



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. Marco Teórico	16
3.1. Principales amenazas y riesgos para PYMEs	16
3.2. Normativas nacionales aplicables	17
3.3. Normativas europeas aplicables	18
3.4. Herramientas de pentesting	18
3.5. Técnicas utilizadas en auditorías de ciberseguridad	19
3.6. Buenas prácticas durante una auditoría de ciberseguridad	21
3.6.1. Buenas prácticas durante una auditoría de ciberseguridad	21
3.6.2. Buenas prácticas dentro de la organización auditada	22
4. Requisitos	23
5. Modelo de auditoría	24
5.1. Diseño	24
5.2. Propuesta de auditoría	24
5.3. Metodología de auditoría	24
6. Caso Práctico	25
6.1. Implementación de la auditoría	25
7. Resultados	26
8. Discusión de resultados o conclusiones	27

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.	Herramientas de pentesting más empleadas	19
7.	Buenas prácticas en auditorías de ciberseguridad según el rol	21

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 3 o 4 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 MSPProject

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	<u>17.791,50 €</u>

Fuente: Elaboración propia

3. Marco Teórico

El presente marco teórico tiene como objetivo fundamentar los conceptos esenciales relacionados con la ciberseguridad en el contexto de las pequeñas y medianas empresas (PYMEs), abordando los principales riesgos y amenazas a los que se enfrentan, así como los marcos normativos que regulan la protección de sistemas y datos. Se incluyen tanto normativas nacionales como europeas, junto con recomendaciones prácticas derivadas de estándares ampliamente reconocidos como OWASP Top 10, NIST u OSSTMM.

Además, se analizan las técnicas empleadas durante una auditoría de ciberseguridad, así como las herramientas más relevantes utilizadas en procesos de pentesting, con el objetivo de identificar vulnerabilidades y mejorar la postura de seguridad organizacional.

Este análisis proporciona una base sólida 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

La ciberseguridad representa un desafío importante para muchas pequeñas y medianas empresas españolas. Según el informe de Hiscox, cerca del 50 % de las empresas en España sufrió algún tipo de ciberataque en 2023. Las PYMEs, en particular, son cada vez más objetivo de estos ataques debido a su limitada preparación en ciberseguridad. De hecho, solo el 61 % de las empresas con menos de 250 empleados se sienten seguras de su preparación en esta materia. (Hiscox, 2022) [11]

El Instituto Nacional de Ciberseguridad (INCIBE) registró en 2022 un total de 118.000 incidentes de ciberseguridad, un 9 % más que el año anterior. Una gran parte de estos incidentes afectaron a pequeñas y medianas empresas, y uno de cada tres se trató de una filtración de datos. (INCIBE, 2023) [12]

Aunque cada vez más PYMEs aumentan sus presupuestos en ciberseguridad y colaboran con empresas especializadas, muchas todavía optan por externalizar sus servicios por falta de personal y recursos internos. Esta externalización, si bien útil, debe complementarse con una adecuada cultura interna de seguridad, especialmente mediante la formación del personal.

Según PwC España, el 86 % de las organizaciones considera que sus empleados carecen de una cultura de ciberseguridad adecuada, lo que pone de relieve la necesidad urgente de concienciación. (PWC, 2021) [13]

Entre los principales tipos de ataques cibernéticos que afectan a las PYMEs se encuentran:

- **Phishing / Suplantación de identidad:** Técnica de ingeniería social mediante la cual el atacante suplanta la identidad de una entidad legítima para obtener información confidencial (credenciales, datos bancarios, etc.) mediante correos electrónicos o sitios web falsos.
- **Ransomware / Secuestro de datos:** Software malicioso que cifra archivos y exige el pago de un rescate para su recuperación. Es uno de los ataques más perjudiciales para PYMEs.
- **Ataques DDoS:** Buscan saturar los servidores de una organización mediante el envío masivo de solicitudes, impidiendo el acceso a usuarios legítimos.
- **Ataques a la cadena de suministro:** Se aprovechan de vulnerabilidades en proveedores o terceros con los que la empresa colabora, explotando relaciones de confianza para infiltrar malware o robar información.
- **Malware:** Software diseñado para dañar sistemas, robar datos o controlar dispositivos. Incluye virus, troyanos y spyware.
- **Amenaza interna:** Proviene de empleados o colaboradores con acceso autorizado que, por negligencia o intención maliciosa, comprometen la seguridad de la organización.

