# PROYECTO FIN DE GRADO

**TÍTULO**: Mecanismo de validación de los resultados del Análisis de Riesgos de un dispositivo IoT médico.

**AUTOR/A:** Javier García Vida

**TITULACIÓN**: Ingeniería Telemática

**DIRECTOR/A**: Gustavo Alberto Gallo Arroyo

**TUTOR/A**: Pedro Castillejo Parrilla

**DEPARTAMENTO**: Ingeniería Telemática y Electrónica

**VºBº TUTOR/A**

**Miembros del Tribunal Calificador:**

**PRESIDENTE/A**: Julia María García Luengo

**TUTOR/A**: Pedro Castillejo Parrilla

**SECRETARIO/A**: Iván Pau de la Cruz

**Fecha de lectura:** 17 de julio de 2024

**Calificación:**

**El Secretario/La Secretaria,**

**Resumen**

En los últimos años, la conversión tecnológica de todas las herramientas que utilizamos a diario ha supuesto una mejora en nuestras vidas en cuanto a comodidad y eficiencia. Algunos objetos han pasado a tener la capacidad de conectarse a la red y funcionar como un pequeño ordenador convencional, como son los denominados dispositivos IoT (Internet de las cosas).

Sin embargo, esta situación ventajosa provoca un gran contrapeso: cualquier dispositivo que nos rodea es capaz de almacenar datos personales valiosos, lo que provoca que hayan crecido de forma abrupta los ataques a los mismos.

En este contexto de crecimiento exponencial del riesgo en los dispositivos IoT, un grupo concreto de ellos, formado por los denominados dispositivos IoT médicos o dispositivos IoMT, destaca por encima del resto. El alto valor que le da la sociedad a la salud, especialmente desde la pandemia ocurrida en el año 2020, se ve reflejado en estudios que, cuatro años después de la pandemia, mantienen la salud como la segunda mayor preocupación de los españoles y provoca que estos dispositivos reúnan todas las condiciones para ser atacados.

Ante esta situación, este proyecto plantea crear un marco normativo de seguridad, inspirado en el Esquema Nacional de Seguridad, que se aplique de forma específica a dispositivos IoMT. Además, el objetivo es automatizar un Análisis de Riesgos con unas cuestiones de seguridad básicas que puedan ser respondidas por el personal técnico sanitario que trabaja a diario con el dispositivo, obviando los parámetros de seguridad más complejos, para los cuales se requiere tener conocimientos en ciberseguridad o en programación.

Los resultados de ese Análisis de Riesgos darán lugar a un programa cuya interfaz gráfica mostrará los resultados de la evaluación de seguridad del dispositivo IoMT, seguidos de una lista ordenada, por prioridad, de las sugerencias de seguridad que se deberían aplicar en el dispositivo, según los cálculos internos realizados.

El objetivo final es que el personal técnico sanitario, utilizando dicho programa, sea capaz de aplicar esos cambios o bien de solicitarlos, ya con conocimiento de causa, a su organización.

La utilización de esta aplicación, idealmente, provocaría un aumento generalizado en la seguridad básica de los dispositivos IoMT de aquellas organizaciones que decidieran utilizarla, como paso previo a la contratación de servicios especializados de ciberseguridad, que ya comenzarían con su labor encontrándose una mejor base de seguridad y solo terminarían por encargarse de los aspectos más complejos y especializados de seguridad del dispositivo.

En el caso de organizaciones con pocos recursos económicos, pocos dispositivos IoMT o pertenecientes a lugares subdesarrollados o incomunicados, que no puedan permitirse el coste de un servicio especializado de ciberseguridad, esta herramienta (y sus futuras mejoras) supondría también elevar el nivel básico de seguridad.

Además, el proyecto pretende también colaborar con la formación en seguridad del personal sanitario, por lo que incluye explicaciones detalladas de las razones por las que una mejora de seguridad es relevante y qué riesgos evita.

**Abstract**

In recent years, the technological conversion of all the tools we use daily has led to an improvement in our lives in terms of comfort and efficiency. Some objects have come to have the ability to connect to the network and function like a small conventional computer, such as the so-called IoT (*Internet of Things*) devices.

However, this advantageous situation causes a great counterbalance: any device around us is capable of storing valuable personal data, which causes attacks on them to have grown abruptly.

In this context of exponential growth in risk in IoT devices, a specific group of them, formed by the so-called medical IoT devices or IoMT devices, stands out above the rest. The high value that society places on health, especially since the pandemic that occurred in 2020, reflected in studies that, four years after the pandemic, maintain health as the second greatest concern of Spaniards, causes this type of devices meet all the conditions to be attacked.

Given this situation, this project proposes creating a security regulatory framework, inspired by the National Security Scheme, which is specifically applied to IoMT devices. Furthermore, the objective is to automate a Risk Analysis with basic security questions that can be answered by the technical health personnel who work daily with the device, ignoring the more complex security parameters, for which knowledge in cybersecurity or in programming is required.

The results of this Risk Analysis will give rise to a program whose graphical interface will show the results of the security evaluation of the IoMT device, followed by an ordered list, by priority, of the security suggestions that should be applied to the device, according to the internal calculations carried out.

The final objective is that the technical health personnel, using said program, can be able to apply these changes or request them, already with knowledge of the facts, to their organization.

The use of this application, ideally, would cause a general increase in the basic security of the IoMT devices of those organizations that decide to use it, as a prior step to hiring specialized cybersecurity services, which would already begin their work, finding a better base of security and would only end up taking care of the more complex and specialized security aspects of the device.

In the case of organizations with few economic resources, few IoMT devices or those which belong to underdeveloped or isolated places, which cannot afford the cost of a specialized cybersecurity service, this tool (and its future improvements) would also mean raising the basic level of security.

In addition, the project also aims to collaborate with the safety training of healthcare personnel, which is why it includes detailed explanations of the reasons why a safety improvement is relevant and what risks it avoids.

# ÍNDICE DE CONTENIDO

Índice de Tablas ..... 9
Índice de Figuras ..... 10
Índice de Anexos ..... 11
Lista de Acrónimos ..... 13
1 Introducción ..... 15
1.1 Objetivos ..... 16
2 Estado del Arte ..... 17
2.1 Características de IoT ..... 17
2.2 Dispositivos IoMT ..... 18
2.3 Principales riesgos de seguridad en los dispositivos IoT ..... 19
2.4 Principales riesgos de seguridad en los dispositivos IoMT ..... 21
2.5 Legislación y Normativa existente para dispositivos IoT ..... 22
2.5.1 ISO/IEC 30141:2018 ..... 22
2.5.2 Guía del INCIBE para Seguridad en la instalación y uso de dispositivos IoT ..... 23
2.5.3 ISO/IEC 27400:2022 ..... 23
2.5.4 Ley de Ciberresiliencia de la Comisión Europea ..... 24
2.5.5 Guía del Ministerio del Interior sobre Seguridad en dispositivos IoT ..... 24
2.6 Legislación y Normativa existente para dispositivos IoMT ..... 24
2.6.1 Reglamento UE 2017/745 (MDR) ..... 25
2.6.2 ISO 14971 ..... 25
2.6.3 NIST Special Publication 800-53 ..... 25
2.7 Controles pertinentes del ENS para dispositivos IoMT ..... 26
2.7.1 Marco organizativo ..... 26
2.7.2 Marco operacional – Planificación ..... 27
2.7.3 Marco operacional – Control de acceso ..... 27
2.7.4 Marco operacional – Explotación ..... 28
2.7.5 Marco operacional – Recursos externos ..... 29
2.7.6 Marco operacional – Servicios en la nube ..... 29
2.7.7 Marco operacional – Continuidad del servicio ..... 29
2.7.8 Marco operacional – Monitorización del sistema ..... 30
2.7.9 Medidas de protección – Protección de las instalaciones e infraestructuras ..... 30
2.7.10 Medidas de protección – Gestión del personal ..... 31
2.7.11 Medidas de protección – Protección de los equipos ..... 31
2.7.12 Medidas de protección – Protección de las comunicaciones ..... 31

2.7.13 Medidas de protección – Protección de los soportes de información ..... 32
2.7.14 Medidas de protección – Protección de las aplicaciones informáticas ..... 32
2.7.15 Medidas de protección – Protección de la información ..... 32
2.7.16 Medidas de protección – Protección de los servicios ..... 33
2.8 Aplicaciones existentes de Análisis de Riesgos ..... 34
2.8.1 PILAR ..... 34
2.8.2 BowTieXP ..... 35
2.8.3 RiskWatch ..... 36
2.8.4 Asimily Risk Simulations ..... 37
2.8.5 Comparativa y aportación de la herramienta propuesta ..... 38
3 Diseño de la solución propuesta: Análisis de Riesgos ..... 41
3.1 Restricciones del proyecto ..... 41
3.2 Creación de un marco normativo para el Análisis de Riesgos ..... 42
3.2.1 Identificación y acceso ..... 43
3.2.2 Mecanismos de autenticación ..... 43
3.2.3 Acceso local y remoto ..... 44
3.2.4 Inventario de activos ..... 44
3.2.5 Registro de incidentes ..... 45
3.2.6 Registro de la actividad ..... 45
3.2.7 Plan de continuidad ..... 45
3.2.8 Pruebas periódicas ..... 45
3.2.9 Control de acceso ..... 45
3.2.10 Identificación del personal ..... 46
3.2.11 Acondicionamiento del área ..... 46
3.2.12 Energía eléctrica ..... 46
3.2.13 Protección frente a incendios ..... 46
3.2.14 Protección frente inundaciones ..... 47
3.2.15 Responsabilidad en el puesto de trabajo ..... 47
3.2.16 Concienciación y formación ..... 47
3.2.17 Bloqueo del dispositivo ..... 47
3.2.18 Protección del dispositivo ..... 48
3.2.19 Protección de datos personales ..... 48
3.2.20 Mantenimiento del dispositivo ..... 48
3.3 Forma de evaluación utilizada en el Análisis de Riesgos ..... 49
3.3.1 Análisis de impacto de cada categoría ..... 51

3.3.2 Ponderación de los niveles y categorías ..... 61
3.4 Creación del cuestionario para el Análisis de Riesgos ..... 63
4 Implementación y validación de la solución propuesta ..... 81
4.1 Automatización del Análisis de Riesgos ..... 82
4.2 Solución desarrollada ..... 83
4.2.1 Clase VentanaCuestionario ..... 84
4.2.2 Clase VentanaResultados ..... 86
4.3 Pruebas realizadas para comprobar el correcto funcionamiento del programa ..... 87
4.4 Comparativa de resultados del Análisis de Riesgos con una solución existente ..... 91
4.4.1 Análisis de Riesgos realizado por expertos en ciberseguridad ..... 91
4.4.2 Análisis de Riesgos realizado con la herramienta creada ..... 94
4.4.3 Conclusiones de la comparativa de resultados ..... 96
5 Presupuesto ..... 97
5.1 Costes de equipo y software ..... 97
5.2 Costes de recursos humanos ..... 97
5.3 Coste total ..... 97
6 Impacto del proyecto ..... 99
6.1 Identificación de impactos y aspectos éticos, sociales y ambientales ..... 99
6.2 Implicaciones éticas, sociales y ambientales ..... 100
6.3 Objetivos de Desarrollo Sostenible ..... 101
7 Conclusiones ..... 103
8 Trabajos futuros ..... 105
9 Referencias ..... 107
10 Anexos ..... 111

Índice de Tablas

Tabla 1: Comparativa de herramientas de Análisis de Riesgos ..... 39
Tabla 2: Identificación y acceso ..... 51
Tabla 3: Mecanismos de autenticación ..... 52
Tabla 4: Acceso local y remoto ..... 52
Tabla 5: Inventario de activos ..... 53
Tabla 6: Registro de incidentes ..... 53
Tabla 7: Registro de la actividad ..... 54
Tabla 8: Plan de continuidad ..... 54
Tabla 9: Pruebas periódicas ..... 55
Tabla 10: Control de acceso ..... 55
Tabla 11: Identificación del personal ..... 56
Tabla 12: Acondicionamiento del área ..... 56
Tabla 13: Energía eléctrica ..... 57
Tabla 14: Protección frente a incendios ..... 57
Tabla 15: Protección frente a inundaciones ..... 58
Tabla 16: Responsabilidad en el puesto de trabajo ..... 58
Tabla 17: Concienciación y formación ..... 59
Tabla 18: Bloqueo del dispositivo ..... 59
Tabla 19: Protección del dispositivo ..... 60
Tabla 20: Protección de datos personales ..... 60
Tabla 21: Mantenimiento del dispositivo ..... 61
Tabla 22: Costes de equipo y software ..... 97
Tabla 23: Coste de recursos humanos ..... 97
Tabla 24: Coste total ..... 97
Tabla 25: Escenario de análisis de impacto ..... 99
Tabla 26: Aspectos relevantes del impacto del proyecto ..... 101

Índice de Figuras

Figura 1: Preocupaciones principales de los españoles en 2024 [3] .....15
Figura 2: Evolución del número de dispositivos IoT (miles de millones) [6] .....17
Figura 3: Número de dispositivos IoT por sector [13] .....21
Figura 4: Aplicación PILAR [22] .....34
Figura 5: Aplicación BowTieXP [23] .....35
Figura 6: Aplicación RiskWatch [24] .....36
Figura 7: Asimily Risk Simulations [25] .....37
Figura 8: Transformación del método de cinco niveles del NIST.....49
Figura 9: Diagrama de clases UML.....83
Figura 10: Ventana del cuestionario.....84
Figura 11: Envío del cuestionario y selección de número de sugerencias .....85
Figura 12: Prueba con nivel máximo de seguridad.....87
Figura 13: Prueba con el nivel mínimo de seguridad .....88
Figura 14: Prueba aleatoria de seguridad.....89
Figura 15: Comprobación prueba aleatoria.....90
Figura 16: Ejemplo de evaluación (I).....91
Figura 17: Ejemplo de evaluación (II).....92
Figura 18: Valoración final (I).....92
Figura 19: Valoración final (II).....93
Figura 20: Valoración final (III).....93
Figura 21: Valoración final (IV).....93
Figura 22: Gráfico de resultados.....94
Figura 23: Resultados del Análisis de Riesgos propio .....95
Figura 24: Objetivos de desarrollo sostenible .....102

Índice de Anexos

Anexo 1: Programa Principal .....111
Anexo 2: Ventana del cuestionario.....112
Anexo 3: Ventana de los resultados .....115

Lista de Acrónimos

| | |
|---|---|
| **AEPD** | *Agencia Española de Protección de Datos* |
| **BOE** | *Boletín Oficial del Estado* |
| **CCN** | *Centro Criptológico Nacional* |
| **DPD** | *Delegado de Protección de Datos* |
| **ENS** | *Esquema Nacional de Seguridad* |
| **IA** | *Inteligencia Artificial* |
| **IEC** | *International Electrotechnical Commission* |
| **INCIBE** | *Instituto Nacional de Ciberseguridad de España* |
| **IoMT** | *Internet of Medical Things* |
| **IoT** | *Internet of Things* |
| **IP** | *Internet Protocol* |
| **ISO** | *International Organization for Standardization* |
| **LOPDGDD** | *Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales* |
| **LSE** | *Ley de Secretos Empresariales* |
| **LSSI** | *Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico* |
| **MAC** | *Media Access Control* |
| **MAGERIT** | *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información* |
| **MDR** | *Medical Device Regulation* |
| **NDA** | *Non-disclosure agreement* |
| **NIST** | *National Institute of Standards and Technology* |
| **ODS** | *Objetivos de Desarrollo Sostenible* |
| **ONU** | *Organización de las Naciones Unidas* |
| **PILAR** | *Procedimiento Informático y Lógico de Análisis de Riesgos* |
| **RGPD** | *Reglamento General de Protección de Datos* |
| **TIC** | *Tecnologías de la Información y la Comunicación* |
| **UE** | *Unión Europea* |
| **VPN** | *Virtual Private Network* |

# 1 Introducción

La seguridad de los dispositivos IoMT (*Internet of Medical Things* o Internet de las Cosas Médicas) es una preocupación creciente en el mundo de la salud, ya que los métodos para atacar estos dispositivos evolucionan constantemente, lo que provoca que los trabajadores sanitarios no estén preparados para responder a dichos ataques. El 70% de los dispositivos ni siquiera cuenta con soporte técnico, debido a quedarse anticuados u obsoletos, lo cual aumenta la cuota de responsabilidad que recae sobre el trabajador sanitario a la hora de prevenir un ataque [1].

El incremento anual de ciberataques cada año a dispositivos conectados a Internet es un mal sufrido por todos los sectores. Sin embargo, el sector de la salud se ha convertido en una diana para este tipo de ataques, especialmente desde que la pandemia del COVID-19 [2] mostrase al mundo la necesidad de un buen funcionamiento de los sistemas sanitarios y el peligro cuando estos colapsan.

En enero de 2024 [3] la sanidad fue la segunda mayor preocupación de los españoles, lo que demuestra que, incluso superada la pandemia, la sociedad seguirá priorizando el funcionamiento del sector salud por encima de otros sectores.

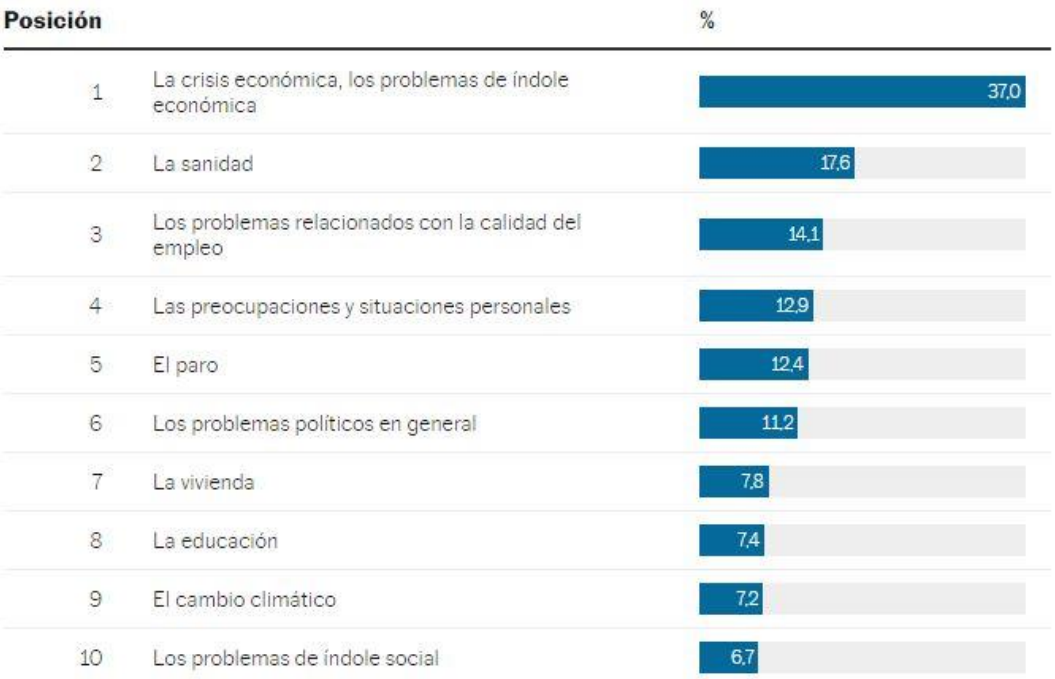



Figura 1: Preocupaciones principales de los españoles en 2024 [3]

En consecuencia, el volumen de entidades sanitarias afectadas por ciberataques también crece cada año. Un estudio [4] realizado en 39 países, entre los que se encuentra España, determinó que hasta el 78% de organizaciones sufrieron al menos un ataque relevante en los últimos doce meses. Este problema se agrava aún más al observar que el 61% de los ataques involucraron de forma directa al tratamiento o al cuidado de los pacientes y el 15% supuso, de forma contrastable, un impacto perjudicial en la salud del paciente.

A este factor principal, el humano, cabe añadir el económico. Este estudio señala que el sector de la salud es el sector que más dinero perdió por cada ciberataque en 2022. En España, más de 600 hospitales sufrieron algún ataque durante dicho año y el coste medio por recuperar los datos osciló entre los 94.000€ y los 470.000€. Se estima, además, que existe un 13% de aumento de coste anual.

Por otro lado, el hecho de que el 47% de todos los ciberataques a las organizaciones de la salud comprometan a los dispositivos médicos, pone en valor la necesidad de protegerlos. Esta protección comienza desde la base de la cadena: la concienciación y formación del propio personal sanitario.

Además de mejorar las normativas de seguridad y los protocolos con los proveedores, las organizaciones sanitarias deben cuestionarse si realmente ofrecen a los trabajadores todas las posibilidades que están en sus manos para prevenir los ataques [5]. Ante esta tesitura, adquiere una especial importancia conseguir que los sanitarios sean capaces de detectar situaciones de claro riesgo e incluso de solventarlas, en la medida de lo posible.

## 1.1 Objetivos

El objetivo principal de este proyecto es desarrollar un mecanismo de validación de los resultados del Análisis de Riesgos de un dispositivo IoMT que permita a los trabajadores del área del sector de la salud conocer un listado ordenado, en base a la prioridad, de los cambios que deberían hacer o solicitar a su organización para maximizar las condiciones de seguridad de dicho dispositivo.

Para llevar a cabo el objetivo principal se definen los siguientes objetivos específicos:

- Automatizar los riesgos a los que puede estar expuesto un dispositivo IoMT.
- Validar las pruebas señalando de forma gráfica los resultados obtenidos del Análisis de Riesgos.
- Aportar un resultado que guíe a los trabajadores sanitarios, sin necesidad de conocimientos en ciberseguridad, a adoptar las medidas necesarias para mejorar la seguridad del dispositivo.
- Garantizar el cumplimiento de las medidas de seguridad internacionales para el tratamiento adecuado de los datos clínicos almacenados.

# 2 Estado del Arte

En este capítulo se va a realizar un estudio de los principales riesgos de seguridad documentados en dispositivos IoT (*Internet of Things* o Internet de las Cosas), profundizando en los dispositivos IoT médicos, y se va a analizar la normativa de seguridad existente para dispositivos IoT e IoMT.

Con la información recopilada, se estudiará la posible adaptación de dicha normativa en el marco del ENS (Esquema Nacional de Seguridad), con el objetivo de seleccionar los controles pertinentes del ENS, que impliquen a los dispositivos IoMT, que se utilizarán en la segunda fase para desarrollar un Análisis de Riesgos propio.

## 2.1 Características de IoT

IoT o Internet de las Cosas es una red de objetos y dispositivos que tienen la capacidad de conectarse entre sí y conectarse a Internet para enviar o recibir datos.

Inicialmente la conexión era de forma inalámbrica, mediante *Wi-Fi*, pero hoy en día encontramos dispositivos equipados con sensores, software y otras tecnologías que permiten el procesamiento y almacenamiento de datos, además de tener la capacidad de compartirlos en tiempo real.

Se estima que en 2021 ya existían diez mil millones de dispositivos IoT en el mundo [6] y que esta cifra se habrá triplicado en 2030. Este incremento continuo evidencia el crecimiento masivo que está teniendo esta tecnología, hasta el punto de que, en países como España, ya existen hasta siete veces más dispositivos IoT que personas.

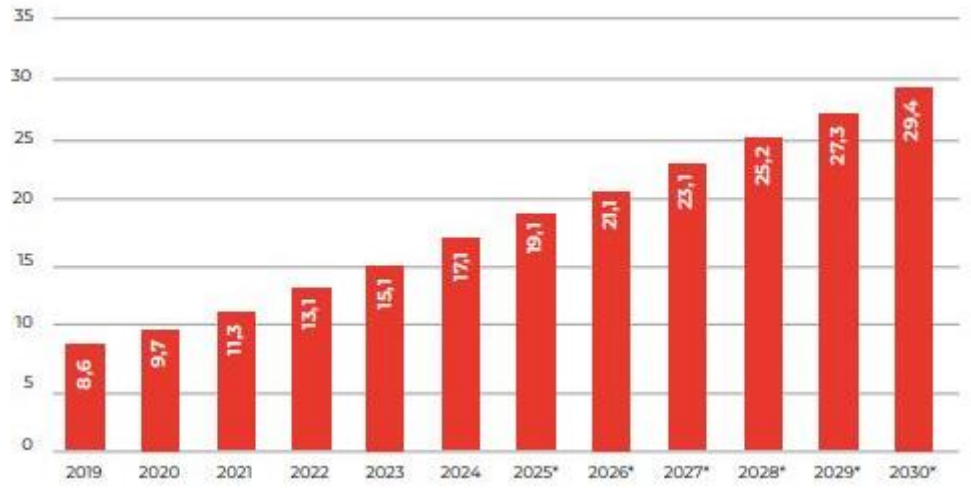



Figura 2: Evolución del número de dispositivos IoT (miles de millones) [6]

Los dispositivos IoT deben ser capaces de capturar, compartir y procesar los datos, y actuar a partir de los resultados obtenidos. Su versatilidad es tal que está presente en todo tipo de sectores: agricultura, comercio, medicina e incluso en los propios hogares.

El factor decisivo para esta evolución tan rápida del número de dispositivos IoT fue la unión y el avance conjunto de distintas tecnologías:

- **Conectividad:** El avance de las tecnologías de conexión a Internet y a la nube, tanto en acceso como en velocidad, permite actualmente conectar gran cantidad de dispositivos a la red de forma simultánea y transmitir o recibir datos al instante.

- **Sensores:** En los últimos veinte años el precio de los sensores para IoT ha caído un 70%, lo que, junto al aumento de funcionalidades y diversidad de los productos, ha mejorado la accesibilidad a los mismos.

- **Computación:** Se estima que, solo en los próximos cinco años, se crearán dos veces más datos [6] que todos los datos creados desde el inicio del almacenamiento digital. Esta evolución, junto con el incipiente desarrollo de las tecnologías de *Big Data,* Inteligencia Artificial, *machine learning* y computación en la nube, ha multiplicado las opciones y calidad de la computación.

## 2.2 Dispositivos IoMT

Un dispositivo IoMT es la aplicación sanitaria de un dispositivo IoT, por lo que se puede definir como un dispositivo médico capaz de conectarse a internet para transferir información sobre los pacientes [7].

Bajo el concepto de IoMT conviven tanto los dispositivos como las aplicaciones médicas dedicadas a la digitalización y atención, actuación e investigación de los procesos sanitarios.

Los principales beneficios que aportan son:

- **Información en tiempo real** sobre el estado del paciente.

- **Seguimiento personalizado** del paciente, que permite modificar tratamientos.

- **Mayor eficiencia** en los recursos médicos disponibles, traduciéndose en una reducción de costes.

- **Reducción de errores** de diagnóstico, aplicación de tratamientos y errores humanos tales como falta de atención, errores de medición o errores de cálculo.

- **Reducción del tiempo** de atención médica, minimizando las listas de espera y permitiendo adelantar cirugías urgentes.

Además, los dispositivos IoMT se pueden clasificar en distintos tipos, según su estructura y su funcionalidad:

- **Telemedicina:** Estos dispositivos prestan servicios sanitarios de forma remota, de forma que pueden estar presentes en zonas poco accesibles o simplemente en lugares con pocos recursos económicos o tecnológicos que no puedan contar físicamente con las herramientas médicas necesarias. Con la telemedicina también es posible tratar a los pacientes sin que tengan que desplazarse al centro médico, siendo especialmente beneficioso para gente con problemas de movilidad o de dependencia.

- ***Wearables*:** Son dispositivos médicos que lleva el propio paciente en su cuerpo, interior o exteriormente, para medir sus datos vitales. La información es enviada a la nube en tiempo real y permite la monitorización a distancia por parte del médico del paciente.

- **Drones:** Permiten entregar medicamentos, productos médicos o muestras de sangre. Son capaces de informar de su localización y del tiempo invertido en la entrega.

- **Realidad aumentada:** Estos dispositivos permiten combinar la realidad virtual con entornos reales. Es especialmente útil para la formación del personal sanitario, al cual se le puede entrenar mediante escenarios virtuales, recreados con gran precisión, a situaciones que podrán vivir en el futuro de forma real. También es clave para la rehabilitación de los pacientes, debido a sus características que permiten reducir el estrés y distraer el dolor.

- **Inteligencia Artificial y *Big Data*:** Los dispositivos IoMT, en su conexión a internet, son capaces de generar una gran cantidad de información, compartida con otros dispositivos o con el personal sanitario. El manejo de esta información de manera inteligente permite procesar los datos y convertirlos en estadísticas o valores que aporten un conocimiento real. Esto permite detectar enfermedades de forma precoz o incluso extraer información de patrones que coincidan con factores de riesgo de suicidios, alcoholismo o consumo de drogas.

## 2.3 Principales riesgos de seguridad en los dispositivos IoT

El 86% de los problemas de seguridad de los dispositivos IoT son calificados [8] como críticos, lo cual evidencia que la forma más eficiente de enfrentar los riesgos es con prevención, ya que solventar una brecha de seguridad crítica puede suponer necesitar conocimientos avanzados, un gran desembolso económico o una importante cantidad de tiempo.

Los mayores errores [9] que cometen las organizaciones que gestionan algún dispositivo IoT son los siguientes:

- No tener un plan de seguridad y protección de la privacidad.

- Centrarse solo en la tecnología y no en los riesgos de seguridad.

- Tener dispositivos que no incluyen una capa de seguridad o esta es poco robusta.
- Falta de conciencia ante las vulnerabilidades del sistema.
- Monitorización insuficiente del dispositivo.
- Ausencia de mantenimiento.
- Falta de inventario y control de los productos.
- Falta de identificación y tratamiento de riesgos en productos heredados.
- Procesos de respuesta a incidentes inexistentes o inmaduros.

Se puede observar cómo la dinámica de estos errores es que se producen por falta de conocimiento o falta de atención. No saber que un riesgo existe, o simplemente despreciar su potencial gravedad, es un comportamiento habitual de las organizaciones que trabajan con dispositivos IoT. Resulta complicado, por tanto, que los empleados tengan herramientas para conocer y prevenir los riesgos, cuando la propia organización no siempre centra su atención en dicho problema.

A causa de ello, el 36% de las compañías [10] admite haber sufrido ataques por parte de terceros en sus dispositivos IoT.

Los ataques típicos que reciben los dispositivos IoT son los siguientes:

- **Espionaje:** Los atacantes pueden tomar control de los micrófonos, las cámaras u otro tipo de datos del uso del dispositivo para recopilar información sobre los usuarios sin su permiso. Además de recopilar información, el objetivo del atacante es no alertar al usuario, de forma que actúe con naturalidad y pueda obtener la información de forma precisa.
- **Ataques de Denegación de Servicio**: En ocasiones los atacantes pueden bloquear el uso del dispositivo y hacer que permanezca inutilizable durante un tiempo. Esto puede provocar graves pérdidas económicas para la organización, cuando la resolución de algunas tareas depende de que el dispositivo deje de estar paralizado.
- **Rapto del dispositivo:** Además del robo físico del dispositivo, se entiende por rapto a la toma de control del mismo sin autorización, con el fin de tomar acciones o simplemente de exigir un rescate económico.

En ocasiones, el ataque a un dispositivo IoT no se realiza como meta sino como puente o punto de entrada [11] para atacar un segundo dispositivo, que es realmente el objetivo, a través del primero.

## 2.4 Principales riesgos de seguridad en los dispositivos IoMT

Además de los riesgos previstos para los dispositivos IoT, existen riesgos adicionales que podemos encontrar cuando vinculamos estos dispositivos a organizaciones dedicadas a la salud médica.

