UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería Informática

Desarrollo de una guía de adecuación a estándares de seguridad para sistemas informáticos

Trabajo Fin de Grado

Grado en Ingeniería Informática

AUTOR/A: Pons Guinot, Joan Manuel

Tutor/a: Oltra Gutiérrez, Juan Vicente

CURSO ACADÉMICO: 2023/2024

Resumen

El aumento de las amenazas de ciberseguridad junto con la tendencia de digitalización ha llevado a las pequeñas y medianas empresas a buscar formas de proteger mejor sus sistemas informáticos y datos. Este Trabajo de Fin de Grado tiene como objetivo desarrollar una guía y una herramienta accesible que permitan a las compañías evaluar y mejorar su nivel de seguridad de la información, independientemente de sus conocimientos previos en ciberseguridad. La herramienta está alineada con normativas, estándares y entidades de seguridad como ISO 27001, NIST, HIPAA, PCI DSS, CIS y ENISA, asegurando tratar conceptos ampliamente estandarizados.

Para la creación de esta herramienta, se ha realizado una revisión exhaustiva de los estándares y mejores prácticas en seguridad de la información, así como un análisis de las principales amenazas que enfrentan las compañías en crecimiento digital, como el *ransomware* y el *phishing*. Se ha puesto especial énfasis en la implementación práctica de estos estándares para hacerlos accesibles y efectivos en el contexto de empresas de pequeño y mediano tamaño.

El resultado es una herramienta de autoevaluación implementada en Excel, que pretende ofrecer una evaluación del estado de madurez de las compañías con respecto a la seguridad de los sistemas informáticos existente. Esta herramienta cuenta con el objetivo de ayudar a identificar áreas de mejora y facilitar la adopción de medidas de protección adecuadas, contribuyendo a una gestión más segura y eficiente de los datos empresariales.

Palabras clave: estándares, herramienta, empresas pequeñas y medianas, sistemas TI, seguridad de la información, evaluación

Resum

L'augment de les amenaces de ciberseguretat junt amb la tendència de digitalització ha portat a les petites i mitjanes empreses a buscar formes de protegir millor els seus sistemes informàtics i dades. Aquest Treball de Fi de Grau té com a objectiu desenvolupar una guia i una eina accessible que permeten a les companyies avaluar i millorar el seu nivell de seguretat de la informació, independentment dels seus coneixements previs en ciberseguretat. L'eina està alineada amb normatives, estàndards i entitats de seguretat com ISO 27001, NIST, HIPAA, PCI DSS, CIS i ENISA, assegurant tractar conceptes àmpliament estandarditzats.

Per a la creació d'aquesta eina, s'ha realitzat una revisió exhaustiva dels estàndards i millors pràctiques en seguretat de la informació, així com una anàlisi de les principals amenaces que enfronten les companyies en creixement digital, com el ransomware i el phishing. S'ha posat especial èmfasi en la implementació pràctica d'aquests estàndards per a fer-los accessibles i efectius en el context d'empreses de xicotet i mitjà tamany.

El resultat és una eina d'autoavaluació implementada en Excel, que pretén oferir una avaluació de l'estat de maduresa de les companyies pel que fa a la seguretat dels sistemes informàtics existents. Aquesta eina compta amb l'objectiu d'ajudar a identificar àrees de millora i facilitar l'adopció de mesures de protecció adequades, contribuint a una gestió més segura i eficient de les dades empresarials.

Paraules clau: estàndards, eina, empreses petites i mitjanes, sistemes TI, seguritat de la informació, avaluació.

Abstract

The increase in cybersecurity threats, along with the trend towards digitalization, has led small and medium-sized enterprises to seek ways to better protect their computer systems and data. This Bachelor's Thesis aims to develop a guide and an accessible tool that allows companies to assess and improve their level of information security, regardless of their prior knowledge in cybersecurity. The tool is aligned with regulations, standards, and security entities such as ISO 27001, NIST, HIPAA, PCI DSS, CIS, and ENISA, ensuring the treatment of widely standardized concepts.

For the creation of this tool, an exhaustive review of standards and best practices in information security has been conducted, as well as an analysis of the main threats faced by companies in digital growth, such as ransomware and phishing. Special emphasis has been placed on the practical implementation of these standards to make them accessible and effective in the context of small and medium-sized enterprises.

The result is a self-assessment tool implemented in Excel, which aims to offer an evaluation of the maturity state of companies concerning the security of existing computer systems. This tool aims to help identify areas for improvement and facilitate the adoption of appropriate protection measures, contributing to a more secure and efficient management of business data.

Keywords: standards, tool, small and medium-sized enterprises, IT systems, cybersecurity, assessment.

Índice

1. INTRODUCCIÓN

En la actualidad, la ciberseguridad representa uno de los mayores desafíos para las pequeñas y medianas empresas, especialmente en un contexto de creciente digitalización. Este Trabajo de Fin de Grado se enfoca en desarrollar una herramienta accesible para que estas compañías puedan evaluar y mejorar su nivel de seguridad de la información, independientemente de sus conocimientos previos en la materia. La herramienta está alineada con normativas, estándares y entidades de seguridad ampliamente reconocidas, como ISO 27001, NIST, HIPAA, PCI DSS, CIS y ENISA garantizando la inclusión de conceptos estandarizados.

Dentro de los criterios para la selección de los estándares de referencia, se ha priorizado su reconocimiento internacional y se han seleccionado entidades que hayan desarrollado matrices de control robustas y ampliamente implementadas en las compañías como el NIST, que se encuentra en sintonía con las guías del CCN-CERT y INCIBE. Adicionalmente, las entidades seleccionadas abarcan aspectos específicos de la seguridad de la información en sectores críticos como el de la salud y el pago electrónico. Este enfoque busca incluir las particularidades de sectores que se encuentran actualmente vinculados con la necesidad de la implementación de medidas de seguridad de la información.

La motivación para llevar a cabo este trabajo surge de la experiencia personal en el campo de la auditoría de Tecnologías de la Información, donde se ha observado que muchas empresas presentan un nivel de seguridad informática insuficiente, exponiéndose a riesgos significativos. Además, se ha detectado que algunas compañías han realizado inversiones considerables en medidas de seguridad que no han resultado ser tan efectivas como se esperaba.

Debido a que la estandarización de la seguridad TIC se encuentra en continuo cambio, al igual que la aparición de nuevas amenazas, se ha considerado necesario contextualizar el panorama actual de la ciberseguridad, realizando un análisis exhaustivo de los ataques más comunes que enfrentan las compañías. Entre estos ataques se destacan el *ransomware* y el *phishing*, que representan amenazas significativas debido a la naturaleza de los datos manejados y la falta de sofisticación en las defensas de muchas de estas empresas. Estos ataques no solo comprometen la confidencialidad de la información, sino que también pueden interrumpir operaciones críticas y causar pérdidas financieras considerables. En este documento se enfatiza los retos específicos que deben abordar las compañías en crecimiento digital, incluyendo entre otros la limitada capacidad de recursos para implementar medidas avanzadas de seguridad y la necesidad urgente de concienciación y formación continua en ciberseguridad para todos los empleados.

En el desarrollo del trabajo se han buscado soluciones basadas en estudios reputados con el fin de dotar a la herramienta de un enfoque más práctico y realista para las empresas de pequeño y mediano tamaño. Con todo esto se ha buscado aportar una solución práctica y efectiva que no solo cumple con los estándares internacionales, sino que también es relevante y aplicable en su contexto operativo específico. El desarrollo de la herramienta resultante busca ofrecer a las empresas un modo de autoevaluarse, identificar áreas de mejora y adoptar medidas de protección adecuadas para fortalecer su postura de seguridad en un entorno digital cada vez más desafiante.

1.1 Motivación

La motivación principal para llevar a cabo este trabajo de fin de grado surge de una observación crítica en el ámbito de la auditoría de Tecnologías de la Información en numerosas compañías de la Comunidad Valenciana. En mi puesto de trabajo actual, como auditor IT, he tenido la oportunidad de evaluar y analizar la seguridad informática en diversas organizaciones y he notado dos problemas recurrentes. Por un lado, muchas de estas compañías presentan un nivel de seguridad muy bajo, lo que las expone a riesgos significativos en términos de ciberseguridad. Por otro lado, algunas empresas han invertido en medidas de seguridad costosas que, lamentablemente, no resultan ser tan eficientes como se esperaba.

Esta situación me ha impulsado a abordar este proyecto con un propósito claro y significativo. Mi motivación radica en la posibilidad de contribuir a resolver estos desafíos. Deseo utilizar mis conocimientos y experiencia en auditoría IT para crear una guía que ayude a las compañías pequeñas y medianas a identificar los riesgos más críticos en el ámbito de la ciberseguridad que podrían afectar sus operaciones y su continuidad. Al hacerlo, aspiro a proporcionarles las herramientas y el conocimiento necesario para fortalecer su seguridad cibernética de manera eficiente y rentable.

1.2 Objetivos

El objetivo principal de este Trabajo de Fin de Grado es la creación de una herramienta que ayude a las compañías medianas y pequeñas a alinear sus prácticas de la seguridad de la información con estándares y normativas de seguridad reconocidos. Esto se logrará a través de la consecución de los siguientes objetivos específicos:

1. Contextualizar el panorama actual con respecto a la seguridad de la información.
2. Identificar las principales barreras a las que se enfrentan la empresas de pequeño tamaño con respecto a la implantación de medidas de seguridad de la información.
3. Profundizar en el aprendizaje sobre normativas, estándares y entidades de seguridad de la información.

1.3 Estructura

Esta memoria se ha estructurado en función del proceso de investigación realizado para desarrollar la herramienta de análisis de la madurez de la seguridad de la información para pequeñas y medianas empresas.

En el primer capítulo, se presenta la introducción, que incluye la motivación del trabajo y una explicación de la estructura de la memoria. En segundo capítulo está dedicado al estado del arte, donde se realiza un recorrido histórico sobre la evolución de los estándares de seguridad de la información y se analizan documentos académicos alineados con el objetivo del presente trabajo. En el tercer capítulo, se evalúan las tendencias y amenazas actuales, así como las tecnologías y normativas existentes. Adicionalmente se analizan las brechas y desafíos principales que enfrentan las compañías en desarrollo tecnológico con respecto a la seguridad IT. El cuarto capítulo detalla la solución propuesta, en la que se establece el enfoque de la solución a desarrollar. En el quinto capítulo, se presenta el diseño de la solución. En este capítulo se seleccionan y describen varios estándares de seguridad relevantes, como ISO 27001 y NIST SP 800, entre otros. Además, se definen las áreas de solución y riesgos en análisis utilizando como fuente principal documentos elaborados por la entidad ENISA. El sexto capítulo se centra en el desarrollo de la solución. Se realiza un mapeo detallado de los controles de seguridad definidos por las normativas con los riesgos de ciberseguridad identificados. Además, se desarrollan formularios y una herramienta práctica para evaluar el estado de madurez en seguridad de la información de las compañías y planificar mejoras. En el séptimo capítulo, se presentan los resultados obtenidos y se discuten los puntos de mejora identificados durante el desarrollo del trabajo. Paralelamente, se sugieren posibles líneas de investigación o proyectos futuros que podrían continuar y expandir el trabajo realizado. Finalmente, los anexos necesarios se incluyen en el último capítulo, proporcionando detalles adicionales y apoyando la comprensión de los temas tratados en la memoria.

2. ESTADO DEL ARTE

En el presente apartado se busca contextualizar al lector sobre la temática principal del documento, la estandarización de la seguridad de los sistemas de información.

Por ello, en el presente apartado se hace referencia al origen de los estándares de la seguridad de la información, con el objetivo de entender la necesidad de estos.

El apartado se ha dividido en diversas hitos tecnológicos y digitales que han marcado un antes y un después en el camino de la estandarización de los sistemas, en el ámbito de la seguridad de la información.

2.1 Historia de la estandarización de la seguridad de los sistemas de información digitales

La historia de la estandarización de la seguridad de los sistemas de información digitales comenzó tras la Segunda Guerra Mundial, cuando especialistas en informática del gobierno estadounidense se preocuparon por el espionaje a través de emisiones electromecánicas de los ordenadores, lo que llevó al establecimiento del estándar TEMPEST(Ulas et al. 2014). Con la aparición de la tecnología de redes en los años 1950 y la creación de ARPANET, surgieron nuevos desafíos de seguridad informática. En 1970, la Junta de Ciencia de la Defensa Americana publicó un informe que destacaba las vulnerabilidades de los sistemas informáticos, subrayando la necesidad de controles adecuados para proteger la información militar(*Defense Science Board Task Force on Computer Security, Security Controls for Computer Systems: Report of the Defense Science Board Task Force on Computer Security. Confidential. | National Security Archive*).

Durante la década de 1970, la necesidad de criterios estándar de seguridad informática llevó a la creación del "Department of Defense Trusted Computer System Evaluation Criteria" (TSEC), conocido como "El Libro Naranja"(US Department of Defense 1985). Este documento estableció estándares rigurosos para evaluar y medir la seguridad de los sistemas informáticos. Posteriormente, la evolución de la tecnología y la interconexión de redes como Internet cuestionaron la efectividad del TCSEC, lo que impulsó el desarrollo de nuevos estándares internacionales, culminando en la serie *Rainbow*, que buscaba abordar las necesidades de seguridad en un entorno tecnológico cambiante(*Rainbow Series and Related Documents*).

En el sector de la salud, la digitalización planteó nuevas preocupaciones sobre la privacidad y la seguridad de los datos. En respuesta, el gobierno británico evaluó la seguridad de la información clínica en el NHS(*Cyber, information governance and data protection guidance*). En 1996, el Dr. Ross Anderson propuso reglas para proteger el consentimiento del paciente en los sistemas informáticos del NHS, estableciendo pautas claras para garantizar la privacidad médica en un entorno tecnológico avanzado(*Security Engineering - A Guide to Building Dependable Distributed Systems*).

En el anexo de historia del presente documento, se ha realizado un análisis más en detalle de esta evolución de los estándares de ciberseguridad.

A modo de conclusión tras analizar toda la información del presente apartado, se puede concluir que la estandarización de la seguridad de la información ha evolucionado junto con los avances digitales, adaptándose a las necesidades y desafíos de cada época. Por tanto, en el presente trabajo se realizará una análisis previo sobre el contexto tecnológico actual de las compañías de pequeño y mediano tamaño, para lograr un enfoque adecuado de la solución a desarrollar.

2.2 Trabajos de Referencia

Previo a el desarrollo del presente trabajo se ha llevado a cabo una búsqueda de documentos y proyectos académicos que guarden similitud con los objetivos propuestos en este trabajo.

Tras un análisis detallado de la documentación existente, se han seleccionado algunos de los principales proyectos que abordan temáticas relacionadas con la seguridad de la información en empresas. Estos proyectos se han elegido por su relevancia, originalidad y contribución al campo de estudio. A través de esta revisión bibliográfica, se busca contextualizar el presente trabajo en el marco de las investigaciones previas y establecer una base sólida para el desarrollo de nuevas propuestas y soluciones en el ámbito de la ciberseguridad empresarial.

2.2.1 Esquema Nacional de Seguridad: Protección de una infraestructura crítica del sector administración

El primer proyecto referenciado es el Trabajo Fin de Grado realizado por Jorge Revert Enguix en la Escola Tècnica Superior d'Enginyeria Informàtica de la Universitat Politècnica de València, durante el curso 2018-2019(Revert Enguix 2019). Este proyecto se centra en el estudio del Esquema Nacional de Seguridad y su normativa, con el objetivo de elaborar una guía para la protección de infraestructuras críticas del sector administrativo. La guía desarrollada permite realizar una adecuación al Esquema Nacional de Seguridad, cumpliendo con las medidas de seguridad necesarias para dichas infraestructuras. Además, se propone el desarrollo de una aplicación que facilite la evaluación de estas infraestructuras y verifique su cumplimiento con la normativa. Los objetivos del proyecto incluyen la identificación de medidas de seguridad, el desarrollo de una guía y la creación de una aplicación para evaluar la seguridad de las infraestructuras críticas.

Destacar que el autor, a modo de conclusión, establece ciertas áreas de mejora relacionadas con las limitaciones en el desarrollo de la aplicación como son la complejidad de la investigación y recopilación de información relacionada con las normativas y guías existentes.

2.2.2 Guía para la Adecuación de Organizaciones al Esquema Nacional de Seguridad

Este proyecto tiene como objetivo principal desarrollar una guía que facilite a organizaciones, tanto públicas como privadas, el cumplimiento del Real Decreto 3/2010(Serrat Troncho 2021). Esta guía se enfoca en el proceso de adecuación al Esquema Nacional de Seguridad, utilizando la metodología PDCA y proporcionando herramientas para la identificación de activos esenciales, la categorización de sistemas de información, el análisis de riesgos, el plan de mejora de seguridad, la declaración de aplicabilidad y demás documentación necesaria para cumplir con la normativa. El proyecto busca nivelar la guía en función de los conocimientos técnicos del lector y seguir las buenas prácticas sugeridas por el Centro Criptológico Nacional. Se enfoca en generar confianza en los ciudadanos respecto al uso de tecnologías en la relación con la Administración Pública, promoviendo el cumplimiento del ENS para proteger la información y los servicios de las organizaciones.

2.2.3 Implantación del Reglamento General de Protección de Datos y adaptación al Esquema Nacional de Seguridad de manera integrada en el Sistema de Gestión de Seguridad de la información basado en la ISO 27001

El proyecto se centra en mitigar los riesgos que afectan a la seguridad del Sistema de Gestión de Seguridad de la Información (SGSI) de una empresa de transporte público(Jiménez Gómez 2019). Se realiza un análisis de riesgo cualitativo basado en la metodología Magerit, identificando activos y amenazas, y se desarrolla un plan para implementar el Reglamento General de Protección de Datos (RGPD) y adaptarse al Esquema Nacional de Seguridad (ENS) utilizando la norma ISO 27001.

El objetivo principal es asesorar y brindar soporte para la adecuación e implantación del RGPD en el SGSI, integrado con la ISO 27001. Se crea un Marco de Convergencia Normativa para alinear las diferentes normativas y garantizar los niveles de seguridad necesarios. Se identifican fortalezas y debilidades de la empresa y se proponen medidas específicas para mejorar la seguridad de la información. Finalmente, se entregan propuestas de proyectos para subsanar los puntos críticos, permitiendo a la empresa seleccionar las medidas a implantar según sus necesidades.

2.2.4 Esquema Nacional de Seguridad: Protección de una infraestructura crítica hospitalaria

El proyecto se centra en el estudio de la normativa relacionada con el Esquema Nacional de Seguridad y su aplicación en una infraestructura crítica hospitalaria(Montó, José 2017). La finalidad es desarrollar una aplicación en Java para ayudar a los auditores a garantizar el cumplimiento de la normativa de manera efectiva. Se destaca la importancia de la seguridad en la era de la informatización, especialmente en el ámbito hospitalario, donde la protección de la vida de las personas depende cada vez más de la seguridad de los sistemas de información. El proyecto propone medidas para adecuar la infraestructura hospitalaria al Esquema Nacional de Seguridad y ofrece una aplicación de escritorio para facilitar el trabajo de los auditores. Se sugiere la necesidad de continuar investigando en este tema, especialmente en la aplicación práctica de la normativa en entornos hospitalarios reales y en la mejora y funcionalidad de la aplicación desarrollada. El autor destaca el desafío de recopilar y analizar la extensa normativa, así como la satisfacción personal que le ha proporcionado el proyecto como culminación de sus estudios de grado.

2.3 Crítica al estado del arte

En el apartado anterior se revela una tendencia predominante en los proyectos académicos españoles relacionados con la seguridad de la información: la referencia recurrente a normativas como la ISO 27001 y el Esquema Nacional de Seguridad (ENS). Estas normativas, si bien son fundamentales para establecer estándares de seguridad y garantizar la protección de la información en sectores críticos como el público y el hospitalario, tienden a dejar de lado a un importante segmento de empresas: las compañías pequeñas y medianas.

La mayoría de los proyectos revisados se centran en grandes entidades, como hospitales, entidades gubernamentales o empresas consolidadas, lo cual refleja una omisión significativa de las necesidades de seguridad de las compañías más pequeñas. Sin embargo, en la era de la creciente digitalización, estas empresas también se están viendo cada vez más expuestas a riesgos relacionados con la seguridad de la información(*Seguridad y biometría | Ciudadanía | INCIBE*).

Es necesario reconocer la importancia de adaptar las políticas de seguridad de la información a las necesidades y capacidades de las pequeñas y medianas empresas. La falta de recursos financieros y técnicos para implementar normativas tan específicas como la ISO 27001 puede resultar prohibitiva para muchas de estas compañías. Por lo tanto, es crucial investigar políticas de seguridad más flexibles y escalables que permitan a las empresas de menor tamaño proteger sus sistemas de manera efectiva sin incurrir en costos excesivos.

En este sentido, se priorizará centrarse en los conceptos fundamentales de seguridad de la información, tales como la confidencialidad, integridad y disponibilidad, en lugar de generar guías de cumplimiento tan específicas que su implementación resulte inaccesible para empresas con recursos limitados. Esta aproximación más pragmática y orientada a los conceptos básicos de seguridad puede facilitar la adopción de medidas de protección adecuadas para empresas de todos los tamaños, promoviendo así un entorno empresarial más seguro y resiliente en el panorama digital actual.

3. ANÁLISIS DEL PROBLEMA

Tras analizar el origen y la necesidad de los estándares de seguridad en respuesta a la evolución digital, este capítulo busca explorar el contexto actual de amenazas digitales, con especial atención en las pequeñas y medianas empresas.

En la sección 3.1. se contextualiza la situación actual con respecto a la evolución de las herramientas informáticas en los negocios y su relación con el mundo de la seguridad de la información.

En la sección 3.2. se analiza las principales problemáticas existentes en la adopción de medidas de seguridad, en específico se detalla los principales problemas de las compañías de pequeño y mediano tamaño al intentar establecer marcos estandarizados de seguridad de las TI.

3.1 Contexto actual

3.1.1 Macrotendencias

En la última década, el mundo ha experimentado una transformación radical impulsada por la digitalización. La expansión exponencial de la tecnología digital ha generado un vasto ecosistema de información interconectada, redefiniendo la forma en que las organizaciones gestionan, almacenan y utilizan los datos. Esta era digital ha desencadenado un crecimiento sin precedentes en la cantidad de datos generados, procesados y compartidos a diario(European Foundation for the Improvement of Living and Working Conditions. 2021).

Tal es el grado de relevancia de este sector que la Unión Europea que ha establecido objetivos digitales como la utilización de la nube, la IA o los macrodatos por el 75 % de las empresas de la UE o conseguir que más del 90 % de las pymes alcanzan al menos un nivel básico de intensidad digital para 2030 (*La década digital de Europa: Objetivos para 2030 Comisión Europea*). Para medir esta evolución la Unión europea ha creado el índice “Digital Economy and Socity Index”(DESI).

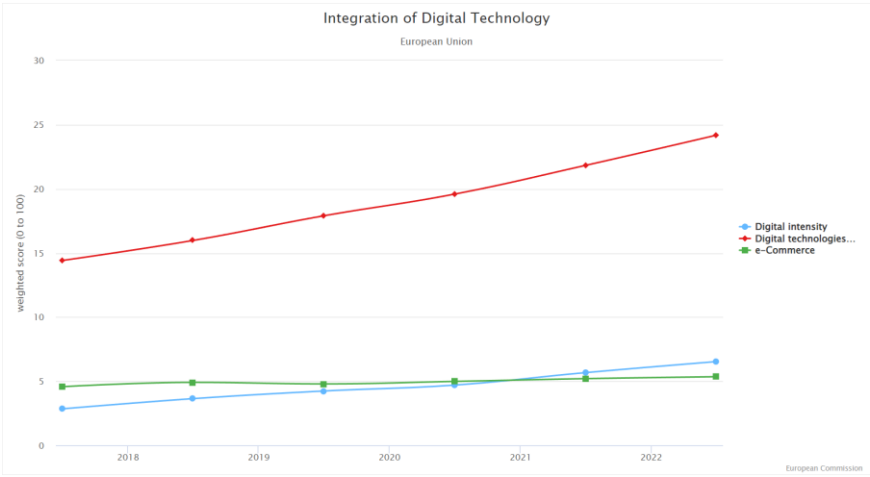


Ilustración 1. Evolución anual de la integración de las tecnologías Digitales en la UE. Fuente: European Commission.

La UE ha establecido tres métricas principales para evaluar el grado de integración de tecnología digital: Uso de tecnologías digitales, intensidad digital y e-commerce. De estas tres, el uso de las tecnologías digitales es la que mayor grado de crecimiento está experimentado.

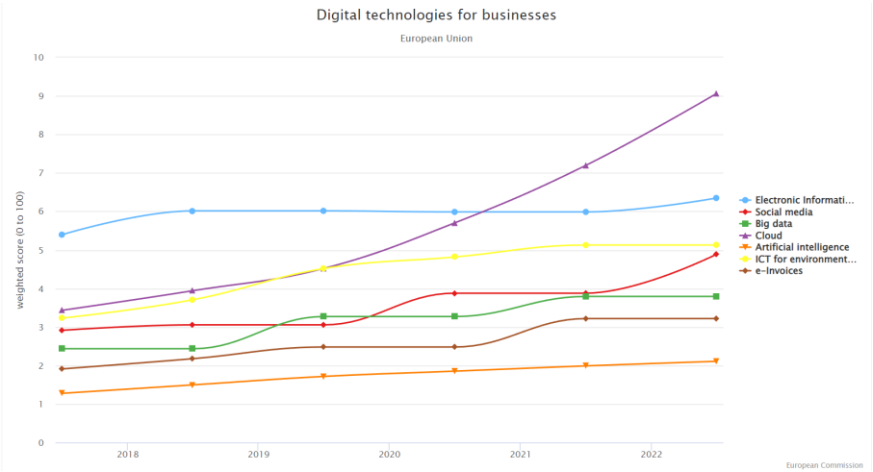


Ilustración 2. Evolución anual de las tecnologías digitales en las empresas de la UE. Fuente: European Commission.

No obstante, el avance de la transformación digital y el uso de nueva tecnologías ha desencadenado un mayor riesgo vinculado a las amenazas de robo de información. Todo lo que antes era físico ahora se ha convertido en datos digitales. Los datos se han convertido en el recurso más importante en el mundo digitalizado. Además, la transformación digital ha permitido que nuestra "información" se almacene en cualquier medio digital, lo que ha creado una nueva área de vulnerabilidad para los ataques.

La digitalización amplía las oportunidades para individuos, grupos u organizaciones, que buscan obtener beneficios, obtener información confidencial, causar daño o simplemente mostrar sus habilidades. Los riesgos son diversos y extensos e incluyen la toma de información mediante cifrado, el espionaje para obtener datos, así como la interrupción de servicios mediante ataques DDoS, entre otros(KAMBOURAKIS, NEISSE, NAI-FOVINO 2021).

La seguridad de la información, en conjunto con la ciberseguridad, constituye un entorno complejo y cambiante que implica interacciones entre individuos, procesos, tecnología y servicios en el Internet de Todo (IoE). Está estrechamente vinculada con la infraestructura de comunicación y física, ya sea por medios cableados o inalámbricos. En este contexto, la seguridad de la información es esencial para mantener la competitividad, no solo a nivel empresarial sino también a nivel nacional e internacional. La Unión Europea reconoce esta necesidad en documentos como JOIN/2017/0450(*JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Resilience, Deterrence and Defence: Building strong cybersecurity for the EU* 2017) y la directiva de la UE 2016/1148(*BOE.es - DOUE-L-2016-81297 Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión*).

3.1.2 Amenazas

Antes de conocer las técnicas de ataque de seguridad más comunes, hay que tener en consideración dos términos muy relevantes, "Incidencia de Seguridad" y "Brecha de Seguridad", conceptos que se encuentran estrechamente relacionados:

> *Incidencia de seguridad*
>
> "Evento o situación en el entorno digital que afecta la confidencialidad, integridad o disponibilidad de sistemas, datos o recursos tecnológicos. Estas incidencias pueden variar desde ataques cibernéticos y vulnerabilidades de software hasta errores humanos y desastres naturales que impactan la seguridad y operatividad de los sistemas y la información"(Cichonski et al. 2012).
>
> "Una ocurrencia que pone en peligro, de manera real o potencial, la confidencialidad, integridad o disponibilidad de un sistema de información o de la información que el sistema procesa, almacena o transmite, o que constituye una violación o una amenaza inminente de violación de las políticas de seguridad, procedimientos de seguridad o políticas de uso aceptable."(NIST)
>
> *Brecha de Seguridad*
>
> "Una brecha de seguridad se refiere a la falla o vulnerabilidad en la seguridad de un sistema, red, aplicación o infraestructura tecnológica que permite a actores no autorizados acceder a información confidencial, realizar acciones maliciosas o comprometer la integridad, disponibilidad y confidencialidad de los activos digitales." (*ISO27000 and Information Security: A Combined Glossary*)
>
> "La pérdida de control, compromiso, divulgación no autorizada, adquisición no autorizada, o cualquier ocurrencia similar en la que: una persona que no sea un usuario autorizado accede o potencialmente accede a información de identificación personal; o un usuario autorizado accede a información de identificación personal con un propósito distinto al autorizado."(NIST)

En resumen, un incidente de seguridad es un evento que afecta la seguridad informática, mientras que una brecha de seguridad es el resultado observable de un incidente exitoso que ha comprometido la seguridad y ha permitido el acceso no autorizado o la exposición de información confidencial. La gestión adecuada de los incidentes de seguridad es crucial para evitar que evolucionen en brechas de seguridad y para mitigar su impacto en la organización.

Para la descripción y clasificación de los diferente incidentes de seguridad existe un marco estandarizado llamado VERIS(*The VERIS Framework*) ("Vocabulary for Event Recording and Incident Sharing"). Este marco proporciona un conjunto de categorías y definiciones que ayudan a las organizaciones a describir los detalles clave de un incidente de seguridad de forma coherente y fácil de comprender. Las categorías principales utilizadas para describir un incidente son las 4As: Actor (quién), Acción (cómo), Activo (dónde) y Atributo (qué).

Relacionado con este estándar, Verizon (compañía de telecomunicaciones de ámbito internacional que ofrece servicios de seguridad cibernética) publica anualmente un informe en el que se analiza las razones principales por las que se producen estas brechas e incidentes de seguridad en los datos(*DBIR Report 2023 - Master's Guide*). En el informe publicado por Verizon en 2023 se destacan las siguientes conclusiones con respecto al panorama actual con relación a los amenazas cibernéticas:

Los ataques de ingeniería social suelen ser muy efectivos y extremadamente lucrativos para los ciberdelincuentes. Por eso los ataques de compromiso de correo electrónico empresarial casi se han duplicado y ahora representan más del 50% de los incidentes.

El 74% de todas las brechas identificadas involucran el elemento humano, ya sea a través de errores, uso indebido de privilegios, uso de credenciales robadas o ingeniería social.

La motivación principal para los ataques es el interés financiero, siendo el objetivo del 95% de las brechas.

Las tres formas principales en que los atacantes acceden a una organización son a través de credenciales robadas, *phishing* y explotación de vulnerabilidades.

El *ransomware* es una de las acciones principales presentes en las brechas, y aunque no ha creció durante el último año, se ha mantenido estadísticamente estable en un 24%.

Paralelamente, Microsoft publica anualmente un informe centrado en las amenazas identificadas de su producto, Microsoft Defender en el que se destacan las siguiente conclusiones(*Microsoft Digital Defense Report 2022 | Microsoft Security*):

La amenaza del *ransomware* y la extorsión se está volviendo más sofisticada con ataques dirigidos a gobiernos, empresas e infraestructuras críticas.

Los atacantes cada vez amenazan más con divulgar datos sensibles para fomentar el pago de rescates.

El *ransomware* es el ataque más comúnmente utilizado, ya que un tercio de los objetivos son comprometidos con éxito y el 5% de ellos son extorsionados.

Los ataques de *phishing* de robo de credenciales que apuntan indiscriminadamente a todas las bandejas de entrada están en aumento, y el compromiso de correo electrónico empresarial, incluido el fraude de facturas, representa un riesgo significativo de ciberdelincuencia para las empresas.

3.1.3 Tecnologías actuales de protección

Este apartado se propone examinar la variedad de herramientas y técnicas existentes para poder salvaguardar la información.

El listado seleccionado de tecnologías representa un conjunto diversificado que abarca desde métodos clásicos de seguridad como firewalls y detección de virus, hasta enfoques más vanguardistas como la autenticación biométrica, el rastreo de vulnerabilidades y la protección de dispositivos del Internet de las Cosas (*IoT*). Cada una de estas herramientas y tecnologías desempeña un papel crucial en la defensa contra amenazas cibernéticas, ya sea asegurando la autenticidad de usuarios, detectando intrusiones o evaluando la seguridad de sistemas(Moallem 2021):

Encriptación: El cifrado constituye una estrategia fundamental en ciberseguridad al transformar el texto original de tal manera que solo aquel usuario en posesión del código secreto o la clave de descifrado pueda acceder a su contenido. Esta técnica brinda una capa adicional de protección a la información sensible(*What is encryption? How it works + types of encryption – Norton*).

Autentificación: Existen distintos sistemas de autenticación para resguardar la identidad del usuario y los recursos del sistema frente a diversos tipos de ataques. La elección del método de autenticación utilizado depende de las necesidades, recursos disponibles y prioridades. Existen tres enfoques principales que delinean la naturaleza de estos sistemas de autenticación, los cuales se fundamentan en la posesión de conocimiento, tokens o biometría, tal como se detalla en las secciones siguientes(Abdulkader, Atia, Mostafa 2015):

1. Autentificación basada en el conocimiento
2. Autenticación basada en los tokens
3. Autentificación basada en la biometría

Firewall: Los tecnología de los dispositivos firewalls son una pieza fundamental en la seguridad de las redes, crean una barrera ficticia que controla el flujo de datos tanto hacia dentro como hacia fuera de una organización. Esta barrera se considera la primera línea de defensa y tiene la capacidad de bloquear ciertos tipos de paquetes entrantes, un proceso conocido como filtrado de ingreso. Su objetivo principal es proteger la red y evitar accesos no autorizados(Scarfone, Hoffman 2009).

Protección *Endpoint:* Las tecnologías basadas en puntos finales (“Endpoint”) son proactivas al permitir una visión detallada de lo que sucede en los dispositivos finales de uso en producción. Estas soluciones permiten la visualización de cambios físicos y lógicos en la configuración, así como la identificación precisa de los datos de configuración disponibles, como la versión del producto o la aplicación de parches específicos. Además, estas tecnologías no se ven afectadas por los protocolos de comunicación utilizados, ya que acceden directamente a los datos de configuración reales. Estos sistemas ofrecen la capacidad de respaldar estos datos, almacenándolos localmente y externamente para su conservación y seguridad(Hollis, Zahn 2017).

Detección de correos electrónicos maliciosos*:* Los navegadores son la primera línea de defensa ante intentos de obtener credenciales de manera fraudulenta a través del correo electrónico. Los mecanismos de seguridad del navegador emplean listas de exclusión

suministradas por plataformas de denuncia como *PhishTank*, *SafeBrowsing* y *SmartScreen*(Catal et al. 2022).

Seguridad de la red: Para poder conseguir la seguridad de la red existen diferente tecnologías que permiten proteger esta área.

- El control de acceso a la red (NAC) se emplea para verificar el estado de cada dispositivo que se conecta a la red. Este mecanismo evalúa cada dispositivo en la red para garantizar que tenga un antivirus adecuado, esté actualizado y tenga las configuraciones correctas antes de permitir su ingreso a la red.(*¿Qué es la seguridad de red? | IBM*):
- Una red privada virtual (VPN), permite ocultar la dirección IP y ubicación de los usuarios(*Seguridad de la red: ¿Qué es, cómo funciona y qué tipos existen?*).
- Detección y respuesta de red (NDR) son técnicas basadas en aprendizaje automático (Machine Learning) que analizan el tráfico de la red y pueden generar alertas ante cualquier actividad de red inusual en base a las reglas definidas.(*Soluciones de seguridad: Network Detection & Response* 2021).
- Los sistema de prevención de intrusiones (IPS) monitorea el tráfico de la red para identificar posibles amenazas y toma medidas automáticas para bloquearlas. Además, alerta al equipo de seguridad, finaliza conexiones riesgosas, elimina contenido malicioso o activa otros dispositivos de seguridad, según sea necesario(*¿Qué es un sistema de prevención de intrusiones (IPS)? | IBM*).

