Prototipo para Gestionar la Ciberseguridad en Pequeñas Empresas

A Prototype to Manage Cybersecurity in Small Companies

M. Rea-Guaman, J. A. Calvo-Manzano, T. San Feliu
Universidad Politécnica de Madrid, ETS Ingenieros Informáticos
Boadilla del Monte, Madrid, España
marcelo.rea.guaman@alumnos.upm.es, {joseantonio.calvomanzano, tomas.sanfeliu}@upm.es

Resumen — **La ciberseguridad se define como la protección de activos de información a través del tratamiento de amenazas que ponen en riesgo la información. Las organizaciones, independientemente de su tamaño, deben gestionar los riesgos de ciberseguridad para mejorar la seguridad y la capacidad de recuperación de sus activos. Las grandes compañías realizan cada vez mayores inversiones en ciberseguridad. Sin embargo, la percepción de este peligro en empresas más pequeñas es reducida y son pocas las que tienen entre su lista de prioridades proteger sus sistemas. En el mercado, existen pocos sistemas de ciberseguridad para pequeñas empresas enfocados en la gestión de activos, y vulnerabilidades y amenazas de ciberseguridad. Es por ello que en este artículo se busca identificar algunas herramientas de gestión de ciberseguridad para pequeñas empresas, y describir algunos requerimientos que debería tener una herramienta de gestión de ciberseguridad para cubrir las necesidades de las pequeñas empresas. Estos requerimientos se plasmarán en un prototipo.**

Palabras Clave - riesgos de ciberseguridad; herramientas de riesgos de ciberseguridad; pequeñas empresas.

Abstract — **Cybersecurity is defined as the protection of information assets through the treatment of threats that put information at risk. Enterprises, regardless of their size, must manage the cybersecurity risks to improve the security and resilience of their assets. The large enterprises are increasingly investing in cybersecurity. However, the perception of this danger in smaller companies is limited, and few of them have among their list of priorities to protect their information systems. In the market, there are few cybersecurity systems for small businesses focused on asset management, and cybersecurity vulnerabilities and threats. For this reason, this paper seeks to identify cybersecurity management tools for small enterprises and it describes some of the requirements that a cybersecurity management tool should have to cover the needs of small enterprises. These requirements will be reflected in a prototype.**

Keywords - cybersecurity risks; cybersecurity risk tools; small companies.

I. INTRODUCCIÓN

La 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 ESET [1], la ciberseguridad se define como "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".

La ciberseguridad es un tema de actualidad y es una de las principales preocupaciones de las organizaciones, debido a la creciente incorporación de tecnologías en las mismas. En sus inicios, la ciberseguridad era relativamente simple (básicamente enfocada a virus y código malicioso). Hoy en día, es una actividad compleja, caracterizada por ataques persistentes a gran escala que permiten entrar en las redes internas empresariales, generando pérdidas económicas, robo de información crítica, caída de los servicios, e incluso llegando hasta la pérdida de la imagen y prestigio de la empresa [2], [3].

La problemática de la ciberseguridad no es exclusiva de las grandes organizaciones, sino de todas aquellas organizaciones, independientemente de su tamaño, que cada día están más interconectadas en tiempo real, pues están expuestas a los daños que las amenazas cibernéticas pueden causar a los activos de la organización. En este contexto, las pequeñas empresas también sienten la necesidad de considerar la ciberseguridad como un elemento importante a considerar en su organización, ya que se encuentran más desamparadas al no disponer ni de personal ni de herramientas enfocadas a la ciberseguridad. Actualmente, para poder gestionar de manera eficaz y eficiente la ciberseguridad (es decir, las amenazas, vulnerabilidades de los activos y los riesgos latentes que puedan llegar a materializarse), es necesario la utilización de una herramienta.