El principal riesgo adicional que encontramos, frente a los dispositivos IoT convencionales, es el hecho de involucrar a pacientes cuyos estados de salud pueden llegar a depender, de forma parcial o total, del correcto funcionamiento de uno o varios dispositivos IoMT. El gran factor diferencial es que, si bien en una empresa estándar se pueden terminar recuperando las pérdidas económicas sufridas por un ataque, empeorar el estado de salud de una vida humana puede terminar en un desenlace grave o incluso irrecuperable.

La implementación de dispositivos IoMT crece cada año en hospitales y organizaciones de la salud, facilitando tareas tales como la extracción de sangre, monitorización del oxígeno en la cama del paciente, automatización de la administración de medicamentos o la emisión de alertas médicas al puesto de control, especialmente útil para pacientes ingresados con movilidad reducida que no tienen compañía nocturna en su habitación.

El pensamiento de que el uso de los dispositivos IoMT supone una innovación en la industria de la salud y mejora la atención al paciente [12] está muy extendido. Sin embargo, este pensamiento convive con la preocupación de los trabajadores sanitarios de que unos dispositivos IoMT desatendidos o inseguros supongan una puerta de entrada sencilla para los atacantes, que termine repercutiendo en consecuencias graves para el estado de salud de los pacientes.

Se estima [13] que en 2027 se llegará a la cifra de mil millones de dispositivos IoT médicos, lo que convertirá a este sector en uno de los punteros dentro de la tecnología IoT.

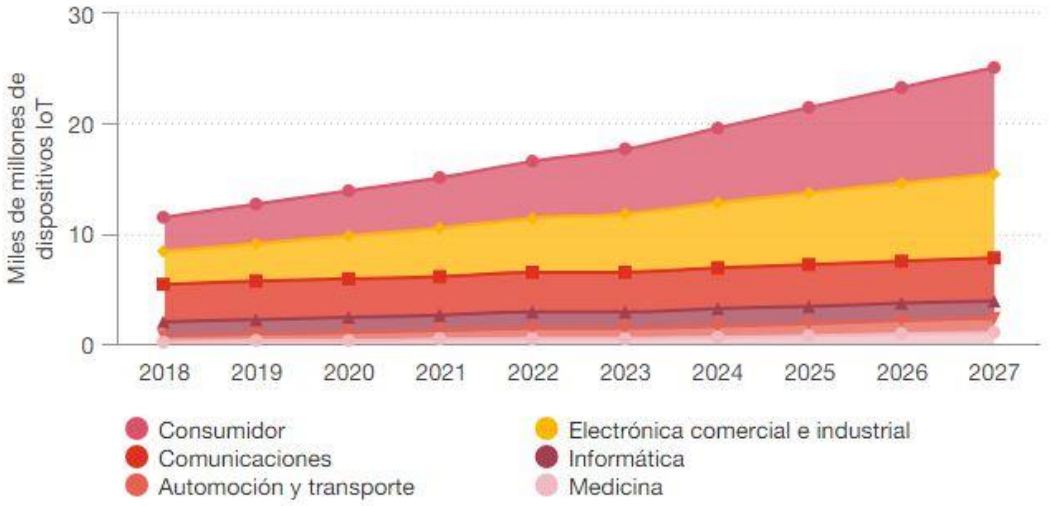



Figura 3: Número de dispositivos IoT por sector [13]

Algunas de las grandes dificultades que entraña la tecnología IoT en medicina se deben a la falta de certificación de los dispositivos IoMT. El proceso de certificación es el que gestiona aspectos tales como:

- **Defensa de los dispositivos:** Los proveedores son los responsables de la inversión en sistemas de seguridad de calidad, que deben ser evaluados por seguridad eléctrica, de software y mecánica, de forma que se corrobore su nivel de protección ante ataques por entidades independientes.

- **Priorizar al paciente:** Tanto la salud del paciente como salvaguardar sus datos clínicos y personales deben ser el foco de los sistemas de seguridad. Los atacantes son conocedores de ello y aprovechan que las organizaciones anteponen la salud del paciente al beneficio económico, pidiendo así rescates tras ataques de *ransomware* (secuestro de datos) en situaciones delicadas.

- **Normativa:** Los dispositivos IoMT deben cumplir con ciertas regulaciones, pero en ocasiones es demasiado costoso para el proveedor, por lo que el dispositivo queda desactualizado y sin soporte.

- **Conectividad e interoperabilidad:** Los dispositivos deben ser compatibles entre sí y cumplir con ciertos protocolos de comunicación.

- **Rendimiento:** Los dispositivos deben ofrecer información fiable, ya que en muchas ocasiones un error puede ser crítico.

## 2.5 Legislación y Normativa existente para dispositivos IoT

El aumento del uso de dispositivos IoT, así como el incremento de los ataques a estos dispositivos, ha forzado que en los últimos años se haya comenzado a desarrollar legislación y normativa que regule el correcto uso y protección de los mismos.

Si bien estamos en el inicio de la era IoT, desde 2018, con la publicación de la normativa ISO/IEC 30141, se ha observado un incremento en la publicación de normativas, leyes y guías respecto a la utilización de dispositivos IoT. En este capítulo se pretende repasar las principales y analizar sus aspectos positivos y negativos en cuanto a su utilidad para cumplir los objetivos de este proyecto.

### 2.5.1 ISO/IEC 30141:2018

Publicada en agosto de 2018, la norma ISO/IEC 30141 sobre el Internet de las Cosas (IoT) – Arquitectura de Referencia proporciona un marco de referencia para diseñadores y desarrolladores de aplicaciones IoT [14].

Esta norma supuso el primer estándar internacional sobre IoT publicado por la ISO (*Internacional Organization for Standardization* u Organización Internacional de

Normalización) y tuvo como objetivo garantizar una gestión eficiente de la automatización de los sistemas, para poder controlar el cambio irruptivo de la tecnología IoT, que hasta entonces crecía sin una normativa internacional a sus espaldas y no ponía freno a la aparición de nuevas vulnerabilidades.

Respecto a la utilidad para el proyecto, el punto positivo es que esta norma es el punto de partida de las normativas internacionales sobre IoT y puede dar un enfoque claro sobre cuáles eran las vulnerabilidades principales y básicas.

Como punto negativo, esta norma está centrada en el propio desarrollo y diseño de los dispositivos, algo bastante alejado del propósito del proyecto, que tiene como objetivo guiar a los trabajadores sanitarios, sin necesidad de conocimientos en el desarrollo de dispositivos IoT, a hacer un uso seguro de los mismos, independientemente del nivel de seguridad con el que estos hayan sido creados.

### 2.5.2 Guía del INCIBE para Seguridad en la instalación y uso de dispositivos IoT

Publicada en 2020, la guía del INCIBE (Instituto Nacional de Ciberseguridad) tiene como objetivo [11] facilitar la protección de las empresas que cuentan con dispositivos IoT.

Al estar centrada en las amenazas para el dispositivo y en la vulneración de la privacidad, llegando incluso a tener un apartado enfocado a los usuarios y al acceso seguro, puede ser de gran utilidad para el desarrollo de este proyecto, y servir como punto de apoyo para determinar las principales vulnerabilidades que pueden sufrir estos dispositivos.

Sin embargo, el lenguaje empleado puede llegar a ser demasiado técnico para trabajadores que no tengan conocimientos en ciberseguridad o tecnología en general, que es, en definitiva, el público objetivo de este proyecto. Es en ese apartado donde se pretende conseguir una visión más sencilla y guiada que aporte al trabajador sanitario unas consignas claras y que estén a su alcance.

### 2.5.3 ISO/IEC 27400:2022

Publicada 7 de junio del 2022, esta norma proporciona medidas técnicas y organizativas para la seguridad y la privacidad de la tecnología IoT [15]. Tiene como objetivo proporcionar controles de seguridad adecuados para mitigar los riesgos existentes.

Esta norma desempeña un papel relevante en cuanto a concienciación tanto para el proveedor como para el cliente, y se puede extraer información importante para el proyecto en cuanto a la normativa sobre protección de datos personales, algo especialmente relevante si hablamos de datos personales clínicos.

Por otro lado, si bien esta norma se centra algo más en el usuario, sigue siendo demasiado técnica para que sea el propio usuario, en el caso de este proyecto, el que sea capaz de interpretarla y de tomar medidas de seguridad al respecto por sí solo.

### 2.5.4 Ley de Ciberresiliencia de la Comisión Europea

Publicada el 15 de septiembre de 2022, la Ley de Ciberresiliencia o Reglamento sobre los requisitos de ciberseguridad de los productos con elementos digitales tiene como objetivo reforzar las normas de ciberseguridad para garantizar la seguridad de productos hardware y software con conectividad a internet, tras analizar la Comisión Europea el alto coste que suponían los ciberataques exitosos, superando la cifra de cinco billones de euros, a nivel mundial, en el año anterior al nacimiento de esta ley [16].

Esta ley tiene como objetivos solventar la baja ciberseguridad incentivando el desarrollo de productos seguros y combatir la falta de información para los usuarios, lo cual es un objetivo que se comparte en este proyecto.

Sin embargo, el hecho de que sea una ley y no un marco normativo amplio que evalúe de forma individual cada caso, hace que no cumpla definitivamente la totalidad de los objetivos de este proyecto.

### 2.5.5 Guía del Ministerio del Interior sobre Seguridad en dispositivos IoT

Publicada el 2 de agosto del 2023, esta guía de reciente creación agrupa distintas normativas nacionales e internacionales sobre dispositivos IoT, y tiene como objetivo ofrecer una visión amplia acerca del estado actual de la seguridad en dichos dispositivos [17].

Uno de los grandes aspectos positivos de esta guía es que recolecta varias normativas y presenta un resumen actualizado de recomendaciones y buenas prácticas.

Sin embargo, el documento en general es bastante informativo y genérico, lo que no permitiría cumplir con el objetivo de este proyecto de ofrecer al trabajador sanitario respuestas individuales para cada dispositivo en cada situación concreta.

## 2.6 Legislación y Normativa existente para dispositivos IoMT

La legislación y normativa existente para dispositivos IoT es escasa y muy reciente. En 2013, la Comisión Europea publicó una estrategia para el desarrollo del Internet de las Cosas (IoT) que incluía aspectos regulatorios y de política. El documento, titulado "*A Digital Agenda for Europe*" mencionaba la necesidad de abordar la privacidad, la seguridad y otros aspectos relacionados con el IoT.

El nacimiento de la primera norma ISO al respecto, la ISO/IEC 30141:2018, seis años antes de la redacción del presente documento, refleja que la normativa que detalla la correcta aplicación de estos dispositivos, concretamente para el ámbito de la salud, aún está evolucionando y no es suficientemente específica para algunos sectores.

Aunque no existen leyes o normativas internacionales específicamente dedicadas a dispositivos IoMT, existen algunas que, o bien porque se centran en la salud e incluyen dispositivos IoT o bien porque se centran en dispositivos IoT e incluyen su aplicación en la salud, reflejan en sus documentos las primeras directrices sobre este tipo de dispositivos:

### 2.6.1 Reglamento UE 2017/745 (MDR)

El Reglamento de Productos Sanitarios (MDR) de la Unión Europea, vigente desde mayo de 2021, regula los requisitos para la comercialización y vigilancia de los dispositivos médicos en Europa, incluyendo los dispositivos IoMT. El MDR establece normas estrictas sobre la seguridad, el rendimiento y la trazabilidad de los dispositivos, así como las obligaciones de los fabricantes, distribuidores e importadores. Requiere la implementación de un sistema de gestión de riesgos, la realización de evaluaciones clínicas y la vigilancia post-comercialización para garantizar la seguridad y eficacia continuas. [18]

En este caso, este reglamento está enfocado en la comercialización y en la fabricación, elementos que no son aplicables a la finalidad de este proyecto.

### 2.6.2 ISO 14971

La norma ISO 14971 proporciona un marco para la gestión de riesgos de los productos sanitarios, incluyendo los dispositivos IoMT. Esta norma describe un proceso sistemático para identificar los peligros asociados con los dispositivos médicos, evaluar los riesgos relacionados, controlar estos riesgos y monitorizar la efectividad de los controles a lo largo del ciclo de vida del producto. Esta norma es relevante para cumplir con los requisitos regulatorios globales y garantizar que los dispositivos médicos sean seguros para su uso previsto. [19]

De nuevo, es una normativa que no puede servir para guiar a trabajadores sanitarios, ya que hace énfasis en regulaciones y seguridad a nivel legal, no tanto práctica.

### 2.6.3 NIST Special Publication 800-53

El NIST SP 800-53 es un conjunto de directrices desarrolladas por el Instituto Nacional de Estándares y Tecnología (NIST) de EE.UU. para la seguridad y privacidad de los sistemas de información. Esta publicación proporciona un catálogo de controles de seguridad y privacidad que pueden aplicarse a dispositivos IoMT para proteger la información sensible y garantizar la seguridad del sistema. Los controles abarcan aspectos como la gestión de accesos, la autenticación, la auditoría, la integridad de los datos y la gestión de incidentes. Estos controles ayudan a asegurar que los dispositivos IoMT cumplan con los requisitos de seguridad y privacidad en entornos regulatorios estrictos. [20]

En este caso, esta norma presenta aspectos útiles que se pretenden tratar en el marco normativo de este proyecto, tales como la gestión de accesos, la autenticación y la gestión de incidentes. Dado que además su descarga es gratuita, el único punto negativo residiría

en que su naturaleza no está estrictamente pensada para los conocimientos de ciberseguridad exigibles a un trabajador sanitario.

Además, el NIST, a diferencia del ENS, centra su normativa en la protección de los activos, sin hacer énfasis en las infraestructuras y otros aspectos que rodean al activo (el dispositivo IoMT).

## 2.7 Controles pertinentes del ENS para dispositivos IoMT

En este capítulo se va a repasar uno por uno cada control presente en las Medidas de Seguridad del Anexo II del ENS para evaluar si su contenido es pertinente para el proyecto o si debe descartarse por no ajustarse a los objetivos que se pretenden conseguir.

La pertinencia de cada control para el proyecto se basará, de forma resumida, en el cumplimiento de los siguientes puntos:

- El control es aplicable a dispositivos IoMT.
- No se necesita de la participación activa del proveedor del dispositivo.
- No se necesitan conocimientos avanzados de ciberseguridad.
- No se necesitan conocimientos avanzados en legislación.
- No se necesitan conocimientos avanzados de programación ni se requiere alterar el software del dispositivo.
- No se necesita modificar las políticas de la organización o interferir en contratos.

En definitiva, el objetivo es que el técnico sanitario responsable del dispositivo sea capaz de responder por sí solo (o con pequeñas consultas a sus compañeros de la organización) a las cuestiones planteadas en el Análisis de Riesgos. Además, deberá ser capaz de tomar la mayoría de las medidas que se le aconsejarán al final del proyecto, en el listado de propuesta de cambios prioritarios, siendo que un número mínimo de ellas requerirán de la participación de la organización.

Para ello se tomará como referencia la última versión publicada en el BOE (Boletín Oficial del Estado): el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad [21].

### 2.7.1 Marco organizativo

El marco organizativo está constituido por un conjunto de medidas relacionadas con la organización global de la seguridad. Principalmente, este control refiere a políticas de seguridad y otras decisiones administrativas que dependen de la gestión de la empresa o

la organización. Por este motivo, este control no se ha determinado como relevante en el contexto del proyecto, que está centrado en la toma de decisiones a baja escala.

Aun así, todos los aspectos que se tratan en las políticas de seguridad se desglosan de forma más detallada en otros controles, en los que sí es posible que el trabajador sanitario encargado de gestionar el dispositivo IoMT pueda involucrarse y realizar cambios.

### 2.7.2 Marco operacional – Planificación

La planificación del marco operacional está constituida por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

- [op.pl.1] Análisis de Riesgos: Este control, que hace referencia al propio Análisis de Riesgos, se tendrá en cuenta para realizar de forma correcta la automatización del mismo.

- [op.pl.2] Arquitectura de Seguridad: Este control no se ha determinado como relevante para el proyecto porque excede de las competencias de un trabajador sanitario.

- [op.pl.3] Adquisición de Nuevos Componentes: Este control no se ha determinado como relevante para el proyecto porque cada Análisis de Riesgos está enfocado en un único dispositivo IoMT.

- [op.pl.4] Dimensionamiento/Gestión de la Capacidad: Este control no se ha determinado como relevante para el proyecto porque excede de las competencias de un trabajador sanitario.

- [op.pl.5] Componentes Certificados: Este control no se ha determinado como relevante para el proyecto porque cada Análisis de Riesgos está enfocado en un único dispositivo IoMT.

### 2.7.3 Marco operacional – Control de acceso

El control de acceso comprende el conjunto de actividades preparatorias y ejecutivas que llevan a permitir o denegar a una entidad, usuario o proceso, el acceso a un recurso del sistema para la realización de una acción concreta.

- [op.acc.1] Identificación: Este control es relevante para el proyecto. Su contenido se refleja en la categoría de **Identificación y Control de acceso.**

- [op.acc.2] Requisitos de Acceso: Este control es relevante para el proyecto. Su contenido se refleja en la categoría de **Identificación y Control de acceso.**

- [op.acc.3] Segregación de Funciones y Tareas: Este control es relevante para el proyecto, particularmente en el ámbito de que un trabajador no pueda darse

acceso a sí mismo. Su contenido se refleja en la categoría de **Identificación del personal.**

- [op.acc.4] Proceso de Gestión de Derechos de Acceso: Este control se ha descartado porque hace referencia a competencias de la organización.

- [op.acc.5] Mecanismos de Autenticación: Este control es relevante para el proyecto. Su contenido se refleja en la categoría de **Mecanismos de autenticación.**

- [op.acc.6] Acceso Local: Este control es relevante para el proyecto. Su contenido se refleja en la categoría de **Acceso local y remoto.**

- [op.acc.7] Acceso Remoto: Este control es relevante para el proyecto. Su contenido se refleja en la categoría de **Acceso local y remoto.**

### 2.7.4 Marco operacional – Explotación

La explotación comprende multitud de temáticas sobre registros y gestión de las actividades realizadas.

- [op.exp.1] Inventario de Activos: Este control es relevante para el proyecto. Su contenido se refleja en la categoría de **Inventario de activos.**

- [op.exp.2] Configuración de seguridad: Este control se descarta para el proyecto porque hace referencia a la configuración que ha realizado el proveedor en el dispositivo IoMT.

- [op.exp.3] Gestión de la configuración de seguridad: Este control se descarta para el proyecto porque hace referencia a la configuración que ha realizado el proveedor en el dispositivo IoMT.

- [op.exp.4] Mantenimiento y actualizaciones de seguridad: Este control es relevante para el proyecto. Su contenido se refleja en la categoría de **Mantenimiento del dispositivo.**

- [op.exp.5] Gestión de cambios: Este control se descarta para el proyecto porque no se pretenden hacer cambios en el software del dispositivo, ya que excede de las competencias del técnico sanitario que se encargue del mismo.

- [op.exp.6] Protección frente a código dañino: Este control se descarta para el proyecto porque hace referencia al uso de antimalware y otras medidas avanzadas de seguridad que exceden de las competencias básicas exigibles al técnico del dispositivo.

- [op.exp.7] Gestión de Incidentes: Este control es relevante para el proyecto. Su contenido se refleja en la categoría de **Registro de incidentes.**

- [op.exp.8] Registro de la Actividad: Este control es relevante para el proyecto. Su contenido se refleja en la categoría de **Registro de la actividad.**

- [op.exp.9] Registro de gestión de incidentes: Este control es relevante para el proyecto. Su contenido se refleja en la categoría de **Registro de incidentes.**

- [op.exp.10] Protección de claves criptográficas: Este control se descarta para el proyecto, ya que el conocimiento de claves criptográficas y algoritmos de cifrado de datos excede de los conocimientos exigibles a los trabajadores sanitarios.

### 2.7.5 Marco operacional – Recursos externos

Este tema comprende aspectos que surgen cuando la organización utiliza recursos externos (servicios, productos, instalaciones o personal), debiendo adoptar las medidas necesarias para ejercer su responsabilidad y mantener el control en todo momento.

- [op.ext.1] Contratación y acuerdos de nivel de servicio: Este control se descarta para el proyecto porque hace referencia al cumplimiento de acuerdos con el proveedor.

- [op.ext.2] Gestión diaria: Este control se descarta para el proyecto porque hace exige comunicación con el proveedor.

- [op.ext.3] Protección de la cadena de suministro: Este control se descarta para el proyecto porque exige comunicación con el proveedor.

- [op.ext.4] Interconexión de sistemas: Este control se descarta para el proyecto porque hace referencia a una situación global que engloba varios sistemas diferentes.

### 2.7.6 Marco operacional – Servicios en la nube

Este control hace referencia a la protección de los servicios en la nube, pero implica tomar medidas relativas a seguridad de la red que no son exigibles a un trabajador sin conocimientos avanzados en ciberseguridad.

### 2.7.7 Marco operacional – Continuidad del servicio

La continuidad del servicio hace referencia a la protección de los datos en caso de que un servicio o dispositivo quede interrumpido o inhabilitado.

- [op.cont.1] Análisis de impacto: Este control se descarta porque la labor de realizar un Análisis de Impacto es propia de un experto en ciberseguridad.

- [op.cont.2] Plan de continuidad: Este control es relevante para el proyecto. Su contenido se refleja en la categoría de **Plan de Continuidad.**

- [op.cont.3] Pruebas periódicas: Este control es relevante para el proyecto. Su contenido se refleja en la categoría de **Pruebas periódicas.**

- [op.cont.4] Medios alternativos: Este control es relevante para el proyecto. Su contenido se refleja en la categoría de **Plan de Continuidad.**

### 2.7.8 Marco operacional – Monitorización del sistema

Este grupo hace referencia a las medidas de monitorización de un sistema y la ejecución de acciones predeterminadas en función de las situaciones de compromiso de la seguridad que figuren en el análisis de riesgos. Los controles de este grupo incluyen aspectos de responsabilidad que incumben a especialistas en ciberseguridad o a programadores que gestionen el tráfico de red, por lo que no se alinean con la finalidad de este trabajo.

### 2.7.9 Medidas de protección – Protección de las instalaciones e infraestructuras

Las medidas de protección estarán dirigidas a proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad. En concreto, este grupo hace referencia a la protección de las instalaciones e infraestructuras de la organización.

- [mp.if.1] Áreas separadas y con control de acceso: Este control es relevante para el proyecto. Su contenido se refleja en la categoría **Control de acceso**.

- [mp.if.2] Identificación de las personas: Este control es relevante para el proyecto. Su contenido se refleja en la categoría **Identificación del personal**.

- [mp.if.3] Acondicionamiento de los locales: Este control es relevante para el proyecto. Su contenido se refleja en la categoría **Acondicionamiento del área.**

- [mp.if.4] Energía eléctrica: Este control es relevante para el proyecto. Su contenido se refleja en la categoría **Energía eléctrica**.

- [mp.if.5] Protección frente a incendios: Este control es relevante para el proyecto. Su contenido se refleja en la categoría **Protección frente a incendios.**

- [mp.if.6] Protección frente a inundaciones: Este control es relevante para el proyecto. Su contenido se refleja en la categoría **Protección frente a inundaciones**.

- [mp.if.7] Registro de entrada y salida de equipamiento: Este control se descarta para el proyecto, ya que está pensado para la entrada y salida de equipamiento, tal como ordenadores portátiles o dispositivos extraíbles. En el caso de los dispositivos IoMT no deberían salir de las instalaciones y su salida por robo ya se contempla en otros controles.

### 2.7.10 Medidas de protección – Gestión del personal

La Gestión del personal abarca problemáticas que surgen de la interacción de los trabajadores con el puesto o material de trabajo.

- [mp.per.1] Caracterización del puesto de trabajo: Este control es relevante para el proyecto. Su contenido se refleja en la categoría **Responsabilidad en el puesto de trabajo.**

- [mp.per.2] Deberes y obligaciones: Este control es relevante para el proyecto. Su contenido se refleja en la categoría **Responsabilidad en el puesto de trabajo.**

- [mp.per.3] Concienciación: Este control es relevante para el proyecto. Su contenido se refleja en la categoría **Concienciación y formación.**

- [mp.per.4] Formación: Este control es relevante para el proyecto. Su contenido se refleja en la categoría **Concienciación y formación.**

### 2.7.11 Medidas de protección – Protección de los equipos

La Protección de los equipos incluye los controles que hacen referencia al uso correcto de los equipos a los que tiene acceso un trabajador.

- [mp.eq.1] Puesto de trabajo despejado: Este control se descarta para el proyecto porque hace referencia a un puesto de trabajo típico, en el que se tiene una mesa para trabajar. En el caso de los dispositivos IoMT, el propio puesto de trabajo es el dispositivo.

- [mp.eq.2] Bloqueo de puesto de trabajo: Este control es relevante para el proyecto. Su contenido se refleja en la categoría **Bloqueo del dispositivo.**

- [mp.eq.3] Protección de dispositivos portátiles: Este control es relevante para el proyecto. Su contenido se refleja en la categoría **Protección del dispositivo.**

- [mp.eq.4] Otros dispositivos conectados a la red: Este control se descarta para el proyecto, ya que hace referencia a “otros dispositivos” y este Análisis de Riesgos se centra exclusivamente en un dispositivo (cada vez que se realiza). Los aspectos relacionados con la conexión a la red del dispositivo se tienen en cuenta en todos los controles pertinentes.

### 2.7.12 Medidas de protección – Protección de las comunicaciones

La Protección de las comunicaciones hacen referencia a la seguridad a nivel de red de las comunicaciones. Estos controles requieren de amplios conocimientos en ciberseguridad o programación para poder aplicarlos, tales como saber segregar el tráfico en la red o el empleo de VPN (*Virtual Private Network* o Red Privada Virtual) cifradas. Como este

desempeño no puede ser exigible a un técnico sanitario, se ha descartado la profundización en estos controles para realizar este proyecto.

### 2.7.13 Medidas de protección – Protección de los soportes de información

Este grupo de controles tiene como objetivo detallar el buen uso de los soportes de información. Como este proyecto se centra en la protección de los dispositivos IoMT, es necesario descartar estos controles que implican actuaciones para soportes de información concretos.

### 2.7.14 Medidas de protección – Protección de las aplicaciones informáticas

La protección de las aplicaciones informáticas hace referencia a la programación segura del software al crear una aplicación, por lo que sus controles no son pertinentes para el propósito de este proyecto, que busca proteger dispositivos IoMT ya creados y programados por su fabricante y que, además, tiene la restricción de no poder exigir conocimientos avanzados de programación al técnico sanitario responsable de la gestión del dispositivo.

### 2.7.15 Medidas de protección – Protección de la información

La protección de la información incumbe todos aquellos aspectos que tengan que ver con la difusión de información y su uso.

- [mp.info.1] Datos Personales: Este control es relevante para el proyecto. Su contenido se refleja en la categoría **Protección de datos personales.**

- [mp.info.2] Calificación de la información: Este control se descarta para el proyecto, ya que la calificación de la información la debe otorgar un experto en ciberseguridad y, en cualquier caso, un dispositivo IoMT solo gestiona información clínica de los pacientes y datos personales de los mismos.

- [mp.info.3] Firma electrónica: Este control se descarta para el proyecto, ya que no es aplicable a dispositivos IoMT.

- [mp.info.4] Sellos de tiempo: Este control se descarta para el proyecto, ya que no es aplicable a dispositivos IoMT.

- [mp.info.5] Limpieza de documentos: Este control se descarta para el proyecto, ya que hace referencia a metadatos y otros factores que exceden de las competencias de un técnico sanitario.

- [mp.info.6] Copias de seguridad: Este control es relevante para el proyecto. Su contenido se refleja en la categoría **Plan de continuidad.**

### 2.7.16 Medidas de protección – Protección de los servicios

La protección de los servicios trata de preservar la seguridad en servicios como el correo electrónico o la navegación web. Aunque un dispositivo IoMT pueda tener acceso a estos servicios, en realidad la seguridad de los mismos no puede recaer sobre el trabajador sanitario que está gestionando el dispositivo, ya que excede de sus competencias.

## 2.8 Aplicaciones existentes de Análisis de Riesgos

En este apartado se han analizado algunas de las aplicaciones automatizadas existentes en Análisis de Riesgos, tratando de evaluar sus aspectos positivos y negativos, con el fin de reunir la mayor cantidad de los aspectos positivos, y evitar los negativos, en la aplicación final de este proyecto.

### 2.8.1 PILAR

La herramienta PILAR (Plataforma Integral para la Localización y Análisis de Riesgos) es un software especializado en el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) y está desarrollada y financiada parcialmente por el CCN. Esta herramienta es utilizada principalmente por organizaciones y empresas para identificar, evaluar y gestionar los riesgos asociados a sus operaciones, infraestructuras y activos críticos. [22]

La ventaja de esta aplicación es que ya está alineada con los estándares del ENS y permite agilizar el proceso de valoración de los activos. Además, tiene un cálculo interno del nivel de riesgo que permite indicar la valoración de los controles y grupos de controles.

El punto negativo es que es una herramienta pensada para expertos en ciberseguridad, hasta el punto de que la valoración de los activos y de los controles del ENS se hace mediante seis niveles de madurez determinados por el experto, que debe conocer cada uno de los controles y salvaguardas en profundidad. Por ello, deben utilizarla profesionales que dominan el significado que implica asignar un determinado nivel de madurez a una categoría.

Al mismo tiempo, es una herramienta antigua y genérica que no permite adaptar su categorización de forma ideal para adaptarla a la evaluación de un dispositivo IoMT.

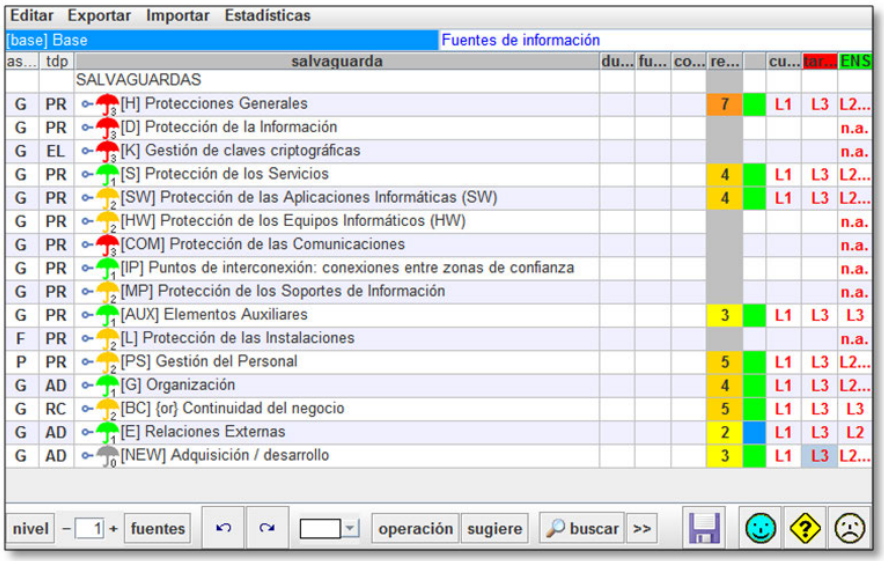



Figura 4: Aplicación PILAR [22]

### 2.8.2 BowTieXP

BowTieXP es una herramienta avanzada de gestión de riesgos que utiliza el modelo de diagrama de lazo para visualizar las relaciones entre riesgos, causas, consecuencias y controles.

El diagrama de lazo, conocido también como "BowTie", que da nombre a esta aplicación, es una herramienta visual utilizada en la gestión de riesgos para analizar y demostrar las relaciones causales en situaciones de alto riesgo. Este método ayuda a identificar y gestionar tanto las causas potenciales de un evento indeseado (amenazas) como las posibles consecuencias del mismo, facilitando una priorización de los aspectos de seguridad que deben resolverse. En general, la aplicación BowTieXP es especialmente útil para análisis detallados y comunicación de riesgos. [23]

Como aspecto positivo, cabe destacar la complejidad de esta herramienta y la posibilidad de trabajar en castellano con ella, aunque no permite realizar el Análisis de Riesgos con el marco normativo del ENS.