- **Contraseñas débiles:** El uso de contraseñas simples o reutilizadas permite a los atacantes acceder fácilmente a los sistemas. Es una vulnerabilidad común que puede prevenirse con políticas de autenticación robustas.
- **Falta de formación y políticas de seguridad:** La ausencia de programas de concienciación y protocolos claros de actuación ante amenazas limita la capacidad de reacción ante incidentes.
- **Falta de actualizaciones de seguridad:** No aplicar los parches y actualizaciones necesarios en sistemas y aplicaciones deja expuestas vulnerabilidades que pueden ser explotadas por atacantes.

Además de los vectores de ataque anteriores, existen ciertos **riesgos estructurales** que afectan especialmente a las PYMEs y que incrementan su vulnerabilidad frente a ciberataques:

- **Falta de recursos de seguridad dedicados:** Muchas pequeñas empresas no cuentan con personal especializado en ciberseguridad (como un CISO o un técnico en protección de datos), lo que dificulta la detección y respuesta ante incidentes.
- **Presupuestos limitados:** La inversión en ciberseguridad suele quedar relegada frente a otras prioridades de negocio, lo que impide implementar soluciones de protección efectivas o actualizadas.
- **Falta de diseño seguro desde el inicio:** Al haber sido creadas por expertos en su sector y no por especialistas en tecnología, muchas PYMEs han desarrollado sus sistemas sin tener en cuenta principios de seguridad por defecto.
- **Ausencia de fondos de emergencia:** La falta de capacidad económica para hacer frente a pagos por rescates o pérdidas prolongadas de ingresos hace que las consecuencias de un ciberataque sean especialmente devastadoras.
- **Impacto operativo total ante incidentes graves:** Un ciberataque que provoque una filtración o la caída de sistemas puede detener completamente la actividad del negocio, ya que las PYMEs no suelen tener infraestructuras de respaldo.

Estos factores, sumados a una falsa sensación de anonimato (“somos demasiado pequeños para que nos ataquen”), aumentan considerablemente el riesgo de que las PYMEs se conviertan en blancos frecuentes y exitosos de los ciberdelincuentes. Implementar medidas preventivas y desarrollar una cultura de seguridad sólida resulta crucial para garantizar su continuidad. (L. Toms, 2021) [14]

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

La selección de herramientas de pentesting desempeña un papel fundamental en la eficacia de las auditorías de seguridad. Identificar las herramientas adecuadas permite detectar vulnerabilidades de forma precisa y eficiente, adaptándose a distintos escenarios como redes, aplicaciones web, servicios en la nube o incluso factores humanos a través de técnicas de ingeniería social. A partir de un análisis conjunto de diversas fuentes especializadas, se recopilieron las diez herramientas más utilizadas y valoradas en el ámbito del pentesting. (F. Redondo & N. Cárdenas, 2024). [10]

Cuadro 6: Herramientas de pentesting más empleadas

Herramienta	Descripción	Donde encontrarlas
 Nmap	Escáner de redes y auditor de seguridad que permite descubrir hosts, servicios y vulnerabilidades activas.	nmap.org
 Metasploit	Framework completo para desarrollar, probar y ejecutar exploits en entornos controlados.	metasploit.com
 Burp Suite	Plataforma integrada para análisis de seguridad en aplicaciones web, capaz de interceptar, modificar y automatizar pruebas.	portswigger.net/burp
 Kali Linux / Parrot OS	Sistemas operativos especializados para pentesting que incluyen múltiples herramientas de auditoría, análisis forense e ingeniería inversa.	kali.org, parrotsec.org
 Nessus	Escáner de vulnerabilidades de red que identifica configuraciones erróneas, parches faltantes y debilidades comunes.	tenable.com/nessus
 John the Ripper	Herramienta para craqueo de contraseñas y evaluación de su fortaleza en diferentes sistemas.	openwall.com/john
 Wireshark	Analizador de protocolos de red que permite capturar y examinar en tiempo real el tráfico que circula por una red.	wireshark.org
 ZAP (Zed Attack Proxy)	Escáner de seguridad de aplicaciones web enfocado en detectar vulnerabilidades durante el desarrollo.	zaproxy.org
SQLmap	Automatiza la detección y explotación de inyecciones SQL en aplicaciones web.	sqlmap.org
 Aircrack-ng	Conjunto de herramientas para auditar redes Wi-Fi, especializado en romper claves WEP y WPA/WPA2.	aircrack-ng.org

Fuente: Elaboración propia en base a (Criterios de selección de herramientas para pentesting, 2024)

3.5. Técnicas utilizadas en auditorías de ciberseguridad

Además de contar con herramientas especializadas, una auditoría de ciberseguridad eficaz debe basarse en técnicas metodológicas contrastadas. Las técnicas descritas a continuación están ampliamente consolidadas y han sido validadas por organismos y marcos de referencia reconocidos internacionalmente, como el **PTES (Penetration Testing Execution Standard)**, el **OSSTMM (Open Source Security Testing Methodology Manual)**, el **NIST SP 800-82** para entornos industriales, y el **OWASP Top 10** en el ámbito de las aplicaciones web.

