúster de internet y otros dos un clúster de intranet (ver resaltado en color rojo).

La Figura IV-12 muestra la dependencia de activos de equipos con el firewall.

Figura IV-12. Diagrama de dependencia de equipos de la plataforma Firewall-IESS

La valoración de los activos se ha realizado con personal técnico a cargo de Firewalls, Ingeniera Silvia Duque encargada de la administración y el stack switch core, ips y stack switch extranet con el ingeniero Fernando Erraez, del Área de redes.

IV.9.1. Actividad 1: Lanzamiento

En esta actividad se define un catálogo de los elementos que participan en el modelo conceptual. Para ello, se han definido las taxonomías de estos elementos, que fueron descritos en el capítulo 2 de esta tesis doctoral, se define la taxonomía de tipos de activos de la organización enfocados en ciberseguridad en base al estándar ISO 27005, la taxonomía de Vulnerabilidades en

ciberseguridad en base al estándar ISO 27005, y se establece la taxonomía de Amenazas en ciberseguridad en base al estándar ENISA 2016 Actividad 1: Identificar Activos – Vulnerabilidades

IV.9.2. Actividad 2: Identificar y evaluar Activos

En esta actividad se identifica los activos de ciberseguridad, determinar el costo del activo y la medición del impacto que tiene el activo en cada una de las dimensiones de seguridad.

La Tabla IV-38 muestra la criticidad de los activos de la plataforma Firewall-IESS.

Tabla IV-38. Costo e impacto en las dimensiones de seguridad de los activos de la plataforma Firewall-IESS

IDENTIFICACIÓN DE ACTIVOS										
#	Tipo Activo	Activo	Costo del Activo	Confidencialidad		Integridad		Disponibilidad		Criticidad
1	Hardware	FIREWALL INTERNET (1)	\$ 130.000,00	7	Media	7	Media	10	Alta	10
2	Hardware	FIREWALL INTERNET (2)	\$ 130.000,00	6	Media	6	Media	9	Alta	9
3	Hardware	FIREWALL INTRANET (1)	\$ 130.000,00	6	Media	7	Media	10	Alta	10
4	Hardware	FIREWALL INTRANET (2)	\$ 130.000,00	7	Media	7	Media	9	Alta	9
5	Hardware	STACK SWITCH CORE	\$ 20.000,00	7	Media	4	Baja	8	Alta	8
6	Hardware	IPS	\$ 500.000,00	6	Media	3	Baja	4	Baja	6
7	Hardware	STACK SWITCH EXTRANET	\$ 20.000,00	7	Media	3	Baja	10	Alta	10

IV.9.3. Actividad 3: Evaluar el nivel de daño para las tuplas Vulnerabilidad – Activo (dimensión)

En esta actividad se ha determinado el daño de las vulnerabilidades en cada uno de los activos de la organización previamente identificados. La organización ha determinado el valor del daño de la vulnerabilidad en cada una de las dimensiones (confidencialidad, integridad, disponibilidad y criticidad) del activo, para ello hay que identificar las vulnerabilidades de los activos de la plataforma Firewall-IESS.

La Tabla IV-39 muestra la valoración del daño de las vulnerabilidades en los activos según las dimensiones de seguridad de la información de la plataforma Firewall, así como el costo del daño de las vulnerabilidades.

Tabla IV-39. Tuplas Vulnerabilidades - Activos, valor y costo del daño de las vulnerabilidades de la plataforma Firewall-IESS

