Universidad de Sevilla

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA INFORMÁTICA

GRADO EN INGENIERÍA INFORMÁTICA DEL SOFTWARE

TRABAJO FIN DE GRADO

Desarrollo de una auditoría de ciberseguridad para PYMEs

Realizado por:

Álvaro Ruiz Gutiérrez

Dirigido por:

Alejandro Carrasco Muñoz

Departamento:

Tecnología Electrónica

2024/2025

Índice

1. Introducción **7**
1.1. Objetivos . . . 8
1.2. Alcance . . . 8
1.3. Motivación . . . 8
1.4. Requisitos formales . . . 9
1.4.1. Documentación e información . . . 9
1.4.2. Normativas y certificaciones . . . 9
1.4.3. Propuesta de metodología de la auditoría . . . 9
1.4.4. Sobre el caso práctico . . . 9
1.5. Estructura del documento . . . 9

2. Planificación **11**
2.1. Fases y lista de actividades . . . 11
2.2. Roles y responsabilidades . . . 13
2.3. Cronograma . . . 13
2.4. Recursos . . . 13
2.4.1. Recursos Humanos . . . 13
2.4.2. Recursos Materiales . . . 14
2.4.3. Costos Asociados . . . 14
2.5. Estimación de Costes . . . 14

3. Fundamentos Teóricos sobre Normativas y Técnicas de Auditoría de Ciberseguridad **16**
3.1. Principales amenazas y riesgos para PYMEs . . . 16
3.2. Normativas nacionales aplicables . . . 16
3.3. Normativas europeas aplicables . . . 17
3.4. Herramientas de pentesting . . . 17
3.5. Técnicas y buenas prácticas de una auditoría . . . 17

4. Requisitos **19**

5. Modelo de auditoría **20**
5.1. Diseño . . . 20
5.2. Propuesta de auditoría . . . 20
5.3. Metodología de auditoría . . . 20

6. Caso Práctico **21**
6.1. Implementación de la auditoría . . . 21

7. Resultados **22**

8. Discusión de resultados o conclusiones **23**

Índice de figuras

Índice de cuadros

1. Distribución de roles y responsabilidades en el proyecto 13
2. Recursos Humanos 13
3. Recursos Materiales 14
4. Costos Asociados 14
5. Resumen de costes del proyecto 15
6. Principales ataques en ciberseguridad 16

Agradecimientos

INTENCIONADAMENTE EN BLANCO

Resumen

Las pequeñas y medianas empresas (PYMEs) desempeñan un papel crucial en la economía global, impulsando la creación de empleo y la innovación. Sin embargo, su creciente digitalización ha aumentado su exposición a ciberataques, debido a infraestructuras de seguridad limitadas y recursos insuficientes para enfrentar amenazas sofisticadas. Este proyecto tiene como objetivo principal desarrollar un modelo de auditoría de ciberseguridad adaptado a las PYMEs, basándose en la normativa europea y nacional vigente. Para garantizar su aplicabilidad, se elaborará una guía accesible para usuarios sin conocimientos técnicos previos, permitiéndoles evaluar y mejorar la seguridad de sus entornos digitales.

El proyecto se divide en dos fases principales. En la primera, se establecerá un marco teórico que explore las herramientas más comunes en auditorías de seguridad, las normativas aplicables y las metodologías más utilizadas en el ámbito de la ciberseguridad. Se examinarán los diferentes tipos de auditorías y se proporcionarán estrategias para mitigar estos riesgos. Esta fase permitirá comprender en profundidad las vulnerabilidades específicas del entorno empresarial y cómo abordarlas.

La segunda fase estará dedicada a la implementación práctica de la auditoría, siguiendo una metodología estructurada que abarcará desde el análisis del perímetro de red hasta la evaluación de la seguridad de los datos. Se incluirán pruebas en aplicaciones web, dispositivos IoT y la infraestructura interna de la empresa. Esta parte culminará con un caso práctico que ilustrará el proceso completo de auditoría en un entorno real, proporcionando una visión clara de cómo aplicar las técnicas aprendidas.