En base a lo anterior, se presenta la necesidad de una herramienta para gestionar la ciberseguridad en pequeñas empresas. Es por ello, que se inició la construcción de un prototipo, que tiene que cumplir un conjunto de requisitos a tener en cuenta. Para ello, previamente se analizaron cuatro herramientas para pequeñas empresas, que sirvieron de base para establecer los requerimientos a aplicar al prototipo desarrollado. Así, el presente artículo se organiza de la siguiente manera: la sección II presenta las normas relacionadas con la gestión de riesgos y las herramientas de gestión de riesgos en ciberseguridad para pequeñas empresas que se van a analizar; la

sección III muestra las herramientas seleccionadas, sus características y particularidades; la sección IV describe los conceptos utilizados en el prototipo; la sección V presenta los requerimientos y el proceso del prototipo definido; y, finalmente, la sección VI presenta las conclusiones.

II. CONTEXTO

El contexto de las herramientas de gestión de riesgos está condicionado por el entorno normativo y por los organismos enfocados a la seguridad informática que son promotores de herramientas.

A. Normas

Las normas internacionales más importantes que se relacionan con la gestión de riesgos son:

- BS 7799, norma publicada por el British Standard Institute, que incluye la identificación y evaluación del riesgo, mediante la mejora continua [4].
- Serie ISO/IEC 27000, familia de estándares sobre gestión de la seguridad de la información derivados de la norma británica BS 7799 [5].
- NIST SP 800-53, que proporciona una guía de gestión de riesgos para el personal con y sin experiencia, en los sistemas de tecnología de la información de EEUU [6].

B. Herramientas

Las pequeñas empresas tienen a su disposición soluciones abiertas (Enterprise Resources Management, ERP) que les permiten una gestión empresarial, como son: Odoo, Openbravo, ERP5, Compiere. Sin embargo, ninguna de ellas dispone de la funcionalidad de gestión de riesgos. Hay que tener en cuenta que para la gestión de riesgos de ciberseguridad, se deben considerar una gran cantidad de activos, y para cada uno de ellos, se deben considerar las vulnerabilidades de ciberseguridad existentes, así como las amenazas de ciberseguridad presentes. Por ello, es necesario que se deba utilizar una herramienta especifica que permita la mejor gestión de estos elementos. La herramienta deberá poder gestionar activos, y vulnerabilidades y amenazas de ciberseguridad desde catálogos prestablecidos.

Para identificar las herramientas que se enfocan en pequeñas empresas, se ha buscado en organismos públicos que ofrecieran herramientas libres para la gestión de riesgos (se han excluido herramientas comerciales de alto coste, como las que indica Gartner para la gestión de activos, vulnerabilidades y amenazas [7], [8], [9]).

Se ha iniciado la búsqueda en el Centro Criptológico Nacional (CCN) de España. CCN promociona el desarrollo de herramientas enfocadas a garantizar la seguridad de los sistemas. Este organismo ofrece herramientas de forma gratuita, y están disponibles para que las pequeñas y medianas empresas puedan empezar a gestionar su seguridad. Entre las herramientas que ofrece, se encuentra EAR (Entorno de Análisis de Riesgos) / PILAR (Procedimiento Informático Lógico para Análisis de Riesgos) que cubre parte de los requisitos iniciales. Se ofrece una versión para pequeñas empresas llamada PILAR Basic.

Se hizo otra búsqueda en la Agencia de la Unión Europea para la Seguridad de las Redes y la Información (ENISA). ENISA es un centro público de conocimientos para la ciberseguridad en Europa. ENISA ofrece RISICARE, que es un software de modelado de riesgos que permite la gestión de un SGSI (Sistema de Gestión de Seguridad de la Información) y utiliza un conjunto de puntos de control que incluye los de ISO 27002.

También se ha realizado una búsqueda en empresas privadas, para determinar si ofrecen productos gratis para la gestión de ciberseguridad en pequeñas empresas. En esta búsqueda, se ha encontrado la herramienta de Evaluación de Seguridad de Microsoft (Microsoft Security Assessment Tool, MSAT), que es una herramienta gratuita diseñada para ayudar a las organizaciones de menos de 1.000 empleados a evaluar los puntos débiles de su entorno de seguridad de Tecnologías de Información.

Asimismo, se revisó SE Risk, que es una herramienta libre, que permite la gestión de riesgos y controles en todos los aspectos del proceso de gestión de riesgos, desde la identificación inicial, evaluación, análisis mitigación y monitorización.