				DIMENSION				VULNERABILIDAD	
	VULNERABILIDAD	ACTIVO	Costo del Activo	Daño Confidencialidad	Daño Integridad	Daño Disponibilidad	Daño Criticidad	Valor del Daño	Costo del Daño
1	Susceptibilidad a las variaciones de temperatura.	FIREWALL INTERNET 1	\$ 130.000,00	10	5	2	10	6,75	\$ 6.000,00
2	Ubicación en un área susceptible a inundaciones.	FIREWALL INTERNET 1		10	5	2	10	6,75	\$ 6.000,00
3	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	FIREWALL INTERNET 1		10	5	2	10	6,75	\$ 6.000,00
4	Falta de soporte preventivo y correctivo	FIREWALL INTERNET 1		8	5	2	10	6,25	\$ 3.000,00
5	No existe la divulgación adecuada del expertise adquirido	FIREWALL INTERNET 1		6	7	2	10	6,25	\$ 2.000,00
6	Falta socialización de políticas internas y externas	FIREWALL INTERNET 1		7	7	2	10	6,50	\$ 3.000,00
7	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	FIREWALL INTERNET 1		1	6	2	10	4,75	\$ 3.000,00
8	Intermitencia en el tráfico de la red	FIREWALL INTERNET 1		5	4	2	10	5,25	\$ 1.000,00
9	No cuenta con mecanismos contra ataques informáticos	FIREWALL INTERNET 1		5	10	10	10	8,75	\$ 2.000,00
10	Gestión inadecuado del accesos a Internet en las unidades de gestión	FIREWALL INTERNET 1		5	9	8	10	8,00	\$ 2.000,00
11	Susceptibilidad a las variaciones de temperatura.	FIREWALL INTERNET 2	\$ 130.000,00	10	5	2	9	6,50	\$ 6.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confidencialidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Críticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
12	Ubicación en un área susceptible a inundaciones.	FIREWALL INTERNET 2		10	5	2	9	6,50	\$ 6.000,00
13	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	FIREWALL INTERNET 2		10	5	2	9	6,50	\$ 6.000,00
14	Falta de soporte preventivo y correctivo	FIREWALL INTERNET 2		8	5	2	9	6,00	\$ 3.000,00
15	No existe la divulgación adecuada del expertise adquirido	FIREWALL INTERNET 2		6	7	2	9	6,00	\$ 2.000,00
16	Falta socialización de políticas internas y externas	FIREWALL INTERNET 2		7	7	2	9	6,25	\$ 3.000,00
17	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	FIREWALL INTERNET 2		1	6	2	9	4,50	\$ 3.000,00
18	Intermitencia en el tráfico de la red	FIREWALL INTERNET 2		5	4	2	9	5,00	\$ 1.000,00
19	No cuenta con mecanismos contra ataques informáticos	FIREWALL INTERNET 2		5	10	10	9	8,50	\$ 2.000,00
20	Gestión inadecuado del accesos a Internet en las unidades de gestión	FIREWALL INTERNET 2		5	9	8	9	7,75	\$ 2.000,00
21	Susceptibilidad a las variaciones de temperatura.	FIREWALL INTRANET 1	\$ 130.000,00	10	5	2	10	6,75	\$ 6.000,00
22	Ubicación en un área susceptible a inundaciones.	FIREWALL INTRANET 1		10	5	2	10	6,75	\$ 6.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confidencialidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Críticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
23	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	FIREWALL INTRANET 1		10	5	2	10	6,75	\$ 6.000,00
24	Falta de soporte preventivo y correctivo	FIREWALL INTRANET 1		8	5	2	10	6,25	\$ 3.000,00
25	No existe la divulgación adecuada del expertise adquirido	FIREWALL INTRANET 1		6	7	2	10	6,25	\$ 2.000,00
26	Falta socialización de políticas internas y externas	FIREWALL INTRANET 1		7	7	2	10	6,50	\$ 3.000,00
27	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	FIREWALL INTRANET 1		1	6	2	10	4,75	\$ 3.000,00
28	Intermitencia en el tráfico de la red	FIREWALL INTRANET 1		5	4	2	10	5,25	\$ 1.000,00
29	No cuenta con mecanismos contra ataques informáticos	FIREWALL INTRANET 1		5	10	10	10	8,75	\$ 2.000,00
30	Gestión inadecuado del accesos a Internet en las unidades de gestión	FIREWALL INTRANET 1		5	9	8	10	8,00	\$ 2.000,00
31	Susceptibilidad a las variaciones de temperatura.	FIREWALL INTRANET 2	\$ 130.000,00	10	5	2	9	6,50	\$ 6.000,00
32	Ubicación en un área susceptible a inundaciones.	FIREWALL INTRANET 2		10	5	2	9	6,50	\$ 6.000,00
