



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

<b>1. Introducción</b>	<b>11</b>
1.1. Objetivos	12
1.2. Alcance	12
1.3. Motivación	12
1.4. Requisitos formales	13
1.4.1. Documentación e información	13
1.4.2. Normativas y certificaciones	13
1.4.3. Propuesta de metodología de la auditoría	13
1.4.4. Sobre el caso práctico	13
1.5. Estructura del documento	13
<b>2. Planificación</b>	<b>15</b>
2.1. Fases y lista de actividades	15
2.2. Cronograma	17
2.3. Roles y responsabilidades	19
2.4. Recursos	19
2.4.1. Recursos Humanos	19
2.4.2. Recursos Materiales	20
2.4.3. Costos Asociados	20
2.5. Estimación de Costes	20
<b>3. Fundamentos teóricos para una auditoría de ciberseguridad en PYMEs</b>	<b>22</b>
3.1. Principales amenazas y riesgos para PYMEs	22
3.2. Planes de Mitigación	25
3.3. Buenas prácticas	26
3.3.1. Buenas prácticas en PYMES	26
3.3.2. Buenas prácticas en auditorías de ciberseguridad	27
3.4. Marco Regulatorio y Metodológico en Ciberseguridad	28
3.4.1. Organismos Reguladores en Ciberseguridad	28
3.4.2. Normativas y Estándares Aplicables	31
3.4.3. Metodologías de Auditoría en Ciberseguridad	34
3.5. Herramientas de pentesting	35
3.6. Certificaciones del sector	35
<b>4. Metodología elegida: NIST SP 800-115</b>	<b>37</b>
4.1. Fase de Planificación (Planning Phase)	37
4.2. Fase de Descubrimiento (Discovery Phase)	37
4.3. Fase de Ataque (Attack Phase)	37
4.4. Fase de Reporte (Reporting Phase)	38
<b>5. Modelo de auditoría</b>	<b>39</b>
5.1. Diseño propuesto por BeeHacker	39
5.2. Análisis del Perímetro de Red	40
5.2.1. Fingerprint y Reconocimiento Interno	42
5.2.2. OSINT e Ingeniería Social	43
5.2.3. Seguridad en IoT	44
5.2.4. Auditoría Web	45
5.2.5. Seguridad de Infraestructura	46
5.2.6. Seguridad de Endpoints y Datos	47
<b>6. Requisitos previos a la auditoría</b>	<b>50</b>
<b>7. Propuesta metodológica de auditoría</b>	<b>51</b>
7.1. Fase de Planificación de la Auditoría	51
7.2. Fase de Descubrimiento	51

<b>8. Caso Práctico</b>	<b>52</b>
8.1. Implementación de la auditoría . . . . .	52
8.2. Planificación de la auditoría . . . . .	52
<b>9. Resultados</b>	<b>53</b>
<b>10. Conclusiones</b>	<b>54</b>
<b>11. Anexos</b>	<b>58</b>

## Índice de figuras

1.	Cronograma del proyecto. Fuente: Elaboración propia. . . . .	18
2.	Evolución histórica de la cantidad total de malware y PUA a nivel mundial. Fuente: AV-TEST [2]. . . . .	23
3.	Mapa global de ciberamenazas en tiempo real. Fuente: Fortinet [4]. . . . .	25
4.	Pilares fundamentales de INCIBE. Fuente: INCIBE [9]. . . . .	28
5.	Funciones del Marco de Ciberseguridad de NIST. Fuente: DEVICE42 Company device42. . . . .	30
6.	Triada de la Información. Fuente: 4IT Networks [41] . . . . .	33
7.	Metodología NIST SP 800-115. Fuente: [14] . . . . .	37
8.	Diagrama de flujo de los bloques del diseño del modelo de auditoría. Fuente: Elaboración propia . . . . .	39

## Índice de cuadros

1.	Distribución de roles y responsabilidades en el proyecto . . . . .	19
2.	Recursos Humanos . . . . .	19
3.	Recursos Materiales . . . . .	20
4.	Costos Asociados . . . . .	20
5.	Resumen de costes del proyecto . . . . .	21
6.	Medidas de mitigación y su efectividad. . . . .	26
7.	Certificaciones GIAC ofrecidas por SANS y sus áreas de especialización . . . . .	31
8.	Comparativa de normativas y estándares en ciberseguridad. . . . .	34
9.	Herramientas de pentesting más empleadas . . . . .	35
10.	Tabla de trazabilidad de objetivos en el análisis del perímetro de red . . . . .	40
11.	Tabla de trazabilidad de objetivos en la fase de Fingerprint interno . . . . .	42
12.	Tabla de trazabilidad de objetivos en la fase OSINT e Ingeniería Social . . . . .	43
13.	Tabla de trazabilidad de objetivos en la auditoría de dispositivos IoT . . . . .	44
14.	Tabla de trazabilidad de objetivos en la auditoría de aplicaciones web . . . . .	45
15.	Tabla de trazabilidad de objetivos en la evaluación de la seguridad de la infraestructura . . . . .	46
16.	Tabla de trazabilidad de objetivos en la auditoría de seguridad de endpoints y datos . . . . .	48
17.	Listado de herramientas utilizadas en auditorías de ciberseguridad y sus referencias oficiales . . . . .	58

## Agradecimientos

### Familiares

A mi familia, por estar siempre presente en cada paso del camino. Gracias por vuestro amor, comprensión y por haberme dado el apoyo necesario, también en lo económico, para poder continuar con mi formación.

## Mi pareja y familiares

A mi pareja y a su familia, por su apoyo incondicional y por sostenerme en los momentos más difíciles. Gracias por estar siempre, por el cariño, la paciencia y por motivarme a seguir adelante cuando más lo necesitaba.

## Mi Tutor

A mi tutor Alejandro, por aceptar ser parte de este camino. Gracias por la confianza depositada en mí, por las facilidades aportadas y por abrirme la puerta hacia una nueva etapa profesional.



**BeeHacker**

A la empresa Beehacker, por su colaboración en este proyecto. Agradezco sinceramente la oportunidad que me han ofrecido para aplicar mis conocimientos en un entorno real y su implicación durante todo el proceso.

## Resumen

Las pequeñas y medianas empresas (PYMEs) desempeñan un papel fundamental en la economía global. Sin embargo, su creciente digitalización ha incrementado su exposición a ciberataques, debido a infraestructuras de seguridad limitadas y a la falta de recursos suficientes para hacer frente a 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 avanzados, que les permita evaluar la seguridad de sus entornos digitales de forma autónoma.

El proyecto se estructura en dos fases principales. La primera está centrada en el establecimiento de un marco teórico que aborde los fundamentos esenciales de la ciberseguridad ofensiva. Esta etapa ofrece una visión general de los aspectos más relevantes en el ámbito de la auditoría de ciberseguridad, incluyendo las herramientas más utilizadas, la normativa vigente y las metodologías comúnmente aplicadas. Además, se incluye una recopilación de certificaciones recomendadas para quienes se inician en este campo, con el objetivo de orientar su formación. También se incorpora una sección dedicada a las buenas prácticas en ciberseguridad, con el fin de fomentar un enfoque ético y profesional desde las etapas iniciales.

La segunda fase está dedicada a la implementación práctica de la auditoría, siguiendo una metodología reconocida que abarca desde el análisis del perímetro de red hasta la evaluación de la seguridad de los datos. El diseño contempla pruebas en aplicaciones web, dispositivos IoT y la infraestructura interna de la organización. Esta fase culmina con un caso práctico que valida la eficacia de la metodología propuesta en un entorno real, proporcionando una guía clara sobre cómo aplicar las técnicas estudiadas.

Finalmente, se presentan los resultados obtenidos, ofreciendo una visión clara y estructurada del estado de ciberseguridad de la organización evaluada.

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

## Abstract

Small and medium-sized enterprises (SMEs) play a fundamental role in the global economy. However, their increasing digitalization has significantly raised their exposure to cyberattacks, due to limited security infrastructures and insufficient resources to address sophisticated threats. This project aims to develop a cybersecurity audit model specifically tailored to SMEs, based on current European and national regulations. To ensure its usability, an accessible guide will be created for users without advanced technical knowledge, enabling them to assess the security of their digital environments independently.

The project is structured into two main phases. The first focuses on establishing a theoretical framework that covers the essential principles of offensive cybersecurity. This stage provides a general overview of the most relevant areas within cybersecurity auditing, including widely used tools, applicable regulations, and common methodologies. In addition, a compilation of recommended certifications is included to guide newcomers in the field. A dedicated section on cybersecurity best practices is also provided, aiming to promote an ethical and professional approach from the early stages of learning.

The second phase is dedicated to the practical implementation of the audit, following a recognized methodology that encompasses everything from network perimeter analysis to data security assessment. The design includes tests on web applications, IoT devices, and the company's internal infrastructure. This phase concludes with a practical case study that demonstrates the validity of the proposed methodology in a real-world environment, offering a clear illustration of how the learned techniques can be applied.

Finally, the results obtained are presented, providing a clear and structured overview of the cybersecurity posture of the evaluated organization.

**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 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 que las PYMEs fortalezcan su seguridad informática 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 los fundamentos necesarios para dar una base inicial a cualquier persona interesada en la ciberseguridad.
- Proponer una metodología de auditoría completa 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.
- Elaborar una guía clara y comprensible, diseñada específicamente para ser utilizada por personas con conocimientos básicos de ciberseguridad.

### 1.2. Alcance

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

1. **Marco teórico:** Se analizarán las principales amenazas y riesgos a los que se enfrentan las PYMEs, así como las herramientas más utilizadas en las auditorías de ciberseguridad. Además, se abordarán las normativas más relevantes tanto a nivel nacional como europeo, junto con las metodologías reconocidas dentro del sector. También se incluirán recomendaciones de buenas prácticas desde la perspectiva de una PYME y de un auditor de seguridad. Por último, se presentará una selección de certificaciones fundamentales en el ámbito de la ciberseguridad, con el objetivo de orientar a quienes deseen iniciarse profesionalmente en este campo.
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 exhaustivo de todos los aspectos a evaluar en una auditoría de ciberseguridad completa. Esta abarcará el perímetro de red, la seguridad inalámbrica, la identificación de vulnerabilidades, 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 de manera parcial 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 un fácil objetivo 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.

Además, una de las principales motivaciones personales que ha impulsado la realización de este trabajo es mi interés en formarme profesionalmente como pentester. Este proyecto representa un primer paso en ese camino, permitiéndome aplicar conocimientos teóricos y prácticos en un entorno real. Al mismo tiempo, me gustaría que esta guía pudiera servir como punto de partida para otros estudiantes en prácticas o personas con poca experiencia que deseen introducirse en el ámbito de la ciberseguridad. De este modo, no solo se contribuye a la protección de las PYMEs, sino también al desarrollo de nuevos profesionales en el sector.

### 1.4. Requisitos formales

Una vez definido el contexto general del trabajo, se establecen los requisitos formales necesarios para la correcta redacción y desarrollo del documento.

#### 1.4.1. Documentación e información

- Los documentos pueden ser extraídos de *Google Scholar* para su posterior citación.
- Se recomienda utilizar publicaciones con una antigüedad no superior a 3 o 4 años, para asegurar la vigencia de la información
- Todos los documentos consultados se citarán en formato APA.
- Deben contener información relevante y actualizada sobre ciberseguridad en PYMEs.

#### 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:** Análisis de principales riesgos y amenazas a las que están expuestas las PYMEs, planes de mitigación, normativas nacionales y europeas aplicables, estándares, herramientas de pentesting, buenas prácticas y sección destinada a las certificaciones principales en el ámbito de la ciberseguridad ofensiva.
- **Metodología elegida:** Se expone la metodología de auditoría base para modelar nuestro propio modelo.
- **Modelo de auditoría:** Propuesta de un modelo de auditoría adaptado a las PYMEs, que incluye fases, herramientas y técnicas específicas.
- **Requisitos:** Definición de los requisitos previos a una auditoría de seguridad.
- **Propuesta 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.
- **Conclusión:** 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.

##### ■ 1.2 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 Definición de objetivos, alcance y requisitos:** Desarrollo de los objetivos específicos del proyecto, delimitación del alcance y definición de los requisitos necesarios para el desarrollo del producto.