III. HERRAMIENTAS DE GESTION DE RIESGOS

A continuación, se presentan las herramientas identificadas y un resumen de los primeros hallazgos.

A. PILAR

Es una herramienta de gestión de riesgos de sistemas de información, que se acopla a la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información). PILAR es una herramienta que [10]:

- Soporta la identificación de activos. Se recopilan los activos del sistema, sus relaciones y su valor para la organización.
- Permite el análisis cualitativo y cuantitativo de riesgos. Se analizan los riesgos desde varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.
- Permite el análisis de impacto y continuidad de operaciones. Una vez conocidos los riesgos, se pueden determinar las salvaguardas y estimar el riesgo residual. Se analiza también el efecto de las interrupciones de servicio teniendo en cuenta la duración de la interrupción.
- Permite el cálculo de calificaciones de seguridad respecto a normas españolas como son UNE-ISO/IEC 27002: 2009: sistemas de gestión de seguridad, RD 1720/2007: datos de carácter personal, y RD 3/2010: Esquema Nacional de Seguridad.

B. RISICARE

Está basada en el método MEHARI que mejora la productividad y la precisión de un enfoque de gestión de riesgos, y está orientada a pequeñas empresas. Las funciones de RISICARE simulan condiciones del mundo real y prueban múltiples situaciones o escenarios de amenazas. RISICARE se puede considerar, además, como un software de modelado de riesgo. RISICARE [11] soporta la:

- Identificación de riesgos. RISICARE considera la combinación del análisis de riesgos, la clasificación de activos, el análisis de vulnerabilidad y el estudio de situaciones de riesgo para identificar los riesgos de acuerdo con el método MEHARI.
- Análisis de riesgos. El enfoque utilizado por RISICARE se basa en una base de conocimiento de la situación de amenaza integral y procedimientos automatizados para la evaluación de factores de reducción de riesgos.
- Evaluación de riesgos. RISICARE proporciona una medida de la gravedad del riesgo (probabilidad de ocurrencia por el impacto).

C. MSAT

Esta herramienta utiliza un enfoque integral para medir el nivel de seguridad y cubrir aspectos tales como usuarios, procesos y tecnología [12]. Utiliza el concepto de defensa en profundidad para implementar capas de defensa que incluyen controles técnicos, estándares organizativos y operativos, basándose en las mejores prácticas aceptadas para reducir el riesgo en entornos de TI como son ISO 17799 y NIST -800.x. MSAT proporciona:

- Un conocimiento constante, completo y fácil de utilizar del nivel de seguridad.
- Un marco de defensa en profundidad con análisis comparativos del sector.
- Informes detallados y actuales, comparando su plan inicial con los progresos obtenidos.
- Recomendaciones comprobadas y actividades prioritarias para mejorar la seguridad.
- Consejos estructurados de Microsoft y de la industria.

MSAT consta de 200 preguntas que abarcan infraestructura, aplicaciones, operaciones y usuarios. Las preguntas se obtienen a partir de estándares como por ejemplo las normas ISO 17799 y NIST-800.x.

La evaluación está diseñada para identificar los posibles riesgos de negocio de su organización y las medidas de seguridad implementadas para mitigarlos.

D. SE Risk

Permite la gestión de riesgos y controles, se puede implementar en varios departamentos de la organización, lo que permite la gestión de riesgos en los procesos, proyectos y estrategias de la empresa, así como en las prácticas de la gobernanza en la gestión de TI, y está alineada con la norma ISO 31000: 2009. SE Risk [14] nos ayuda a:

- Identificar los riesgos, evaluarlos y analizarlos, hasta la mitigación y la monitorización.
- Gestionar los incidentes.
- Evaluar los riesgos de forma cualitativa y cuantitativa.
- Monitorizar planes de acción.

E. Hallazgos

Del análisis realizado, se puede determinar que:

- PILAR es una herramienta que no relaciona las vulnerabilidades con otros elementos, pero si maneja riesgos residuales, y la última versión está actualizada al 2017.
- RISICARE realiza una identificación de riesgos, pero no relaciona las vulnerabilidades con otros elementos, y la última versión es del 2007.
- El enfoque de MSAT es un análisis de riesgos, por medio de cuestionarios. A partir del perfil del negocio, se calcula el riesgo de la empresa.
- SE Risk es una herramienta que contempla todo el proceso de gestión de riesgos, puede ser instalado en todos los departamentos de una organización, pudiendo estar la información disponible en cualquier momento.