33	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	FIREWALL INTRANET 2		10	5	2	9	6,50	\$ 6.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confidencialidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Críticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
34	Falta de soporte preventivo y correctivo	FIREWALL INTRANET 2		8	5	2	9	6,00	\$ 3.000,00
35	No existe la divulgación adecuada del expertise adquirido	FIREWALL INTRANET 2		6	7	2	9	6,00	\$ 2.000,00
36	Falta socialización de políticas internas y externas	FIREWALL INTRANET 2		7	7	2	9	6,25	\$ 3.000,00
37	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	FIREWALL INTRANET 2		1	6	2	9	4,50	\$ 3.000,00
38	Intermitencia en el tráfico de la red	FIREWALL INTRANET 2		5	4	2	9	5,00	\$ 1.000,00
39	No cuenta con mecanismos contra ataques informáticos	FIREWALL INTRANET 2		5	10	10	9	8,50	\$ 2.000,00
40	Gestión inadecuado del accesos a Internet en las unidades de gestión	FIREWALL INTRANET 2		5	9	8	9	7,75	\$ 2.000,00
41	Ubicación en un área susceptible a inundaciones.	STACK SWITCH CORE	\$ 20.000,00	10	0	0	8	4,50	\$ 20.000,00
42	Susceptibilidad a las variaciones de temperatura.	STACK SWITCH CORE		10	0	0	8	4,50	\$ 20.000,00
43	Falta de soporte preventivo y correctivo	STACK SWITCH CORE		10	5	0	8	5,75	\$ 10.000,00
44	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	STACK SWITCH CORE		10	0	0	8	4,50	\$ 20.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confidencialidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Críticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
45	Falta de planes de crecimiento y expansión de servicios de TI	STACK SWITCH CORE		8	0	0	8	4,00	\$ 20.000,00
46	No existe la divulgación adecuada del expertise adquirido	STACK SWITCH CORE		10	10	5	8	8,25	\$ 2.000,00
47	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	STACK SWITCH CORE		10	10	10	8	9,50	\$ 20.000,00
48	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	STACK SWITCH CORE		8	10	10	8	9,00	\$ 2.000,00
49	Presenta cableado deficiente	STACK SWITCH CORE		10	0	0	8	4,50	\$ 10.000,00
50	Ubicación en un área susceptible a inundaciones.	IPS	\$ 500.000,00	10	0	0	6	4,00	\$ 500.000,00
51	Susceptibilidad a las variaciones de temperatura.	IPS		10	0	0	6	4,00	\$ 500.000,00
52	Falta de soporte preventivo y correctivo	IPS		10	5	0	6	5,25	\$ 250.000,00
53	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	IPS		10	0	0	6	4,00	\$ 500.000,00
54	Falta de planes de crecimiento y expansión de servicios de TI	IPS		9	0	0	6	3,75	\$ 500.000,00
55	No existe la divulgación adecuada del expertise adquirido	IPS		10	10	5	6	7,75	\$ 10.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confidencialidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Críticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
56	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	IPS		10	10	10	6	9,00	\$ 500.000,00
57	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	IPS		8	10	10	6	8,50	\$ 10.000,00
58	Presenta cableado deficiente	IPS		10	0	0	6	4,00	\$ 250.000,00
59	Espacio físico designado no reúne condiciones técnicas	STACK SWITCH EXTRANET	\$ 20.000,00	10	0	0	10	5,00	\$ 10.000,00
60	Ubicación en un área susceptible a inundaciones.	STACK SWITCH EXTRANET		10	0	0	10	5,00	\$ 20.000,00
61	Susceptibilidad a las variaciones de temperatura.	STACK SWITCH EXTRANET		10	0	0	10	5,00	\$ 20.000,00
62	Falta de soporte preventivo y correctivo	STACK SWITCH EXTRANET		10	5	0	10	6,25	\$ 10.000,00
63	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	STACK SWITCH EXTRANET		10	0	0	10	5,00	\$ 20.000,00
64	Falta de planes de crecimiento y expansión de servicios de TI	STACK SWITCH EXTRANET		8	0	0	10	4,50	\$ 20.000,00
65	No existe la divulgación adecuada del expertise adquirido	STACK SWITCH EXTRANET		10	10	5	10	8,75	\$ 2.000,00
66	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	STACK SWITCH EXTRANET		10	10	10	10	10,00	\$ 20.000,00