El objetivo final de este estudio no es solo facilitar la ejecución de auditorías de ciberseguridad en PYMEs, sino también promover la adopción de buenas prácticas. La guía ofrecerá recomendaciones para la gestión continua de la seguridad, la creación de políticas internas efectivas y la concienciación del personal, asegurando que las empresas no solo cumplan con las normativas vigentes, sino que también desarrollen una cultura de seguridad robusta y sostenible en el tiempo.

Palabras clave: ciberseguridad, auditoría, PYMEs, vulnerabilidades, normativas, metodologías, buenas prácticas.

Abstract

Small and medium-sized enterprises play a crucial role in the global economy, driving job creation and innovation. However, their increasing digitalization has heightened their exposure to cyberattacks due to limited security infrastructures and insufficient resources to face sophisticated threats. This project aims to develop a cybersecurity audit model tailored to SMEs, based on current European and national regulations. To ensure its applicability, an accessible guide will be created for users without prior technical knowledge, enabling them to evaluate and improve the security of their digital environments.

The project is divided into two main phases. The first phase will establish a theoretical framework exploring the most common tools in security audits, applicable regulations, and the most widely used methodologies in cybersecurity. Different types of audits will be examined, and strategies to mitigate risks will be provided. This phase will allow for a deep understanding of the specific vulnerabilities within the business environment and how to address them.

The second phase will focus on the practical implementation of the audit, following a structured methodology that will cover everything from network perimeter analysis to data security evaluation. It will include tests on web applications, IoT devices, and the company's internal infrastructure. This part will culminate in a practical case study illustrating the complete audit process in a real environment, providing a clear view of how to apply the learned techniques.

The ultimate goal of this study is not only to facilitate the execution of cybersecurity audits in SMEs but also to promote the adoption of best practices. The guide will offer recommendations for continuous security management, the creation of effective internal policies, and staff awareness, ensuring that companies not only comply with current regulations but also develop a robust and sustainable security culture over time.

Keywords: cybersecurity, audit, SMEs, vulnerabilities, regulations, methodologies, best practices.

1. Introducción

En el mundo digital actual, la ciberseguridad ya no es una opción, sino una necesidad. Las pequeñas y medianas empresas (PYMEs), pilares fundamentales de la economía global, se encuentran entre los objetivos más vulnerables frente a ciberataques. A pesar de su importancia económica, muchas de estas empresas subestiman su exposición a amenazas digitales, creyendo erróneamente que su tamaño las hace pasar desapercibidas para los ciberdelincuentes. Sin embargo, esta percepción es un error crítico, ya que la limitada infraestructura de seguridad de las PYMEs las convierte en blancos fáciles.

Un claro ejemplo de la creciente amenaza cibernética es el ataque sufrido por el portal de afiliación del sindicato Comisiones Obreras (CCOO) en diciembre de 2023 [1]. El atacante explotó una vulnerabilidad en el formulario de afiliación, accediendo a la configuración interna del sitio web. Esta brecha permitió la subida de un archivo malicioso que otorgó control total sobre el sistema, facilitando el acceso a información sensible, incluyendo contraseñas sin la protección adecuada. Como resultado, el atacante alteró la página de inicio de aproximadamente 50 subdominios de ccoo.es, demostrando la facilidad con la que se puede comprometer la seguridad digital de una organización.

Este incidente subraya la necesidad urgente de fortalecer la ciberseguridad en organizaciones de todos los tamaños. Las PYMEs, en particular, son especialmente susceptibles debido a la escasez de recursos y, en muchos casos, a una falta de concienciación sobre las amenazas digitales. La creciente digitalización y la dependencia de sistemas conectados a la red han ampliado la superficie de ataque, exponiendo a estas organizaciones a riesgos significativos.

En este contexto, es crucial que las PYMEs adopten medidas proactivas para proteger sus activos digitales. Este trabajo propone una guía práctica para la realización de auditorías de ciberseguridad, con el objetivo de identificar vulnerabilidades, evaluar riesgos y establecer estrategias de mitigación efectivas. A través de esta guía, se busca empoderar a las PYMEs para que fortalezcan su postura de seguridad y enfrenten con mayor confianza los desafíos del entorno digital actual.