3.1.4 Normativas y estándares de seguridad de la información

Vinculado a este proceso de digitalización nace una necesidad de establecer un mayor grado de seguridad en la información en relación con las nuevas tecnologías utilizadas. Por ello, las compañías comparten un especial interés en cómo mejorar la gestión del riesgo de ciberseguridad mediante el uso del marco de seguridad estandarizados.

Esta necesidad se puede evidenciar en el proyecto de la comisión europea planificado en su agenda del 2019 al 2024 en el que se pretende establecer un conjunto estandarizado de normas de seguridad de la información de alto nivel para todas las instituciones, organismos, oficinas y agencias de la Unión para garantizar un nivel mejorado y consistente de protección contra las amenazas en constante evolución a su información(*Security at the Commission - European Commission*).

En el contexto actual los estándares juegan un papel importante en mejorar los enfoques de seguridad de la información en diferentes regiones geográficas y comunidades ya que pueden(*Standards for Cyber Security*):

- Mejorar la eficiencia y efectividad de procesos clave.
- Facilitar la integración e interoperabilidad de sistemas.
- Permitir la comparación significativa entre diferentes productos o métodos.
- Estructurar el enfoque para implementar nuevas tecnologías o modelos de negocios.
- Simplificar entornos complejos.
- Promover el crecimiento económico.

Aunque la selección de un marco de gestión de la seguridad de la información no cuenta con un enfoque único para gestionar el riesgo de ciberseguridad en las organizaciones, su objetivo principal es reducir y gestionar mejor los riesgos relacionados con la seguridad de la información(*Quick Start Guide* 2023).

3.2 Brechas y desafíos identificados

En el contexto dinámico y siempre cambiante del panorama tecnológico actual, las pequeñas y medianas empresas se encuentran cada vez más expuestas a diversas amenazas cibernéticas que podrían comprometer la seguridad de su información sensible(*DBIR Report 2023 - Small Medium Business (SMBs) Data Breaches*). Ante este desafío, la implementación de estándares de ciberseguridad se presenta como una estrategia fundamental para salvaguardar los activos digitales y garantizar la continuidad operativa.

Este apartado tiene como objetivo abordar detenidamente las brechas y desafíos que surgen al momento de seleccionar y aplicar estándares de seguridad de la información en el entorno específico de las PYMEs.

Fundamentalmente el siguiente apartado se analizará el informe publicado por la ENISA (Agencia de la Unión Europea para la ciberseguridad) en la que han identificado los retos principales en la estandarización de la ciberseguridad(*Standards for Cyber Security*):

3.2.1 Desafío organizacional

Uno de los desafíos más significativos que enfrentan las empresas pequeñas y PYMEs al implementar normativas de ciberseguridad radica en la diversidad de estándares desarrollados por múltiples Organizaciones de Desarrollo de Estándares (SDOs) en los últimos diez años. Este fenómeno, impulsado en gran medida por la industria y motivado por la necesidad de agilizar procesos, ha generado una abundancia de marcos normativos que buscan abordar diferentes aspectos de la ciberseguridad.

El surgimiento de SDOs como Oasis(*OASIS Open Home*), W3C(*Web Standards*), ITIL(*ITIL - ITIL*), entre otros, ha sido en parte una respuesta a la inversión sustancial de tiempo y recursos humanos requeridos por los SDOs tradicionales, como el Instituto Europeo de Normas de Telecomunicaciones (ETSI)(*Ministerio para la Transformación Digital y de la Función Pública - Instituto Europeo de Normas de Telecomunicaciones (ETSI)*) y la Unión Internacional de Telecomunicaciones (ITU)(*Sobre la Unión Internacional de Telecomunicaciones (UIT)*). Además, la convergencia de la estandarización, que antes se centraba en sectores específicos, ahora se ha extendido a varias industrias.

Esta proliferación de SDOs ha llevado a un aumento en la cantidad de estándares publicados, lo que, paradójicamente, puede convertirse en una fuente de confusión para los usuarios finales, especialmente para las PYMEs y empresas pequeñas con recursos limitados. La diversidad de estándares disponibles puede plantear un desafío organizacional significativo en términos de la selección adecuada del marco normativo que mejor se adapte a las necesidades y capacidades específicas de una PYME en particular(Arora).

La gestión de esta diversidad normativa se convierte en una tarea crucial, requiriendo una comprensión profunda de los requisitos de cada estándar y su alineación con los objetivos de seguridad de la información de la empresa.

Además, este desafío organizacional se ve acelerado por la rapidez con la que evolucionan y se actualizan estos estándares, lo que puede generar la necesidad constante de ajustar y mantener las prácticas de ciberseguridad en conformidad con las últimas normativas. En este sentido, abordar la diversidad de estándares no solo implica una elección inicial informada, sino también la capacidad de adaptarse y mantenerse actualizado en un entorno normativo en

constante cambio(*The Evolution of Security Operations and Strategies for Building an Effective SOC*).

3.2.2 Áreas de estandarización

La participación de los intereses industriales en actividades de estandarización tiende a ser impulsada por áreas de trabajo que se alinean con los intereses centrales de los proveedores de servicios, como la autenticación y la facturación. Aunque se observa un interés general creciente en el ámbito de la privacidad, se espera que el interés específico de la industria disminuya.

Actualmente, no existe una única y continua línea de estándares relacionada con la ciberseguridad, sino más bien varias áreas discretas que son objeto de estandarización(*Standards for Cyber Security*):

- Estándares técnicos.
- Métricas (principalmente relacionadas con la continuidad del negocio).
- Definiciones.
- Aspectos organizativos.

Algunas áreas pueden estar potencialmente sobre estandarizadas, como es el caso de la gobernanza de la seguridad de la información y la gestión de riesgos, donde existen numerosos estándares. Por otro lado, en algunas áreas faltan estándares, como en el caso de la privacidad y la legislación de protección de datos, donde hay relativamente pocos estándares. De manera similar, existen pocas normativas que aborden los niveles de servicio, o más ampliamente, los acuerdos y contratos de servicio, términos de uso y condiciones, etc.

Un análisis rápido a través de las ofertas de diferentes proveedores de servicios en la nube revela que cada proveedor tiene un texto legal diferente (a menudo extenso) que describe los términos de uso y las excepciones a las obligaciones. Esta diversidad legal subraya la falta de estándares en áreas críticas que afectan directamente la relación entre proveedores de servicios y usuarios finales.

En este panorama, es evidente que la estandarización en el campo de la ciberseguridad no sigue una ruta uniforme, y algunas áreas pueden ser objeto de mayor atención y desarrollo normativo que otras. Este análisis crítico busca arrojar luz sobre las disparidades existentes y resaltar la necesidad de un enfoque equilibrado que aborde tanto la sobre estandarización como la falta de estándares en áreas esenciales para la seguridad de la información y la privacidad(*Key Performance Indicators for Security Governance, Part 2: Security Reporting for Senior Management*).

3.2.3 Falta de agilidad

El proceso de diseñar y aprobar estándares es largo, a menudo extendiéndose por meses o incluso años, mientras que el entorno de tecnología de la información (TI) evoluciona rápidamente. La falta de agilidad en este proceso puede conducir a estándares obsoletos o parcialmente aplicables a situaciones del mundo real(Cardinal, Sitkin, Long 2004).

Para abordar esta problemática, una de las alternativa existentes plantea utilizar documentos de buenas prácticas(*5. National Cybersecurity Strategy Good Practice*). Estos documentos, sometidos a procedimientos de control de cambios menos estrictos, podrían desarrollarse de manera más rápida hasta alcanzar la madurez necesaria. Una vez maduros, estos documentos

podrían servir de base para la creación de estándares correspondientes. Esta aproximación proporciona flexibilidad y agilidad, permitiendo la actualización constante y asegurando que los estándares resultantes sean pertinentes y aplicables a las cambiantes necesidades de la ciberseguridad([CSL STYLE ERROR: reference with no printed form.]).

3.2.4 Consideraciones económicas

En el estudio de Verizon, anteriormente analizado, se comprobó si el tamaño de la compañías es un factor influyente en la cantidad y tipos de amenazas detectadas, concluyendo finalmente que no. Cada vez más, tanto las PYMES como las grandes empresas están utilizando servicios e infraestructuras similares, lo que significa que sus superficies de ataque comparten más similitudes que nunca. Sin embargo, lo que es muy diferente son los recursos que dispone cada compañía para ser capaz de responder ante las amenazas(*DBIR Report 2023 - Small Medium Business (SMBs) Data Breaches*).

DigitalOcean fue un paso más allá y consulto directamente a las compañías pequeñas y medianas cuál es su principal preocupación en materia de ciberseguridad. En este estudio se confirmó que la falta de tiempo para gestionar la seguridad era la mayor preocupación (25%). Esto demuestra que muchas pequeñas empresas encuentran desafiante dedicar personal y tiempo a mantener sus sistemas de seguridad, lo que puede ponerlas en mayor riesgo de sufrir diversos tipos de ataques de seguridad(2023).

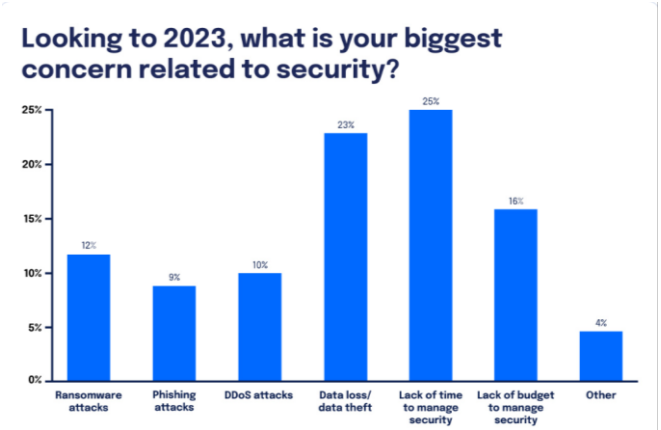


Ilustración 3.Mayores preocupaciones ciberseguridad empresas pequeño y mediano tamaño. Fuente: Digital Ocean.

3.2.5 Falta de concienciación

La implementación efectiva de estándares de seguridad se ve obstaculizada cuando los usuarios y organizaciones no están plenamente conscientes del riesgo derivado del uso de herramientas tecnológicas. Esta falta de concienciación puede derivar en una adopción pasiva de soluciones que podrían no ser las más beneficiosas a largo plazo.

Esto se puede reflejar en un caso reciente de ciberataque a una de las empresas proveedoras de internet más grande de España, Orange. En este caso la compañía no estableció medidas de seguridad de acceso lo suficientemente robustas para su sistemas principal de gestión de red(Aguiar 2024).

A modo de obtener una referencia del estado actual de la concienciación del estado español en relación con la concienciación en ciberseguridad se ha utilizado el reporte anual de 2024 Cisco Cybersecurity Readiness Index Spain(*2024 Cisco Cybersecurity Readiness Index* 2024). Cisco plantea un Índice de Preparación en Ciberseguridad, como métrica para aborda

el panorama actual de la ciberseguridad y evaluar la preparación de las organizaciones a nivel global para enfrentar los riesgos actuales en este ámbito basado en 5 pilares fundamentales: inteligencia de identidad, resiliencia de red, confianza en las máquinas, reforzamiento de la nube y fortificación de la Inteligencia Artificial (IA).

Tras el análisis realizado por CISCO en este 2024 en base a su índice, se ha concluido que solo el 3% de las organizaciones encuestadas califican en la categoría Madura. Casi tres cuartos (71%) se encuentran en las dos categorías más bajas (Formativa, 60% y Principiante, 11%). En España, el 2% de las organizaciones están en la etapa Madura de preparación, el 18% en la etapa Progresiva, el 61% en la etapa Formativa y el 19% en la etapa de Principiante.

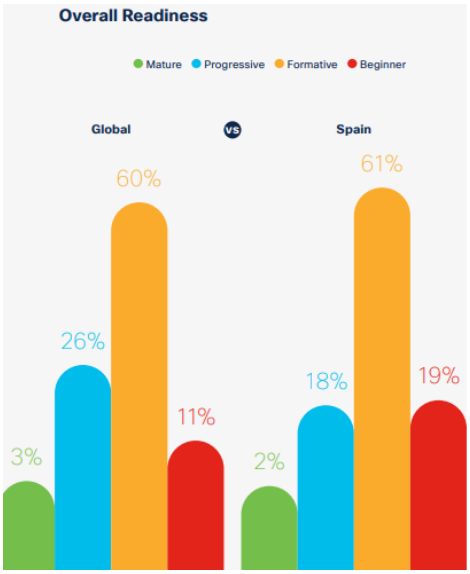


Ilustración 4. Índice de preparación en ciberseguridad 2024. Fuente: CISCO

4. SOLUCIÓN PROPUESTA

Tras el análisis exhaustivo de la historia de los estándares de seguridad y en la comprensión del contexto actual de amenazas digitales, se desarrollará una herramienta integral que aborde las brechas y desafíos identificados para las empresas pequeñas y medianas (PYMEs) en cuanto a la seguridad de la información.

Esta herramienta tiene como objetivo principal permitir a las PYMEs realizar un análisis del estado de madurez de su compañía en relación con la seguridad de la información de sus sistemas informáticos y ofrecer soluciones basadas en estándares e instituciones líderes en este campo en la actualidad.

La herramienta proporcionará un cuestionario exhaustivo que permitirá a las empresas de pequeño y mediano tamaño evaluar su estado actual en términos de seguridad de la información. Este cuestionario abarcará áreas como la infraestructura de TI, las políticas de seguridad, la concienciación del personal y la gestión de riesgos.

Una vez completada la evaluación, la herramienta comparará los resultados con los estándares de seguridad de la información reconocidos a nivel internacional. De esta forma las compañías podrán identificar áreas de mejora y establecer objetivos claros.

Con base en los resultados de la evaluación y el análisis comparativo, la herramienta generará recomendaciones personalizadas para cada compañía. Estas recomendaciones estarán alineadas con las mejores prácticas de seguridad de la información y podrán incluir entre ostros aspectos, la implementación de medidas específicas, la adopción de políticas de seguridad y la formación del personal…

5. DISEÑO DE LA SOLUCIÓN

En este capítulo, se explicará de forma detallada la manera en la que se ha diseñado la solución para que esta sea eficaz y eficiente.

5.1 Selección de estándares de seguridad

La seguridad de la información se ha convertido en un pilar fundamental para la protección de activos digitales, datos confidenciales y la continuidad operativa de las organizaciones en un mundo cada vez más interconectado. Sin embargo, este panorama de creciente complejidad también ha dado lugar a un desafío paradójico: el exceso de información y la proliferación de normativas de seguridad.

La existencia de múltiples normativas y enfoques puede llevar a una confusión generalizada. Las organizaciones pueden encontrarse en una encrucijada al intentar discernir cuáles son las medidas de seguridad más adecuadas para su entorno específico. El esfuerzo por cumplir con todas las normativas puede dispersar los recursos y desviar la atención de los riesgos cibernéticos más críticos.

La adopción de un enfoque estratégico se vuelve esencial en este contexto. En lugar de abordar ciegamente cada normativa individual, las organizaciones deben priorizar la identificación de sus activos más valiosos y los riesgos más probables que enfrentan.

Por ello, en esta guía se ha planteado un enfoque generalizado, realizando un análisis sobre: ISO 27001, NIST SP 800, HIPAA, PCI DSS V. 3.2.1 y CIS.

5.1.1 ISO 27001

La normativa ISO 27001 es un estándar internacional ampliamente reconocido que se centra en el establecimiento, implementación, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI) efectivo dentro de una organización. Este estándar proporciona un marco sólido para gestionar los riesgos de seguridad de la información y proteger los activos valiosos de una organización, incluyendo datos, sistemas, procesos y personas (ISO, 2023).

La ISO 27001 es parte de la serie ISO 27000, que está dedicada a la gestión de la seguridad de la información. Fue publicada por primera vez en 2005 por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), en respuesta a la creciente necesidad de abordar los desafíos de seguridad cibernética y de la información que enfrentan las organizaciones en todo el mundo(Spencer 2019).

El principal objetivo de la ISO 27001 es proporcionar un enfoque sistemático y coherente para identificar, evaluar y tratar los riesgos relacionados con la seguridad de la información. Ayuda a las organizaciones a establecer un marco de trabajo integral para la gestión de la seguridad, alineando los objetivos de seguridad con los objetivos comerciales y operativos más amplios. Además, busca garantizar la confidencialidad, integridad y disponibilidad de la información, así como minimizar la posibilidad de incidentes de seguridad(14:00-17:00 2023).

5.1.2 NIST SP 800

La serie de publicaciones NIST SP 800 es un conjunto de estándares, directrices y recomendaciones desarrolladas por el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos en el ámbito de la ciberseguridad y la protección de la información. Estas publicaciones están diseñadas para ayudar a las organizaciones a fortalecer sus prácticas de seguridad, mitigar riesgos y mejorar la resiliencia frente a las amenazas cibernéticas en un entorno en constante evolución(Spencer 2019).

El NIST, una agencia del Departamento de Comercio de los Estados Unidos se dedica a promover la innovación y la competitividad a través de estándares técnicos y tecnológicos. La serie NIST SP 800 comenzó en respuesta a la creciente necesidad de establecer lineamientos y mejores prácticas para asegurar sistemas de información y tecnología en un mundo digital interconectado. Desde entonces, ha evolucionado y ampliado sus enfoques para abordar una amplia gama de desafíos de seguridad cibernética (*NIST Special Publication 800-series General Information* 2018).

El principal objetivo de la serie NIST SP 800 es proporcionar un enfoque coherente y práctico para mejorar la seguridad de la información y los sistemas de tecnología de la información. Las publicaciones dentro de esta serie abordan diversos aspectos de la ciberseguridad, desde la gestión de riesgos hasta la implementación de controles técnicos y operativos. Estas publicaciones se desarrollan en consulta con expertos de la industria y son ampliamente reconocidas en todo el mundo por su calidad y enfoque integral (*NIST Special Publication 800-series General Information* 2018).

5.1.3 HIPAA

La Ley de Portabilidad y Responsabilidad del Seguro de Salud (HIPAA, por sus siglas en inglés) es una legislación de los Estados Unidos que se centra en la protección de la privacidad y la seguridad de la información médica y de salud. HIPAA fue promulgada en 1996 con el objetivo de abordar la creciente necesidad de proteger la confidencialidad de la información médica y garantizar los derechos de los pacientes en un entorno cada vez más digital y conectado(Alder 2022).

HIPAA es una ley federal que establece estándares y regulaciones para la privacidad y seguridad de la información de salud en los sistemas de atención médica. Fue promulgada el 21 de agosto de 1996 y se compone de dos partes principales: el Título I se enfoca en la cobertura y la portabilidad del seguro médico, mientras que el Título II se centra en la privacidad y seguridad de la información de salud(*HIPAA History*).

Los principales objetivos de la normativa HIPAA son(*Health Insurance Portability and Accountability Act of 1996 (HIPAA) | CDC* 2022):

1. Protección de la Privacidad: HIPAA garantiza que la información médica de los pacientes se mantenga confidencial y que los pacientes tengan control sobre quién puede acceder a sus registros médicos.

2. Seguridad de la Información: HIPAA establece requisitos para garantizar que los sistemas de atención médica implementen medidas de seguridad adecuadas para proteger la información de salud contra accesos no autorizados y divulgación no autorizada.

3. Uso y Divulgación Adecuados: La normativa establece reglas para el uso y la divulgación de la información médica, asegurando que se comparta solo con fines autorizados, como el tratamiento médico, el pago y las operaciones de atención médica.

5.1.4 PCI DSS

El PCI DSS es un conjunto de requisitos y medidas de seguridad diseñadas para asegurar que las organizaciones que manejan información de tarjetas de pago mantengan un alto nivel de seguridad para proteger los datos confidenciales de los titulares de tarjetas. Esta normativa establece un marco de referencia para abordar los riesgos de seguridad relacionados con el almacenamiento, procesamiento y transmisión de datos de tarjetas de pago(*Industria de Tarjetas de Pago (PCI) Norma de seguridad de datos* 2016).

El PCI DSS fue establecido en 2006 por las principales compañías de tarjetas de pago, incluyendo Visa, MasterCard, American Express, Discover y JCB. Estas organizaciones formaron el Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago (PCI SSC) con el propósito de crear un estándar común para la seguridad de los datos de tarjetas de pago y prevenir el fraude en la industria(*Industria de Tarjetas de Pago (PCI) Norma de seguridad de datos* 2016).

Los objetivos principales del PCI DSS son(*Industria de Tarjetas de Pago (PCI) Norma de seguridad de datos* 2016):

1. Protección de Datos Sensibles: Asegurar que los datos confidenciales de los titulares de tarjetas, como números de tarjetas y códigos de seguridad, se mantengan seguros contra accesos no autorizados.

2. Prevención de Fraude: Reducir el riesgo de fraude en las transacciones con tarjetas de pago al establecer medidas de seguridad sólidas.

3. Estándar Global: Proporcionar un estándar de seguridad uniforme para la industria de tarjetas de pago que sea aplicable a nivel global.

5.1.5 CIS

Las normativas CIS (Center for Internet Security) son conjuntos de estándares y controles de seguridad cibernética desarrollados por el Center for Internet Security, una organización sin fines de lucro dedicada a promover la seguridad cibernética y la resiliencia en todo el mundo. Estas normativas ofrecen directrices y mejores prácticas para ayudar a las organizaciones a proteger sus sistemas, redes y datos contra amenazas cibernéticas(*CIS Controls*).

El organismo CIS comenzó a trabajar en los controles por primera vez en 2008 en colaboración con diversas instituciones gubernamentales, empresas y otras organizaciones. Fue un movimiento surgido desde la base debido a la necesidad de seguridad. El detonante fue una violación de seguridad en la base de defensa de Estados Unidos, que también ocurrió en 2008. Fue la pérdida de datos más significativa que un equipo informático militar estadounidense había experimentado. Por lo tanto, resaltó la importancia de establecer sólidos procedimientos de defensa cibernética(*The Guide: CIS Security Controls*).

Los objetivos principales de las normativas CIS son(*CIS Controls*):

1. Proporcionar directrices prácticas y efectivas para mejorar la seguridad cibernética.

2. Promover la adopción de buenas prácticas de seguridad a nivel global.

3. Facilitar la colaboración y el intercambio de conocimientos entre la comunidad de seguridad cibernética.

4. Ayudar a las organizaciones a proteger sus activos digitales, datos sensibles y sistemas críticos.

5.2 Búsqueda de controles definidos por las normativas

Una vez seleccionadas las normativas de control pertinentes para la evaluación de la madurez de las empresas, se ha realizado una búsqueda de los controles asociados a cada una de ellas. El objetivo de este proceso es establecer una métrica para poder valorar el grado de implementación de medidas de seguridad de la información de las distintas compañías.

Para ello, se ha llevado a cabo una investigación minuciosa, consultando diferentes fuentes confiables y autorizadas. Se ha recurrido a documentos oficiales proporcionados por las organizaciones encargadas de la elaboración y mantenimiento de cada normativa, así como a guías de implementación, manuales de cumplimiento y otros recursos disponibles públicamente. A continuación, se detalla la estructura principal de los controles extraídos de cada una de las normativas:

5.2.1. ISO 27001

Controles extraídos del libro ISO 27001 controls – A guide to implementing and auditing(*ISO 27001 controls – A guide to implementing and auditin*) Es esta fuente se detalla como los controles de seguridad de esta normativa se agrupan en 14 cláusulas principales que cubren áreas como el contexto de la organización, el liderazgo, la planificación, el soporte, la operación, la evaluación del desempeño y la mejora. Cada cláusula contiene requisitos específicos que las organizaciones deben cumplir para establecer y mantener un sistema de gestión de seguridad de la información efectivo y robusto.

5.2.2. NIST SP 800

Controles extraídos de la web oficial de NIST(Computer Security Division 2021). En el documento NIST SP 800-53 adjunto en la web, se detalla los controles de seguridad y privacidad de la información para sistemas de información federales en los Estados Unidos. La estructura de la normativa se desglosa en 18 familias, cada una cubriendo diferentes aspectos de la seguridad de la información, como control de acceso, identificación y autenticación, auditoría y responsabilidad, entre otros. Cada familia contiene controles específicos que proporcionan orientación detallada sobre las medidas que las organizaciones deben implementar para garantizar la seguridad de sus sistemas. Además, el documento incluye suplementos de controles para situaciones específicas, como controles de privacidad y controles para sistemas industriales y críticos.

5.2.3 HIPAA

Controles extraídos la revista oficial online de la asociación HIPAA(Alder 2023). Sus controles se organizan en tres áreas principales: administrativos, físicos y técnicos. Los controles definidos en esta normativa abordan principalmente temáticas relacionadas con la privacidad y el cumplimiento legal del uso de sistemas informatizados.

5.2.4 PCI DSS

Controles extraídos del repositorio de documentos oficial de la asociación PCI(*Document Library*). Los controles se estructuran en 12 áreas que abarcan desde la construcción y

mantenimiento de una red segura, la protección de los datos de las tarjetas de pago mediante cifrado y limitaciones de almacenamiento, hasta la implementación de medidas de control de acceso y la realización de pruebas y monitoreo regular de la seguridad de la red. Estos controles proporcionan principalmente una guía detallada sobre la protección de la información confidencial.

5.2.5 CIS

Controles extraídos de la web oficial del centro para la seguridad de internet (CIS)(*CIS Controls Version 8*). Originalmente, existían 20 controles en el marco CIS, pero en versiones más recientes se han expandido a 18 para proporcionar un enfoque más pragmático y manejable. Estos controles están organizados en tres grupos principales: controles básicos de ciberseguridad, controles de higiene de ciberseguridad y controles avanzados de ciberseguridad. Juntos, proporcionan una estructura sólida para mejorar la seguridad de la información y proteger las organizaciones contra una gran cantidad de amenazas online.

El proceso de búsqueda e identificación de controles normativos ha implicado una investigación exhaustiva y meticulosa, con tal de garantiza que la herramienta de evaluación sea respaldada por una base sólida de controles reconocidos internacionalmente y alineados con las mejores prácticas de seguridad y cumplimiento legal.

5.3 Áreas de solución para Pymes

Después de recopilar todos los controles de diversas normativas, se han identificado un total de 856 controles que abordan temáticas complejas y diversas. Con el fin de crear una herramienta específica para las pequeñas y medianas empresas españolas, se ha realizado una reasignación y selección de controles, evitando realizar sugerencias que por limitaciones de coste y personal puede ser complejo de ser llevado a cabo por este tipo de empresas.

Por lo tanto, el propósito principal de este apartado es determinar las áreas principales en las que se centrarán las recomendaciones y evaluaciones de las compañías.

Para identificar y establecer estas áreas críticas de enfoque, se ha realizado una investigación utilizando estudios y publicaciones de organizaciones especializadas en ciberseguridad y seguridad de la información como el INCIBE(*Seguridad y biometría | Ciudadanía | INCIBE*). No obstante, se ha optado como resultado utilizar un informe publicado por ENISA, el principal organismo europeo en ciberseguridad, que establece 12 directrices fundamentales para proteger a las empresas pequeñas y medianas (SMEs)(*ENISA Cybersecurity guide for SMEs_ES*):

5.3.1 Desarrollo de una buena cultura de ciberseguridad

Se ha de designar a un responsable dentro de la empresa para gestionar eficazmente los recursos destinados a la seguridad de la información TI, como tiempo del personal, compra de software y hardware, formación y desarrollo de políticas efectivas. Además, se enfatiza la importancia de aumentar la participación y concienciación de los empleados mediante una comunicación clara, formación adecuada y el establecimiento de normas específicas en las políticas de ciberseguridad.

5.3.2 Impartir formación adecuada

Es crítico que las empresas proporcionen formación regular en ciberseguridad para todos los empleados, con un enfoque adaptado a las necesidades específicas de las pymes y centrado en situaciones prácticas. Además, se ha de ofrecer formación especializada a los responsables de la gestión de la ciberseguridad, garantizando que estén equipados con los conocimientos y habilidades necesarios para proteger eficazmente la empresa contra las amenazas cibernéticas.

5.3.3 Garantizar una gestión eficaz de terceros

Asegurar una gestión activa de todos los proveedores, especialmente aquellos con acceso a datos sensibles o sistemas críticos. Se deben establecer acuerdos detallados que especifiquen los requisitos de seguridad y garanticen el cumplimiento por parte de los proveedores, lo que asegurará la protección adecuada de la información empresarial.

5.3.4 Desarrollar un plan de respuesta ante incidentes

Elaborar un plan de respuesta ante incidentes que contemple directrices claras, roles definidos y responsabilidades documentadas para asegurar una respuesta oportuna y profesional a cualquier incidente de seguridad. La implementación de herramientas que permitan monitorear y generar alertas ante actividades sospechosas o fallos de seguridad facilitará una respuesta rápida y eficaz ante posibles amenazas.

5.3.5 Proteger el acceso a los sistemas

Fomentar el uso de frases de contraseña, que consisten en una combinación de al menos tres palabras aleatorias para formar una frase fácil de recordar y segura. En caso de optar por una contraseña convencional, es importante asegurarse de que sea larga y contenga una variedad

de caracteres, incluyendo mayúsculas, minúsculas, números y caracteres especiales, evitando términos obvios o secuencias predecibles. Además, se aconseja no utilizar información personal accesible en Internet y evitar compartir contraseñas con otros usuarios. Es fundamental activar la autenticación de doble factor y considerar el uso de un gestor de contraseñas dedicado para una gestión segura y eficiente de las credenciales.

5.3.6 Proteger los dispositivos

Dentro de un programa de ciberseguridad se debe mantener protegidos todos los dispositivos utilizados por el personal, incluyendo computadoras de escritorio, portátiles, tabletas y teléfonos móviles. Para ello, se recomienda mantener el software actualizado periódicamente, utilizando una plataforma centralizada para gestionar los parches y activando las actualizaciones automáticas siempre que sea posible. Además, es crítico implementar una solución de antivirus en todos los dispositivos y evitar la instalación de software pirata para prevenir la presencia de programas maliciosos. Asimismo, se deben utilizar herramientas de protección de la web y del correo electrónico para bloquear correos no deseados y potencialmente peligrosos. Es crucial cifrar los datos almacenados en dispositivos móviles y durante su transmisión a través de redes públicas, utilizando tecnologías como VPN o SSL/TLS. Por último, se recomienda el uso de un gestor de dispositivos móviles (MDM) para controlar y proteger los dispositivos utilizados por el personal, garantizando la actualización del software, la implementación de medidas de seguridad y la posibilidad de borrar datos de manera remota en caso de pérdida o robo del dispositivo.

5.3.7 Proteger su red

El uso de cortafuegos ayuda a gestionar el tráfico entrante y saliente de una red, siendo una herramienta fundamental para proteger los sistemas TI. Se han de implementar cortafuegos para salvaguardar todos los sistemas importantes, especialmente aquellos conectados a Internet. Además, las empresas deben realizar revisiones regulares de las soluciones de acceso remoto para garantizar su seguridad. Esto incluye asegurarse de que todo el software esté actualizado, restringir el acceso desde ubicaciones sospechosas, limitar el acceso a sistemas específicos, utilizar contraseñas seguras y activar la autenticación de doble factor. También es importante contar con un sistema de control y alerta para detectar posibles ataques o actividades inusuales.

5.3.8 Mejorar la seguridad física

Implementar controles físicos adecuados en los lugares donde se almacena información es importante para garantizar su seguridad. Por ejemplo, los dispositivos móviles y los ordenadores portátiles de la empresa no deben dejarse sin supervisión, y se recomienda bloquearlos cuando el usuario se aleje. Además, los documentos impresos sensibles deben guardarse de manera segura cuando no estén en uso para evitar posibles fugas de información. Estas medidas ayudan a proteger los activos de la empresa y a prevenir accesos no autorizados a datos confidenciales.

5.3.9 Proteger las copias de seguridad

Realizar copias de seguridad periódicas y automáticas para garantizar la recuperación de datos clave en caso de desastres como ataques de *ransomware*. Estas copias deben mantenerse separadas del entorno de producción de la empresa y estar cifradas, especialmente si se trasladan a otra ubicación. Es importante realizar pruebas periódicas para verificar la capacidad de recuperación de datos, idealmente con una restauración completa de inicio a fin. Estas medidas ayudan a asegurar la integridad y disponibilidad de la información empresarial en situaciones críticas.

5.3.10 Trabajar en la nube

Al adoptar soluciones en la nube, las compañías deben considerar tanto los beneficios como los riesgos asociados. Antes de elegir un proveedor de servicios en la nube, es crucial que las empresas consulten guías de seguridad específicas para comprender mejor los requisitos y desafíos.

5.3.11 Proteger sus sitios web

Las compañías deben garantizar la seguridad de sus sitios web, especialmente protegiendo datos sensibles como información financiera o datos de tarjetas de crédito. Esto implica realizar pruebas de seguridad regulares para identificar posibles vulnerabilidades y llevar a cabo actualizaciones frecuentes para mantener la protección adecuada.

5.3.12 Buscar y compartir información

El intercambio de información es relevante en la lucha contra la ciberdelincuencia, ya que permite a las compañías comprender mejor los riesgos a los que se enfrentan. Aquellas empresas que reciben información sobre problemas de ciberseguridad de sus compañeros están más inclinadas a tomar medidas para proteger sus sistemas en comparación con aquellas que obtienen información de informes del sector o encuestas sobre ciberseguridad.

5.4 Clasificación de riesgos de ciberseguridad

Paralelamente, para poder evaluar el estado de madurez de las distintas organizaciones y ofrecer una visión general del grado de implicación de las compañías con respecto a la seguridad de sus sistemas, se ha decidido establecer una unidad de métrica basada en el análisis de riesgos cibernéticos en alcance.

De forma similar al apartado anterior, se ha tomado como referencia la institución ENISA como fuente principal para establecer las 8 áreas de amenazas cibernéticas existentes(*Threat Taxonomy*): Ataques intencionales, Daños involuntarios, Desastres naturales, Fallos/Mal funcionamiento, Disponibilidad de recursos, Intercepciones, Actividades Maliciosas y Legal.

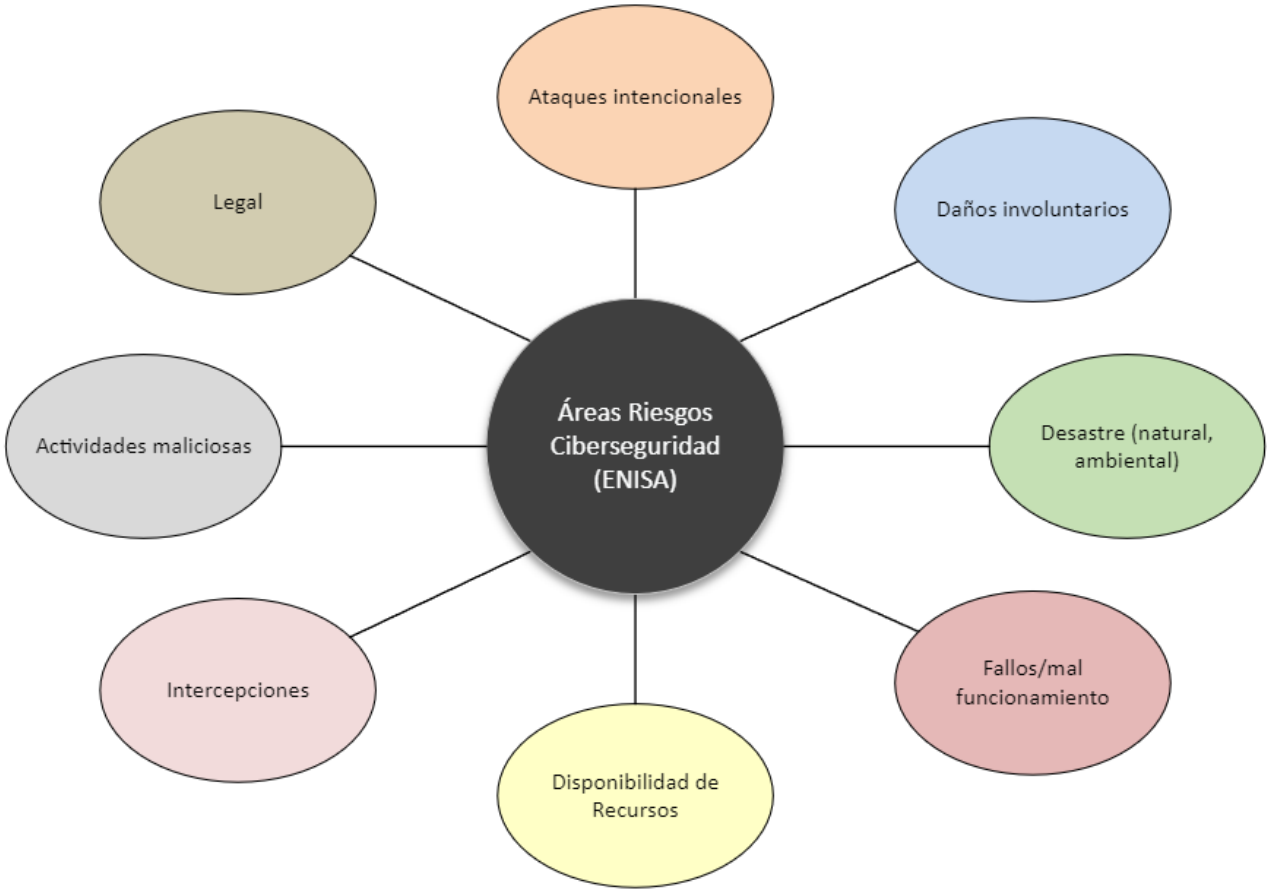


Ilustración 5. Área de riesgos de ciberseguridad según ENISA. Fuente: Elaboración propia.