				<i>DIMENSION</i>				<i>VULNERABILIDAD</i>	
	<i>VULNERABILIDAD</i>	<i>ACTIVO</i>	<i>Costo del Activo</i>	<i>Daño Confidencialidad</i>	<i>Daño Integridad</i>	<i>Daño Disponibilidad</i>	<i>Daño Críticidad</i>	<i>Valor del Daño</i>	<i>Costo del Daño</i>
67	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	STACK SWITCH EXTRANET		8	10	10	10	9,50	\$ 2.000,00
68	Presenta cableado deficiente	STACK SWITCH EXTRANET		10	0	0	10	5,00	\$ 10.000,00

IV.9.4. Actividad 4: Identificación de Amenazas de ciberseguridad

En esta actividad se identifican las amenazas para cada una de las vulnerabilidades asociadas a los activos de ciberseguridad, como se muestra en la Tabla IV-40.

Tabla IV-40. Tripleta Amenazas – Vulnerabilidades -Activos con el valor y costo del daño de la Amenaza para la plataforma Firewall-IESS

	AMENAZAS	VULNERABILIDADES	ACTIVOS	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
1	Fuego	Susceptibilidad a las variaciones de temperatura.	FIREWALL INTERNET 1	6,75	\$ 6.000,00
2	Agua	Ubicación en un área susceptible a inundaciones.	FIREWALL INTERNET 1	6,75	\$ 6.000,00
3	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	FIREWALL INTERNET 1	6,75	\$ 6.000,00
4	Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	FIREWALL INTERNET 1	6,25	\$ 3.000,00
5	Uso erróneo o administración de dispositivos y sistemas	No existe la divulgación adecuada del expertise adquirido	FIREWALL INTERNET 1	6,25	\$ 2.000,00
6	Uso erróneo o administración de dispositivos y sistemas	Falta socialización de políticas internas y externas	FIREWALL INTERNET 1	6,50	\$ 3.000,00
7	Uso erróneo o administración de dispositivos y sistemas	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	FIREWALL INTERNET 1	4,75	\$ 3.000,00
8	Fallo de dispositivos o sistemas	Intermitencia en el tráfico de la red	FIREWALL INTERNET 1	5,25	\$ 1.000,00
9	Código malicioso / software / actividad	No cuenta con mecanismos contra ataques informáticos	FIREWALL INTERNET 1	8,75	\$ 2.000,00
10	Corte de internet	Gestión inadecuado del accesos a Internet en las unidades de gestión	FIREWALL INTERNET 1	8,00	\$ 2.000,00
11	Fuego	Susceptibilidad a las variaciones de temperatura.	FIREWALL INTERNET 2	6,50	\$ 6.000,00
12	Agua	Ubicación en un área susceptible a inundaciones.	FIREWALL INTERNET 2	6,50	\$ 6.000,00

	AMENAZAS	VULNERABILIDADES	ACTIVOS	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
13	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	FIREWALL INTERNET 2	6,50	\$ 6.000,00
14	Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	FIREWALL INTERNET 2	6,00	\$ 3.000,00
15	Uso erróneo o administración de dispositivos y sistemas	No existe la divulgación adecuada del expertise adquirido	FIREWALL INTERNET 2	6,00	\$ 2.000,00
16	Uso erróneo o administración de dispositivos y sistemas	Falta socialización de políticas internas y externas	FIREWALL INTERNET 2	6,25	\$ 3.000,00
17	Uso erróneo o administración de dispositivos y sistemas	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	FIREWALL INTERNET 2	4,50	\$ 3.000,00
18	Fallo de dispositivos o sistemas	Intermitencia en el tráfico de la red	FIREWALL INTERNET 2	5,00	\$ 1.000,00
19	Código malicioso / software / actividad	No cuenta con mecanismos contra ataques informáticos	FIREWALL INTERNET 2	8,50	\$ 2.000,00
20	Corte de internet	Gestión inadecuado del accesos a Internet en las unidades de gestión	FIREWALL INTERNET 2	7,75	\$ 2.000,00
21	Fuego	Susceptibilidad a las variaciones de temperatura.	FIREWALL INTRANET 1	6,75	\$ 6.000,00
22	Agua	Ubicación en un área susceptible a inundaciones.	FIREWALL INTRANET 1	6,75	\$ 6.000,00
23	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	FIREWALL INTRANET 1	6,75	\$ 6.000,00
24	Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	FIREWALL INTRANET 1	6,25	\$ 3.000,00
25	Uso erróneo o administración de dispositivos y sistemas	No existe la divulgación adecuada del expertise adquirido	FIREWALL INTRANET 1	6,25	\$ 2.000,00