En la Tabla I se muestran algunas características de las herramientas analizadas.

TABLA I. HERRAMIENTAS REVISADAS

Criterios	***PILAR***	***RISICARE***	***MSAT***	***SE Risk***
Análisis de activos, y amenazas y vulnerabilidades	NO	SI	NO	NO
Análisis de macro y situacional de riesgos	SI	SI	SI	SI
Relación de vulnerabilidades con activos y amenazas	NO	NO	NO	NO
Gestiona mitigación y monitorización de controles	SI	NO	NO	SI
Revisión en los últimos 5 años	SI	NO	NO	SI

Cada herramienta tendrá su particularidad, y muchas de ellas tendrán su utilidad en las organizaciones según la necesidad y enfoque de cada empresa. Sin embargo, lo que NO se muestra en estas herramientas es la relación directa que debe existir ente las vulnerabilidades y amenazas de ciberseguridad con cada activo de la organización. Por ello, se presenta a continuación, los principales conceptos y los requisitos que se deberían establecer para la gestión de riesgos en ciberseguridad.

IV. CONCEPTOS

A continuación, se definen los principales conceptos que se han tenido en cuenta:

- Activo. Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización [15].
- Categoría de activo / vulnerabilidad / amenaza. Es la clasificación que puede tener un activo / vulnerabilidad / amenaza.
- Dimensión de la valoración. Las dimensiones son las características o atributos que hacen valioso un activo. Las dimensiones típicas son con la confidencialidad, la integridad y la disponibilidad [16].

- Vulnerabilidad. Defecto o debilidad en el diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza [17].
- Amenaza. Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización [15].
- Riesgo. Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización [17]. El riesgo es el impacto por la probabilidad de ocurrencia de la amenaza.

V. PROTOTIPO

Este prototipo nos servirá de base para construir una 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, así como el prototipo realizado en una hoja de cálculo.

A. Activos

La organización deberá poder identificar las categorías de activos y activos que quiere gestionar. Además, la organización tendrá que valorar cada uno de estos activos. Para la identificación oportuna de los activos y sus tipos, la herramienta debe de ser capaz de gestionar un catálogo de activos y sus tipos. A partir de este catálogo, la organización seleccionaría las categorías de activos y activos a gestionar.

La Fig. 1 muestra el prototipo relativo a la selección de las categorías de activos y sus activos correspondientes por parte de la organización.

VALOR DEL ACTIVO	ACTIVOS	CATEGORÍA DE ACTIVOS
3000,00	Servidor	Equipos de Hardware
6000,00	Equipos de Comunicación	Equipos de Hardware
6000,00	Robots de Cinta	Equipos de Hardware
300,00	PC	Equipos de Hardware
1000,00	Sistemas Financieros y de negocio	Equipos de Software
600,00	Almacenamiento de Datos	Equipos de Software
100,00	Correo Electronico	Equipos de Software
1000,00	Virtualización	Equipos de Software
100,00	Internet	Equipos de Software
	Centro de Datos	Instalaciones
	Cuartos de Red	Instalaciones
500,00	UPS	Equipamiento Auxiliar

Figura 1. Categoría de activos y activos de la organización

B. Vulnerabilidades de ciberseguridad

La organización deberá poder identificar las categorías de vulnerabilidades y vulnerabilidades de ciberseguridad que quiere gestionar. Al igual que con los activos de la organización, para la identificación oportuna de las vulnerabilidades de ciberseguridad, la herramienta debe de ser capaz de gestionar un catálogo de vulnerabilidades de ciberseguridad. A partir de este catálogo, la organización seleccionaría las vulnerabilidades de ciberseguridad a gestionar.

Además, se deberán poder identificar las vulnerabilidades que están presentes en cada uno de los diferentes activos de la organización.