Sin embargo, esa misma complejidad se aleja del objetivo del proyecto de acercar al personal médico el Análisis de Riesgos, ya que necesita de la participación de un experto en ciberseguridad.

Por otro lado, su configuración tampoco permite realizar una evaluación de un dispositivo IoMT con la categorización y los riesgos adecuados.

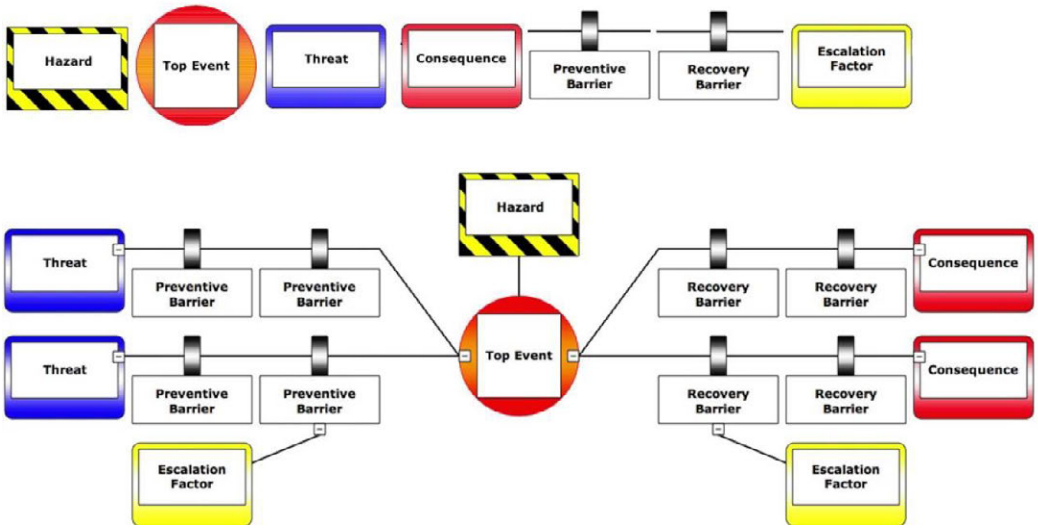



Figura 5: Aplicación BowTieXP [23]

### 2.8.3 RiskWatch

RiskWatch es una herramienta bien valorada por su enfoque visual y práctico en la gestión de riesgos, utilizando también el modelo de diagrama de lazo y gráficos variados para la presentación de resultados. Su aplicación es transversal en industrias de alto riesgo como la aviación, la minería, y el petróleo y gas, donde la claridad y la facilidad de comprensión son cruciales para la seguridad operacional. [24]

La ventaja de esta aplicación es que uno de esos sectores de riesgo con los que está habituada a trabajar es con el sector salud, así como la utilización de IA avanzada para realizar los análisis.

Al mismo tiempo, permite realizar un Análisis de Riesgos guiado sin exigir conocimientos avanzados en ciberseguridad, aunque sí se requieren conocimientos de legislación, normativa y programación de software.

Por otro lado, a pesar de ser utilizada habitualmente en el sector salud, no está enfocada de manera directa en los dispositivos IoMT y tampoco ofrece actualmente una versión en castellano ni permite regirse por el marco normativo del ENS.


Figura 6: Aplicación RiskWatch [24]

### 2.8.4 Asimily Risk Simulations

El software Asimily Risk Simulations [25] es una herramienta especializada en detección de riesgos, siendo la única en el mercado que obtiene soluciones únicas para dispositivos IoMT.

El Análisis de Riesgos, creado por la empresa estadounidense, permite seleccionar marcos normativos basados en el NIST y en ISO/IEC, aunque no en el ENS ni tiene aún una versión en castellano.

Como aspectos positivos, la herramienta tiene una interfaz gráfica en la que se representan los resultados de forma visual y clara, y se ofrecen sugerencias de mejora para los aspectos de seguridad que fallan.

En general, la herramienta destaca porque permite identificar y analizar las vulnerabilidades presentes en los dispositivos médicos y otros sistemas IoT. Esto incluye vulnerabilidades de seguridad conocidas, debilidades en la configuración y problemas de diseño.

Sin embargo, la complejidad de los parámetros analizados no permite que el Análisis de Riesgos sea realizado por trabajadores sanitarios que no tengan amplios conocimientos en ciberseguridad. Además, las sugerencias ofrecidas también necesitan de un elevado nivel técnico para ponerlas en práctica, y no siguen ningún orden prioritario.


Figura 7: Asimily Risk Simulations [25]

### 2.8.5 Comparativa y aportación de la herramienta propuesta

A continuación, se realizará una tabla comparativa con los aspectos positivos y negativos de cada aplicación existente y se pondrá en valor la aportación de la herramienta propuesta como una solución útil para solventar los aspectos negativos del resto de aplicaciones.

En el contexto del proyecto, se busca una herramienta que sea capaz de cumplir los siguientes aspectos:

- **Realizar un Análisis de Riesgos específico para dispositivos IoMT:** Tener un Análisis de Riesgos específico para un tipo de activos permite centrarse en los riesgos que les afectan de manera concreta, darles mayor importancia, eliminar riesgos genéricos que no afecten a estos dispositivos e incluir los nuevos riesgos específicos.

- **Facilitar que el Análisis de Riesgos sea completado por el propio trabajador que utiliza y conoce el dispositivo, sin necesidad de contratar un experto en ciberseguridad:** Cumplir este requisito permite que la organización se ahorre costes en la contratación de un experto de seguridad y, así, cualquier organización sin grandes recursos económicos tenga la oportunidad de incrementar el nivel básico de seguridad de sus dispositivos. Incluso si se desea contratar un servicio de ciberseguridad, es positivo para la organización iniciarlo con un nivel mínimo de seguridad, para ahorrar tiempo y costes más altos.

- **Mostrar unos resultados gráficos que permitan a cualquier usuario entender a simple vista si el nivel de seguridad es alto o bajo:** El trabajador sanitario debe poder conocer, de manera simple, si el nivel de seguridad es alto o bajo, sin tener que descifrar códigos o nomenclaturas complejas que no son propias de su campo de trabajo. De esta forma, podrá tener una visión comparativa cada vez que evalúe el dispositivo y podrá comprobar cómo cambian los niveles de seguridad.

- **Mostrar una lista personalizada de los cambios prioritarios necesarios para mejorar la seguridad del dispositivo analizado en función de los resultados obtenidos:** Lo que da valor a realizar un Análisis de Riesgos es facilitar que las vulnerabilidades detectadas sean solucionadas de forma eficaz y rápida. Para ello es preciso ordenar las vulnerabilidades en función de la urgencia que exige su resolución. Esto, además, no solo facilita que la medida prioritaria se realice antes que si no se indicara su prioridad, sino que el simple hecho de presentar un orden prioritario permite a la organización estructurar de forma más rápida su plan que si recibiese un amplio listado de cambios sin ningún orden.

- **Regirse por un marco normativo que cumpla el Esquema Nacional de Seguridad:** Tener un marco normativo basado en el ENS permite que la herramienta pueda ser utilizada por cualquier organización pública española, ya que es de obligado cumplimiento para ellas.

- **Estar disponible en lenguaje castellano:** Este factor es importante, teniendo en cuenta que se espera que el Análisis de Riesgos sea completado por trabajadores sanitarios que no necesariamente dominan el inglés.

Atendiendo al cumplimiento de dichos requisitos, se realiza la siguiente comparativa:

| | PILAR | BowTieXP | RiskWatch | Asimily Risk Simulations | Herramienta propuesta PFG |
|---|---|---|---|---|---|
| **Análisis de Riesgos específico para IoMT** | ✗ | ✗ | ✗ | ✓ | ✓ |
| **Análisis de Riesgos no necesita experto en ciberseguridad** | ✗ | ✗ |  | ✗ | ✓ |
| **Muestra resultados gráficos sencillos** |  | ✓ | ✓ | ✓ | ✓ |
| **Sugiere cambios prioritarios** | ✗ | ✓ |  |  | ✓ |
| **Cumple ENS** | ✓ | ✗ | ✗ | ✗ | ✓ |
| **Castellano** | ✓ | ✓ | ✗ | ✗ | ✓ |

Tabla 1: Comparativa de herramientas de Análisis de Riesgos

Tras analizar la tabla comparativa, la única herramienta existente en el mercado que es capaz de realizar Análisis de Riesgos específicos para dispositivos IoMT es Asimily Risk Simulations.

Sin embargo, esta herramienta está diseñada para la evaluación de expertos en ciberseguridad, no permite regirse por un marco normativo que cumpla el ENS y no permite configurarse en castellano.

En cuanto a las sugerencias de cambios que propone, no es capaz de priorizar unos cambios sobre otros ni son cambios que puedan realizarse por el propio técnico sanitario que trabaja con el dispositivo, debido a su complejidad.

Tampoco tiene en cuenta los cambios en el entorno del dispositivo o en protocolos que afecten al dispositivo, únicamente proporciona cambios en la configuración del mismo en base al número de vulnerabilidades en un campo de seguridad.

En el caso de RiskWatch, está más cerca de permitir que un usuario sin conocimientos en ciberseguridad pueda completar el Análisis de Riesgos debido a su interfaz interactiva, sin embargo, sí se necesitan conocer ciertos conceptos legales y de programación de software para responder con precisión al cuestionario. Además, igual que ocurre con Asimily, es capaz de proporcionar sugerencias de cambios que mejorarían la seguridad del activo evaluado, pero no las ordena en base a su prioridad.

BowTieXP, sin embargo, sí ofrece una lista ordenada de posibles mejoras de seguridad, además de mostrar los resultados de forma clara y tener una versión de la aplicación en castellano, pero no es suficiente para satisfacer los seis requisitos, ya que no contiene Análisis de Riesgos específicos para dispositivos IoMT, no pueden ser realizados por trabajadores sin conocimientos en ciberseguridad y tampoco sigue el marco normativo del ENS.

Por otro lado, PILAR solo cumple con la aplicación del ENS y del lenguaje en castellano. Sus resultados gráficos no son extremadamente complejos, pero atienden a la nomenclatura de los niveles de madurez (L0 a L5) que representan porcentajes que no tienen por qué ser intuitivos.

En conclusión, la herramienta creada en este proyecto permite cumplir todos los requisitos necesarios al mismo tiempo, demostrando ser la más útil para satisfacer los objetivos del proyecto. Concretamente, esta herramienta supone una innovación que aporta valor al sector salud español en un campo específico: la evaluación y mejora guiada de seguridad básica en dispositivos IoMT sin necesidad de contratar expertos de ciberseguridad.

# 3 Diseño de la solución propuesta: Análisis de Riesgos

Para desarrollar una solución que afronte los problemas expuestos en el apartado anterior se propone diseñar un Análisis de Riesgos, en el que se evaluarán ciertos parámetros de seguridad de un dispositivo IoMT concreto. Para ello, se creará un cuestionario guiado que deberá ser completado por el técnico sanitario, junto a su equipo, que gestione y utilice regularmente dicho dispositivo y que tenga acceso a la información del mismo. Las respuestas al cuestionario del Análisis de Riesgos serán automatizadas por un programa que guardará los resultados y, al finalizar, proporcionará un gráfico con la evaluación general, desglosado según diferentes áreas de seguridad seleccionadas (más adelante se detallará el modelo), y un listado ordenado de acciones, según su prioridad, que se deberían tomar para mejorar la situación del dispositivo IoMT en términos de seguridad.

El cuestionario debe estar pensado para evaluar exclusivamente información a la que el personal sanitario, sin amplios conocimientos en ciberseguridad, pueda responder con certeza. Es posible que ciertas respuestas requieran de un estudio de uso o de recopilación de información por parte del personal, pero en ningún caso debe ser necesario tener que consultar al proveedor del hardware o del software, ni tampoco a un experto en ciberseguridad.

Para resolver la problemática de las normativas y guías sobre IoT e IoMT, habitualmente pensadas para trabajadores con conocimientos en ciberseguridad, el listado que proporcionará el programa estará pensado para dar instrucciones sencillas y sin coste económico, buscando que cualquier técnico sanitario las pueda implementar. El propósito es maximizar la eficiencia, consiguiendo detectar qué acciones sencillas pueden suponer una notable mejoría en cuanto a la situación de riesgo a la que estaba expuesto el dispositivo antes de tomar dichas acciones. Además, a la hora de sugerir los cambios que deben realizarse, se añadirá una breve explicación, con la intención de contribuir a la formación en ciberseguridad del equipo sanitario.

Para aportar el gráfico con la evaluación del Análisis de Riesgos, así como para el listado de acciones a tomar, se buscará ponderar los parámetros de la forma más objetiva posible, documentando por qué se les atribuye cierto nivel de riesgo y por qué se prioriza tomar una acción sobre el dispositivo y no otra.

## 3.1 Restricciones del proyecto

En el anteproyecto se fijaron una serie de restricciones que debía satisfacer el proyecto final. En este apartado se analizará el cumplimiento de cada una de las restricciones iniciales:

- **Debe ser entendible y utilizable para cualquier trabajador sanitario sin conocimientos avanzados en tecnología o ciberseguridad:** Para que los resultados del Análisis de Riesgos sean de provecho, el cuestionario debe ser realizado, o al menos guiado, por el técnico sanitario encargado del dispositivo. Por lo tanto, los conocimientos en tecnología (o al menos en la tecnología que usa el dispositivo) son

necesarios para el proyecto. Por ello, se ha reformulado esta restricción quedando como “debe ser entendible y utilizable para cualquier trabajador sanitario sin conocimientos avanzados en programación o ciberseguridad”, manteniendo el espíritu del proyecto, pero siendo más precisos en la definición, que se cumple en todo momento.

- **Para el Análisis de Riesgos se utilizará como referencia el marco normativo del Esquema Nacional de Seguridad (ENS):** Se cumple esta restricción.
- **La forma de presentar el resultado de forma gráfica deberá estar lo más sujeta posible a la objetividad:** Se cumple esta restricción, ya que se argumenta en todo momento por qué se da cada valor a cada categoría de seguridad y a las cuestiones que la componen.
- **Deberán argumentarse de forma contrastable durante el trabajo (no necesariamente al usuario en la presentación de resultados) los motivos por los que se priorizan unos aspectos de seguridad sobre otros:** Se cumple esta restricción, ya que se argumenta siempre el motivo por el que unos aspectos de seguridad tienen más valor y cómo varía su prioridad dependiendo de la valoración que tenga cada uno de los cuatro niveles.
- **La presentación de resultados de forma gráfica, así como el listado de acciones prioritarias a tomar por parte del trabajador, se obtendrán a través de un programa codificado por el alumno:** Se cumple esta restricción, con un programa en código Java que presenta una interfaz gráfica con varias ventanas.

## 3.2 Creación de un marco normativo para el Análisis de Riesgos

En apartados previos se realizó un estudio de los controles del ENS que resultaban pertinentes para el objetivo del proyecto, que presenta dos grandes restricciones para el Análisis de Riesgos: debe enfocarse exclusivamente a riesgos existentes en dispositivos IoMT, tanto los comunes a otros equipos sanitarios como los propios por su conectividad a Internet, y al mismo tiempo debe estar dirigido a trabajadores sanitarios sin conocimientos en ciberseguridad ni en programación de software, de forma que puedan utilizar la aplicación final como una guía que les facilite minimizar los riesgos existentes.

A partir de la información recabada se ha establecido una estructura propia de 20 categorías, con el fin de generar un nuevo marco normativo básico pensado específicamente para los riesgos existentes en un dispositivo IoMT y para las condiciones limitantes del proyecto.

Cada categoría refleja los requisitos de seguridad para considerar al dispositivo seguro. Esos requisitos han sido establecidos tras realizar un estudio en profundidad, y adaptarlo a los objetivos y restricciones del proyecto, de los siguientes documentos:

- Guía de Seguridad de las TIC, CCN-STIC 804 [26]
- Guía de implantación del ENS que extiende el Real Decreto 311/2022 [21]

- Contenido de otras guías o normativas de IoT, analizadas previamente en el Estado del Arte, que puedan aportar riesgos relevantes para los dispositivos IoMT que no aparezcan en la Guía CCN-STIC 804.

A continuación, se detallan los requisitos de seguridad exigibles para cada una de las 20 categorías que forman parte del marco normativo:

### 3.2.1 Identificación y acceso

Cada trabajador sanitario que accede a un dispositivo IoMT debe hacerlo con un identificador único, de forma que se pueda identificar quién ha estado utilizando el dispositivo en un momento determinado.

Esa identificación debe ir asociada a una cuenta de usuario, de forma que no baste con anotar un identificador para acceder al dispositivo, sino que se compruebe que la persona que lo está utilizando tiene el derecho de hacerlo. Además, las cuentas deben ser inhabilitadas cuando el usuario deja la organización o cuando ya no está autorizado a realizar la tarea por lo que, si el identificador está asociado con la cuenta de usuario, la organización tiene el control inmediato para impedir el acceso a sus dispositivos.

Los identificadores no deben compartirse, sino que cada trabajador tiene el derecho de utilizar exclusivamente su identificador, salvo emergencia que lo justifique.

### 3.2.2 Mecanismos de autenticación

La autenticación es el mecanismo que permite validar la identidad de un usuario. Existen distintos tipos:

- Mecanismos basados en una información que se conoce (p.ej.: una contraseña).
- Mecanismos basados en un objeto que se posee (p.ej.: una llave).
- Mecanismos basados en algo que pertenece físicamente al usuario (p.ej.: huella biométrica).

Comúnmente, estos mecanismos pueden utilizarse a pares para dificultar la suplantación por parte de un tercero que hubiera descifrado el mecanismo inicial. Esto se conoce como autenticación de doble factor.

En el caso de un dispositivo IoMT, lo ideal es que exista un mecanismo de autenticación principal basado en la identificación del usuario por medio de su cuenta asociada a la organización y, por si el identificador y su contraseña fueran filtrados, exista un segundo factor de autenticación propio del dispositivo. Además, con ello se evita que, conociendo los identificadores de un trabajador, se tenga acceso a varios dispositivos diferentes.

Teniendo en cuenta que prácticamente la totalidad de los ataques a dispositivos IoMT suceden de forma remota, si bien no hay que abandonar la seguridad física del dispositivo,

no parece del todo eficiente la utilización de un mecanismo de autenticación basado en objetos, como llaves o tarjetas.

Por otro lado, un mecanismo basado en biometría es demasiado avanzado como para que la mayoría de los dispositivos IoMT cuenten con él.

Las credenciales, del mismo modo que los identificadores, no deben compartirse salvo en caso de emergencia. El usuario es responsable del uso que hace de ellas, esto incluye:

- Crear credenciales robustas.
- Custodiarlas de forma segura.
- Actualizarlas cada aproximadamente 3 meses.

### 3.2.3 Acceso local y remoto

A la hora de acceder a un dispositivo, por seguridad, debe limitarse el número de intentos seguidos con fallo de contraseña y, cuando se alcance dicho límite, debe bloquearse temporalmente al acceso.

Una vez se ha accedido al dispositivo, es importante que quede guardado en un registro qué persona y a qué hora se ha producido el acceso. Es conveniente que, cada vez que se realice un acceso, se informe al usuario, por un medio alternativo, del inicio de sesión. Esta medida de seguridad alertará al usuario cuando sea informado de que alguien ha iniciado sesión con su identidad y éste no haya protagonizado dicho acceso.

En caso de que el dispositivo permita el acceso remoto, la conexión deberá realizarse mediante la VPN corporativa de la organización sanitaria, evitando utilizar en todo momento redes Wi-Fi públicas.

### 3.2.4 Inventario de activos

Debe existir un inventario de dispositivos IoMT en el que se identifiquen aspectos como:

- Dónde está ubicado un dispositivo.
- Quién o quiénes son los responsables del dispositivo.
- Versión de software instalada.
- Fabricante del dispositivo.
- Proveedor del dispositivo.
- Tipo de conexión a la red.
- Equipamiento de red (MAC, IP).

Es posible que algunos de esos datos, siguiendo la lógica del proyecto, no se puedan exigir obtener a un trabajador sanitario estándar. Sin embargo, al ser todos datos estáticos, es probable que ya estén almacenados en cualquier otro documento creado en el momento de adquirir/actualizar el dispositivo y el trabajador sanitario solo tenga que recopilarlos o solicitar que la organización se los facilite.

### 3.2.5 Registro de incidentes

Uno de los aspectos más importantes que involucra de forma directa al personal sanitario es la gestión de incidentes. Cuando se produce un incidente, no siempre el propio sistema es capaz de reportarlo y que la información llegue al responsable de seguridad. Por ello, resulta clave que exista un procedimiento de reporte y actuación frente a incidentes, y que sea respetado y puesto en práctica por parte de todo el personal.

### 3.2.6 Registro de la actividad

El registro periódico de la actividad es una tarea con importancia ya que, al revisar el historial de accesos a un dispositivo, se puede obtener información que en vivo había pasado desapercibida, y detectar así anomalías que no se habían tenido en cuenta.

### 3.2.7 Plan de continuidad

El plan de continuidad define las funciones y actividades que se deben realizar, en caso de desastre, para tratar de maximizar la prestación de los servicios habituales.

### 3.2.8 Pruebas periódicas

Las pruebas periódicas del Plan de Continuidad permiten comprobar, en forma de simulacro, cómo funcionaría realmente el plan.

Estos simulacros se pueden realizar de forma parcial y comprobar, inutilizando a propósito un dispositivo, si funciona la recuperación de los datos mediante las copias de seguridad y si es posible replicar la labor de este dispositivo con otro alternativo o directamente sin dispositivos.

### 3.2.9 Control de acceso

El área en la que se encuentre el dispositivo IoMT debe estar delimitada, existiendo un inventario que determine qué personas están autorizadas a acceder, quiénes autorizan el acceso y cómo se vigila que estos accesos se cumplan.

Si el acceso a dicho área se realiza mediante el uso de llaves, tarjetas u otro tipo de credenciales físicas, en el inventario se debe incluir un registro de quién y en qué momento las tiene y se responsabiliza de su uso.

Adicionalmente deben existir medios que eviten el acceso por puntos alternativos al lugar en el que está establecido el control de acceso o fuera del horario laboral.

### 3.2.10 Identificación del personal

En las áreas de acceso restringido se debe verificar que la persona autorizada es realmente la misma que accede. Además, deben quedar registrados todos los accesos con la fecha de entrada y salida.

Es importante que la persona que solicita un acceso no sea la misma que lo autoriza, de este modo el proceso de autorización no sería neutral.

Periódicamente debe existir una revisión de las autorizaciones para verificar si sigue vigente el motivo por el cual se concedió cada autorización de acceso.

### 3.2.11 Acondicionamiento del área

El dispositivo debe estar en unas instalaciones que cumplan una serie de requisitos que verifiquen que su utilización sea adecuada.

El área en la que se usa el dispositivo debe respetar los márgenes de temperatura y humedad que establece el fabricante, debe estar protegida de amenazas externas, como daños procedentes de climatología adversa, y también de amenazas internas, como la presencia de otros dispositivos inflamables.

Por último, el cableado del dispositivo debe estar etiquetado, controlado y protegido.

### 3.2.12 Energía eléctrica

Deben existir medidas para solventar un potencial corte eléctrico que pueda comprometer el uso del dispositivo. Para ello debe existir un plan de emergencia y recuperación en el que se incluya el dispositivo.

Para afrontar dicha situación deben existir suministros alternativos como generadores u otros sistemas de alimentación.

### 3.2.13 Protección frente a incendios

Debe estudiarse si el entorno en el que está el dispositivo, esto incluye las instalaciones, el exterior, otros equipos y el propio dispositivo, tiene un riesgo de incendio elevado.

Para el caso en el que el incendio del dispositivo y del área en el que se encuentra no pudiera evitarse, en dicha área deben existir medios de extinción y alarmas de detección de humos.

En caso de que el incendio se produjera en otra área contigua, elementos de aislamiento como puertas ignífugas podrían evitar su extensión al área en la que se encuentra el dispositivo.

### 3.2.14 Protección frente inundaciones

Se debe realizar un estudio, tanto de origen natural como estructural, del riesgo de inundación en el entorno en el que se encuentra el dispositivo.

En caso de que la inundación ya se hubiera producido, deben existir medios para limitar el impacto reflejados en un plan de recuperación frente a inundaciones.

### 3.2.15 Responsabilidad en el puesto de trabajo

Deben existir responsabilidades definidas, en el ámbito de seguridad, en el puesto en el que se trabaja con el dispositivo. Deben existir ciertos requisitos de confidencialidad y verificar la trayectoria laboral del sanitario que se hará cargo del dispositivo.

Cada trabajador que utilice el dispositivo debe conocer sus deberes y obligaciones, sobre todo con el manejo de datos clínicos y datos personales, y ser informado de las posibles medidas disciplinarias en caso de incumplimiento de los mismos.

Esto incluye tanto a trabajadores externos que trabajen con el dispositivo como a los propios trabajadores internos una vez dejen de trabajar con el dispositivo.

### 3.2.16 Concienciación y formación

Se debe concienciar y formar, inicialmente pero también regularmente, al personal que trabaja con el dispositivo del buen uso del mismo, los riesgos asociados y la identificación y reporte de incidentes. Esta formación debe actualizarse cuando haya cambios relevantes en el dispositivo, o en su entorno, que cambien o acentúen alguno de los aspectos de seguridad.

Particularmente este proyecto está comprometido de manera reseñable con este punto, puesto que, además de realizar un Análisis de Riesgos y valorar el nivel de seguridad, tiene un componente importante de formación para el personal.

### 3.2.17 Bloqueo del dispositivo

El dispositivo debe bloquearse automáticamente al cabo de un tiempo de inactividad y exigir al usuario una nueva autenticación para continuar la actividad.

El tiempo de inactividad estará determinado en la configuración del dispositivo para evitar ser alterado por el trabajador a conveniencia, salvo causa urgente justificada.

Tras otro tiempo de inactividad, configurado de la misma forma, las sesiones abiertas tanto físicas como remotas se cerrarán automáticamente.

### 3.2.18 Protección del dispositivo

Los accesos a internet con el dispositivo deben realizarse utilizando la red corporativa. Si el acceso es remoto, debe estar configurado para limitar la información y los servicios accesibles, teniendo en cuenta el aumento del riesgo de esta modalidad.

Los trabajadores deberán conocer un canal de comunicación y un procedimiento para el momento en el que suceda una incidencia con su uso o bien una avería, pérdida o robo.

Si el dispositivo es susceptible de ser robado, debe ser protegido con el uso de herramientas como llaves o candados. Además, si contiene datos clínicos o datos personales, la configuración no debe permitir que se extraiga información mediante un soporte extraíble.

### 3.2.19 Protección de datos personales

La protección de datos personales es uno de los grandes objetivos de este proyecto. Su valor económico y social convierte estos datos en el principal activo a proteger a sabiendas de que, por otro lado, los datos personales y clínicos también son el principal aspecto a obtener por parte de un atacante de dispositivos IoMT, dada la vulnerabilidad que generan a la organización a la cual se los roban.

Por ello, debe existir una política de protección de datos personales aplicable al dispositivo y designarse un DPD (Delegado de Protección de Datos), especialmente si la organización pertenece al sector público, como ocurre con los principales hospitales españoles.

Además, deben existir procedimientos internos que permitan identificar los incidentes de seguridad relacionados con los datos personales, reportarlos e informar desde la organización a las personas cuyos datos personales hayan podido ser vulnerados.

### 3.2.20 Mantenimiento del dispositivo

El dispositivo debe seguir unas condiciones de mantenimiento óptimas, favoreciendo la ejecución de actualizaciones cuando sea posible y estando informado de forma proactiva de los anuncios que realice el fabricante o proveedor.

Debe existir un documento que señale cuándo, cómo y con qué frecuencia deben realizarse los mantenimientos del dispositivo.

## 3.3 Forma de evaluación utilizada en el Análisis de Riesgos

Para presentar los resultados del Análisis de Riesgos debe establecerse un método de evaluación propia, en la que se establezca de forma argumentada qué aspectos se van a evaluar y en base a qué criterios, buscando que la evaluación sea consistente y objetiva.

Para ello se ha optado por un modelo, basado en el método NIST de cinco niveles (Identificar, Proteger, Detectar, Responder y Recuperar) pero adaptado a las condiciones de las 20 categorías que componen este Análisis de Riesgos. [27]

Para ello habrá, en este caso, cuatro niveles que reflejarán la evaluación final del Análisis de Riesgos, agrupando varias categorías en cada nivel.

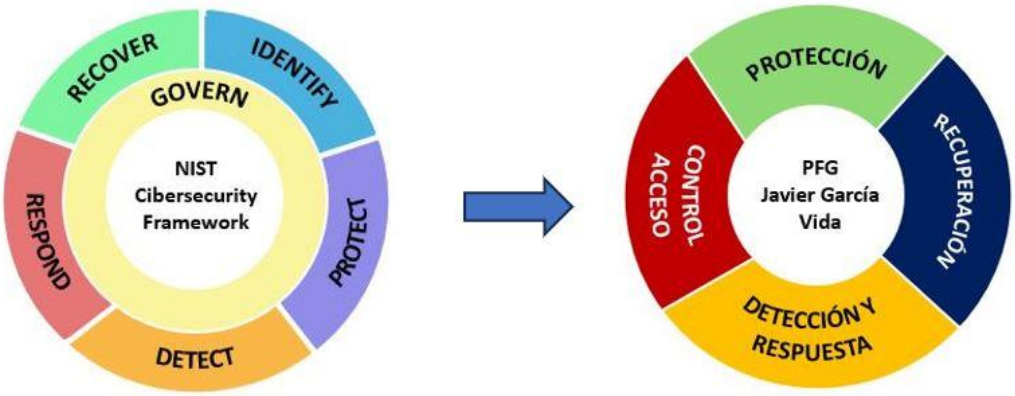



Figura 8: Transformación del método de cinco niveles del NIST

**Capacidad de control de acceso:**

Este nivel reflejará la evaluación de aquellas categorías que tengan que ver con el control de acceso al dispositivo: con qué eficacia se controla quién accede, en qué condiciones puede acceder y cómo se gestionan los accesos. Las categorías que forman parte de este nivel son las siguientes:

- Identificación y acceso.
- Mecanismos de autenticación.
- Acceso local y remoto.
- Registro de la actividad.
- Control de acceso.
- Identificación del personal.

**Capacidad de protección:**

Este nivel reflejará la evaluación de aquellas categorías que tengan relación con la protección del dispositivo, ya sea a nivel de protección física o de protección de la información o datos que contiene éste.

En cuanto a la protección física, estas son las categorías que se incluyen:

- Acondicionamiento del área.
- Protección frente a incendios.
- Protección frente inundaciones.

En cuanto a la protección de la información o de los datos, son las siguientes:

- Protección del dispositivo.
- Protección de datos personales.
- Bloqueo del dispositivo.

**Capacidad de detección y respuesta:**

Este nivel reflejará la evaluación de aquellas categorías que tengan relación con la detección y respuesta de incidentes, ya sea debido a la monitorización del dispositivo o debido a la preparación del personal que trabaja con éste.

Respecto a la monitorización, las categorías incluidas son las siguientes:

- Inventario de activos.
- Registro de incidentes.

Respecto a la preparación del personal sanitario, son estas:

- Responsabilidad en el puesto de trabajo.
- Concienciación y formación.