	AMENAZAS	VULNERABILIDADES	ACTIVOS	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
26	Uso erróneo o administración de dispositivos y sistemas	Falta socialización de políticas internas y externas	FIREWALL INTRANET 1	6,50	\$ 3.000,00
27	Uso erróneo o administración de dispositivos y sistemas	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	FIREWALL INTRANET 1	4,75	\$ 3.000,00
28	Fallo de dispositivos o sistemas	Intermitencia en el tráfico de la red	FIREWALL INTRANET 1	5,25	\$ 1.000,00
29	Código malicioso / software / actividad	No cuenta con mecanismos contra ataques informáticos	FIREWALL INTRANET 1	8,75	\$ 2.000,00
30	Corte de internet	Gestión inadecuado del accesos a Internet en las unidades de gestión	FIREWALL INTRANET 1	8,00	\$ 2.000,00
31	Fuego	Susceptibilidad a las variaciones de temperatura.	FIREWALL INTRANET 2	6,50	\$ 6.000,00
32	Agua	Ubicación en un área susceptible a inundaciones.	FIREWALL INTRANET 2	6,50	\$ 6.000,00
33	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	FIREWALL INTRANET 2	6,50	\$ 6.000,00
34	Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	FIREWALL INTRANET 2	6,00	\$ 3.000,00
35	Uso erróneo o administración de dispositivos y sistemas	No existe la divulgación adecuada del expertise adquirido	FIREWALL INTRANET 2	6,00	\$ 2.000,00
36	Uso erróneo o administración de dispositivos y sistemas	Falta socialización de políticas internas y externas	FIREWALL INTRANET 2	6,25	\$ 3.000,00
37	Uso erróneo o administración de dispositivos y sistemas	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	FIREWALL INTRANET 2	4,50	\$ 3.000,00
38	Fallo de dispositivos o sistemas	Intermitencia en el tráfico de la red	FIREWALL INTRANET 2	5,00	\$ 1.000,00
39	Código malicioso / software / actividad	No cuenta con mecanismos contra ataques informáticos	FIREWALL INTRANET 2	8,50	\$ 2.000,00

	AMENAZAS	VULNERABILIDADES	ACTIVOS	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
40	Corte de internet	Gestión inadecuado del accesos a Internet en las unidades de gestión	FIREWALL INTRANET 2	7,75	\$ 2.000,00
41	Agua	Ubicación en un área susceptible a inundaciones.	STACK SWITCH CORE	4,50	\$ 20.000,00
42	Fuego	Susceptibilidad a las variaciones de temperatura.	STACK SWITCH CORE	4,50	\$ 20.000,00
43	Fallo o interrupción del suministro principal	Falta de soporte preventivo y correctivo	STACK SWITCH CORE	5,75	\$ 10.000,00
44	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	STACK SWITCH CORE	4,50	\$ 20.000,00
45	Fallo de software /aplicaciones o servicio	Falta de planes de crecimiento y expansión de servicios de TI	STACK SWITCH CORE	4,00	\$ 20.000,00
46	Uso erróneo o administración de dispositivos y sistemas	No existe la divulgación adecuada del expertise adquirido	STACK SWITCH CORE	8,25	\$ 2.000,00
47	Acceso físico no autorizado / Entrada no autorizada a las instalaciones	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	STACK SWITCH CORE	9,50	\$ 20.000,00
48	Robo de identidad (Fraude de identidad / Cuenta)	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	STACK SWITCH CORE	9,00	\$ 2.000,00
49	Pérdida de recursos	Presenta cableado deficiente	STACK SWITCH CORE	4,50	\$ 10.000,00
50	Agua	Ubicación en un área susceptible a inundaciones.	IPS	4,00	\$ 500.000,00
51	Fuego	Susceptibilidad a las variaciones de temperatura.	IPS	4,00	\$ 500.000,00
52	Fallo o interrupción del suministro principal	Falta de soporte preventivo y correctivo	IPS	5,25	\$ 250.000,00
53	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	IPS	4,00	\$ 500.000,00