A continuación, se detalla las características y riesgos específicos de cada una de las áreas de ciberseguridad según ENISA:

5.4.1 Ataques intencionales

Amenazas de acciones hostiles intencionales por parte de humanos. Estas amenazas se refieren a acciones deliberadas llevadas a cabo por individuos con la intención de dañar o comprometer la seguridad de una organización, sus sistemas o sus datos. Los riesgos específicos de esta área son:

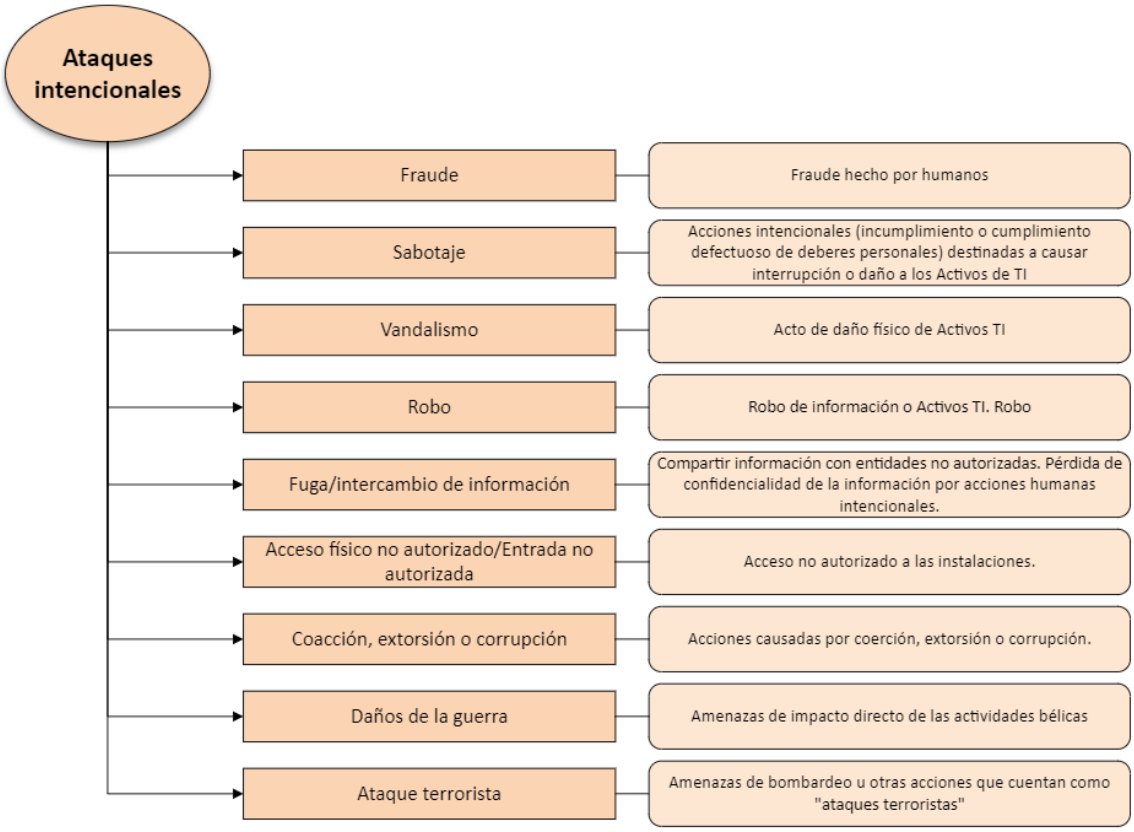


Ilustración 6. Riesgos de ataques intencionales. Fuente: Elaboración propia.

5.4.2 Daños involuntarios

Amenazas de acciones humanas no intencionales o errores. Estas amenazas se refieren a situaciones en las que los errores humanos, ya sea por descuido, falta de capacitación o malentendidos, pueden provocar incidentes de seguridad. Los riesgos específicos de esta área son:

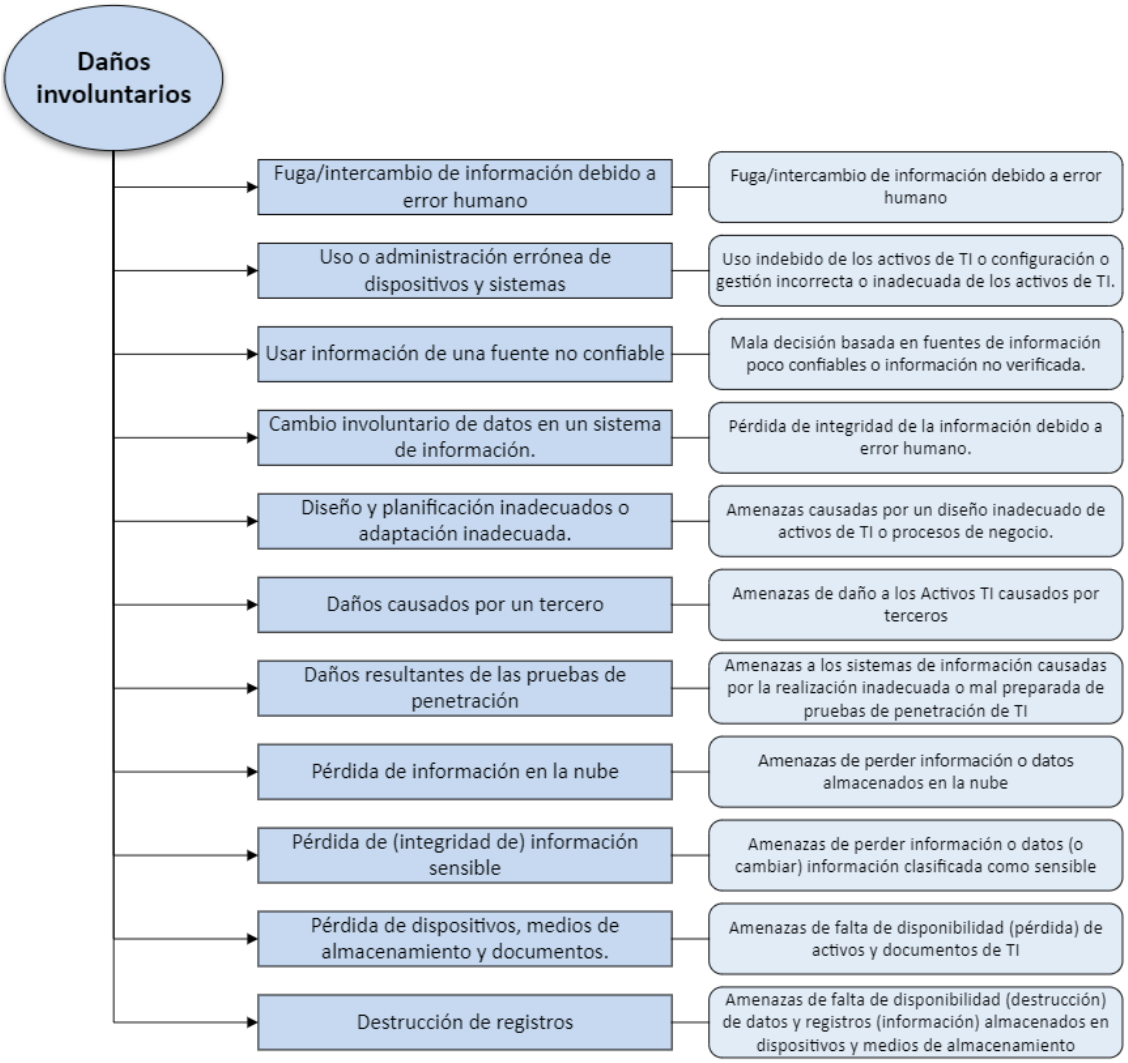


Ilustración 7. Riesgos de daños involuntarios. Fuente: Elaboración propia.

5.4.3 Desastre (natural, ambiental)

Amenazas de daño a los activos de información causadas por elementos naturales o ambientales. Estas amenazas se refieren a riesgos como incendios, inundaciones, terremotos u otros desastres naturales que pueden afectar negativamente a los activos de información de una organización. Los riesgos específicos de esta área son:

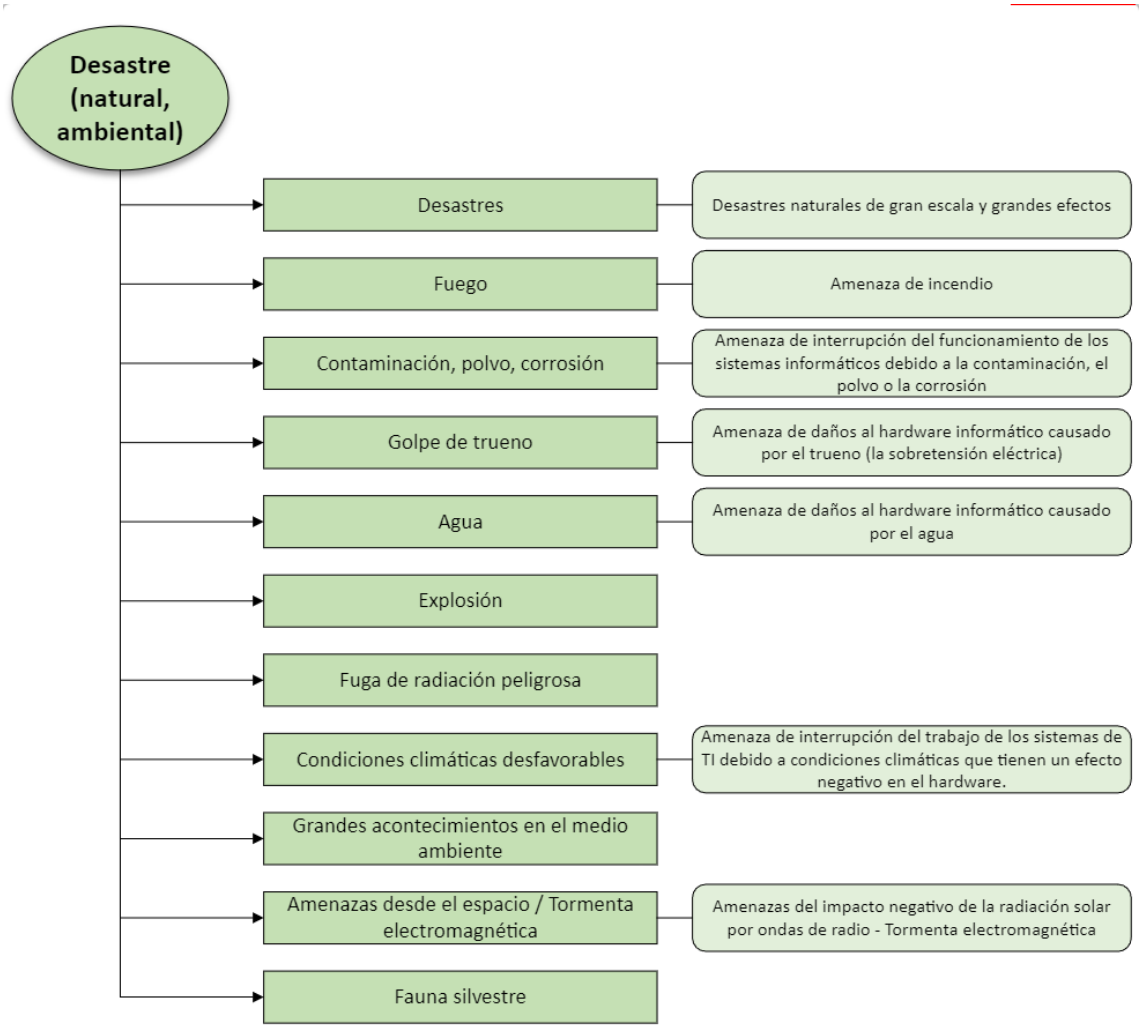


Ilustración 8. Riesgos de desastres naturales/ambientales. Fuente: Elaboración propia.

5.4.4 Fallos/Mal funcionamiento

Amenaza de fallo o mal funcionamiento de la infraestructura de soporte de TI (es decir, degradación de la calidad, parámetros de funcionamiento incorrectos, interferencias). Esta amenaza está relacionada con la posibilidad de que la infraestructura de TI experimente fallos o mal funcionamiento debido a problemas internos, como la sobrecarga en la red eléctrica de un edificio, lo que podría afectar negativamente la disponibilidad y funcionalidad de los sistemas de tecnología de la información. Los riesgos específicos de esta área son:

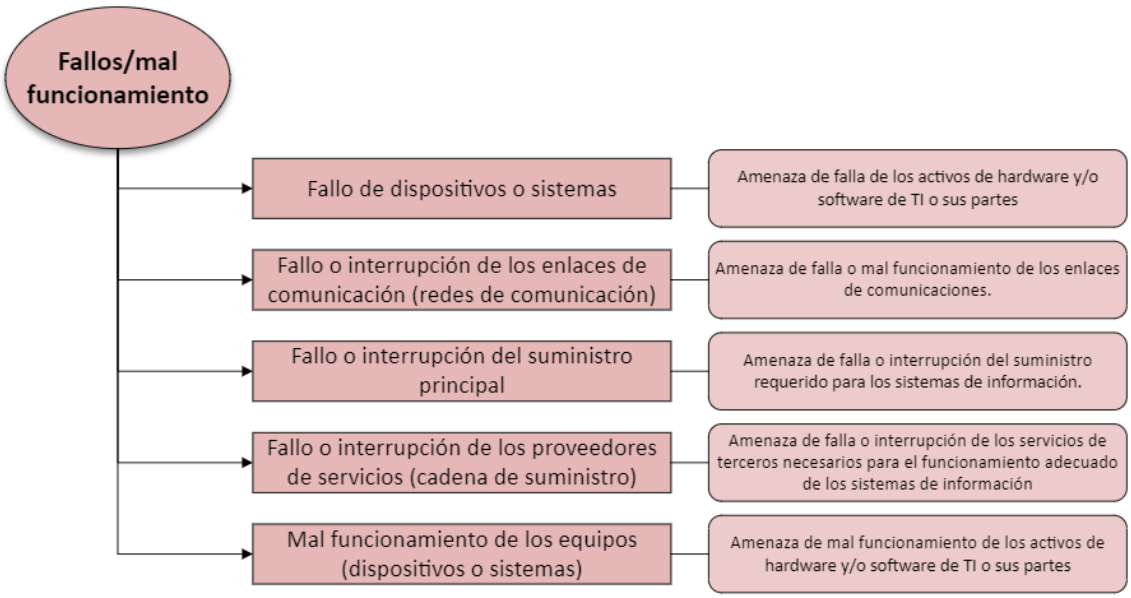


Ilustración 9. Riesgos de fallos/mal funcionamiento de los sistemas. Fuente: Elaboración propia.

5.4.5 Disponibilidad de recursos

Amenaza de completa falta o pérdida de recursos necesarios para la infraestructura de TI. Esta amenaza implica el riesgo de que la infraestructura de TI experimente una interrupción completa debido a la falta o pérdida de recursos esenciales, como electricidad o conectividad de red, causada principalmente por problemas externos, como un apagón generalizado en la ciudad. Los riesgos específicos de esta área son:

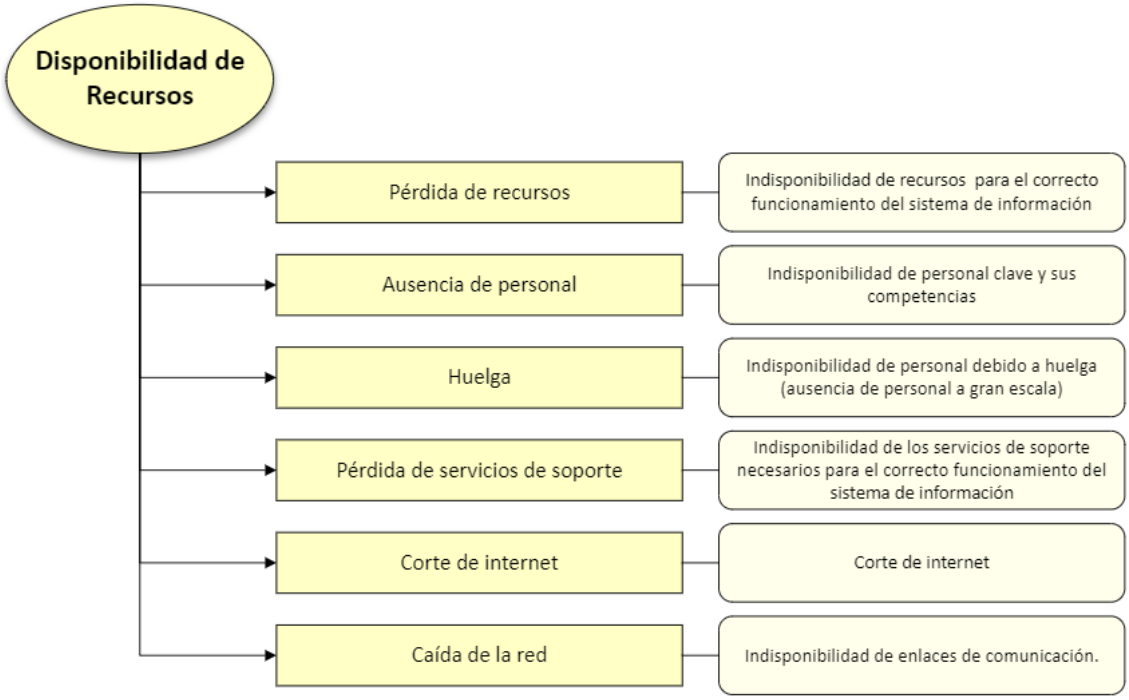


Ilustración 10. Riesgos de disponibilidad de recursos. Fuente: Elaboración propia.

5.4.6 Intercepciones

Amenaza en alteraciones de la comunicación entre dos partes y no requiere la instalación de herramientas o software adicionales en el sitio de la víctima. Estos ataques pueden comprometer la integridad o la confidencialidad de la comunicación, lo que puede resultar en la divulgación de información sensible o la manipulación de datos. Los riesgos específicos de esta área son:

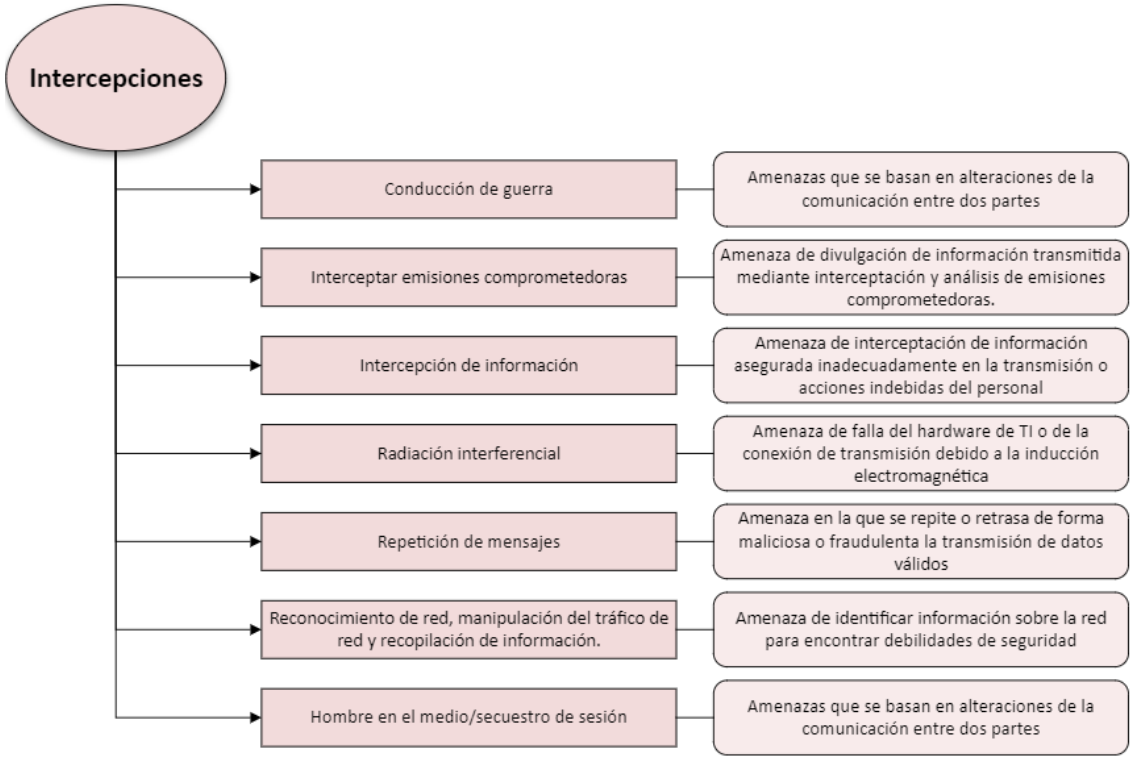


Ilustración 11. Riesgos de intercepciones. Fuente: Elaboración propia.

5.4.7 Actividades maliciosas

Estas amenazas involucran actividades maliciosas que requieren el uso de herramientas por parte del atacante. Para llevar a cabo estos ataques, es necesario instalar software adicional o realizar pasos adicionales en la infraestructura o el software de la víctima. Estas acciones pueden incluir la implantación de malware, la explotación de vulnerabilidades o la realización de ingeniería social para comprometer los sistemas de la víctima. Los riesgos específicos de esta área son:

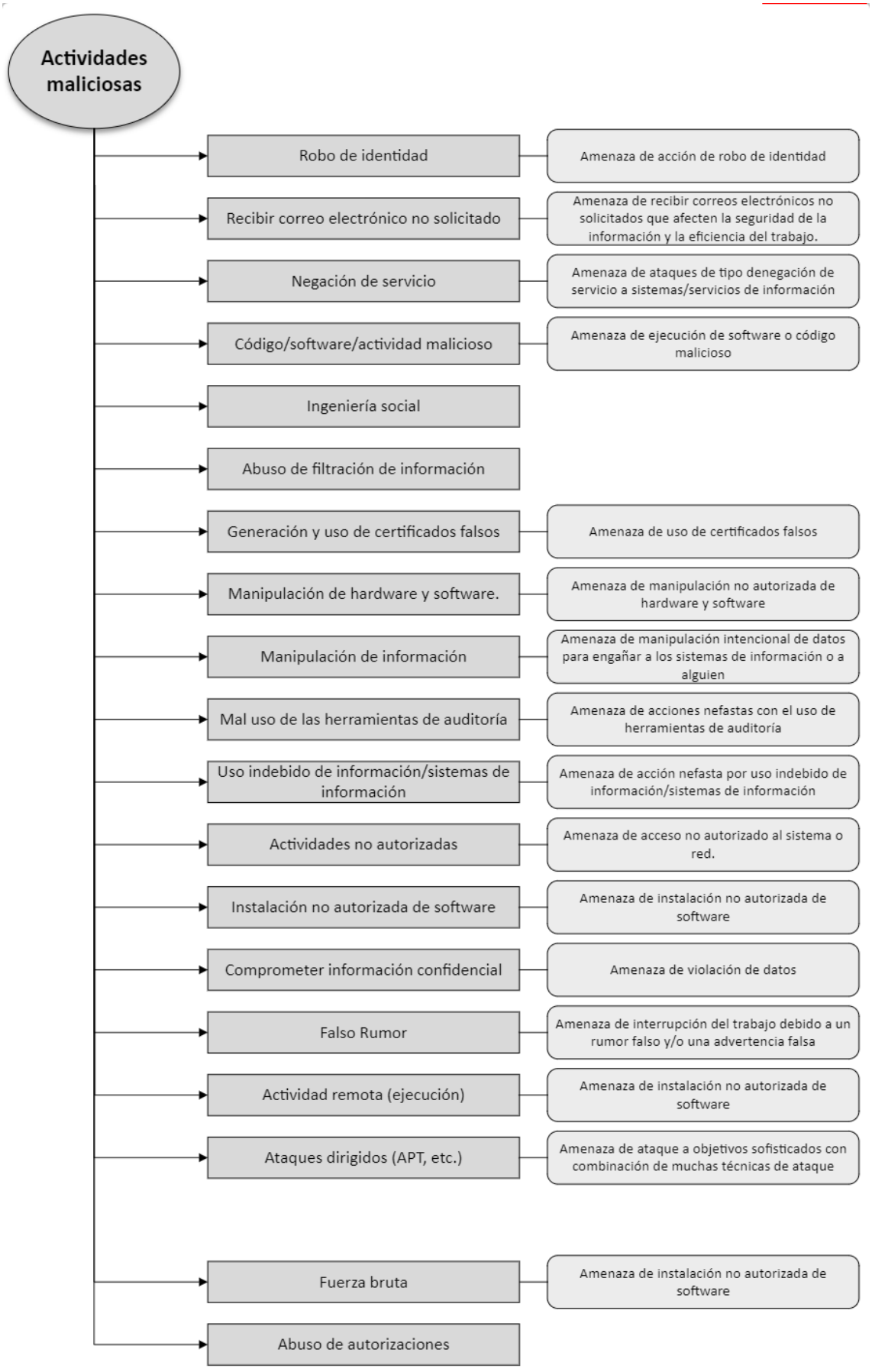


Ilustración 12. Riesgos de actividades maliciosas. Fuente: Elaboración propia.

5.4.8 Legal

Amenaza sobre la posibilidad de enfrentar sanciones financieras o legales, así como la pérdida de confianza por parte de clientes y colaboradores debido a incumplimientos legislativos. Esto puede ocurrir si una organización no cumple con las regulaciones y leyes establecidas en su industria o jurisdicción, lo que podría resultar en multas, demandas judiciales u otras consecuencias legales. La pérdida de confianza por parte de clientes y colaboradores también puede ser perjudicial para la reputación y la imagen de la empresa, lo que puede afectar negativamente su desempeño y relaciones comerciales a largo plazo. Los riesgos específicos de esta área son:

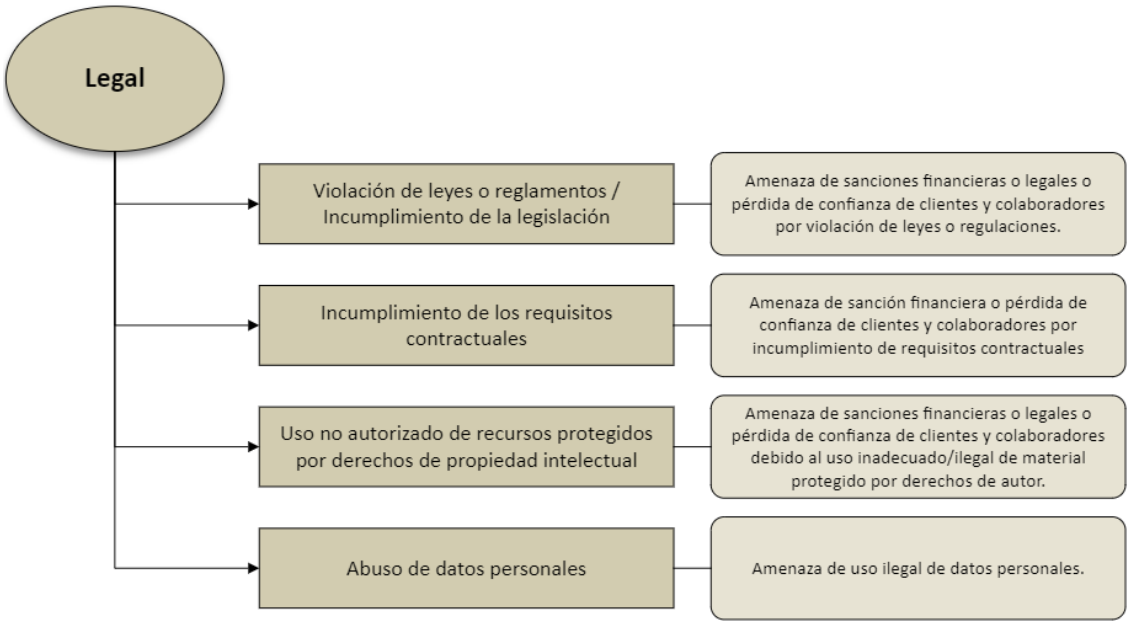


Ilustración 13. Riesgos legales. Fuente: Elaboración propia.

Tras establecer las área de riesgos se procederá a establecer una trazabilidad entre los controles en alcance y los riesgos de ciberseguridad que cubre cada uno.

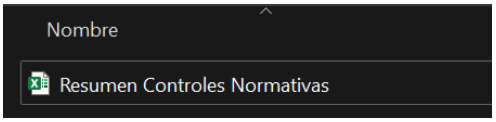
6. DESARROLLO DE LA SOLUCIÓN

Teniendo en cuenta los controles de las normativas anteriores, las áreas de solución y riesgos de ciberseguridad identificados, se ha procedido al desarrollo de la solución.

Fase 1. Matriz de normativas agrupadas

Tomando como referencia las fuentes de información detalladas en el apartado *"5.2 2 Búsqueda de controles definidos por las normativas"* de este documento, se ha procedido a analizar y entender la estructura de cada una de ellas con el fin de tratar los datos y agrupar la totalidad de controles en una única tabla.

Para la elaboración de este tabla se ha creado el documento "Resumen Controles Normativas":



A continuación, se muestra como primer paso para la estandarización de los datos, las tablas originales utilizadas y su versión formateada en las que se ha extraído para cada normativa los campos para la tabla maestra.

	A	B	C
1	ISO27001:2013 - ANEXO A		
2	OBJETIVOS DE CONTROL Y CONTROLES		
3			
4	A.5. POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN.	A.5.1. Orientación de la Dirección para la Gestión de la Seguridad de la Información.	A.5.1.1. Políticas para la Seguridad de la Información. Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la Dirección, publicada y comunicada a los empleados y partes interesadas.
5		Objetivo. Brindar orientación y soporte, por parte de la dirección, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.	A.5.1.2. Revisión de las Políticas para seguridad de la información. Las Políticas para Seguridad de la Información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continúas.
6	A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.	A.6.1. Organización Interna.	A.6.1.1. Seguridad de la Información Roles y Responsabilidades. Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
7		Objetivo. Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación del SGSI.	A.6.1.2. Separación de deberes. Las tareas y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización.
8			A.6.1.3. Contacto con las autoridades. Se debe mantener contactos apropiados con las autoridades pertinentes.
9			A.6.1.4. Contacto con grupos de interés especial. Se deben mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
10			A.6.1.5. Seguridad de la información en Gestión de Proyectos. La seguridad de la información se debe tratar en la gestión de proyectos, independiente del tipo de proyecto,
11		A.6.2. Dispositivos Móviles y Teletrabajo.	A.6.2.1. Política para dispositivos móviles. Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
		Objetivo. Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.	A.6.2.2. Teletrabajo. Se deben implementar una política y medidas de seguridad de soporte para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza

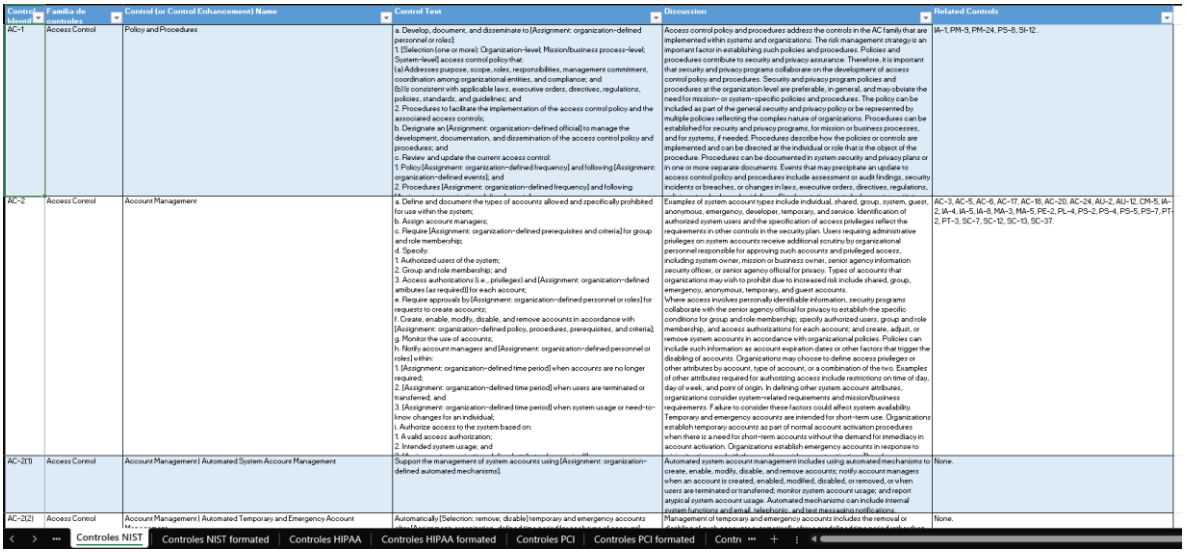
Controles ISO | Controles ISO formated | Controles NIST | Controles NIST formated | Controles HIPAA | Controles

Ilustración 14. Tabla Controles ISO27001 Original. Fuente: Elaboración propia.

Control	ID Control	Descripción Control
A.5.1.1. Políticas para la Seguridad de la Información. Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la Dirección, publicada y comunicada a los empleados y partes interesadas.	A.5.1.1. Políticas para la Seguridad de la Información	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la Dirección, publicada y comunicada a los empleados y partes interesadas.
A.5.1.2. Revisión de las Políticas para seguridad de la información. Las Políticas para Seguridad de la Información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continúas.	A.5.1.2. Revisión de las Políticas para seguridad de la información	Las Políticas para Seguridad de la Información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continúas.
A.6.1.1. Seguridad de la Información Roles y Responsabilidades. Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	A.6.1.1. Seguridad de la Información Roles y Responsabilidades	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
A.6.1.2. Separación de deberes. Las tareas y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización.	A.6.1.2. Separación de deberes	Las tareas y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización.
A.6.1.3. Contacto con las autoridades. Se debe mantener contactos apropiados con las autoridades pertinentes.	A.6.1.3. Contacto con las autoridades	Se debe mantener contactos apropiados con las autoridades pertinentes.
A.6.1.4. Contacto con grupos de interés especial. Se deben mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	A.6.1.4. Contacto con grupos de interés especial	Se deben mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
A.6.1.5. Seguridad de la información en Gestión de Proyectos. La seguridad de la información se debe tratar en la gestión de proyectos, independiente del tipo de	A.6.1.5. Seguridad de la información en Gestión de Proyectos	La seguridad de la información se debe tratar en la gestión de proyectos, independiente del tipo de proyecto,

Controles ISO | Controles ISO formated | Controles NIST | Controles NIST formated | Controles HIPAA | Controles HIPAA form

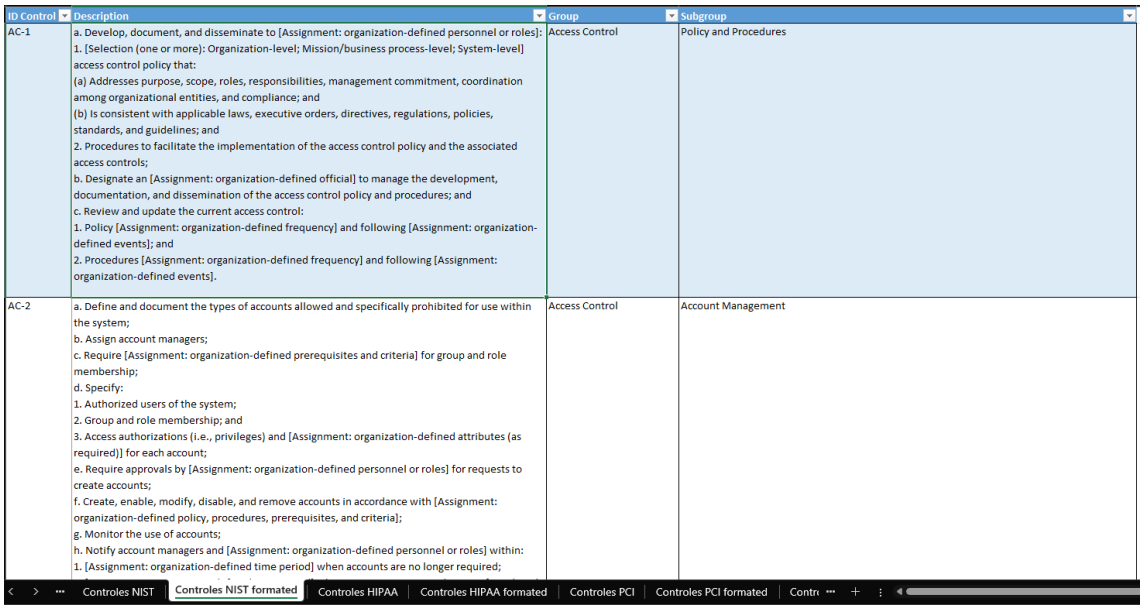
Ilustración 15. Tabla Controles ISO27001 Formateada. Fuente: Elaboración propia.