1.1. Objetivos

El objetivo principal de este trabajo es diseñar un modelo de auditoría de ciberseguridad específico para PYMEs, que sea fácil de implementar por personas sin conocimientos técnicos avanzados. Los objetivos específicos incluyen:

- Establecer un marco teórico que contemple las herramientas, técnicas y normativas actuales en ciberseguridad.
- Proponer una metodología de auditoría clara y estructurada.
- Desarrollar un caso práctico en una PYME real para validar la metodología propuesta.
- Redactar un informe detallado que incluya el análisis de riesgos, vulnerabilidades detectadas y recomendaciones de mejora.

1.2. Alcance

El alcance de este trabajo está diseñado para cubrir de manera integral todos los aspectos necesarios para realizar una auditoría de ciberseguridad efectiva en PYMEs, basándose en estándares y metodologías reconocidas internacionalmente.

1. **Marco teórico:** Se explorarán las herramientas más utilizadas en auditorías de ciberseguridad, las normativas relevantes tanto a nivel nacional como europeo, los distintos tipos de auditoría existentes y las recomendaciones de organizaciones como OWASP, SANS y OSSTM.
2. **Requisitos previos:** Se detallarán los conocimientos, habilidades y recursos técnicos necesarios para realizar auditorías efectivas, incluyendo la configuración de entornos de prueba y el uso de herramientas especializadas.
3. **Propuesta de metodología:** Se desarrollará una metodología estructurada que incluirá el análisis del perímetro de red, la seguridad inalámbrica, la identificación de vulnerabilidades en dispositivos IoT, pruebas sobre aplicaciones web, evaluación de la infraestructura interna y análisis de seguridad en endpoints y sistemas de almacenamiento de datos.
4. **Caso práctico:** Se implementará un caso práctico que aplicará la metodología propuesta en un entorno real, permitiendo ilustrar de manera tangible el proceso completo de una auditoría de ciberseguridad.
5. **Informe final:** Elaboración de un documento que refleje el estado actual de la ciberseguridad en la empresa auditada y las recomendaciones pertinentes.

1.3. Motivación

La creciente digitalización ha expuesto a las Pequeñas y Medianas Empresas (PYMEs) a una variedad de ciberamenazas que, de no ser gestionadas adecuadamente, pueden poner en riesgo la continuidad de sus operaciones. A diferencia de las grandes corporaciones, las PYMEs suelen carecer de los recursos humanos y financieros necesarios para implementar medidas robustas de ciberseguridad, lo que las convierte en objetivos atractivos para los ciberdelincuentes.

El aumento en el volumen de software malicioso, que supera los 450.000 nuevos programas diarios [2], y el hecho de que el 70 por ciento de los ciberataques en la Península Ibérica afectan a PYMEs, subrayan la urgencia de desarrollar herramientas accesibles y eficaces para proteger a estas organizaciones. Este proyecto surge como respuesta a esa necesidad, proporcionando una guía práctica que permite a cualquier persona, independientemente de su nivel técnico, llevar a cabo una auditoría básica de ciberseguridad.

La implementación del modelo propuesto no solo mejorará la seguridad digital de las PYMEs, sino que también fomentará una mayor concienciación sobre la importancia de la ciberseguridad en el entorno empresarial. De esta manera, se busca fortalecer el tejido empresarial frente a las crecientes amenazas cibernéticas.

1.4. Requisitos formales

Una vez dado un contexto general del trabajo, nos centraremos en describir que requisitos son necesarios para la redacción del documento.

1.4.1. Documentación e información

- Los documentos pueden ser extraídos de *Google Scholar* para su posterior citación, recomendando documentos no más antiguos de 2 o 3 años para asegurar la vigencia de la información.
- Se citarán en el documento en formato APA todos los documentos de los que se ha extraído información.
- Deben contener información relevante y actualizada sobre ciberseguridad en PYMEs, incluyendo normativas, estándares, herramientas y técnicas de auditoría.

1.4.2. Normativas y certificaciones

- Deben ser oficiales y de libre acceso, proporcionadas por organismos reguladores tanto de ámbito europeo como internacional.

1.4.3. Propuesta de metodología de la auditoría

- Debe atender a los requerimientos de ciberseguridad descritos en la documentación oficial.
- Describir las implementaciones de hardware y software necesarias para proteger los sistemas.