**Capacidad de recuperación:**

Este nivel reflejará la evaluación de aquellas categorías que guarden relación con la capacidad de recuperación ante un incidente grave que ocasione pérdida de información o inutilización de recursos necesarios para el funcionamiento del dispositivo. Las categorías involucradas son:

- Plan de continuidad.

- Pruebas periódicas.
- Energía eléctrica.
- Mantenimiento del dispositivo.

### 3.3.1 Análisis de impacto de cada categoría

Una vez se ha determinado qué categoría corresponde a cada nivel, se propone realizar una evaluación descendente en tres bloques. Primero se evaluará el porcentaje que aporta cada nivel a la calificación global, posteriormente se evaluará el porcentaje que aporta cada categoría a su nivel y, por último, se evaluará el porcentaje que aporta cada cuestión del Análisis de Riesgos a su categoría.

Para ello, se ha decidido ponderar cada categoría según su impacto (probabilidad de incidente que involucre a dicha categoría y gravedad del mismo si el dispositivo no está protegido con las recomendaciones de esa categoría) en cuanto a la seguridad del dispositivo.

Siguiendo el modelo de diversos documentos como [28] en donde se habla de los riesgos representados en forma de matriz, en la que un eje representa la probabilidad y otro eje la gravedad en caso de producirse el incidente, se entenderá el impacto del riesgo de una categoría como la multiplicación de su grado de probabilidad de incidente (1-bajo, 2-medio, 3-alto) y su gravedad en caso de producirse (1-bajo, 2-medio, 3-alto), en base al estudio realizado en los apartados previos este documento y en nuevas fuentes consultadas [29][30][31][32][33][34][35].

De esta forma se pretende equiparar la importancia de un riesgo con impacto alto con la importancia de varios riesgos de impacto medio, y la importancia de un riesgo de impacto medio con la de varios riesgos de impacto bajo. Así, las puntuaciones finales de impacto quedarían comprendidas entre 1 y 9.

- **Identificación y acceso:** Crucial para evitar accesos no autorizados. Probabilidad alta y gravedad alta. Impacto: 9.

| | | | |
|---|---|---|---|
| **PROBABILIDAD** | | | • |
| | | | |
| | | | |
| | **GRAVEDAD** | | |

Tabla 2: Identificación y acceso

- **Mecanismos de autenticación:** Previene accesos no autorizados, pero está fortalecido por la categoría anterior. Probabilidad alta y gravedad media. Impacto: 6.

| | | | |
|---|---|---|---|
| **PROBABILIDAD** | | • | |
| | | | |
| | | | |
| | **GRAVEDAD** | | |

Tabla 3: Mecanismos de autenticación

- **Acceso local y remoto:** Supone un riesgo significativo para dispositivos IoMT y es uno de los principales riesgos que diferencia a estos dispositivos del resto. Probabilidad alta y gravedad alta. Impacto: 9.

| | | | |
|---|---|---|---|
| **PROBABILIDAD** | | | • |
| | | | |
| | | | |
| | **GRAVEDAD** | | |

Tabla 4: Acceso local y remoto

- **Inventario de activos:** Tiene cierta importancia para la gestión y seguimiento del dispositivo, pero no es crítico ni entra dentro del grupo de riesgos prioritarios. Probabilidad baja y gravedad baja. Impacto: 1.

| | | | |
|---|---|---|---|
| **PROBABILIDAD** | | | |
| | | | |
| | • | | |
| | **GRAVEDAD** | | |

Tabla 5: Inventario de activos

- **Registro de incidentes:** Es fundamental para poder responder a tiempo y con conocimientos claros a los incidentes. Probabilidad alta (involucra todos los incidentes) y gravedad alta. Impacto: 9.

| | | | |
|---|---|---|---|
| **PROBABILIDAD** | | | • |
| | | | |
| | | | |
| | **GRAVEDAD** | | |

Tabla 6: Registro de incidentes

- **Registro de la actividad:** Importante para controlar el uso permitido del dispositivo. Probabilidad media, gravedad media. Impacto: 4.

| | | | |
|---|---|---|---|
| **PROBABILIDAD** | | | |
| | | • | |
| | | | |
| | **GRAVEDAD** | | |

Tabla 7: Registro de la actividad

- **Plan de continuidad:** Es imprescindible una recuperación rápida, ordenada y preparada ante un incidente. Probabilidad alta, gravedad alta. Impacto: 9.

| | | | |
|---|---|---|---|
| **PROBABILIDAD** | | | • |
| | | | |
| | | | |
| | **GRAVEDAD** | | |

Tabla 8: Plan de continuidad

- **Pruebas periódicas:** Ayuda a identificar vulnerabilidades en el Plan de Continuidad y le sirve como apoyo. Probabilidad baja, gravedad alta. Impacto: 3.

| | | | |
|---|---|---|---|
| **PROBABILIDAD** | | | |
| | | | |
| | | | • |
| | **GRAVEDAD** | | |

Tabla 9: Pruebas periódicas

- **Control de acceso:** Es fundamental para controlar la situación del dispositivo. Probabilidad alta, gravedad alta. Impacto: 9.

| | | | |
|---|---|---|---|
| **PROBABILIDAD** | | | • |
| | | | |
| | | | |
| | **GRAVEDAD** | | |

Tabla 10: Control de acceso

- **Identificación del personal:** Es un aspecto relevante, pero no crítico en cuanto a dispositivos IoMT. Probabilidad media, gravedad media. Impacto: 4.

| | | | |
|---|---|---|---|
| **PROBABILIDAD** | | | |
| | | • | |
| | | | |
| | **GRAVEDAD** | | |

Tabla 11: Identificación del personal

- **Acondicionamiento del área:** Supone un bajo riesgo, en general. Probabilidad baja, gravedad baja. Impacto: 1.

| | | | |
|---|---|---|---|
| **PROBABILIDAD** | | | |
| | | | |
| | • | | |
| | **GRAVEDAD** | | |

Tabla 12: Acondicionamiento del área

- **Energía eléctrica:** Importante, ya que una interrupción eléctrica puede afectar de forma crítica a los procesos médicos urgentes. Probabilidad media, gravedad alta. Impacto: 6.

| | | | |
|---|---|---|---|
| **PROBABILIDAD** | | | |
| | | | • |
| | | | |
| | **GRAVEDAD** | | |

Tabla 13: Energía eléctrica

- **Protección frente a incendios:** Determinante solo en pocas ocasiones. Probabilidad baja, gravedad baja. Impacto: 1.

| | | | |
|---|---|---|---|
| **PROBABILIDAD** | | | |
| | | | |
| | • | | |
| | **GRAVEDAD** | | |

Tabla 14: Protección frente a incendios

- **Protección frente inundaciones:** Del mismo modo que ocurre con los incendios, es un factor a tener en cuenta, pero determinante en pocas ocasiones respecto a dispositivos IoMT. Probabilidad baja, gravedad baja. Impacto: 1.

| | | | |
|---|---|---|---|
| **PROBABILIDAD** | | | |
| | | | |
| | • | | |
| | **GRAVEDAD** | | |

Tabla 15: Protección frente a inundaciones

- **Responsabilidad en el puesto de trabajo:** Es imprescindible que el trabajador conozca su responsabilidad con el trato de datos personales y clínicos. Probabilidad alta, gravedad alta. Impacto: 9.

| | | | |
|---|---|---|---|
| **PROBABILIDAD** | | | • |
| | | | |
| | | | |
| | **GRAVEDAD** | | |

Tabla 16: Responsabilidad en el puesto de trabajo

- **Concienciación y formación:** Su importancia disminuye en el contexto de este proyecto, en el que ya se usa una labor formativa que puede suplir algunas carencias de formación. Además, los aspectos clave sobre responsabilidad en el puesto de trabajo se cubren con la categoría anterior. Probabilidad media, gravedad baja. Impacto: 2.

| | | | |
|---|---|---|---|
| **PROBABILIDAD** | | | |
| | • | | |
| | | | |
| | **GRAVEDAD** | | |

Tabla 17: Concienciación y formación

- **Bloqueo del dispositivo:** Puede llegar a prevenir accesos no autorizados cuando el dispositivo no está en uso. Probabilidad media, gravedad alta. Impacto: 6.

| | | | |
|---|---|---|---|
| **PROBABILIDAD** | | | |
| | | | • |
| | | | |
| | **GRAVEDAD** | | |

Tabla 18: Bloqueo del dispositivo

- **Protección del dispositivo:** Es especialmente relevante ya que combina aspectos de protección de información del dispositivo con aspectos de protección física. Probabilidad alta, gravedad alta. Impacto: 9.

| | | | |
|---|---|---|---|
| **PROBABILIDAD** | | | • |
| | | | |
| | | | |
| | **GRAVEDAD** | | |

Tabla 19: Protección del dispositivo

- **Protección de datos personales:** La protección prioritaria de datos personales supone una de las restricciones claves del proyecto. Probabilidad alta, gravedad alta. Impacto: 9.

| | | | |
|---|---|---|---|
| **PROBABILIDAD** | | | • |
| | | | |
| | | | |
| | **GRAVEDAD** | | |

Tabla 20: Protección de datos personales

- **Mantenimiento del dispositivo:** Tiene cierta importancia para maximizar la seguridad del dispositivo. Probabilidad media, gravedad media. Impacto: 4.

| | | | |
|---|---|---|---|
| **PROBABILIDAD** | | | |
| | | • | |
| | | | |
| | **GRAVEDAD** | | |

Tabla 21: Mantenimiento del dispositivo

Con esta calificación no se pretende en ningún caso obviar algunos de los riesgos, sino establecer grados de impacto que ayuden a priorizar la solución de algunos riesgos, de forma que la ponderación final del Análisis de Riesgos incida en su importancia. También resulta importante dejar establecidas ciertas prioridades para la tarea final del proyecto, en la que se tendrá que automatizar una lista ordenada de cambios, con una labor formativa incluida, que se proponen al personal sanitario que realice el Análisis de Riesgos.

### 3.3.2 Ponderación de los niveles y categorías

Teniendo en cuenta estas consideraciones, los cuatro niveles quedan formados por categorías con la siguiente puntuación:

- **Capacidad de control de acceso:** Tres categorías de Impacto 9, una categoría de Impacto 6 y dos categorías de Impacto 4 = 3x9 + 1x6 + 2x4 = 27 + 6 + 8 = 41 puntos.

- **Capacidad de protección:** Dos categorías de Impacto 9, una categoría de Impacto 6 y tres categorías de Impacto 1 = 2x9 + 1x6 + 3x1 = 18 + 6 + 3 = 27 puntos.

- **Capacidad de detección y respuesta:** Dos categorías de Impacto 9, una categoría de Impacto 2 y una categoría de Impacto 1 = 2x9 + 1x2 + 1x1 = 18 + 2 + 1 = 21 puntos.

- **Capacidad de recuperación:** Una categoría de Impacto 9, una categoría de Impacto 6, una categoría de Impacto 4 y una categoría de Impacto 3 = 1x9 + 1x6 + 1x4 + 1x3 = 9 + 6 + 4 + 3 = 22 puntos.

Con una suma final de 111 puntos, se establece el porcentaje de valor de cada nivel para aportar la calificación global:

- **Capacidad de control de acceso:** 36.94%.

- **Capacidad de protección:** 24.32%.
- **Capacidad de detección y respuesta:** 18.92%.
- **Capacidad de recuperación:** 19.82%.

Posteriormente, para evaluar ahora cada nivel por separado, cada categoría vuelve a asumir su impacto de forma individual para obtener su representación porcentual dentro de su nivel:

**Capacidad de control de acceso:**

- Identificación y acceso: Impacto 9 sobre 41 = 21.95%
- Mecanismos de autenticación: Impacto 6 sobre 41 = 14.63%
- Acceso local y remoto: Impacto 9 sobre 41 = 21.95%
- Registro de la actividad: Impacto 4 sobre 41 = 9.76%
- Control de acceso: Impacto 9 sobre 41 = 21.95%
- Identificación del personal: Impacto 4 sobre 41 = 9.76%

**Capacidad de protección:**

- Acondicionamiento del área: Impacto 1 sobre 27 = 3.70%
- Protección frente a incendios: Impacto 1 sobre 27 = 3.70%
- Protección frente inundaciones: Impacto 1 sobre 27 = 3.70%
- Protección del dispositivo: Impacto 9 sobre 27 = 33.34%
- Protección de datos personales: Impacto 9 sobre 27 = 33.34%
- Bloqueo del dispositivo: Impacto 6 sobre 27 = 22.22%

**Capacidad de detección y respuesta:**

- Inventario de activos: Impacto 1 sobre 21 = 4.76%
- Registro de incidentes: Impacto 9 sobre 21 = 42.86%
- Responsabilidad en el puesto de trabajo: Impacto 9 sobre 21 = 42.86%
- Concienciación y formación: Impacto 2 sobre 21 = 9.52%

**Capacidad de recuperación:**

- Plan de continuidad: Impacto 9 sobre 22 = 40.91%
- Pruebas periódicas: Impacto 3 sobre 22 = 13.64%
- Energía eléctrica: Impacto 6 sobre 22 = 27.27%
- Mantenimiento del dispositivo: Impacto 4 sobre 22 = 18.18%

## 3.4 Creación del cuestionario para el Análisis de Riesgos

Tras el estudio realizado de los requisitos de seguridad de cada categoría y el análisis del impacto en cada una de ellas, se ha creado un cuestionario propio para el Análisis de Riesgos que cumple las siguientes condiciones:

- Todos los aspectos evaluados en el cuestionario guardan relación directa o indirecta con la seguridad de los dispositivos IoMT.
- El cuestionario está pensado para ser respondido por el técnico sanitario que trabaja habitualmente con el dispositivo IoMT, sin necesidad de conocimientos en ciberseguridad o en programación.
- Cumplir los requisitos de cada una de las preguntas de una categoría supone cumplir todos los requisitos de seguridad de dicha categoría.
- Cada pregunta tiene asociado un valor numérico, en porcentaje, en base a su importancia dentro de la categoría, priorizando siempre los aspectos de seguridad más básicos de cada categoría. Este valor se utilizará para calcular los resultados de los niveles de seguridad.
- Las preguntas de cada categoría están ordenadas de forma descendente en base a su importancia para la seguridad de dicha categoría.
- Cada pregunta tiene asociado un texto de sugerencia, que podrá aparecer en el listado final de sugerencias de mejoras de seguridad cuando no se hayan cumplido los requisitos evaluados en esa pregunta, siempre que se haya determinado que esa sugerencia debe ser uno de los cambios prioritarios, en base a los cálculos de valoración.

**Identificación y acceso**

*1: ¿Existe un método de identificación para acceder al dispositivo?*

Valoración: 60%. Es imprescindible que exista cualquier tipo de identificación.

Sugerencia: El dispositivo debe configurarse para solicitar un identificador en cada acceso que se realice. De esta forma se consigue que solo las personas que conozcan el identificador puedan acceder al dispositivo.

*2: ¿Existe un método de identificación único, relacionado con la cuenta de usuario de la organización, para acceder al dispositivo?*

Valoración: 30%. Relacionar la identificación con una cuenta de usuario de la organización mejora notablemente la seguridad.

Sugerencia: El identificador personal de acceso al dispositivo debe ser único y asociarse a la cuenta de usuario de la organización, de forma que la ésta pueda, cuando sea necesario, borrar un usuario o controlar sus permisos a un determinado dispositivo. Este identificador será intransferible salvo que una emergencia justifique su transferencia puntual a otro trabajador.

*3: ¿Existe un protocolo para deshabilitar las cuentas de aquellos usuarios que ya no necesiten utilizar el dispositivo?*

Valoración: 10%. Deshabilitar las cuentas en desuso es un proceso que aporta seguridad, pero no es determinante por sí solo.

Sugerencia: Debe existir un protocolo para deshabilitar aquellas cuentas de usuarios que ya no participen en la actividad con el dispositivo o que se hayan ido de la organización. De esta forma de evitan accesos indeseados.

**Mecanismos de autenticación**

*4: ¿Existe una contraseña, que haga de autenticación de doble factor respecto al identificador personal, para utilizar el dispositivo?*

Valoración: 50%. Tener un doble factor de autenticación es clave para proteger el dispositivo ante un robo de identidad.

Sugerencia: Se debe añadir una contraseña al dispositivo que haga de doble factor de autenticación. De esta manera se protege el dispositivo en caso de que las credenciales de identificación de un trabajador hayan sido robadas o filtradas.

*5: ¿Se limita el número de intentos fallados seguidos de acceso?*

Valoración: 35%. No permitir fallos ilimitados evita un ingreso mediante “prueba y error”.

Sugerencia: Se debe limitar el número de intentos fallados seguidos de acceso. Una cierta cantidad de fallos seguidos es un indicativo de que la contraseña no se conoce y se está probando. No limitar estas pruebas podría terminar en un intento correcto tras una gran cantidad de intentos.

*6: ¿La contraseña combina mayúsculas, minúsculas y números?*

Valoración: 10%. Una contraseña intuible aumenta las posibilidades de ataque.

Sugerencia: La contraseña del dispositivo debe combinar mayúsculas, minúsculas y números para hacerla más robusta.

*7: ¿Se ha cambiado la contraseña en los últimos 3 meses?*

Valoración: 5%. Cambiar la contraseña es importante, pero no ajustarse a las fechas marcadas no debe ser determinante.

Sugerencia: Debe cambiarse la contraseña del dispositivo mínimo una vez cada 3 meses, sin repetir antiguas.

**Acceso local y remoto**

*8: ¿Existe un registro de accesos al sistema que identifique el usuario que ha iniciado sesión y a qué hora lo ha hecho?*

Valoración: 40%. La existencia de este registro es vital para hacer comprobaciones de acceso.

Sugerencia: Debe establecerse un registro que identifique qué usuario accede al dispositivo y a qué hora lo hace, ya sea en el propio dispositivo o bien guardándose en una base de datos de la organización. De esta forma se consigue tener información para investigar incidentes que hayan podido suceder en el pasado.

*9: ¿Existe algún mecanismo que avise al trabajador, mediante medios alternativos como SMS o correo electrónico, que se ha accedido a un dispositivo con su identificador personal?*

Valoración: 25%. El uso de este mecanismo permitiría detectar intrusiones al dispositivo en tiempo real.

Sugerencia: Debe ponerse en marcha un mecanismo que notifique a cada trabajador, en tiempo real, de sus accesos a un dispositivo. De esta forma, el trabajador podrá alertar cuando se le notifique de un acceso con su identidad que él no ha realizado.

*10: ¿Está permitido realizar un acceso remoto sin conectarse a la red VPN corporativa?*

Valoración: 20%. Hacer un acceso remoto al dispositivo sin usar la VPN corporativa aumenta la vulnerabilidad.

Sugerencia: Se debe obligar a los trabajadores a realizar los accesos remotos al dispositivo mediante conexión por la VPN corporativa y, en caso de urgencia e imposibilidad de acceso mediante VPN, evitar conectarse mediante redes Wi-Fi públicas. La VPN es un sistema que incrementa la seguridad de un proceso tan crítico como la conexión remota a un dispositivo médico.

*11: ¿Está permitido realizar un acceso local a internet mediante red inalámbrica (Wi-Fi)?*

Valoración: 15%. Realizar el acceso mediante conexión por cable mejora ligeramente la seguridad.

Sugerencia*: La conexión a internet debe realizarse mediante conexión por cable, de esta forma se incrementa la seguridad del proceso de conexión.*

**Inventario de activos**

*12: ¿Está el dispositivo incluido en un inventario específico de dispositivos IoMT?*

Valoración: 45%. Tener documentado un inventario es esencial para controlar todos los aspectos sobre el dispositivo.

Sugerencia: Debe incluirse el dispositivo en un inventario específico de dispositivos IoMT en el que se recoja información como: dónde está ubicado el dispositivo, quién es el responsable, fabricante y proveedor del dispositivo, versión de software instalada, tipo de conexión y equipamiento de red. Si el inventario no existe, debe crearse, ya que es un documento esencial para recopilar información de la situación del dispositivo.

13*: ¿Se detalla en el inventario dónde está ubicado el dispositivo?*

Valoración: 20%. Conocer su ubicación física permite atajar rápidamente un problema.

Sugerencia: Debe detallarse en el inventario de dispositivos IoMT dónde está ubicado el dispositivo. De esta forma se le puede tener plenamente localizado ante cualquier incidencia en su área o áreas contiguas.

*14: ¿Se detalla en el inventario quién o quiénes son los últimos responsables del dispositivo?*

Valoración: 20%. Conocer quiénes son los responsables acelera el proceso de contacto.

Sugerencia: Debe detallarse en el inventario de dispositivos IoMT quién o quiénes son los últimos responsables del dispositivo. Así se puede contactar de manera inmediata con ellos en caso de necesidad.

*15: ¿Se detalla en el inventario cuál es el fabricante y/o proveedor del dispositivo?*

Valoración: 5%. Importancia baja.

Sugerencia: Debe detallarse en el inventario de dispositivos IoMT cuál es el fabricante y/o proveedor del dispositivo. Esta información es útil ante un problema técnico que tenga una solución específica, y es importante para estar atento a las actualizaciones que publiquen.

*16: ¿Se detalla en el inventario cuál es la versión de software instalada en el dispositivo?*

Valoración: 5%. Importancia baja.

Sugerencia: Debe detallarse en el inventario de dispositivos IoMT cuál es la versión de software instalada en el dispositivo. Este factor es importante en caso de que se comuniquen vulnerabilidades de una determinada versión.

*17: ¿Se detalla en el inventario cuál es el tipo de conexión y el equipamiento de red?*

Valoración: 5%. Importancia baja.

Sugerencia: Debe detallarse en el inventario de dispositivos IoMT cuál es el tipo de conexión y el equipamiento de red. De esta forma se conocerá más información para evaluar el dispositivo.

**Registro de incidentes**

*18: ¿Existe un documento de reporte de incidentes para este dispositivo?*

Valoración: 30%. Este documento es imprescindible para un correcto seguimiento de incidentes.

Sugerencia: Debe crearse un documento de reporte de incidentes para este dispositivo, en el que se recoja el historial de incidentes, incluyendo su tipología, fecha y recopilación de evidencias que puedan ayudar a detectar un nuevo incidente, se señalice a quién debe reportarse cada incidente, en caso de suceder, se detalle si un incidente en este dispositivo puede afectar a datos personales y se muestren los protocolos de aislamiento que mejor funcionaron para este sistema en otros incidentes o, en caso de no haber habido ninguno, los que se recomiendan seguir según las condiciones del dispositivo.

*19: ¿En el documento de reporte de incidentes se recoge el historial de incidentes, incluyendo su tipología, la fecha en la que ocurrió y la recopilación de evidencias de los incidentes pasados?*

Valoración: 20%. Para que el registro esté completo, estos datos tienen una gran importancia.

Sugerencia: Debe incluirse en el documento de reporte de incidentes el historial de incidentes, incluyendo su tipología, la fecha en la que ocurrió y la recopilación de evidencias de los incidentes pasados. De esta forma, sabiendo el tipo de incidente, su frecuencia y qué evidencias se recolectaron, el trabajador puede familiarizarse con incidentes reiterados y estar mejor preparado para detectarlo y reportarlo.

*20: ¿En el documento de reporte de incidentes se señaliza a quién o quiénes debe reportarse cada incidente en función de su tipología?*

Valoración: 20%. Es muy importante para agilizar el reporte de incidentes.

Sugerencia: Debe añadirse al documento de reporte de incidentes a quién o quiénes debe reportarse cada incidente en función de su tipología u otros factores. Esto agiliza el proceso de reporte y de solución al incidente.

*21: ¿En el documento de reporte de incidentes se especifica si éstos tienen la capacidad de afectar a datos personales accesibles desde este dispositivo?*

Valoración: 20%. De gran relevancia, dado que los datos personales es el principal aspecto a proteger en este proyecto.

Sugerencia: Debe especificarse en el documento de reporte de incidentes si es posible afectar a datos personales accesibles desde este dispositivo. De esta forma los expertos en seguridad gestionarán el protocolo de resolución de incidentes de la forma más adecuada.

*22: ¿En el documento de reporte de incidentes se especifica qué protocolos de aislamiento funcionaron de forma más efectiva en incidentes anteriores o, si no los hubo, qué protocolo se recomienda seguir?*

Valoración: 10%. Es un aspecto que puede servir como orientación para resolver un incidente.

Sugerencia: Debe especificarse en el documento de reporte de incidentes qué protocolos de aislamiento del dispositivo funcionaron de forma más efectiva en incidentes anteriores o, si no los hubo, qué protocolo se recomienda seguir para este dispositivo.

**Registro de la actividad**

*23: ¿Se revisa periódicamente el historial de accesos al dispositivo?*

Valoración: 100%, al ser el único parámetro que se evalúa de esta categoría.

Sugerencia: Debe revisarse periódicamente el historial de accesos al dispositivo. De esta forma se pueden detectar anomalías en la actividad de algún trabajador y reportarlas con cierta rapidez para esclarecer la situación.

**Plan de continuidad**

*24: ¿Está el dispositivo incluido en el Plan de Continuidad de la organización?*

Valoración: 50%. Estar incluido en el Plan de Continuidad permite salvaguardar los datos en caso de catástrofe o problema grave.

Sugerencia: Debe incluirse el dispositivo en el Plan de Continuidad de la organización, facilitando además dónde se encuentran las copias de seguridad y qué dispositivos alternativos podrían utilizarse en caso de inutilizarse este.

25*: ¿Existen copias seguridad en la nube, o en otros dispositivos físicos, del contenido de este dispositivo y están indicadas en el Plan de Continuidad?*

Valoración: 30%. Es la forma más efectiva de no perder los datos.

Sugerencia: Deben crearse copias de seguridad periódicas en la nube, o en su defecto almacenarlas en otros dispositivos físicos, del contenido de este dispositivo e indicarse en el Plan de Continuidad su localización. De esta forma se podrán recuperar los datos en caso de catástrofe.

26: *¿Está establecido en el Plan de Continuidad qué dispositivos alternativos podrían sustituir la labor de este dispositivo?*

Valoración: 20%. Importante para no perder tiempo buscando otro dispositivo sobre la marcha y retrasando actividades urgentes.

Sugerencia: Debe establecerse qué dispositivos alternativos podrían sustituir la labor de este dispositivo actual, en caso de inutilización, y añadirlo al Plan de Continuidad.

**Pruebas periódicas**

*27: ¿Se realizan pruebas periódicas de continuidad con el dispositivo para evaluar el impacto en caso de inutilización o borrado de datos?*

Valoración: 75%. Es un aspecto clave para prepararse en un escenario real.

Sugerencia: Se deben realizar pruebas periódicas de continuidad con el dispositivo, tales como pruebas de recuperación de las copias de seguridad y pruebas de utilización de medios alternativos para suplir la labor del dispositivo actual, para simular una situación de catástrofe en la que el dispositivo quedase inutilizado o su información fuese borrada. Es necesario documentar los resultados de estas pruebas en un informe que los analice.

*28: ¿Se realizan periódicamente pruebas de recuperación de las copias de seguridad del dispositivo?*

Valoración: 10%. Es relevante para comprobar que existan las copias, pero lo realmente importante es que éstas existan.

Sugerencia: Deben realizarse pruebas periódicas de recuperación de las copias de seguridad del dispositivo, para comprobar si, en caso de pérdida o robo de datos del dispositivo original, se puede salvaguardar de forma óptima la información haciendo uso de las copias de seguridad.

29*: ¿Se realizan periódicamente pruebas de utilización de medios alternativos para suplir la labor del dispositivo en caso de inutilización?*

Valoración: 10%. Del mismo modo, es una comprobación importante, pero no tanto como el hecho de conocer que existen estos medios alternativos.

Sugerencia: Deben realizarse pruebas periódicas de utilización de medios alternativos, con el fin de poder suplir de la forma más eficiente y completa posible la labor del dispositivo actual, en caso de quedar éste inutilizado por algún motivo.

30*: ¿Existe un informe en el que se analicen los resultados de las pruebas periódicas de continuidad?*

Valoración: 5%. No es muy determinante si se realizan correctamente los pasos anteriores.

Sugerencia: Debe elaborarse un informe en el que se analicen los resultados de las pruebas periódicas de continuidad. De esta forma, y en función de los resultados obtenidos, se podrá mejorar el Plan de Continuidad respecto al dispositivo.

**Control de acceso**

*31 - ¿Se encuentra el dispositivo dentro de un área delimitada con condiciones físicas para poder establecer un control de acceso?*

Valoración: 50%. Estar en este tipo de área es lo que permitirá llevar a cabo el resto de medidas.

Sugerencia: El dispositivo debe encontrarse en un área delimitada, ya sea una sala o un armario, que tenga las condiciones físicas para poder establecer un control de acceso. Tener el dispositivo en un área delimitada permite gestionar mejor su vigilancia.

*32 - ¿Existe un inventario que determina quién está autorizado a acceder al área en la que se encuentra el dispositivo?*

Valoración: 30%. Es importante que queden claros los accesos autorizados.

Sugerencia: Debe existir un inventario que determine quién está autorizado a acceder al área en la que se encuentra el dispositivo. Con este documento se pueden gestionar los accesos de forma más eficiente y automática.

*33 - ¿Se garantiza mediante un control de acceso que solo acceda el personal sanitario autorizado al área en la que se encuentra el dispositivo?*

Valoración: 10%. Permite validar los accesos autorizados de forma práctica.

Sugerencia: Debe garantizarse mediante un control de acceso que solo acceda el personal sanitario autorizado al área en la que se encuentra el dispositivo. El control de acceso, que puede ser una llave, un código o un vigilante de seguridad, permite conceder o denegar el acceso a cada trabajador sanitario, lo cual evita accesos indebidos que pueden poner en peligro al dispositivo y, en consecuencia, a la organización.

*34 - ¿Existen cámaras de seguridad que permitan detectar si alguien accede indebidamente al lugar en el que se encuentra el dispositivo, ya sea fuera del horario laboral o por un punto alternativo?*

Valoración: 10%. Es un aspecto importante, pero depende de factores económicos, así que se prioriza la protección de otros modos.

Sugerencia: Deben situarse cámaras de seguridad que permitan detectar si alguien accede indebidamente al lugar en el que se encuentra el dispositivo, ya que sea fuera del horario laboral o por un punto alternativo. Las cámaras son un complemento de seguridad al control de acceso, ya que éste puede fallar, no estar operativo fuera del horario laboral, no cubrir todos los puntos de acceso o incluso ser manipulado.

**Identificación del personal**

*35 - ¿Se verifica que la persona que solicita el acceso al área en la que se encuentra el dispositivo no es la misma que tiene la potestad de autorizar dicho acceso?*

Valoración: 50%. Es un aspecto clave de seguridad no generar duplicidad de funciones.

Sugerencia: Debe verificarse que la persona que solicita el acceso al área en la que se encuentra el dispositivo no es la misma que tiene la potestad de autorizar dicho acceso. Con esta situación, el control de acceso pierde su sentido, ya que el proceso previo de autorización carece de neutralidad si no participan al menos dos personas distintas.

*36 - ¿Se verifica que las personas que acceden al área en la que se encuentra el dispositivo son realmente las que tienen acceso?*

Valoración: 20%. No debe bastar con mostrar una identificación, sin mayores comprobaciones periódicas rutinarias.

Sugerencia: Debe verificarse que las personas que acceden al área en la que se encuentra el dispositivo son realmente las que tienen acceso. De lo contrario, una persona con autorización tendría, en la práctica, el poder de autorizar a cualquier otro compañero al quien le preste sus credenciales de acceso.

*37 - ¿Se guarda un registro con las fechas de entrada y salida de cada sanitario en el área en la que se encuentra el dispositivo?*

Valoración: 20%. Esta información es valiosa para comprobaciones futuras, en caso de incompatibilidad.