##### ■ 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.

### Fase 2 - Desarrollo del Producto

- **2.1 Marco teórico**
  - **2.1.1 Desarrollo del marco teórico:** Investigación, análisis, redacción y estructuración del marco conceptual.
- **2.2 Metodología de auditoría**
  - **2.2.1 Elección de metodología:** Investigación, análisis, redacción de una metodología reconocida.
- **2.3 Diseño de auditoría**
  - **2.3.1 Desarrollo de objetivos:** Definición de objetivos propuestos para el desarrollo de una auditoría.
- **2.4 Requisitos previos a una auditoría**
  - **2.4.1 Desarrollo de requisitos:** Análisis y desarrollo de los requisitos formales necesarios previos a la evaluación de una auditoría de ciberseguridad.
- **2.5 Propuesta de auditoría**
  - **2.5.1 Diseño del modelo:** Definición de la estructura metodológica y los procedimientos a seguir.
  - **2.5.2 Revisión del modelo:** Revisión y aprobación del modelo de auditoría.
- **2.6 Caso práctico**
  - **2.6.1 Desarrollo del caso práctico:** Ejecución y aplicación en la PYME.
  - **2.6.2 Seguimiento de la práctica:** Monitorización y análisis del proceso.
- **2.7 Resultados**
  - **2.7.1 Descripción de resultados:** Descripción de los resultados obtenidos en el caso práctico.

### 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. Cronograma

El cronograma presentado a continuación muestra la planificación general del proyecto, centrada en las fases clave del desarrollo sin entrar en el detalle de cada tarea individual. La duración total del trabajo ha sido de nueve meses, dado que se le ha dado mayor importancia a partir del mes de mayo, una vez finalizadas las asignaturas del curso actual.

Para consultar un desglose más detallado de las actividades realizadas, incluyendo descripciones y tiempos invertidos en cada una, puede accederse al recurso utilizado para el seguimiento del proyecto [5].

En la siguiente figura se muestra el diagrama de Gantt, que recoge visualmente las distintas fases del proyecto y su distribución temporal.

# GRÁFICO GANTT

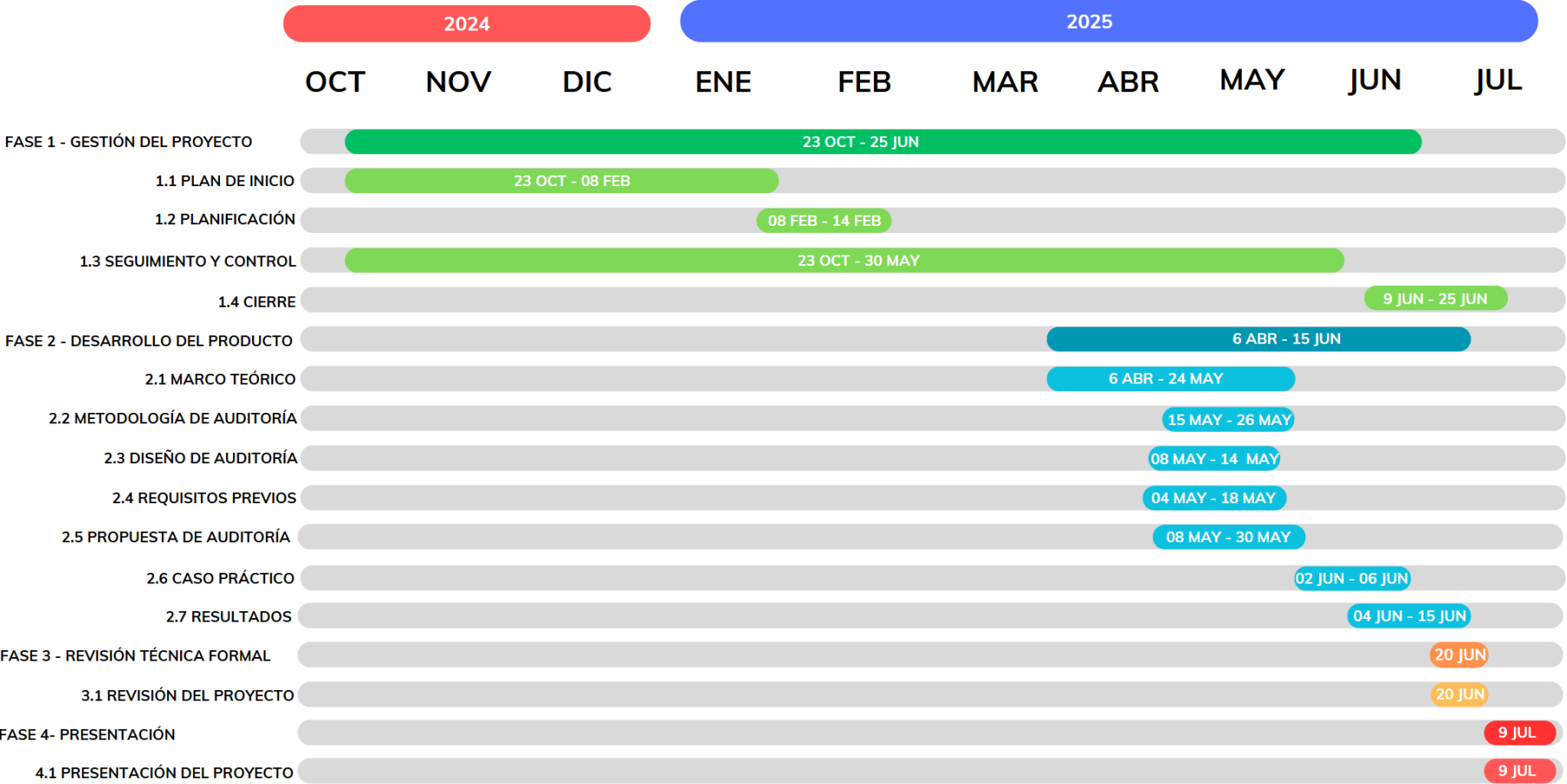


Figura 1: Cronograma del proyecto. Fuente: Elaboración propia.

### 2.3. 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

### 2.4. 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 [6], 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
Herramientas Hacking	Material	€500,00	1	€500,00

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 1230 €, 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	1230 €
Costos Asociados	1.100 €
<b>Total Estimado</b>	<b><u>18.291,50 €</u></b>

**Fuente:** Elaboración propia

### 3. Fundamentos teóricos para una auditoría de ciberseguridad en PYMEs

El presente marco teórico tiene como objetivo establecer una base sólida sobre los principios fundamentales de la ciberseguridad aplicados al contexto de las pequeñas y medianas empresas (PYMEs). A lo largo del capítulo se abordarán los principales riesgos y amenazas que enfrentan estas organizaciones en el entorno digital, así como planes de mitigación que ofrecen estrategias prácticas para reducir su exposición a ciberataques.

Posteriormente, se detallan las buenas prácticas recomendadas, distinguiendo entre aquellas que deben adoptar internamente las PYMEs y las que se aplican durante las auditorías de seguridad, contribuyendo así a un enfoque integral desde ambas perspectivas.

A continuación, se exponen las normativas nacionales y europeas más relevantes, que definen el marco legal y regulatorio que debe ser respetado por las PYMEs para asegurar la protección de sus activos digitales. Además, se presentan los estándares y metodologías de auditoría más reconocidos internacionalmente, para basar la propuesta de auditoría en algunos de ellos.

Finalmente, se describe las herramientas más usadas en auditorías de ciberseguridad y se dedica un último apartado para orientar a quienes deseen especializarse en ciberseguridad ofensiva, incluyendo las certificaciones profesionales más relevantes, organizadas por nivel de dificultad, que permiten diseñar un itinerario formativo progresivo y efectivo.

Esta exposición teórica sentará las bases para el desarrollo posterior de una propuesta concreta de auditoría de ciberseguridad adaptada a las necesidades específicas de las PYMEs.

#### 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 este sector. [38]

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.[39]

Aunque cada vez más PYMEs aumentan sus presupuestos en ciberseguridad y colaboran con empresas especializadas, muchas todavía optan por contratar a otras empresas especializadas para que se encarguen de gestionar sus servicios de ciberseguridad, por falta de personal y recursos internos. Esta externalización, 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 en pie la necesidad urgente de concienciación.[40]

Entre las principales ciberamenazas que afectan a las PYMEs según la empresa de Software Treyder [43] se encuentran:

- **Malware:** El término engloba todo tipo de software malicioso diseñado para infiltrarse o dañar un sistema sin el consentimiento del usuario. Incluye virus, troyanos, spyware y especialmente ransomware, que cifra los datos del sistema y exige un rescate económico para su recuperación. Las

PYMES suelen ser víctimas de malware distribuido por correos adjuntos infectados o a través de enlaces maliciosos en páginas aparentemente legítimas. Además del daño económico, el malware puede provocar la pérdida permanente de datos, el control remoto de equipos y el espionaje corporativo.

La relevancia del malware como una de las principales ciberamenazas se refleja claramente en su evolución histórica. Tal y como muestra el informe de AV-TEST, la cantidad total de software malicioso (malware) y aplicaciones potencialmente no deseadas (PUA) ha experimentado un crecimiento exponencial en las últimas décadas, superando en 2024 los 1.500 millones de muestras registradas a nivel mundial. Este aumento constante evidencia que las amenazas digitales siguen sofisticándose y expandiéndose, afectando por igual a grandes empresas y a pequeñas organizaciones como las PYMES.

TOTAL AMOUNT OF MALWARE AND PUA

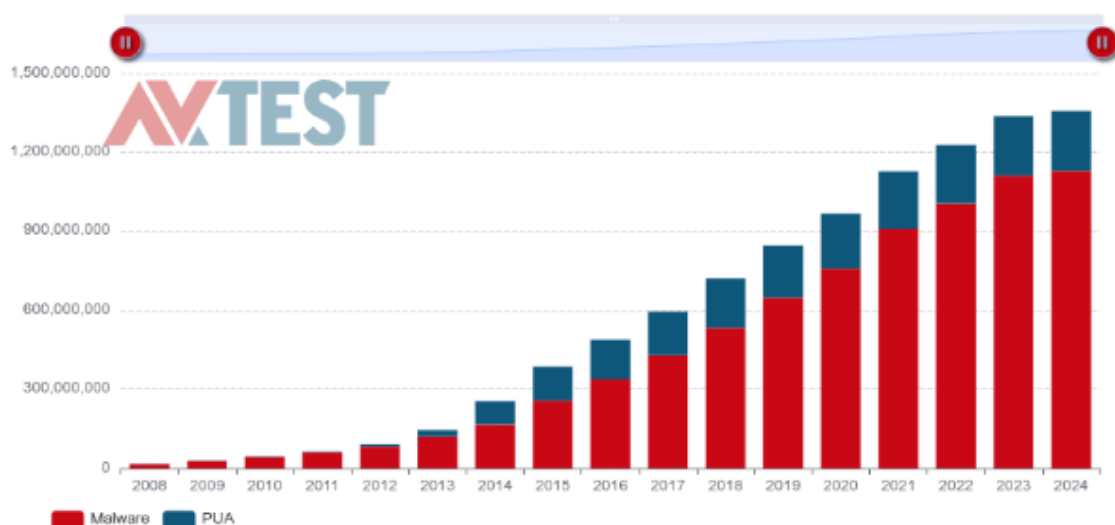


Figura 2: Evolución histórica de la cantidad total de malware y PUA a nivel mundial. Fuente: AVTEST [2].

Aparte del malware, existen otras amenazas igualmente relevantes para las PYMES:

- **Phishing:** Consiste en técnicas de suplantación de identidad para engañar y obtener datos confidenciales, como contraseñas, credenciales bancarias o información sensible de clientes. Suele realizarse mediante correos electrónicos o mensajes falsificados que imitan a bancos, plataformas de pago o servicios tecnológicos conocidos. En las PYMES, donde el nivel de concienciación en ciberseguridad suele ser limitado, el phishing representa una puerta de entrada frecuente a ataques más complejos, como el acceso remoto a sistemas o la instalación de malware. [7]
- **Ataques de denegación de servicio (DDoS):** Este tipo de ataque busca hacer que los servidores, aplicaciones o sitios web de una empresa queden inoperativos mediante el envío masivo de peticiones falsas. Se trata de una sobrecarga intencionada de los recursos tecnológicos de la organización, que impide el funcionamiento normal de servicios clave. Aunque muchas veces se asocian a grandes empresas, las PYMES también son objetivo, especialmente si ofrecen servicios digitales o tiendas online. Un DDoS puede paralizar las operaciones durante horas o días, con pérdidas económicas importantes y daño reputacional. [7]
- **Brechas de datos:** Ocurren cuando un atacante consigue acceder sin autorización a bases de datos internas, habitualmente mediante credenciales robadas, vulnerabilidades no parcheadas o ingeniería



social. Estas brechas pueden afectar a información crítica como datos de clientes, contraseñas, información financiera o planes estratégicos. Para una PYME, una brecha de datos no solo puede suponer sanciones legales (por ejemplo, si no cumple con el Reglamento General de Protección de Datos (RGPD)), sino también pérdida de confianza por parte de clientes y socios. [7]

- **Errores de configuración:** Son fallos humanos o técnicos al configurar correctamente sistemas, redes o aplicaciones. Por ejemplo, dejar puertos abiertos innecesarios, permitir contraseñas por defecto, o no establecer permisos adecuados. Estos errores abren puertas invisibles a los ciberatacantes y son especialmente comunes en entornos donde no existe un departamento de TI dedicado. La falta de mantenimiento o revisión de estas configuraciones puede convertir una infraestructura aparentemente segura en un objetivo fácil. [7]

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

- **Falta de recursos de seguridad:** 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 ser muy pobre 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. [42]

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, donde se muestran los ciberataques que se acontecen en tiempo real, proporcionado por Fortinet.