1.4.4. Sobre el caso práctico

- Descripción del sistema auditado, incluyendo modelo y vulnerabilidades.
- Aplicación de la metodología de ciberseguridad en la PYME seleccionada.
- Detalle de las pruebas realizadas y la obtención de información sobre riesgos, amenazas y vulnerabilidades.

1.5. Estructura del documento

El documento está organizado en once capítulos que abordan de manera integral todos los aspectos necesarios para realizar una auditoría de ciberseguridad en PYMEs:

- **Agradecimientos:** Reconocimiento a las personas y entidades que han contribuido al desarrollo de este trabajo.
- **Resumen:** Síntesis del contenido, objetivos y resultados del trabajo.
- **Introducción:** Presentación del contexto de la ciberseguridad en PYMEs, objetivos, alcance, motivación, requisitos formales para el desarrollo del proyecto y estructura del documento.
- **Planificación:** Descripción de la organización del trabajo, incluyendo cronograma, recursos utilizados, costes y fases del proyecto.
- **Marco Teórico (Estado del arte):** Análisis de normativas nacionales y europeas aplicables, estándares, herramientas de pentesting y técnicas relevantes en el ámbito de la ciberseguridad para PYMEs.
- **Requisitos:** Definición de los requisitos técnicos, legales y organizativos necesarios para llevar a cabo una auditoría de seguridad.
- **Modelo de auditoría:** Propuesta de un modelo de auditoría dividido en diseño, metodología y fases específicas.
- **Caso Práctico:** Implementación de la auditoría en un entorno real de una PYME, aplicando las herramientas y técnicas descritas.

- **Resultados:** Presentación y análisis de los resultados obtenidos en el caso práctico.
- **Discusión de resultados:** Reflexión sobre los hallazgos, lecciones aprendidas y posibles trabajos futuros.
- **Referencias:** Fuentes consultadas para la realización del trabajo.
- **Anexos:** Material complementario que apoya el desarrollo del caso práctico y la comprensión de la metodología.

2. Planificación

Este capítulo presenta la planificación detallada para el desarrollo del trabajo. Se describirán las fases y tareas específicas a desarrollar, los roles y responsabilidades de los participantes en el proyecto, así como un cronograma que permitirá visualizar el progreso del trabajo a lo largo del tiempo. Además, se identificarán los recursos necesarios para llevar a cabo el proyecto y se realizará un análisis de los costes asociados.

2.1. Fases y lista de actividades

Fase 1 - Gestión del Proyecto

- **1.1 Plan de Inicio**
  - **1.1.1 Reunión inicial:** Primer encuentro con el tutor para explorar posibles temas de interés para el TFG.
  - **1.1.2 Investigación preliminar:** Análisis de las diferentes opciones y selección del tema más adecuado.
  - **1.1.3 Adjudicación TFG:** Confirmación oficial del tema y asignación del trabajo.
  - **1.1.4 Inicio del trabajo:** Comienzo formal de la redacción y desarrollo del trabajo.
  - **1.1.5 Investigación orientada a los objetivos:** Ampliación del conocimiento sobre el tema seleccionado.
  - **1.1.6 Segunda reunión con el tutor:** Reunión para debatir la estructura y organización del TFG.
  - **1.1.7 Reunión con CTO BeeHacker:** Análisis de la viabilidad del trabajo y perspectivas del sector.
  - **1.1.8 Segunda reunión con CTO BeeHacker:** Obtención de información adicional.
  - **1.1.9 Desarrollo de la introducción:** Definición clara de los objetivos, alcance, motivación y requisitos.
  - **1.1.10 Revisión de la introducción:** Revisión y aprobación del plan de inicio.
- **1.2 Planificación**
  - **1.2.1 Definición de fases y tareas:** Establecimiento de las fases y actividades del proyecto.
  - **1.2.2 Definición de roles y responsables:** Asignación de roles y responsabilidades del proyecto.
  - **1.2.3 Cronograma:** Desarrollo del cronograma en MSProject.
  - **1.2.4 Recursos:** Identificación de recursos humanos y materiales.
  - **1.2.5 Estimación de costes:** Cálculo del presupuesto estimado.
  - **1.2.6 Revisión de la planificación:** Revisión y aprobación de la planificación.
- **1.3 Seguimiento y Control**
  - **1.3.1 Corrección de la introducción:** Corrección y ajuste de la introducción.
  - **1.3.2 Corrección de la planificación:** Corrección y ajuste de la planificación.
  - **1.3.3 Corrección del marco teórico:** Corrección y ajuste del marco teórico.
  - **1.3.4 Corrección del modelo de auditoría:** Corrección y ajuste del modelo de auditoría.
  - **1.3.5 Informe y control del desempeño:** Generación de informes de seguimiento.
- **1.4 Cierre**
  - **1.4.1 Informe final con resultados:** Documentación final con las conclusiones.