	AMENAZAS	VULNERABILIDADES	ACTIVOS	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
	nevadas, vientos fuertes)				
54	Fallo de software /aplicaciones o servicio	Falta de planes de crecimiento y expansión de servicios de TI	IPS	3,75	\$ 500.000,00
55	Uso erróneo o administración de dispositivos y sistemas	No existe la divulgación adecuada del expertise adquirido	IPS	7,75	\$ 10.000,00
56	Acceso físico no autorizado / Entrada no autorizada a las instalaciones	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	IPS	9,00	\$ 500.000,00
57	Robo de identidad (Fraude de identidad / Cuenta)	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	IPS	8,50	\$ 10.000,00
58	Pérdida de recursos	Presenta cableado deficiente	IPS	4,00	\$ 250.000,00
59	Condiciones climáticas desfavorables	Espacio físico designado no reúne condiciones técnicas	STACK SWITCH EXTRANET	5,00	\$ 10.000,00
60	Agua	Ubicación en un área susceptible a inundaciones.	STACK SWITCH EXTRANET	5,00	\$ 20.000,00
61	Fuego	Susceptibilidad a las variaciones de temperatura.	STACK SWITCH EXTRANET	5,00	\$ 20.000,00
62	Fallo o interrupción del suministro principal	Falta de soporte preventivo y correctivo	STACK SWITCH EXTRANET	6,25	\$ 10.000,00
63	Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	STACK SWITCH EXTRANET	5,00	\$ 20.000,00
64	Fallo de software /aplicaciones o servicio	Falta de planes de crecimiento y expansión de servicios de TI	STACK SWITCH EXTRANET	4,50	\$ 20.000,00
65	Uso erróneo o administración de dispositivos y sistemas	No existe la divulgación adecuada del expertise adquirido	STACK SWITCH EXTRANET	8,75	\$ 2.000,00
66	Acceso físico no autorizado / Entrada no autorizada a las instalaciones	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	STACK SWITCH EXTRANET	10,00	\$ 20.000,00

	AMENAZAS	VULNERABILIDADES	ACTIVOS	Valor del Daño de la Vulnerabilidad	Costo del Daño de la Vulnerabilidad
67	Robo de identidad (Fraude de identidad / Cuenta)	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	STACK SWITCH EXTRANET	9,50	\$ 2.000,00
68	Pérdida de recursos	Presenta cableado deficiente	STACK SWITCH EXTRANET	5,00	\$ 10.000,00

La Tabla IV-41 muestra las amenazas de las vulnerabilidades identificadas a los activos de la plataforma Firewall-IESS, que se han identificado y analizado en la las tareas de la actividad 4.

Tabla IV-41. Tupla Amenazas – Vulnerabilidades con los valores y costo del daño de las vulnerabilidades para plataforma Firewall-IESS

AMENAZA	VULNERABILIDAD	Valor del Daño Promedio de la Vulnerabilidad	Costo del Daño Total de la Vulnerabilidad
Acceso físico no autorizado / Entrada no autorizada a las instalaciones	Uso inadecuado o descuidado del control de acceso físico a edificios y habitaciones	9,50	\$ 540.000,00
Agua	Ubicación en un área susceptible a inundaciones.	5,71	\$ 564.000,00
Código malicioso / software / actividad	No cuenta con mecanismos contra ataques informáticos	8,63	\$ 8.000,00
Condiciones climáticas desfavorables	Espacio físico designado no reúne condiciones técnicas	5,00	\$ 10.000,00
Condiciones climáticas desfavorables	Falta de soporte preventivo y correctivo	6,13	\$ 12.000,00
Corte de internet	Gestión inadecuado del accesos a Internet en las unidades de gestión	7,88	\$ 8.000,00
Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	5,71	\$ 564.000,00
Fallo de dispositivos o sistemas	Intermitencia en el tráfico de la red	5,13	\$ 4.000,00
Fallo de software /aplicaciones o servicio	Falta de planes de crecimiento y expansión de servicios de TI	4,08	\$ 540.000,00
Fallo o interrupción del suministro principal	Falta de soporte preventivo y correctivo	5,75	\$ 270.000,00
Fuego	Susceptibilidad a las variaciones de temperatura.	5,71	\$ 564.000,00
Pérdida de recursos	Presenta cableado deficiente	4,50	\$ 270.000,00

AMENAZA	VULNERABILIDAD	Valor del Daño Promedio de la Vulnerabilidad	Costo del Daño Total de la Vulnerabilidad
Robo de identidad (Fraude de identidad / Cuenta)	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	9,00	\$ 14.000,00
Uso erróneo o administración de dispositivos y sistemas	Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	4,63	\$ 12.000,00
Uso erróneo o administración de dispositivos y sistemas	Falta socialización de políticas internas y externas	6,38	\$ 12.000,00
Uso erróneo o administración de dispositivos y sistemas	No existe la divulgación adecuada del expertise adquirido	7,04	\$ 22.000,00

La Tabla IV-42 muestra las amenazas identificadas que pueden afectar a los activos de la plataforma Host-IESS.