Figura 3: Mapa global de ciberamenazas en tiempo real. Fuente: Fortinet [4].

### 3.2. Planes de Mitigación

Para reducir los riesgos derivados de incidentes de ciberseguridad, es fundamental contar con planes de mitigación bien estructurados, que contemplen diversas medidas técnicas y organizativas. Entre las estrategias más efectivas destacan el uso de **firewalls y filtros de red**, que actúan como barreras de protección frente a accesos no autorizados; el **monitoreo continuo de red**, que permite la detección temprana de comportamientos anómalos; y la **protección frente a ataques DDoS**, que asegura la disponibilidad de los servicios durante intentos de saturación del sistema.

Otras medidas incluyen la aplicación periódica de **actualizaciones y parches** para corregir vulnerabilidades conocidas, la implementación de **mecanismos de autenticación y control de acceso** robustos, y el **cifrado del tráfico de datos** para garantizar la confidencialidad durante la transmisión. La **segmentación de red** también se presenta como una medida eficaz para contener amenazas, al limitar su propagación a segmentos específicos.

Asimismo, la **gestión proactiva de vulnerabilidades**, la **educación en ciberseguridad** del personal, y la adopción de **políticas de seguridad claras y bien definidas** son elementos esenciales para una postura de seguridad integral. Finalmente, contar con sistemas de **respaldo y recuperación de datos**, así como fomentar la **colaboración con la comunidad de ciberseguridad**, fortalece significativamente la capacidad de respuesta ante incidentes y la resiliencia organizacional frente a amenazas emergentes [3].

Cuadro 6: Medidas de mitigación y su efectividad.

Medida de mitigación	Características
Firewalls y filtros de red	Establecen barreras de protección, controlan el tráfico y bloquean accesos no autorizados. Efectivos ante intrusiones externas.
Monitoreo de red continuo	Permite la detección temprana de comportamientos anómalos y actividades sospechosas para una respuesta rápida.
Protección contra DDoS	Mitiga ataques de denegación de servicio distribuido, asegurando la continuidad operativa.
Actualizaciones y parches	Mantiene el software actualizado, cerrando vulnerabilidades conocidas y reduciendo el riesgo de explotación.
Autenticación y control de acceso	Implementa verificación de identidad y restricciones de acceso a recursos sensibles, previniendo accesos no autorizados.
Cifrado de tráfico	Protege la confidencialidad de los datos durante su transmisión entre servidores y usuarios.
Segmentación de red	Divide la red en zonas aisladas para limitar la propagación de amenazas internas.
Gestión de vulnerabilidades	Identifica y corrige debilidades de forma proactiva, fortaleciendo la postura de seguridad.
Educación en ciberseguridad	Capacita al personal en buenas prácticas y prevención de ataques como la ingeniería social.
Políticas de seguridad robustas	Define protocolos, responsabilidades y buenas prácticas para fomentar una cultura de seguridad.
Respaldo y recuperación de datos	Garantiza la disponibilidad y restauración ante pérdida de datos o ciberataques.
Colaboración con la comunidad de ciberseguridad	Facilita el intercambio de información y estrategias para enfrentar amenazas comunes.

**Fuente:** EXPLORACIÓN INTEGRAL DE LA SEGURIDAD EN REDES DE PROVEEDORES DE SERVICIOS DE INTERNET [3]

### 3.3. Buenas prácticas

Las buenas prácticas en el ámbito de la ciberseguridad constituyen un conjunto de acciones, políticas y medidas preventivas que buscan minimizar riesgos, proteger la información y garantizar la continuidad operativa ante posibles amenazas. En este apartado se diferenciarán dos perspectivas clave: por un lado, las buenas prácticas que una PYME debe implementar de forma interna para fortalecer su seguridad digital; y por otro, aquellas prácticas recomendadas y seguidas durante las auditorías de ciberseguridad, las cuales permiten evaluar el estado real de la infraestructura tecnológica y proponer mejoras efectivas.

#### 3.3.1. Buenas prácticas en PYMES

La ciberseguridad en pequeñas y medianas empresas requiere un enfoque integral que combine herramientas, políticas, concienciación y planificación estratégica. Una única medida no es suficiente para garantizar la protección frente a las amenazas actuales. A continuación, se detallan algunas de las buenas prácticas más relevantes que una PYME debe adoptar para construir un entorno digital más seguro, según las recomendaciones de expertos [42]:

- **Documentación de procesos y protocolos:** Muchas PYMEs asignan a una sola persona la responsabilidad de la configuración y gestión de la seguridad informática. Sin embargo, esto supone un riesgo si esa persona abandona la empresa, ya que el conocimiento no queda registrado. Documentar todos los procesos, configuraciones y políticas de seguridad permite mantener la continuidad operativa, facilita auditorías internas y evita que la salida de personal clave comprometa la seguridad.

- **Contraseñas seguras y autenticación multifactorial (MFA):** El uso de contraseñas débiles es una de las principales vulnerabilidades explotadas por los atacantes. Se recomienda utilizar contraseñas largas (mínimo 12 caracteres), con combinación de letras, números y símbolos especiales. Además, es esencial implementar mecanismos de autenticación de doble factor (por ejemplo, mediante contraseña y huella dactilar, o código de un solo uso vía SMS), lo que añade una capa adicional de protección frente a accesos no autorizados.
- **Formación continua de los empleados:** Los empleados suelen ser tanto la primera como la última línea de defensa ante ciberataques. Sin una formación adecuada, es más probable que caigan en fraudes por correo electrónico, enlaces maliciosos o campañas de phishing dirigidas. Las PYMES deben establecer programas de concienciación en ciberseguridad que incluyan formación sobre detección de amenazas, políticas de uso de dispositivos personales, buenas prácticas en navegación, y respuesta ante incidentes.
- **Enfoque de seguridad por capas (defensa en profundidad):** La protección de los sistemas debe estar basada en múltiples niveles de seguridad que actúen de forma coordinada. Entre las medidas recomendadas se incluyen: antivirus y antispyware actualizados, configuración adecuada del firewall, control de accesos, cifrado de los datos en tránsito y en reposo, y uso de firmas digitales para garantizar la integridad de los documentos. Esta arquitectura de defensa en profundidad mejora la resiliencia frente a ataques dirigidos o automatizados.
- **Copias de seguridad regulares y distribuidas:** Las copias de seguridad son fundamentales para asegurar la recuperación de datos tras incidentes como ransomware, fallos de hardware o errores humanos. Se recomienda realizar copias frecuentes, almacenarlas en diferentes ubicaciones (local, nube o dispositivos externos), y verificar periódicamente que pueden restaurarse correctamente. Esta práctica sencilla puede marcar la diferencia entre la continuidad del negocio o la pérdida irreversible de información crítica.

#### 3.3.2. Buenas prácticas en auditorías de ciberseguridad

Las auditorías son procesos estructurados que permiten evaluar el estado de la seguridad informática de una organización. Para que sean eficaces, deben llevarse a cabo bajo un conjunto de buenas prácticas que garanticen no solo la calidad técnica del análisis, sino también la ética profesional, la trazabilidad de los hallazgos y la aplicabilidad de las recomendaciones. A continuación, se describen las principales buenas prácticas que deben seguirse durante una auditoría de ciberseguridad:

- **Definición clara del alcance:** Antes de iniciar cualquier auditoría, es fundamental delimitar qué sistemas, redes, aplicaciones, ubicaciones y personas serán objeto de evaluación. Un alcance bien definido evita malentendidos, asegura que los recursos estén disponibles y permite centrar los esfuerzos en los activos más críticos.
- **Formalización mediante acuerdos previos:** Toda auditoría debe comenzar con la firma de acuerdos de confidencialidad (NDA) y documentos de autorización por parte de la empresa auditada. Esto garantiza que el proceso se realice dentro del marco legal y ético, y protege tanto al auditor como a la organización.
- **Aplicación de metodologías reconocidas:** Las auditorías deben basarse en estándares y marcos metodológicos ampliamente aceptados, como PTES (Penetration Testing Execution Standard), OSSTMM (Open Source Security Testing Methodology Manual), o las guías del NIST (por ejemplo, SP 800-115). Esto asegura un enfoque sistemático, riguroso y alineado con las mejores prácticas internacionales.
- **Uso controlado de herramientas especializadas:** El empleo de herramientas debe realizarse de forma responsable, en entornos previamente autorizados, y con medidas que minimicen posibles interrupciones del servicio. Se recomienda documentar cada herramienta utilizada, junto con su propósito y los resultados obtenidos.
- **Documentación exhaustiva de hallazgos:** Cada vulnerabilidad o debilidad detectada debe registrarse con claridad, incluyendo una descripción técnica, nivel de riesgo, posible impacto y evidencias que lo respalden. Esta documentación será esencial para la elaboración del informe final.

- **Informe técnico y ejecutivo:** El resultado de la auditoría debe presentarse en dos formatos: uno técnico, dirigido al personal de sistemas, y otro ejecutivo, accesible para la dirección de la empresa. Ambos informes deben incluir un plan de acción priorizado y recomendaciones específicas y viables.
- **Propuesta de mejora continua:** La auditoría no debe verse como un fin en sí misma, sino como parte de un proceso de mejora continua. Es importante que el informe incluya sugerencias para establecer controles recurrentes, políticas de seguridad y mecanismos de revisión periódica.
- **Ética profesional y confidencialidad:** Durante todo el proceso, el equipo auditor debe actuar con responsabilidad, integridad y confidencialidad. Cualquier hallazgo crítico debe comunicarse de inmediato a los responsables de seguridad de la organización, sin esperar al informe final.

## 3.4. Marco Regulatorio y Metodológico en Ciberseguridad

### 3.4.1. Organismos Reguladores en Ciberseguridad

En España, diversos organismos desempeñan un papel clave en la regulación, supervisión y fomento de la ciberseguridad. Entre ellos destacan:

#### Instituto Nacional de Ciberseguridad (INCIBE)

Es una entidad pública de referencia nacional en materia de ciberseguridad, vinculada al Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial. INCIBE desempeña un papel esencial en el impulso de la ciberseguridad en España, especialmente orientado al sector empresarial. [9]

Los pilares fundamentales sobre los que se estructura la actividad de esta organización son:

- **Protección, Prevención y Reacción** ante incidentes de ciberseguridad.
- **Investigación** y desarrollo de tecnologías aplicadas a la seguridad.
- **Generación de inteligencia** para anticipar amenazas y vulnerabilidades.
- **Mejora de servicios** y capacidades en ciberseguridad.
- **Colaboración activa** con entidades públicas y privadas para reforzar el ecosistema de seguridad digital.



Figura 4: Pilares fundamentales de INCIBE. Fuente: INCIBE [9].

#### Centro Nacional de Inteligencia (CNI)

Es el organismo responsable de proporcionar al Gobierno información y análisis necesarios para prevenir y contrarrestar cualquier amenaza contra la soberanía, integridad y seguridad nacional, incluyendo las de naturaleza cibernética. A través de estrategias de inteligencia y cooperación con otras agencias, tanto nacionales como internacionales, el CNI participa activamente en la defensa frente a ciberamenazas que puedan poner en riesgo los intereses fundamentales del país. [10]

#### Centro Criptológico Nacional (CCN-CERT)

Forma parte del Centro Nacional de Inteligencia (CNI) y actúa como el equipo de respuesta a incidentes de ciberseguridad para las administraciones públicas y entidades que gestionan infraestructuras críticas. Su función principal es prevenir, detectar y responder a ciberamenazas que puedan comprometer los sistemas del sector público español. Además, el CCN-CERT emite guías técnicas, alertas, buenas prácticas y herramientas diseñadas para aumentar la capacidad defensiva del Estado ante ciberincidentes. [11]

#### Agencia Española de Protección de Datos (AEPD)

Autoridad independiente encargada de supervisar el cumplimiento del Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica 3/2018 (LOPD-GDD), además de ofrecer orientación y recursos a organizaciones para gestionar datos personales de manera segura [12].