- **1.4.2 Plan de mitigación de riesgos:** Propuesta de acciones correctivas.
- **1.4.3 Lecciones aprendidas:** Reflexión sobre los conocimientos adquiridos.

Fase 2 - Desarrollo del Producto

- **2.1 Marco teórico**
  - **2.1.1 Desarrollo del marco teórico:** Investigación, análisis, redacción y estructuración del marco conceptual.
  - **2.1.2 Revisión del marco teórico:** Revisión y aprobación del marco teórico.
- **2.2 Modelo de auditoría**
  - **2.2.1 Diseño del modelo:** Definición de la estructura metodológica y los procedimientos a seguir.
  - **2.2.2 Revisión del modelo:** Revisión y aprobación del modelo de auditoría.
- **2.3 Caso práctico**
  - **2.3.1 Desarrollo del caso práctico:** Ejecución y aplicación en la PYME.
  - **2.3.2 Seguimiento de la práctica:** Monitorización y análisis del proceso.

Fase 3 - Revisión técnica formal

- **3.1 Revisión del proyecto**
  - **3.1.1** Análisis completo del trabajo desarrollado y correcciones necesarias.

Fase 4 - Presentación

- **4.1 Presentación del proyecto**
  - **4.1.1** Exposición y defensa del trabajo realizado.

2.2. Roles y responsabilidades

Cuadro 1: Distribución de roles y responsabilidades en el proyecto

Rol	Responsabilidad
Analista/Desarrollador (Alumno)	Planificación y redacción del documento
Analista/Desarrollador (Alumno)	Investigación y análisis de ciberseguridad en PYMEs
Analista/Desarrollador (Alumno)	Desarrollo del marco teórico
Analista/Desarrollador (Alumno)	Agrupación y redacción de requisitos previos para auditoría
Analista/Desarrollador (Alumno)	Identificación y documentación de normativas aplicables
Analista/Desarrollador (Alumno)	Creación de plan de auditoría propio
Analista/Desarrollador (Alumno)	Diseño de la metodología de auditoría
Analista/Desarrollador (Alumno)	Implementación práctica de la auditoría
Analista/Desarrollador (Alumno)	Ejecución del caso práctico
Analista/Desarrollador (Alumno)	Análisis de resultados y redacción del informe final
Jefe de proyecto (Tutor)	Asesoramiento en la selección del tema y enfoque del proyecto
Jefe de proyecto (Tutor)	Orientación y supervisión del trabajo del alumno
Jefe de proyecto (Tutor)	Organizar el desarrollo del caso práctico
Jefe de proyecto (Tutor)	Correcciones y evaluación del proyecto
Jefe de equipo (CTO de BeeHacker)	Proporcionar información técnica relevante y feedback
Jefe de equipo (CTO de BeeHacker)	Validación de la metodología y resultados del caso práctico

Fuente: Elaboración propia

2.3. Cronograma

ANALISIS FINAL CON EL MSProject

2.4. Recursos

Los recursos necesarios para el desarrollo de la auditoría de ciberseguridad se dividen en tres categorías principales: recursos humanos, materiales y costos asociados. A continuación, se detallan cada uno de ellos.

2.4.1. Recursos Humanos

En virtud del documento oficial de la Agencia Digital de Andalucía [3], se establecen los costes por hora de los perfiles profesionales necesarios para la realización del proyecto.