Sugerencia: Debe guardarse un registro con las fechas de entrada y salida de cada sanitario en el área en la que se encuentra el dispositivo. Este registro es útil para comprobar distintos datos, no solo el tiempo que pasa cada persona dentro del área restringida, sino también comprobar que las credenciales de ese usuario no se están utilizando en dos lugares al mismo tiempo.

*38 - ¿Se realiza una revisión periódica de las autorizaciones de acceso al área en la que se encuentra el dispositivo?*

Valoración: 10%. Es importante revisar la vigencia de las autorizaciones.

Sugerencia: Se debe realizar una revisión periódica de las autorizaciones de acceso al área en la que se encuentra el dispositivo. De esta forma se impide que un usuario que ha

finalizado su tarea, para la cual se le concedió el acceso, continúe haciendo uso de una autorización de acceso que debería haber caducado.

**Acondicionamiento del área**

*39 - ¿El área en la que se utiliza el dispositivo respeta los márgenes de temperatura y humedad que establece el fabricante?*

Valoración: 60%. Siendo una categoría no excesivamente importante, la mayoría de su importancia reside en controlar los aspectos de temperatura y humedad.

Sugerencia: El área en la que se utiliza el dispositivo debe respetar los márgenes de temperatura y de humedad que establece el fabricante. No respetarlos puede suponer un deterioro progresivo del dispositivo.

*40 - ¿El área en la que se utiliza el dispositivo está protegida de amenazas externas, como daños procedentes de climatología adversa, y de amenazas internas, como la presencia de otros dispositivos inflamables?*

Valoración: 20%. Este factor es importante, aunque muchas veces depende solo de factores naturales.

Sugerencia: El área en la que se utiliza el dispositivo debe estar protegida de amenazas externas, como daños procedentes de climatología adversa, y de amenazas internas, como la presencia de otros dispositivos inflamables. La presencia de goteras, ventanas que no cierran correctamente o incluso otros dispositivos inflamables, pueden poner en peligro el dispositivo médico que queremos proteger y además al resto de equipos presentes en el área.

*41 - ¿El cableado del dispositivo está etiquetado, controlado y protegido para no suponer una amenaza al personal sanitario ni a otros dispositivos médicos?*

Valoración: 20%. Es importante, aunque no decisivo.

Sugerencia: El cableado, en caso de existir, del dispositivo debe estar etiquetado, controlado y protegido para no suponer una amenaza al personal sanitario ni a otros dispositivos médicos. Con esta medida se evitan posibles accidentes del personal médico, de otros dispositivos o incluso de pacientes sufridos por un cableado que está en condiciones inseguras.

**Energía eléctrica**

42 - *¿Existe un plan de emergencia y recuperación frente a un corte eléctrico en el que esté incluido el dispositivo?*

Valoración: 80%. Este plan es vital para conseguir un funcionamiento de emergencia en el dispositivo.

Sugerencia: El dispositivo debe estar incluido en un plan de emergencia y recuperación frente a un corte eléctrico. De esta forma, en caso de suceder un corte eléctrico, se puede garantizar un orden que priorice dispositivos esenciales, como puede llegar a ser el caso de este dispositivo según las circunstancias.

*43 - ¿Existen suministros alternativos, tales como generadores u otros sistemas de alimentación, que fueran capaces de proporcionar energía para el uso mínimo indispensable del dispositivo?*

Valoración: 20%. Es importante, pero podría ocurrir que sea necesario adquirir esos equipos y, se debe equilibrar su importancia con el gasto económico.

Sugerencia: Deben existir suministros alternativos, tales como generadores u otros sistemas de alimentación, que fueran capaces de proporcionar energía para el uso mínimo indispensable del dispositivo. Así, en caso de un corte eléctrico, si se requiere por emergencia el uso del dispositivo, se asegura que no quede inutilizado.

**Protección frente a incendios**

*44 - ¿Existe un estudio del entorno, que incluya las instalaciones, el exterior, otros equipos y el propio dispositivo, que señale cuál es el riesgo de incendio?*

Valoración: 50%. Importante para controlar el riesgo.

Sugerencia: Debe existir un estudio del entorno, que incluya las instalaciones, el exterior, otros equipos y el propio dispositivo, que señale cuál es el riesgo de incendio. De esta forma, y en función de la probabilidad de incendio, se podrá diseñar el plan de emergencia teniendo estos factores en cuenta.

*45 - ¿Existen medios de extinción y alarmas de detección de humos en el área en la que se encuentra el dispositivo?*

Valoración: 30%. Una vez conocido el riesgo, se debe saber cómo afrontarlo.

Sugerencia: Deben existir medios de extinción y alarmas de detección de humos en el área en la que se encuentra el dispositivo. En caso de que el incendio ya se haya producido, tener elementos que alerten del mismo y que sean capaces de apagarlo supone una gran ventaja para poder salvar dispositivos de gran importancia.

*46 - ¿Existen materiales ignífugos que sean capaces de proteger el área en la que se encuentra el dispositivo de un incendio producido en un área contigua?*

Valoración: 20%. Tiene importancia, pero limitada, puede depender de factores económicos.

Sugerencia: Deben existir materiales ignífugos, como puertas ignífugas, que sean capaces de proteger el área en la que se encuentra el dispositivo de un incendio producido en un

área contigua. Así se evita que, aunque el área del dispositivo tenga toda la preparación interna contra incendios, tampoco se vea afectada por incendios externos.

**Protección frente inundaciones**

*47 - ¿Existe un estudio del entorno en el que se encuentra el dispositivo que analice el riesgo de inundación tanto de origen natural como estructural?*

Valoración: 60%. Importante para estudiar el riesgo, de la misma forma que en la categoría previa.

Sugerencia: Debe existir un estudio del entorno en el que se encuentra el dispositivo que analice el riesgo de inundación, tanto de origen natural como estructural. Con ese estudio se puede recopilar información sobre qué áreas son más propensas a qué tipos de inundaciones, y colocar al dispositivo, en caso de ser posible, en un área del edificio sin alto riesgo de encharcamiento o de goteras.

*48 - ¿Existe un plan de recuperación frente a inundaciones en el que se establezca qué medios pueden ayudar a minimizar o resolver las inundaciones?*

Valoración: 40%. Muy relevante conocer esa información previamente a que suceda la inundación.

Sugerencia: Debe existir un plan de recuperación frente a inundaciones en el que se establezca qué medios qué medios pueden ayudar a minimizar o resolver las inundaciones, en caso de producirse. Este plan es importante para conocer si la organización cuenta con medios tales como bombas de achique automático o bombas portátiles y detallar dónde se encuentran y cómo utilizarlas, para agilizar el proceso de emergencia minimizando el impacto en el dispositivo.

**Responsabilidad en el puesto de trabajo**

*49 - ¿Existe un documento que refleje las responsabilidades, en el ámbito de seguridad, que se deben exigir al trabajador que utilice el dispositivo?*

Valoración: 60%. Es imprescindible que el trabajador conozca esa información para poder usar el dispositivo.

Sugerencia: Debe existir un documento que refleje las responsabilidades, en el ámbito de seguridad, que se deben exigir al trabajador que utilice el dispositivo. Este documento es útil a la hora de contrastar la trayectoria laboral del trabajador con las exigencias solicitadas y marca los mínimos para la firma de los acuerdos de confidencialidad.

*50 - ¿Existe un procedimiento para informar a todos los trabajadores que utilicen el dispositivo de sus deberes y obligaciones respecto al uso de datos clínicos, datos personales y datos confidenciales?*

Valoración: 40%. Tiene una gran importancia por el hecho de saber gestionar adecuadamente los datos personales.

Sugerencia: Debe existir un procedimiento para informar a los trabajadores que utilicen el dispositivo de sus deberes y obligaciones respecto al uso de datos clínicos, datos personales y datos confidenciales. Estos deberes y obligaciones están dirigidos tanto para trabajadores internos como externos, tanto para el periodo de trabajo como para el posterior, y tienen vinculadas unas medidas disciplinarias en caso de incumplimiento.

**Concienciación y formación**

*51 - ¿Existe un plan de formación y/o concienciación para el personal que debe utilizar este dispositivo?*

Valoración: 50%. Su existencia es importante, aunque no decisiva, ya que los conocimientos se pueden obtener por otras vías.

Sugerencia: Debe existir un plan de formación y/o concienciación para el personal que deba utilizar este dispositivo. En este plan de debe definir cómo hacer un buen uso del mismo y cuáles son sus riesgos asociados.

*52 - ¿Se ejecuta periódicamente el plan de formación y/o concienciación para el personal involucrado en el uso del dispositivo?*

Valoración: 30%. El plan no solo debe existir, sino que debe aplicarse.

Sugerencia: Debe ejecutarse periódicamente el plan de formación y/o concienciación para el personal involucrado en el uso del dispositivo. Esto es importante porque es frecuente que, con el paso del tiempo, el trabajador olvide información importante que se le comunicó solo inicialmente.

*53 - ¿Se actualiza el plan de formación y/o concienciación cuando aparecen cambios relevantes en el dispositivo o en su entorno?*

Valoración: 20%. Es importante, ya que un plan anticuado pierde valor.

Sugerencia: Se debe actualizar el plan de formación y/o concienciación cuando aparecen cambios relevantes en el dispositivo o en su entorno. De esta forma se maximiza la efectividad del plan de formación/concienciación y se evita que pueda quedar obsoleto o aportar información contradictoria que no se ajusta a las cualidades del dispositivo en el presente.

**Bloqueo del dispositivo**

*54 – ¿Está determinado el tiempo de inactividad en el uso del dispositivo que provoca su bloqueo automático y después, si persiste la inactividad, el cierre de sesiones automático?*

Valoración: 35%. El bloqueo automático es un elemento clave de protección.

Sugerencia: Se debe determinar un tiempo de inactividad en el uso del dispositivo que provoque su bloqueo automático y después, si persiste la inactividad, el cierre de sesiones automático. Con esta medida se minimiza el riesgo de que un tercero aproveche un momento en el que el trabajador ha dejado el dispositivo desatendido y decida utilizarlo para fines irresponsables.

*55 - ¿Está el tiempo de inactividad en el uso del dispositivo configurado dentro del mismo y es inalterable por el trabajador?*

Valoración: 25%. Es un factor importante el hecho de su inalterabilidad.

Sugerencia: Se debe configurar el tiempo de inactividad en el uso del dispositivo dentro del propio dispositivo y provocar que sea inalterable por el trabajador. De lo contrario, el trabajador podría tener la tendencia de extender ese periodo de tiempo por comodidad para evitar el proceso de autenticarse de nuevo, si bien esta idea aumenta el riesgo para el dispositivo.

*56 - ¿El equipo permanece apagado cuando no se está utilizando?*

Valoración: 20%. Estar encendido sin usarse hace vulnerable al dispositivo.

Sugerencia: El equipo debe permanecer apagado cuando no se está utilizando. Aunque puede resultar incómodo, así se asegura que el equipo quede protegido.

*57 - ¿El equipo permanece siempre conectado a la red o solo cuando hace uso de ella?*

Valoración: 20%. Mismo motivo que el apartado anterior.

Sugerencia: El equipo debe permanecer desconectado de la red cuando no esté haciendo uso de ella, para minimizar el riesgo de ataque.

**Protección del dispositivo**

*58 - ¿Está configurado el dispositivo para que solo se pueda acceder a internet mediante el uso de la red corporativa?*

Valoración: 40%. Tanto de forma local como remota, no usar la red corporativa compromete la seguridad del dispositivo.

Sugerencia: El dispositivo debe estar configurado para que solo se pueda acceder a internet mediante el uso de la red corporativa. Utilizar cualquier otra red alternativa, sobre todo si es pública, pone en riesgo al dispositivo y además no permite a la organización mantener un control del tráfico de datos.

*59 - ¿Está vetado el acceso remoto al dispositivo o bien está disponible con limitación en la información y los servicios accesibles?*

Valoración: 25%. Si existe la posibilidad de acceso remoto debe ser siempre en condiciones limitadas respecto al acceso local, por su mayor vulnerabilidad.

Sugerencia: Debe estar vetado el acceso remoto al dispositivo o bien, si está disponible, debe dar acceso a información y servicios limitados, solo cuando sean esenciales. El acceso remoto supone un aumento de riesgo para el dispositivo por lo que, en caso de que sea útil y necesario utilizarlo, debe estar limitado a las tareas imprescindibles.

*60 - ¿Existe un canal de comunicación y un procedimiento a seguir en caso de que el trabajador se percate de una incidencia en el dispositivo o descubra su avería, pérdida o robo?*

Valoración: 15%. Importante para que el trabajador conozca de antemano los pasos a seguir.

Sugerencia: Debe existir un canal de comunicación y un procedimiento a seguir en caso de que el trabajador se percate de una incidencia en el dispositivo o bien descubra su avería, pérdida o robo. Agilizar el proceso de comunicación aumenta las posibilidades de que la organización esté a tiempo de solventar, total o parcialmente, el problema reportado.

*61 - ¿El dispositivo está diseñado estructuralmente de forma que no pueda ser robado o bien está protegido mediante llaves o candados cuando no está en uso?*

Valoración: 10%. No es el factor principal de ataques, pero debe tenerse en cuenta.

Sugerencia: Dado que el dispositivo no está diseñado estructuralmente de forma que no pueda ser robado, debe estar protegido mediante llaves o candados cuando no está en uso. De esta forma se busca dificultar su robo, sobre todo cuando hablamos de dispositivos de pequeño tamaño.

*62 - ¿Permite la configuración del dispositivo que se extraiga información mediante un soporte extraíble?*

Valoración: 5%. Impacto ligero, dentro de una categoría con parámetros tan importantes.

Sugerencia: Dado que el dispositivo puede contener datos clínicos o personales, la configuración del mismo no debe permitir que se extraiga información mediante un soporte extraíble. De esta forma se limita la posibilidad de que esos datos se extraigan aun en caso de que una persona no autorizada logre acceder físicamente al dispositivo.

*63 - ¿Se suele utilizar el dispositivo con cámara y micrófono activados aun sin estar utilizándolos?*

Valoración: 5%. Impacto ligero, dentro de una categoría con parámetros tan importantes.

Sugerencia: La cámara y el micrófono deben estar siempre desactivados mientras no se esté haciendo un uso controlado de ellos. En caso de que el sistema haya sido hackeado, estos dos elementos serían una fuente muy poderosa de información para el atacante.

**Protección de datos personales**

*64 - ¿Existe una política de protección de datos personales aplicable a los datos personales gestionados por este dispositivo?*

Valoración: 55%. Aspecto imprescindible para los objetivos de este proyecto.

Sugerencia: Debe existir una política de protección de datos personales aplicable a los datos personales gestionados por este dispositivo. Los datos personales son el mayor activo a proteger de un dispositivo IoMT y requieren de una política propia.

*65 - ¿Existe un protocolo que defina con qué periodicidad se deben borrar los datos personales tanto en el dispositivo como en sus copias de seguridad?*

Valoración: 25%. El borrado de datos en desuso es clave, ya que multiplica la información potencial a ser robada.

Sugerencia: Debe existir un protocolo que defina con qué periodicidad se deben borrar los datos personales tanto en el dispositivo como en sus copias de seguridad. De esta forma la organización se asegura de que cualquier ataque no tenga acceso, en ningún caso, a datos personales antiguos que no deberían estar guardados en el dispositivo.

*66 - ¿Se ha nombrado un DPD (Delegado de Protección de Datos) cuya labor cubra la vigilancia de este dispositivo?*

Valoración: 10%. Esta figura, si se puede conseguir, aumenta notablemente la seguridad de los datos personales gestionados en el dispositivo.

Sugerencia: Se debe nombrar un DPD (Delegado de Protección de Datos) cuya labor cubra la vigilancia de este dispositivo. La figura del DPD es importante, especialmente en organizaciones públicas, para mejorar la protección de datos personales, ya que se encarga de asesorar en el cumplimiento de la legislación al respecto.

*67 - ¿Existen procedimientos internos para identificar incidentes relativos a la vulneración de datos personales, facilitar su reporte a la AEPD (Agencia Española de Protección de Datos) y la pertinente comunicación a las personas afectadas?*

Valoración: 10%. El correcto reporte debe tener importancia pese a ser el último aspecto de la categoría.

Sugerencia: Deben crearse procedimientos internos para identificar incidentes relativos a la vulneración de datos personales, facilitar su reporte a la AEPD (Agencia Española de Protección de Datos) y la pertinente comunicación a las personas afectadas. De esta forma se organizan y se agilizan los procesos de comunicación a las autoridades, lo que facilitará una resolución rápida y efectiva.

**Mantenimiento del dispositivo**

*68 - ¿Se realizan de forma periódica mantenimientos del dispositivo?*

Valoración: 60%. Es un aspecto clave, porque los proveedores suelen solucionar amenazas con parches y actualizaciones.

Sugerencia: Deben realizarse de forma periódica mantenimientos del dispositivo, ya sea por parte del fabricante/proveedor o solicitarlos a la organización. Los mantenimientos son necesarios para comprobar que el dispositivo funciona correctamente y es seguro.

*69 - ¿Existe un procedimiento que determine cuándo ejecutar las nuevas actualizaciones?*

Valoración: 20%. Es importante para que todos los dispositivos actualicen cuando deben.

Sugerencia: Debe existir un procedimiento que determine cuándo ejecutar las nuevas actualizaciones. De esta forma se podrá decidir si probar la actualización en un dispositivo de forma controlada o bien instalarla en todos los dispositivos semejantes para no general incompatibilidades.

*70 - ¿Existe en el procedimiento un mecanismo para recuperar el estado original en caso de que una nueva actualización genere problemas?*

Valoración: 20%. Aspecto importante para subsanar errores surgidos con la actualización.

Sugerencia: Debe existir en el procedimiento de actualizaciones del dispositivo un mecanismo que permita seguir unos pasos que recuperen el estado original o anterior del dispositivo, en caso de que la nueva actualización genere problemas propios del dispositivo o de incompatibilidad con otros.

# 4 Implementación y validación de la solución propuesta

Para validar el cuestionario del Análisis de Riesgos se ha decidido realizar un programa sencillo en Java que permita automatizar las respuestas al mismo, la presentación de resultados siguiendo los parámetros establecidos durante el proyecto y la presentación de un listado de sugerencias con los cambios prioritarios, ordenados, que deberían realizarse para maximizar la mejora de seguridad del dispositivo.

Este programa se implementará con la codificación de dos clases Java de tipo *JFrame*, que servirán para mostrar en su interfaz gráfica dos ventanas: una inicial en la que aparecen las 70 preguntas del cuestionario con sus posibles respuestas "sí/no" y otra que emerge al enviar el cuestionario, en la que se muestra un gráfico de barras con la valoración de cada uno de los cuatro niveles de seguridad, la seguridad general del dispositivo y la lista de cambios prioritarios sugeridos para mejorar la seguridad de dicho dispositivo.

Algunas características que debe cumplir el programa son las siguientes:

- El número de sugerencias de cambios a realizar será elegido por el usuario en la primera ventana. Estará limitado de uno a diez, puesto que la idea es que no aparezca un gran número de cambios, ya que el personal médico debe centrarse en resolverlos de forma ordenada e, idealmente, reevaluar el cuestionario tras realizar los primeros cambios que aparecen en dicha lista, actualizando las respuestas y atendiendo a los nuevos resultados y sugerencias.

- Las sugerencias no solo indicarán el cambio que debe realizarse, siempre que sea posible, sino que, en una labor formativa y de concienciación, se explicará el motivo por el que este cambio es importante para la seguridad de un dispositivo IoMT.

- Aquellas sugerencias relacionadas con cuestiones que se hayan respondido positivamente (que cumplen los criterios de seguridad) no deben aparecer en ningún caso en la lista de propuesta de cambios.

- La prioridad de un cambio no solo debe depender de manera estática de la valoración otorgada a ese riesgo y a su categoría, sino que debe ser dinámico en función de lo avanzado que esté cada nivel en cuanto a puntuación: es decir, si un nivel tiene menos porcentaje de seguridad que el resto, adquieren mayor prioridad los cambios que se puedan realizar para reducir los riesgos asociados a las categorías de ese nivel, con el fin de tender a igualar la seguridad de los niveles de abajo a arriba, y fortalecer el nivel básico de seguridad del dispositivo.

## 4.1 Automatización del Análisis de Riesgos

En este apartado se explica por qué el programa realizado cumple con los requisitos para considerarse una herramienta de automatización del Análisis de Riesgos, tal como se estableció en las restricciones del proyecto, al satisfacer las siguientes condiciones propias de una automatización [36][37]:

- **Reducción de la intervención humana:** Realizar un Análisis de Riesgos es una tarea compleja que para cualquier humano requiere de las siguientes acciones:
    - **Analizar la normativa existente:** Esta herramienta evita que el usuario necesite conocer ni analizar la normativa existente.
    - **Identificar los posibles riesgos:** Esta herramienta evita que el usuario necesite conocer qué situaciones suponen, o no, un riesgo, ya que su intervención en el cuestionario se limita a responder sin saber si un factor es positivo o negativo.
    - **Definir la probabilidad y gravedad (impacto) de cada riesgo:** Esta herramienta evita que el usuario necesite conocer ni definir qué impacto supone cada riesgo.
    - **Plantear un cuestionario que evalúe la presencia de esos riesgos:** Esta herramienta evita que el usuario tenga que crear ningún cuestionario.
    - **Transformar las respuestas en unos resultados medibles:** Esta herramienta le ofrece al usuario directamente unos resultados medibles en función de sus respuestas.
    - **Analizar qué medidas deben tomarse en función de los resultados:** Esta herramienta le ofrece al usuario directamente un listado de medidas, ordenadas por prioridad, que deben tomarse.
- **Análisis de datos y generación de resultados:** El programa procesa las respuestas y las convierte en resultados de forma automática.
- **Aportación de sugerencias variables personalizadas:** El programa es capaz de evaluar los resultados y de reordenar una lista interna de sugerencias, asociadas a cada riesgo, en función de los resultados obtenidos. De esta forma, el programa solo ofrece sugerencias de aspectos de seguridad respondidos negativamente por el usuario y su orden de prioridad varía en función de la relación de valoración entre los cuatro niveles de seguridad, haciendo que dos aspectos de seguridad incumplidos no tengan en cada ejecución la misma prioridad sobre el otro.

Los beneficios que aporta la automatización de una herramienta de Análisis de Riesgos son los siguientes:

- **Eficiencia:** Permite un ahorro de tiempo tanto para el usuario que responde a las cuestiones como para los evaluadores, cuya participación se limita a realizar una configuración correcta del programa.

- **Consistencia:** El Análisis de Riesgos se rige siempre por los mismos criterios, al ser siempre las mismas preguntas, el mismo mecanismo de evaluación y limitarse las respuestas a "sí" o "no", sin admitir respuestas intermedias en las que entre en juego la subjetividad.

- **Escalabilidad:** La herramienta podría llegar a ser utilizada por numerosos usuarios al mismo tiempo sin que esto requiera mayor participación humana.

## 4.2 Solución desarrollada

El programa desarrollado está compuesto por una clase principal, que únicamente ejecuta el programa invocando a la clase VentanaCuestionario, y dos clases de tipo *JFrame,* VentanaCuestionario y VentanaResultados, donde están codificados todos los aspectos que deben aparecer en cada una de las dos ventanas.

En los Anexos se adjuntan las partes más relevantes del código realizado (se omiten las partes repetitivas o cuyo algoritmo ya está incluido en el documento escrito).

Para la realización de las pruebas debe tenerse en cuenta que la respuesta "sí", que aparece por defecto, implica el cumplimiento de los requisitos de seguridad en todas las cuestiones excepto en las cuestiones: 10, 11, 57, 62 y 63, cuya respuesta que implica el cumplimiento de los requisitos de seguridad es "no". Por lo tanto, enviar el cuestionario con las respuestas que aparecen por defecto no es la respuesta que permite obtener un nivel de seguridad del 100%.

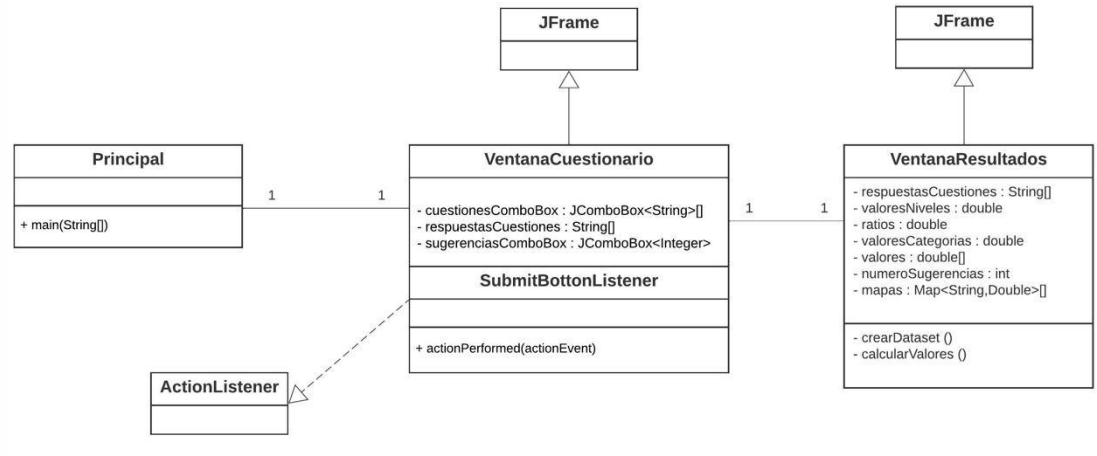



Figura 9: Diagrama de clases UML

### 4.2.1 Clase VentanaCuestionario

Esta clase de tipo *JFrame* se encarga de mostrar la ventana con las 70 preguntas del cuestionario, a las que se podrá responder afirmativamente o negativamente.

Tras completar el cuestionario, antes de pulsar en el botón “Enviar”, se podrá seleccionar las sugerencias que se desean ver en la siguiente ventana, una vez el programa haya analizado las respuestas dadas y los resultados obtenidos.

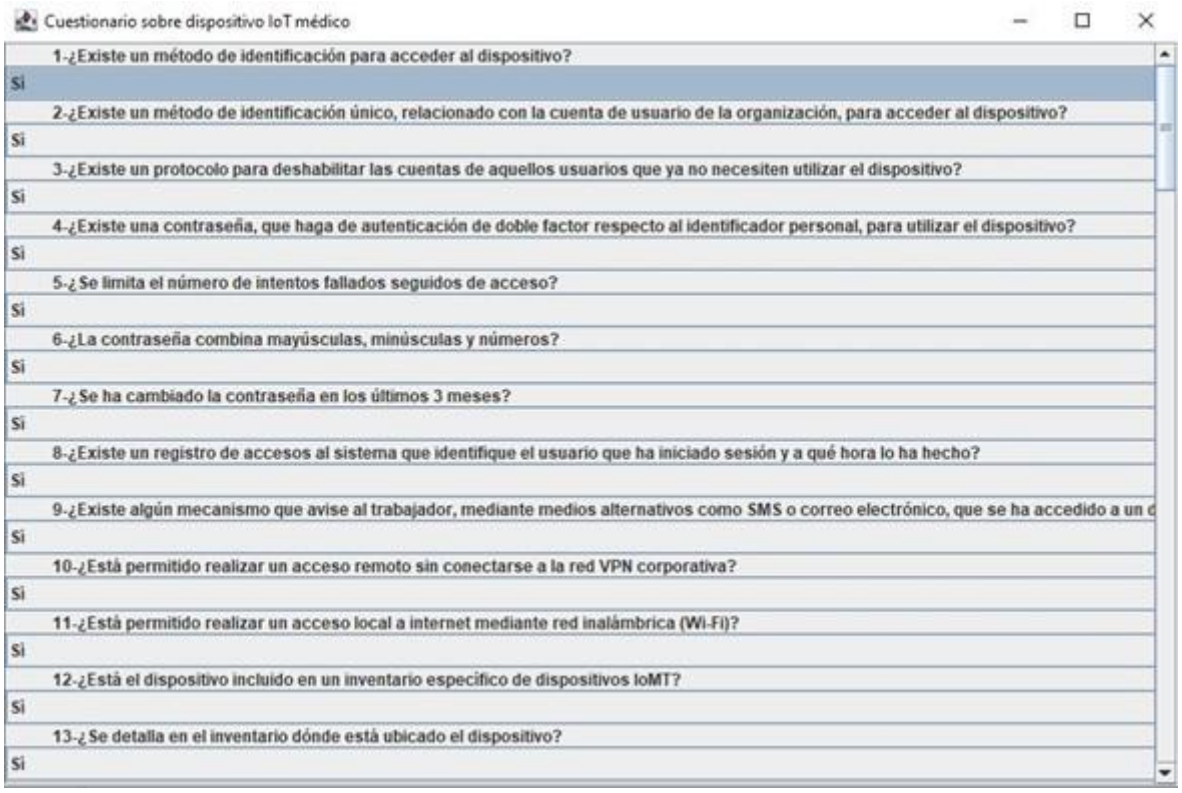



Figura 10: Ventana del cuestionario

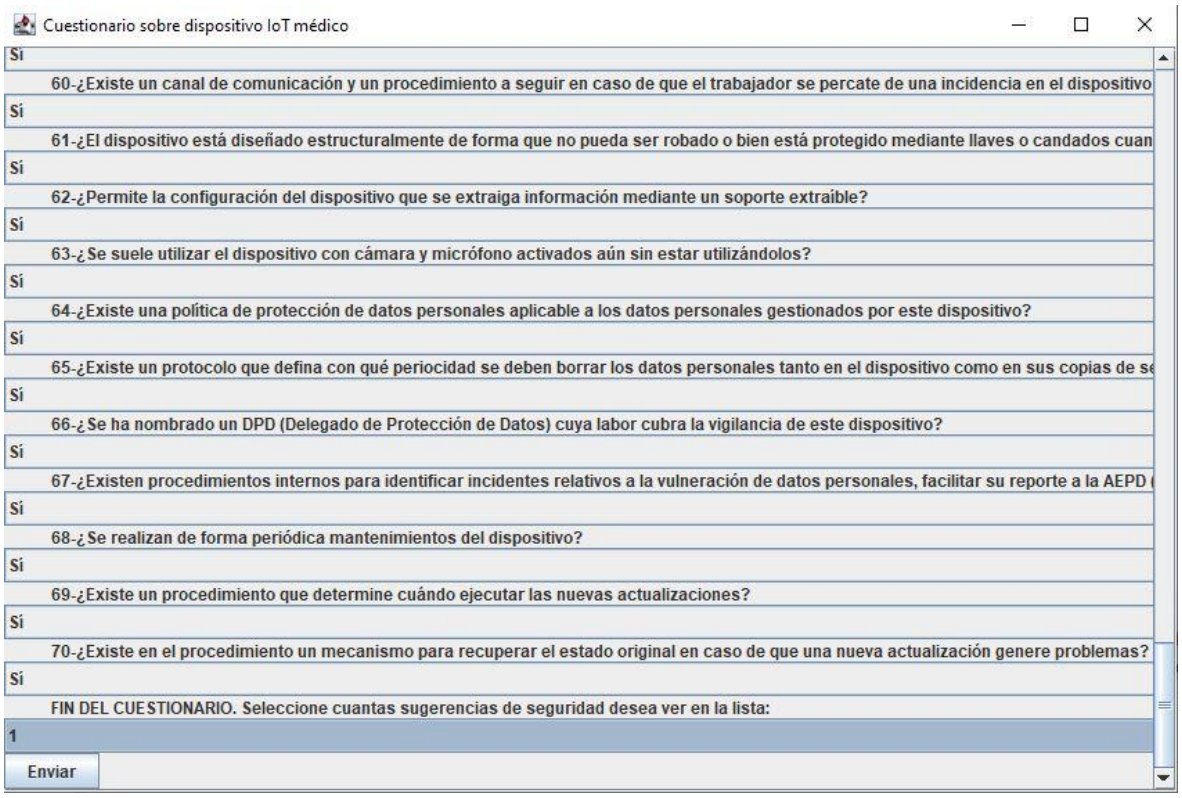



Figura 11: Envío del cuestionario y selección de número de sugerencias

La clase VentanaCuestionario está codificada de la siguiente forma:

1) Se guarda espacio para las 70 cuestiones en un *array* de *JComboBox* formado por *String*.