Además, existen organismos internacionales relevantes cuya influencia en ciberseguridad tiene alcance global, incluidos España y Europa:

#### National Institute of Standards and Technology (NIST)

Es una agencia federal estadounidense que desarrolla estándares, directrices y mejores prácticas en ciberseguridad. Reconocido a nivel internacional, el NIST ha establecido marcos de referencia ampliamente adoptados por organizaciones públicas y privadas para gestionar eficazmente los riesgos asociados a la seguridad digital [13].

Uno de sus marcos más influyentes es el **NIST Cybersecurity Framework (CSF)**, una guía estructurada para que cualquier organización pueda identificar, proteger, detectar, responder y recuperar frente a ciberincidentes. Este modelo se basa en cinco funciones clave:

1. **Identificar (Identify)**: comprender el entorno organizativo, sus activos y riesgos para establecer un enfoque de gestión de seguridad adecuado.
2. **Proteger (Protect)**: desarrollar y aplicar medidas de salvaguarda para limitar o contener el impacto de un incidente.
3. **Detectar (Detect)**: implementar actividades que permitan identificar de forma oportuna la ocurrencia de eventos de ciberseguridad.
4. **Responder (Respond)**: tomar medidas para contener el impacto de un evento detectado, mediante planes, comunicaciones, análisis y mitigación.
5. **Recuperar (Recover)**: restaurar las capacidades afectadas para garantizar la continuidad del negocio tras un incidente.

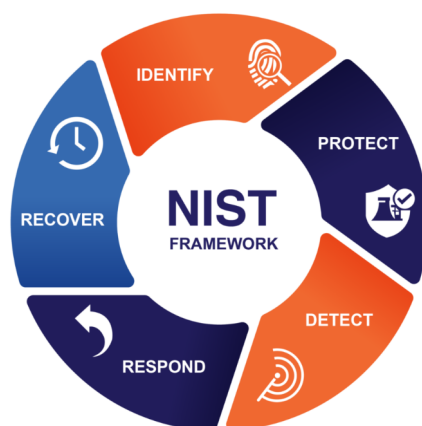


Figura 5: Funciones del Marco de Ciberseguridad de NIST. Fuente: DEVICE42 Company device42.

Este enfoque es adaptable y escalable, y ha sido adoptado no solo en Estados Unidos, sino también en muchos países como referencia para desarrollar políticas nacionales de ciberseguridad y estándares corporativos.

Otra pieza fundamental desarrollada por esta entidad es la **serie NIST Special Publications 800 (SP 800)**, que comprende más de 130 documentos gratuitos disponibles para descarga, en los que se describen políticas, procedimientos y directrices sobre ciberseguridad, evaluaciones de riesgos, controles técnicos y auditoría. Esta colección se considera una de las fuentes más completas y detalladas en materia de seguridad de la información.

Dentro de esta serie, se encuentran guías ampliamente reconocidas como la NIST SP 800-53 (controles de seguridad y privacidad) o la SP 800-115 (metodología para pruebas técnicas de seguridad). En capítulos posteriores, se seleccionarán y adaptarán varias de estas metodologías como base para diseñar nuestra propia propuesta de auditoría adaptada al contexto de PYMES.

## SANS Institute (SysAdmin, Audit, Networking, and Security Institute)

Es una de las organizaciones más reconocidas a nivel mundial en el ámbito de la ciberseguridad. Su objetivo principal es proporcionar formación avanzada y especializada en seguridad informática a profesionales, empresas y organismos públicos. SANS ofrece una amplia variedad de cursos presenciales y virtuales, que cubren áreas como análisis forense, respuesta ante incidentes, seguridad ofensiva, defensiva y gestión de riesgos.

Además de sus programas de formación, SANS es responsable de desarrollar y mantener recursos ampliamente utilizados en la industria, como el Top 20 Critical Security Controls y el proyecto GIAC (Global Information Assurance Certification). GIAC es un sistema de certificación reconocido internacionalmente que valida las competencias técnicas en múltiples especialidades de ciberseguridad, desde pentesting hasta auditoría o administración de sistemas seguros. [15]



Cuadro 7: Certificaciones GIAC ofrecidas por SANS y sus áreas de especialización

Área de especialización	Certificación GIAC
Seguridad general	GSEC (Security Essentials)
Pentesting y hacking ético	GPEN (Penetration Tester), GXPEN (Exploit Researcher)
Respuesta ante incidentes	GCIH (Incident Handler)
Análisis forense	GCFA (Forensic Analyst), GCFE (Forensic Examiner)
Administración de sistemas seguros	GCWN (Windows), GCUX (Unix/Linux)
Gestión de riesgos y auditoría	GSNA (Systems and Network Auditor), GRCP (Risk and Compliance)
Defensa de redes y sistemas	GCIA (Intrusion Analyst), GCCC (Critical Controls)

### 3.4.2. Normativas y Estándares Aplicables

En el contexto nacional y europeo, las normativas más relevantes en ciberseguridad aplicables especialmente a PYMEs son:

#### Esquema Nacional de Seguridad (ENS)

Regulado por el Real Decreto 311/2022, el Esquema Nacional de Seguridad (ENS) establece los principios básicos y los requisitos mínimos necesarios para una adecuada protección de la información manejada por medios electrónicos. Está dirigido tanto a las administraciones públicas como a aquellas entidades del sector privado que colaboran con el sector público.

Su objetivo principal es garantizar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad y la conservación de los datos. Para ello, el ENS define tres niveles de seguridad (bajo, medio y alto) y obliga a realizar un análisis de riesgos para aplicar las medidas correspondientes. El marco del ENS también contempla la implantación de una política de seguridad y la designación de responsables de seguridad en las organizaciones [16].

#### Reglamento General de Protección de Datos (RGPD)

Es una normativa implementada en la Unión Europea que regula la legislación sobre protección de datos en todos los Estados miembros. Su aplicación es obligatoria para todas las organizaciones que procesen datos personales de ciudadanos de la UE, independientemente de su ubicación [17].

El RGPD introduce aspectos clave incorporar la protección de datos desde el diseño y por defecto (privacy by design and by default), garantizando que la privacidad sea un elemento central desde las fases iniciales de cualquier proceso o sistema que trate información personal. Asimismo, establece el principio de responsabilidad activa (accountability), que obliga a las organizaciones no solo a cumplir con la normativa, sino a poder demostrarlo mediante documentación adecuada, análisis de riesgos, aplicación de medidas técnicas y organizativas proporcionales, y políticas de concienciación y formación continuas.

También establece el deber de notificar las brechas de seguridad a la autoridad de control en un plazo máximo de 72 horas, y en ciertos casos, también a los afectados.

#### Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPD-GDD)

La Ley Orgánica 3/2018 adapta al ordenamiento jurídico español el Reglamento Europeo RGPD, estableciendo obligaciones detalladas sobre la protección de datos personales, el tratamiento seguro de datos sensibles y la respuesta ante incidentes relacionados [18].



#### Directiva NIS2 (Directiva UE 2022)

Es una directiva europea diseñada para fortalecer y verificar las medidas de seguridad de la información que deben adoptar las empresas de los estados miembros de la Unión Europea, con el fin de garantizar un nivel elevado de ciberseguridad.[19].

Esta normativa afecta principalmente a medianas y grandes empresas pertenecientes a sectores críticos, estableciendo dos niveles de clasificación:

- **Entidades esenciales (EE)**: grandes empresas de sectores como energía, transporte, salud, DNS, administración pública, y otras definidas como críticas por los Estados miembros o por la Directiva (UE) 2022/2557.
- **Entidades importantes (EI)**: organizaciones medianas y grandes que, aunque no sean esenciales, cumplen tres criterios: ubicación en la UE, tamaño y pertenencia a uno de los 18 sectores regulados.

A diferencia de otras normativas como ISO/IEC 27001, la NIS2 **no es certificable**, pero **sí es obligatoria y sancionable** en caso de incumplimiento, lo que otorga un fuerte carácter legal a su aplicación.

Entre las medidas de seguridad requeridas por la Directiva NIS2 se incluyen:

- Implantación de un sistema de autenticación multifactor (MFA).
- Control de acceso basado en el principio de mínimo privilegio.
- Seguridad en la cadena de suministro, extendiendo la responsabilidad a proveedores y terceros.
- Implementación de sistemas para detectar, bloquear y mitigar ciberataques como el ransomware.
- Políticas de continuidad del negocio, como copias de seguridad y recuperación ante desastres.
- Formación en ciberhigiene y concienciación de seguridad para todos los empleados.

#### ISO/IEC 27001

Es un estándar de seguridad desarrollado por la Organización Internacional de Normalización (ISO), con el fin de ayudar a gestionar la seguridad de la información de una empresa. Su última versión fue publicada en Octubre de 2022. La ISO/IEC 27001 es certificable, permitiendo a las empresas solicitar auditorías externas a entidades certificadoras acreditadas. Si la empresa cumple con los requisitos definidos, obtiene una certificación que refleja públicamente su compromiso con la gestión segura de la información [20].

Un elemento clave de esta norma es el **Sistema de Gestión de Seguridad de la Información (SGSI)**, el cual consiste en un enfoque sistemático que permite establecer, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información dentro de una organización. El SGSI se basa en una evaluación de riesgos que define la forma en que estos riesgos deben ser tratados, estableciendo sus niveles de aceptación para gestionarlos eficazmente.

Asimismo, la seguridad de la información está fundamentada en la **triada de la información**, formada por tres principios esenciales: Confidencialidad, Integridad y Disponibilidad



Figura 6: Triada de la Información. Fuente: 4IT Networks [41]

- **Confidencialidad:** Garantiza que la información esté accesible únicamente para personas autorizadas. Utiliza mecanismos como la autenticación, controles de acceso y cifrado para evitar accesos indebidos.
- **Integridad:** Asegura la precisión y confiabilidad de los datos a lo largo de su ciclo de vida. Se mantiene a través de controles de versión, sumas de verificación, copias de seguridad, autenticación y cifrado.
- **Disponibilidad:** Busca asegurar que la información y los recursos tecnológicos sean accesibles y utilizables cuando sean necesarios. Se apoya en mecanismos y protocolos específicos diseñados para proteger la información crítica.

A continuación, se presenta una tabla comparativa que resume los objetivos principales de estas normativas y estándares, así como los grupos a los que afectan:

Normativa / Estándar	Objetivo Principal	Afectan a
ENS	<ul style="list-style-type: none"> <li>■ Establecer requisitos mínimos de seguridad.</li> <li>■ Proteger la información digital pública.</li> <li>■ Promover un enfoque basado en riesgos.</li> </ul>	<ul style="list-style-type: none"> <li>■ Organismos públicos.</li> <li>■ Empresas proveedoras del sector público.</li> </ul>
LOPD-GDD	<ul style="list-style-type: none"> <li>■ Garantizar los derechos digitales.</li> <li>■ Proteger datos personales.</li> <li>■ Adaptar el RGPD al ordenamiento español.</li> </ul>	<ul style="list-style-type: none"> <li>■ Empresas y entidades que traten datos personales en España.</li> </ul>
RGPD (UE)	<ul style="list-style-type: none"> <li>■ Unificar normas de protección de datos en la UE.</li> <li>■ Asegurar el control de los ciudadanos sobre sus datos.</li> <li>■ Establecer principios como la responsabilidad proactiva.</li> </ul>	<ul style="list-style-type: none"> <li>■ Cualquier organización que trate datos de ciudadanos europeos.</li> </ul>
Directiva NIS2	<ul style="list-style-type: none"> <li>■ Aumentar la resiliencia cibernética.</li> <li>■ Proteger sectores críticos.</li> <li>■ Establecer obligaciones de notificación de incidentes.</li> </ul>	<ul style="list-style-type: none"> <li>■ Empresas en sectores esenciales (energía, transporte, salud, servicios digitales, etc).</li> </ul>
ISO/IEC 27001:2022	<ul style="list-style-type: none"> <li>■ Implementar un SGSI efectivo.</li> <li>■ Proteger la confidencialidad, integridad y disponibilidad de la información.</li> <li>■ Gestionar riesgos de forma continua.</li> </ul>	<ul style="list-style-type: none"> <li>■ Organizaciones que buscan certificación en gestión de seguridad.</li> </ul>

Cuadro 8: Comparativa de normativas y estándares en ciberseguridad.

### 3.4.3. Metodologías de Auditoría en Ciberseguridad

Para ejecutar auditorías completas y rigurosas en ciberseguridad, existen metodologías reconocidas a nivel global que garantizan un marco estructurado. Algunas de las más relevantes son:

**OWASP (Open Web Application Security Project):** Proporciona directrices y metodologías específicas enfocadas en la identificación y mitigación de vulnerabilidades en aplicaciones web, siendo clave para desarrolladores y auditores en la protección contra ataques comunes [22].