Control Identifier	Familia de controles	Control (or Control Enhancement) Name	Control Text	Discussion	Related Controls
AC-1	Access Control	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] access control policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the access control policy and the associated access controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and c. Review and update the current access control: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and 2. Procedures [Assignment: organization-defined frequency] and following	Access control policy and procedures address the controls in the AC family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of access control policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies reflecting the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to access control policy and procedures include assessment or audit findings, security incidents or breaches, or changes in laws, executive orders, directives, regulations,	IA-1, PM-9, PM-24, PS-8, SI-12.
AC-2	Access Control	Account Management	a. Define and document the types of accounts allowed and specifically prohibited for use within the system; b. Assign account managers; c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership; d. Specify: 1. Authorized users of the system; 2. Group and role membership; and 3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account; e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts; f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria]; g. Monitor the use of accounts; h. Notify account managers and [Assignment: organization-defined personnel or roles] within: 1. [Assignment: organization-defined time period] when accounts are no longer required; 2. [Assignment: organization-defined time period] when users are terminated or transferred; and 3. [Assignment: organization-defined time period] when system usage or need-to-know changes for an individual; i. Authorize access to the system based on: 1. A valid access authorization; 2. Intended system usage; and	Examples of system account types include individual, shared, group, system, guest, anonymous, emergency, developer, temporary, and service. Identification of authorized system users and the specification of access privileges reflect the requirements in other controls in the security plan. Users requiring administrative privileges on system accounts receive additional scrutiny by organizational personnel responsible for approving such accounts and privileged access, including system owner, mission or business owner, senior agency information security officer, or senior agency official for privacy. Types of accounts that organizations may wish to prohibit due to increased risk include shared, group, emergency, anonymous, temporary, and guest accounts. Where access involves personally identifiable information, security programs collaborate with the senior agency official for privacy to establish the specific conditions for group and role membership; specify authorized users, group and role membership, and access authorizations for each account; and create, adjust, or remove system accounts in accordance with organizational policies. Policies can include such information as account expiration dates or other factors that trigger the disabling of accounts. Organizations may choose to define access privileges or other attributes by account, type of account, or a combination of the two. Examples of other attributes required for authorizing access include restrictions on time of day, day of week, and point of origin. In defining other system account attributes, organizations consider system-related requirements and mission/business requirements. Failure to consider these factors could affect system availability. Temporary and emergency accounts are intended for short-term use. Organizations establish temporary accounts as part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to	AC-3, AC-5, AC-6, AC-17, AC-18, AC-20, AC-24, AU-2, AU-12, CM-5, IA-2, IA-4, IA-5, IA-8, MA-3, MA-5, PE-2, PL-4, PS-2, PS-4, PS-5, PS-7, PT-2, PT-3, SC-7, SC-12, SC-13, SC-37.
AC-2(1)	Access Control	Account Management | Automated System Account Management	Support the management of system accounts using [Assignment: organization-defined automated mechanisms].	Automated system account management includes using automated mechanisms to create, enable, modify, disable, and remove accounts; notify account managers when an account is created, enabled, modified, disabled, or removed, or when users are terminated or transferred; monitor system account usage; and report atypical system account usage. Automated mechanisms can include internal system functions and email, telephonic, and text messaging notifications.	None.
AC-2(2)	Access Control	Account Management | Automated Temporary and Emergency Account	Automatically [Selection: remove; disable] temporary and emergency accounts	Management of temporary and emergency accounts includes the removal or	None.

Controles NIST | Controles NIST formated | Controles HIPAA | Controles HIPAA formated | Controles PCI | Controles PCI formated | Contr

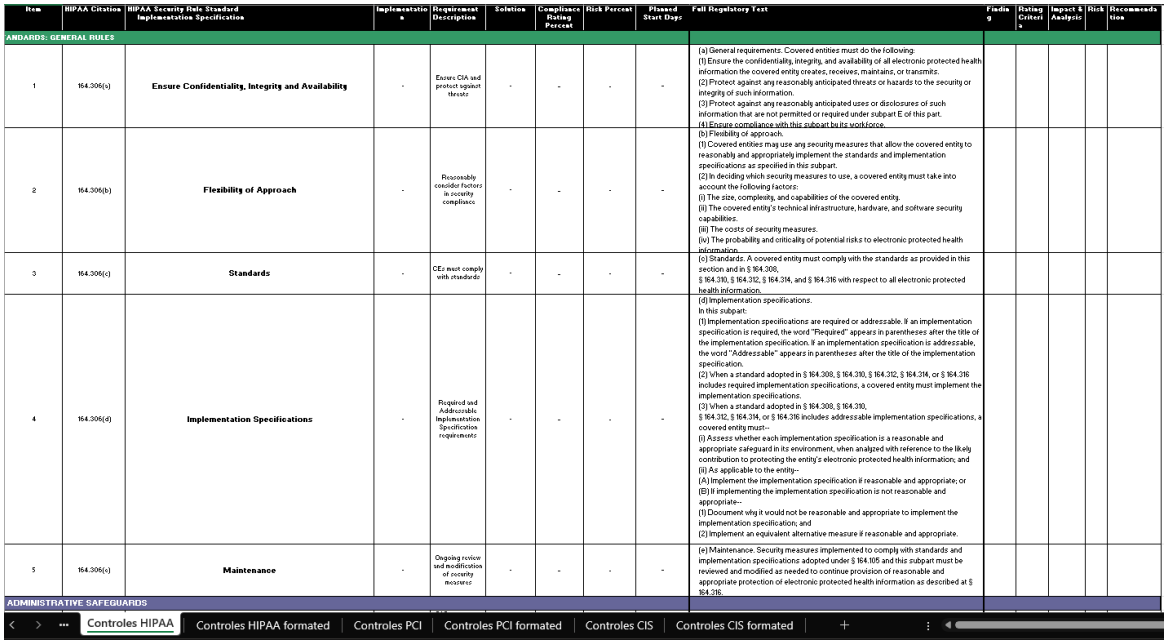
Ilustración 16. Tabla Controles NIST Original. Fuente: Elaboración propia.



ID Control	Description	Group	Subgroup
AC-1	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more): Organization-level; Mission/business process-level; System-level] access control policy that: (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and 2. Procedures to facilitate the implementation of the access control policy and the associated access controls; b. Designate an [Assignment: organization-defined official] to manage the development, documentation, and dissemination of the access control policy and procedures; and c. Review and update the current access control: 1. Policy [Assignment: organization-defined frequency] and following [Assignment: organization-defined events]; and 2. Procedures [Assignment: organization-defined frequency] and following [Assignment: organization-defined events].	Access Control	Policy and Procedures
AC-2	a. Define and document the types of accounts allowed and specifically prohibited for use within the system; b. Assign account managers; c. Require [Assignment: organization-defined prerequisites and criteria] for group and role membership; d. Specify: 1. Authorized users of the system; 2. Group and role membership; and 3. Access authorizations (i.e., privileges) and [Assignment: organization-defined attributes (as required)] for each account; e. Require approvals by [Assignment: organization-defined personnel or roles] for requests to create accounts; f. Create, enable, modify, disable, and remove accounts in accordance with [Assignment: organization-defined policy, procedures, prerequisites, and criteria]; g. Monitor the use of accounts; h. Notify account managers and [Assignment: organization-defined personnel or roles] within: 1. [Assignment: organization-defined time period] when accounts are no longer required;	Access Control	Account Management

Controles NIST | Controles NIST formated | Controles HIPAA | Controles HIPAA formated | Controles PCI | Controles PCI formated | Contr

Ilustración 17. Tabla Controles NIST Formateada. Fuente: Elaboración propia.



Item	HIPAA Citation	HIPAA Security Rule Standard Implementation Specification	Implementation	Requirement Description	Solution	Compliance Rating Percent	Risk Percent	Planned Start Days	Full Regulatory Text	Finding	Rating Criteria	Impact & Analysis	Risk	Recommendation
ANDARDS: GENERAL RULES														
1	164.306(a)	**Ensure Confidentiality, Integrity and Availability**	-	Ensure CIA and protect against threats	-	-	-	-	(a) General requirements. Covered entities must do the following: (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part. (4) Ensure compliance with this subpart by its workforce.					
2	164.306(b)	**Flexibility of Approach**	-	Reasonably consider factors in security compliance	-	-	-	-	(b) Flexibility of approach. (1) Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart. (2) In deciding which security measures to use, a covered entity must take into account the following factors: (i) The size, complexity, and capabilities of the covered entity. (ii) The covered entity's technical infrastructure, hardware, and software security capabilities. (iii) The costs of security measures. (iv) The probability and criticality of potential risks to electronic protected health information.					
3	164.306(c)	**Standards**	-	CEs must comply with standards	-	-	-	-	(c) Standards. A covered entity must comply with the standards as provided in this section and in § 164.308, § 164.310, § 164.312, § 164.314, and § 164.316 with respect to all electronic protected health information.					
4	164.306(d)	**Implementation Specifications**	-	Required and Addressable Implementation Specification requirements	-	-	-	-	(d) Implementation specifications. In this subpart: (1) Implementation specifications are required or addressable. If an implementation specification is required, the word "Required" appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word "Addressable" appears in parentheses after the title of the implementation specification. (2) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity must implement the implementation specifications. (3) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity must-- (i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic protected health information; and (ii) As applicable to the entity-- (A) Implement the implementation specification if reasonable and appropriate; or (B) If implementing the implementation specification is not reasonable and appropriate-- (1) Document why it would not be reasonable and appropriate to implement the implementation specification; and (2) Implement an equivalent alternative measure if reasonable and appropriate.					
5	164.306(e)	**Maintenance**	-	Ongoing review and modification of security measures	-	-	-	-	(e) Maintenance. Security measures implemented to comply with standards and implementation specifications adopted under § 164.105 and this subpart must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of electronic protected health information as described at § 164.316.					
ADMINISTRATIVE SAFEGUARDS														

Controles HIPAA | Controles HIPAA formated | Controles PCI | Controles PCI formated | Controles CIS | Controles CIS formated

Ilustración 18. Tabla Controles HIPAA Original. Fuente: Elaboración propia.

ID Control	Description	Group
164.306(a) Ensure Confidentiality, Integrity and Availability	(a) General requirements. Covered entities must do the following: (1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits. (2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information. (3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of this part.	SECURITY STANDARDS: GENERAL RULES
164.306(b) Flexibility of Approach	(b) Flexibility of approach. (1) Covered entities may use any security measures that allow the covered entity to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart. (2) In deciding which security measures to use, a covered entity must take into account the following factors: (i) The size, complexity, and capabilities of the covered entity. (ii) The covered entity's technical infrastructure, hardware, and software security capabilities. (iii) The costs of security measures.	SECURITY STANDARDS: GENERAL RULES
164.306(c) Standards	(c) Standards. A covered entity must comply with the standards as provided in this section and in § 164.308, § 164.310, § 164.312, § 164.314, and § 164.316 with respect to all electronic protected health information.	SECURITY STANDARDS: GENERAL RULES
164.306(d) Implementation Specifications	(d) Implementation specifications. In this subpart: (1) Implementation specifications are required or addressable. If an implementation specification is required, the word "Required" appears in parentheses after the title of the implementation specification. If an implementation specification is addressable, the word "Addressable" appears in parentheses after the title of the implementation specification. (2) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a covered entity must implement the implementation specifications. (3) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes addressable implementation specifications, a covered entity must-- (i) Assess whether each implementation specification is a reasonable and appropriate safeguard in its environment, when analyzed with reference to the likely contribution to protecting the entity's electronic protected health information; and (ii) As applicable to the entity-- (A) Implement the implementation specification if reasonable and appropriate; or (B) If implementing the implementation specification is not reasonable and appropriate-- (1) Document why it would not be reasonable and appropriate to implement the implementation specification; and	SECURITY STANDARDS: GENERAL RULES
164.306(e) Maintenance	(e) Maintenance. Security measures implemented to comply with standards and implementation specifications adopted under § 164.105 and this subpart must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of electronic protected health information as	SECURITY STANDARDS: GENERAL RULES
164.308(a)(1)(i) Security Management Process	Implement policies and procedures to prevent, detect, contain and correct security violations	ADMINISTRATIVE SAFEGUARDS
164.308(a)(1)(ii)(A) Risk Analysis	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered	ADMINISTRATIVE SAFEGUARDS
164.308(a)(1)(ii)(B) Risk Management	Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Sec 164.206(a).	ADMINISTRATIVE SAFEGUARDS
164.308(a)(1)(ii)(C) Sanction Policy	Apply appropriate sanctions against workforce members who fail to comply with the security policies and	ADMINISTRATIVE SAFEGUARDS

Controles HIPAA | Controles HIPAA formated | Controles PCI | Controles PCI formated | Controles CIS | Controles CIS formated

Ilustración 19. Tabla Controles HIPAA Formateada. Fuente: Elaboración propia.

PCI DSS Requirements v3.2.1	Milestone	Status *Please enter "yes" if fully compliant with the requirement*	If status is "N/A", please explain why requirement is Not Applicable	If status is "No", please complete the following		
				Stage of Implementation	Estimated Date for Completion of Milestone	Comments
Requirement 1: Install and maintain a firewall configuration to protect cardholder data						
1.1 Establish and implement firewall and router configuration standards that include the following:						
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	6					
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	1					
1.1.3 Current diagram that shows all cardholder data flows across systems and networks	1					
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	2					
1.1.5 Description of groups, roles, and responsibilities for management of network components	6					
1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	2					
1.1.7 Requirement to review firewall and router rule sets at least every six months	6					
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. ***Note:*** *An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*						
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	2					
1.2.2 Secure and synchronize router configuration files.	2					
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	2					
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.						
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	2					
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	2					
1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)	2					
1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	2					
1.3.5 Permit only "established" connections into the network.	2					

Controles HIPAA | Controles HIPAA formated | Controles PCI | Controles PCI formated | Controles CIS | Controles CIS formated

Ilustración 20. Tabla Controles PCI Original. Fuente: Elaboración propia.

ID Control	Description	Group	Subgroup
1.1.1	A formal process for approving and testing all network connections and changes to the firewall and router configurations	*Install and maintain a firewall configuration to protect cardholder data*	**1.1** Establish and implement firewall and router configuration standards that include the following:
1.1.2	Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	*Install and maintain a firewall configuration to protect cardholder data*	**1.1** Establish and implement firewall and router configuration standards that include the following:
1.1.3	Current diagram that shows all cardholder data flows across systems and networks	*Install and maintain a firewall configuration to protect cardholder data*	**1.1** Establish and implement firewall and router configuration standards that include the following:
1.1.4	Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	*Install and maintain a firewall configuration to protect cardholder data*	**1.1** Establish and implement firewall and router configuration standards that include the following:
1.1.5	Description of groups, roles, and responsibilities for management of network components	*Install and maintain a firewall configuration to protect cardholder data*	**1.1** Establish and implement firewall and router configuration standards that include the following:
1.1.6	Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	*Install and maintain a firewall configuration to protect cardholder data*	**1.1** Establish and implement firewall and router configuration standards that include the following:
1.1.7	Requirement to review firewall and router rule sets at least every six months	*Install and maintain a firewall configuration to protect cardholder data*	**1.1** Establish and implement firewall and router configuration standards that include the following:
1.2.1	Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	*Install and maintain a firewall configuration to protect cardholder data*	**1.2** Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.
1.2.2	Secure and synchronize router configuration files.	*Install and maintain a firewall configuration to protect cardholder data*	**1.2** Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.
1.2.3	Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	*Install and maintain a firewall configuration to protect cardholder data*	**1.2** Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible	*Install and maintain a firewall configuration to*	**1.3** Prohibit direct public access between the Internet and any system component in the cardholder data environment.

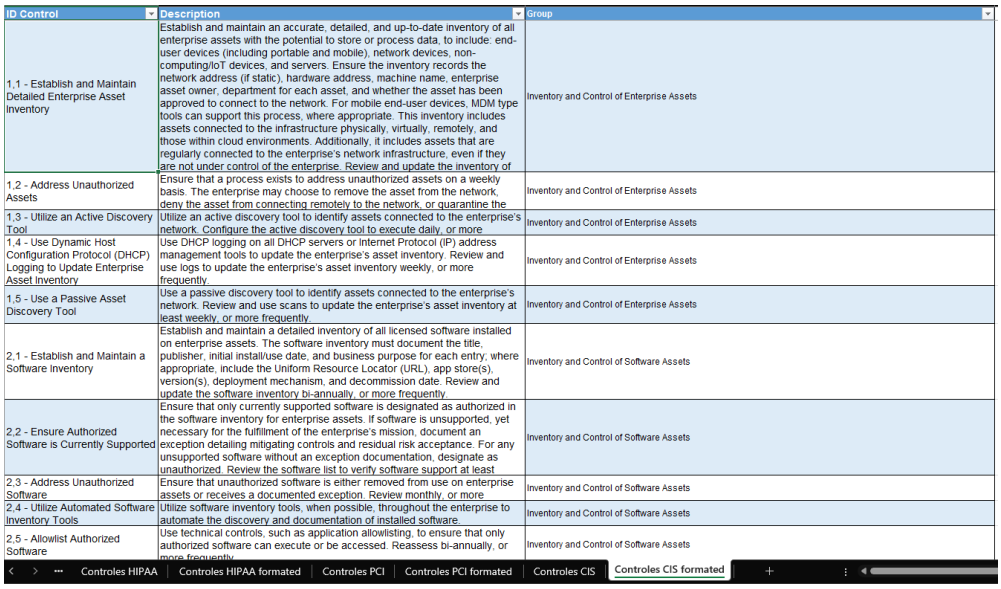
Controles HIPAA | Controles HIPAA formated | Controles PCI | Controles PCI formated | Controles CIS | Controles CIS formated

Ilustración 21. Tabla Controles PCI Formateada. Fuente: Elaboración propia.

CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description	IG1	IG2	IG3
1				**Inventory and Control of Enterprise Assets**	***Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.***			
1	1,1	Devices	Identify	Establish and Maintain Detailed Enterprise Asset Inventory	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently.	x	x	x
1	1,2	Devices	Respond	Address Unauthorized Assets	Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.	x	x	x
1	1,3	Devices	Detect	Utilize an Active Discovery Tool	Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more frequently.		x	x
1	1,4	Devices	Identify	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.		x	x
1	1,5	Devices	Detect	Use a Passive Asset Discovery Tool	Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.			x
2				**Inventory and Control of Software Assets**	***Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.***			
2	2,1	Applications	Identify	Establish and Maintain a Software Inventory	Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	x	x	x
2	2,2	Applications	Identify	Ensure Authorized Software is Currently Supported	Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the	x	x	x

Controles HIPAA | Controles HIPAA formated | Controles PCI | Controles PCI formated | Controles CIS | Controles CIS formated

Ilustración 22. Tabla Controles CIS Original. Fuente: Elaboración propia.

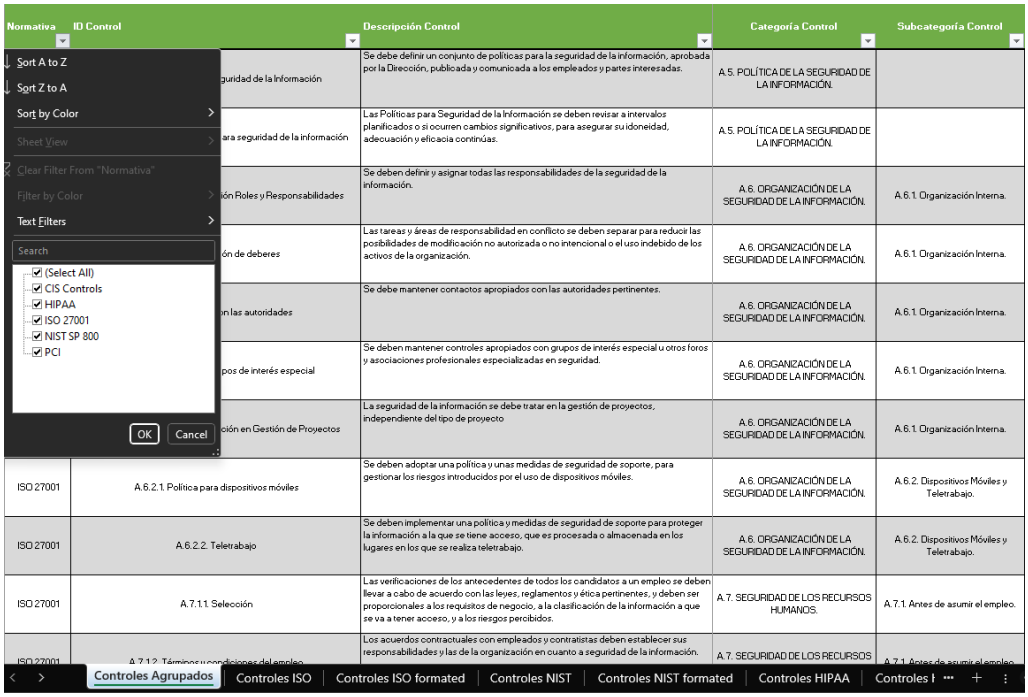


ID Control	Description	Group
1,1 - Establish and Maintain Detailed Enterprise Asset Inventory	Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of	Inventory and Control of Enterprise Assets
1,2 - Address Unauthorized Assets	Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the	Inventory and Control of Enterprise Assets
1,3 - Utilize an Active Discovery Tool	Utilize an active discovery tool to identify assets connected to the enterprise's network. Configure the active discovery tool to execute daily, or more	Inventory and Control of Enterprise Assets
1,4 - Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory	Use DHCP logging on all DHCP servers or Internet Protocol (IP) address management tools to update the enterprise's asset inventory. Review and use logs to update the enterprise's asset inventory weekly, or more frequently.	Inventory and Control of Enterprise Assets
1,5 - Use a Passive Asset Discovery Tool	Use a passive discovery tool to identify assets connected to the enterprise's network. Review and use scans to update the enterprise's asset inventory at least weekly, or more frequently.	Inventory and Control of Enterprise Assets
2,1 - Establish and Maintain a Software Inventory	Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	Inventory and Control of Software Assets
2,2 - Ensure Authorized Software is Currently Supported	Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least	Inventory and Control of Software Assets
2,3 - Address Unauthorized Software	Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more	Inventory and Control of Software Assets
2,4 - Utilize Automated Software Inventory Tools	Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.	Inventory and Control of Software Assets
2,5 - Allowlist Authorized Software	Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.	Inventory and Control of Software Assets

Controles HIPAA | Controles HIPAA formated | Controles PCI | Controles PCI formated | Controles CIS | Controles CIS formated

Ilustración 23. Tabla Controles CIS Formateada. Fuente: Elaboración propia.

Tras formatear y extraer las columnas principales bajo interés de desarrollo de la herramienta, se ha procedido a traducir al español las normativas las cuales estaban en inglés y se ha creado una única tabla en la que se agrupan la totalidad de las normativas:



Normativa	ID Control	Descripción Control	Categoría Control	Subcategoría Control
		Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la Dirección, publicada y comunicada a los empleados y partes interesadas.	A.5. POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN.	
		Las Políticas para Seguridad de la Información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continúas.	A.5. POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN.	
		Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.	A.6.1. Organización Interna.
		Las tareas y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización.	A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.	A.6.1. Organización Interna.
		Se debe mantener contactos apropiados con las autoridades pertinentes.	A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.	A.6.1. Organización Interna.
		Se deben mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.	A.6.1. Organización Interna.
		La seguridad de la información se debe tratar en la gestión de proyectos, independiente del tipo de proyecto	A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.	A.6.1. Organización Interna.
ISO 27001	A.6.2.1. Política para dispositivos móviles	Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.	A.6.2. Dispositivos Móviles y Teletrabajo.
ISO 27001	A.6.2.2. Teletrabajo	Se deben implementar una política y medidas de seguridad de soporte para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.	A.6.2. Dispositivos Móviles y Teletrabajo.
ISO 27001	A.7.1.1. Selección	Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	A.7. SEGURIDAD DE LOS RECURSOS HUMANOS.	A.7.1. Antes de asumir el empleo.
ISO 27001	A.7.1.2. Términos y condiciones del empleo	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información.	A.7. SEGURIDAD DE LOS RECURSOS	A.7.1. Antes de asumir el empleo.

Sort A to Z
Sort Z to A
Sort by Color
Sheet View
Clear Filter From "Normativa"
Filter by Color
Text Filters
Search
(Select All)
CIS Controls
HIPAA
ISO 27001
NIST SP 800
PCI
OK
Cancel

Controles Agrupados | Controles ISO | Controles ISO formated | Controles NIST | Controles NIST formated | Controles HIPAA | Controles H

Ilustración 24. Tabla Agrupación de Controles. Fuente: Elaboración propia.

Como resultado se ha desarrollado una matriz que agrupa la totalidad de controles de las 5 normativas bajo alcance (CIS, HIPAA, ISO 27001, NIST y PCI) detallando los siguientes campos de cada control:

- Identificador ("ID Control").
- Descripción breve del control ("Descripción Control").
- Categorización del área establecida por la normativa, si existe ("Categoría Control").
- Subcategorización del área establecida por la normativa, si existe ("Subcategoría Control").

Fase 2. Mapeo de los controles de las normativas con las áreas en alcance

En base a la matriz resultado del documento anterior *"Resumen Controles Normativas"* y las áreas en alcance identificadas en el apartado "*5.3 Áreas de solución para Pymes"* y establecidas por la entidad ENISA, se ha procedido a mapear cada uno de los controles de las normativas con las áreas y subáreas de solución establecidas por ENISA.

Cabe destacar que, de cara a cumplir con los objetivos de este trabajo de ofrecer una guía para empresas de pequeño y mediano tamaño, no se han seleccionado la totalidad de controles de las normativas. En este caso se ha utilizado un criterio propio de selección de controles en base a la relación de cada control con las áreas de solución propuestas por ENISA, descartando aquellos controles complejos que requieran de un alto coste de personal o recursos.

Como resultado se ha elaborado el documento "Mapping Controles - Áreas ENISA"

Normativa	ID Control	Descripción Control	En alcance	Área ENISA	Subárea ENISA
ISO 27001	A.6.1.4. Contacto con grup	Se deben mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	X	BUSCAR Y COMPARTIR INFORMACIÓN	
NIST SP 800	PM-15	Establecer e institucionalizar el contacto con grupos y asociaciones seleccionadas dentro de las comunidades de seguridad y privacidad: a. Facilitar la seguridad y la capacitación continua de seguridad y privacidad para el personal organizacional; b. Mantener moneda con prácticas de seguridad y privacidad recomendadas, técnicas y tecnologías; y C. Para compartir información actual de seguridad y privacidad, incluidas amenazas, vulnerabilidades e	X	BUSCAR Y COMPARTIR INFORMACIÓN	
PCI	10.4.1	Los sistemas críticos tienen el tiempo correcto y consistente.		PROTEGER LOS DISPOSITIVOS	PROTEGER LOS DISPOSITIVOS
		Revise y pruebe el plan de respuesta a incidentes	X	DESARROLLAR UN PLAN DE RESPUESTA ANTE INCIDENTES	

Controles - Áreas ENISA

Ilustración 25. Tabla Mapping controles - Áreas ENISA. Fuente: Elaboración propia.

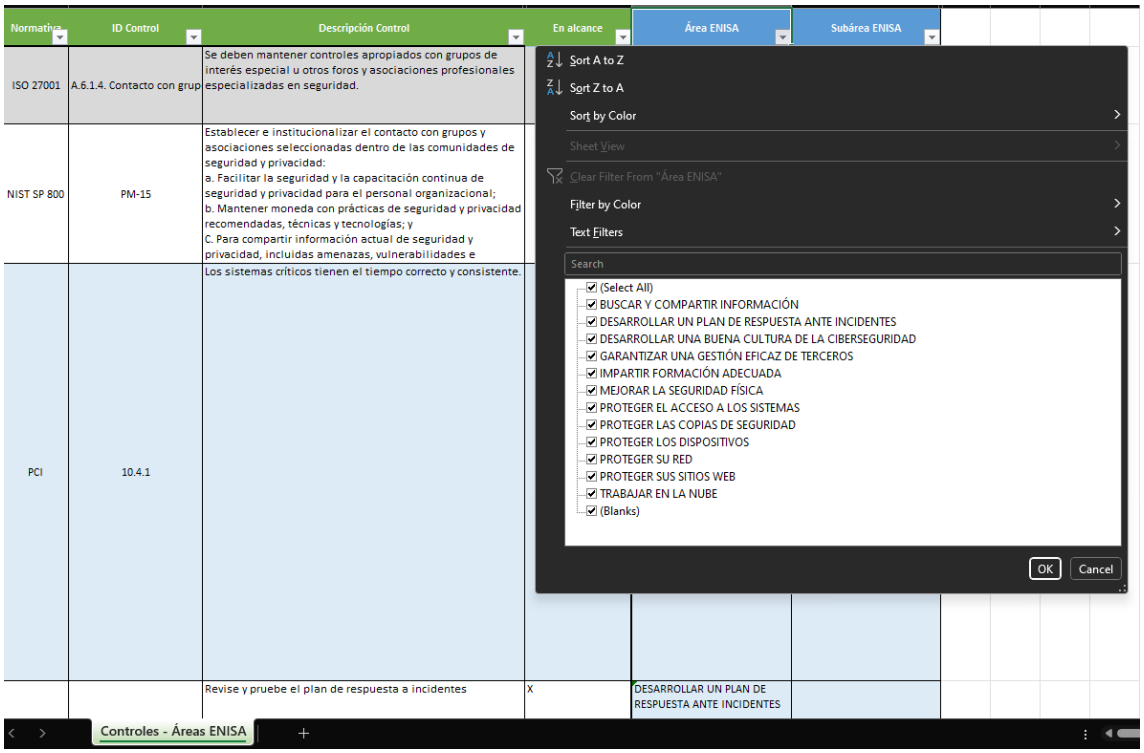


Ilustración 26. Tabla Mapping controles - Áreas ENISA desplegable columna "Área ENISA". Fuente: Elaboración propia.

En las ilustraciones 24 y 25 se puede evidenciar la tabla resultado que cuenta con las siguientes campos:

- Identificador (“ID Control”).
- Descripción breve del control (“Descripción Control”).
- Detalle de si el control ha sido seleccionado o no (“En alcance”).
- Clasificación del control según el área definida ENISA de solución para empresas PYMES (“Área ENISA”).
- Clasificación de los controles según las subáreas definidas por ENISA como solución para empresas PYMES(“Subárea ENISA”).

Fase 3. Mapeo controles con riesgos de ciberseguridad

Partiendo de la tabla resultante del archivo anterior "Mapping Controles - Áreas ENISA", en el que ya se ha realizado una selección de los controles en alcance, se ha procedido a asignar a cada control los riesgos de ciberseguridad que cubre al ser implementado.

Para la definición de los riesgos de ciberseguridad, se ha utilizado la fuente detallada en el apartado *"5.4 Clasificación de riesgos de ciberseguridad"*. Esta clasificación establece ocho áreas principales de riesgos de ciberseguridad que agrupan un total de 81 riesgos específicos.

Para completar esta fase del proyecto, se ha creado una matriz en la que cada fila corresponde a un control en alcance y se han definido 81 columnas, una por cada riesgo de ciberseguridad. De este modo, si un control cubre alguno de los riesgos definidos, se ha marcado con una "X".

La documentación soporte a esta fase ha sido documentada en el fichero "Mapping Controles – Riesgos ENISA".

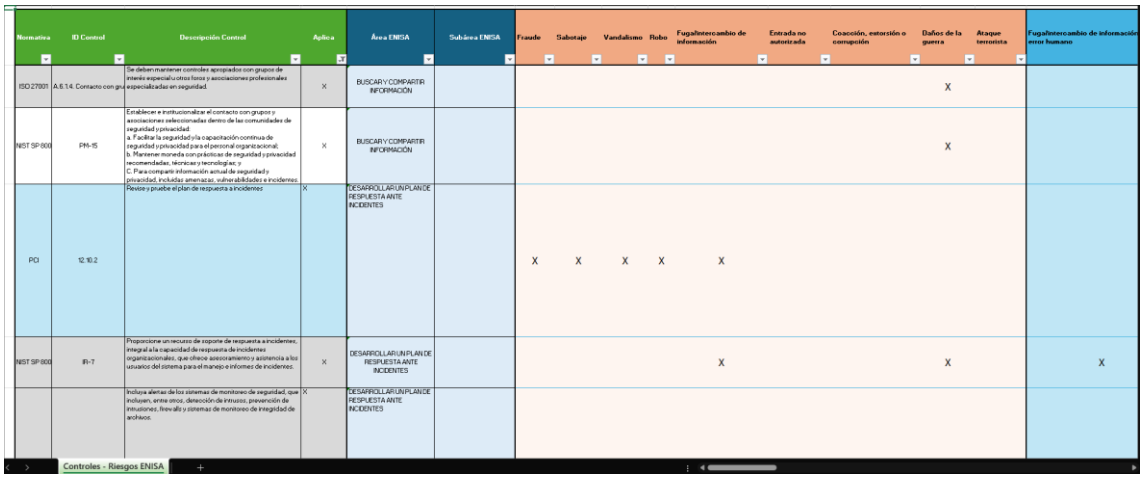
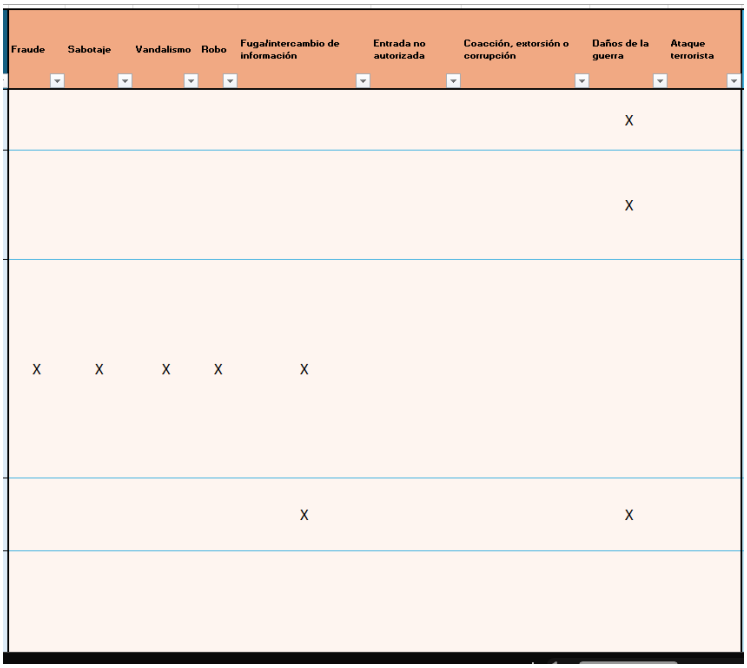


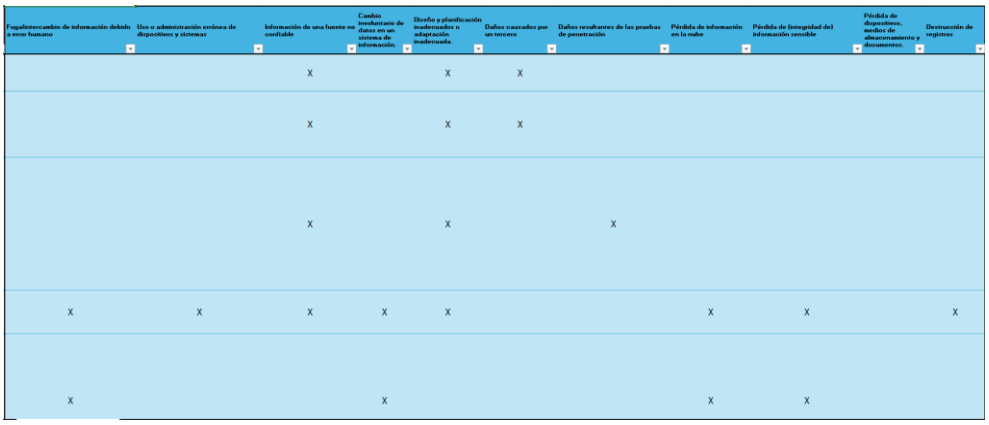
Ilustración 27. Tabla Mapping controles - Riesgos ENISA. Fuente: Elaboración propia.