2) Se guarda en un *array* de *String* los títulos de las 70 cuestiones.

3) Se configuran las dos respuestas posibles y se añade al panel el primer *array* de *JComboBox* creado que mostrará las preguntas con sus respuestas desplegables.

4) Se configura la pregunta con el número de sugerencias siguiendo el mismo mecanismo.

5) Se crea el botón “Enviar” y la barra de *scroll*, ajustando su velocidad para permitir una mejor navegación por el cuestionario.

6) Se configura el *ActionListener* para cerrar esta ventana al pulsar el botón “Enviar” y abrir la nueva ventana con los resultados, perteneciente a la clase VentanaResultados, a la que se le pasará un *String* de 70 posiciones con las respuestas al cuestionario y un *Integer* con el número de sugerencias.

### 4.2.2 Clase VentanaResultados

Esta clase, también de tipo *JFrame*, se encarga de mostrar la ventana con los resultados y con la lista de sugerencias, ordenadas de forma prioritaria, que deberían tomarse para mejorar la seguridad del dispositivo.

Esta clase está codificada siguiendo los siguientes pasos:

1) Se crea un mapa de 70 posiciones, donde el elemento *key* será la sugerencia asociada y el elemento *value* será el valor potencial que puede tener requisito de seguridad.

2) En un *array* de valores, se añade cada una de las puntuaciones potenciales que puede tener cada requisito de seguridad, en base a la multiplicación del valor de la cuestión por el valor de su categoría, con los parámetros calculados en este documento.

3) En los casos en los que la respuesta a una cuestión sea insatisfactoria en términos de seguridad, se guarda en su mapa correspondiente la sugerencia asociada y su valor potencial. Posteriormente, se inicializa el valor a 0, para realizar posteriormente los cálculos de resultados sabiendo que esta cuestión no cumple con los requisitos de seguridad y, por tanto, no aporta valor a la puntuación final.

4) Se analizan las puntuaciones de los cuatro niveles y se crea un cálculo que establece un ratio entre las puntuaciones de cada nivel respecto al nivel más alto, de forma que exista un factor multiplicador para aumentar la prioridad de las sugerencias de seguridad correspondientes a los niveles con puntuaciones de seguridad más bajas.

5) Se realiza una comparación de los *value* guardados en los mapas, incluyendo el factor multiplicatorio para los niveles con puntuaciones más bajas, para ordenar en función de su prioridad la lista de sugerencias, para las cuales se mostrará el elemento *key* asociado a dicho valor del mapa.

6) Se crea el gráfico de resultados, editando algunos parámetros como el degradado del color de la barra de cada nivel en función de su puntuación.

7) Se añade al panel la puntuación global, calculada en base a los parámetros del proyecto (aclaración: la puntuación global no es la media de los niveles) y la lista ordenada con las sugerencias de cambios de seguridad prioritarios.

Más adelante, en el apartado donde se realizan pruebas para comprobar el correcto funcionamiento del programa, se aportan imágenes de la información que aparece en esta ventana.

## 4.3 Pruebas realizadas para comprobar el correcto funcionamiento del programa

Para comprobar el correcto funcionamiento del programa, se han realizado una serie de pruebas básicas, simulando los dos casos extremos y simulando un caso aleatorio, al que se le realizan una serie de modificaciones para comprobar el funcionamiento correcto del orden de las sugerencias en función de su prioridad.

- **Prueba con todos los parámetros de seguridad correctos:** Se espera un 100% de seguridad en cada nivel y en el nivel de seguridad total. No debería aparecer ninguna sugerencia de cambios.

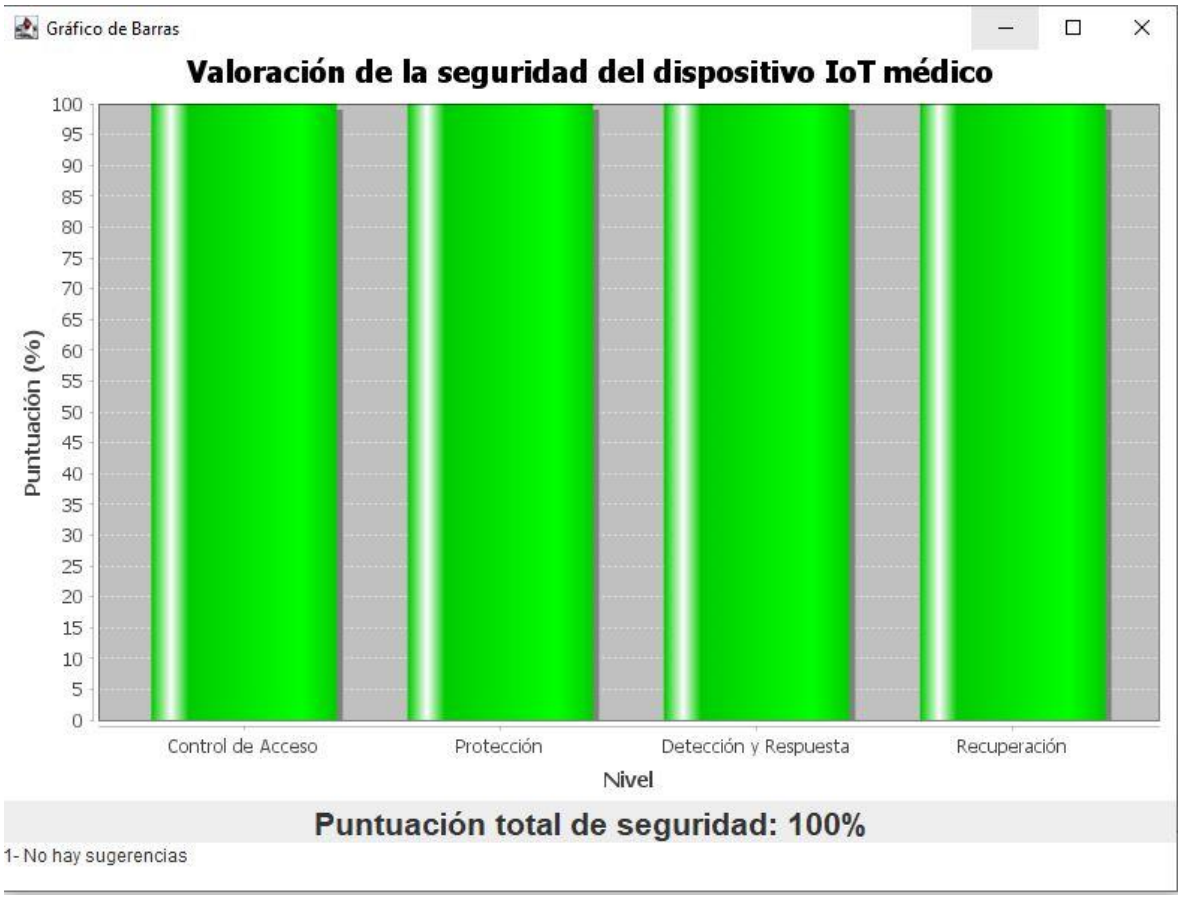



Figura 12: Prueba con nivel máximo de seguridad

- **Prueba con todos los parámetros de seguridad incorrectos:** Se espera un 0% de seguridad en cada nivel y en el nivel de seguridad total. El orden de las sugerencias de cambios debería coincidir con aquellas cuestiones y categorías de seguridad a las que mayor valoración se les ha dado.

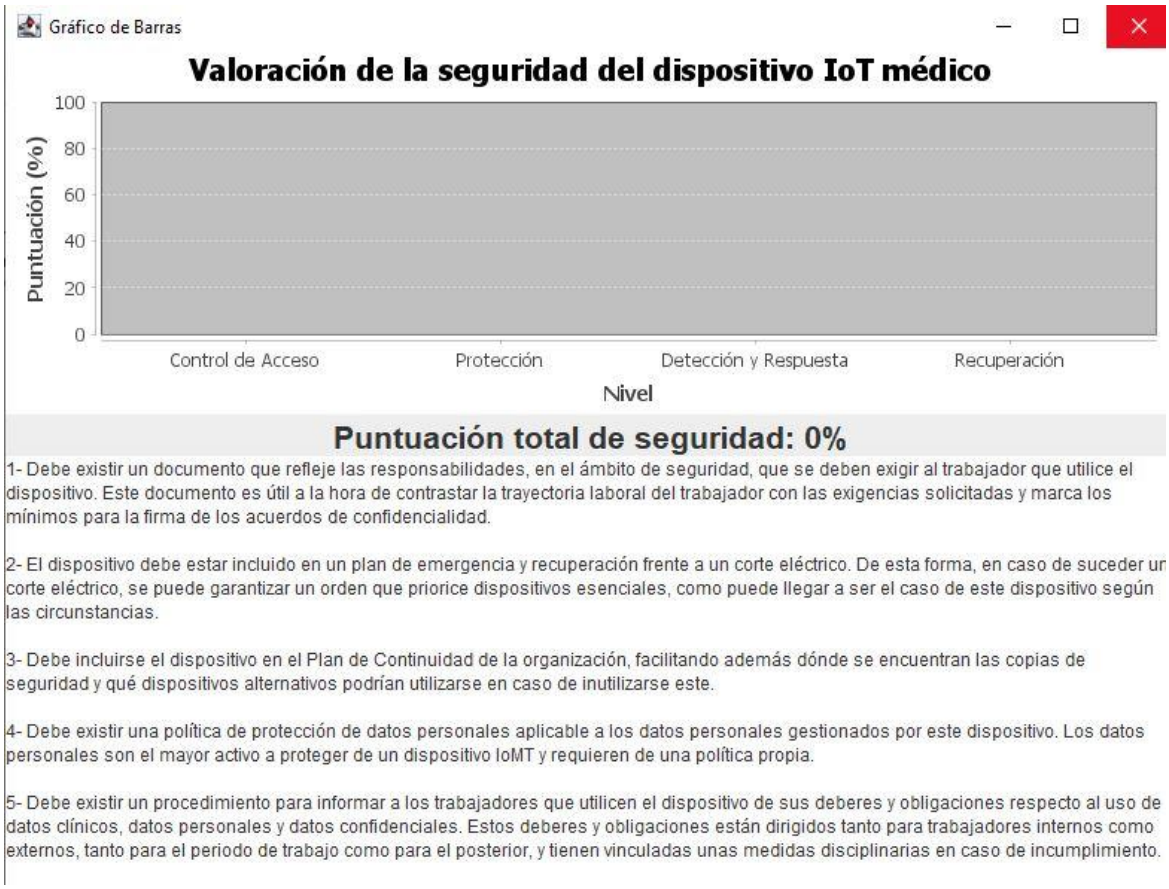



Figura 13: Prueba con el nivel mínimo de seguridad

Como se puede observar, la primera instrucción corresponde con la pregunta 49. Comprobando el documento observamos cómo esa cuestión es la más valiosa de su categoría, con un 60%, y al mismo tiempo su categoría es de las más valiosas. En el caso de otras categorías de valor similar o más alto, observamos cómo ninguna tiene una cuestión que alcance ese 60% de nivel, lo cual hace que esta cuestión se convierta en la más valiosa del Análisis de Riesgos.

- **Prueba de cambio dinámico de prioridades:** Para esta prueba se hace una respuesta aleatoria al cuestionario, obteniendo el siguiente resultado y las siguientes sugerencias:

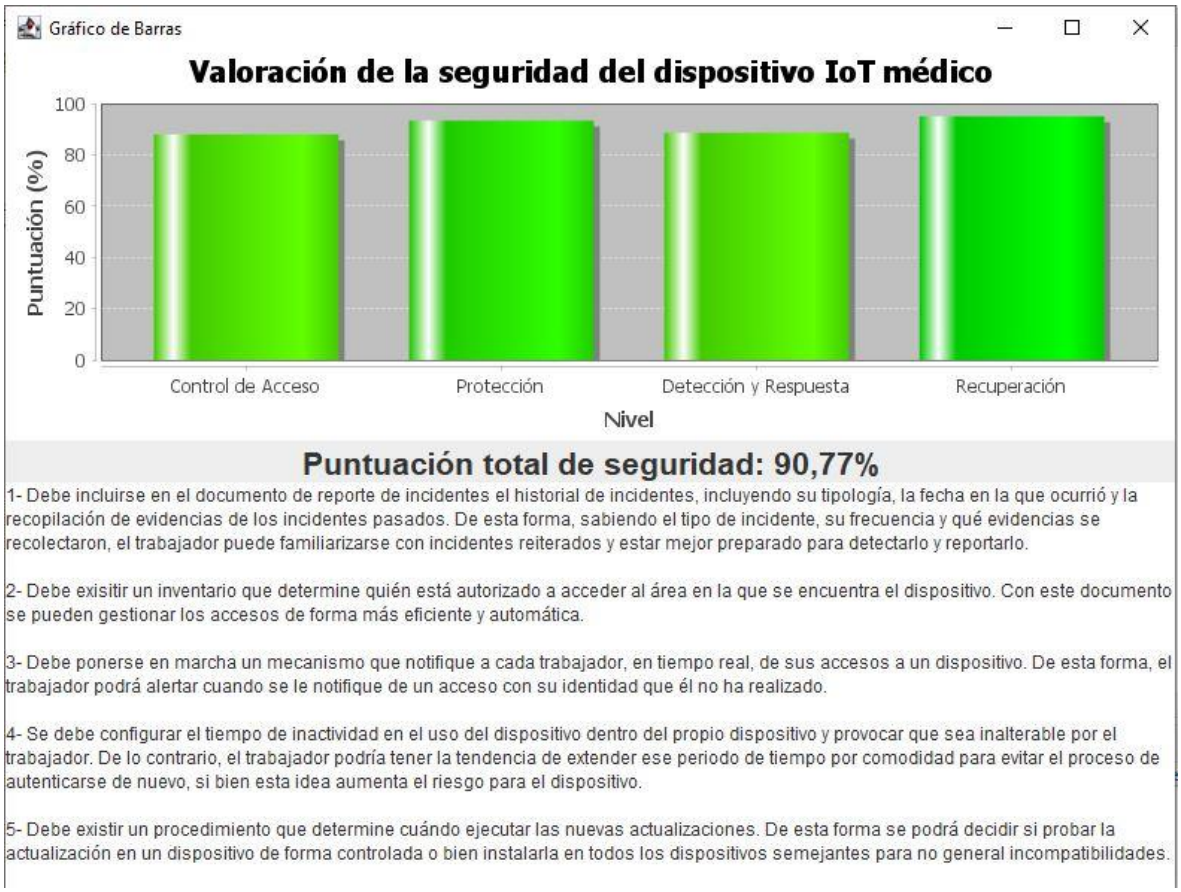



Figura 14: Prueba aleatoria de seguridad

La prueba aleatoria se ha realizado incumpliendo los requisitos de las cuestiones: 9, 19, 28, 32, 45, 52, 55 y 69, lo que supone dos por nivel.

Como podemos observar, la sugerencia número 1 hace referencia a la cuestión 19 (perteneciente al nivel de Detección y Respuesta), la sugerencia número 2 hace referencia a la cuestión 32 (perteneciente al nivel de Control de Acceso) y la sugerencia número 3 hace referencia a la cuestión número 9 (también del nivel de Control de Acceso). Ahora, lo que se pretende es rebajar el nivel de Control de Acceso y comprobar si, tal como se espera, las sugerencias asociadas a las cuestiones número 32 y 9 adelantan en prioridad a la sugerencia asociada a la cuestión 19, al multiplicarse su prioridad debido a la deficiencia de seguridad que tendrá el nivel al que pertenecen (Control de Acceso).

Para ello, se repiten las respuestas anteriores y además se incluye el incumplimiento de seguridad de cuatro cuestiones más pertenecientes al nivel de Control de Acceso: 4, 8, 31 y 35.


Figura 15: Comprobación prueba aleatoria

Como se puede observar, aunque con los nuevos incumplimientos de seguridad han entrado en el top3 tres nuevas sugerencias (todas del Control de Acceso), también podemos observar cómo, efectivamente, las anteriores sugerencias 2 y 3 ahora se sitúan en los puestos 4 y 5 mientras que, por otro lado, la anterior sugerencia número 1 ahora se sitúa en el puesto 6, detrás de estas dos sugerencias que ahora adquieren mayor prioridad.

Esta prueba también sirve para comprobar cómo, habiendo doce cuestiones que no satisfacen los requisitos de seguridad, y siendo solo seis de ellas del nivel de Control de Acceso, cinco de las seis sugerencias prioritarias de mejora de seguridad instan a cambiar parámetros relativos al Control de Acceso, al estar la valoración de este nivel muy por debajo del resto.

## 4.4 Comparativa de resultados del Análisis de Riesgos con una solución existente

En este apartado se comprobará la precisión del cálculo de resultados realizada durante el Análisis de Riesgos. Para ello, se utilizará el programa creado para realizar una evaluación real de un dispositivo IoMT, por parte de un técnico sanitario, y se compararán los resultados respecto a los obtenidos previamente en un Análisis de Riesgos realizado por un equipo de expertos en ciberseguridad, de la empresa española Cipherbit, al mismo dispositivo, siguiendo una evaluación mediante niveles de madurez basada en el marco normativo del Esquema Nacional de Seguridad.

Debido a los acuerdos de confidencialidad, los datos que se pueden aportar sobre el dispositivo son exclusivamente los siguientes:

- Es un dispositivo IoMT utilizado para tratamiento de diálisis.
- El dispositivo pertenece a un hospital español y se usa diariamente.

### 4.4.1 Análisis de Riesgos realizado por expertos en ciberseguridad

En este apartado se presentarán los detalles del Análisis de Riesgos realizado previamente por un equipo de expertos en ciberseguridad al dispositivo IoMT que se evaluará utilizando la herramienta creada.

Este Análisis de Riesgos consiste en realizar un estudio exhaustivo de cada control del Esquema Nacional de Seguridad, otorgando un nivel de madurez (L0-L1-L2-L3-L4-L5) a cada código de cada control (subcontrol), añadiendo resultados de posibles evidencias y hallazgos, una valoración de cumplimiento de los refuerzos y las novedades legales.

A continuación, se muestra un ejemplo de cómo se muestra la evaluación de cada control:

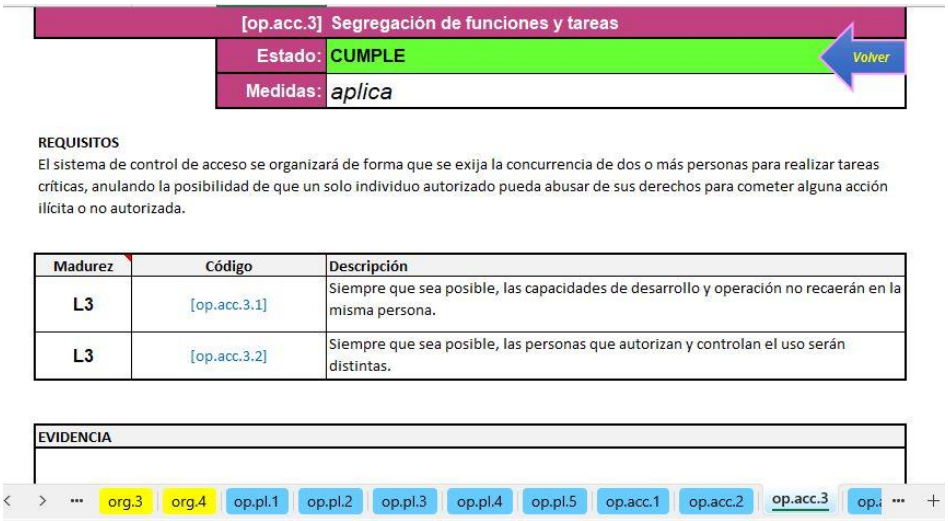



Figura 16: Ejemplo de evaluación (I)

| Implantado | REFUERZO | Código | Descripción |
|---|---|---|---|
| ☑ | R1 | [op.acc.3.r1.1] | Siempre que sea posible, la misma persona no aunará funciones de configuración y mantenimiento del sistema. |
| ☑ | R1 | [op.acc.3.r1.2] | La misma persona no puede aunar funciones de auditoría o supervisión con cualquier otra función. |
| ☐ | R2 | [op.acc.3.r2.1] | Existirán cuentas con privilegios de auditoría estrictamente controladas y personalizadas. |
| ☐ | R3 | [op.acc.3.r3.1] | El acceso a la información de seguridad del sistema estará permitido únicamente a los administradores de seguridad/sistema autorizados, utilizando los mecanismos de acceso imprescindibles (consola, interfaz web, acceso remoto, etc.). |

| NOVEDADES |
|---|
| La ley 2022 agrega el refuerzo R1 para Sistemas categorizados como ALTO para crear una segregación de funciones más rigurosa.<br>La existencia de cuentas de auditoría contemplado en la ley anterior para Sistemas de Información categorizados como MEDIO o ALTO pasa a ser un refuerzo no imprescindible para el cumplimiento.<br>Se añade el refuerzo R2, no necesario para el cumplimiento, para limitar el acceso de la información de seguridad únicamente a los administradores de seguridad/sistema autorizados. |

org.3 | org.4 | op.pl.1 | op.pl.2 | op.pl.3 | op.pl.4 | op.pl.5 | op.acc.1 | op.acc.2 | op.acc.3 | op.

Figura 17: Ejemplo de evaluación (II)

Por políticas internas y acuerdos con el cliente, en este caso los niveles de madurez L3 y superiores implican el cumplimiento de los requisitos necesarios, y los niveles de madurez L2 e inferiores implican que no se cumplen los requisitos previstos.

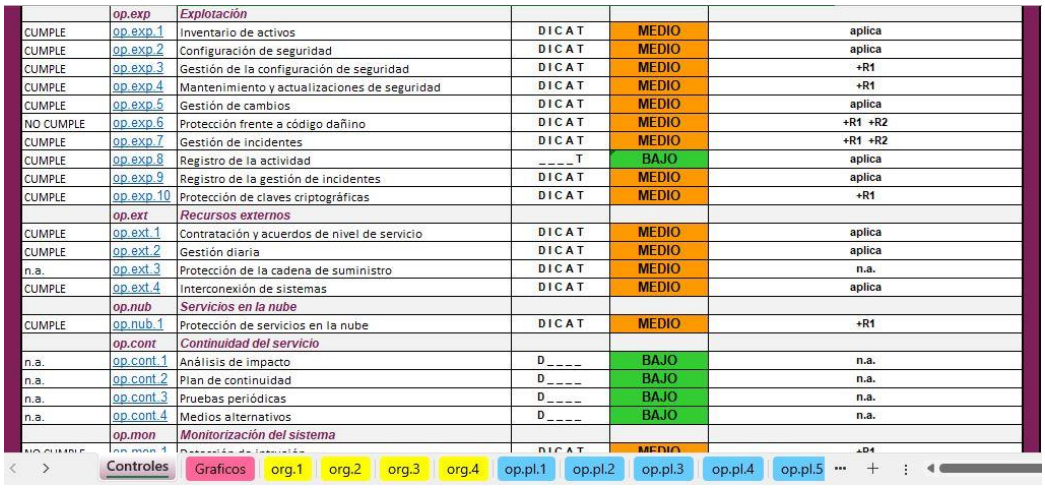
Aun así, para comparar este Análisis de Riesgos con el realizado en este proyecto, se tomará como referencia el estado general del control, definido como CUMPLE o NO CUMPLE, ya que es el que utiliza este análisis para realizar la evaluación definitiva del dispositivo.

Para ello, se muestra la valoración final (columna ESTADO a la izquierda del documento) de cada uno de los controles:

| | | | | | CATEGORIA POR DIMENSIÓN DEL SISTEMA | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Estado | Código | Descripción | Dimensiones | Cat. Sistema | D | I | C | A | T |
| | | | | MEDIO | BAJO | BAJO | MEDIO | BAJO | BAJO |
| | org | Marco organizativo | | | | | | | |
| CUMPLE | org.1 | Política de seguridad | D I C A T | MEDIO | aplica | | | | |
| CUMPLE | org.2 | Normativa de seguridad | D I C A T | MEDIO | aplica | | | | |
| CUMPLE | org.3 | Procedimientos de seguridad | D I C A T | MEDIO | aplica | | | | |
| CUMPLE | org.4 | Proceso de autorización | D I C A T | MEDIO | aplica | | | | |
| | op | Marco operacional | | | | | | | |
| | op.pl | Planificación | | | | | | | |
| CUMPLE | op.pl.1 | Análisis de riesgos | D I C A T | MEDIO | +R1 | | | | |
| NO CUMPLE | op.pl.2 | Arquitectura de Seguridad | D I C A T | MEDIO | +R1 | | | | |
| NO CUMPLE | op.pl.3 | Adquisición de nuevos componentes | D I C A T | MEDIO | aplica | | | | |
| CUMPLE | op.pl.4 | Dimensionamiento/gestión de la capacidad | D_ _ _ _ | BAJO | aplica | | | | |
| CUMPLE | op.pl.5 | Componentes certificados | D I C A T | MEDIO | aplica | | | | |
| | op.acc | Control de acceso | | | | | | | |
| CUMPLE | op.acc.1 | Identificación | _ _ _ A T | BAJO | aplica | | | | |
| CUMPLE | op.acc.2 | Requisitos de acceso | _ I C A T | MEDIO | aplica | | | | |
| CUMPLE | op.acc.3 | Segregación de funciones y tareas | _ I C A T | MEDIO | aplica | | | | |
| CUMPLE | op.acc.4 | Proceso de gestión de derechos de acceso | _ I C A T | MEDIO | aplica | | | | |
| NO CUMPLE | op.acc.5 | Mecanismo de autenticación (usuarios externos) | _ I C A T | MEDIO | + [R2 o R3 o R4] + R5 | | | | |
| NO CUMPLE | op.acc.6 | Mecanismo de autenticación (usuarios de la organización) | _ I C A T | MEDIO | + [R1 o R2 o R3 o R4] + R5 + R8 + R9 | | | | |

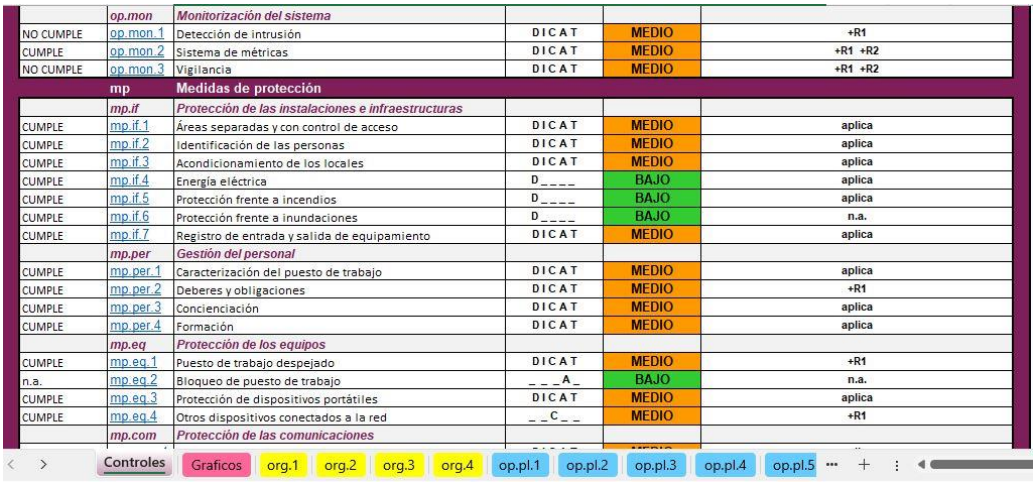
Controles | Graficos | org.1 | org.2 | org.3 | org.4 | op.pl.1 | op.pl.2 | op.pl.3 | op.pl.4 | op.pl.5

Figura 18: Valoración final (I)



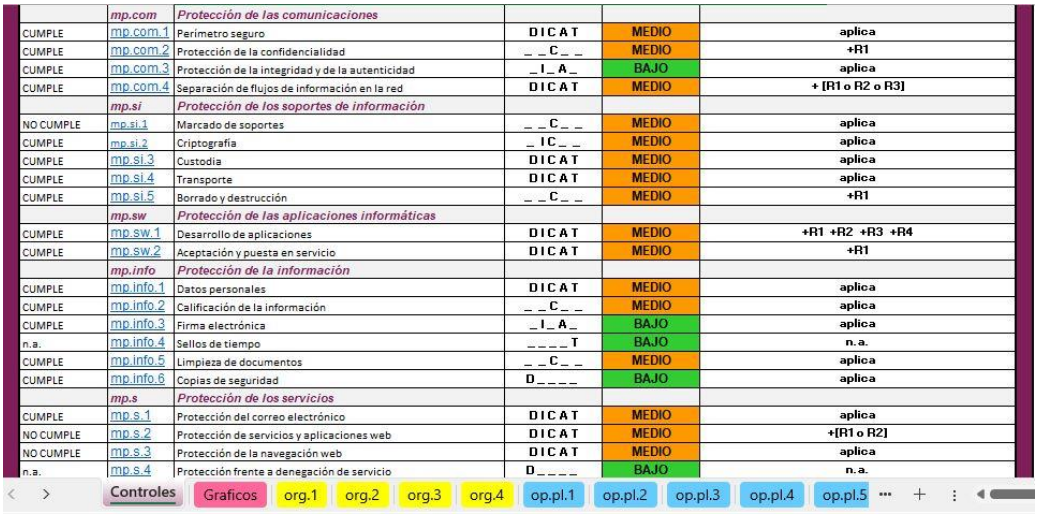
| | | | | | |
|---|---|---|---|---|---|
| | *op.exp* | *Explotación* | | | |
| CUMPLE | op.exp.1 | Inventario de activos | D I C A T | MEDIO | aplica |
| CUMPLE | op.exp.2 | Configuración de seguridad | D I C A T | MEDIO | aplica |
| CUMPLE | op.exp.3 | Gestión de la configuración de seguridad | D I C A T | MEDIO | +R1 |
| CUMPLE | op.exp.4 | Mantenimiento y actualizaciones de seguridad | D I C A T | MEDIO | +R1 |
| CUMPLE | op.exp.5 | Gestión de cambios | D I C A T | MEDIO | aplica |
| NO CUMPLE | op.exp.6 | Protección frente a código dañino | D I C A T | MEDIO | +R1 +R2 |
| CUMPLE | op.exp.7 | Gestión de incidentes | D I C A T | MEDIO | +R1 +R2 |
| CUMPLE | op.exp.8 | Registro de la actividad | _ _ _ _ T | BAJO | aplica |
| CUMPLE | op.exp.9 | Registro de la gestión de incidentes | D I C A T | MEDIO | aplica |
| CUMPLE | op.exp.10 | Protección de claves criptográficas | D I C A T | MEDIO | +R1 |
| | *op.ext* | *Recursos externos* | | | |
| CUMPLE | op.ext.1 | Contratación y acuerdos de nivel de servicio | D I C A T | MEDIO | aplica |
| CUMPLE | op.ext.2 | Gestión diaria | D I C A T | MEDIO | aplica |
| n.a. | op.ext.3 | Protección de la cadena de suministro | D I C A T | MEDIO | n.a. |
| CUMPLE | op.ext.4 | Interconexión de sistemas | D I C A T | MEDIO | aplica |
| | *op.nub* | *Servicios en la nube* | | | |
| CUMPLE | op.nub.1 | Protección de servicios en la nube | D I C A T | MEDIO | +R1 |
| | *op.cont* | *Continuidad del servicio* | | | |
| n.a. | op.cont.1 | Análisis de impacto | D _ _ _ _ | BAJO | n.a. |
| n.a. | op.cont.2 | Plan de continuidad | D _ _ _ _ | BAJO | n.a. |
| n.a. | op.cont.3 | Pruebas periódicas | D _ _ _ _ | BAJO | n.a. |
| n.a. | op.cont.4 | Medios alternativos | D _ _ _ _ | BAJO | n.a. |
| | *op.mon* | *Monitorización del sistema* | | | |
| NO CUMPLE | op.mon.1 | Detección de intrusión | D I C A T | MEDIO | +R1 |