**OSSTMM (Open Source Security Testing Methodology Manual):** Metodología abierta que ofrece procedimientos exhaustivos para realizar pruebas de seguridad técnica, enfocada en un análisis objetivo, cuantitativo y ético de vulnerabilidades técnicas y operativas [23].

**TIBER-EU (Threat Intelligence-Based Ethical Red Teaming):** Marco metodológico europeo para pruebas controladas de simulación de ataques informáticos complejos, utilizando inteligencia de amenazas reales para evaluar la resiliencia de entidades críticas frente a ataques avanzados [24].

**NIST SP 800-53:** Publicación que ofrece un conjunto exhaustivo de controles recomendados por el NIST para mejorar la seguridad y privacidad de sistemas informáticos en organizaciones federales










y comerciales, cubriendo aspectos desde la gestión del riesgo hasta controles técnicos y operacionales detallados [25].

**NIST SP 800-115:** Guía técnica específica sobre cómo realizar pruebas de seguridad (pentesting) en redes y sistemas, estableciendo procedimientos detallados para planificación, ejecución y evaluación de resultados, siendo ampliamente usada para pruebas de seguridad profundas y efectivas [14].

### 3.5. 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. [37]

Cuadro 9: Herramientas de pentesting más empleadas

Herramienta	Aplicación	Descripción
 <b>Nmap</b>	Test de penetración de redes	Escáner de redes y auditor de seguridad que permite descubrir hosts, servicios y vulnerabilidades activas.
 <b>Metasploit</b>	Desarrollo y ejecución de exploits	Framework completo para desarrollar, probar y ejecutar exploits en entornos controlados.
 <b>Burp Suite</b>	Auditoría de seguridad en aplicaciones web	Plataforma integrada para análisis de seguridad en aplicaciones web, capaz de interceptar, modificar y automatizar pruebas.
 <b>Kali Linux / Parrot OS</b>	Entornos completos para pentesting	Sistemas operativos especializados para pentesting que incluyen múltiples herramientas de auditoría, análisis forense e ingeniería inversa.
 <b>Nessus</b>	Escaneo de vulnerabilidades de red	Escáner que identifica configuraciones erróneas, parches faltantes y debilidades comunes en sistemas y redes.
 <b>John the Ripper</b>	Craqueo de contraseñas	Herramienta para descifrar contraseñas y evaluar su fortaleza en diferentes sistemas.
 <b>Wireshark</b>	Análisis de tráfico de red	Analizador de protocolos que captura y examina en tiempo real el tráfico que circula por una red.
 <b>ZAP (Zed Attack Proxy)</b>	Escaneo de seguridad en aplicaciones web	Escáner enfocado en detectar vulnerabilidades durante el desarrollo de aplicaciones web.
<b>SQLmap</b>	Detección y explotación de inyecciones SQL	Automatiza la identificación y explotación de vulnerabilidades de inyección SQL en aplicaciones web.
 <b>Aircrack-ng</b>	Auditoría de redes Wi-Fi	Conjunto de herramientas para romper claves WEP y WPA/WPA2 y auditar la seguridad de redes inalámbricas.

**Fuente:** Criterios de selección de herramientas para pentesting. [37]

### 3.6. Certificaciones del sector

Por último, para aquellas personas interesadas en iniciarse en el campo de la ciberseguridad ofensiva, es fundamental contar con una guía clara que oriente su aprendizaje y desarrollo profesional. Las certificaciones profesionales cumplen un papel importante en este sentido, ya que no solo validan los conocimientos técnicos y las habilidades de la persona, sino que también proporcionan una formación progresiva para adquirir competencias en distintas áreas de la ciberseguridad. A continuación, se presentan algunas de

las certificaciones más relevantes, ordenadas por nivel de dificultad dentro del área ofensiva, incluyendo una certificación fundamental en administración de sistemas Linux, que sirve de base para el dominio de entornos seguros.

- **LPIC-1/2 (Linux Professional Institute Certification)**: Es la certificación de nivel básico/intermedio para administradores de sistemas Linux. Valida competencias en instalación, configuración, mantenimiento y administración de sistemas basados en Linux, incluyendo tareas de red y scripting en bash. Resulta especialmente útil como base sólida para profesionales que quieran profundizar en seguridad ofensiva y defensiva en entornos Unix. [26]
- **eJPTv2 (eLearnSecurity Junior Penetration Tester)**: Ideal para principiantes en el campo del pentesting. Evalúa conocimientos básicos sobre redes, sistemas operativos, metodologías de pruebas de penetración y explotación de vulnerabilidades comunes. El examen es práctico y se realiza en un entorno de laboratorio simulado.[27]
- **eWPT (eLearnSecurity Web Penetration Tester)**: Certificación especializada en seguridad de aplicaciones web. Cubre ataques como inyecciones SQL, cross-site scripting (XSS), CSRF, gestión de sesiones, autenticación insegura, entre otros. [28]
- **eCPPTv2 (eLearnSecurity Certified Professional Penetration Tester)**: De nivel intermedio, esta certificación evalúa habilidades prácticas en pentesting interno y externo, incluyendo explotación de vulnerabilidades, escalada de privilegios, evasión de antivirus y generación de informes. [29]
- **PNPT (Practical Network Penetration Tester)**: Emitida por TCM Security, esta certificación simula una auditoría real de red empresarial. El candidato debe realizar tareas de reconocimiento, explotación, post-explotación, pivoting y red teaming básico, y entregar un informe técnico al estilo profesional. [30]
- **OSCP (Offensive Security Certified Professional)**: Considerada una de las certificaciones más exigentes y prestigiosas en pentesting. Exige comprometer múltiples máquinas en un entorno controlado durante un examen de 24 horas. Requiere dominio de técnicas como buffer overflows, escalada de privilegios, evasión de defensas, explotación manual y redacción exhaustiva de informes. Es un estándar de referencia en la industria de seguridad ofensiva. [31]

## 4. Metodología elegida: NIST SP 800-115

Para la propuesta metodológica planteada en este trabajo, se toma como base fundamental la metodología NIST SP 800-115 debido a su amplia aceptación y versatilidad en auditorías técnicas de seguridad informática. Esta metodología se selecciona específicamente por su capacidad para adaptarse eficazmente a los objetivos establecidos por la empresa BeeHacker, sobre los cuales se sustenta nuestra propuesta de auditoría.

El documento original consta de 80 páginas, divididas en cuatro fases fundamentales: planificación, descubrimiento, ataque y reporte. Estas fases aseguran una cobertura completa desde la definición del alcance hasta la generación de informes y recomendaciones finales. [14]

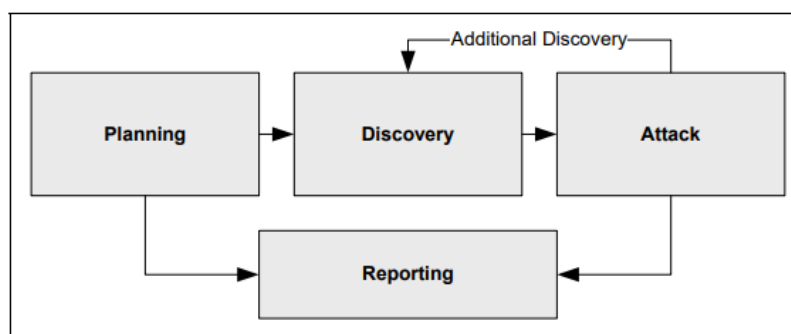


Figura 7: Metodología NIST SP 800-115. Fuente: [14]

A continuación, se presenta un desglose adaptado y resumido del contenido de la metodología NIST SP 800-115:

### 4.1. Fase de Planificación (Planning Phase)

Esta fase inicial implica la definición clara de los objetivos, el alcance y las restricciones de la auditoría. Se identifican los sistemas y activos a evaluar, se asignan responsabilidades, se establecen las reglas de compromiso (Rules of Engagement), y se gestiona la aprobación por parte de los responsables de la organización. La planificación también contempla la recopilación de información preliminar sobre la infraestructura, políticas de seguridad y nivel de madurez de la organización.

### 4.2. Fase de Descubrimiento (Discovery Phase)

En esta etapa se lleva a cabo la recolección de datos sobre los sistemas objetivo mediante técnicas pasivas y activas. Las técnicas pasivas incluyen el análisis de información disponible públicamente (OSINT), mientras que las técnicas activas abarcan escaneos de red, detección de puertos abiertos, identificación de servicios y sistemas operativos, así como la enumeración de posibles vulnerabilidades. El propósito es obtener una visión detallada del entorno evaluado sin interferir en su funcionamiento.

### 4.3. Fase de Ataque (Attack Phase)

Esta fase simula un escenario real de intrusión con el fin de explotar las vulnerabilidades detectadas previamente. Las pruebas pueden incluir ataques de penetración, escalamiento de privilegios, evasión de controles de seguridad y acceso no autorizado a recursos. Aunque esta fase puede resultar intrusiva, es crucial para evaluar la efectividad de los mecanismos de defensa implementados. Siempre se ejecuta bajo estrictos parámetros éticos y de autorización.

#### **4.4. Fase de Reporte (Reporting Phase)**

Finalmente, se documentan los hallazgos obtenidos durante la auditoría. El informe debe ser claro, técnico y ejecutivo, incluyendo descripciones detalladas de las vulnerabilidades encontradas, evidencias de explotación (cuando corresponda), análisis de riesgos y recomendaciones específicas para mitigar o corregir las debilidades identificadas. Este reporte sirve como base para la toma de decisiones estratégicas de seguridad por parte de la organización.

## 5. Modelo de auditoría

El presente capítulo tiene como objetivo presentar un modelo de auditoría de ciberseguridad diseñado específicamente para las PYMES. Este modelo ha sido construido siguiendo el **roadmap de auditoría de seguridad de la empresa BeeHacker**, una guía actualizada basada en la experiencia real de entornos empresariales.

### 5.1. Diseño propuesto por BeeHacker

El modelo de auditoría propuesto se basa en un enfoque estructurado por capas, abarcando todos los vectores de ataque potenciales desde el perímetro exterior hasta los datos almacenados internamente. Este diseño tiene como objetivo principal proporcionar un listado de actividades que permita auditar la ciberseguridad en una pyme sin necesidad de poseer conocimientos técnicos avanzados.

El modelo se compone específicamente de siete grandes bloques que permiten un análisis completo de la seguridad:



Figura 8: Diagrama de flujo de los bloques del diseño del modelo de auditoría. Fuente: Elaboración propia

1. **Perímetro de Red:** Se analiza la exposición externa de la infraestructura desde la perspectiva de un atacante sin conocimiento previo. Se evalúan routers con configuraciones por defecto (telnet, SSH abiertos), firewalls mal configurados, accesos remotos sin cifrado, y redes inalámbricas vulnerables. Se incluyen pruebas sobre sistemas RADIUS, bypass de portales cautivos, detección de APs maliciosos (Rogue AP / Karma WiFi), análisis de seguridad inalámbrica y cifrado.
2. **Fingerprint (Reconocimiento Interno):** Se realiza un reconocimiento de red interno: análisis de la topología de red, detección activos en la red, enumeración de puertos abiertos y servicios activos en cada activo. El mapeo de red se complementa con un análisis de vulnerabilidades.



3. **OSINT (Inteligencia de Fuentes Abiertas):** Se recopila y analiza información pública sobre la organización para descubrir posibles vectores de ataque. Se utilizan motores como Google (GHDB), Shodan, Censys y Maltego para identificar servidores expuestos, credenciales filtradas, tecnologías empleadas y datos personales. Además, se evalúan técnicas de ingeniería social como phishing.
4. **Seguridad en IoT:** Dado que muchas pymes incorporan dispositivos inteligentes como cámaras, sensores, esta fase analiza posibles accesos no autorizados a través de estos dispositivos, los cuales suelen estar poco protegidos. Se revisa su firmware, autenticación, cifrado y su exposición en la red.
5. **Auditoría Web:** Se realizan pruebas de seguridad siguiendo las recomendaciones de OWASP.
6. **Seguridad de Infraestructura:** Se revisa la arquitectura interna de la empresa: servidores, redes privadas, Active Directory, firewalls internos, y sistemas IDS/IPS. Se ejecutan pruebas de escalada de privilegios, pivoting, análisis de red, y se evalúa la configuración segura de cada elemento. También se estudian los logs y mecanismos de monitoreo, identificando posibles brechas de seguridad.
7. **Seguridad de Endpoints y Datos:** Se analiza la protección de los dispositivos finales utilizados por los empleados, donde suele recaer una parte crítica de la seguridad. Se auditan políticas de contraseñas, cifrado de disco, control de dispositivos USB, protección frente a malware, uso de software legítimo, backup de información, y sistemas de almacenamiento.