Igualmente, la organización deberá poder identificar, por cada activo, las dimensiones del activo que se van a valorar (por ejemplo, confidencialidad, disponibilidad e integridad). Y también será necesario identificar el tipo de valoración (cualitativo o cuantitativo) a realizar para determinar el impacto de la pareja vulnerabilidad – activo. La Tabla II muestra un ejemplo de ambos tipos de valoraciones. En la primera columna se muestra un ejemplo en el caso de valoración cualitativa, y en las columnas segunda y tercera se muestra el valor superior e inferior en el caso de valoración cuantitativa.

TABLA II. TIPOS DE VALORACIÓN DEL IMPACTO

Tipos de Valoración	*Valor Superior*	*Valor Inferior*
Daño Extremo	10	10
Muy Alto	9	9
Alto	8	6
Medio	5	3
Bajo	2	1
Despreciable	0	0

La Fig. 2 muestra el prototipo relativo a la valoración del impacto para cada par *vulnerabilidad de ciberseguridad y activo de la organización*, en cada una de las dimensiones del activo consideradas.

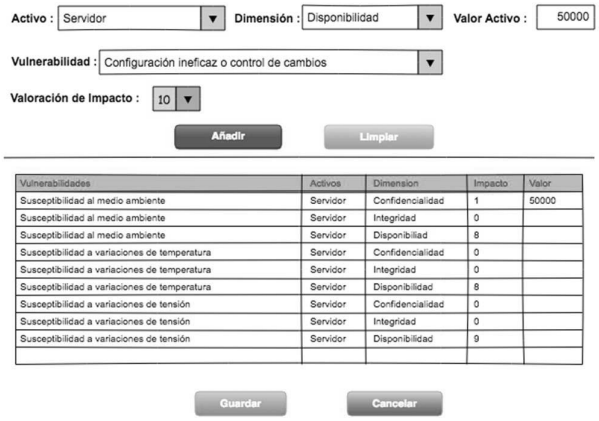

Figura 2. Valoración del impacto para cada dimensión del activo en cada pareja vulnerabilidad de ciberseguridad – activo

Una vez valoradas cada una de las dimensiones, se puede calcular el valor del impacto total de cada pareja vulnerabilidad – activo. Por ejemplo, para calcular el impacto total se podría utilizar la función promedio. Así, en el ejemplo de la Fig. 2, el impacto total para la vulnerabilidad "susceptibilidad al medio ambiente" y activo "servidor" sería de 3 (véase Fig. 3). Otra opción para calcular el impacto total, podría ser utilizar una función ponderada en función de la dimensión.

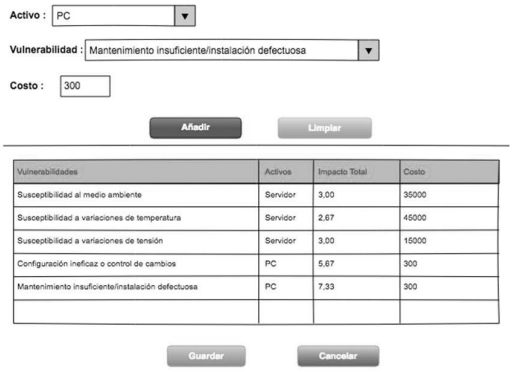

Figura 3. Valoración del impacto total por vulnerabilidad y su costo asociado

Una vez conocido el impacto total vulnerabilidad de ciberseguridad – activo, también se podría introducir el costo, que es el valor que determina la organización para un activo expuesto a una vulnerabilidad de ciberseguridad (véase Fig. 3).

C. Amenazas de ciberseguridad

La organización deberá poder identificar las categorías de amenazas y amenazas de ciberseguridad que quiere gestionar. Al igual que con los activos de la organización y vulnerabilidades de ciberseguridad, para la identificación oportuna de las amenazas de ciberseguridad, la herramienta debe de ser capaz de gestionar un catálogo de amenazas de ciberseguridad. A partir de este catálogo, la organización seleccionaría las amenazas de ciberseguridad que presentan los activos de la organización. Para ello, se deben relacionar las amenazas de ciberseguridad con las vulnerabilidades de seguridad existentes (véase Fig. 4).