Figura 19: Valoración final (II)



| | | | | | |
|---|---|---|---|---|---|
| | *op.mon* | *Monitorización del sistema* | | | |
| NO CUMPLE | op.mon.1 | Detección de intrusión | D I C A T | MEDIO | +R1 |
| CUMPLE | op.mon.2 | Sistema de métricas | D I C A T | MEDIO | +R1 +R2 |
| NO CUMPLE | op.mon.3 | Vigilancia | D I C A T | MEDIO | +R1 +R2 |
| | **mp** | **Medidas de protección** | | | |
| | *mp.if* | *Protección de las instalaciones e infraestructuras* | | | |
| CUMPLE | mp.if.1 | Áreas separadas y con control de acceso | D I C A T | MEDIO | aplica |
| CUMPLE | mp.if.2 | Identificación de las personas | D I C A T | MEDIO | aplica |
| CUMPLE | mp.if.3 | Acondicionamiento de los locales | D I C A T | MEDIO | aplica |
| CUMPLE | mp.if.4 | Energía eléctrica | D _ _ _ _ | BAJO | aplica |
| CUMPLE | mp.if.5 | Protección frente a incendios | D _ _ _ _ | BAJO | aplica |
| CUMPLE | mp.if.6 | Protección frente a inundaciones | D _ _ _ _ | BAJO | n.a. |
| CUMPLE | mp.if.7 | Registro de entrada y salida de equipamiento | D I C A T | MEDIO | aplica |
| | *mp.per* | *Gestión del personal* | | | |
| CUMPLE | mp.per.1 | Caracterización del puesto de trabajo | D I C A T | MEDIO | aplica |
| CUMPLE | mp.per.2 | Deberes y obligaciones | D I C A T | MEDIO | +R1 |
| CUMPLE | mp.per.3 | Concienciación | D I C A T | MEDIO | aplica |
| CUMPLE | mp.per.4 | Formación | D I C A T | MEDIO | aplica |
| | *mp.eq* | *Protección de los equipos* | | | |
| CUMPLE | mp.eq.1 | Puesto de trabajo despejado | D I C A T | MEDIO | +R1 |
| n.a. | mp.eq.2 | Bloqueo de puesto de trabajo | _ _ _ A _ | BAJO | n.a. |
| CUMPLE | mp.eq.3 | Protección de dispositivos portátiles | D I C A T | MEDIO | aplica |
| CUMPLE | mp.eq.4 | Otros dispositivos conectados a la red | _ _ C _ _ | MEDIO | +R1 |
| | *mp.com* | *Protección de las comunicaciones* | | | |

Figura 20: Valoración final (III)



| | | | | | |
|---|---|---|---|---|---|
| | *mp.com* | *Protección de las comunicaciones* | | | |
| CUMPLE | mp.com.1 | Perímetro seguro | D I C A T | MEDIO | aplica |
| CUMPLE | mp.com.2 | Protección de la confidencialidad | _ _ C _ _ | MEDIO | +R1 |
| CUMPLE | mp.com.3 | Protección de la integridad y de la autenticidad | _ I _ A _ | BAJO | aplica |
| CUMPLE | mp.com.4 | Separación de flujos de información en la red | D I C A T | MEDIO | + [R1 o R2 o R3] |
| | *mp.si* | *Protección de los soportes de información* | | | |
| NO CUMPLE | mp.si.1 | Marcado de soportes | _ _ C _ _ | MEDIO | aplica |
| CUMPLE | mp.si.2 | Criptografía | _ I C _ _ | MEDIO | aplica |
| CUMPLE | mp.si.3 | Custodia | D I C A T | MEDIO | aplica |
| CUMPLE | mp.si.4 | Transporte | D I C A T | MEDIO | aplica |
| CUMPLE | mp.si.5 | Borrado y destrucción | _ _ C _ _ | MEDIO | +R1 |
| | *mp.sw* | *Protección de las aplicaciones informáticas* | | | |
| CUMPLE | mp.sw.1 | Desarrollo de aplicaciones | D I C A T | MEDIO | +R1 +R2 +R3 +R4 |
| CUMPLE | mp.sw.2 | Aceptación y puesta en servicio | D I C A T | MEDIO | +R1 |
| | *mp.info* | *Protección de la información* | | | |
| CUMPLE | mp.info.1 | Datos personales | D I C A T | MEDIO | aplica |
| CUMPLE | mp.info.2 | Calificación de la información | _ _ C _ _ | MEDIO | aplica |
| CUMPLE | mp.info.3 | Firma electrónica | _ I _ A _ | BAJO | aplica |
| n.a. | mp.info.4 | Sellos de tiempo | _ _ _ _ T | BAJO | n.a. |
| CUMPLE | mp.info.5 | Limpieza de documentos | _ _ C _ _ | MEDIO | aplica |
| CUMPLE | mp.info.6 | Copias de seguridad | D _ _ _ _ | BAJO | aplica |
| | *mp.s* | *Protección de los servicios* | | | |
| CUMPLE | mp.s.1 | Protección del correo electrónico | D I C A T | MEDIO | aplica |
| NO CUMPLE | mp.s.2 | Protección de servicios y aplicaciones web | D I C A T | MEDIO | +[R1 o R2] |
| NO CUMPLE | mp.s.3 | Protección de la navegación web | D I C A T | MEDIO | aplica |
| n.a. | mp.s.4 | Protección frente a denegación de servicio | D _ _ _ _ | BAJO | n.a. |

Figura 21: Valoración final (IV)

El último elemento que servirá de comparativa de este documento es el gráfico de resultados finales, que se muestra a continuación:

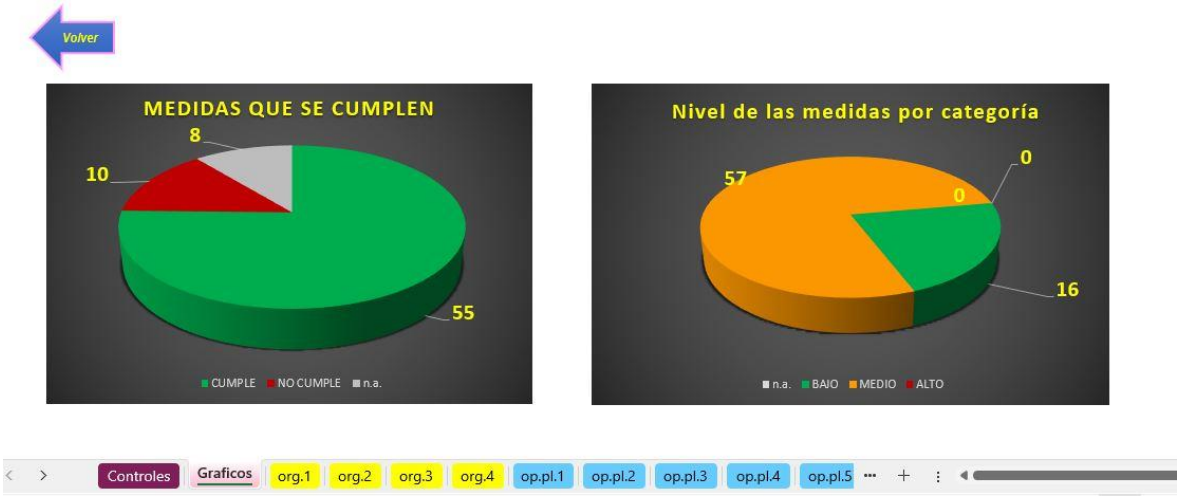



Figura 22: Gráfico de resultados

Como se puede observar en el gráfico de la izquierda, para la comparación futura con la herramienta creada en este proyecto, se cumplen los requisitos de 55 de los 73 controles del ENS, siendo 10 de los 18 restantes incumplidos y los otros 8 no analizados y evaluados como “no aplica”, lo que significa que, debido a la categoría por dimensión del sistema establecida, no son de necesario cumplimiento.

En el gráfico de la derecha se muestra el resumen del nivel de categoría del sistema, que refleja que 16 de los 73 controles presentan un nivel de categoría bajo (el nivel de categoría señala la exigencia que tendrán los requisitos de seguridad, no se debe asociar necesariamente con un nivel de seguridad bajo, sino con unas exigencias de seguridad más bajas a la hora de evaluar el dispositivo) y la mayoría, 57 de los 73 controles, presentan un nivel de categoría medio. El hecho de que predominen las exigencias de nivel medio, tendiendo a bajo, se alinea con las exigencias básicas de seguridad que tiene el Análisis de Riesgos de la herramienta creada en este proyecto.

### 4.4.2 Análisis de Riesgos realizado con la herramienta creada

Para comprobar el correcto funcionamiento del Análisis de Riesgos creado, se propone completar el cuestionario por parte del equipo técnico sanitario que trabaja con el dispositivo IoMT y comparar los resultados con el Análisis de Riesgos previo estudiado anteriormente.

El resultado del cuestionario reflejó que se cumplían los requisitos de 59 de las 70 categorías, siendo los 11 incumplidos los pertenecientes a las siguientes cuestiones:

*4: ¿Existe una contraseña, que haga de autenticación de doble factor respecto al identificador personal, para utilizar el dispositivo?*

*5: ¿Se limita el número de intentos fallados seguidos de acceso?*

*7: ¿Se ha cambiado la contraseña en los últimos 3 meses?*

*24: ¿Está el dispositivo incluido en el Plan de Continuidad de la organización?*

*25: ¿Existen copias seguridad en la nube, o en otros dispositivos físicos, del contenido de este dispositivo y están indicadas en el Plan de Continuidad?*

*26: ¿Está establecido en el Plan de Continuidad qué dispositivos alternativos podrían sustituir la labor de este dispositivo?*

*27: ¿Se realizan pruebas periódicas de continuidad con el dispositivo para evaluar el impacto en caso de inutilización o borrado de datos?*

*29: ¿Se realizan periódicamente pruebas de utilización de medios alternativos para suplir la labor del dispositivo en caso de inutilización?*

*30: ¿Existe un informe en el que se analicen los resultados de las pruebas periódicas de continuidad?*

*54 – ¿Está determinado el tiempo de inactividad en el uso del dispositivo que provoca su bloqueo automático y después, si persiste la inactividad, el cierre de sesiones automático?*

*55 - ¿Está el tiempo de inactividad en el uso del dispositivo configurado dentro del mismo y es inalterable por el trabajador?*

Al introducir los datos recibidos en la herramienta, los resultados fueron los siguientes:

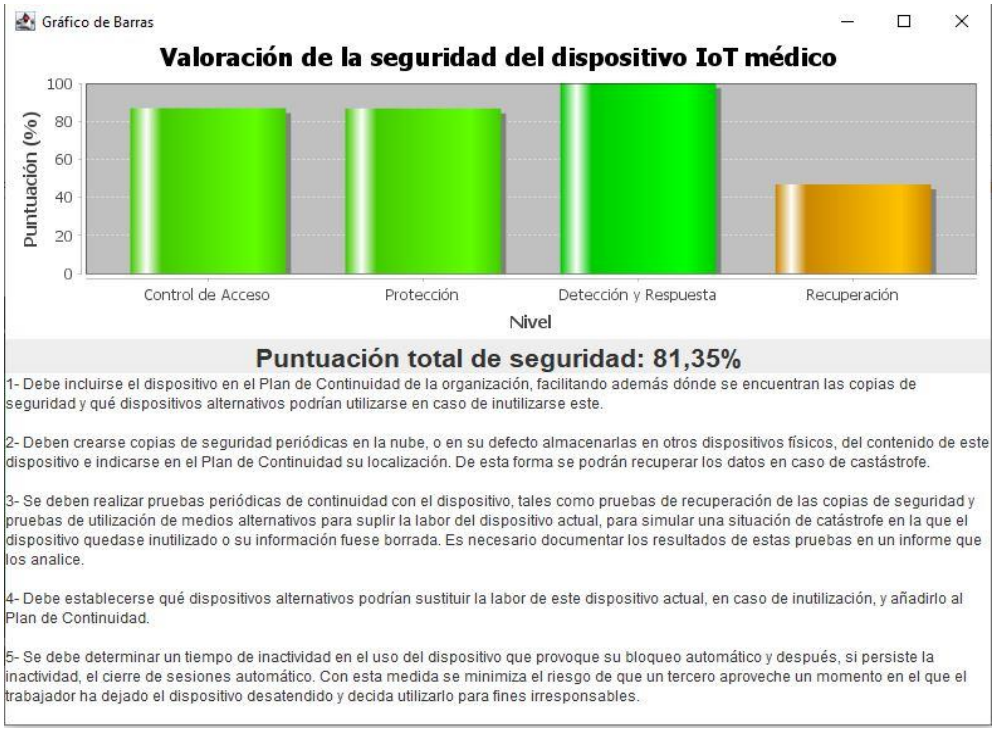



Figura 23: Resultados del Análisis de Riesgos propio

### 4.4.3 Conclusiones de la comparativa de resultados

Como se puede observar, la puntuación de seguridad calculada por la herramienta (81.35%) se muestra en sintonía con el resultado calculado en el Análisis de Riesgos hecho por los expertos en ciberseguridad, en el que el porcentaje de controles del ENS cumplidos era del 75%, si contamos los controles que “no aplican” como incumplidos (55 cumplidos de 73), o del 84%, si obviamos en el cálculo los controles que “no aplican” (55 cumplidos de 65).

Teniendo en cuenta las siguientes consideraciones:

- Hay controles en el Análisis de Riesgos realizado por los expertos que no se contemplan en la herramienta creada, por la naturaleza del proyecto y sus objetivos.

- Hay requisitos en la herramienta creada que, por su importancia, se repiten en varias cuestiones, se evalúan con mayor peso o sus exigencias están más detalladas.

- Todos los controles que “no aplican” en el primer Análisis de Riesgos son tenidos en cuenta en la herramienta creada, ya que sus exigencias están específicamente adaptadas a los dispositivos IoMT.

Con estas consideraciones, que hacen que cada uno de los dos Análisis de Riesgos tenga una naturaleza distinta, se puede deducir que el resultado comparativo obtenido es satisfactorio y que ayuda a validar la efectividad de la herramienta creada en este proyecto, teniendo en cuenta que, a pesar de todas las diferencias mencionadas que existen en la evaluación, los porcentajes de cumplimiento de los requisitos básicos apuntan en la misma línea.

# 5 Presupuesto

En este apartado se desglosa el presupuesto utilizado para la realización del proyecto, tanto a nivel de recursos técnicos como humanos:

## 5.1 Costes de equipo y software

El proyecto se ha realizado utilizando un ordenador portátil personal, con sistema operativo *Windows 10 Home*, generando un coste aproximado de 600€.

Además, se ha utilizado el software de Eclipse para la realización del programa en Java que muestra la interfaz gráfica con los resultados del Análisis de Riesgos.

| Recurso | Descripción | Coste |
|---|---|---|
| Ordenador portátil | Equipo personal con sistema operativo *Windows 10 Home* | 600€ |
| Eclipse | Entorno de desarrollo integrado para programación | 0€ |

Tabla 22: Costes de equipo y software

## 5.2 Costes de recursos humanos

El coste de los recursos humanos del proyecto se corresponde con el salario de un trabajador junior de ciberseguridad, con la titulación de Grado en Ingeniería Telemática, durante las 310 horas de trabajo invertidas.

Dado que este salario oscila entre los 23.000€ y los 27.000€ brutos anuales, a razón de 40 horas semanales, se puede estimar que el coste para un trabajo de 310 horas sería de aproximadamente 3.725€.

| Recurso | Descripción | Coste |
|---|---|---|
| Salario trabajador | Salario bruto medio para un trabajador junior de ciberseguridad durante 310h | 3725€ |

Tabla 23: Coste de recursos humanos

## 5.3 Coste total

A continuación, se resume el coste total demandado:

| | |
|---|---|
| Coste de equipo y software | 600€ |
| Coste de recursos humanos | 3725€ |
| **Coste total** | **4325€** |

Tabla 24: Coste total

# 6 Impacto del proyecto

En este apartado se analizará el impacto, en diversas áreas, que puede suponer la utilización de la herramienta creada en este proyecto.

## 6.1 Identificación de impactos y aspectos éticos, sociales y ambientales

En primer lugar, se define el escenario de análisis:

| | |
|---|---|
| Sector tecnológico | Ciberseguridad/salud |
| Ámbito organizativo/estratégico | Desarrollo de un producto |
| Ciclo de vida | Fase de diseño (proyecto universitario) |
| Contexto | De forma prioritaria, zonas de bajos recursos económicos y geográficamente incomunicadas |
| Grupos de interés | Empresas y organizaciones de la salud, tanto públicas como privadas |

Tabla 25: Escenario de análisis de impacto

En segundo lugar, se exponen los impactos, positivos y negativos que se deben tener en cuenta en uso de esta herramienta:

- **Aspectos éticos y legales:**
  - **Propiedad intelectual:** Se debe respetar el derecho de propiedad intelectual del Análisis de Riesgos creado para el proyecto y la herramienta que representa la interfaz gráfica con los resultados del mismo.
  - **Gestión de datos personales:** El proyecto resalta en todo momento, y así se refleja en las ponderaciones de seguridad, la necesidad de proteger los datos personales que suponen los datos clínicos de los pacientes que utilizan los dispositivos evaluados.
  - **Filtración de resultados:** El personal que trabaje con el dispositivo debe tener en cuenta que publicar o filtrar los resultados de la situación de seguridad de un dispositivo puede facilitar que se conozca una brecha de seguridad concreta del mismo e incentivar un ataque organizado.
- **Aspectos sociales:**
  - **Mejora de la seguridad básica:** Este proyecto tiene como objetivo ser utilizado por organizaciones en la fase inicial de mejora de seguridad de sus productos, contribuyendo a alcanzar unos mínimos de seguridad básicos.
  - **Ahorro de costes:** Esta herramienta gratuita supondría una gran oportunidad de negocio para organizaciones de zonas subdesarrolladas o con dificultades económicas, que no pueden permitirse la contratación de un servicio de consultoría de ciberseguridad.
  - **Labor formativa:** El proyecto contribuye, además de a mejorar la seguridad de los dispositivos, a la labor formativa del personal técnico sanitario que gestiona el dispositivo y, no necesariamente, tiene conocimientos en

ciberseguridad. Por ello todas las sugerencias de seguridad se explican razonadamente y en un lenguaje básico de ciberseguridad.

- **Alcance geográfico:** Es común que en muchas zonas incomunicadas tengan dispositivos IoMT cedidos por otra organización una vez deja de utilizarlos, muchas veces obsoletos. Sin embargo, su situación geográfica impide que un experto en seguridad o un trabajador del proveedor acudan presencialmente a evaluarlos, por los que no les dan uso o les dan un uso incorrecto. Esta herramienta interactiva tiene el propósito de que el propio personal técnico sanitario pueda hacer un uso seguro del dispositivo tras completar el Análisis de Riesgos y realizar las mejoras de seguridad sugeridas.

- **Aspectos ambientales:**
  - **Consumo de energía:** La mejora de la seguridad en dispositivos que consumen energía supondría una mayor utilización de estos dispositivos y, en consecuencia, un mayor uso energético. Por ello, se debe tener en cuenta que ese uso de energía se haga de manera eficiente. El proyecto, por una razón de seguridad y también de eficiencia, contempla el apagado y bloqueo de los dispositivos que no se están utilizando como un aspecto positivo que se busca conseguir.

## 6.2 Implicaciones éticas, sociales y ambientales

A continuación, se detallan los aspectos más relevantes que pueden suponer implicaciones negativas a tener en cuenta, si no se gestionan de forma correcta:

| Aspectos más relevantes | Descripción | Grupos/Sectores afectados | Normativas, leyes, estándares, códigos éticos | Posibilidades de evaluación |
|---|---|---|---|---|
| **Gestión de datos personales** | Es necesario proteger los datos personales que suponen los datos clínicos de los pacientes que utilizan los dispositivos evaluados. | Clientes (pacientes médicos) de la organización sanitaria | • Reglamento General de Protección de Datos (RGPD).<br>• Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).<br>• Ley 41/2002, regula aspectos del manejo de información clínica. | Monitorización del uso de datos personales, revisión periódica del tratamiento correcto de los datos clínicos, así como revisiones del borrado de los mismos cuando la normativa así lo exija. |

| | | | | |
|---|---|---|---|---|
| **Filtración de resultados** | El personal que trabaje con el dispositivo debe tener en cuenta que publicar o filtrar los resultados de la situación de seguridad de un dispositivo puede facilitar que se conozca una brecha de seguridad concreta del mismo e incentivar un ataque organizado. | La organización sanitaria, su prestigio y su balance económico | • Ley de Secretos Empresariales (LSE).<br>• Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI).<br>• Acuerdos de Confidencialidad (NDA). | Concienciación a los nuevos trabajadores de la herramienta, explicando las graves consecuencias de una filtración de resultados. |
| **Consumo energético** | La mejora de la seguridad en dispositivos que consumen energía supondría una mayor utilización de estos dispositivos y, en consecuencia, un mayor uso energético. Por ello, se debe tener en cuenta que ese uso de energía se haga de manera eficiente. | Sociedad, de forma general | • Directiva de Eficiencia Energética (2012/27/UE).<br>• Reglamento de Etiquetado Energético (2017/1369/UE).<br>• Plan de Acción de Ahorro y Eficiencia Energética. | Informes periódicos de consumo energético, haciendo énfasis en cuándo éste se produce sin que el dispositivo se esté utilizando. |

Tabla 26: Aspectos relevantes del impacto del proyecto

## 6.3 Objetivos de Desarrollo Sostenible

En relación a los Objetivos de Desarrollo Sostenible de la ONU, se espera que este proyecto aporte valor de forma positiva a los siguientes:


Figura 24: Objetivos de desarrollo sostenible

**3-Salud y bienestar:** Es el principal objetivo que abarca este proyecto. La protección en seguridad de los dispositivos médicos genera, sin duda alguna, un aumento de la calidad de vida de los pacientes, al disminuir los ataques (o su gravedad) a los dispositivos IoT médicos, lo que podría suponer la anulación de tratamientos, cirugías, etc.

**4-Educación de calidad:** La contribución a este objetivo se aporta, de forma muy tangencial, con el compromiso en formación en ciberseguridad a la hora de aportar las sugerencias que mejorarían la seguridad del dispositivo.

**9-Industria, innovación e infraestructura:** Este proyecto se puede considerar como una herramienta de innovación, que aporta valor a la sociedad en un campo de creación reciente y se ajusta a los nuevos problemas que surgen del continuo avance tecnológico, lo que inevitablemente supone, al mismo tiempo, un avance en los ataques a las tecnologías y a nuestros datos que guardamos en ellas.

**10-Reducción de las desigualdades:** El hecho de ser una aplicación sin coste, que fortalece los aspectos básicos de seguridad de los dispositivos IoMT, es fundamental para ayudar a países en desarrollo o zonas incomunicadas, que en muchas ocasiones reciben la donación de estos dispositivos, generalmente obsoletos, pero no pueden gestionar la seguridad de los mismos por la falta de recursos económicos y de conocimiento de la protección en seguridad del propio dispositivo, ya que el proveedor no se implica en productos obsoletos.

# 7 Conclusiones

En este proyecto se ha conseguido de forma satisfactoria crear un Análisis de Riesgos específico para dispositivos IoMT que pueda ser respondido por los trabajadores técnicos sanitarios sin necesidad de tener conocimientos en ciberseguridad.

Para ello, se realizó un estudio inicial sobre los dispositivos IoT y sus riesgos, así como, en mayor profundidad, de forma concreta en los dispositivos IoT médicos.

Tras estudiar los marcos normativos que hacen referencia a este tipo de dispositivos se llegó a la conclusión de que, entre las principales leyes y normativas, ninguna estaba orientada de forma concreta al uso diario del dispositivo, sino que se centraban en la creación del producto, su distribución y en las políticas de uso de la organización. Por ello, se propone crear un marco normativo básico pensado exclusivamente para dispositivos IoMT, para el cual se decide tomar el ENS como referencia, al ser el marco normativo que deben cumplir todas las organizaciones relacionadas con el sector público español. Para conseguirlo, se seleccionaron todos los controles pertinentes del ENS, se creó una nueva categorización a partir de ellos y se simplificaron las exigencias de seguridad para que todas las exigencias de cada nueva categoría se enfocaran en el uso diario del dispositivo por parte de los trabajadores sanitarios, obviando temas relacionados con la política de empresa, los contratos con proveedores y los temas avanzados de programación.

Tras ello, se hizo un estudio detallado de las principales herramientas de Análisis de Riesgos existentes, y se verificó que ninguna de ellas juntaba en su herramienta, al mismo tiempo, todos los requisitos específicos planteados para este proyecto.

Posteriormente, se puso en marcha la solución propuesta: crear un Análisis de Riesgos propio en el que las cuestiones planteadas y el método de valoración fueran ideados específicamente para el proyecto. Para conseguirlo, se realiza un estudio de los posibles métodos de valoración, se busca información sobre el impacto de cada riesgo, con el fin de otorgarle una valoración distinta a cada categoría de seguridad, se adaptan las conclusiones obtenidas a los dispositivos IoMT y al resto de características del proyecto y se generan las 70 cuestiones que permiten verificar las exigencias de seguridad de cada una de las 20 categorías que forman el marco normativo previamente creado.

Adicionalmente, se redacta una sugerencia personalizada para el caso de incumplimiento de los requisitos de seguridad, asociada a cada una de las 70 cuestiones. Cada sugerencia señala el cambio de seguridad que debería realizarse para lograr esos requisitos y explica por qué este cambio aporta mayor seguridad a cualquier dispositivo IoMT, haciendo una labor formativa para el personal sanitario en cuanto a ciberseguridad.

Por último, se valida el Análisis de Riesgos creado con una aplicación básica en Java que permita que un técnico sanitario pueda evaluar cada uno de los dispositivos IoMT con los que trabaja. Para ello, el programa ofrece una interfaz gráfica para que el usuario navegue por el cuestionario y responda a las cuestiones, procesa los datos respondidos y muestra una valoración de seguridad del dispositivo mediante un gráfico de barras, representando cada uno de los cuatro niveles de seguridad. Junto a la valoración de seguridad se

proporciona un listado ordenado de las sugerencias prioritarias que deberían modificarse para mejorar la seguridad del dispositivo IoMT evaluado.

Para comprobar el correcto funcionamiento del programa y la correcta selección del mecanismo de valoración, se realizan dos pruebas de verificación.

Previamente a la realización del proyecto se plantearon una serie de objetivos de diseño que debían cumplirse, cuyo cumplimiento se evalúa a continuación:

- **Automatizar los riesgos a los que puede estar expuesto un dispositivo IoMT**: Se cumple con la realización de un programa que automatiza un Análisis de Riesgos con 70 preguntas, que evalúan los riesgos más comunes a los que puede enfrentarse un dispositivo IoMT. Para ello se obvian aquellas cuestiones cuya respuesta necesitaría de conocimientos avanzados de ciberseguridad o de programación, que impedirían que el cuestionario fuera respondido íntegramente por los trabajadores sanitarios, tal como exigen las restricciones.
- **Validar las pruebas señalando de forma gráfica los resultados obtenidos del Análisis de Riesgos:** Se cumple presentado un gráfico de barras con los resultados del Análisis de Riesgos, dividiendo la valoración en cuatro niveles, siempre justificándose la valoración de cada uno de ellos y de cada una de sus categorías inferiores.
- **Aportar un resultado que guíe a los trabajadores sanitarios, sin necesidad de conocimientos en ciberseguridad, a adoptar las medidas necesarias para mejorar la seguridad del dispositivo:** Se cumple con el listado de sugerencias prioritarias para mejorar la seguridad, explicando los motivos por los que cada cambio es relevante, asumiendo siempre que el trabajador sanitario no debería tener conocimientos en ciberseguridad y realizando, además, una labor formativa.
- **Garantizar el cumplimiento de las medidas de seguridad internacionales para el tratamiento adecuado de los datos clínicos almacenados:** Se cumple incluyendo en todo momento, y dándoles una gran importancia en cuando a ponderación, los controles del ENS que hacen referencia al tratamiento de datos personales, provocando que, siempre que un dispositivo no cumpla con el correcto tratamiento de datos personales, un cambio prioritario sea la corrección de esta vulnerabilidad.

En definitiva, el proyecto cumple con los objetivos previstos, sin necesitar para ello vulnerar las restricciones planteadas. Además, se puede considerar que la herramienta creada parte de una idea original, es útil para su propósito específico y las decisiones tomadas para crearla se sostienen mediante un dedicado estudio a un campo de trabajo complejo como es la ciberseguridad.

# 8 Trabajos futuros

Tras la realización del proyecto, se plantean los siguientes escenarios de mejora para el futuro:

- **Ajuste de la ponderación:** Pese a que se ha tratado de realizar la ponderación y la valoración de cada categoría de manera objetiva y argumentada, una revisión por parte de expertos de las valoraciones y un estudio del impacto a largo plazo causado por las sugerencias de seguridad (evaluar si realmente son tan efectivas como se presupone), facilitaría un ajuste de la ponderación que se adecuara con mayor precisión a la realidad.
- **Utilización de IA (inteligencia artificial) para complementar los parámetros de seguridad evaluados:** En todo el proyecto se advierte de la limitación de los parámetros de seguridad para que sean básicos y, así, el personal médico pueda completar el cuestionario del Análisis de Riesgos sin necesidad de conocimientos en ciberseguridad y en programación. Sin embargo, la inclusión de inteligencia artificial podría facilitar que también se evaluaran los aspectos más complejos de seguridad, siempre sin necesidad de conocimientos avanzados por parte del personal sanitario y sin la necesidad de contratar a expertos en ciberseguridad, manteniendo el espíritu del proyecto.
- **Añadir persistencia al programa:** El hecho de añadir persistencia permitiría guardar datos de cada dispositivo (aunque surgirían nuevas problemáticas de impacto que habría que vigilar), para facilitar la reevaluación del mismo una vez se hayan aplicado algunos cambios de seguridad, guardando los datos del Análisis de Riesgos previo, e incluso utilizar esos datos guardados para poder realizar una gráfica que muestre la evolución de seguridad del dispositivo desde que se utilizó inicialmente el programa.
- **Gráficas dinámicas:** Un factor de mejora, a nivel de comodidad del usuario, sería conseguir que éste pudiera ver la variación de la gráfica según responde o cambia las respuestas del Análisis de Riesgos.
- **Respuestas abiertas en el Análisis de Riesgos:** Con un algoritmo más complejo, sería posible cambiar las respuestas de “sí/no” por respuestas abiertas que reflejen cifras, fechas, etc. En este aspecto también podría ser positivo incluir el uso de IA para dejar respuestas totalmente abiertas, que sean interpretadas por la inteligencia artificial y que las traduzca a una evaluación fija.