Cada área de riesgos de ciberseguridad ha sido diferenciada por colores:



Fraude	Sabotaje	Vandalismo	Robo	Fuga/intercambio de información	Entrada no autorizada	Coacción, extorsión o corrupción	Daños de la guerra	Ataque terrorista
							X	
							X	
X	X	X	X	X				
				X			X	

Ilustración 28. Tabla Mapping controles - Riesgos ENISA - Área de ataques intencionales. Fuente: Elaboración propia.



Fuga/intercambio de información debido a error humano	Uso o administración errónea de dispositivos y sistemas	Información de una fuente no confiable	Cambio inoportuno de datos en un sistema de información.	Diseño y planificación inadecuados o adaptación inadecuada.	Daños causados por un tercero	Daños resultantes de las pruebas de penetración	Pérdida de información en la nube	Pérdida de (integridad de) información sensible	Pérdida de dispositivos, medios de almacenamiento y documentos.	Destrucción de registros
		X		X	X					
		X		X	X					
		X		X		X				
X	X	X	X	X			X	X		X
X			X				X	X		

Ilustración 29. Tabla Mapping controles - Riesgos ENISA - Área de daños involuntarios. Fuente: Elaboración propia.

Desastres	Fuego	Contaminación, polvo, corrosión	Golpe de trueno	Agua	Explosión	Fuga de radiación peligrosa	Condiciones climáticas desfavorables	Grandes acontecimientos en el medio ambiente	Amenazas desde el espacio / Tormenta electromagnética	Fauna silvestre

Ilustración 30. Tabla Mapping controles - Riesgos ENISA - Área de desastres. Fuente: Elaboración propia.

Fallo de dispositivos o sistemas	Fallo o interrupción de los enlaces de comunicación (redes de comunicación)	Fallo o interrupción del suministro principal	Fallo o interrupción de los proveedores de servicios (cadena de suministro)	Mal funcionamiento de los equipos (dispositivos o sistemas)
		X		X
X	X	X	X	X

Ilustración 31. Tabla Mapping controles - Riesgos ENISA - Área de fallos/Mal funcionamiento. Fuente: Elaboración propia.

Pérdida de recursos	Ausencia de personal	Huelga	Pérdida de servicios de soporte	Corte de internet	Caída de la red
X		X	X		
X		X	X		
			X	X	X

Ilustración 32. Tabla Mapping controles - Riesgos ENISA - Área de disponibilidad de recursos. Fuente: Elaboración propia.

Conducción de guerra	Interceptar emisiones comprometedoras	Intercepción de información	Radiación interferencial	Repetición de mensajes	Reconocimiento de red, manipulación del tráfico de red y recopilación de información.	Hombre en el medio/secuestro de sesión
X						
X						
	X	X		X	X	X

Ilustración 33. Tabla Mapping controles - Riesgos ENISA - Área de intercepciones. Fuente: Elaboración propia.

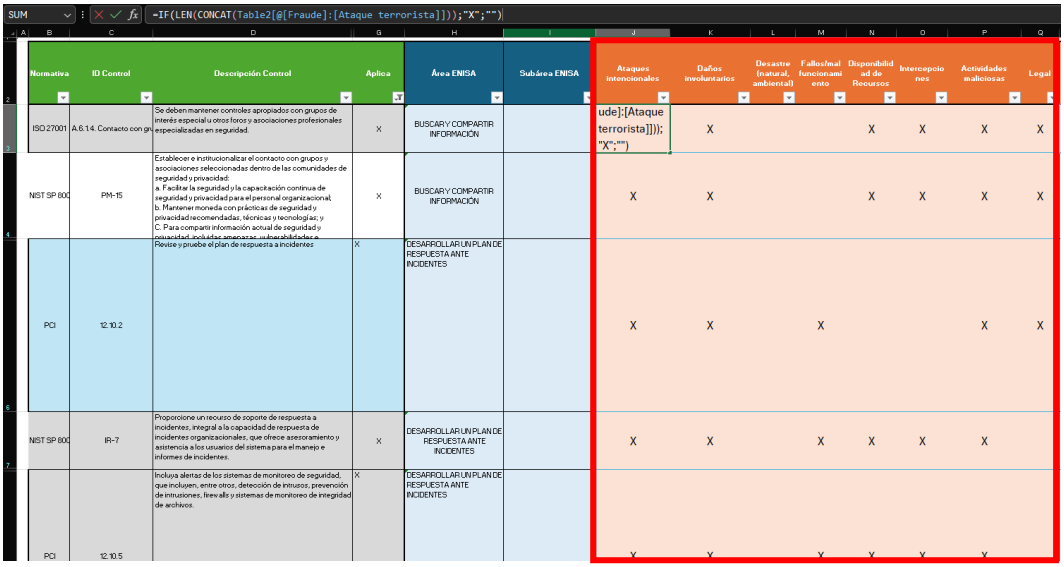
Robo de identidad (fraude de identidad/cuenta)	Recibir correo electrónico no solicitado	Negación de servicio	Código/software/actividad malicioso	Ingeniería social	Abuso de filtración de información	Generación y uso de certificados falsos	Manipulación de hardware y software	Manipulación de información	Mal uso de las herramientas de auditoría	Uso indebido de información/sistemas de información (incluidas aplicaciones móviles)
					X					X
					X					X
									X	X
	X	X	X	X	X					X
X	X	X	X		X	X	X	X		

Ilustración 34. Tabla Mapping controles - Riesgos ENISA - Parte del Área de actividades maliciosas. Fuente: Elaboración propia.

Violación de leyes o reglamentos / Incumplimiento de la legislación	Incumplimiento de los requisitos contractuales	Uso no autorizado de recursos protegidos por derechos de propiedad inteleotual	Abuso de datos personales
X			
X			
X	X		

Ilustración 35. Tabla Mapping controles - Riesgos ENISA - Área legal. Fuente: Elaboración propia.

Cabe destacar que en esta misma tabla se puede observar la aplicabilidad de cada control sobre las ocho áreas principales de riesgos. Esto se logró implementando una fórmula que detectaba si alguno de los riesgos correspondientes al área tenía asignada una “X”, indicando que el control cubre ese riesgo. De este modo, se marca con una “X” el área de riesgo en cuestión.



Normativa	ID Control	Descripción Control	Aplica	Área ENISA	Subárea ENISA	Ataques intencionales	Daños involuntarios	Desastre (natural, ambiental)	Fallos/mal funcionamiento	Disponibilidad de Recursos	Intercepciones	Actividades maliciosas	Legal
ISO 27001	A.6.1.4. Contacto con gr	Se deben mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	X	BUSCAR Y COMPARTIR INFORMACIÓN		ude]:[Ataque terrorista]])); "X";"")	X			X	X	X	X
NIST SP 800	PM-15	Establecer e institucionalizar el contacto con grupos y asociaciones seleccionadas dentro de las comunidades de seguridad y privacidad: a. Facilitar la seguridad y la capacitación continua de seguridad y privacidad para el personal organizacional; b. Mantener moneda con prácticas de seguridad y privacidad recomendadas, técnicas y tecnologías; y C. Para compartir información actual de seguridad y	X	BUSCAR Y COMPARTIR INFORMACIÓN		X	X			X	X	X	X
PCI	12.10.2	Revise y pruebe el plan de respuesta a incidentes	X	DESARROLLAR UN PLAN DE RESPUESTA ANTE INCIDENTES		X	X		X			X	X
NIST SP 800	IR-7	Proporcione un recurso de soporte de respuesta a incidentes, integral a la capacidad de respuesta de incidentes organizacionales, que ofrece asesoramiento y asistencia a los usuarios del sistema para el manejo e informes de incidentes.	X	DESARROLLAR UN PLAN DE RESPUESTA ANTE INCIDENTES		X	X		X	X	X	X	
PCI	12.10.5	Incluya alertas de los sistemas de monitoreo de seguridad, que incluyen, entre otros, detección de intrusos, prevención de intrusiones, firewalls y sistemas de monitoreo de integridad de archivos.	X	DESARROLLAR UN PLAN DE RESPUESTA ANTE INCIDENTES		X	X		X	X	X	X	

Ilustración 36. Tabla mapping controles - áreas principales riesgos ciberseguridad. Fuente: Elaboración propia.

Definición de la fórmula:

=IF(LEN(CONCAT(*“Columnas de riesgos que cubre el área”*));"X";"")

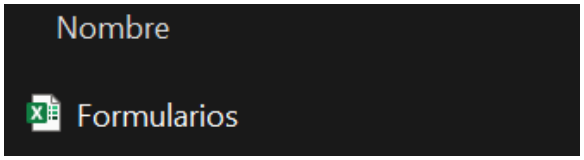
Como resultado de esta fase se ha logrado mapear los controles de cada una de las normativas en alcance, con las áreas descritas por ENISA como soluciones para PYMES y los riesgos que cubre cada control.

Fase 4. Formularios

Una vez identificados los controles en alcance, se ha procedido a desarrollar una herramienta para las empresas. Para facilitar su uso, se optó por crear un formulario en Excel, dado que esta es una herramienta ampliamente utilizada y familiar para muchas organizaciones. Así, se diseñó un Excel con diferentes preguntas, simulando una encuesta.

Se han creado doce formularios, uno para cada área de solución para Pymes establecidas por ENISA (detalladas en el apartado "5.3 Áreas de solución para Pymes"). Las preguntas de cada formulario se formularon en base a la clasificación de controles desarrollada en fases anteriores. Las respuestas a estas preguntas se restringieron a tres opciones: Sí, No y N/A, para facilitar un análisis posterior. Adicionalmente se ha añadido una columna de observaciones que permite a los usuarios hacer un seguimiento detallado del cumplimiento de cada control.

La definición de las preguntas se ha desarrollado en el documento "Formularios".



1. DESARROLLO DE LA CULTURA DE CIBERSEGURIDAD

Se ha de designar a un responsable dentro de la empresa para gestionar eficazmente los recursos destinados a la seguridad de la información TI, como tiempo del personal, compra de software y hardware, formación y desarrollo de políticas efectivas. Además, se enfatiza la importancia de aumentar la participación y concienciación de los empleados mediante una comunicación clara, formación adecuada y el establecimiento de normas específicas en las políticas de ciberseguridad.

Responsabilidades de la gestión de activos empresariales	**Si - No - N/A**	**Observaciones**
Controles NIST SP 800: AC-2, PS-9, PM-2 · Controles ISO 27001: A.6.1.2 · Controles CIS: 17.5 · Controles HIPAA · Controles PCI		
Se han desarrollado y documentado políticas y procedimientos relacionados con la gestión de los roles/permisos en los sistemas informáticos en los que se generan registros para su posterior trazabilidad. Ejemplo (procedimientos de modificación, asignación o revocación de roles/permisos)		
Se han establecido roles y responsabilidades de seguridad y privacidad en base a los puestos laborales.		
Las tareas y áreas de responsabilidad en conflicto se separan para reducir las posibilidades de modificación no autorizada o el uso indebido de los activos de la organización.		
Se ha designado un responsable oficial de la seguridad de la información encargado de coordinar, desarrollar, implementar y mantener la seguridad de la información en toda la organización.		
Se han asignado roles y responsabilidades clave para la respuesta a los incidentes de seguridad informática.		
Se ha establecido un proceso de gestión de roles/permisos críticos, en los que se existe una aprobación por parte de un responsable competente.		
Se realiza una revisión anual para comprobar que los roles/permisos asignados a cada usuario en el sistema informático siguen alineados con las funciones desarrolladas.		

Implicaciones de los empleados	**Si - No - N/A**	**Observaciones**
Controles NIST SP 800: PL-4 · Controles ISO 27001: A.7.2.1 · Controles CIS · Controles HIPAA · Controles PCI: 12.6.2, 12.5.2		
Se proporciona a las personas que requieren acceso al sistema, las reglas que describen sus responsabilidades y el comportamiento esperado para la información y el uso del sistema, la seguridad y la privacidad.		
La dirección exige a todos los empleados, la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización.		
Se generan registros, al menos anualmente, en los que el personal reconoce que han leído y entendido las política y los procedimientos de seguridad establecidos.		
Ante la detección de alertas o intentos de ataques a la seguridad informática, se distribuye y notifica al personal correspondiente.		
Se revisan y actualizan las reglas de responsabilidades y comportamientos de los empleados.		

Auditorías de seguridad	**Si - No - N/A**	**Observaciones**
Controles NIST SP 800: Au-4 · Controles ISO 27001 · Controles CIS: 8.2, 8.11, 16.6 · Controles HIPAA · Controles PCI: 10.1,10.2.2,10.2.4, 10.2.5, 10.2.6, 10.5.1, 10.5.2, 10.7, 11.3.2, 11.2.1 11.3.1,11.3.3, 12.2		
Se ha configurado el registro de auditoría para los activo empresariales.		
Se implementan pistas de auditoría para vincular todo el acceso a los componentes del sistema a cada usuario individual.		
Se generan registros de las acciones tomadas por cualquier individuo con privilegios de raíz o administrativa.		
Se generan registros de intentos de acceso lógico no válidos.		
Se generan registros del uso/cambios en los mecanismos de identificación y autenticación, incluidos, entre otros, la creación de nuevas cuentas y la elevación de privilegios, y todos los cambios, adiciones o deleciones a cuentas con privilegios raíz o administrativo.		
Se generan registros de inicialización, parada o pausa de los registros de auditoría.		
Los registros de auditoría contiene información sobre qué tipo de evento ocurrió.		
Los registros de auditoría contiene información sobre cuando ocurrió el evento.		
Los registros de auditoría contiene información sobre donde ocurrió el evento.		
Los registros de auditoría contiene información sobre la fuente del evento.		
Los registros de auditoría contiene información sobre el resultado del evento.		
Los registros de auditoría contiene información sobre la identidad de cualquier individuo, sujeto u objetos/entidades asociadas con el evento.		
Se realizan revisiones de registros de auditoría para detectar anomalías o eventos anormales que podrían indicar una amenaza potencial.		
Se ha limitado la visualización de los registros de auditoría al personal que lo precisa.		
Los registros de auditoría se encuentran protegidos de modificaciones no autorizadas.		
Se conservan los registros de auditoría en los activos empresariales durante un mínimo de un año.		
Se realizan pruebas de penetración internas al menos anualmente o después de cualquier cambio en la infraestructura significativo, actualización o modificación de las aplicaciones.		
Se realizan escaneos de vulnerabilidad internos trimestrales en los que se abordan las vulnerabilidades y realizan rescans para verificar todas las vulnerabilidades de "alto riesgo" se resuelven.		
Se realizan pruebas de penetración externa al menos anualmente y después de cualquier cambio en la infraestructura significativo, actualización o modificación de las aplicaciones.		
Se ha establecido un sistema de calificación de gravedad de amenazas que facilita la priorización del orden en que se fijan las vulnerabilidades descubiertas.		
Las vulnerabilidades explotables encontradas durante las pruebas de penetración internas y externas se corrigen y las pruebas se repiten para verificar las correcciones.		
Existe un proceso de evaluación de riesgos que se realiza al menos anualmente y en cambios significativos empresariales, en el que se identifica activos críticos, amenazas y vulnerabilidades, y se concluye con un análisis formal y documentado del riesgo.		

Publicación de las políticas de ciberseguridad					Si - No - N/A	Observaciones
Controles NIST SP 800	Controles ISO 27001	Controles CIS	Controles HIPAA	Controles PCI		
CM-1, IA-1	A.5.1.1, A12.1.1, A.8.3.1, A.12.5.1, A.5.1.2, A.7.2.3		164.310 (a) (1), 164.312 (c) (1), 164.310 (d) (1), 164.310 (d) (2) (iii), 164.308 (a) (7) (ii) (a), 164.308 (a) (5) (ii) (d), 164.308 (a) (7) (ii) (b), 164.308 (a) (1) (ii) (c)	12.5.1, 9.2, 2.5, 16.1		
Se han establecido y documentado procedimientos de seguridad.						
Los políticas y procedimientos establecidos han sido aprobados por la dirección previo a su implantación.						
Las implantación de nuevos procedimientos o políticas son comunicados a todos las partes interesadas.						
Los procedimientos operativos documentado están a la disposición de todos los usuarios que los necesitan.						
Existen políticas y procedimientos para limitar el acceso físico a sus sistemas de información electrónica y las instalaciones en las que se encuentran, al tiempo que se asegura que se permita el acceso adecuadamente autorizado.						
Existe un procedimiento para distinguir fácilmente entre el personal interno y los visitantes.						
Existe una política de gestión de configuración a nivel de sistema.						
Existen políticas de seguridad y procedimientos operativos para administrar los valores predeterminados de los proveedores y otros parámetros de seguridad.						
Existe una política de identificación y autenticación a nivel del sistema						
Existen políticas y procedimientos para proteger la información de la alteración o destrucción inadecuada.						
Existen políticas y procedimientos que rigen el recibo y la eliminación de hardware y medios electrónicos que contienen información.						
Existen procedimientos para la eliminación de la información de los medios electrónicos antes de que los medios estén disponibles para su reutilización.						
Existe un procedimiento seguro de desarrollo de aplicaciones.						
Existe un procedimiento para crear y mantener copias exactas recuperables de la información.						
Existe un procedimiento para crear, cambiar y salvaguardar contraseñas.						
Existen procedimientos para restaurar la pérdida de datos.						
Existen procedimientos para la gestión de medios de soporte removibles.						
Existen procedimientos para controlar la instalación de software en sistemas operativos.						
Las políticas y procedimientos de seguridad de la información se revisan a intervalos planificados o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continúas.						
Se aplican las sanciones apropiadas contra los miembros de la fuerza laboral que no cumplen con las políticas y procedimientos de seguridad de la entidad cubierta.						
Existe un proceso formal y comunicado para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.						

Medidas para la protección de datos					Si - No - N/A	Observaciones
Controles NIST SP 800	Controles ISO 27001	Controles CIS	Controles HIPAA	Controles PCI		
MP-8	14.1.3, A.11.2.7	3.2, 3.13, 3.7, 3.12, 3.4, 3.5, 4.11	164.312 (c) (2)	4.1.1, 3.1		
Existe un inventario de datos sensibles, basado en el proceso de gestión de datos de la compañía, el cual se revisa y actualiza anualmente, como mínimo, con una prioridad sobre los datos confidenciales.						
Se utilizan herramientas automatizada de prevención de pérdidas de datos basada en host (DLP) para identificar todos los datos confidenciales almacenados, procesados o transmitidos a través de activos empresariales.						
Existe y se mantiene un esquema general de clasificación de datos para la empresa utilizando etiquetas, como "sensibles", "confidenciales" y "públicas", y clasificar sus datos de acuerdo con esas etiquetas.						
En el caso de que exista un esquema general de clasificación, este se revisa y actualiza anualmente, o cuando ocurran cambios empresariales significativos que podrían afectar esta protección.						
Se cuentan con mecanismos electrónicos para corroborar que la información protegida no es alterada ni destruida de manera no autorizada.						
Se ha asegurado de que la información involucrada en las transacciones de servicios de aplicaciones están protegidas para prevenir la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensaje, la divulgación no autorizada y la duplicación o reproducción de mensajes no autorizados.						
Las redes inalámbricas que transmiten datos críticos usan las mejores prácticas de la industria para implementar un cifrado sólido para la autenticación y la transmisión.						
Se procesan y almacenan los datos según la sensibilidad de los datos. Los datos confidenciales no son procesados o almacenados en los activos empresariales destinados a datos de menor sensibilidad.						
Los datos se retienen de acuerdo con el proceso de gestión de datos de la empresa estableciendo plazos mínimos y máximos.						
Existe un proceso trimestral para identificar y eliminar de forma segura los datos almacenado que excede la retención definida.						
Al borrar datos se han establecido procesos de eliminación acorde con la sensibilidad de los datos.						
Se han establecido procedimientos para el borrado de forma remota de los datos empresariales de dispositivos de usuario final portátil de propiedad de la empresa cuando se considere apropiados, como dispositivos perdidos o robados, o cuando un individuo ya no admite la empresa.						
Se verifican los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software con licencia haya sido retirado o sobre escrito en forma segura antes de su disposición o reúso.						
Existe un proceso de degradación de medios del sistema definido por la organización que incluye mecanismos de degradación acorde con la categoría de seguridad o la clasificación de la información.						

Ilustración 37. Formulario Desarrollo de la cultura de ciberseguridad. Fuente: Elaboración propia.

2. IMPARTIR UNA FORMACIÓN ADECUADA						
Es crítico que las empresas proporcionen formación regular en ciberseguridad para todos los empleados, con un enfoque adaptado a las necesidades específicas de las pymes y centrado en situaciones prácticas. Además, se ha de ofrecer formación especializada a los responsables de la gestión de la ciberseguridad, garantizando que estén equipados con los conocimientos y habilidades necesarios para proteger eficazmente la empresa contra las amenazas cibernéticas.						
Controles NIST SP 800	Controles ISO 27001	Controles CIS	Controles HIPAA	Controles PCI	Si - No - N/A	Observaciones
AT-1, AT-4, AT-6		14.9, 16.9, 14.3, 14.3, 14.4, 14.5, 14.6, 14.7, 14.8	164.308 (a) (5) (i)	12.6.1, 9.9.3		
Se ha establecido una política de conciencia y capacitación de los empleados la cual se revisa y actualiza periódicamente.						
Existe un programa de concienciación de seguridad y capacitación para todos los miembros de la fuerza laboral (incluida la gerencia).						
Se documentan y monitorizan las actividades de seguridad y capacitación de privacidad de la información.						
La concienciación de seguridad y capacitación de habilidades ofertadas se encuentra alineados con los roles específicos de cada empleado/departamento.						
El personal de desarrollo de software recibe capacitación para la escritura de código seguro para su entorno y responsabilidades de desarrollo específico.						
Se educa al personal al contratarlo y al menos anualmente.						
Se proporciona formación al personal que ha de tener en cuenta el intento de manipulación o reemplazo de dispositivo. Tratando tópicos cómo: la verificación de la identidad de cualquier persona tercera que afirme ser personal de reparación o mantenimiento; la instalación, reemplazo o retirada de dispositivos sin verificación; detección de comportamiento sospechoso en torno a los dispositivos; y reporte sobre el comportamiento sospechoso e indicaciones de manipulación o sustitución del dispositivo al personal apropiado .						
Se proporciona formación al personal para reconocer los ataques de ingeniería social, como el phishing.						
Se proporciona formación al persona sobre las mejores prácticas de autenticación.						
Se proporciona formación al personal sobre cómo identificar y almacenar, transferir, archivar y destruir datos confidenciales.						
Se proporciona formación al persona para que conozcan las causas de la exposición no intencional de los datos						
Se proporciona formación al persona para que puedan reconocer un incidente potencial y poder informar dicho incidente.						
Se proporciona formación al personal sobre cómo notificar al personal de TI sobre cualquier fallas en procesos y herramientas automatizados.						
Se proporciona formación al personal sobre los peligros de conectarse y transmitir datos sobre redes inseguras para actividades empresariales. Si la compañía cuenta con trabajadores remotos, la capacitación incluye orientación para garantizar que todos los usuarios configuren de forma segura su infraestructura de red doméstica.						
Se proporcionan comentarios sobre los resultados de la capacitación organizacional a un responsable designado.						

Ilustración 38. Formulario formación. Fuente: Elaboración propia.

3. GESTIÓN EFICAZ DE TERCEROS						
Asegurar una gestión activa de todos los proveedores, especialmente aquellos con acceso a datos sensibles o sistemas críticos. Se deben establecer acuerdos detallados que especifiquen los requisitos de seguridad y garanticen el cumplimiento por parte de los proveedores, lo que asegurará la protección adecuada de la información empresarial.						
Controles NIST SP 800	Controles ISO 27001	Controles CIS	Controles HIPAA	Controles PCI	Si - No - N/A	Observaciones
PS-7	A.15.1.2, A.15.1.3	15.1, 15.3, 5.5, 6.4, 8.12, 15.7		12.9, 12.8.4, 8.1.5		
Existe un inventario de proveedores de servicios en el que se enumera a todos los proveedores de servicios y el contacto empresarial vinculado.						
En el caso de que exista un inventario de proveedores, este se evalúa al menos mensualmente para identificar cualquier cambio o actualización.						
Se clasifican los proveedores de servicios. La consideración de clasificación puede incluir una o más características, como la sensibilidad de los datos, el volumen de datos, los requisitos de disponibilidad, las regulaciones aplicables, el riesgo inherente y el riesgo mitigado.						
Si existe una clasificación de proveedores esta se actualiza y revisa anualmente, o cuando ocurran cambios empresariales significativos que podrían afectar esta salvaguarda.						
Existe un acuerdo por escrito con los proveedores en los que se incluye un reconocimiento de que los proveedores de servicios son responsables de la seguridad de los datos que tratan.						
En los acuerdos con proveedores se incluyen requisitos de seguridad de la información pertinentes con cada proveedor que pueda acceder, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.						
En los acuerdos con proveedores se incluyen requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.						
Se monitorear el estado de cumplimiento de los requerimientos de seguridad de los proveedores de servicios al menos anualmente.						
Existe un inventario de cuentas de servicio.						
En el caso de existir un inventario de cuentas de servicio, se realizan revisiones de las cuenta de servicio para validar que todas las cuentas activas están autorizadas con una periodicidad mínima trimestral.						
Se habilitan las cuentas de servicio solo durante el período de tiempo necesario y se deshabilitan cuando no están en uso.						
Se monitorean las cuenta de servicios cuando están en uso.						
Se establecen requisitos de seguridad de personal, incluidos roles de seguridad y responsabilidades para cuentas utilizadas por proveedores externos.						
Se exige una autentificación multifactor ("MFA") para el acceso a la red remota por parte de los proveedores.						
Existen registros de proveedores de servicios, relacionados con eventos de autenticación y autorización, eventos de creación y eliminación de datos y eventos de gestión de usuarios...						
Al dar de baja un proveedor se tiene en cuenta la desactivación de las cuentas de usuario y de servicio, terminación de flujos de datos y eliminación segura de datos empresariales dentro de los sistemas de proveedores de servicios.						

Ilustración 39. Formulario gestión de terceros. Fuente: Elaboración propia.

4. DESARROLLO DE UN PLAN DE RESPUESTA ANTE INCIDENTES		
Elaborar un plan de respuesta ante incidentes que contemple directrices claras, roles definidos y responsabilidades documentadas para asegurar una respuesta oportuna y profesional a cualquier incidente de seguridad. Se recomienda la implementación de herramientas que permitan monitorear y generar alertas ante actividades sospechosas o fallos de seguridad facilitará una respuesta rápida y eficaz ante posibles amenazas.		
Controles NIST SP 800 Controles ISO 27001 Controles CIS Controles HIPAA Controles PCI IR-8, IR-7 17.9, 7.2, 17.6,17.1, 17.7, 17.2, 17.8 164.308 (a) (6) (i) 12.10.2, 12.10.5, 12.10.3, 12.5.3, 12.10.6	**Si - No - N/A**	**Observaciones**
Se han implantado políticas y/o procedimientos para abordar los incidentes de seguridad.		
Se ha desarrollado un plan de respuesta ante incidentes en el que se detalla la estrategia y recursos disponibles.		
Se revisa y prueba el plan de respuesta ante incidentes, al menos anualmente.		
Existencia de alertas creadas para la detección de intrusos, prevención de intrusiones, incidentes en firewalls, anomalías en los sistemas de monitoreo de integridad de archivos…		
Existen umbrales de incidentes de seguridad, incluido, como mínimo, diferenciando entre un incidente y un evento. Los ejemplos pueden incluir: actividad anormal, vulnerabilidad de seguridad, debilidad de seguridad, violación de datos, incidentes de privacidad, etc.		
Se revisa anualmente los umbrales de incidentes de seguridad, o cuando ocurren cambios empresariales significativos que podrían afectar.		
Se han habilitado recursos de soporte de respuesta a incidentes, que ofrecen asesoramiento y asistencia a los usuarios del sistema para el manejo e informes de incidentes.		
Se ha establecido una estrategia de remediación de incidentes basada en el análisis de los riesgos de seguridad de la compañía.		
Se han establecido mecanismos primarios y secundarios utilizados para comunicarse e informar durante un incidente de seguridad. Los mecanismos pueden incluir llamadas telefónicas, correos electrónicos o cartas.		
La compañía cuenta como mínimo con una persona clave, que administra el proceso de manejo de incidentes de la empresa. El personal de gestión en cuestión, es el responsable de la coordinación y documentación de los esfuerzos de respuesta y recuperación de incidentes.		
Existe personal específico encargado de dar soporte a las alertas identificadas disponible las 24 horas del día, los 7 días de la semana.		
Se planifican y realizan ejercicios y escenarios de respuesta a incidentes de rutina para el personal clave involucrado en el proceso de respuesta.		
Existe un inventario de contacto para todas las partes que necesitan estar informadas de los incidentes de seguridad. Los contactos pueden incluir personal interno, proveedores de terceros, proveedores de seguros cibernéticos, agencias gubernamentales relevantes…		
Anualmente se revisa el listado de contactos de comunicación de incidentes para garantizar que la información esté actualizada.		
Todo incidentes se documenta y distribuye la respuesta y los procedimientos de escalada para garantizar el manejo oportuno y efectivo de todas las situaciones.		
Se realizan revisiones posteriores al incidente.		
Existe un proceso para modificar y evolucionar el plan de respuesta de incidentes de acuerdo con las lecciones aprendidas e incorporaciones de desarrollos de la industria.		

Ilustración 40. Formulario desarrollo de un plan de respuesta ante incidentes. Fuente: Elaboración propia.

5. PROTECCIÓN DEL ACCESO A LOS SISTEMAS

Fomentar el uso de frases de contraseña, que consisten en una combinación de al menos tres palabras aleatorias para formar una frase fácil de recordar y segura. En caso de optar por una contraseña convencional, es importante asegurarse de que sea larga y contenga una variedad de caracteres, incluyendo mayúsculas, minúsculas, números y caracteres especiales, evitando términos obvios o secuencias predecibles. Además, se aconseja no utilizar información personal accesible en Internet y evitar compartir contraseñas con otros usuarios. Es fundamental activar la autenticación de doble factor y considerar el uso de un gestor de contraseñas dedicado para una gestión segura y eficiente de las credenciales.

Controles NIST SP 800	Controles ISO 27001	Controles CIS	Controles HIPAA	Controles PCI
IA-5, AC-8	A.9.1.1, A.7.3.1, A.9.2.5, A.9.2.3, A.9.4.3	5.1, 6.6, 5.6, 6.7, 6.1, 6.8, 6.2, 5.2, 6.5, 4.7, 7.3		8.4, 12.5.4, 7.1.3, 7.2.2, 8.1.1, 8.5, 8.1.3, 8.1.4, 7.1.4, 8.2.4, 8.2.3, 8.2.5, 8.1.6, 8.1.7, 2.2.4, 2.2.5

	Sí - No - N/A	Observaciones
Se ha establecido, documentado y revisado una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.		
Se han documentado y comunicado políticas y procedimientos de autenticación a todos los usuarios relacionados con la orientación sobre la selección de credenciales de autenticación fuertes, orientación sobre la protección de credenciales de autenticación, instrucciones para cambiar las contraseñas si hay alguna sospecha de que la contraseña pueda verse comprometida...		
Existe un inventario de todas las cuentas administradas en la empresa en el que se registra como mínimo, el nombre de la persona, el nombre de usuario, las fechas de inicio/parada y el departamento.		
Se valida como mínimo de forma trimestral que todas las cuentas activas del inventario de cuentas están autorizadas.		
Existe un inventario de los sistemas de autenticación y autorización de la empresa, incluidos los alojados en el sitio o en un proveedor de servicios remotos.		
Se valida como mínimo de forma anual el inventario de sistemas de autenticación y autorización de la empresa.		
Se centraliza la gestión de cuentas a través de un directorio o servicio de identidad.		
Se centraliza el control de acceso para todos los activos empresariales a través de un servicio de directorio o proveedor de SSO, donde sea compatible.		
Se administran las cuentas de usuario, incluidas adiciones, deleciones y modificaciones.		
Existe un proceso para otorgar acceso a activos empresariales sobre nuevas contrataciones, subvención de derechos o cambio de roles de un usuario.		
Se ha definido un control de acceso basado en roles, mediante la determinación y documentación de los derechos de acceso necesarios para cada papel dentro de la empresa para llevar a cabo con éxito sus deberes asignados.		
Se asigna el acceso de un usuario a los distintos activos de la compañía en base a la clasificación y función de trabajo del personal individual.		
Se asigna los privilegios de los usuarios en base a la clasificación y función de trabajo.		
Se asigna a todos los usuarios una identificación(ID) única antes de permitirles acceder a los componentes del sistema.		
Las ID de usuario genéricas están deshabilitadas o eliminadas.		
Se han establecido procedimientos administrativos para la distribución inicial del autenticador, para autenticadores perdidos o comprometidos o dañados.		
Se solicita cambiar los autenticadores predeterminados antes del primer uso.		
Existe un proceso para revocar el acceso a los activos empresariales, a través de la deshabilitación de las cuentas inmediatamente después de la terminación, la revocación de los derechos o el cambio de roles de un usuario.		
Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se definen, comunican al empleado o contratista y se hacen cumplir.		
Se revoca inmediatamente el acceso para cualquier usuario dado de baja en la compañía.		
Se eliminan/deshabilitan las cuentas de usuario inactivas dentro de los 90 días.		
Los responsable de los activos revisan los derechos de acceso de los usuarios en intervalos regulares.		
Se restringe y controla la asignación y uso de derechos de acceso privilegiado.		
Se establece el principio de asignación de permisos al mínimo privilegio, asignando los autorización mínimos de los usuarios en base a las labores desempeñadas.		
En caso de existir la necesidad de asignación de algún permisos adicional al establecido, este requiere la aprobación documentada por parte de las partes autorizadas que especifiquen los privilegios requeridos.		
Se trata de garantizar que los sistemas de contraseñas deben sen interactivos y aseguran contraseñas de calidad.		
Relacionado con la configuración de las contraseñas se establece que las contraseñas de usuario deben ser cambiadas al menos una vez cada 90 días.		
Relacionado con la configuración de las contraseñas se establece que un individuo no puede cambiar su contraseña a una que sea la misma que cualquiera de las últimas cuatro contraseñas que ha utilizado.		
Relacionado con la configuración de las contraseñas se establece que estas deben contener caracteres numéricos y alfabéticos.		
Relacionado con la configuración de las contraseñas se establece que las contraseñas de usuario con doble factor de autentificación(MFA) deben contener como mínimo 8 caracteres.		
Relacionado con la configuración de las contraseñas se establece que las contraseñas de usuario sin doble factor de autentificación(MFA) deben contener como mínimo 14 caracteres.		
Se exige a todas la cuentas con permisos privilegiados que utilicen métodos de doble factor de autentificación(MFA).		
Se ha limitado los intentos de acceso repetidos a no más de seis intentos, bloqueando los ID de usuario.		
Se ha establecido una duración del bloqueo de usuario por accesos erróneos repetidos en un mínimo de 30 minutos o hasta que un administrador permita la ID de usuario.		
Se administran las cuentas predeterminadas en activos y software empresarial, como root, administrador y otras cuentas de proveedores preconfiguradas.		
Se han configurado los parámetros de seguridad del sistema para evitar el mal uso.		
Se ha eliminado toda la funcionalidad innecesaria, como scripts, controladores, características, subsistemas, sistemas de archivos y servidores web innecesarios.		
Se realizan las actualizaciones del sistema operativo sobre los activos empresariales a través de la administración de parches automatizado de una base mensual o más frecuente.		