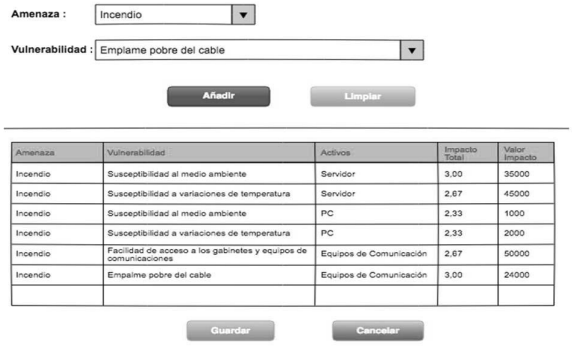

Figura 4. Asignación de vulnerabilidades, por amenazas de ciberseguridad

En la Fig.4 se observa que se tiene la valoración del impacto relativa a cada trío amenaza de ciberseguridad – vulnerabilidad de ciberseguridad – activo de la organización.

También se podría conocer el impacto de cada pareja amenaza de ciberseguridad – vulnerabilidad de seguridad. Por ejemplo, en la Fig. 4 se observa que la vulnerabilidad "susceptibilidad al medio ambiente" afecta a varios activos (servidor y PC). Entonces, para calcular el impacto de cada pareja amenaza de ciberseguridad – vulnerabilidad de ciberseguridad, se promedia su impacto (para la vulnerabilidad susceptibilidad al medio ambiente, véase 2,67 en la Fig. 5, que corresponde con el valor de 3 y 2,33 que se muestran en la Fig. 4) y se suma el valor del costo (véase 36.000 en la Fig. 5, que corresponde con la suma de 35.000 y 1.000 de la Fig. 4).

Figura 5. Amenazas de ciberseguridad ligadas a las vulnerabilidades de seguridad

Además, es necesario que la organización introduzca la frecuencia de la amenaza. En la Tabla III se muestra un ejemplo que puede ayudar a la organización a introducir el rango de frecuencia. Por ejemplo, si la amenaza es algo que ocurre mensualmente, su rango de frecuencia es Alto (A).

TABLA III. ESCALA DE CUANTIFICACIÓN DE LAS AMENAZAS

Rango de Frecuencia	***Probabilidad***	***Frecuencia***
MA (Muy Alto)	100	a diario
A (Alto)	10	mensualmente
M (Medio)	1	una vez al año
B (Bajo)	1 / 10	cada varios años
MB (Muy Bajo)	1 / 100	Cada varias décadas

En el caso del prototipo, y teniendo en cuenta la escala de cuantificación de la amenaza mostrada en la Tabla III, se asigna el rango de frecuencia a la amenaza (véase Fig. 6).

A continuación, es necesario calcular el riesgo de que ocurra la amenaza. El riesgo se calcula mediante el producto de probabilidad de la ocurrencia de la amenaza (Rango de Frecuencia) por el impacto. La Fig. 7 muestra cómo se calcula el riesgo.

Figura 6. Impacto y Rango de Frecuencia de las Amenazas de Ciberseguridad

Así, para ayudar a la organización a la toma de decisiones (p.ej., enfocarse en los riesgos de color rojo), podría establecer:

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

Rango de Frecuencia → Impacto ↓	MA	A	M	B	MB
10	10	10	7	6	3
9	10	9	7	6	3
8	9	8	6	5	2
7	9	8	5	3	2
6	9	6	5	3	1
5	8	5	3	2	1
4	8	5	2	2	1
3	6	4	1	1	0
2	5	3	1	1	0
1	4	2	1	0	0
0	2	1	0	0	0

Figura 7. Calculo del Riesgo

La Fig. 8 muestra el cálculo de los riesgos para las amenazas identificadas.

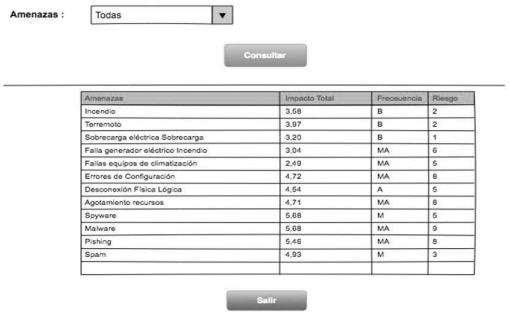

Figura 8. Riesgo de las amenazas de ciberseguridad

VI. CONCLUSIONES

En este artículo, se presentan las características y particularidades identificadas de las herramientas para la gestión de riesgos en ciberseguridad para pequeñas empresas, así como los requisitos y el proceso del prototipo elaborado, como una alternativa para el análisis y gestión de riesgos en ciberseguridad para pequeñas empresas.