A continuación, se detallan los objetivos y actividades que componen este diseño:

## 5.2. Análisis del Perímetro de Red

Con el análisis del perímetro de red, intentamos identificar los puntos débiles de la infraestructura desde la perspectiva de un atacante externo, sin conocimiento de la arquitectura interna.

ID	Objetivo	Actividades	Herramientas
OBJ-01	Detectar redes inalámbricas disponibles	Enumeración de SSIDs visibles y ocultos	Airodump-ng, Wireshark
OBJ-02	Evaluar seguridad de cifrado WiFi	Identificar tipo de cifrado (WEP/WPA/WPA2/Enterprise) captura de handshake	Airodump-ng, hcxdump-tool, Aircrack-ng
OBJ-03	Realizar ataques de fuerza bruta a redes inseguras	Diccionario sobre handshake capturado	Aircrack-ng, hashcat
OBJ-04	Validar seguridad de portal cautivo	Intento de bypass (DNS spoof, phishing, MitM)	Bettercap, mitmproxy, macchanger
OBJ-05	Simular Rogue AP y ataques Karma	Clonado de SSID, AP falso para interceptar clientes	WiFi Pineapple, Hostapd, EvilTrust
OBJ-06	Detectar APs mal configurados o sospechosos	Escaneo de redes abiertas, SSID duplicados, canales raros	Airodump-ng, Wireshark
OBJ-07	Identificar routers con credenciales por defecto	Prueba de acceso a SSH, Telnet, interfaces web	Nmap, Hydra

Cuadro 10: Tabla de trazabilidad de objetivos en el análisis del perímetro de red

### Resultados esperados:

- Inventario de redes inalámbricas detectadas (visibles y ocultas), con información detallada sobre SSID, canal, BSSID (OBJ-01, OBJ-06).
- Diagnóstico del tipo de cifrado implementado en cada red, con identificación de aquellas que presenten algoritmos débiles o configuraciones inseguras (OBJ-02).

- Registro de contraseñas vulneradas mediante fuerza bruta, con indicación del tiempo estimado (OBJ-03).
- Evidencias de portales cautivos vulnerables ante técnicas de evasión o manipulación del tráfico (OBJ-04).
- Clientes conectados a AP falsos y evaluación del impacto potencial del ataque mediante Rogue AP o Karma (OBJ-05).
- Listado de routers o dispositivos accesibles remotamente con interfaces mal protegidas o credenciales por defecto (OBJ-07).

### **Limitaciones:**

- El análisis externo puede verse obstaculizado por la presencia de firewalls avanzados, WAFs, mecanismos de bloqueo o listas blancas, que filtran escaneos o conexiones sospechosas (OBJ-07).
- La detección de redes ocultas depende de la presencia activa de clientes conectados; de no haber tráfico asociado, podrían no identificarse (OBJ-01, OBJ-06).
- Las pruebas de fuerza bruta pueden requerir tiempos prolongados y recursos computacionales considerables, lo que limita su viabilidad en escenarios reales (OBJ-03).
- Algunas herramientas utilizadas en pruebas como Rogue AP o ataques MitM requieren hardware específico y tráfico en la red. (OBJ-05, OBJ-04).
- El uso de técnicas intrusivas, como la simulación de APs maliciosos o la manipulación del portal cautivo, debe realizarse en entornos controlados, ya que podrían provocar interrupciones en la conectividad de usuarios reales si se ejecutan en producción.

### 5.2.1. Fingerprint y Reconocimiento Interno

Una vez dentro de la red, se analizan los diferentes dispositivos conectados y sus diferentes vulnerabilidades, para trazar un plan de ataque.

ID	Objetivo	Actividades	Herramientas
OBJ-08	Mapeo de la red interna	Descubrimiento de dispositivos, gateways, rutas, subredes	Nmap, Neptus
OBJ-09	Análisis de puertos abiertos	Escaneo de red interna, detección de servicios accesibles	Nmap, Masscan, Neptus
OBJ-10	Identificación de servicios y versiones	Fingerprinting de servicios, banner grabbing, OS detection	Nmap, WhatWeb, Netcat
OBJ-11	Detección de vulnerabilidades conocidas	Escaneo de CVEs, servicios sin parches, versiones antiguas	Nessus, Exploit-db, WhatWeb

Cuadro 11: Tabla de trazabilidad de objetivos en la fase de Fingerprint interno

#### Resultados esperados:

- Topología detallada de la red interna, con identificación de dispositivos, gateways, y subredes (OBJ-08).
- Listado exhaustivo de puertos abiertos y servicios en cada host, con indicación del tipo de protocolo (OBJ-09).
- Información precisa sobre los servicios activos, versiones detectadas y sistemas operativos (OBJ-10).
- Inventario de vulnerabilidades conocidas asociadas a los servicios detectados, incluyendo identificadores CVE y criticidad (OBJ-11).

#### Limitaciones:

- La ejecución de escaneos internos requiere acceso a la red local, lo cual puede estar fuera del alcance del auditor en ciertas condiciones (OBJ-08–11).
- Las herramientas de escaneo pueden generar falsos positivos o negativos debido a la presencia de firewalls internos, IDS/IPS, o configuraciones personalizadas de los servicios (especialmente en OBJ-09 y OBJ-10).
- En redes grandes o mal segmentadas, los tiempos de escaneo aumentan significativamente, lo que puede limitar la cobertura o el rendimiento de las herramientas utilizadas (OBJ-08).

### 5.2.2. OSINT e Ingeniería Social

Esta fase se centra en la obtención de información utilizando fuentes abiertas (Open Source Intelligence), recopilando datos públicos que puedan ser útiles para identificar vectores de ataque antes de cualquier interacción directa con los sistemas. Se complementa con técnicas de ingeniería social para evaluar el factor humano.

ID	Objetivo	Actividades	Herramientas
OBJ-12	Recolectar información de buscadores genéricos	Búsquedas avanzadas con dorks, índice de documentos, paneles expuestos	Google, Google Hacking DB (GHDB)
OBJ-13	Identificar activos expuestos	Recolección de IPs públicas, puertos y servicios accesibles	Shodan, Censys
OBJ-14	Analizar relaciones y metadatos en redes y dominios	Investigación de nombres, emails, metadatos de documentos y relaciones entre entidades	Maltego, theHarvester
OBJ-15	Buscar credenciales filtradas y contraseñas públicas	Consultas sobre leaks, validación de emails y dominios comprometidos	DeHashed, HaveIBeenPwned
OBJ-16	Evaluar la respuesta humana frente a ataques simulados	Pruebas de phishing, manipulación, evaluación de políticas internas	GoPhish, RubberDucky

Cuadro 12: Tabla de trazabilidad de objetivos en la fase OSINT e Ingeniería Social

#### Resultados esperados:

- Identificación de documentos, paneles de administración u otros recursos accesibles desde motores de búsqueda mediante el uso de dorks avanzados (OBJ-12).
- Inventario de activos públicos expuestos (direcciones IP, puertos, servicios abiertos), con detalles sobre su localización (OBJ-13).
- Mapas de relaciones entre dominios, cuentas de correo, nombres de empleados o entidades asociadas, así como metadatos incrustados en documentos (OBJ-14).
- Listado de credenciales potencialmente comprometidas, asociadas a dominios corporativos o emails internos (OBJ-15).
- Evaluación de la resiliencia del personal frente a técnicas de ingeniería social (OBJ-16).

#### Limitaciones:

- La información obtenida mediante OSINT puede estar desactualizada, parcial o haber sido ya mitigada por la organización en el momento del análisis (OBJ-12–15).
- Las herramientas de búsqueda tienen limitaciones en cuanto al alcance de indexación, especialmente en contenidos dinámicos, servicios protegidos o entornos internos no expuestos (OBJ-12, OBJ-13).
- La interpretación de relaciones en herramientas como Maltego puede generar asociaciones erróneas si no se valida manualmente el contexto (OBJ-14).
- Las pruebas de ingeniería social requieren autorización explícita y un entorno controlado. Además, su ejecución puede estar condicionada por la normativa laboral y la cultura organizativa de la empresa (OBJ-16).

### 5.2.3. Seguridad en IoT

Los dispositivos IoT suelen carecer de medidas de seguridad sólidas y se convierten en vectores frecuentes de ataque. Esta fase se enfoca en el análisis del tráfico de red, servicios inseguros, firmware, y protocolos específicos utilizados por dispositivos conectados.

ID	Objetivo	Actividades	Herramientas
OBJ-17	Identificar dispositivos IoT en la red	Escaneo de red, fingerprinting de fabricantes, búsqueda de dispositivos por MAC y puertos comunes	Nmap, Wireshark
OBJ-18	Analizar protocolos IoT y tráfico de red	Captura y análisis de paquetes en protocolos propietarios (MQTT, CoAP, BLE, UPnP)	Wireshark
OBJ-19	Evaluar la seguridad de interfaces y APIs	Inspección de endpoints HTTP, comandos remotos, autenticación débil o inexistente	Postman, Burp Suite
OBJ-20	Detectar firmware inseguro o mal configurado	Extracción y análisis de firmware, validación de backdoors y servicios inseguros	Wireshark
OBJ-21	Atacar dispositivos vulnerables	Explotación de servicios abiertos, contraseñas por defecto, ejecución remota de comandos	Metasploit, hydra, scripts personalizados

Cuadro 13: Tabla de trazabilidad de objetivos en la auditoría de dispositivos IoT

#### Resultados esperados:

- Inventario detallado de dispositivos IoT detectados en la red, con su identificación por fabricante, modelo y dirección MAC (OBJ-17).
- Análisis del tráfico de red IoT, con detección de protocolos inseguros, datos transmitidos en texto plano o configuraciones por defecto (OBJ-18).
- Evaluación del nivel de exposición de las APIs o paneles de gestión, incluyendo endpoints sin autenticación, tokens expuestos o comandos inseguros (OBJ-19).
- Extracción exitosa y análisis estático de firmware, con identificación de puertas traseras, claves embebidas, certificados obsoletos o servicios inseguros habilitados (OBJ-20).
- Demostración controlada de vulnerabilidades explotables, como ejecución remota de comandos, credenciales por defecto y escalada de privilegios (OBJ-21).
- Recomendaciones específicas de mitigación para cada dispositivo vulnerable o mal configurado.

#### Limitaciones:

- Muchos dispositivos IoT no responden a técnicas de escaneo convencionales o emplean protocolos inusuales, lo que dificulta su identificación (OBJ-17, OBJ-18).
- El análisis de tráfico requiere que los dispositivos estén activos y generen comunicaciones durante el período de captura, de lo contrario, ciertos vectores podrían pasar desapercibidos (OBJ-18).
- La extracción de firmware puede no ser posible sin acceso físico al dispositivo o sin credenciales propietarias del fabricante, lo que limita la evaluación completa de vulnerabilidades (OBJ-20).
- La explotación directa puede ser peligrosa si se realiza en un entorno de producción, pudiendo provocar bloqueos, reinicios o corrupción del sistema (OBJ-21).

#### 5.2.4. Auditoría Web

En esta fase se analiza por completo la plataforma web, partiendo desde el propio servidor donde se aloja. Se siguen los pasos establecidos por la metodología OWASP para detectar las vulnerabilidades más críticas.