Ilustración 41. Formulario protección del acceso a los sistemas. Fuente: Elaboración propia.

6. PROTECCIÓN DE LOS DISPOSITIVOS

Dentro de un programa de ciberseguridad se debe mantener protegidos todos los dispositivos utilizados por el personal, incluyendo computadoras de escritorio, portátiles, tabletas y teléfonos móviles. Para ello, se recomienda mantener el software actualizado periódicamente, utilizando una plataforma centralizada para gestionar los parches y activando las actualizaciones automáticas siempre que sea posible. Además, es crítico implementar una solución de antivirus en todos los dispositivos y evitar la instalación de software pirata para prevenir la presencia de programas maliciosos. Asimismo, se deben utilizar herramientas de protección de la web y del correo electrónico para bloquear correos no deseados y potencialmente peligrosos. Es crucial cifrar los datos almacenados en dispositivos móviles y durante su transmisión a través de redes públicas, utilizando tecnologías como VPN o SSL/TLS. Por último, se recomienda el uso de un gestor de dispositivos móviles (MDM) para controlar y proteger los dispositivos utilizados por el personal, garantizando la actualización del software, la implementación de medidas de seguridad y la posibilidad de borrar datos de manera remota en caso de pérdida o robo del dispositivo.

Mantenimiento del software	**Si - No - N/A**	**Observaciones**
Controles NIST SP 800 / Controles ISO 27001 / Controles CIS / Controles HIPAA / Controles PCI A.12.6.2 / 2.4, 2.2, 4.8, 2.5, 2.3, 7.4, 16.8 / 6.4.3		
Se utilizan herramientas de inventariado de software en las que se documenta el software instalado.		
Se ha asegurado que solo el software compatible se designa como autorizado en el inventario de software para activos empresariales		
Se ha establecido un reglamento de instalación de software por parte de los usuarios.		
Se desinstalan o deshabilitan los servicios innecesarios en activos y software empresariales, como un servicio de intercambio de archivos no utilizado, módulo de aplicación web o función de servicio.		
Existentes controles técnicos, como la lista de la lista de aplicaciones, para garantizar que solo el software autorizado pueda ejecutar o acceder.		
Se evalúa semestralmente o con mayor frecuencia el listado de software autorizado.		
Se ha asegurado que el software no autorizado se elimine del uso en los activos empresariales o reciba una excepción documentada.		
Se evalúa mensualmente o con mayor frecuencia la eliminación de software no autorizado.		
Se realizan actualizaciones de aplicaciones sobre activos empresariales a través de la administración de parches automatizado sobre una base mensual o más frecuente.		
Existen entornos separados para los sistemas de producción y no producción.		
El entorno de producción no se utiliza para pruebas o desarrollos.		

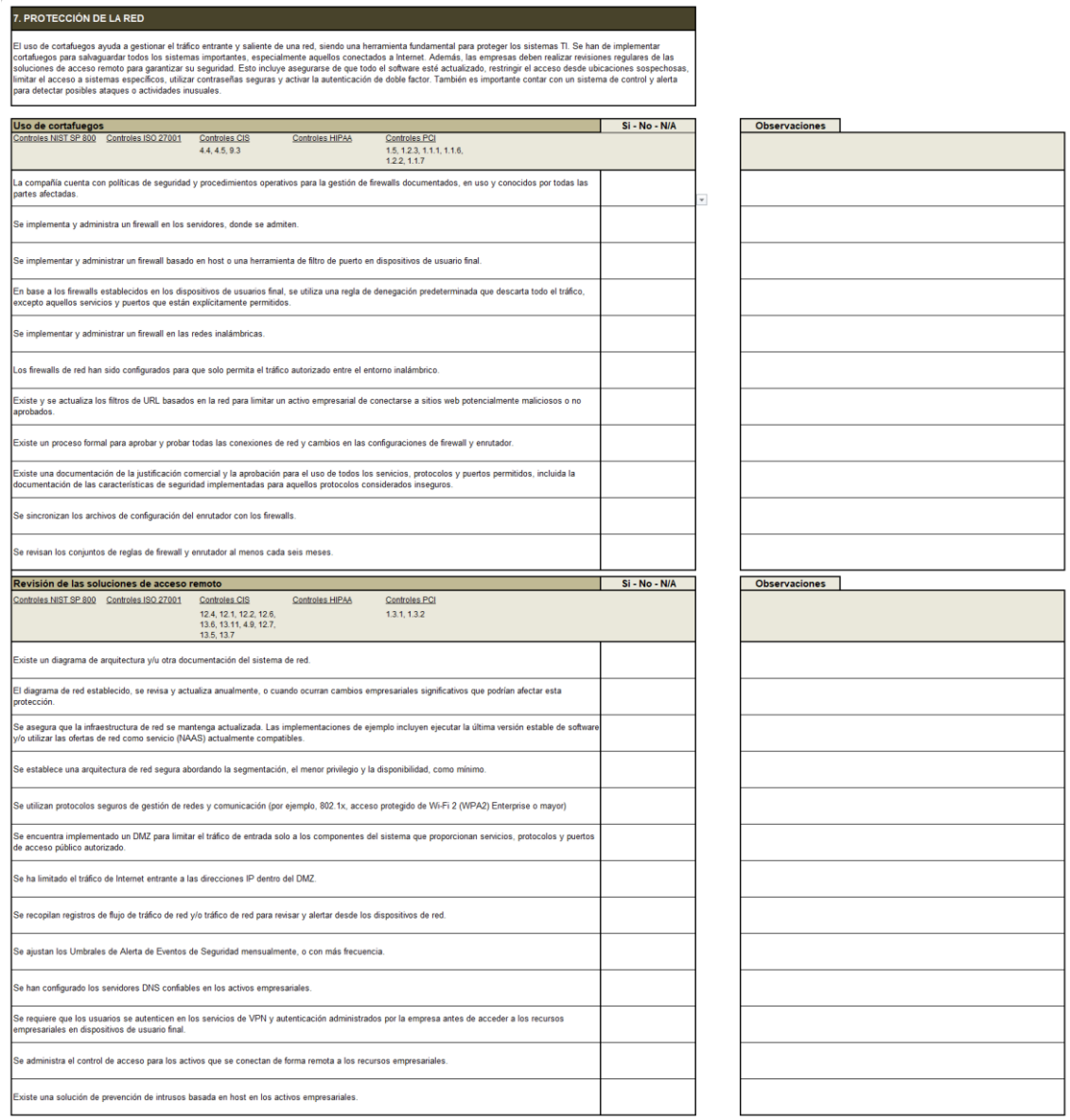
Uso de antivirus	**Si - No - N/A**	**Observaciones**
Controles NIST SP 800 / Controles ISO 27001 / Controles CIS / Controles HIPAA / Controles PCI SI-5 / 10.1, 10.4, 10.7, 7.6, 7.7, 16.2, 10.6, 13.1 / 5.1.1, 5.3		
Se ha instalado un antivirus en todos los activos empresariales.		
Se ha configurado el antivirus para escanear automáticamente los medios extraíbles.		
Los antivirus utilizados son capaces de detectar, eliminar y proteger contra todos los tipos conocidos de software malicioso.		
Los antivirus utilizados detectan amenazas en base al comportamiento de los activos.		
Se han configurado el antivirus para realizar escaneos de vulnerabilidades automatizados de activos.		
Se analizan y revisan los informes de amenazas de los antivirus con una periodicidad mensual o menor.		
Existe un proceso para aceptar y abordar los informes de vulnerabilidades de software identificadas mediante los antivirus.		
El antivirus se gestiona centralmente.		
Se han configurado alertas de seguridad internas, avisos y directivas a través del antivirus.		
Se ha centralizado los alertas de seguridad en los activos empresariales para la correlación y el análisis del registro.		
Los mecanismos antivirus se ejecuten activamente y no puedan ser desactivados o alterados por los usuarios, a menos que la administración autorice específicamente caso por caso por un período de tiempo limitado.		

Uso de herramientas de protección web y correo electrónico	**Si - No - N/A**	**Observaciones**
Controles NIST SP 800 / Controles ISO 27001 / Controles CIS / Controles HIPAA / Controles PCI SI-8 / 9.1, 9.4, 9.7, 9.6, 9.2		
Se ha comprobado que solo los navegadores y los clientes de correo electrónico compatibles puedan ejecutarse en la empresa, solo utilizando la última versión de los navegadores y los clientes de correo electrónico proporcionados a través del proveedor.		
Se ha desinstalado cualquier navegador no autorizado o innecesario o complementos de clientes, extensiones y aplicaciones complementarias.		
Existen implementadas protecciones antimalware del servidor de correo electrónico, como escaneo de archivos adjuntos y/o sandboxing.		
Se han bloqueado todos los tipos de archivos innecesarios que intentan ingresar la puerta de enlace de correo electrónico de la empresa.		
Se utilizan servicios de filtrado DNS en todos los activos empresariales para bloquear el acceso a dominios maliciosos conocidos.		
Se utilizan mecanismos de protección de spam en los puntos de entrada y salida del sistema para detectar y actuar en mensajes no solicitados		

Cifrado de los datos	Si - No - N/A	Observaciones
Controles NIST SP 800 / Controles ISO 27001: A.10.1.2 / Controles CIS: 3.9, 3.6, 3.1, 3.11 / Controles HIPAA / Controles PCI: 3.5.2, 3.6.8, 3.6.1, 8.2.1, 3.6.5, 3.5.3, 3.5.4		
Existe una política sobre el uso, protección y tiempo de vida de claves criptográficas, durante todo su ciclo de vida.		
Se ha restringido el acceso a las claves criptográficas a la menor cantidad de custodios necesarios.		
Los que custodian las clave criptográficos han reconocido formalmente que entienden y aceptan sus responsabilidades clave-custodiadas.		
Se generan claves criptográficas fuertes.		
Se utiliza la encriptación para que todos las credenciales de autenticación sean ilegibles durante la transmisión y el almacenamiento en todos los componentes del sistema.		
Se realiza el reemplazo de las claves como se considera necesario cuando la integridad de la clave se ha debilitado o se sospecha que las claves se ven comprometidas.		
Las claves secretas y privadas utilizadas para cifrar/descifrar datos se almacenan dentro de un dispositivo criptográfico seguro.		
Las claves criptográficas se almacenan en la menor cantidad de ubicaciones posibles.		
Se cifran los datos en medios extraíbles.		
Se cifran los datos en dispositivos de usuario final que contienen datos confidenciales.		
Se cifran los datos confidenciales en tránsito.		
Se cifran los datos confidenciales en reposo sobre servidores, aplicaciones y bases de datos que contienen datos confidenciales.		

Uso de dispositivos móviles	Si - No - N/A	Observaciones
Controles NIST SP 800: AC-17, SC-18, AC-19, AC-12 / Controles ISO 27001: A.6.2.1, A.8.1.4, A.6.2.2, / Controles CIS: 1.1, 1.2, 1.3, 4.3, 4.1 / Controles HIPAA / Controles PCI		
Existe una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.		
Se ha establecido un inventario preciso, detallado y actualizado de todos los activos empresariales con el potencial de almacenar o procesar datos empresariales.		
Se utiliza una herramienta de descubrimiento activo para identificar activos conectados a la red de la empresa.		
La herramienta de identificación de activos en la red ha sido configurada para ejecutar escaneos diariamente, o con más frecuencia.		
Existe un proceso para abordar los activos no autorizados semanalmente.		
Todos los empleados y usuarios de partes externas devuelven todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.		
Existe una política y medidas de seguridad de soporte para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.		
Se han establecido restricciones de uso, requisitos de configuración/conexión y orientación de implementación para cada tipo de acceso remoto permitido.		
Las conexiones para el acceso remoto son previamente autorizadas antes de su uso.		
Se han definido las tecnologías de código móvil aceptables e inaceptables.		
Se han establecido los requisitos de configuración, requisitos de conexión y orientación de implementación para dispositivos móviles controlados por la organización, para incluir cuándo dichos dispositivos están fuera de las áreas controladas.		
Se ha limitado el número de sesiones concurrentes para cada cuenta definida por la organización y/o tipo de cuenta.		
Se ha configurado el bloqueo de la sesión automática en los activos empresariales después de un período definido de inactividad.		
Se bloquean automáticamente los dispositivos después de un umbral predeterminado de intentos de autenticación fallidos locales en dispositivos portátiles de usuario final.		

Ilustración 42. Formulario protección de los dispositivos. Fuente: Elaboración propia.



7. PROTECCIÓN DE LA RED

El uso de cortafuegos ayuda a gestionar el tráfico entrante y saliente de una red, siendo una herramienta fundamental para proteger los sistemas TI. Se han de implementar cortafuegos para salvaguardar todos los sistemas importantes, especialmente aquellos conectados a Internet. Además, las empresas deben realizar revisiones regulares de las soluciones de acceso remoto para garantizar su seguridad. Esto incluye asegurarse de que todo el software esté actualizado, restringir el acceso desde ubicaciones sospechosas, limitar el acceso a sistemas específicos, utilizar contraseñas seguras y activar la autenticación de doble factor. También es importante contar con un sistema de control y alerta para detectar posibles ataques o actividades inusuales.

Uso de cortafuegos	**Si - No - N/A**	**Observaciones**
Controles NIST SP 800 · Controles ISO 27001 · Controles CIS: 4.4, 4.5, 9.3 · Controles HIPAA · Controles PCI: 1.5, 1.2.3, 1.1.1, 1.1.6, 1.2.2, 1.1.7		
La compañía cuenta con políticas de seguridad y procedimientos operativos para la gestión de firewalls documentados, en uso y conocidos por todas las partes afectadas.		
Se implementa y administra un firewall en los servidores, donde se admiten.		
Se implementar y administrar un firewall basado en host o una herramienta de filtro de puerto en dispositivos de usuario final.		
En base a los firewalls establecidos en los dispositivos de usuarios final, se utiliza una regla de denegación predeterminada que descarta todo el tráfico, excepto aquellos servicios y puertos que están explícitamente permitidos.		
Se implementar y administrar un firewall en las redes inalámbricas.		
Los firewalls de red han sido configurados para que solo permita el tráfico autorizado entre el entorno inalámbrico.		
Existe y se actualiza los filtros de URL basados en la red para limitar un activo empresarial de conectarse a sitios web potencialmente maliciosos o no aprobados.		
Existe un proceso formal para aprobar y probar todas las conexiones de red y cambios en las configuraciones de firewall y enrutador.		
Existe una documentación de la justificación comercial y la aprobación para el uso de todos los servicios, protocolos y puertos permitidos, incluida la documentación de las características de seguridad implementadas para aquellos protocolos considerados inseguros.		
Se sincronizan los archivos de configuración del enrutador con los firewalls.		
Se revisan los conjuntos de reglas de firewall y enrutador al menos cada seis meses.		

Revisión de las soluciones de acceso remoto	**Si - No - N/A**	**Observaciones**
Controles NIST SP 800 · Controles ISO 27001 · Controles CIS: 12.4, 12.1, 12.2, 12.6, 13.6, 13.11, 4.9, 12.7, 13.5, 13.7 · Controles HIPAA · Controles PCI: 1.3.1, 1.3.2		
Existe un diagrama de arquitectura y/u otra documentación del sistema de red.		
El diagrama de red establecido, se revisa y actualiza anualmente, o cuando ocurran cambios empresariales significativos que podrían afectar esta protección.		
Se asegura que la infraestructura de red se mantenga actualizada. Las implementaciones de ejemplo incluyen ejecutar la última versión estable de software y/o utilizar las ofertas de red como servicio (NAAS) actualmente compatibles.		
Se establece una arquitectura de red segura abordando la segmentación, el menor privilegio y la disponibilidad, como mínimo.		
Se utilizan protocolos seguros de gestión de redes y comunicación (por ejemplo, 802.1x, acceso protegido de Wi-Fi 2 (WPA2) Enterprise o mayor)		
Se encuentra implementado un DMZ para limitar el tráfico de entrada solo a los componentes del sistema que proporcionan servicios, protocolos y puertos de acceso público autorizado.		
Se ha limitado el tráfico de Internet entrante a las direcciones IP dentro del DMZ.		
Se recopilan registros de flujo de tráfico de red y/o tráfico de red para revisar y alertar desde los dispositivos de red.		
Se ajustan los Umbrales de Alerta de Eventos de Seguridad mensualmente, o con más frecuencia.		
Se han configurado los servidores DNS confiables en los activos empresariales.		
Se requiere que los usuarios se autenticen en los servicios de VPN y autenticación administrados por la empresa antes de acceder a los recursos empresariales en dispositivos de usuario final.		
Se administra el control de acceso para los activos que se conectan de forma remota a los recursos empresariales.		
Existe una solución de prevención de intrusos basada en host en los activos empresariales.		

Ilustración 43. Formulario protección de la red. Fuente: Elaboración propia.

8. SEGURIDAD FÍSICA					
Implementar controles físicos adecuados en los lugares donde se almacena información es importante para garantizar su seguridad. Por ejemplo, los dispositivos móviles y los ordenadores portátiles de la empresa no deben dejarse sin supervisión, y se recomienda bloquearlos cuando el usuario se aleje. Además, los documentos impresos sensibles deben guardarse de manera segura cuando no estén en uso para evitar posibles fugas de información. Estas medidas ayudan a proteger los activos de la empresa y a prevenir accesos no autorizados a datos confidenciales.					
Controles NIST SP 800	Controles ISO 27001	Controles CIS	Controles HIPAA	Controles PCI	Si - No - N/A
PE-2, PE-5, PE-6, PE-15, PE-8, PE-10, PE-12, PE-14	A.11.1.3, A.11.2.8, A.11.1.2., A.11.2.8, A.11.2.5, A.11.1.4		164.310 (a) (2) (iii), 164.310 (a) (2) (iii), 164.310 (a) (2) (iv)	9.1.3, 9.4.2, 9.4.3, 9.4.4, 9.1.2	
Se ha diseñado y implementado medidas de seguridad física en las oficinas, salones e instalaciones.					
Se ha restringido el acceso físico a los puntos de acceso inalámbrico, las puertas de enlace, los dispositivos portátiles, el hardware de redes/comunicaciones y líneas de telecomunicaciones.					
Existen políticas y procedimientos para salvaguardar la instalación y el equipo allí desde acceso físico no autorizado, manipulación y robo.					
Existe una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.					
Existen procedimientos para controlar y validar el acceso de una persona a las instalaciones en función de su papel o función, incluido el control de los visitantes, y el control del acceso a programas de software para pruebas y revisiones.					
Existen políticas y procedimientos para documentar las reparaciones y modificaciones a los componentes físicos de una instalación relacionadas con la seguridad (por ejemplo, hardware, paredes, puertas y cerraduras).					
Las áreas seguras están protegidas mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.					
Existe un listado de personas con acceso autorizado a las instalaciones.					
Se emiten credenciales de autorización para el acceso a las instalaciones					
Se elimina a las personas de la lista de acceso de la instalación cuando ya no se requiere acceso.					
Se controla el acceso físico a la salida para evitar que las personas no autorizadas obtengan la salida.					
Se monitorea el acceso físico a la instalación para detectar y responder a incidentes de seguridad física.					
Los visitantes son identificados y se les da una insignia u otra identificación que expira y que distinga visiblemente a los visitantes del personal en el sitio.					
Se les pide a los visitantes que entreguen la insignia o la identificación antes de salir de la instalación o en la fecha de vencimiento.					
Existe un registro de visitantes para mantener una pista de auditoría física de la actividad de los visitantes en la instalación, así como en salas de computadoras y centros de dato.					
Se han implementado controles físicos y/o lógicos para restringir el acceso por cable a redes.					
Los usuarios se aseguran de que el equipo sin supervisión tiene la protección apropiada.					
Los equipos, información o software no se retiran de su sitio sin autorización previa.					
Existe un diseño de protección física contra desastres naturales, ataques maliciosos o accidentes.					
Se han establecido medidas de seguridad física para prevenir los daños resultantes de la fuga de agua al proporcionar válvulas de cierre maestro o aislamiento que sean accesibles, funcionan correctamente y conocen el personal clave.					
Se han establecido medidas de seguridad física para prevenir daños provocados por el equipo de energía y el cableado de potencia.					
Se han establecido medidas de seguridad física para prevenir un apagado de los dispositivos por fallos en el suministros de la energía, estableciendo fuentes de alimentación alternativas ante casos de riesgo.					
Se han establecido medidas de seguridad física para prevenir incendios mediante sistemas de detección y supresión de incendios respaldados por una fuente de energía independiente.					
Se han establecido medidas de seguridad física para prevenir daños en los componentes hardware mediante sensores de temperatura.					
Se han establecido medidas de seguridad física para prevenir daños en los componentes hardware mediante sensores de humedad.					

Observaciones

Ilustración 44. Formulario seguridad física. Fuente: Elaboración propia.

9. PROTECCIÓN DE LAS COPIAS DE SEGURIDAD						
Realizar copias de seguridad periódicas y automáticas para garantizar la recuperación de datos clave en caso de desastres como ataques de ransomware. Estas copias deben mantenerse separadas del entorno de producción de la empresa y estar cifradas, especialmente si se trasladan a otra ubicación. Es importante realizar pruebas periódicas para verificar la capacidad de recuperación de datos, idealmente con una restauración completa de inicio a fin. Estas medidas ayudan a asegurar la integridad y disponibilidad de la información empresarial en situaciones críticas.						
Controles NIST SP 800	Controles ISO 27001	Controles CIS	Controles HIPAA	Controles PCI	Si - No - N/A	Observaciones
CP-2	12.3.1	11.1, 11.2, 11.3		9.5.1		
Existe un plan de contingencia para los sistemas principales que establecen entre otro puntos, objetivos de recuperación, prioridades de restauración y métricas.						
Se ha establecido un proceso copias de seguridad, en el que se detalla entre otros puntos, el alcance de las actividades de recuperación de datos, la priorización de recuperación y la seguridad de los datos de copia de seguridad.						
Se revisa y actualiza la documentación de los procesos de copias de seguridad anualmente, o cuando ocurran cambios empresariales significativos que podrían afectar esta protección.						
Se realizan copias de respaldo de la información, software e imágenes de los sistemas y se ponen a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.						
Se realizan copias de seguridad automatizadas semanalmente, o con más frecuencia, en función de la sensibilidad de los datos.						
Existe una instancia aislada de copia de seguridad fuera de los servicios en línea.						
Se almacena las copias de seguridad en una ubicación segura.						

Ilustración 45. Formulario protección de las copias de seguridad. Fuente: Elaboración propia.

10. PROTECCIÓN EN LA NUBE						
Al adoptar soluciones en la nube, las compañías deben considerar tanto los beneficios como los riesgos asociados. Antes de elegir un proveedor de servicios en la nube, es crucial que las empresas consulten guías de seguridad específicas para comprender mejor los requisitos y desafíos.						
Controles NIST SP 800	Controles ISO 27001	Controles CIS	Controles HIPAA	Controles PCI	Si - No - N/A	Observaciones
	11.2..1			2.6, 10.8		
Los proveedores de alojamiento compartido deben proteger el entorno alojado de cada entidad y estos proveedores deben confirmar su alineación de controles de seguridad con los establecidos por la compañía.						
Se ha asegurado que los equipos ubicados en el cloud están protegidos para reducir los riesgos de amenazas y peligros ambientales y las posibilidades de acceso no autorizado.						
Se ha implementado un proceso para la detección oportuna e informes de fallas de los sistemas ubicados en el cloud, en los que se incluyen el informe de fallos en: firewalls, IDS/IPS, FIM, antivirus, controles de acceso físico, controles de acceso lógicos...						

Ilustración 46. Formulario protección en la nube. Fuente: Elaboración propia.

11. PROTECCIÓN DE LOS SITIOS WEB						
Las compañías deben garantizar la seguridad de sus sitios web, especialmente protegiendo datos sensibles como información financiera o datos de tarjetas de crédito.						
Controles NIST SP 800	Controles ISO 27001	Controles CIS	Controles HIPAA	Controles PCI	Si - No - N/A	Observaciones
SC-35, SC-22				6.6, 2.2.1		
Se realizan revisiones de aplicaciones web de orientación pública a través de herramientas o métodos de evaluación de seguridad de vulnerabilidades de aplicaciones manuales o automatizadas, al menos anualmente y después de cualquier cambio relevante.						
Existe instalada una solución técnica automatizada que detecte y evite ataques basados en la web frente a aplicaciones web orientadas al público, para verificar continuamente todo el tráfico.						
Existen componentes del sistema que buscan proactivamente identificar código malicioso basado en la red o sitios web maliciosos.						
Se ha implementado solo una función principal por servidor para evitar funciones que requieran diferentes niveles de seguridad coexistir en el mismo servidor.						
Se ha comprobado que el servicio de resolución de nombres/direcciones utilizado es tolerable a fallos e implementan una separación de roles interna y externa.						

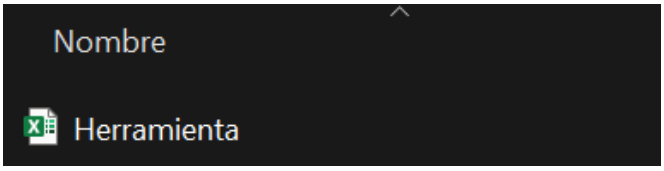
Ilustración 47. Formulario protección de los sitios web. Fuente: Elaboración propia.

12. BUSQUEDA Y DIFUSIÓN DE INFORMACIÓN DE CIBERSEGURIDAD						
El intercambio de información es relevante en la lucha contra la ciberdelincuencia, ya que permite a las compañías comprender mejor los riesgos a los que se enfrentan. Aquellas empresas que reciben información sobre problemas de ciberseguridad de sus compañeros están más inclinadas a tomar medidas para proteger sus sistemas en comparación con aquellas que obtienen información de informes del sector o encuestas sobre ciberseguridad.						
Controles NIST SP 800	Controles ISO 27001	Controles CIS	Controles HIPAA	Controles PCI	Si - No - N/A	Observaciones
PM-15	A.6.1.4					
Se mantienen controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.						
Se ha establecido contacto con grupos y asociaciones seleccionadas dentro de las comunidades de seguridad y privacidad para facilitar la seguridad y la capacitación continua de seguridad y privacidad para el personal organizacional.						
Se ha establecido contacto con grupos y asociaciones seleccionadas dentro de las comunidades de seguridad y privacidad para mantener prácticas de seguridad y privacidad recomendadas, técnicas y tecnologías.						
Se ha establecido contacto con grupos y asociaciones seleccionadas dentro de las comunidades de seguridad y privacidad para compartir información actual de seguridad y privacidad, incluidas amenazas, vulnerabilidades e incidentes.						

Ilustración 48. Formulario búsqueda y difusión de información de ciberseguridad. Fuente: Elaboración propia.

Fase 5. Desarrollo de la herramienta

Para finalizar, tras definir las preguntas del formulario y vincular cada una con un control específico, se ha procedido a fusionar los documentos "Formulario", "Mapping Controles - Áreas ENISA" y "Mapping Controles – Riesgos ENISA". Esta integración se ha realizado utilizando el documento "Herramienta".



Como resultado, se ha creado una nueva ventana denominada "Resultados" que tiene como objetivo mostrar el nivel de cumplimiento de las áreas de solución para pymes establecidas por ENISA, así como el grado de cobertura de los riesgos definidos por ENISA en base a las respuestas dadas en cada uno de los formularios.

ANÁLISIS POR ÁREAS

	SI	NO	N/A	Nivel de cumplimiento
1. DESARROLLO DE LA CULTURA DE CIBERSEGURIDAD	**0**	**0**	**0**	**N/A**
1.1 Responsabilidades de la gestión de activos empresariales	0	0	0	N/A
1.2 Implicaciones de los empleados	0	0	0	N/A
1.3 Auditorías de seguridad	0	0	0	N/A
1.4 Publicación de las políticas de ciberseguridad	0	0	0	N/A
1.5 Medidas para la protección de datos	0	0	0	N/A
2. IMPARTIR UNA FORMACIÓN ADECUADA	**0**	**0**	**0**	**N/A**
3. GESTIÓN EFICAZ DE TERCEROS	**0**	**0**	**0**	**N/A**
4. DESARROLLO DE UN PLAN DE RESPUESTA ANTE INCIDENTES	**0**	**0**	**0**	**N/A**
5. PROTECCIÓN DEL ACCESO A LOS SISTEMAS	**0**	**0**	**0**	**N/A**
6. PROTECCIÓN DE LOS DISPOSITIVOS	**0**	**0**	**0**	**N/A**
6.1 Mantenimiento del software	0	0	0	N/A
6.2 Uso de antivirus	0	0	0	N/A
6.3 Uso de herramientas de protección web y correo electronico	0	0	0	N/A
6.4 Cifrado de los datos	0	0	0	N/A
6.5 Uso de dispositivos móviles	0	0	0	N/A
7. PROTECCIÓN DE LA RED	**0**	**0**	**0**	**N/A**
7.1 Uso de cortafuegos	0	0	0	N/A
7.2 Revisión de las soluciones de acceso remoto	0	0	0	N/A
8. SEGURIDAD FÍSICA	**0**	**0**	**0**	**N/A**
9. PROTECCIÓN DE LAS COPIAS DE SEGURIDAD	**0**	**0**	**0**	**N/A**
10. PROTECCIÓN EN LA NUBE	**0**	**0**	**0**	**N/A**
11. PROTECCIÓN DE LOS SITIOS WEB	**0**	**0**	**0**	**N/A**
12. BUSQUEDA Y DIFUSIÓN DE INFORMACIÓN DE CIBERSEGURIDAD	**0**	**0**	**0**	**N/A**

Nivel de Cumplimiento	Porcentaje	Color
Muy Bajo	0% - 10%	
Bajo	11% - 50 %	
Medio	51% - 80%	
Alto	81% - 90%	
Muy Alto	91% - 100%	

RIESGOS DE CIBERSEGURIDAD

	Nivel de cumplimiento
Ataques intencionales	**N/A**
Fraude	N/A
Sabotaje	N/A
Vandalismo	N/A
Robo	N/A
Fuga/Intercambio de información	N/A
Coacción, extorsión o corrupción	N/A
Entrada no autorizada	N/A
Daños de guerra	N/A
Ataque	N/A
Daños involuntarios	**N/A**
Fuga/Intercambio de información debido a un error humano	N/A
Uso o administración errónea de dispositivos y sistemas	N/A
Información de una fuente no confiable	N/A
Cambio involuntario de datos en un sistema de información	N/A
Diseño y planificación inadecuados o adaptación inadecuadas	N/A
Daños causados por un tercero	N/A
Daño resultantes de las pruebas de penetración	N/A
Perdida de infromación en la nube	N/A
Pérdida de la integridad de información sensible	N/A
Pérdida de dispositivos, medios de almacenamiento y documentos	N/A
Destrucción de registros	N/A
Desastre natural/ambiental	**N/A**
Desastres	N/A
Fuego	N/A
Contaminación, polvo o corrosión	N/A
Golpe de trueno	N/A
Agua	N/A
Explosión	N/A
Fuga de radiación peligrosa	N/A
Condiciones climáticas desfavorables	N/A
Grandes acontecimientos en el medio ambiente	N/A
Amenazas desde el espacio/Tormenta electromagnética	N/A
Fauna sivestre	N/A
Fallos/Mal funcionamiento	**N/A**
Fallo de dispositivos o sistemas	N/A
Fallo o interrupción de los enlaces de comunicación	N/A
Fallo o interrupción del suministro principal	N/A
Fallo o interrupción de los proveedores de servicio	N/A
Mal funcionamiento de los equipos	N/A
Disponibilidad de recursos	**N/A**
Pérdida de recursos	N/A
Ausencia de personal	N/A
Huelga	N/A
Pérdida de servicios de soporte	N/A
Corte de internet	N/A
Caida de la red	N/A
Intercepciones	**N/A**
Conducción de guerra	N/A
Interceptar emisiones comprometedoras	N/A
Intercepción de información	N/A
Radiación interferencial	N/A
Repetición de mensajes	N/A
Reconocimiento de red, manipulación del tráfico de red y recopilación de información	N/A
Hombre en el medio/secuestro de sesión	N/A
Actividades maliciosas	**N/A**
Robo de identidad	N/A
Recibir correo electrónico no deseado	N/A
Negación de servicio	N/A
Código/Software/Actividad maliciosa	N/A
Igeniería social	N/A
Abuso de filtración de información	N/A
Generación y uso de certificados falsos	N/A
Manipulación de hardware y software	N/A
Manipulación de información	N/A
Mal uso de herramientas de auditoría	N/A
Uso indebido de información/sistemas de información	N/A
Actividades no autorizadas	N/A
Instalación no autorizada de software	N/A
Comprometer información confidencial	N/A
Falso rumor	N/A
Actividad remota	N/A
Ataque dirigido	N/A
Fallo en el proceso de negocio	N/A
Fuerza bruta	N/A
Aabuso de autorizaciones	N/A
Legal	**N/A**
Incumplimiento de la legislación	N/A
Incumplimiento de los requisitos contractuales	N/A
Uso no autorizado de recursos protegidos por derechos de propiedad intelectual	N/A
Abuso de datos personales	N/A

Nivel de Cumplimiento	Porcentaje	Color
Muy Bajo	0% - 10%	
Bajo	11% - 50 %	
Medio	51% - 80%	
Alto	81% - 90%	
Muy Alto	91% - 100%	

Ilustración 49. Ventana "Resultados" del documento Herramienta. Fuente: Elaboración propia.

Resultado de las áreas de solución

En primer lugar, se analizará cómo se han obtenido los resultados de las áreas de solución establecidas por ENISA.

ANÁLISIS POR ÁREAS

	SI	NO	N/A	Nivel de cumplimiento
1. DESARROLLO DE LA CULTURA DE CIBERSEGURIDAD	0	0	0	N/A
1.1 Responsabilidades de la gestión de activos empresariales	0	0	0	N/A
1.2 Implicaciones de los empleados	0	0	0	N/A
1.3 Auditorías de seguridad	0	0	0	N/A
1.4 Publicación de las políticas de ciberseguridad	0	0	0	N/A
1.5 Medidas para la protección de datos	0	0	0	N/A
2. IMPARTIR UNA FORMACIÓN ADECUADA	0	0	0	N/A
3. GESTIÓN EFICAZ DE TERCEROS	0	0	0	N/A
4. DESARROLLO DE UN PLAN DE RESPUESTA ANTE INCIDENTES	0	0	0	N/A
5. PROTECCIÓN DEL ACCESO A LOS SISTEMAS	0	0	0	N/A
6. PROTECCIÓN DE LOS DISPOSITIVOS	0	0	0	N/A
6.1 Mantenimiento del software	0	0	0	N/A
6.2 Uso de antivirus	0	0	0	N/A
6.3 Uso de herramientas de protección web y correo electronico	0	0	0	N/A
6.4 Cifrado de los datos	0	0	0	N/A
6.5 Uso de dispositivos móviles	0	0	0	N/A
7. PROTECCIÓN DE LA RED	0	0	0	N/A
7.1 Uso de cortafuegos	0	0	0	N/A
7.2 Revisión de las soluciones de acceso remoto	0	0	0	N/A
8. SEGURIDAD FÍSICA	0	0	0	N/A
9. PROTECCIÓN DE LAS COPIAS DE SEGURIDAD	0	0	0	N/A
10. PROTECCIÓN EN LA NUBE	0	0	0	N/A
11. PROTECCIÓN DE LOS SITIOS WEB	0	0	0	N/A
12. BUSQUEDA Y DIFUSIÓN DE INFORMACIÓN DE CIBERSEGURIDAD	0	0	0	N/A

Nivel de Cumplimiento	Porcentaje	Color
Muy Bajo	0% - 10%	
Bajo	11% - 50 %	
Medio	51% - 80%	
Alto	81% - 90%	
Muy Alto	91% - 100%	

Ilustración 50. Análisis resultados por áreas ENISA. Fuente: Elaboración propia.