De las herramientas de análisis y gestión de riesgos en ciberseguridad revisadas, ninguna de ellas relaciona las vulnerabilidades de ciberseguridad con los activos. Un elemento importante que identifica a este prototipo es el análisis 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.

La validación del prototipo y la implementación final como herramienta, se espera realizar en Ecuador, donde se cuenta con empresas para realizar los ensayos finales. Como resultado de los ensayos, se espera mejorar la interfaz de usuario a fin de lograr una mejor experiencia de usuario.

El prototipo desarrollado en el presente trabajo, a diferencia de las aplicaciones analizadas, no cuenta aún con un nombre comercial. Las pequeñas empresas necesitan el acceso a soluciones completas, de bajo coste y que les permitan gestionar el riesgo.

Como conclusión final, podemos indicar que en la actualidad existe una deficiencia de sistemas informáticos orientados a la gestión de vulnerabilidades de ciberseguridad, pues la gran mayoría se enfocan únicamente en las amenazas de ciberseguridad.

REFERENCIAS BIBLIOGRÁFICAS

[1] Mendoza, M.A., ¿Ciberseguridad o seguridad de la información? Aclarando la diferencia, "https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/", consultado el 12 de febrero de 2018, 12 am.

[2] Scott E. Donaldson, Stanley G. Siegel, Chris K. Williams, Abdul Aslam. New York, NY: "Enterprise Cybersecurity: How to Build a Successful Cyberdefense Program Against Advanced Threats", pp 24-25, 2015.

[3] Ponemon Institute, 2015 Cost of Cyber Crime Study: Global, Recuperado de "http://engage.hpe.com/PDFViewer?ID={81e3f9d9-32fc-43ba-907a-1fda52800f8a}_Cost_of_Cyber_Crime", consultado el 15 de Diciembre de 2017.

[4] 7799BS, Code of Practice for Information Security Management, Department of Trade and Industry, DISC PD003, British Standard Institute, London, UK (1995)

[5] ISO/IEC 27000:2009, "Information technology — Security techniques — Information security management systems — Overview and vocabulary".

[6] NIST SP 800-53 Rev.4, NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 (including updates as of January 15, 2014). http://dx.doi.org/10.6028/NIST.SP.800- 53r4.

[7] GARTNET, "https://www.gartner.com/reviews/market/software-asset-management-tools", consultado el 20 d emarzo de 2018, 10 am.

[8] GARTNET, "https://www.gartner.com/reviews/market/vulnerability-assessment", consultado el 21 marzo de 2018, 10 am.

[9] GARTNET, "https://www.gartner.com/reviews/market/unified-threat-management-worldwide", consultado el 19 d emarzo de 2018, 10 am.

[10] CCN-CERT, "https://www.ccn-cert.cni.es/herramientas-de-ciberseguridad/ear-pilar/pilar.html. Rceuperado el 20 enero de 2018, 11 am.

[11] ENISA,"https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools/t_risicare.html", recuperado el 16 enero 2018, 10 am.

[12] Microsoft,"https://technet.microsoft.com/es-es/security/cc185712.aspx", recuperado el 15 enero 2018, 10 am.

[13] IBM,"https://www.ibm.com/es-es/marketplace/ibm-qradar-siem", recuperado el 16 enero 2018, 11 am.

[14] SOFTEXPERT, https://www.softexpert.es/produto/gestion-riesgos-controles/, recuperado el 20 enero de 2018, 11 am.

[15] UNE 71504 UNE 71504:2008, "Metodología de análisis y gestión de riesgos para los sistemas de informa-ción".

[16] 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.

[17] ISO 73 ISO Guie 73:2009, "Risk management — Vocabulary". UNE-ISO Guía 73:2010, "Gestión del riesgo. Vocabulario