- **Reconocimiento (Reconnaissance):** Técnicas previas al ataque que permiten recolectar información del objetivo. Se utilizan metodologías OSINT (Open Source Intelligence), como análisis de redes sociales, WHOIS, Shodan o Google Hacking. También incluye *footprinting* y *fingerprinting* para identificar sistemas, servicios y versiones.
- **Escaneo y enumeración:** Se identifican puertos abiertos, servicios activos y configuraciones usando herramientas como Nmap o WhatWeb. La enumeración permite descubrir detalles específicos de servicios expuestos en la red.
- **Explotación (Exploitation):** Consiste en aprovechar vulnerabilidades detectadas para obtener acceso no autorizado a sistemas.
- **Post-explotación:** Tras comprometer un sistema, se buscan técnicas de escalado de privilegios, mantenimiento de acceso y técnicas de pivoting.

- **Análisis de vulnerabilidades:** Permite identificar y evaluar debilidades sin necesidad de explotación directa. Se emplean escáneres automáticos o revisión manual, especialmente útil en aplicaciones web, móviles o APIs.
- **Ingeniería social:** Técnica que explota el factor humano mediante engaños. Incluye phishing (correos falsos), y pretexting (identidades falsas para obtener información). Se pueden realizar simulaciones controladas para evaluar la concienciación del personal.
- **Pentesting web:** Se prueban vulnerabilidades específicas en aplicaciones web. Para ello se suelen usar las recomendaciones de OWASP Top 10 para identificar problemas comunes en este entorno.
- **Pentesting de redes Wi-Fi:** Incluye captura de handshakes y ataques a redes WPA/WPA2/WPA3. También se realizan ataques tipo *Evil Twin*, donde se simula un punto de acceso para engañar a los usuarios.
- **Ataques físicos y hardware hacking:** Cuando se tiene acceso físico a dispositivos, se pueden explotar puertos inseguros, configuraciones erróneas en BIOS, dispositivos IoT vulnerables o mediante el uso de USBs maliciosos.

3.6. Buenas prácticas durante una auditoría de ciberseguridad

Cuadro 7: Buenas prácticas en auditorías de ciberseguridad según el rol

Rol	Buenas prácticas clave
Equipo auditor	<ul style="list-style-type: none"> ■ Definir claramente el alcance de la auditoría. ■ Firmar acuerdos de confidencialidad y autorización. ■ Aplicar metodologías estándar (PTES, OSSTMM, NIST). ■ Utilizar entornos de prueba cuando sea posible. ■ Documentar cada fase del proceso de auditoría. ■ Actuar siempre con profesionalidad y ética. ■ Redactar un informe técnico claro, útil y comprensible. ■ Recomendar un plan de acción adaptado a la realidad de la empresa.
PYME auditada	<ul style="list-style-type: none"> ■ Colaborar activamente con el equipo auditor. ■ Tener identificados sus activos críticos (datos, sistemas, personas). ■ Mantener un inventario actualizado de hardware y software. ■ Aplicar el principio de mínimo privilegio en los accesos. ■ Establecer políticas básicas de seguridad internas. ■ Realizar copias de seguridad periódicas y probadas. ■ Mantener los sistemas actualizados. ■ Concienciar al personal sobre amenazas (phishing, ingeniería social). ■ Implementar doble factor de autenticación en accesos sensibles. ■ Contar con un plan básico de respuesta ante incidentes.

3.6.1. Buenas prácticas durante una auditoría de ciberseguridad

Durante la realización de una auditoría, es esencial aplicar buenas prácticas que garanticen la calidad y efectividad del proceso. Entre ellas se incluyen:

- **Aplicación de estándares reconocidos:** seguir marcos de trabajo como OWASP Top 10 y OSSTMM asegura una cobertura exhaustiva de las vulnerabilidades más comunes y relevantes.
- **Documentación clara y trazabilidad:** mantener registros detallados de pruebas realizadas, resultados obtenidos y medidas propuestas facilita el seguimiento de las recomendaciones y la toma de decisiones informadas.
- **Comunicación constante con la organización auditada:** establecer un canal de comunicación fluido con los responsables técnicos y de seguridad permite ajustar el alcance, resolver dudas y aumentar la efectividad del proceso.
- **Evaluación del factor humano:** incluir simulaciones de ataques de ingeniería social, como campañas de phishing controladas, para identificar debilidades en la concienciación del personal.