Este análisis se ha dividido según las áreas de solución a la ciberseguridad establecidas por ENISA. Para cada área, se ha contado la cantidad de respuestas "Sí", "No", y "N/A" obtenidas. A continuación, se muestra un ejemplo de la fórmula utilizada para contabilizar estos casos en cada ventana:

- Caso “Si”

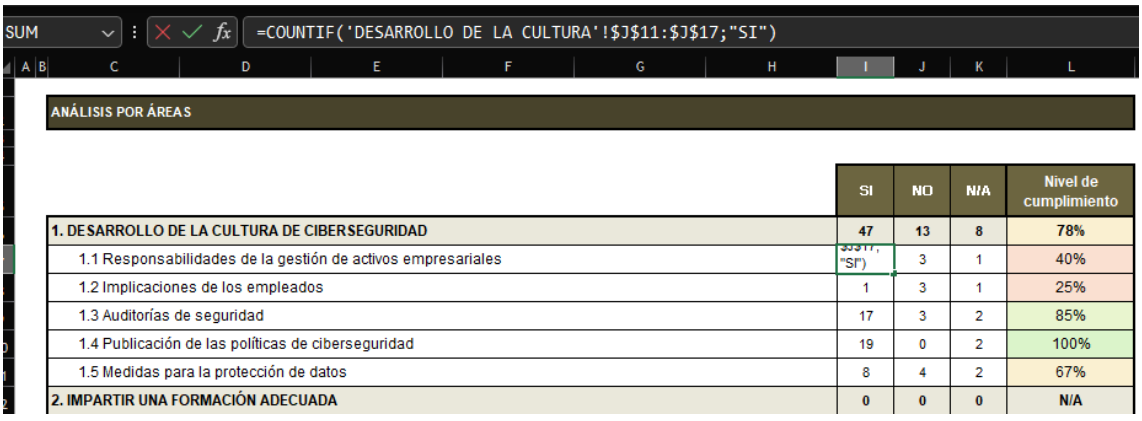


Ilustración 51. Formula en caso de "Si", Análisis por áreas. Fuente: Elaboración propia.

Formula:

=COUNTIF('DESARROLLO DE LA CULTURA'!$J$11:$J$17;"SI")

Donde 'DESARROLLO DE LA CULTURA'!$J$11:$J$17 hace referencia a la columna de respuestas del formulario de Desarrollo de la cultura, en este caso en específico sobre la subárea 1.1 Responsabilidad de la gestión de activos empresariales.

1. DESARROLLO DE LA CULTURA DE CIBERSEGURIDAD					
Se ha de designar a un responsable dentro de la empresa para gestionar eficazmente los recursos destinados a la seguridad de la información TI, como tiempo del personal, compra de software y hardware, formación y desarrollo de políticas efectivas. Además, se enfatiza la importancia de aumentar la participación y concienciación de los empleados mediante una comunicación clara, formación adecuada y el establecimiento de normas específicas en las políticas de ciberseguridad.					
Responsabilidades de la gestión de activos empresariales					**Si - No - N/A**
Controles NIST SP 800	Controles ISO 27001	Controles CIS	Controles HIPAA	Controles PCI	
AC-2, PS-9, PM-2	A.6.1.2	17.5			
Se han desarrollado y documentado políticas y procedimientos relacionados con la gestión de los roles/permisos en los sistemas informáticos en los que se generan registros para su posterior trazabilidad. Ejemplo (procedimientos de modificación, asignación o revocación de roles/permisos)					No
Se han establecido roles y responsabilidades de seguridad y privacidad en base a los puestos laborales.					No
Las tareas y áreas de responsabilidad en conflicto se separan para reducir las posibilidades de modificación no autorizada o el uso indebido de los activos de la organización.					Si
Se ha designado un responsable oficial de la seguridad de la información encargado de coordinar, desarrollar, implementar y mantener la seguridad de la información en toda la organización.					N/A
Se han asignado roles y responsabilidades clave para la respuesta a los incidentes de seguridad informática.					Si
Se ha establecido un proceso de gestión de roles/permisos críticos, en los que se existe una aprobación por parte de un responsable competente.					No
Se realiza una revisión anual para comprobar que los roles/permisos asignados a cada usuario en el sistema informático siguen alineados con las funciones desarrolladas.					No

Ilustración 52. Área en alcance bajo la fórmula analizada. Fuente: Elaboración propia.

- Caso “No”

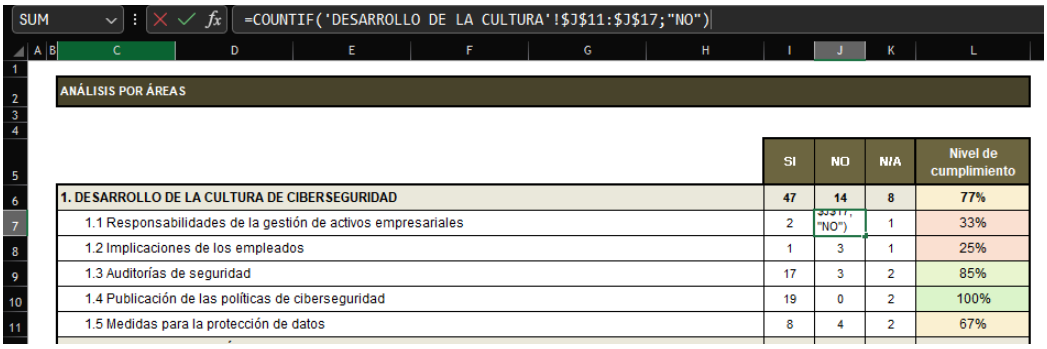


Ilustración 53. Formula en caso de "No", Análisis por áreas. Fuente: Elaboración propia.

Formula:

=COUNTIF('DESARROLLO DE LA CULTURA'!$J$11:$J$17;"NO")

Donde 'DESARROLLO DE LA CULTURA'!$J$11:$J$17 hace referencia a la columna de respuestas del formulario de Desarrollo de la cultura, en este caso en específico sobre la subárea 1.1 Responsabilidad de la gestión de activos empresariales.

- Caso “N/A”

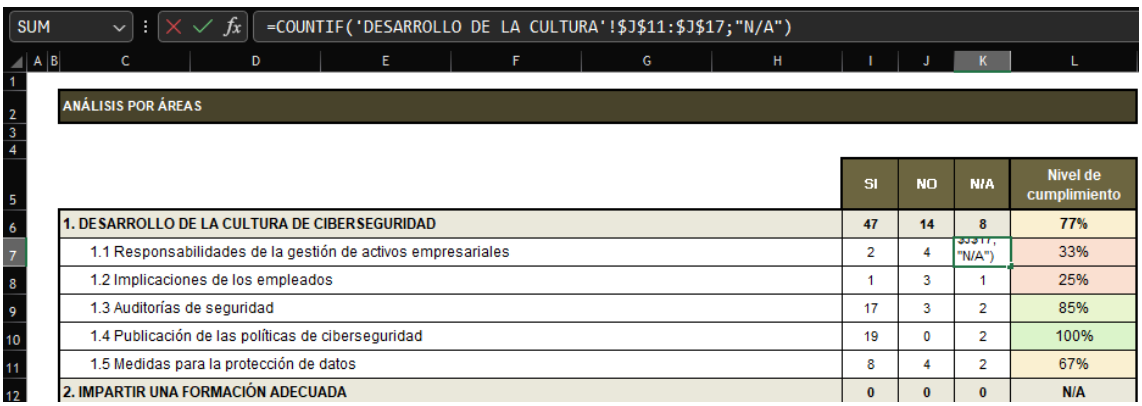
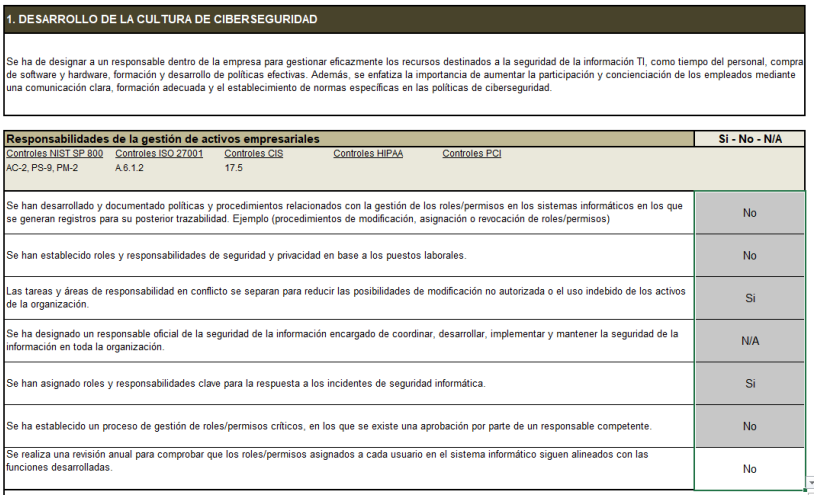


Ilustración 54. Formula en caso de "N/A", Análisis por áreas. Fuente: Elaboración propia.

Formula:

=COUNTIF('DESARROLLO DE LA CULTURA'!$J$11:$J$17;"N/A")

Donde 'DESARROLLO DE LA CULTURA'!$J$11:$J$17 hace referencia a la columna de respuestas del formulario de Desarrollo de la cultura, en este caso en específico sobre la subárea 1.1 Responsabilidad de la gestión de activos empresariales.

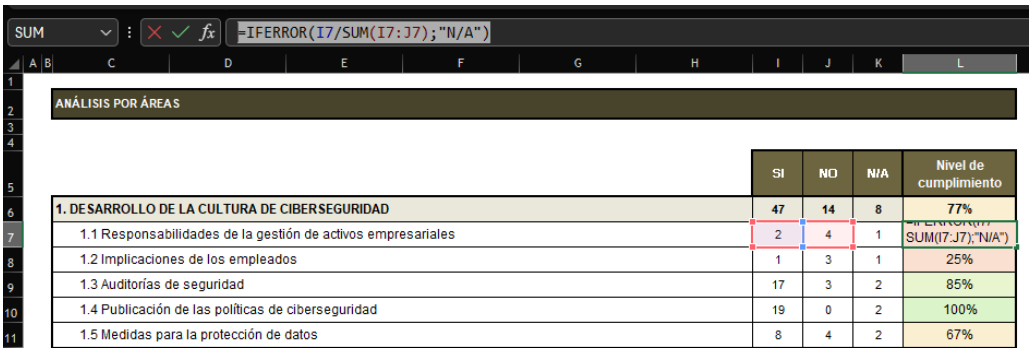


1. DESARROLLO DE LA CULTURA DE CIBERSEGURIDAD	
Se ha de designar a un responsable dentro de la empresa para gestionar eficazmente los recursos destinados a la seguridad de la información TI, como tiempo del personal, compra de software y hardware, formación y desarrollo de políticas efectivas. Además, se enfatiza la importancia de aumentar la participación y concienciación de los empleados mediante una comunicación clara, formación adecuada y el establecimiento de normas específicas en las políticas de ciberseguridad.	
Responsabilidades de la gestión de activos empresariales Controles NIST SP 800: AC-2, PS-9, PM-2 Controles ISO 27001: A.6.1.2 Controles CIS: 17.5 Controles HIPAA Controles PCI	**Si - No - N/A**
Se han desarrollado y documentado políticas y procedimientos relacionados con la gestión de los roles/permisos en los sistemas informáticos en los que se generan registros para su posterior trazabilidad. Ejemplo (procedimientos de modificación, asignación o revocación de roles/permisos)	No
Se han establecido roles y responsabilidades de seguridad y privacidad en base a los puestos laborales.	No
Las tareas y áreas de responsabilidad en conflicto se separan para reducir las posibilidades de modificación no autorizada o el uso indebido de los activos de la organización.	Si
Se ha designado un responsable oficial de la seguridad de la información encargado de coordinar, desarrollar, implementar y mantener la seguridad de la información en toda la organización.	N/A
Se han asignado roles y responsabilidades clave para la respuesta a los incidentes de seguridad informática.	Si
Se ha establecido un proceso de gestión de roles/permisos críticos, en los que se existe una aprobación por parte de un responsable competente.	No
Se realiza una revisión anual para comprobar que los roles/permisos asignados a cada usuario en el sistema informático siguen alineados con las funciones desarrolladas.	No

Ilustración 55. Área en alcance bajo la fórmula analizada. Fuente: Elaboración propia.

Por último, el nivel de cumplimiento de cada área se calcula siguiendo la siguiente fórmula:

=IFERROR(I7/SUM(I7:J7);"N/A")



SUM | =IFERROR(I7/SUM(I7:J7);"N/A")

ANÁLISIS POR ÁREAS

	SI	NO	N/A	Nivel de cumplimiento
1. DESARROLLO DE LA CULTURA DE CIBERSEGURIDAD	**47**	**14**	**8**	**77%**
1.1 Responsabilidades de la gestión de activos empresariales	2	4	1	=IFERROR(I7/SUM(I7:J7);"N/A")
1.2 Implicaciones de los empleados	1	3	1	25%
1.3 Auditorías de seguridad	17	3	2	85%
1.4 Publicación de las políticas de ciberseguridad	19	0	2	100%
1.5 Medidas para la protección de datos	8	4	2	67%

Ilustración 56. Fórmula utilizada para el cálculo del nivel de cumplimiento de las áreas. Fuente: Elaboración propia.

Esta fórmula calcula el resultado dividiendo los sí, entre la suma de si y no marcados. Cabe destacar que para mostrar los resultados del nivel de cumplimiento de las distintas áreas se ha optado por una escalera de color definida tal y como se muestra en la ilustración siguiente:

Nivel de Cumplimiento	Porcentaje	Color
Muy Bajo	0% - 10%	
Bajo	11% - 50 %	
Medio	51% - 80%	
Alto	81% - 90%	
Muy Alto	91% - 100%	

Ilustración 57. Escala de color por nivel de cumplimiento. Fuente: Elaboración propia.

Resultado de los riesgos de ciberseguridad

En segundo lugar, se analizará cómo se han obtenido los resultados de los riesgos de ciberseguridad definidos.

RIESGOS DE CIBERSEGURIDAD	
	Nivel de cumplimiento
Ataques intencionales	**N/A**
Fraude	N/A
Sabotaje	N/A
Vandalismo	N/A
Robo	N/A
Fuga/Intercambio de información	N/A
Coacción, extorsión o corrupción	N/A
Entrada no autorizada	N/A
Daños de guerra	N/A
Ataque	N/A
Daños involuntarios	**N/A**
Fuga/Intercambio de información debido a un error humano	N/A
Uso o administración errónea de dispositivos y sistemas	N/A
Información de una fuente no confiable	N/A
Cambio involuntario de datos en un sistema de información	N/A
Diseño y planificación inadecuados o adaptación inadecuadas	N/A
Daños causados por un tercero	N/A
Daño resultantes de las pruebas de penetración	N/A
Perdida de infromación en la nube	N/A
Pérdida de la integridad de información sensible	N/A
Pérdida de dispositivos, medios de almacenamiento y documentos	N/A
Destrucción de registros	N/A
Desastre natural/ambiental	**N/A**
Desastres	N/A
Fuego	N/A
Contaminación, polvo o corrosión	N/A
Golpe de trueno	N/A
Agua	N/A
Explosión	N/A
Fuga de radiación peligrosa	N/A
Condiciones climáticas desfavorables	N/A
Grandes acontecimientos en el medio ambiente	N/A
Amenazas desde el espacio/Tormenta electromagnética	N/A
Fauna sivestre	N/A
Fallos/Mal funcionamiento	**N/A**
Fallo de dispositivos o sistemas	N/A
Fallo o interrupción de los enlaces de comunicación	N/A
Fallo o interrupción del suministro principal	N/A
Fallo o interrupción de los proveedores de servicio	N/A
Mal funcionamiento de los equipos	N/A
Disponibilidad de recursos	**N/A**
Pérdida de recursos	N/A
Ausencia de personal	N/A
Huelga	N/A
Pérdida de servicios de soporte	N/A
Corte de internet	N/A
Caida de la red	N/A
Intercepciones	**N/A**
Conducción de guerra	N/A
Interceptar emisiones comprometedoras	N/A
Intercepción de información	N/A
Radiación interferencial	N/A
Repetición de mensajes	N/A
Reconocimiento de red, manipulación del tráfico de red y recopilación de información	N/A
Hombre en el medio/secuestro de sesión	N/A
Actividades maliciosas	**N/A**
Robo de identidad	N/A
Recbir correo electrónico no deseado	N/A
Negación de servicio	N/A
Código/Software/Actividad maliciosa	N/A
Igeniería social	N/A
Abuso de filtración de información	N/A
Generación y uso de certificados falsos	N/A
Manipulación de hardware y software	N/A
Manipulación de información	N/A
Mal uso de herramientas de auditoría	N/A
Uso indebido de información/sistemas de información	N/A
Actividades no autorizadas	N/A
Instalación no autorizada de software	N/A
Comprometer información confidencial	N/A
Falso rumor	N/A
Actividad remota	N/A
Ataque dirigido	N/A
Fallo en el proceso de negocio	N/A
Fuerza bruta	N/A
Aabuso de autorizaciones	N/A
Legal	**N/A**
Incumplimiento de la legislación	N/A
Incumplimiento de los requisitos contractuales	N/A
Uso no autorizado de recursos protegidos por derechos de propiedad intelectual	N/A
Abuso de datos personales	N/A

Ilustración 58. Análisis resultados por riesgos de ciberseguridad. Fuente: Elaboración propia.

En este caso el análisis ha sido más complejo y se ha precisado la creación de una nueva ventana para realizar el cálculo del nivel de cumplimiento de los riesgos de ciberseguridad (ventana “Resultado Mapping”).

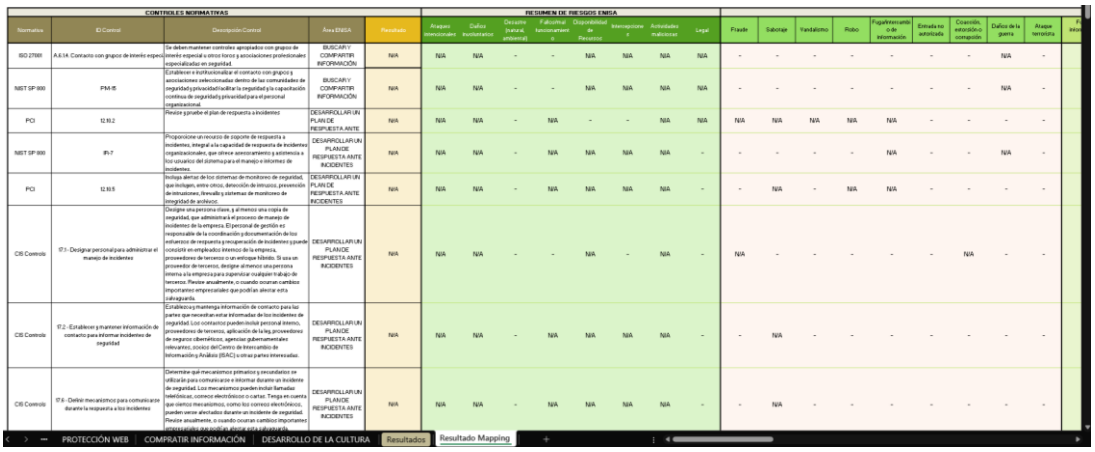


Ilustración 59. Ventana "Resultado Mapping" de la herramienta. Fuente: Elaboración propia.

En esta ventana se ha utilizado como base el documento “Mapping Controles – Riesgos ENISA”, el cual se había hecho el trabajo de mapear cada control con los riesgos de ciberseguridad que cubre. Adicionalmente a forma de automatizar los resultados se ha añadido la columna Resultado. Cada control de esta columna se encuentra vinculado con cada respuesta del formulario, mediante la siguiente fórmula:

=IF(ISBLANK(*[Celda de respuesta del formulario]*);"N/A";*[Celda de respuesta del formulario]*)

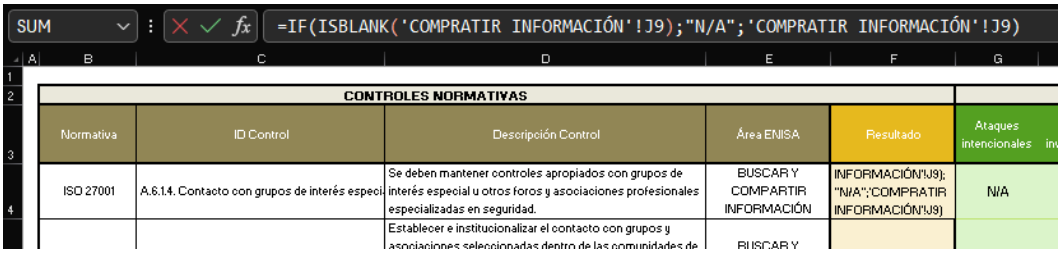


Ilustración 60. Fórmula columna resultado. Fuente: Elaboración propia.

En este caso se ha vinculado cada una de estas casillas con la respuesta de formulario que cubre el control en cuestión, devolviendo los valores predefinidos para cada respuesta del formulario (Si, No o N/A) o N/A en caso de que la pregunta del cuestionario se quede vacía.

Paralelamente se han querido modificar los valores del mapeo de cada control con sus riesgos de ciberseguridad para que en vez de mostrar un “X” por cada riesgo que cubra el control, muestre la respuesta de la encuesta.

Para ello se ha precisado vincular el documento “Mapping Controles – Riesgos ENISA” en una ventana del fichero Herramienta y se ha aplicado la siguiente fórmula sobre cada una de las celdas de los riesgos de ciberseguridad:

=IF('Mapping Controles - Riesgos'!N6="";"-";'Resultado Mapping'!F6)

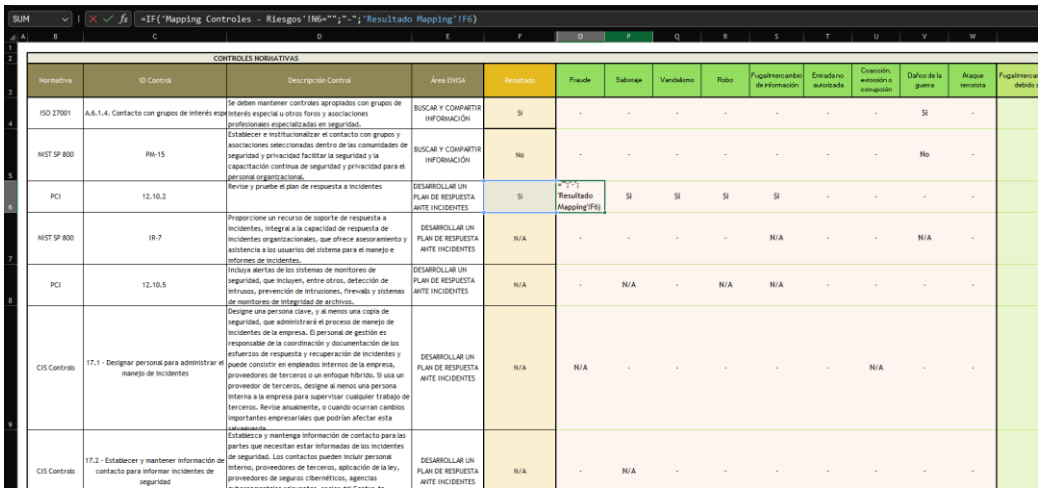


Ilustración 61. Fórmula riesgos ciberseguridad - respuesta encuesta. Fuente: Elaboración propia.

Esta fórmula lo que hace es comprobar en base a la ventana "Mapping Controles – Riesgos", si el control cubre el riesgo de ciberseguridad establecido según el mapping desarrollado en la *"Fase 3. Mapeo controles con riesgos de ciberseguridad"* y en caso de que aplique modificar su celda en base a la respuesta dada en el encuesta, para ello se vincula con la celda correspondiente de la columna "Resultado".

Finalmente, tras tratar la ventana de "Resultado Mapping" esta ha sido utilizada para definir el nivel de cumplimiento de riesgos de ciberseguridad mediante la siguiente fórmula:

=IF(AND(COUNTIF('Resultado Mapping'!O4:O280;"Si")<=0;COUNTIF('Resultado Mapping'!O4:O280;"No")<=0);"N/A";COUNTIF('Resultado Mapping'!O4:O280;"Si")/(COUNTIF('Resultado Mapping'!O4:O280;"Si")+COUNTIF('Resultado Mapping'!O4:O280;"No")))

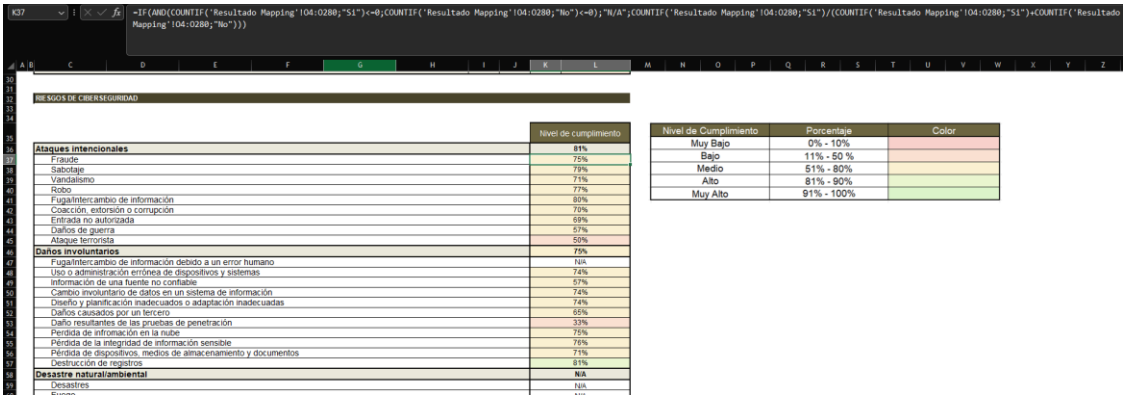


Ilustración 62. Fórmula utilizada para el cálculo del nivel de cumplimiento de los riesgos de ciberseguridad. Fuente: Elaboración propia.

En el caso de ejemplo mostrado en la anterior ilustración se puede evidenciar como esta fórmula comprueba los valores de la columna de fraude del fichero de "Resultado Mapping" (Columnas O4 a la O280), y en el caso de que no identifique ninguna celda con valor "Si" o "No" devuelve el valor "N/A". En caso contrario, se procederá a calcular el porcentaje de nivel de cumplimiento sumando el total de respuestas "Si" de la columna del riesgo asociado en la ventana "Resultado Mapping" dividido el total de respuestas "Si" más el de "No".

Cabe destacar que para mostrar los resultados de nivel de cumplimiento de riesgos de ciberseguridad se ha optado también por una escalera de color definida tal y como se muestra en la ilustración siguiente:

Nivel de Cumplimiento	Porcentaje	Color
Muy Bajo	0% - 10%	
Bajo	11% - 50 %	
Medio	51% - 80%	
Alto	81% - 90%	
Muy Alto	91% - 100%	

Ilustración 63. Escala de color por nivel de cumplimiento. Fuente: Elaboración propia.

Por último, a modo de facilitar el uso de la herramienta para los posibles usuarios que la quieran utilizar se ha definido la ventana introducción en la que se detalla la finalidad de la herramienta, una guía de uso y un resumen de la estructura del documento:

HERRAMIENTA DE AUTOEVALUACIÓN DE LA MADUREZ DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

La Herramienta de Autoevaluación de la Madurez de la Seguridad de la Información está diseñada para proporcionar a las organizaciones medianas y pequeñas que no cuentan con un marco de IT robusto, un medio eficaz para **evaluar su nivel actual de madurez** en la implementación de prácticas de **seguridad de la información**. Esta herramienta permite a las organizaciones identificar áreas clave de fortaleza y oportunidades de mejora en diversos aspectos críticos de la seguridad.

El desarrollo de esta herramienta se fundamenta en un enfoque integral, abarcando **múltiples dominios de seguridad** como el desarrollo de la cultura, la formación, la gestión de terceros, la respuesta a incidentes, la protección de acceso, dispositivos y red, la seguridad física, copias de seguridad, protección en la nube, protección web, y el compartir información.

Cada uno de estos dominios está desglosado en controles específicos que ayudan a las organizaciones a medir su desempeño y madurez de manera detallada y estructurada. Además, la herramienta incluye un análisis exhaustivo y un mapeo de controles contra riesgos, proporcionando una visión clara y coherente de cómo cada control contribuye a la mitigación de riesgos específicos.

USO DE LA HERRAMIENTA

La Herramienta está diseñada como un **formulario** estructurado en el que los usuarios deben responder preguntas relacionadas con doce áreas críticas de seguridad. Para cada control detallado en estas áreas, los usuarios deben seleccionar una de tres respuestas posibles:

- Sí: Indica que la organización cumple con el control especificado.
- No: Indica que la organización no cumple con el control especificado.
- N/A: Indica que el control no es aplicable a la organización.

Además, cada control incluye una **columna de observaciones** que permite a los usuarios hacer un **seguimiento** detallado del cumplimiento de cada control. Esta columna es fundamental para documentar el estado actual de implementación, proporcionar comentarios adicionales y destacar medidas resolutivas para abordar los riesgos asociados a cada control. De esta manera, la herramienta no solo facilita la evaluación del estado de seguridad actual, sino que también actúa como un registro dinámico de las acciones tomadas y las mejoras necesarias, ayudando a las organizaciones a mantener un enfoque proactivo en la gestión de la seguridad de la información.

ESTRUCTURA

La Herramienta está organizada en trece pestañas principales, cada una de las cuales aborda diferentes aspectos cruciales de la seguridad de la información. Estas pestañas están diseñadas para guiar a los usuarios a través de un proceso completo de evaluación y análisis. A continuación se describen de forma resumida las doce pestañas de formulario y la última pestaña de resultados:

Formularios

- **Desarrollo de la Cultura:** Evalúa la promoción y el fomento de una cultura de seguridad dentro de la organización.
- **Formación:** Examina la capacitación y concienciación en seguridad de la información para todos los miembros del personal.
- **Gestión de Terceros:** Revisa las políticas y prácticas para gestionar la seguridad en las relaciones con terceros.
- **Respuesta a Incidentes:** Evalúa la capacidad de la organización para detectar, responder y recuperarse de incidentes de seguridad.
- **Protección de Acceso:** Analiza los controles implementados para gestionar y asegurar el acceso a sistemas y datos.
- **Protección de Dispositivos:** Revisa las medidas de seguridad para proteger los dispositivos utilizados dentro de la organización.
- **Protección de Red:** Evalúa la seguridad de las redes internas y externas de la organización.
- **Seguridad Física:** Examina los controles físicos que protegen las instalaciones y equipos de la organización.
- **Protección en la Nube:** Analiza la seguridad de los servicios y datos alojados en la nube.
- **Protección Web:** Evalúa las medidas de seguridad implementadas para proteger las aplicaciones y servicios web.
- **Compartir Información:** Revisa las prácticas para compartir información de manera segura dentro y fuera de la organización.

Resultados

- **Análisis de Resultados:** Esta última pestaña está dedicada a presentar los resultados de la evaluación de manera clara y concisa. Aquí, los usuarios pueden ver un resumen detallado de las puntuaciones de madurez para cada una de las doce áreas evaluadas.

Ilustración 64.Ventana "Introducción" de la herramienta. Fuente: Elaboración propia.

7. CONCLUSIÓN

En este capítulo, se presentan las conclusiones obtenidas tras la elaboración de este Trabajo de Fin de Grado y se plantean posibles mejoras o trabajos futuros que podrían complementar este proyecto.

La creación de la herramienta de soporte para la evaluación del estado de madurez en la seguridad de la información en pequeñas y medianas empresas ha supuesto un gran reto en diversas áreas. En particular, la alineación de la herramienta con normativas y estándares de seguridad ha sido la tarea más costosa.

Para lograr este objetivo, se ha realizado un análisis exhaustivo sobre las normativas, estándares y entidades de seguridad ISO 27001, NIST, HIPAA, PCI DSS, CIS y ENISA. Controles que han sido seleccionados debido a su popularidad internacional y su éxito en su comercialización, como por ejemplo el NIST, que trata conceptos similares a los que se pueden encontrar en las guías del CNN-CERT e INCIBE. Cabe matizar que adicionalmente se ha buscado incluir estándares que abarcan aspectos específicos de la seguridad de la información sobre sectores críticos como el de la salud y el pago electrónico, ya que se detallan medidas de seguridad específicas sobre datos muy sensible que precisan de especial atención.

Por tanto, tras identificar las fuentes de información principales a utilizar como referencia, se ha realizado un trabajo de análisis sobre las áreas, objetivos y estructura de cada una de las matrices de controles utilizadas. Este trabajo se ha visto reflejado en los apartados "5.1 Selección de estándares de seguridad" y "5.2 Búsqueda de controles definidos por las normativas".

Adicionalmente, aprovechando el conocimiento obtenido sobre los controles en alcance, se ha buscado establecer métricas de evaluación de estos controles que puedan favorecer a las compañías de pequeño y mediano tamaño. En este apartado la entidad ENISA ha jugado un papel clave, ya que se han utilizado reportes oficiales de la organización para ello. En concreto, se han establecido las áreas de solución en la sección “5.3 Áreas de solución para Pymes” y se ha utilizado su taxonomía establecida para la definición de los riesgos de ciberseguridad “5.4 Clasificación de riesgos de ciberseguridad”. Estos dos apartados han sido de suma importancia para todo el desarrollo de la sección de evaluación de la herramienta.

Una vez establecidas las bases, se ha iniciado el proceso de desarrollo de la herramienta representado un gran coste de tiempo las tareas de formateo y clasificación de cada uno de los controles. Este proceso ha sido detallado en el apartado “6. DESARROLLO DE LA SOLUCIÓN” donde se ha especificado la metodología seguida para la asignación de cada control con su área de solución y los riesgos de seguridad que cubren su implementación. Para poder lograr este punto ha sido necesario la creación de tablas complejas que permitieran establecer métricas de evaluación sobre las áreas de solución y los riesgos de ciberseguridad establecidos por ENISA.

Paralelamente se ha diseñado la herramienta en Excel, optando por un formato de formulario que facilita la recopilación de información a analizar. El detalle de los formularios creados ha sido plasmado en la cuarta fase del punto de desarrollo. El diseño de estos formulario se ha basado en los controles seleccionados, es decir cada una de las respuestas dadas en el formulario hace referencia a un control en alcance y su respuesta condiciona el resultado final de la evaluación.

Hay que destacar que el trabajo de investigación realizado previo al desarrollo de la herramienta, ha servido de gran ayuda para establecer la primera toma de contacto con el mundo de la estandarización y las complejidades asociadas. En concreto, el apartado “2. ESTADO DEL ARTE” se ha analizado la base histórica de la necesidad de la estandarización de procesos de

seguridad de la información y ha servido de gran ayudad el análisis de trabajos académicos similares a los objetivos establecidos.

Seguidamente se ha realizado un análisis de las amenazas y macrotendencias de seguridad de la información en el punto "3.1 Contexto actual", donde se ha podido identificar las riesgos de seguridad más populares actualmente y las medidas de seguridad existentes para la mitigación de estos. Como conclusión de este apartado, se ha evidenciado que en la era actual la gestión del personal juega un gran riesgo debido al incremento de ataques *ransomware* y la efectividad de los ataques *phishing*.

Con el objetivo de comprender como estos cambios e incrementos de riesgos en la seguridad de la información están afectando a las empresas pequeñas y medianas, se ha analizado diversos reportes de seguridad de la información actuales relacionados con este tema. Como resultado se ha identificado que las principales barreras existentes son la capacidad de recursos, tanto económicos como de personal, al igual que una falta de concienciación sobre el impacto de las brechas de seguridad. Problemas que se pretenden cubrir parcialmente con la herramienta desarrollada.

En resumen, el trabajo realizado ha representado un gran reto personal, ya que la temática seleccionada se encuentra en pleno auge y crecimiento, existiendo una gran cantidad de información que a corto plazo es difícil de comprender. De esta misma forma que a mí me ha supuesto un reto la gestión de la información existente, se ha creado la presente herramienta en un formato de formulario, para facilitar el entendimiento de conceptos estandarizados mediante una interfaz sencilla, a la vez que permite evaluar el estado de madurez de una compañía y las repercusiones de no establecer controles adecuados.

7.1 Puntos de mejora

Para optimizar y ampliar el alcance del Trabajo de Fin de Grado, se identifican varios puntos de mejora que pueden fortalecer el enfoque del proyecto.