Cuadro 2: Recursos Humanos

Recurso	Tipo	Costo por Hora
Director de Proyecto	Trabajo	63,75 €/h
Jefe de Equipo	Trabajo	53,55 €/h
Analista	Trabajo	47,17 €/h

Fuente: Elaboración propia

2.4.2. Recursos Materiales

Cuadro 3: Recursos Materiales

Recurso	Tipo	Costo Unitario	Unidades	Costo Total
Impresora	Material	€50,00	1	€50,00
Disco Duro Externo	Material	€60,00	1	€60,00
Pen Drive	Material	€20,00	1	€20,00
Ordenador	Material	€600,00	1	€600,00

Fuente: Elaboración propia

2.4.3. Costos Asociados

Cuadro 4: Costos Asociados

Recurso	Tipo	Costo Total	Coste Estimado
Reserva de Contingencia	Costo	Variable	1000€
Licencias Software	Costo	Variable	100€

Fuente: Elaboración propia

2.5. Estimación de Costes

Considerando los recursos descritos anteriormente, se prevé que el **Analista** desempeñe un total de **300 horas de trabajo**, lo que supone un coste estimado de 14.151 €.

En cuanto al **Director de Proyecto**, se estima una dedicación de **20 horas** centradas en tareas de corrección, revisión y supervisión general del proyecto, lo que representa un coste de 1.275 €.

Respecto al **Jefe de Equipo**, se calcula un total de **10 horas** destinadas a la asistencia técnica y apoyo en el desarrollo de la auditoría, con un coste asociado de 535,50 €.

Además, es necesario considerar los **costos adicionales asociados** al proyecto, entre los que destacan una **reserva de contingencia** de 1.000 € para posibles imprevistos y el coste de las **licencias de software** necesarias, estimado en 100 €, lo que suma un total de 1.100 €.

En lo que respecta a los **recursos materiales**, se ha calculado un coste global de 730 €, correspondiente a la adquisición de los elementos físicos indispensables para el desarrollo del trabajo.

Este cálculo corresponde a una **duración estimada del proyecto de 4 meses**, durante los cuales se prevé que los profesionales involucrados realicen las tareas planificadas dentro de las horas estipuladas.

De esta manera, los costes totales estimados son los siguientes:

Cuadro 5: Resumen de costes del proyecto

Concepto	**Monto (€)**
Recursos Humanos	15.961,50 €
Recursos Materiales	730 €
Costos Asociados	1.100 €
Total Estimado	**17.791,50 €**

Fuente: Elaboración propia

3. Fundamentos Teóricos sobre Normativas y Técnicas de Auditoría de Ciberseguridad

El presente marco teórico tiene como objetivo proporcionar un contexto detallado sobre las auditorías de ciberseguridad, sus metodologías y herramientas, así como los estándares y normativas que rigen este campo.

Adicionalmente, se presentará un análisis de las normativas y regulaciones relevantes en el ámbito de la ciberseguridad, tanto a nivel nacional como europeo. También se describirán las principales metodologías utilizadas en auditorías de ciberseguridad y las herramientas más utilizadas en la industria.

Este marco teórico servirá como base para el diseño e implementación de un modelo de auditoría de ciberseguridad orientado a PYMEs, permitiendo establecer un procedimiento claro y estructurado para mejorar la seguridad, identificar vulnerabilidades y mitigar riesgos.

3.1. Principales amenazas y riesgos para PYMEs

Las PYMEs enfrentan riesgos significativos como **accesos no autorizados, robo de datos y alteración de información confidencial** , lo que compromete la integridad de sus sistemas. Para hacer frente a estos desafíos, muchas organizaciones integran personal especializado en ciberseguridad, adoptan soluciones tecnológicas y promueven la formación continua de sus empleados para prevenir y responder eficazmente ante posibles ataques (Morales-López & Taipe-Yanez & Pallo-Tulmo, 2024). [4]

Entre los principales tipos de ataques cibernéticos se encuentran:

Cuadro 6: Principales ataques en ciberseguridad

Tipo de Ataque	Descripción
Malware	Programas informáticos maliciosos diseñados para acceder a información confidencial o interrumpir servicios. Ejemplos comunes son troyanos, spyware y virus.
Ransomware	Tipo de malware que cifra los datos de una organización y exige un rescate para su liberación. Representa una forma de extorsión altamente perjudicial.
Ataque de intermediario (Man-in-the-Middle)	Consiste en interceptar las comunicaciones entre dos partes para acceder a información sensible, como credenciales o datos financieros.
Phishing	Técnica de ingeniería social que engaña a los usuarios para que revelen información confidencial, como contraseñas o datos bancarios, mediante correos electrónicos o sitios web falsos.
Ataques DDoS	Buscan saturar un servidor mediante el envío masivo de solicitudes, impidiendo el acceso a usuarios legítimos.
Amenaza interna	Proviene de empleados o colaboradores con acceso autorizado que, intencionadamente o por negligencia, comprometen la seguridad de la organización.

Fuente: Elaboración propia en base a (Estrategias de Auditoría en ciberseguridad y su importancia en las empresas una revisión bibliográfica año 2024)

3.2. Normativas nacionales aplicables

En el contexto español, la legislación vigente en materia de ciberseguridad establece un conjunto de normas esenciales que las PYMEs deben tener en cuenta para garantizar la protección de sus sistemas y datos. Estas normativas buscan no solo proteger la información sensible de las organizaciones, sino también fomentar una cultura de prevención y resiliencia ante los ciberataques.

Una de las normativas más relevantes es el **Esquema Nacional de Seguridad (ENS)**, regulado por el Real Decreto 311/2022. Este marco establece los principios básicos y requisitos mínimos necesarios

para una protección adecuada de la información manejada por medios electrónicos, y es de obligado cumplimiento para las entidades del sector público y recomendable para las empresas privadas. El ENS promueve un enfoque basado en riesgos y establece diferentes niveles de seguridad en función del impacto que una amenaza pueda tener sobre la organización. (Boletín Oficial del Estado, 2024). [5]

Asimismo, el **Real Decreto-ley 12/2018**, sobre seguridad de las redes y sistemas de información, incorpora al derecho español la Directiva NIS de la Unión Europea. Este decreto impone obligaciones a los operadores de servicios esenciales y proveedores de servicios digitales para garantizar un nivel adecuado de seguridad en sus operaciones, además de establecer la necesidad de notificar los incidentes de seguridad más relevantes a la autoridad competente. (Boletín Oficial del Estado, 2024). [5]

Otra normativa destacable es la **Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)**, que adapta el Reglamento General de Protección de Datos (RGPD) al ordenamiento jurídico español. Esta ley establece obligaciones específicas en cuanto al tratamiento, almacenamiento y seguridad de los datos personales, lo cual es especialmente relevante en escenarios donde se procesan grandes volúmenes de datos sensibles. (Boletín Oficial del Estado, 2024). [5]

Además, organismos nacionales como el **Instituto Nacional de Ciberseguridad (INCIBE)** y el **Centro Criptológico Nacional (CCN)** han reforzado su colaboración para coordinar acciones frente a las ciberamenazas que afectan tanto a ciudadanos como a empresas, proporcionan directrices, guías técnicas y herramientas de apoyo que complementan el cumplimiento normativo, especialmente adaptadas a las capacidades de las pequeñas y medianas empresas. (Escudo Digital, 2023). [9]

3.3. Normativas europeas aplicables

La Unión Europea ha desarrollado un marco normativo sólido para fortalecer la ciberseguridad en sus Estados miembros, afectando directamente a las PYMEs. Estas regulaciones buscan establecer un nivel común de seguridad y resiliencia operativa en el entorno digital europeo.

Una pieza clave es la **Directiva NIS2** (Directiva (UE) 2022/2555), que entró en vigor en enero de 2023. Esta directiva amplía el alcance de su predecesora, la Directiva NIS, imponiendo requisitos de seguridad más estrictos y procesos de notificación de incidentes más concretos. Se aplica a medianas y grandes empresas de sectores críticos, incluyendo energía, transporte, salud y administración pública. Las empresas deben implementar políticas de gestión de riesgos, autenticación multifactor y formación en ciberseguridad para empleados. (Cadena SER, 2024). [6]