Tabla IV-42.- Amenazas con los valores y costo del daño de la amenaza para la plataforma Firewall-IESS

AMENAZAS	VALOR DEL DAÑO DE LA AMENAZA	COSTO DEL DAÑO DE LA AMENAZA
Acceso físico no autorizado / Entrada no autorizada a las instalaciones	9,50	\$ 540.000,00
Agua	5,71	\$ 564.000,00
Código malicioso / software / actividad	8,63	\$ 8.000,00
Condiciones climáticas desfavorables	5,56	\$ 22.000,00
Corte de internet	7,88	\$ 8.000,00
Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	5,71	\$ 564.000,00
Fallo de dispositivos o sistemas	5,13	\$ 4.000,00
Fallo de software /aplicaciones o servicio	4,08	\$ 540.000,00
Fallo o interrupción del suministro principal	5,75	\$ 270.000,00
Fuego	5,71	\$ 564.000,00
Pérdida de recursos	4,50	\$ 270.000,00
Robo de identidad (Fraude de identidad / Cuenta)	9,00	\$ 14.000,00
Uso erróneo o administración de dispositivos y sistemas	6,01	\$ 46.000,00

IV.9.5. Actividad 5: Medición del Riesgo

La Figura IV-13 muestra la matriz de riesgo de la plataforma Firewall-IESS.

AMENAZA	VALOR DEL DAÑO	FRECUENCIA	RIESGO	COSTO DEL DAÑO
Acceso físico no autorizado / Entrada no autorizada a las instalaciones	10,00	B	6	\$ 540.000,00
Agua	6,00	A	6	\$ 564.000,00
Código malicioso / software / actividad	9,00	MA	10	\$ 8.000,00
Condiciones climáticas desfavorables	6,00	A	6	\$ 22.000,00
Corte de internet	8,00	MA	9	\$ 8.000,00
Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	6,00	B	3	\$ 564.000,00
Fallo de dispositivos o sistemas	5,00	A	5	\$ 4.000,00
Fallo de software /aplicaciones o servicio	4,00	B	2	\$ 540.000,00
Fallo o interrupción del suministro principal	6,00	M	5	\$ 270.000,00
Fuego	6,00	B	3	\$ 564.000,00
Pérdida de recursos	5,00	B	2	\$ 270.000,00
Robo de identidad (Fraude de identidad / Cuenta)	9,00	B	6	\$ 14.000,00
Uso erróneo o administración de dispositivos y sistemas	6,00	B	3	\$ 46.000,00

Figura IV-13. Matriz de riesgos de la plataforma Firewall-IESS

IV.9.6. Actividad 6: Contramedidas

La Tabla IV-43 muestra las contramedidas para cada una de las vulnerabilidades identificadas en los activos de la plataforma Firewall.

Tabla IV-43. Contramedidas para las vulnerabilidades plataforma Firewall-IESS

VULNERABILIDADES	CONTRAMEDIDA
Espacio físico designado no reúne condiciones técnicas	Adecuación de espacios físicos según las necesidades tecnológicas de los activos
Falta de mecanismos de identificación y autenticación como la autenticación de usuarios.	Establecer lineamientos de gestión de identificación y autenticación de usuarios para el acceso a los activos de la organización
Falta de planes de crecimiento y expansión de servicios de TI	Implementar una Arquitectura Empresarial
Falta de soporte preventivo y correctivo	Contratos de soporte y mantenimiento en vigencia
Falta socialización de políticas internas y externas	Socializar de forma continua las políticas internas y externas de la organización
Gestión inadecuada de los accesos a Internet en las unidades de gestión	Política y regularización de accesos a internet
Intermitencia en el tráfico de la red	Implementar una medida de réplica de la red de información
No cuenta con mecanismos contra ataques informáticos	Implementar medidas que repelan los ataques informáticos hacia los activos de la organización
No existe la divulgación adecuada del conocimiento adquirido	Capacitación continua en la administración del activo
Presenta cableado deficiente	Control preventivo y correctivo del cableado estructurado

VULNERABILIDADES	CONTRAMEDIDA
Susceptibilidad a las variaciones de temperatura.	Sistema contra incendios y ventilación adecuada
Susceptibilidad a movimientos e impactos excesivos en la estructura del edificio	Instalaciones sismo-resistentes
Ubicación en un área susceptible a inundaciones.	Mejora física de las instalaciones, drenajes adecuados
Uso inadecuado o descuido del control de acceso físico a edificios y habitaciones	Mejora en los accesos físicos al edificio y habitación

IV.9.6.1 Gráfica de radar de los riesgos por amenazas

En esta sección se muestra los valores de los riesgos de las amenazas identificadas, con los valores actuales, el valor objetivo que como organización se desea tener, y valor permisible y controlable de los mismos.