3.6.2. Buenas prácticas dentro de la organización auditada

Más allá de las técnicas aplicadas por el equipo auditor, las organizaciones deben adoptar un conjunto de buenas prácticas estructurales para mejorar su postura de seguridad a largo plazo:

- **Segmentación adecuada de la red:** separar físicamente o virtualmente las distintas áreas de la red reduce la superficie de ataque y limita el daño potencial de un incidente.
- **Gestión continua de parches y actualizaciones:** mantener todo el software actualizado es crucial para evitar vulnerabilidades conocidas.
- **Implementación de sistemas avanzados de detección y prevención de intrusiones (IDS/IPS):** estos sistemas permiten detectar amenazas en tiempo real y reaccionar rápidamente.
- **Planes de respuesta ante incidentes:** preparar protocolos claros que guíen las acciones inmediatas ante una brecha de seguridad o incidente detectado.
- **Formación y concienciación continuas del personal:** sesiones periódicas sobre buenas prácticas, manejo de información sensible, identificación de amenazas comunes como phishing o ransomware, y cómo responder adecuadamente ante incidentes.
- **Monitorización continua y análisis de amenazas:** emplear herramientas y recursos comunitarios como **Exploit DB** y el estándar **CVE (Common Vulnerabilities and Exposures)**, permite a los equipos de seguridad mantenerse actualizados sobre nuevas amenazas y vulnerabilidades.
- **Gestión profesional desde un SOC (Security Operations Center):** contar con un Centro de Operaciones de Seguridad activo permite centralizar la supervisión, detección y respuesta ante incidentes de forma continua. Un SOC bien gestionado ofrece una visión integral del estado de la seguridad de la organización, automatiza alertas, coordina respuestas y permite tomar decisiones informadas basadas en datos en tiempo real. Este trabajo es llevado a cabo habitualmente por un equipo **Blue Team**, responsable de defender los activos frente a ataques reales. Su función es crítica para asegurar la continuidad del negocio y minimizar el impacto de amenazas, tanto externas como internas.

Finalmente, para ilustrar en tiempo real la magnitud y frecuencia global de estos ataques y reforzar la importancia de adoptar medidas proactivas, puede consultarse el mapa interactivo proporcionado por Fortinet en el siguiente enlace: fortiguard.fortinet.com/threat-map.

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/cmadril/2024/10/22/que-cambia-la-directiva-de-la-ue-que-mejora-la-ciberseguridad-y-ya-aplican-los-estados-ser-madril/>
- [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] Felipe Redondo, A. M., & Núñez Cárdenas, F. J. (2024). *Criterios de selección de herramientas para pentesting*. Ciencia Huasteca Boletín Científico de la Escuela Superior de Huejutla, 12(24), 31-35. Recuperado de <https://repository.uaeh.edu.mx/revistas/index.php/huejutla/article/view/12763/11251>
- [11] Hiscox (2022). *44 % de las pymes españolas sufrió al menos un ciberataque durante 2021* Recuperado de <https://www.hiscox.es/el-44-de-las-pymes-espanolas-sufrio-al-menos-un-ciberataque-durante-2021>
- [12] INCIBE (2023). *INCIBE gestionó más de 118.000 incidentes de ciberseguridad durante 2022, un 9 % más que en 202* Recuperado de <https://www.incibe.es/incibe/sala-de-prensa/incibe-gestiono-mas-115000-incidentes-ciberseguridad-durante-2022-9-mas>
- [13] POW (2021). *El 86 % de las compañías españolas carecen de una cultura de ciberseguridad entre los empleados* Recuperado de <https://www.pwc.es/es/sala-prensa/notas-prensa/2021/companias-espanolas-cultura-ciberseguridad-empleados.html>
- [14] Toms, L. (2021). *5 riesgos de seguridad para las PYMEs que se deben tener en cuenta* Recuperado de <https://www.globalsign.com/es/blog/top-5-pequena-empresa-grandes-riesgos-5-riesgos-de-seguridad-para-las-pymes-que-se-deben-tener-en-cuenta>