Otra regulación relevante es el **Reglamento DORA** (Reglamento (UE) 2022/2554), que establece un marco para la resiliencia operativa digital del sector financiero. Su objetivo es garantizar que todas las entidades financieras puedan soportar, responder y recuperarse de incidentes relacionados con las TIC, asegurando la estabilidad del sistema financiero europeo. (Banco Central Europeo, 2025). [7]

Además, la propuesta de la **Ley de Ciberresiliencia** de la UE, presentada en septiembre de 2022, busca introducir requisitos horizontales obligatorios de ciberseguridad para productos con elementos digitales, garantizando que los consumidores y empresas puedan confiar en productos digitales seguros. (Comisión Europea, 2023). [8]

3.4. Herramientas de pentesting

3.5. Técnicas y buenas prácticas de una auditoría

Además, existen plataformas y recursos comunitarios que permiten a los profesionales de la ciberseguridad mantenerse actualizados sobre las amenazas más recientes. Por ejemplo, sitios como **Exploit DB** ofrecen una base de datos pública de exploits y vulnerabilidades conocidas, categorizadas por tipo de software o sistema afectado. Asimismo, los **CVE (Common Vulnerabilities and Exposures)** constituyen un estándar internacional para identificar vulnerabilidades de seguridad; cada entrada en el CVE representa una amenaza específica y es asignada por organizaciones autorizadas como el MITRE

Corporation, en colaboración con instituciones públicas y privadas a nivel global. Estas fuentes resultan esenciales para el análisis y priorización de riesgos durante una auditoría de ciberseguridad (MITRE Corporation, 2024). [10]

4. Requisitos

5. Modelo de auditoría

5.1. Diseño

5.2. Propuesta de auditoría

5.3. Metodología de auditoría

6. Caso Práctico

6.1. Implementación de la auditoría

7. Resultados

8. Discusión de resultados o conclusiones

Referencias

[1] DefSec. (s.f.). *Mariscada virtual en el servidor de CCOO*. Recuperado el 08 de febrero de 2025, de https://defsec.noblogs.org/mariscada-virtual-en-el-servidor-de-ccoo/

[2] AV-TEST. (s.f.). *AV-Atlas Malware Portal*. Recuperado el 10 de enero de 2025, de https://portal.av-atlas.org/malware

[3] Agencia Digital de Andalucía. (2024). *Documento de transparencia sobre costes laborales en perfiles TIC*. Encontrado el 13 de febrero de 2025, de https://ws040.juntadeandalucia.es/webconsejos/cgobierno/transparencia/240730/documentos/30Expediente.pdf

[4] Morales-López & Taipe-Yanez & Pallo-Tulmo, (2024) *Estrategias de Auditoría en ciberseguridad y su importancia en las empresas una revisión bibliográfica* Encontrado el 07 de abril de 2025 de https://www.investigarmqr.com/ojs/index.php/mqr/article/view/1436/4849

[5] Boletín Oficial del Estado. (2024). Código Electrónico de Ciberseguridad. el 08 de abril de 2025 Recuperado de: https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=173

[6] Cadena SER. (2024). ¿Qué cambia la directiva de la UE que mejora la ciberseguridad y ya aplican los Estados?. el 08 de abril de 2025 Recuperado de: https://cadenaser.com/cmadrid/2024/10/22/que-cambia-la-directiva-de-la-ue-que-mejora-la-ciberseguridad-y-ya-aplican-los-estados-ser-madr

[7] Banco Central Europeo. (2025). Decisiones adoptadas por el Consejo de Gobierno del BCE. el 08 de abril de 2025 Recuperado de: https://www.ecb.europa.eu/press/govcdec/otherdec/2025/html/ecb.gc250131~d2c6d582b0.es.html

[8] Comisión Europea. (2023). Una Europa Adaptada a la Era Digital. Recuperado de:el 08 de abril de 2025 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_es

[9] Escudo Digital. (2023). *INCIBE, CNI y CCN se reúnen para impulsar su coordinación en ciberseguridad*. Recuperado de: https://www.escudodigital.com/ciberseguridad/incibe-cni-ccn-se-reunen-impulsar-su-coordinacion-en-ciberseguridad_54930_102.html

[10] MITRE. (2024). *Common Vulnerabilities and Exposures (CVE)*.el 08 de abril de 2025 Recuperado de: https://www.cve.org/About/Overview