ID	Objetivo	Actividades	Herramientas
OBJ-22	Analizar el servidor web y servicios asociados	Fingerprinting, detección de versiones, servicios activos, configuración	WhatWeb, Nikto, Nmap scripts
OBJ-23	Identificar servicios vulnerables o expuestos	Enumeración de directorios, endpoints, tecnologías utilizadas	Dirb, Gobuster, Wap-palyzer
OBJ-24	Detectar vulnerabilidades OWASP	SQLi, XSS, IDOR, RCE, SSRF, CSRF, XXE, etc.	Burp Suite, gestores de contenido
OBJ-25	Validar mecanismos de autenticación	Fuerza bruta, evasión de login, análisis de formularios	Hydra, Burp Intruder, wfuzz, GoBuster
OBJ-26	Evaluar la gestión de sesiones	Análisis de cookies, tokens, regeneración y caducidad de sesiones	Burp Suite
OBJ-27	Probar mecanismos de autorización	Escalada de privilegios, acceso a funciones restringidas	Burp Suite, Postman
OBJ-28	Validar controles de entrada/salida	Pruebas de validación del lado cliente y servidor, bypasses comunes	Burpsuite, payloads manuales
OBJ-29	Explorar la aplicación (crawling/spidering)	Recolección automatizada de rutas y formularios	Burpsuite
OBJ-30	Realizar fuerza bruta y fuzzing sobre parámetros	Testeo de inputs, formularios	wfuzz, Burpsuite, sql-map
OBJ-31	Evaluar la criptografía usada en la aplicación	Análisis de algoritmos de hash, cifrados, tokens y secretos	Burp Crypto

Cuadro 14: Tabla de trazabilidad de objetivos en la auditoría de aplicaciones web

#### Resultados esperados:

- Identificación de versiones del servidor web y servicios expuestos, con posibles configuraciones inseguras (OBJ-22).
- Descubrimiento de rutas ocultas, endpoints sensibles y tecnologías potencialmente vulnerables (OBJ-23, OBJ-29).
- Detección de vulnerabilidades OWASP (como SQLi, XSS, CSRF, etc.), clasificadas según nivel de criticidad (OBJ-24).
- Evidencia de fallos en los mecanismos de autenticación, como contraseñas débiles, formularios vulnerables o bypasses de login (OBJ-25).
- Análisis de sesiones inseguras: cookies sin flags de seguridad, tokens sin caducidad, falta de regeneración en login/logout (OBJ-26).
- Accesos indebidos o escaladas de privilegio mediante manipulación de permisos o tokens de autorización (OBJ-27).

- Pruebas de validación inadecuada de entrada/salida que permitan inyecciones o manipulaciones en el flujo de datos (OBJ-28, OBJ-30).
- Evaluación de la criptografía utilizada, identificando algoritmos inseguros o mal implementados en la gestión de contraseñas, tokens o almacenamiento (OBJ-31).
- Recomendaciones específicas para cada vulnerabilidad detectada, priorizadas por impacto técnico y facilidad de explotación.

#### Limitaciones:

- Muchas vulnerabilidades solo se manifiestan tras autenticación o en condiciones específicas (estado de sesión, tipo de usuario, datos introducidos), lo que puede limitar la cobertura si no se dispone de credenciales o acceso completo (OBJ-24, OBJ-25, OBJ-27).
- Los sistemas con WAF, captcha, rate limiting o mecanismos de detección de automatización pueden bloquear ataques de fuzzing, fuerza bruta o crawling automatizado (OBJ-25, OBJ-29, OBJ-30).
- La validación criptográfica se limita a los elementos accesibles desde el frontend (tokens, cookies, headers), sin acceso al código backend o configuración de librerías criptográficas (OBJ-31).
- La ejecución de pruebas intrusivas como SQLi o RCE debe realizarse con extremo cuidado en entornos de producción, ya que pueden comprometer la integridad del sistema.

#### 5.2.5. Seguridad de Infraestructura

Esta fase abarca pruebas sobre el núcleo central de la seguridad en la organización.

ID	Objetivo	Actividades	Herramientas
OBJ-32	Evaluar configuración del firewall	Identificación de puertos permitidos, pruebas de evasión, reglas de filtrado	Nmap, Scapy, tcptrace-route
OBJ-33	Verificar funcionamiento de IDS/IPS	Generación de tráfico sospechoso, análisis de alertas y detección de ataques	Metasploit, Nmap
OBJ-34	Analizar seguridad del servidor interno	Revisión de servicios, versiones, credenciales por defecto y vulnerabilidades conocidas	Nmap, Nikto, Nessus
OBJ-35	Realizar pruebas sobre Active Directory	Enumeración de usuarios, grupos, GPOs, tickets Kerberos	NetExec, CrackMapExec, Kerbrute, impacket
OBJ-36	Analizar tráfico y segmentación de red	Sniffing, detección de redes planas, protocolos en claro, ARP poisoning	Bettercap, Responder, Wireshark, tcpdump
OBJ-37	Realizar escalada de privilegios en el entorno	Búsqueda de binarios SUID, permisos mal configurados, exploits locales	GTF0Bins, ExploitDB
OBJ-38	Ejecutar técnicas de pivoting y movimiento lateral	Conexión a otras redes o máquinas a través de un host comprometido	Chisel, ProxyChains, SSH tunneling, Metasploit

Cuadro 15: Tabla de trazabilidad de objetivos en la evaluación de la seguridad de la infraestructura

**Resultados esperados:**

- Listado de reglas del firewall efectivas, puertos abiertos innecesariamente o configuraciones que permiten tráfico no autorizado (OBJ-32).
- Comprobación del funcionamiento de IDS/IPS ante tráfico anómalo, identificación de firmas activas o ausencia de detección (OBJ-33).
- Evaluación de seguridad de servidores internos: servicios inseguros, credenciales por defecto, vulnerabilidades sin parchear (OBJ-34).
- Enumeración de la estructura del Active Directory: usuarios, políticas de grupo, servicios Kerberos y relaciones de confianza (OBJ-35).
- Detección de segmentación inadecuada en redes mediante análisis de tráfico y técnicas de sniffing (OBJ-36).
- Identificación de rutas para escalada de privilegios: binarios mal configurados, exploits locales disponibles y configuraciones débiles (OBJ-37).
- Mapeo de movimiento lateral y pivoting: hosts accesibles desde un nodo comprometido, redes internas accesibles sin controles adecuados (OBJ-38).
- Recomendaciones de mitigación técnica, incluyendo segmentación, refuerzo de controles de acceso y actualización de servicios vulnerables.

**Limitaciones:**

- La ejecución de pruebas sobre firewall, AD o escalada de privilegios requiere permisos elevados, a menudo restringidos por la política de la organización (OBJ-32, OBJ-35, OBJ-37).
- Las técnicas de pivoting y movimiento lateral pueden causar interferencias en la red o en servicios productivos si no se realizan en entornos aislados (OBJ-38).
- El análisis de tráfico puede estar limitado por la encriptación de extremo a extremo o el uso de VLANs y redes virtuales que impidan el sniffing pasivo (OBJ-36).
- Las herramientas de enumeración como CrackMapExec o Kerbrute pueden generar tráfico considerado agresivo, que puede activar alarmas de IDS o sistemas de bloqueo temporal (OBJ-33, OBJ-35).
- La recopilación de logs, políticas de grupo o información sensible del dominio puede estar regulada por normativas internas o leyes de protección de datos, limitando el alcance de algunas técnicas (OBJ-35, OBJ-36).

**5.2.6. Seguridad de Endpoints y Datos**

Esta fase se enfoca en los dispositivos cliente de la organización, evaluando su configuración de seguridad, control de accesos, privilegios de usuario, y posibles vectores de evasión de controles mediante proxies, software no autorizado o escaladas locales. Además, se evalúan un conjunto de test sobre el almacenamiento de los datos y su sistema de respaldo.



ID	Objetivo	Actividades	Herramientas
OBJ-39	Evaluar configuración de roles y perfiles de usuario	Verificación de restricciones según rol, acceso a configuraciones y consolas	Manual, PowerShell
OBJ-40	Verificar control de puertos USB y dispositivos externos	Comprobación de bloqueo, acceso a discos externos, ejecución automática	USB Rubber Ducky, scripts batch, manual
OBJ-41	Comprobar bypass de proxy corporativo	Intento de acceso directo a Internet, uso de túneles y software alternativo	proxychains, TOR, chisel, VPN port forwarding
OBJ-42	Instalar y ejecutar software no autorizado	Prueba con aplicaciones portables o autoejecutables desde usuarios limitados	TOR Browser, portable apps, reverse shells
OBJ-43	Verificar restricciones sobre terminales y consolas	Evaluar si un perfil básico puede lanzar CMD, PowerShell o intérpretes	Terminal
OBJ-44	Evaluar políticas y mecanismos de backup	Revisión de la frecuencia, almacenamiento, redundancia y pruebas de restauración de copias de seguridad	Documentación, entrevistas, herramientas de backup
OBJ-45	Analizar almacenamiento y cifrado de datos	Identificar dónde y cómo se almacenan datos sensibles, qué bases de datos se usan y si los datos están cifrados en reposo y en tránsito	Auditoría documental, herramientas de análisis de cifrado
OBJ-46	Evaluar políticas de privacidad y protección de datos sensibles	Revisión de políticas internas para manejo de datos sensibles, control de acceso y auditorías de cumplimiento	Entrevistas, revisión documental
OBJ-47	Verificar uso de contraseñas robustas y controles de autenticación	Comprobación de políticas de longitud, complejidad, expiración y almacenamiento seguro de contraseñas	Auditoría técnica, herramientas de análisis de políticas

Cuadro 16: Tabla de trazabilidad de objetivos en la auditoría de seguridad de endpoints y datos

**Resultados esperados:**

- Verificación del cumplimiento de políticas de acceso según perfil de usuario: restricciones adecuadas, acceso limitado a configuraciones del sistema o consolas administrativas (OBJ-39, OBJ-43).
- Comprobación del control físico de dispositivos: detección de políticas activas sobre uso de puertos USB, ejecución automática o instalación de drivers externos (OBJ-40).
- Evidencia de posibles bypasses del proxy corporativo mediante uso de túneles cifrados o canales alternativos de comunicación externa (OBJ-41).
- Informe sobre medidas de protección de datos locales y sistemas de backup, incluyendo cifrado de disco, políticas de restauración y almacenamiento redundante (OBJ-44, OBJ-45).
- Evaluación del cumplimiento de políticas internas de privacidad y manejo adecuado de datos sensibles (OBJ-46).
- Revisión del uso de contraseñas robustas y mecanismos de autenticación seguros (OBJ-47).

**Limitaciones:**

- Algunos sistemas de protección avanzados como antivirus pueden interferir en la ejecución de pruebas o generar falsos negativos/positivos (OBJ-41, OBJ-42).
- Las pruebas de ejecución de software no autorizado, túneles o bypasses de proxy pueden entrar en conflicto con políticas internas o requerir una autorización explícita (OBJ-41, OBJ-42).
- El análisis de backup, cifrado de disco o políticas de privacidad puede no ser viable sin credenciales administrativas o acceso a la documentación interna de TI (políticas, scripts, logs) (objetivo general).
- Las técnicas de evaluación manual pueden depender del entorno operativo (Windows, Linux) y requerir diferentes enfoques para cada uno.

## 6. Requisitos previos a la auditoría

Conforme a la metodología establecida, es imprescindible cumplir con los siguientes requisitos previos:

1. **Formalización previa:** Establecer por escrito los siguientes documentos:
  - **Acuerdo de Confidencialidad (NDA):** Define el compromiso de confidencialidad respecto a toda la información sensible, técnica u organizativa que sea compartida durante la auditoría. Su objetivo es garantizar que ningún dato se utilice con fines ajenos al proyecto ni se divulgue sin autorización.
  - **Acuerdo de Servicios:** Establece los objetivos concretos, el alcance detallado, la duración estimada y las condiciones generales de la colaboración. Sirve como base para planificar y organizar el trabajo de forma estructurada y transparente.
  - **Autorización para Pruebas Técnicas:** Permite expresamente la realización de actividades técnicas como análisis de red, detección de vulnerabilidades, pruebas de acceso o campañas controladas de ingeniería social. Además, delimita qué sistemas están autorizados y bajo qué condiciones deben desarrollarse las pruebas.
2. **Identificación detallada de activos:** Solicitar un inventario completo (en caso de que lo tengan y se encuentre actualizado), de sistemas, redes, aplicaciones y dispositivos que serán objeto de análisis durante la auditoría
3. **Análisis de riesgos y medidas preventivas:** Antes de ejecutar cualquier acción técnica, es fundamental realizar una evaluación de los riesgos asociados a las pruebas de seguridad. Este análisis considera el impacto potencial sobre la disponibilidad, integridad y confidencialidad de los sistemas auditados. Se identifican los servicios críticos y se diseñan estrategias de mitigación para evitar interrupciones no deseadas, como realizar pruebas en entornos controlados o fuera del horario operativo.
4. **Preparación técnica previa:** Asegurar disponibilidad y funcionamiento de herramientas y recursos técnicos.
5. **Definición del equipo auditor:** La conformación del equipo de trabajo es un factor clave para el éxito del proceso de auditoría. En este apartado se detallan los miembros que participarán, sus roles específicos, y sus responsabilidades. Además, se establece la cadena de comunicación interna y con los responsables de la organización auditada.

### 7. Propuesta metodológica de auditoría

Esta propuesta combina el modelo estructurado por bloques sugerido por BeeHacker con las fases claramente definidas de la metodología NIST SP 800-115: Planificación, Descubrimiento, Ataque y Reporte.