- Valor actual: promedio de todos los riesgos.
- Valor objetivo: recomendación de la SDNSI de reducción de riesgo (al menos el 50%).
- Valor límite: valor dado por condiciones gráficas, al que nunca se debería llegar.

Tabla IV-44 Valores de riesgos de las amenazas Firewall-IESS

ACTIVO	ACTUAL	OBJETIVO	LIMITE
Acceso físico no autorizado / Entrada no autorizada a las instalaciones	6,00	3,00	7
Agua	6,00	3,00	7
Código malicioso / software / actividad	10,00	5,00	7
Condiciones climáticas desfavorables	6,00	3,00	7
Corte de internet	9,00	4,50	7
Desastres (terremotos naturales, inundaciones, deslizamientos de tierra, tsunamis, lluvias intensas, fuertes nevadas, vientos fuertes)	3,00	1,50	7
Fallo de dispositivos o sistemas	5,00	2,50	7
Fallo de software /aplicaciones o servicio	2,00	1,00	7
Fallo o interrupción del suministro principal	5,00	2,50	7
Fuego	3,00	1,50	7
Pérdida de recursos	2,00	1,00	7
Robo de identidad (Fraude de identidad / Cuenta)	6,00	3,00	7
Uso erróneo o administración de dispositivos y sistemas	3,00	1,50	7

La Figura IV-14 muestra los valores de los riesgos actuales, riesgo objetivo y el riesgo permisible definido por la organización.

Figura IV-14. Reporte de riesgos plataforma firewall y equipos dependientes

IV.10. Resumen del Anexo IV

En este anexo se han recogido los resultados obtenidos de haber implementado el modelo conceptual definido en el Capítulo 2, y siguiendo el marco de trabajo de evaluación y análisis AVARCIBER definido en el Capítulo 4.

Se han implementado las definiciones de activos, vulnerabilidades, amenazas y riesgos de ciberseguridad, y se han utilizado los conceptos definidos y recopilados en el modelo conceptual, y se ha seguido las actividades definidas en el marco de trabajo de evaluación y análisis AVARCIBER.

Luego de la aplicación del marco de trabajo AVARCIBER y de la validación de los elementos del modelo conceptual, se han encontrado las siguientes observaciones:

- Todos los elementos del modelo conceptual y el marco de trabajo definido se han complementado, generando resultados que responden a las necesidades de la organización.
- El modelo conceptual utilizado se ha acoplado a las necesidades de la organización priorizando la identificación y gestión de las vulnerabilidades.
- Los parámetros cualitativos y cuantitativos utilizados permitieron una mejor identificación y diferenciación de la importancia e impacto de los activos de ciberseguridad evaluados.
- La utilización de las taxonomías generadas de vulnerabilidades y amenazas permitieron una mejor gestión de las mismas, así como se ha evitado la duplicidad de las mismas.
- La identificación de los costos de los activos y valoración de las vulnerabilidades de los activos ha ayudado a identificar de una forma cuantitativa el impacto de las amenazas al materializar las vulnerabilidades, mejorando la comprensión del daño económico al que están expuestos.
- Se han agrupado las amenazas por vulnerabilidades y activos, permitiendo tener trazabilidades de las amenazas y de las vulnerabilidades asociadas por activo, tanto de forma individual como agrupadas.

- La agrupación de las amenazas por vulnerabilidades y activos, ha generado mayor visibilidad de las amenazas críticas y de las vulnerabilidades más recurrentes, que, complementadas con la valoración de cada uno de ellas, han generado información detallada y cuantificable para la toma de decisiones.
- Las contramedidas identificadas se asociaron a las vulnerabilidades identificadas para solucionarlas, generando una respuesta más efectiva porque las contramedidas solucionan las vulnerabilidades de todos los activos en los cuales están presentes.
- Como conclusión final, podemos indicar que la gestión de riesgos utilizando el modelo conceptual sugerido y el marco de trabajo AVARCIBER, les ha permitido tener una mejor visión de las relaciones que pueden tener los elementos de la gestión de riesgos de ciberseguridad, la valoración de los activos y vulnerabilidades ha permitido mejorar la toma de decisiones en la criticidad de los riesgos y de las contramedidas que se deben aplicar.