# 9 Referencias

[1] Check Point Software, «Check Point Software alerta de los riesgos de los dispositivos IoT en la Sanidad: el 70% de los dispositivos médicos no cuentan con soporte», Comunicae, 10 de enero de 2024. https://comunicae.es/notas-de-prensa/los-riesgos-de-los-dispositivos-iot-en-la (accedido 24 de febrero de 2024)

[2] Interpol, «COVID-19-Cybercrime-Analysis-Report-August-2020-1.pdf», Agosto 2020.

[3] CIS, «Barómetro de Enero 2024», CIS, 5 de enero de 2024. https://www.cis.es/documents/d/cis/es3435mar_a (accedido 26 de abril de 2024).

[4] Claroty, «claroty-healthcare-survey-report-aug-2023-cg-2.pdf», Agosto 2023.

[5] R. Gallego, «Ciberataques a nuestro sistema de salud, ¿estamos preparados?», Secure&IT, 29 de enero 2024. https://www.secureit.es/ciberataques-a-nuestro-sistema-de-salud-estamos-preparados (accedido 27 de febrero de 2024).

[6] Sap, «¿Qué es internet de las cosas (IoT)?», https://www.sap.com/spain/products/artificial-intelligence/what-is-iot.html#:~:text=Internet%20de%20las%20cosas%20(IoT)%20es%20una%20red%20de%20objetos,hacia%20otras%20cosas%20y%20sistemas%E2%80%93 (accedido 6 de marzo de 2024).

[7] Ambit Bst, «Internet de las cosas médicas (IoMT). Tecnología aplicada a la salud», 15 de junio de 2021. https://www.ambit-bst.com/blog/internet-de-las-cosas-m%C3%A9dicas-iomt-tecnolog%C3%ADa-aplicada-a-la-salud (accedido 6 de marzo de 2024).

[8] RiskRecon & Cyentia Institute, «El 86% de los problemas de seguridad de los dispositivos IoT son calificados como críticos», 3 de marzo de 2021. https://www.itdigitalsecurity.es/endpoint/2021/03/el-86-de-los-problemas-de-seguridad-de-los-dispositivos-iot-son-calificados-como-criticos (accedido 5 de marzo de 2024).

[9] D. Garrote, «Riesgos de Seguridad en IoT», 22 de octubre de 2022. https://nuclio.school/blog/riesgos-de-seguridad-en-iot (accedido 5 de marzo de 2024).

[10] Kaspersky, «2020_Kaspersky_IoT_report.pdf», 2020.

[11] Incibe, «https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia-de-seguridad-iot.pdf», 26 de mayo de 2020.

[12] E. Nieva, Check Point Research, «Los riesgos de los dispositivos IoT en la Sanidad», 9 de enero de 2024. https://revistabyte.es/actualidad-it/iot-sanidad (accedido 6 de marzo de 2024).

[13] PWC, «Informe Global Telecom Outlook 2023-2027», Global Telecom Outlook, 15 de noviembre de 2023. https://www.pwc.es/es/telecomunicaciones/global-telecom-outlook-2023-2027.html (accedido 3 de mayo de 2024).

[14] ISOTools, «Norma ISO/IEC 30141 sobre Internet de las Cosas (IoT)», https://www.isotools.us/2018/11/21/norma-iso-iec-30141-internet-cosas-iot (accedido 7 de marzo de 2024).

[15] Service Manage Institute, «ISO/IEC 27400:2022 para la ciberseguridad y privacidad del IoT», 23 de enero de 2023. https://news.itsmf.es/iso-iec-274002022-para-la-ciberseguridad-y-privacidad-del-iot (accedido 7 de marzo de 2024).

[16] Wireless Logic, «Nuevas regulaciones en seguridad IoT: Ley de Ciberresiliencia», 27 de octubre de 2023, https://internetdelascosas.xyz/articulo.php?id=4195 (accedido 7 de marzo de 2024).

[17] Ministerio del Interior, «Guía sobre Seguridad en Dispositivos IoT.pdf», 2 de agosto de 2023.

[18] Parlamento Europeo, «REGLAMENTO (UE) 2017/745 DEL PARLAMENTO EUROPEO Y DEL CONSEJO», 5 de abril de 2017, https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32017R0745 (accedido 12 de abril de 2024).

[19] ISO 14971:2019(es), «Dispositivos médicos/productos sanitarios (MD) — Aplicación de la gestión del riesgo a los MD», 10 de diciembre de 2019, https://www.iso.org/obp/ui#iso:std:iso:14971:ed-3:v1:es (accedido 12 de abril de 2024).

[20] NIST SP 800-53 Rev. 5, «Security and Privacy Controls for Information Systems and Organizations», 23 de septiembre de 2020, https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final (accedido 18 de abril de 2024).

[21] BOE, «Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad», https://www.boe.es/buscar/act.php?id=BOE-A-2022-7191 (accedido 11 de marzo de 2024).

[22] CCN, «Solución PILAR», https://pilar.ccn-cert.cni.es/index.php/pilar/que-es-pilar (accedido 27 de abril de 2024).

[23] Wolters Kluwer, «BowTieXP visión general de propiedades», https://www.wolterskluwer.com/es-es/solutions/enablon/bowtie/bowtiexp (accedido 4 de junio de 2024).

[24] RiskWatch, «Manage Risk, Meet Compliance, Improve Security», https://www.riskwatch.com/ (accedido 11 de mayo de 2024).

[25] Asimily, «Introducing Asimily Risk Simulations», https://asimily.com/blog/introducing-new-asimily-risk-simulations/ (accedido 14 de junio de 2024).

[26] CCN-cert, «Guía de Seguridad de las TIC CCN-STIC 804», junio de 2017, https://www.ccn-cert.cni.es/es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/505-ccn-stic-804-medidas-de-implantancion-del-ens/file?format=html (accedido 1 de mayo de 2024).

[27] SilverIT, «Entendiendo: El "Framework for Improving Critical Infrastructure Cybersecurity" del NIST», 28 de mayo de 2020, https://blog.silverit.co/entendiendo-el-framework-for-improving-critical-infrastructure-cybersecurity-del-nist (accedido 22 de mayo de 2024).

[28] McKinsey&Company, «Cyber risk measurement and the holistic cybersecurity approach», noviembre de 2018, https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Cyber%20risk%20measurement%20and%20the%20holistic%20cybersecurity%20approach/Cyber-risk-measurement-and-the-holistic-cybersecurity-approach-vf.pdf

[29] NIST, «Consideraciones para la gestión de riesgos a la ciberseguridad y la privacidad de internet de las cosas (IoT)», junio de 2019, https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8228es.pdf#:~:text=URL%3A%20https%3A%2F%2Fnvlpubs.nist.gov%2Fnistpubs%2Fir%2F2021%2FNIST.IR.8228es.pdf%0AVisible%3A%200%25%20

[30] Kaspersky, «Los riesgos de seguridad y las buenas prácticas de la Internet de las cosas», https://latam.kaspersky.com/resource-center/preemptive-safety/best-practices-for-iot-security (accedido 2 de mayo de 2024).

[31] Delta Protect, «Seguridad en Internet de las cosas (IoT): todo lo que debes saber», fecha, https://www.deltaprotect.com/blog/seguridad-iot-ciberseguridad-de-internet-de-las-cosas (accedido 2 de mayo de 2024).

[32] HEALTH IT SECURITY, «53% of Connected Medical Devices Contain Critical Vulnerabilities», 21 de enero de 2022, https://healthitsecurity.com/news/53-of-connected-medical-devices-contain-critical-vulnerabilities (accedido 5 de mayo de 2024).

[33] Binariks, «Understanding IoMT Security: A Comprehensive Guide», 20 de diciembre de 2023, https://binariks.com/blog/iomt-security-risks-best-practices/ (13 de abril de 2024).

[34] Empeek, «Healthcare IoT Security: Risks, Issues, Best Practices, and Our Advice», 14 de abril de 2023, https://empeek.com/insights/healthcare-iot-security-risks-issues-best-practices-and-our-advice/ (accedido 13 de abril de 2024).

[35] Claroty, «IoMT 101: Guide to Internet of Medical Things Security», 10 de marzo de 2023, https://claroty.com/blog/iomt-101-guide-to-the-internet-of-medical-things (accedido 15 de abril de 2024).

[36] Wrike, «Unlocking Efficiency: How to Automate Tasks Effectively», 2 de septiembre de 2023, https://www.wrike.com/blog/unlocking-efficiency-with-automation/ (accedido 13 de junio de 2024).

[37] TechTarget, «IT automation», diciembre de 2022, https://www.techtarget.com/searchitoperations/definition/IT-automation#:~:text=IT%20automation%20is%20the%20use,data%20centers%20and%20cloud%20deployments (accedido 13 de junio de 2024).

# 10 Anexos

## Anexo 1: Programa Principal

```
public class Principal {

    public static void main(String[] args) {
        SwingUtilities.invokeLater(() -> {
            new VentanaCuestionario().setVisible(true);
        });
    }
}
```

## Anexo 2: Ventana del cuestionario

```
import java.awt.Component;
import java.awt.Dimension;
import java.awt.event.ActionEvent;
import java.awt.event.ActionListener;

import javax.swing.BoxLayout;
import javax.swing.JButton;
import javax.swing.JComboBox;
import javax.swing.JFrame;
import javax.swing.JLabel;
import javax.swing.JPanel;
import javax.swing.JScrollPane;
import javax.swing.SwingUtilities;

/**
 * Esta clase de tipo JFrame muestra una ventana con un cuestionario de 70 preguntas
 * correspondientes a la evaluación de seguridad del dispositivo IoT médico
 * determinada en el documento escrito del proyecto
 *
 * @author Javier Garcia Vida
 * @version 1.0
 *
 */
class VentanaCuestionario extends JFrame {

	/**
	 *
	 */
	private static final long serialVersionUID = 1L;
	private JComboBox<String>[] cuestionesComboBox;  //array para incluir los ComboBox de las 70 preguntas
	private String[] respuestasCuestiones=new String[70];
	private JComboBox<Integer> sugerenciasComboBox;

    @SuppressWarnings("unchecked")
	public VentanaCuestionario() {

	cuestionesComboBox=new JComboBox[70];
	  for (int i=0; i<cuestionesComboBox.length; i++) {
	      cuestionesComboBox[i]=new JComboBox<>();
	  }

	  setTitle("Cuestionario sobre dispositivo IoT médico");
	  setSize(400,300);
	  setExtendedState(JFrame.MAXIMIZED_BOTH); //pantalla completa
	  setLocationRelativeTo(null);
	  setDefaultCloseOperation(JFrame.EXIT_ON_CLOSE);

	  JPanel panel=new JPanel();
	  panel.setLayout(new BoxLayout(panel,BoxLayout.Y_AXIS));
	  add(panel);

	  String[] cuestiones={
```

```
                "1-¿Existe un método de identificación para acceder al
dispositivo?",
// SE OMITE LA LISTA CON TODAS LAS CUESTIONES
            };


        for (int i=0; i<cuestiones.length; i++) {  //edicion del comboBox para
que se responda con un SÍ/NO
            panel.add(new JLabel(cuestiones[i]));
            cuestionesComboBox[i]=new JComboBox<>(new String[]{"Sí", "No"});
            cuestionesComboBox[i].setMaximumSize(new
Dimension(Integer.MAX_VALUE,cuestionesComboBox[i].getPreferredSize().height));
            panel.add(cuestionesComboBox[i]);
        }

        Integer[] opcionesSugerencias=new Integer[10];   //max 10 sugerencias,
la idea es dar solo una pequeña
        for (int i=0; i<10; i++) {                       //lista de cambios
prioritarios, aunque el programa
            opcionesSugerencias[i]=i+1;                  //internamente haya
ordenado todos los cambios necesarios
        }
        sugerenciasComboBox=new JComboBox<>(opcionesSugerencias);
        sugerenciasComboBox.setMaximumSize(new
Dimension(Integer.MAX_VALUE,sugerenciasComboBox.getPreferredSize().height));
        panel.add(new JLabel("FIN DEL CUESTIONARIO. Seleccione cuantas
sugerencias de seguridad desea ver en la lista:"));
        panel.add(sugerenciasComboBox);    //se guardan en esta ventana las
sugerencias para utilizarlas en la siguiente

        JButton enviar=new JButton("Enviar");
        enviar.setAlignmentX(Component.CENTER_ALIGNMENT);
        panel.add(enviar);
        enviar.addActionListener(new SubmitButtonListener());

        JScrollPane scroll=new JScrollPane(panel);

scroll.setVerticalScrollBarPolicy(JScrollPane.VERTICAL_SCROLLBAR_AS_NEEDED);

scroll.setHorizontalScrollBarPolicy(JScrollPane.HORIZONTAL_SCROLLBAR_NEVER);
        scroll.getVerticalScrollBar().setUnitIncrement(16); //velocidad de la
barra scroll vertical
        add(scroll);
    }

    private class SubmitButtonListener implements ActionListener {
        @Override
        public void actionPerformed(ActionEvent e) {

            for (int i=0; i<70; i++) {  //se guarda en un array todas las
respuestas para usarlas en los resultados

respuestasCuestiones[i]=(String)cuestionesComboBox[i].getSelectedItem();
            }

            int
numeroSugerencias=(Integer)sugerenciasComboBox.getSelectedItem();
```

```
            //cerrar ventana cuestionario
            dispose();

            //ventana con los resultados (gráfico de barras)
            SwingUtilities.invokeLater(() -> {

             VentanaResultados resultados=new VentanaResultados(   //se le pasa
el array de respuestas y el numero de sugerencias
                        respuestasCuestiones,numeroSugerencias
                    );


                resultados.setSize(800,600);
                resultados.setVisible(true);
            });
        }
    }
}
```

## Anexo 3: Ventana de los resultados

```
import java.awt.BorderLayout;
import java.awt.Color;
import java.awt.Dimension;
import java.awt.Paint;

import javax.swing.BoxLayout;
import javax.swing.JFrame;
import javax.swing.JLabel;
import javax.swing.JPanel;

import org.jfree.chart.ChartFactory;
import org.jfree.chart.ChartPanel;
import org.jfree.chart.JFreeChart;
import org.jfree.chart.axis.ValueAxis;
import org.jfree.chart.plot.CategoryPlot;
import org.jfree.chart.plot.PlotOrientation;
import org.jfree.chart.renderer.category.BarRenderer;
import org.jfree.data.category.CategoryDataset;
import org.jfree.data.category.DefaultCategoryDataset;

import java.util.Arrays;
import java.util.HashMap;
import java.util.Map;

import javax.swing.JTextArea;
import javax.swing.SwingConstants;

import java.text.DecimalFormat;
/**
 * Esta clase de tipo JFrame muestra una ventana con un gráfico de barras tras la evaluación por niveles del
 * dispositivo IoT médico, la puntuación global de seguridad y la lista de sugerencias prioritarias
 * (numero a elegir por usuario, de 1 a 8) que deberían tomarse para maximizar la mejora de seguridad
 *
 * @author Javier Garcia Vida
 * @version 1.0
 *
 */
public class VentanaResultados extends JFrame {

	/**
	 *
	 */
	private static final long serialVersionUID = 1L;

	@SuppressWarnings("unused")
	private String[] respuestasCuestiones=new String[70];
	private double valorControlAcceso, valorProteccion, valorDetYRes,
valorRecuperacion;
    private double ratioControlAcceso, ratioProteccion, ratioDetYRes,
ratioRecuperacion;
    private double valorCategoria1, valorCategoria2, valorCategoria3,
valorCategoria4, valorCategoria5, valorCategoria6, valorCategoria7,
```

```
    valorCategoria8, valorCategoria9, valorCategoria10, valorCategoria11,
valorCategoria12, valorCategoria13, valorCategoria14,
    valorCategoria15, valorCategoria16, valorCategoria17, valorCategoria18,
valorCategoria19, valorCategoria20;
    private double valores[]=new double[70];
    @SuppressWarnings("unused")
      private int numeroSugerencias=0;

    @SuppressWarnings("unchecked")
      private Map<String, Double>[] mapas=new HashMap[70];

    public VentanaResultados(String[] respuestasCuestiones, int
numeroSugerencias) {
          this.respuestasCuestiones=respuestasCuestiones;
          this.numeroSugerencias=numeroSugerencias;

          for (int i=0; i<mapas.length; i++) {
              mapas[i]=new HashMap<>();
              mapas[i].put("No hay sugerencias", 0.0);
          }

          valores[0] = 0.6 * 0.2195;       //se multiplica el porcentaje de
importancia de cada valor por el de su categoría
          valores[1] = 0.3 * 0.2195;       //estos valores están
predeterminados en el documento escrito del proyecto
          valores[2] = 0.1 * 0.2195;
          valores[3] = 0.5 * 0.1463;
          valores[4] = 0.35 * 0.1463;
          valores[5] = 0.1 * 0.1463;
          valores[6] = 0.05 * 0.1463;
          valores[7] = 0.4 * 0.2195;
          valores[8] = 0.25 * 0.2195;
          valores[9] = 0.2 * 0.2195;
          valores[10] = 0.15 * 0.2195;
          valores[11] = 0.45 * 0.0476;
          valores[12] = 0.2 * 0.0476;
          valores[13] = 0.2 * 0.0476;
          valores[14] = 0.05 * 0.0476;
          valores[15] = 0.05 * 0.0476;
          valores[16] = 0.05 * 0.0476;
          valores[17] = 0.3 * 0.4286;
          valores[18] = 0.2 * 0.4286;
          valores[19] = 0.2 * 0.4286;
          valores[20] = 0.2 * 0.4286;
          valores[21] = 0.1 * 0.4286;
          valores[22] = 1.0 * 0.0976;
          valores[23] = 0.5 * 0.4091;
          valores[24] = 0.3 * 0.4091;
          valores[25] = 0.2 * 0.4091;
          valores[26] = 0.75 * 0.1364;
          valores[27] = 0.1 * 0.1364;
          valores[28] = 0.1 * 0.1364;
          valores[29] = 0.05 * 0.1364;
          valores[30] = 0.5 * 0.2195;
          valores[31] = 0.3 * 0.2195;
          valores[32] = 0.1 * 0.2195;
          valores[33] = 0.1 * 0.2195;
          valores[34] = 0.5 * 0.0976;
          valores[35] = 0.2 * 0.0976;
```

```
            valores[36] = 0.2 * 0.0976;
            valores[37] = 0.1 * 0.0976;
            valores[38] = 0.6 * 0.037;
            valores[39] = 0.2 * 0.037;
            valores[40] = 0.2 * 0.037;
            valores[41] = 0.8 * 0.2727;
            valores[42] = 0.2 * 0.2727;
            valores[43] = 0.5 * 0.037;
            valores[44] = 0.3 * 0.037;
            valores[45] = 0.2 * 0.037;
            valores[46] = 0.6 * 0.037;
            valores[47] = 0.4 * 0.037;
            valores[48] = 0.6 * 0.4286;
            valores[49] = 0.4 * 0.4286;
            valores[50] = 0.5 * 0.0952;
            valores[51] = 0.3 * 0.0952;
            valores[52] = 0.2 * 0.0952;
            valores[53] = 0.35 * 0.2222;
            valores[54] = 0.25 * 0.2222;
            valores[55] = 0.2 * 0.2222;
            valores[56] = 0.2 * 0.2222;
            valores[57] = 0.4 * 0.3334;
            valores[58] = 0.25 * 0.3334;
            valores[59] = 0.15 * 0.3334;
            valores[60] = 0.1 * 0.3334;
            valores[61] = 0.05 * 0.3334;
            valores[62] = 0.05 * 0.3334;
            valores[63] = 0.55 * 0.3334;
            valores[64] = 0.25 * 0.3334;
            valores[65] = 0.1 * 0.3334;
            valores[66] = 0.1 * 0.3334;
            valores[67] = 0.6 * 0.1818;
            valores[68] = 0.2 * 0.1818;
            valores[69] = 0.2 * 0.1818;

                setTitle("Gráfico de Barras");
                setDefaultCloseOperation(JFrame.EXIT_ON_CLOSE);

                //se guarda el texto de sugerencia para el caso en el que no
cumpla los requisitos de seguridad
                //después se guarda el valor potencial máximo, antes de
inicializarlo a cero para los cálculos de puntuación
                if (respuestasCuestiones[0].equals("No")) {
                    mapas[0].put("El dispositivo debe configurarse para solicitar
un identificador en cada acceso que se realice. De esta forma se "
                            + "consigue que solo las personas que conozcan el
identificador puedan acceder al dispositivo.", valores[0]);
                    valores[0] = 0;
                }
//SE OMITE EL BUCLE CON CADA UNA DE LAS CUESTIONES Y SU SUGERENCIA ASOCIADA

                calcularValores();

                //comprobar el valor máximo de los 4 niveles para aumentar la
prioridad de los cambios
                //correspondientes a las categorías que se encuentran en los
niveles con porcentajes más bajos de seguridad
```

```
            double maxValor=Math.max(Math.max(valorControlAcceso,
valorProteccion), Math.max(valorDetYRes, valorRecuperacion));
            ratioControlAcceso=(Math.max(maxValor,
0.1))/(Math.max(valorControlAcceso,0.1)); //para que exista la división si el
valor de un nivel fuera 0
            ratioProteccion=(Math.max(maxValor,
0.1))/(Math.max(valorProteccion,0.1));
            ratioDetYRes=(Math.max(maxValor,
0.1))/(Math.max(valorDetYRes,0.1));
            ratioRecuperacion=(Math.max(maxValor,
0.1))/(Math.max(valorRecuperacion,0.1));

            //multiplico el valor potencial de cada cuestión que no cumple
los requisitos por el ratio de su nivel
            //ya actualizado con las puntuaciones reales, para priorizar aún
más las cuestiones de aquellos niveles con más
            //carencias de seguridad respecto al nivel más alto
            double[] ratios={ratioControlAcceso, ratioProteccion,
ratioDetYRes, ratioRecuperacion};
            int[][] grupos={
                {0,1,2,3,4,5,6,7,8,9,10,22,30,31,32,33,34,35,36,37},

{38,39,40,43,44,45,46,47,53,54,55,56,57,58,59,60,61,62,63,64,65,66},
                {11,12,13,14,15,16,17,18,19,20,21,48,49,50,51,52},
                {23,24,25,26,27,28,29,41,42,67,68,69}
            };
            for (int i=0; i<grupos.length; i++) {
                double ratio=ratios[i];
                for (int j=0; j<grupos[i].length; j++) {
                    int mapaIndex=grupos[i][j];
                    Map<String, Double> mapaAux=mapas[mapaIndex];

                    for (Map.Entry<String, Double> entry :
mapaAux.entrySet()) {
                       double valorModificado=entry.getValue()*ratio;
                       mapaAux.put(entry.getKey(),valorModificado);
                     }
                }
            }


            //proceso de seleccion de orden prioritario buscando el valor
(potencial) más alto
            //de entre las respuestas que no satisfacen los requisitos de
seguridad de su categoría
                String[] topClaves=new String[numeroSugerencias];
                double[] topValores=new double[numeroSugerencias];
                Arrays.fill(topValores,Double.NEGATIVE_INFINITY);

                for (int i=0; i<numeroSugerencias; i++) {
                    for (Map<String, Double> mapa : mapas) {
                        for (Map.Entry<String, Double> entry :
mapa.entrySet()) {
                            String clave=entry.getKey();
                            double valor=entry.getValue();
                            if (valor>topValores[i]) {
                                topValores[i]=valor;
                                topClaves[i]=clave;
                            }
```

```
                        }
                    }

                    //valor máximo pasa a 0 para que en el siguiente bucle el
mayor sea el siguiente
                    for (Map<String, Double> mapa : mapas) {
                        if (mapa.containsKey(topClaves[i])) {
                            mapa.put(topClaves[i], 0.0);
                        }
                    }
                }

        CategoryDataset dataset=crearDataset();

        //edición gráfico
        JFreeChart grafico=ChartFactory.createBarChart(
                "Valoración de la seguridad del dispositivo IoT médico",
                "Nivel",
                "Puntuación (%)",
                dataset,
                PlotOrientation.VERTICAL,
                false,true,false);

        CategoryPlot plot=grafico.getCategoryPlot();
        ValueAxis ejeY=plot.getRangeAxis();
        ejeY.setRange(0,100);

        //editar color de las barras del gráfico de forma degradada de verde a
rojo
        BarRenderer colores=new BarRenderer() {
            /**
                     *
                     */
                    private static final long serialVersionUID = 1L;

                    @Override
            public Paint getItemPaint(int fila,int columna) {
                double valor=dataset.getValue(fila,columna).doubleValue();
                if (valor < 10) {
                    return Color.getHSBColor(0f, 1.0f, 0.8f); //rojo
                } else if (valor < 15) {
                    return Color.getHSBColor(5/360f, 1.0f, 0.8f);
                } else if (valor < 20) {
                    return Color.getHSBColor(10/360f, 1.0f, 0.8f);
                } else if (valor < 25) {
                    return Color.getHSBColor(15/360f, 1.0f, 0.8f);
                } else if (valor < 30) {
                    return Color.getHSBColor(20/360f, 1.0f, 0.8f);
                } else if (valor < 35) {
                    return Color.getHSBColor(25/360f, 1.0f, 0.8f);
                } else if (valor < 40) {
                    return Color.getHSBColor(30/360f, 1.0f, 0.8f); //naranja
                } else if (valor < 45) {
                    return Color.getHSBColor(35/360f, 1.0f, 0.8f);
                } else if (valor < 50) {
                    return Color.getHSBColor(40/360f, 1.0f, 0.8f);
                } else if (valor < 55) {
                    return Color.getHSBColor(45/360f, 1.0f, 0.8f);
                } else if (valor < 60) {
```

```
                    return Color.getHSBColor(50/360f, 1.0f, 0.8f);
                } else if (valor < 65) {
                    return Color.getHSBColor(55/360f, 1.0f, 0.8f);
                } else if (valor < 70) {
                    return Color.getHSBColor(60/360f, 1.0f, 0.8f); //amarillo
                } else if (valor < 75) {
                    return Color.getHSBColor(70/360f, 1.0f, 0.8f);
                } else if (valor < 80) {
                    return Color.getHSBColor(80/360f, 1.0f, 0.8f);
                } else if (valor < 85) {
                    return Color.getHSBColor(90/360f, 1.0f, 0.8f);
                } else if (valor < 90) {
                    return Color.getHSBColor(100/360f, 1.0f, 0.8f);
                } else if (valor < 95) {
                    return Color.getHSBColor(110/360f, 1.0f, 0.8f);
                } else {
                    return Color.getHSBColor(120/360f, 1.0f, 0.8f); //verde
                }
            }
        };
        plot.setRenderer(colores);

        ChartPanel panelGrafico=new ChartPanel(grafico);
        panelGrafico.setPreferredSize(new Dimension(800,400));

        JPanel panelPrincipal=new JPanel();
        panelPrincipal.setLayout(new BorderLayout());

        panelPrincipal.add(panelGrafico,BorderLayout.CENTER);

        JPanel panelTexto=new JPanel();
        panelTexto.setLayout(new BoxLayout(panelTexto,BoxLayout.Y_AXIS));

        //puntuación total con la valoración dada a cada nivel en el documento escrito del proyecto
        double puntuacion=(valorControlAcceso*100*0.3694+valorProteccion*100*0.2432+valorDetYRes*100*0.1892+valorRecuperacion*100*0.1982);
        DecimalFormat decimales=new DecimalFormat("#.##");
        String puntuacionDecimales=decimales.format(puntuacion);


        JLabel puntuacionLabel=new JLabel("<html><div style='text-align: center; font-size: 16px; font-weight: bold;'>Puntuación total de seguridad: " + puntuacionDecimales +"%"+ "</div></html>");
        puntuacionLabel.setHorizontalAlignment(SwingConstants.CENTER);

        JPanel puntuacionPanel=new JPanel(new BorderLayout());
        puntuacionPanel.add(puntuacionLabel,BorderLayout.CENTER);
        panelTexto.add(puntuacionPanel);


        for (int i=0; i<topClaves.length; i++) {
            JTextArea textArea=new JTextArea((i+1) + "- " + topClaves[i]+"\n");
        //  la siguiente orden queda comentada para que pueda observarse cómo se gestiona la puntuación interna
        //  se debe tener en cuenta que esta puntuación puede ir más allá de 0 a 100, ya que depende de la diferencia entre niveles
```

```
        //  JTextArea textArea=new JTextArea((i+1) + "- " + topClaves[i] + "
(Puntuación: " + decimales.format(topValores[i]*100) + ")");
            textArea.setLineWrap(true);
            textArea.setWrapStyleWord(true);
            textArea.setEditable(false);
            panelTexto.add(textArea);
        }


        panelPrincipal.add(panelTexto,BorderLayout.SOUTH);
        setContentPane(panelPrincipal);
        pack();

      }

    /**
     * Añade a un dataset la puntuación, la etiqueta asociada y el nombre del
nivel
     *
     * @param void
     * @return un dataset con los valores de cada uno de los 4 niveles del
gráfico
     */
    private CategoryDataset crearDataset() {
        DefaultCategoryDataset dataset = new DefaultCategoryDataset();

        dataset.addValue(valorControlAcceso*100, "Valores", "Control de
Acceso");
        dataset.addValue(valorProteccion*100, "Valores", "Protección");
        dataset.addValue(valorDetYRes*100, "Valores", "Detección y Respuesta");
        dataset.addValue(valorRecuperacion*100, "Valores", "Recuperación");

        return dataset;
    }

    /**
     * Calcula los valores con la estructura diseñada en el documento escrito
del proyecto
     * 4 niveles de seguridad -> cada uno agrupa varias categorías
     * 20 categorías -> cada una agrupa varias cuestiones
     *
     * @param void
     * @return void
     */
    private void calcularValores() {
        valorCategoria1 = valores[0] + valores[1] + valores[2];
        valorCategoria2 = valores[3] + valores[4] + valores[5] + valores[6];
        valorCategoria3 = valores[7] + valores[8] + valores[9] + valores[10];
        valorCategoria4 = valores[11] + valores[12] + valores[13] + valores[14]
+ valores[15] + valores[16];
        valorCategoria5 = valores[17] + valores[18] + valores[19] + valores[20]
+ valores[21];
        valorCategoria6 = valores[22];
        valorCategoria7 = valores[23] + valores[24] + valores[25];
        valorCategoria8 = valores[26] + valores[27] + valores[28] +
valores[29];
        valorCategoria9 = valores[30] + valores[31] + valores[32] +
valores[33];
```

```
        valorCategoria10 = valores[34] + valores[35] + valores[36] +
valores[37];
        valorCategoria11 = valores[38] + valores[39] + valores[40];
        valorCategoria12 = valores[41] + valores[42];
        valorCategoria13 = valores[43] + valores[44] + valores[45];
        valorCategoria14 = valores[46] + valores[47];
        valorCategoria15 = valores[48] + valores[49];
        valorCategoria16 = valores[50] + valores[51] + valores[52];
        valorCategoria17 = valores[53] + valores[54] + valores[55] +
valores[56];
        valorCategoria18 = valores[57] + valores[58] + valores[59] +
valores[60] + valores[61] + valores[62];
        valorCategoria19 = valores[63] + valores[64] + valores[65] +
valores[66];
        valorCategoria20 = valores[67] + valores[68] + valores[69];

        valorControlAcceso = valorCategoria1 + valorCategoria2 +
valorCategoria3 + valorCategoria6 + valorCategoria9 + valorCategoria10;
        valorProteccion = valorCategoria11 + valorCategoria13 +
valorCategoria14 + valorCategoria17 + valorCategoria18 + valorCategoria19;
        valorDetYRes = valorCategoria4 + valorCategoria5 + valorCategoria15 +
valorCategoria16;
        valorRecuperacion = valorCategoria7 + valorCategoria8 +
valorCategoria12 + valorCategoria20;
    }
}
```