Cada uno de los siete bloques será abordado secuencialmente, siguiendo estas cuatro etapas fundamentales:

#### 7.1. Fase de Planificación de la Auditoría

La fase de planificación representa el punto de partida formal del proceso de auditoría. En esta etapa se establecen las bases necesarias para garantizar que el trabajo se desarrolle de forma estructurada, controlada y alineada con los objetivos del proyecto. Es aquí donde se consolidan todos los acuerdos documentales previos, como el Acuerdo de Confidencialidad (NDA), el Acuerdo de Servicios y la Autorización para Pruebas Técnicas, descritos previamente en los requisitos.

El propósito principal de esta fase es definir con precisión el alcance de la auditoría, delimitar los sistemas y procesos que serán objeto de análisis y establecer el marco operativo bajo el cual se ejecutarán las pruebas. Para ello, resulta esencial mantener una comunicación directa con el responsable de seguridad de la empresa.

Una entrevista estructurada con esta persona clave permitirá al auditor obtener una visión global del entorno a auditar. A través de esta conversación se abordarán los grandes bloques que guiarán el resto de la auditoría, enfocándose especialmente en:

- La solicitud de un inventario de activos actualizado, que incluya servidores, estaciones de trabajo, dispositivos de red y servicios relevantes.
- La obtención de un esquema detallado de la topología de red, incluyendo segmentaciones, conexiones externas, y sistemas críticos.
- El acceso a las políticas de seguridad vigentes, tanto técnicas como organizativas, que regulan el comportamiento del personal y la gestión de los sistemas, con el fin de analizarlas y comprobar su cumplimiento efectivo durante el desarrollo de las fases técnicas de la auditoría
- La revisión, si procede, de informes o resultados de auditorías previas que puedan aportar contexto o antecedentes sobre el entorno.
- La evaluación inicial del nivel de seguridad mediante una batería de preguntas dirigidas a cada uno de los bloques propuestos. Esto permite contrastar las afirmaciones del personal entrevistado con las evidencias técnicas que se obtendrán posteriormente.

Toda esta información permitirá afinar el enfoque técnico, ajustar las herramientas a utilizar, establecer prioridades en el análisis de riesgos y adecuar la metodología al entorno específico.

Una vez realizado este análisis preliminar y formalizada la documentación legal y técnica, se considerará que existe un marco de trabajo completamente definido. A partir de este momento, el equipo auditor podrá organizarse internamente, verificar la disponibilidad de las herramientas necesarias, confirmar la composición del equipo de trabajo y establecer fecha para el inicio de la siguiente fase.

#### 7.2. Fase de Descubrimiento

## 8. Caso Práctico

En esta sección se presenta el caso práctico de auditoría realizado en una empresa real, siguiendo la metodología propuesta en el capítulo anterior. El objetivo es aplicar los conceptos teóricos aprendidos y demostrar la viabilidad de la metodología en un entorno real.

### 8.1. Implementación de la auditoría

El entorno auditado corresponde a una **pyme del sector industrial** ubicada en territorio nacional. Por motivos de confidencialidad, hemos decidido mantener el anonimato de la entidad analizada, la cual será mencionada en este documento como **Empresa X**.

Además, se utilizarán nombres de dominio ficticios para proteger la identidad de los sistemas y aplicaciones involucradas, evitando así cualquier posible asociación con la empresa real. Asimismo, las direcciones IP públicas y nombres de host utilizados durante la práctica serán también ficticios y no corresponden a sistemas reales.

La auditoría se estructuró conforme a las cinco fases metodológicas descritas en el capítulo anterior:

### 8.2. Planificación de la auditoría

#### Definición del alcance

El alcance de la auditoría se estableció atendiendo a los recursos disponibles y a las posibles limitaciones que pudiera surgir durante la práctica que pudieran afectar al rendimiento de la empresa auditada.

Para ello, se ha definido un entorno de pruebas que incluye:

**Encuesta**

**Bloques y Objetivos**

**Batería de preguntas**

**Estructuras externas e internas**

**Responsables**

**Inventario de activos**

## 9. Resultados

## 10. 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] Por Alguien. (2222) [http://perspectivas.esPOCH.edu.ec:8081/index.php/RCP\\_ESPOCH/article/view/215/146consultadoel5/5/2025](http://perspectivas.esPOCH.edu.ec:8081/index.php/RCP_ESPOCH/article/view/215/146consultadoel5/5/2025)
- [4] Por Alguien. (2222) <https://fortiguard.fortinet.com/threat-map>
- [5] <https://fortiguard.fortinet.com/threat-map>
- [6] 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>
- [7] Morales-López & Taípe-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>
- [8] 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](https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=173)
- [9] Instituto Nacional de Ciberseguridad (INCIBE). (s.f.). *Página oficial de INCIBE*. Recuperado el 24 de mayo de 2025, de <https://www.incibe.es/>
- [10] Centro Nacional de Inteligencia (CNI). (s.f.). *Quiénes somos*. Recuperado el 24 de mayo de 2025, de <https://www.cni.es/>
- [11] Centro Criptológico Nacional (CCN-CERT). (s.f.). *Portal del CCN-CERT*. Recuperado el 24 de mayo de 2025, de <https://www.ccn-cert.cni.es/>
- [12] Agencia Española de Protección de Datos (AEPD). (s.f.). *Portal de la AEPD*. Recuperado el 24 de mayo de 2025, de <https://www.aepd.es/>
- [13] National Institute of Standards and Technology (NIST). (s.f.). *Cybersecurity Framework*. Recuperado el 24 de mayo de 2025, de <https://www.nist.gov/cyberframework>
- [14] Scarfone, K., & Mell, P. (2008). *Technical Guide to Information Security Testing and Assessment (NIST SP 800-115)*. National Institute of Standards and Technology. Recuperado el 24 de mayo de 2025, de <https://csrc.nist.gov/publications/detail/sp/800-115/final>
- [15] SANS Institute. (s.f.). *SANS Cyber Security Training and Certifications*. Recuperado el 24 de mayo de 2025, de <https://www.sans.org/>
- [16] Boletín Oficial del Estado. (2022). *Real Decreto 311/2022, por el que se regula el Esquema Nacional de Seguridad*. Recuperado el 24 de mayo de 2025, de <https://www.boe.es/eli/es/rd/2022/05/03/311>
- [17] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. (2016). *Reglamento General de Protección de Datos (RGPD)*. Recuperado el 24 de mayo de 2025, de <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679>
- [18] Boletín Oficial del Estado. (2018). *Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales*. Recuperado el 24 de mayo de 2025, de <https://www.boe.es/eli/es/lo/2018/12/05/3>
- [19] Parlamento Europeo. (2022). *Directiva (UE) 2022/2555 sobre medidas para un alto nivel común de ciberseguridad en la Unión (NIS2)*. Recuperado el 24 de mayo de 2025, de <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32022L2555>



- [20] International Organization for Standardization. (2022). *ISO/IEC 27001:2022 – Information security, cybersecurity and privacy protection*. Recuperado el 24 de mayo de 2025, de <https://www.iso.org/standard/27001>
- [21] 4IT Networks. (s.f.). *La triada de la seguridad de la información: Confidencialidad, Integridad y Disponibilidad*. Recuperado el 24 de mayo de 2025, de <https://www.4itn.mx/ciberseguridad/triada-de-la-informacion/>
- [22] OWASP Foundation. (s.f.). *Open Web Application Security Project*. Recuperado el 24 de mayo de 2025, de <https://owasp.org/>
- [23] ISECOM. (s.f.). *OSSTMM – Open Source Security Testing Methodology Manual*. Recuperado el 24 de mayo de 2025, de <https://www.isecom.org/OSSTMM.3.pdf>
- [24] European Central Bank. (s.f.). *TIBER-EU Framework*. Recuperado el 24 de mayo de 2025, de [https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber\\_eu\\_framework.en.pdf](https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf)
- [25] National Institute of Standards and Technology. (2020). *NIST Special Publication 800-53 Revision 5: Security and Privacy Controls*. Recuperado el 24 de mayo de 2025, de <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final>
- [26] Linux Professional Institute. (s.f.). *LPIC-1/2 Linux Professional Certification*. Recuperado el 24 de mayo de 2025, de <https://www.lpi.org/>
- [27] eLearnSecurity. (s.f.). *eJPTv2 - Junior Penetration Tester Certification*. Recuperado el 24 de mayo de 2025, de <https://elearnsecurity.com/product/ejpt-certification/>
- [28] eLearnSecurity. (s.f.). *Web Application Penetration Tester (eWPT)*. Recuperado el 24 de mayo de 2025, de <https://elearnsecurity.com/product/ewpt-certification/>
- [29] eLearnSecurity. (s.f.). *Certified Professional Penetration Tester (eCPPTv2)*. Recuperado el 24 de mayo de 2025, de <https://elearnsecurity.com/product/ecppt-certification/>
- [30] TCM Security. (s.f.). *Practical Network Penetration Tester (PNPT)*. Recuperado el 24 de mayo de 2025, de <https://tcm-sec.com/pnpt-certification/>
- [31] Offensive Security. (s.f.). *Offensive Security Certified Professional (OSCP)*. Recuperado el 24 de mayo de 2025, de <https://www.offensive-security.com/pwk-oscp/>
- [32] 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-madrid/>
- [33] Device42. (2024). *Device42: The Ultimate Guide to Network Mapping*. Recuperado el 24 de mayo de 2025, de <https://www.device42.com/compliance-standards/nist-csf-categories/>
- [34] 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>
- [35] 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](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age_es)
- [36] 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](https://www.escudodigital.com/ciberseguridad/incibe-cni-ccn-se-reunen-impulsar-su-coordinacion-en-ciberseguridad_54930_102.html)
- [37] 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>

- [38] 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>
- [39] INCIBE (2023). *INCIBE gestionó más de 118.000 incidentes de ciberseguridad durante 2022, un 9 % más que en 2021* Recuperado de <https://www.incibe.es/incibe/sala-de-prensa/incibe-gestiono-mas-115000-incidentes-ciberseguridad-durante-2022-9-mas>
- [40] 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>
- [41] Triada, A. (2023). *Ciberseguridad para pymes: ¿Por qué es importante?* Recuperado del 07 de abril <https://www.4itn.mx/ciberseguridad/>
- [42] 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>
- [43] Treider, A. (2021). *Ciberseguridad para pymes: ¿Por qué es importante?* Recuperado del 07 de abril <https://www.treyder.com/blog/ciberseguridad-en-las-pymes/>

## 11. Anexos

Herramienta	URL de referencia / descarga
Kali Linux	<a href="https://www.kali.org">https://www.kali.org</a>
Parrot OS	<a href="https://www.parrotsec.org">https://www.parrotsec.org</a>
Nmap	<a href="https://nmap.org">https://nmap.org</a>
Nessus	<a href="https://www.tenable.com/products/nessus">https://www.tenable.com/products/nessus</a>
OpenVAS	<a href="https://www.greenbone.net/en/">https://www.greenbone.net/en/</a>
Nikto	<a href="https://github.com/sullo/nikto">https://github.com/sullo/nikto</a>
SQLMap	<a href="https://sqlmap.org">https://sqlmap.org</a>
Burp Suite	<a href="https://portswigger.net/burp">https://portswigger.net/burp</a>
OWASP ZAP	<a href="https://www.zaproxy.org">https://www.zaproxy.org</a>
Shodan	<a href="https://www.shodan.io">https://www.shodan.io</a>
Censys	<a href="https://censys.io">https://censys.io</a>
TheHarvester	<a href="https://github.com/laramies/theHarvester">https://github.com/laramies/theHarvester</a>
Maltego	<a href="https://www.maltego.com">https://www.maltego.com</a>
Wireshark	<a href="https://www.wireshark.org">https://www.wireshark.org</a>
Tcpdump	<a href="https://www.tcpdump.org">https://www.tcpdump.org</a>
Metasploit	<a href="https://www.metasploit.com">https://www.metasploit.com</a>
BloodHound	<a href="https://github.com/BloodHoundAD/BloodHound">https://github.com/BloodHoundAD/BloodHound</a>
CrackMapExec	<a href="https://github.com/Porchetta-Industries/CrackMapExec">https://github.com/Porchetta-Industries/CrackMapExec</a>
Mimikatz	<a href="https://github.com/gentilkiwi/mimikatz">https://github.com/gentilkiwi/mimikatz</a>
Flipper Zero	<a href="https://flipperzero.one">https://flipperzero.one</a>
USB Rubber Ducky	<a href="https://shop.hak5.org/products/usb-rubber-ducky-deluxe">https://shop.hak5.org/products/usb-rubber-ducky-deluxe</a>
Cactus WHID	<a href="https://github.com/spacehuhntech/WHID-Injector">https://github.com/spacehuhntech/WHID-Injector</a>

Cuadro 17: Listado de herramientas utilizadas en auditorías de ciberseguridad y sus referencias oficiales