Una mejora significativa sería incorporar a la herramienta una capacidad de sugerir puntos de mejora personalizada en base a las evaluaciones realizadas por la herramienta. Actualmente, la herramienta en Excel permite a las compañías evaluar su estado de madurez en términos de seguridad de la información mediante un conjunto de formularios y preguntas estructuradas. Sin embargo, el siguiente paso en la evolución de esta herramienta sería integrar un módulo de análisis que, tras la evaluación, ofrezca recomendaciones específicas y accionables. Este módulo podría utilizar algoritmos de análisis de datos para identificar las áreas más débiles de la empresa y sugerir mejoras concretas, tales como la implementación de nuevos controles de seguridad, la capacitación del personal en ciberseguridad, o la actualización de políticas y procedimientos de seguridad.

Para mejorar la accesibilidad y la comodidad del proceso de evaluación, la herramienta podría ser desarrollada e implementada en un portal web. Esto no solo haría más cómodo el apartado de encuestas, sino que también mejoraría la visualización de los resultados. Un portal web permitiría a las compañías acceder a la herramienta desde cualquier dispositivo con conexión a internet, eliminando las limitaciones de una solución basada en Excel. Además, una plataforma en línea podría ofrecer una interfaz más intuitiva y atractiva, facilitando la navegación a través de los distintos módulos de evaluación y proporcionando una experiencia de usuario más fluida.

7.2 Propuestas de trabajos posteriores

Un proyecto futuro podría centrarse en la mejora de la presentación de datos en la herramienta de evaluación de seguridad de la información. Este proyecto podría desarrollar nuevos métodos de visualización de datos que faciliten la interpretación de los resultados de la evaluación. Por ejemplo, se podrían implementar gráficos interactivos, dashboards personalizables y reportes dinámicos que muestren los resultados de manera clara y comprensible. Además, se podrían explorar técnicas avanzadas de visualización, como mapas de calor y diagramas, para representar de manera efectiva las relaciones y flujos de datos dentro de la empresa.

Otro proyecto interesante sería la creación de un sistema automatizado de elaboración de informes de recomendaciones. Este sistema podría utilizar algoritmos de análisis de datos para generar informes detallados que incluyan no solo los resultados de la evaluación, sino también recomendaciones personalizadas para mejorar la seguridad de la información. Estos informes podrían ofrecer un análisis en profundidad de las áreas más débiles, sugerir medidas correctivas específicas y proporcionar una hoja de ruta para la implementación de mejoras. Además, los informes podrían ser personalizables según las necesidades de cada empresa, permitiendo a los usuarios seleccionar los aspectos más relevantes para su contexto particular.

Adicionalmente, el trabajo realizado en este TFG puede servir como base para desarrollar herramientas similares que ayuden a las compañías a cumplir con normativas específicas que empiecen a ser obligatorias. Por ejemplo, un proyecto podría enfocarse en el desarrollo de una herramienta para el cumplimiento de la Ley de Seguridad de la Información de un país específico o nuevas regulaciones emergentes en ciberseguridad. Este proyecto implicaría adaptar la estructura y los cuestionarios de la herramienta existente para alinearse con los requisitos específicos de la nueva normativa, proporcionando una guía paso a paso para que las empresas puedan asegurar su conformidad.

ANEXO ODS

OBJETIVOS DE DESARROLLO SOSTENIBLE

Grado de relación del trabajo con los Objetivos de Desarrollo Sostenible (ODS).

Objetivos de Desarrollo Sostenibles	Alto	Medio	Bajo	No Procede
ODS 1. **Fin de la pobreza.**				X
ODS 2. **Hambre cero.**				X
ODS 3. **Salud y bienestar.**			X	
ODS 4. **Educación de calidad.**	X			
ODS 5. **Igualdad de género.**				X
ODS 6. **Agua limpia y saneamiento.**				X
ODS 7. **Energía asequible y no contaminante.**				X
ODS 8. **Trabajo decente y crecimiento económico.**	X			
ODS 9. **Industria, innovación e infraestructuras.**	X			
ODS 10. **Reducción de las desigualdades**.			X	
ODS 11. **Ciudades y comunidades sostenibles**.				X
ODS 12. **Producción y consumo responsables.**				X
ODS 13. **Acción por el clima.**				X
ODS 14. **Vida submarina.**				X
ODS 15. **Vida de ecosistemas terrestres.**				X
ODS 16. **Paz, justicia e instituciones sólidas.**		X		
ODS 17. **Alianzas para lograr objetivos.**			X	

Reflexión sobre la relación del TFG/TFM con los ODS y con el/los ODS más relacionados.

El Trabajo de Fin de Grado (TFG) desarrollado aborda un tema crucial y contemporáneo: la ciberseguridad en pequeñas y medianas empresas. En un contexto de creciente digitalización, estas empresas enfrentan desafíos significativos para proteger su información y sistemas. A través del desarrollo de una herramienta accesible para evaluar y mejorar su nivel de seguridad de la información, el TFG se alinea con varias metas establecidas por los Objetivos de Desarrollo Sostenible (ODS), a pesar de no estar directamente relacionado con todos ellos.

Relación con el ODS 8: Trabajo Decente y Crecimiento Económico

El ODS 8 busca promover el crecimiento económico inclusivo y sostenible, el empleo pleno y productivo, y el trabajo decente para todos. La ciberseguridad es un componente esencial para la estabilidad económica de las empresas. La falta de medidas adecuadas de ciberseguridad puede llevar a pérdidas financieras significativas, afectando negativamente a las empresas y, por ende, a la economía en general. Al proporcionar una herramienta que ayuda a evaluar y mejorar su seguridad de la información, el TFG contribuye a la protección de estos negocios, promoviendo un entorno más seguro y estable para el crecimiento económico.

Relación con el ODS 9: Industria, Innovación e Infraestructura

El ODS 9 se centra en construir infraestructuras resilientes, promover la industrialización inclusiva y sostenible, y fomentar la innovación. La herramienta desarrollada en este TFG está alineada con normativas de seguridad ampliamente reconocidas, como ISO 27001, NIST, HIPAA, PCI DSS y CIS. Esto no solo asegura la adopción de estándares internacionales, sino que también fomenta la innovación en la gestión de la ciberseguridad dentro de las empresas. Al mejorar su infraestructura de seguridad, las empresas están mejor preparadas para enfrentar y recuperarse de posibles ciberataques, lo que es crucial para la resiliencia y la sostenibilidad de sus operaciones.

Relación con el ODS 4: Educación de Calidad

Aunque no es el objetivo principal, el TFG también toca aspectos del ODS 4, que busca garantizar una educación inclusiva y equitativa de calidad y promover oportunidades de aprendizaje permanente para todos. La herramienta no solo proporciona una evaluación de la seguridad de la información, sino que también fomenta la concienciación y la formación continua en ciberseguridad. Al hacerlo, se promueve un entorno de aprendizaje dentro de las empresas, ayudando a los empleados a entender mejor las amenazas cibernéticas y las medidas de protección necesarias.

Relación con el ODS 16: Paz, Justicia e Instituciones Sólidas

El ODS 16 promueve sociedades pacíficas e inclusivas para el desarrollo sostenible, proporcionando acceso a la justicia para todos y construyendo instituciones eficaces, responsables e inclusivas. La ciberseguridad es fundamental para mantener la integridad y la confianza en las instituciones y negocios. Al ayudar a las compañías a protegerse contra ciberataques, el TFG contribuye a la creación de instituciones más seguras y resilientes, lo que es esencial para la paz y la justicia en la sociedad.

Reflexión sobre la falta de relación con otros ODS

Es cierto que el TFG no se relaciona directamente con algunos ODS, como aquellos enfocados en la salud y el bienestar (ODS 3), el hambre cero (ODS 2), o la vida submarina (ODS 14), entre otros. Sin embargo, esto no disminuye su importancia. La ciberseguridad es un tema transversal que, aunque no impacte directamente en todos los ODS, es fundamental para el desarrollo sostenible en el ámbito digital y económico.

Impacto indirecto en otros ODS

Aunque no de manera directa, el fortalecimiento de la ciberseguridad en las PYMES puede tener impactos positivos indirectos en otros ODS. Por ejemplo, el ODS 10 (Reducción de las Desigualdades) pueden beneficiarse indirectamente, ya que las empresas más seguras y resilientes pueden ofrecer empleo más estable y contribuir a una economía más equitativa. Además, la seguridad digital puede ayudar a prevenir el fraude y otros delitos cibernéticos, promoviendo así un entorno más justo y seguro para todos.

En conclusión, aunque el TFG desarrollado sobre ciberseguridad en PYMES no se relaciona directamente con todos los ODS, sí tiene una conexión significativa con varios de ellos, especialmente aquellos enfocados en el crecimiento económico sostenible, la innovación y la infraestructura, y la educación de calidad. La ciberseguridad es una pieza clave en el entorno digital moderno y su mejora contribuye de manera importante al desarrollo sostenible y a la creación de un mundo más seguro y equitativo. Al proporcionar herramientas prácticas y accesibles para que las empresas en crecimiento fortalezcan su postura de seguridad, este TFG no solo aborda un desafío crítico actual, sino que también contribuye a la realización de varios objetivos globales importantes.

ANEXO Historia

Segunda Guerra Mundial

La historia de los estándares de seguridad informática presenta algunas similitudes con el establecimiento de estándares técnicos, desarrollándose en contextos únicos y con desafíos particulares. Aunque los estándares de seguridad informática han sido menos influyentes y útiles en su inicio que los estándares técnicos, su evolución ha estado marcada por hitos significativos(Yost 2007).

Durante la década de 1950, tras la segunda guerra mundial, algunos especialistas en informática del gobierno norteamericano se preocuparon por la posibilidad de que existieran espías que pudieran capturar y descifrar emisiones de los ordenadores principales. Por aquel momento los ordenadores que se utilizaban emitían ciertos niveles de radiación electromecánica que dependiendo de la radiación electrónica y la distancia del potencial espía electrónico, eran capaces de descifrar estas señales. Hacia finales de la década de 1950, el gobierno estableció el primer estándar, denominado TEMPEST, para establecer el nivel de radiación que seguía siendo aceptable cuando se procesaba información clasificada. TEMPEST se convirtió en un término amplio para la tecnología que suprimía las emanaciones de señales de equipos electrónicos(Ulas et al. 2014).

Inicio de los Ordenadores Digitales

A finales de la década de 1950, el aislamiento físico de las máquinas para proteger sus datos y programas comenzó gradualmente a desaparecer debido a la aparición de la tecnología de redes de ordenadores digitales, alterando para siempre el panorama de la seguridad informática. Lo que llevo gradualmente a los orígenes de la creación de la red ARPANET, descubrimiento que conllevó un dilema con respecto a la seguridad de la informática digital para la comunidad de defensa militar. Tal fue el grado de inquietud que la Junta de Ciencia de la Defensa Americana estableció un grupo de trabajo en octubre de 1967 para examinar los problemas de seguridad con dichos sistemas informáticos. Este grupo reconoció la amplia gama de sistemas de hardware y software ya existentes y buscó proporcionar una compilación general de técnicas y procedimientos que pudieran ser flexibles y ampliamente útiles para proteger la información militar confidencial(Redmond, Smith 2000).

El 11 de febrero de 1970, la Junta de Ciencia de la Defensa completó su informe clasificado, titulado "Computer Systems: Report of Defense Science Board Task Force on Computer Security"(*Defense Science Board Task Force on Computer Security, Security Controls for Computer Systems: Report of the Defense Science Board Task Force on Computer Security. Confidential. | National Security Archive*). Este informe de la Junta de Ciencia de la Defensa fue el estudio más importante y exhaustivo sobre cuestiones técnicas y operativas relacionadas con los sistemas informáticos seguros de la época. En el documento se detalla como por naturaleza de los sistemas informáticos, estos conllevaban ciertas vulnerabilidades relacionadas con el factor humano, el hardware y el software. En general, el informe destacó cómo la tecnología había superado el conocimiento y la complejidad que existía para implementar controles adecuados que garantizaran la seguridad de la información militar confidencial(*Defense Science Board Task Force on Computer Security, Security Controls for Computer Systems: Report of the Defense Science Board Task Force on Computer Security. Confidential. | National Security Archive*).

Evolución de la Seguridad Informática: De la Militarización a la Protección de datos Sensibles

Con el paso de los años esta inquietud militar por la seguridad de los sistemas informáticos se trasladó a otros contextos, identificando nuevas amenazas más complejas alejadas del entorno militar y la clasificación de la información.

A principios de 1972, James P. Anderson, un consultor informático de Fort Washington, Pennsylvania, y su grupo publicaron el informe “Computer Security technology Planning Study” donde se realizó una evaluación desalentadora de la situación, indicando que no había un sistema actual que pudiera operar de manera segura y tener múltiples niveles de acceso diferencial. En el centro del problema estaba el hecho de que los sistemas de intercambio de recursos dependían de los sistemas operativos para mantener su separación, y los usuarios comúnmente programaban estos sistemas operativos para realizar su trabajo. En esencia, los usuarios con diferentes autorizaciones de seguridad accedían al mismo almacenamiento primario y, por lo tanto, tenían acceso a los mismos datos(Anderson).

A modo de solución al problema de seguridad identificado por el grupo liderado por Anderson, se introdujo un concepto innovador en el ámbito de la seguridad informática: el monitor de referencia(Anderson). Este monitor tenía como objetivo principal hacer cumplir las relaciones de acceso autorizado entre sujetos y objetos en los sistemas informáticos. En otras palabras, se buscaba garantizar que solo las personas autorizadas pudieran acceder a la información adecuada en los sistemas.

Adicionalmente, se pretendía implementar un sistema de "no lectura ascendente" para los datos clasificados(Anderson). Esto significaba que la información clasificada solo podía ser accedida por aquellos usuarios que tenían el nivel de autorización necesario. De esta manera, se buscaba prevenir filtraciones de información confidencial y proteger la integridad de los datos sensibles.

El Libro Naranja: Estándares de Seguridad en la Era Militar de la Informática

Durante la década de 1970, el ámbito militar reconoció la necesidad imperante de contar con criterios estándar de seguridad informática para evaluar los sistemas. Este reconocimiento fue el resultado de un contexto en el que la tecnología informática estaba adquiriendo una importancia cada vez mayor en las operaciones militares y gubernamentales.

En respuesta a esta necesidad, el National Computer Security Center (NCSC) y MITRE colaboraron en la creación de un documento: el "Department of Defense Trusted Computer System Evaluation Criteria" (TSEC), conocido comúnmente como "El Libro Naranja" debido al color de su portada. Este libro se convirtió en la piedra angular de la seguridad informática en el ámbito militar y gubernamental(US Department of Defense 1985).

En el libro se establecieron estándares rigurosos para la seguridad de los sistemas informáticos, con el objetivo de estandarizar los requisitos de adquisición gubernamentales. Proporcionó una estructura para que los fabricantes evaluaran y midieran la seguridad de sus sistemas, permitiendo designar diferentes niveles de seguridad y probar si un sistema cumplía con un nivel específico.

Evolución de los Estándares de Seguridad Informática: De TCSEC a ITSEC y Más Allá

No obstante, la evolución hacia un mundo interconectado, impulsada por la transformación de redes como la ARPANET en la Internet que conocemos hoy en día, ha tenido un impacto significativo en los modelos de seguridad informática. En este contexto, se cuestionó la efectividad del modelo de seguridad utilizado por el ejército, conocido como el libro naranja (TCSE), argumentando que era insuficiente para garantizar la confidencialidad e integridad en entornos comerciales(Clark, Wilson 1987).

En paralelo a estos desarrollos, a nivel internacional se llevó a cabo una intensa investigación y establecimiento de estándares en países europeos. Estos países lideraron la creación de estándares reconocidos a nivel mundial bajo el nombre de Criterios de Evaluación de Seguridad de Tecnologías de la Información (ITSEC)(*ITSEC - Information Technology Security Evaluation Criteria - CCN-STIC 401*). Aunque estos estándares guardaban similitudes con los delineados en los Estados Unidos en el TCSEC, se llevaron a cabo investigaciones y proyectos innovadores para aplicar estándares de seguridad a nuevos tipos de sistemas.

En la primera mitad de la década de 1980, se reconoció la creciente eficiencia que podría lograrse mediante la cooperación internacional en investigación, establecimiento de estándares y procesos de adquisición en el campo de la seguridad informática. Como resultado de este reconocimiento, se llevó a cabo un esfuerzo para reunir a varias naciones aliadas con el objetivo de establecer un conjunto común de estándares de seguridad informática a nivel global. Este esfuerzo culminó en la creación de un conjunto de estándares internacionales que superaron al Libro Naranja o TCSEC en los Estados Unidos, al ITSEC en los países europeos y al Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) (*ITSEC - Information Technology Security Evaluation Criteria - CCN-STIC 401*).

Estos estándares creados fueron plasmados en varios libros con diferentes colores, comúnmente conocidos como la serie Rainbow, que modificaron y ampliaron el TCSEC para una mayor especialización y buscaron abordar las necesidades de seguridad dentro del entorno cambiante de la tecnología informática, de software y de redes. Al igual que el TCSEC, los libros posteriores tenían como objetivo proporcionar un estándar para los fabricantes en cuanto a características de seguridad y niveles de garantía para ofrecer sistemas ampliamente disponibles que cumplieran con ciertos requisitos de "confianza" para aplicaciones sensibles(*Rainbow Series and Related Documents*).

Privacidad en la Era Digital: Desafíos y Respuestas en el Sector de la Salud

La creciente presencia de enormes bancos de datos de información sobre individuos avivó la controversia sobre el papel del gobierno como organismo encargado de la gestión de los datos. Esta preocupación se intensificó con la proliferación de redes informáticas comerciales, que facilitan la infiltración de sistemas corporativos y gubernamentales. En respuesta a estos desafíos, en Gran Bretaña, el gobierno encargó que se evaluara y definiera los estándares de seguridad para la información clínica de pacientes en la red del Servicio Nacional de Salud (NHS)(*Cyber, information governance and data protection guidance*).

A diferencia de los enfoques centrados en la seguridad nacional, los protocolos y estándares para sistemas seguros de información médica se desarrollaron con un enfoque ético centrado en el paciente. Este cambio en la perspectiva ha sido influenciado tanto por grupos nacionales como internacionales. Esto se puede ver reflejado en el caso del grupo de Estandarización Europea para la Seguridad y Privacidad de la Informática Médica (CEN TC 251/WG6)(*About CEN/TC 251 – Ehealth standards*), que ha promovido el cifrado de los datos médicos de salud de los pacientes en redes más amplias.

En 1996, el Dr. Ross Anderson propuso un conjunto de reglas destinadas a salvaguardar el principio fundamental del consentimiento del paciente en el contexto de los sistemas informáticos empleados por el Servicio Nacional de Salud (NHS) en Gran Bretaña(*Security Engineering - A Guide to Building Dependable Distributed Systems*). Estas reglas fueron concebidas con el objetivo de proteger la privacidad de los pacientes, independientemente de los detalles específicos de los sistemas informáticos utilizados en el NHS.

El enfoque de Anderson no se limitó a la identificación de problemas, sino que también ofreció soluciones prácticas. Proporcionó modelos y protocolos que permitieron a la comunidad médica responder de manera inicial a las preocupaciones cada vez mayores sobre la violación de la privacidad del paciente debido a la implementación de sistemas informáticos en el NHS.

Estas medidas representaron un intento significativo de establecer pautas claras y sólidas para garantizar que el consentimiento del paciente y la privacidad médica se mantuvieran como prioridades fundamentales en el contexto del avance tecnológico en la atención médica. El trabajo de Anderson sentó las bases para abordar los desafíos emergentes relacionados con la seguridad y la privacidad de la información médica en entornos de atención de la salud cada vez más digitalizados(*Security Engineering - A Guide to Building Dependable Distributed Systems*).

A medida que las inquietudes por la privacidad han aumentado, también ha crecido la preocupación pública por la privacidad, debido al aumento de los ordenadores personales en la red, los hackers y los criminales informáticos.

Bibliografía

5. National Cybersecurity Strategy Good Practice, *NCS guide* [en línea]. Recuperado a partir de : https://ncsguide.org/the-guide/good-practice/ [accedido 14 enero 2024].

14:00-17:00, 2023. ISO/IEC 27001:2022. *ISO* [en línea]. 2 febrero 2023. Recuperado a partir de : https://www.iso.org/standard/27001 [accedido 26 noviembre 2023].

2024 Cisco Cybersecurity Readiness Index, 2024 [en línea]. CISCO. Recuperado a partir de : https://newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/documents/Cisco_Cybersecurity_Readiness_ES.pdf

ABDULKADER, Sarah, ATIA, Ayman y MOSTAFA, Mostafa-Sami, 2015. Authentication systems: principles and threats. *Computer and Information Science*. Vol. 8. DOI 10.5539/cis.v8n3p155.

About CEN/TC 251 – Ehealth standards, [en línea]. Recuperado a partir de : https://www.ehealth-standards.eu/about/ [accedido 29 marzo 2024].

AGUIAR, Alberto R., 2024. Así ha sido el «ciberataque» a Orange que ha dejado a muchos españoles sin internet: por qué el primer gran incidente de 2024 es tan preocupante. *Business Insider España* [en línea]. 4 enero 2024. Recuperado a partir de : https://www.businessinsider.es/por-que-ciberataque-orange-mas-preocupante-parece-1354237 [accedido 14 enero 2024].

ALDER, Steve, 2022. What is HIPAA? *HIPAA Journal* [en línea]. 23 febrero 2022. Recuperado a partir de : https://www.hipaajournal.com/what-is-hipaa/ [accedido 26 noviembre 2023].

ALDER, Steve, 2023. HIPAA Risk Assessment - updated for 2024. *HIPAA Journal* [en línea]. 1 diciembre 2023. Recuperado a partir de : https://www.hipaajournal.com/hipaa-risk-assessment/ [accedido 3 marzo 2024].

ANDERSON, James P. Computer Security Technology Planning Study (Volume I). .

ARORA, Varun. Comparing different information security standards: COBIT vs. ISO 2700. .

BOE.es - DOUE-L-2016-81297 Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión, [en línea]. Recuperado a partir de : https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-81297 [accedido 7 enero 2024].

CARDINAL, Laura B., SITKIN, Sim B. y LONG, Chris P., 2004. Balancing and Rebalancing in the Creation and Evolution of Organizational Control. *Organization Science*. DOI 10.1287/orsc.1040.0084.

CATAL, Cagatay et al., 2022. Applications of deep learning for phishing detection: a systematic literature review. *Knowledge and Information Systems*. Vol. 64, n.º 6, pp. 1457-1500. DOI 10.1007/s10115-022-01672-x.

CICHONSKI, Paul R. et al., 2012. Computer Security Incident Handling Guide. *NIST* [en línea]. Recuperado a partir de : https://www.nist.gov/publications/computer-security-incident-handling-guide [accedido 21 octubre 2023]. Last Modified: 2021-05-04T09:18-04:00

CIS Controls, *CIS* [en línea]. Recuperado a partir de : https://www.cisecurity.org/controls/ [accedido 26 noviembre 2023].

CIS Controls Version 8, *CIS* [en línea]. Recuperado a partir de : https://www.cisecurity.org/controls/v8/ [accedido 3 marzo 2024].

CLARK, David D. y WILSON, David R., 1987. A Comparison of Commercial and Military Computer Security Policies. En : *1987 IEEE Symposium on Security and Privacy*, pp. 184-184. Oakland, CA, USA : IEEE. abril 1987. ISBN 978-0-8186-0771-4. DOI 10.1109/SP.1987.10001.

COMPUTER SECURITY DIVISION, Information Technology Laboratory, 2021. Control Catalog and Baselines as Spreadsheets | CSRC. *CSRC | NIST* [en línea]. 26 enero 2021. Recuperado a partir de : https://csrc.nist.gov/news/2021/control-catalog-and-baselines-as-spreadsheets [accedido 9 diciembre 2023].

Cyber, information governance and data protection guidance, *NHS England Digital* [en línea]. Recuperado a partir de : https://digital.nhs.uk/services/internet-first/internet-first-guidance/cyber-information-governance-and-data-protection-guidance [accedido 29 marzo 2024].

DBIR Report 2023 - Master's Guide, *Verizon Business* [en línea]. Recuperado a partir de : https://www.verizon.com/business/resources/reports/dbir/2023/master-guide/ [accedido 21 octubre 2023].

DBIR Report 2023 - Small Medium Business (SMBs) Data Breaches, *Verizon Business* [en línea]. Recuperado a partir de : https://www.verizon.com/business/resources/reports/dbir/2023/small-business-data-breaches/ [accedido 25 noviembre 2023].

Defense Science Board Task Force on Computer Security, Security Controls for Computer Systems: Report of the Defense Science Board Task Force on Computer Security. Confidential. | National Security Archive, [en línea]. Recuperado a partir de : https://nsarchive.gwu.edu/document/21583-document-01-defense-science-board-task-force [accedido 28 marzo 2024].

DigitalOcean, 2023. *Small businesses and cybersecurity* [en línea]. DigitalOcean. Recuperado a partir de : https://anchor.digitalocean.com/rs/113-DTN-266/images/Security-Report_DigitalOcean.pdf

Document Library, *PCI Security Standards Council* [en línea]. Recuperado a partir de : https://www.pcisecuritystandards.org/document_library/ [accedido 3 marzo 2024].

ENISA Cybersecurity guide for SMEs_ES, *ENISA* [en línea]. Recuperado a partir de : https://www.enisa.europa.eu/publications/report-files/smes-leaflet-translations/enisa-cybersecurity-guide-for-smes_es.pdf/view [accedido 30 marzo 2024].

EUROPEAN FOUNDATION FOR THE IMPROVEMENT OF LIVING AND WORKING CONDITIONS., 2021. *The digital age: implications of automation, digitisation and platforms for work and employment.* [en línea]. LU : Publications Office. Recuperado a partir de : https://data.europa.eu/doi/10.2806/288 [accedido 7 enero 2024].

Health Insurance Portability and Accountability Act of 1996 (HIPAA) | CDC, 2022 [en línea]. Recuperado a partir de : https://www.cdc.gov/phlp/publications/topic/hipaa.html [accedido 26 noviembre 2023].

HIPAA History, *HIPAA Journal* [en línea]. Recuperado a partir de : https://www.hipaajournal.com/hipaa-history/ [accedido 26 noviembre 2023].

HOLLIS, Scott y ZAHN, David, 2017. ICS Cybersecurity: Protecting the Industrial Endpoints That Matter Most. .

Industria de Tarjetas de Pago (PCI) Norma de seguridad de datos, 2016. PCI. PCI . Recuperado a partir de : https://listings.pcisecuritystandards.org/documents/PCI_DSS_v3-2es-LA.pdf

ISO 27001 controls – A guide to implementing and auditin, [en línea]. ISBN 978-1-78778-146-7. Recuperado a partir de : https://learning.oreilly.com/library/view/iso-27001-controls/9781787781467/xhtml/Chapter_02.html [accedido 3 marzo 2024].

ISO27000 and Information Security: A Combined Glossary, [en línea]. ISBN 978-1-84928-165-2. Recuperado a partir de : https://learning.oreilly.com/library/view/iso27000-and-information/9781849281652/ [accedido 21 octubre 2023].

ITIL - ITIL, [en línea]. Recuperado a partir de : https://www.itlibrary.org/ [accedido 14 enero 2024].

ITSEC - Information Technology Security Evaluation Criteria - CCN-STIC 401, [en línea]. Recuperado a partir de : https://www.dit.upm.es/~pepe/401/index.html#!5112 [accedido 28 marzo 2024].

JIMÉNEZ GÓMEZ, Pablo, 2019. *Implantación del Reglamento General de Protección de Datos y adaptación al Esquema Nacional de Seguridad de manera integrada en el Sistema de Gestión de Seguridad de la Información (SGSI) basado en la ISO 27001* [en línea]. Proyecto/Trabajo fin de carrera/grado . Universitat Politècnica de València. Recuperado a partir de : https://riunet.upv.es/handle/10251/127849 [accedido 14 abril 2024]. Accepted: 2019-10-09T07:21:51Z

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, 2017 [en línea]. Recuperado a partir de : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN%3A2017%3A450%3AFIN [accedido 7 enero 2024].

KAMBOURAKIS, G., NEISSE, R. y NAI-FOVINO, I, 2021. *Information security in the age of EUInstitutions digitalisation, a landscape analysis* [en línea]. European Commission. JRC125214. Recuperado a partir de : https://commission.europa.eu/system/files/2022-03/jrc_study_en.pdf

Key Performance Indicators for Security Governance, Part 2: Security Reporting for Senior Management, *ISACA* [en línea]. Recuperado a partir de : https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-2 [accedido 14 enero 2024].

La década digital de Europa: Objetivos para 2030 Comisión Europea, [en línea]. Recuperado a partir de : https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_es [accedido 7 enero 2024].

Microsoft Digital Defense Report 2022 | Microsoft Security, [en línea]. Recuperado a partir de : https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022 [accedido 7 enero 2024].

Ministerio para la Transformación Digital y de la Función Pública - Instituto Europeo de Normas de Telecomunicaciones (ETSI), [en línea]. Recuperado a partir de : https://avancedigital.mineco.gob.es/es-es/servicios/normalizacion/seguimiento/paginas/seguimiento-etsi.aspx [accedido 14 enero 2024].

MOALLEM, Abbas, 2021. *Understanding Cybersecurity Technologies: A Guide to Selecting the Right Cybersecurity Tools*. CRC Press. ISBN 978-1-00-050615-0. Google-Books-ID: sO5LEAAAQBAJ

MONTÓ, Arnedo y JOSÉ, Pedro, 2017. *Esquema Nacional de Seguridad: protección de una infraestructura crítica hospitalaria* [en línea]. Proyecto/Trabajo fin de carrera/grado . Universitat Politècnica de València. Recuperado a partir de : https://riunet.upv.es/handle/10251/86739 [accedido 14 abril 2024]. Accepted: 2017-09-07T16:09:22Z

NIST, CSRC Content. incident - Glossary | CSRC. [en línea]. Recuperado a partir de : https://csrc.nist.gov/glossary/term/incident [accedido 25 junio 2024 a].

NIST, CSRC Content. breach - Glossary | CSRC. [en línea]. Recuperado a partir de : https://csrc.nist.gov/glossary/term/breach [accedido 25 junio 2024 b].

NIST Special Publication 800-series General Information, 2018*NIST* [en línea]. Recuperado a partir de : https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information [accedido 26 noviembre 2023]. Last Modified: 2018-05-21T13:51-04:00

OASIS Open Home, *OASIS Open* [en línea]. Recuperado a partir de : https://www.oasis-open.org/ [accedido 14 enero 2024].

¿Qué es la seguridad de red? | IBM, [en línea]. Recuperado a partir de : https://www.ibm.com/es-es/topics/network-security [accedido 7 enero 2024].

¿Qué es un sistema de prevención de intrusiones (IPS)? | IBM, [en línea]. Recuperado a partir de : https://www.ibm.com/es-es/topics/intrusion-prevention-system [accedido 7 enero 2024].

Quick Start Guide, 2023*NIST* [en línea]. Recuperado a partir de : https://www.nist.gov/cyberframework/getting-started/quick-start-guide [accedido 7 enero 2024]. Last Modified: 2023-06-08T09:44-04:00

Rainbow Series and Related Documents, [en línea]. Recuperado a partir de : https://irp.fas.org/nsa/rainbow.htm [accedido 29 marzo 2024].

REDMOND, Kent C. y SMITH, Thomas M., 2000. *From Whirlwind to MITRE: The R&D Story of The SAGE Air Defense Computer*. MIT Press. ISBN 978-0-262-26426-6. Google-Books-ID: nERmDQAAQBAJ

REVERT ENGUIX, Jorge, 2019. *Esquema Nacional de Seguridad: protección de una infraestructura crítica del sector administración* [en línea]. Proyecto/Trabajo fin de carrera/grado . Universitat Politècnica de València. Recuperado a partir de : https://riunet.upv.es/handle/10251/127166 [accedido 14 abril 2024]. Accepted: 2019-10-03T12:31:56Z

SCARFONE, Karen y HOFFMAN, Paul, 2009. *Guidelines on Firewalls and Firewall Policy*. National Institute of Standards and Technology. NIST Special Publication (SP) 800-41 Rev. 1. DOI 10.6028/NIST.SP.800-41r1.

Security at the Commission - European Commission, [en línea]. Recuperado a partir de : https://commission.europa.eu/about-european-commission/service-standards-and-principles/security-commission_en [accedido 7 enero 2024].

Security Engineering - A Guide to Building Dependable Distributed Systems, [en línea]. Recuperado a partir de : https://www.cl.cam.ac.uk/~rja14/book.html [accedido 29 marzo 2024].

Seguridad de la red: ¿Qué es, cómo funciona y qué tipos existen?, [en línea]. Recuperado a partir de : https://www.deltaprotect.com/blog/seguridad-de-la-red [accedido 7 enero 2024].

Seguridad y biometría | Ciudadanía | INCIBE, [en línea]. Recuperado a partir de : https://www.incibe.es/ciudadania/blog/seguridad-y-biometria [accedido 3 diciembre 2023].

SERRAT TRONCHO, Alba, 2021. *Guía para la Adecuación de Organizaciones al Esquema Nacional de Seguridad* [en línea]. Proyecto/Trabajo fin de carrera/grado . Universitat Politècnica de València. Recuperado a partir de : https://riunet.upv.es/handle/10251/171643 [accedido 14 abril 2024]. Accepted: 2021-09-08T10:46:26Z

Sobre la Unión Internacional de Telecomunicaciones (UIT), *ITU* [en línea]. Recuperado a partir de : https://www.itu.int:443/es/about/Pages/default.aspx [accedido 14 enero 2024].

Soluciones de seguridad: Network Detection & Response, 2021*Satec* [en línea]. Recuperado a partir de : https://www.satec.es/blog/2021/03/01/soluciones-avanzadas-de-seguridad-network-detection-response/ [accedido 7 enero 2024].

SPENCER, Traci, 2019. What Is the NIST SP 800-171 and Who Needs to Follow It? *NIST* [en línea]. Recuperado a partir de : https://www.nist.gov/blogs/manufacturing-innovation-blog/what-nist-sp-800-171-and-who-needs-follow-it-0 [accedido 26 noviembre 2023]. Last Modified: 2019-11-14T21:05-05:00

Standards for Cyber Security, *ENISA* [en línea]. Recuperado a partir de : https://www.enisa.europa.eu/publications/articles/standards-for-cyber-security/view [accedido 7 enero 2024].

The Evolution of Security Operations and Strategies for Building an Effective SOC, *ISACA* [en línea]. Recuperado a partir de : https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/the-evolution-of-security-operations-and-strategies-for-building-an-effective-soc [accedido 14 enero 2024].

The Guide: CIS Security Controls, *Fresh Security* [en línea]. Recuperado a partir de : https://freshsec.com/cis-controls/#5f5c4c59ca83 [accedido 26 noviembre 2023].

The VERIS Framework, [en línea]. Recuperado a partir de : https://verisframework.org/index.html [accedido 21 octubre 2023].

Threat Taxonomy, *ENISA* [en línea]. Recuperado a partir de : https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view [accedido 1 abril 2024].

ULAS, Cihan et al., 2014. Automatic Tempest Test and Analysis System Design. *International Journal on Cryptography and Information Security*. Vol. 4, pp. 1-12. DOI 10.5121/ijcis.2014.4301.

UNIDO. *MAKING STANDARDS WORK FOR SUSTAINABLE DEVELOPMENT*. . United Nations Industrial Development Organization.

US DEPARTMENT OF DEFENSE, 1985. Department of Defense Trusted Computer System Evaluation Criteria. En : US DEPARTMENT OF DEFENSE (ed.), *The 'Orange Book' Series*, pp. 1-129. London : Palgrave Macmillan UK. ISBN 978-0-333-53947-7. DOI 10.1007/978-1-349-12020-8_1.

Web Standards, *W3C* [en línea]. Recuperado a partir de : https://www.w3.org/standards/ [accedido 14 enero 2024].

What is encryption? How it works + types of encryption – Norton, [en línea]. Recuperado a partir de : https://us.norton.com/blog/privacy/what-is-encryption [accedido 2 diciembre 2023].

YOST, Jeffrey R., 2007. 20 - A history of computer security standards. En : LEEUW, Karl De y BERGSTRA, Jan (eds.), *The History of Information Security*, pp. 595-621. Amsterdam : Elsevier Science B.V. ISBN 978-0-444-51608-4. DOI 10.1016/B978-044451608-4/50021-3.