Producto 3

Crear la documentación necesaria, técnica y no técnica, en base a los resultados obtenidos en los productos anteriores

FP.051 – (P) Diseño e implantación de elementos de seguridad informática

Daniel de la Cruz García

Arnau Medina Coca

Rubén Vicente Gilabert

Víctor Jodar Rus

Equipo: MetasploitOps

Consultor: Gerard Baiget Pellicer

Convocatoria: septiembre 2025

JESUÏTES educació
Formación Profesional

Universitat Oberta de Catalunya

Índice

1. Introducción

Este tercer producto de la asignatura Diseño e implantación de elementos de seguridad informática tiene como objetivo recopilar, analizar y documentar de forma estructurada todos los resultados obtenidos en los dos productos anteriores. A partir de las pruebas que hemos realizado (como enrutamiento, análisis de servicios, explotación controlada y simulación de ataques), en este producto se ha creado un informe que ayudaría en la toma de decisiones.

Por un lado, se ha creado un informe técnico de vulnerabilidades, que sería para el personal informático de la organización. En este informe, se describen las vulnerabilidades que se hayan detectado en el proyecto, y se clasifican según el impacto. Además, se proponen algunas medidas para evitarlas, y a su vez, acciones de mejora.

Por otro lado, se elabora un informe no técnico que va dirigido a la gerencia de la empresa. De esta forma, se pueden presentar los riesgos y recomendaciones de una forma clara y que sea entendible para alguien que no tiene conocimientos de ciberseguridad ni informática.

2. Informe técnico de las vulnerabilidades

En este apartado se desarrolla el informe técnico de las vulnerabilidades que se han detectado durante el proyecto. Además, se analizan los organismos de referencia relacionados con la ciberseguridad, las métricas para evaluar la criticidad, las vulnerabilidades identificadas en los otros productos anteriores.

2.1. Organismos relevantes en ciberseguridad

En el ecosistema de la seguridad de la información, existen entidades con distintos alcances (europeo, nacional y comunitario) que son fundamentales para la estandarización y defensa.

❖ ENISA (European Union Agency for Cybersecurity)

A qué se dedican:

Es la agencia de la Unión Europea para la ciberseguridad. Su misión principal es lograr un alto nivel común de ciberseguridad en toda Europa. Actúan como un puente entre los Estados miembros para armonizar estrategias.

Qué ofrecen:

Esquemas de Certificación: Desarrollan marcos para certificar productos y servicios TIC en la UE.

Informes de Amenazas: Publican el *ENISA Threat Landscape*, un informe anual crucial sobre las tendencias de amenazas.

Ejercicios Cyber Europe: Organizan simulacros de ciberataques a gran escala para entrenar la respuesta de los países miembros.

❖ INCIBE (Instituto Nacional de Ciberseguridad de España)

A qué se dedican:

Es la entidad de referencia en España para el desarrollo de la ciberseguridad y la confianza digital. A diferencia del CCN-CERT (que se enfoca en administración pública y sistemas clasificados), INCIBE se centra en **ciudadanos, empresas (especialmente PYMES) y profesionales**.

Qué ofrecen:

Línea de Ayuda 017: Un servicio gratuito y confidencial para resolver dudas de ciberseguridad.

INCIBE-CERT: Su centro de respuesta a incidentes para empresas y ciudadanos.

Kit Digital y Formación: Herramientas gratuitas para proteger negocios y cursos de concienciación.

❖ OWASP (Open Web Application Security Project)

A qué se dedican:

Es una fundación sin ánimo de lucro a nivel mundial dedicada a mejorar la seguridad del software. Funciona como una comunidad abierta. Su enfoque es puramente técnico y de desarrollo seguro.

Qué ofrecen:

OWASP Top 10: El documento más famoso del sector que lista los 10 riesgos de seguridad más críticos en aplicaciones web.

Herramientas: Como *OWASP ZAP* (para escaneo de vulnerabilidades) o *Dependency Check*.

Guías de Testing: Metodologías estándar para realizar pruebas de penetración (ASVS, WSTG).

2.2. Métrica DREAD

La metodología DREAD fue adoptada y referenciada por comunidades como OWASP en el pasado para el **modelado de amenazas**. Es una forma cualitativa de clasificar el riesgo.

El acrónimo **DREAD** corresponde a los 5 factores que se evalúan (generalmente en una escala del 1 al 10):

1. **Damage (Daño Potencial):** Cuánto daño causaría el ataque si tiene éxito.
   1 = Nada ⟶ 10 = Destrucción total del sistema/datos.

2. **Reproducibility (Reproducibilidad):** Qué tan fácil es reproducir el ataque
   1 = Muy difícil ⟶ 10 = Siempre funciona.
3. **Exploitability (Explotabilidad):** Cuánto esfuerzo o habilidad técnica se requiere para lanzar el ataque
   1 = Experto en criptografía/kernel ⟶ 10 = Un script o navegador básicos.
4. **Affected Users (Usuarios Afectados):** Cantidad de personas impactadas
   1 = Un usuario ⟶ 10 = Todos los usuarios del sistema.
5. **Discoverability (Detectabilidad):** Como de complicado es encontrar la vulnerabilidad.
   1 = Muy difícil, código oscuro ⟶ 10 = Visible casi a simple vista.

Fórmula de Cálculo

Para obtener la criticidad final, se suele utilizar el promedio de los valores:

$$RIESGO = \frac{(Damage + Reproducibility + Exploitability + Users + Discoverability)}{5}$$

2.3. Métrica CVSS

Antes de analizar las diferencias entre la métrica CVSS y DREAD, lo primero que tenemos que hacer es entender que es CVSS.

CVSS (Common Vulnerability Scoring System) es el estándar industrial actual, mantenido por FIRST.org.

Característica	DREAD	CVSS
Enfoque	Modelado de amenazas (fase de diseño).	Gestión de vulnerabilidades (fase de operación/mantenimiento).
Subjetividad	**Alta.** Depende mucho de la opinión del analista ("¿Qué tan fácil es esto?").	**Baja.** Intenta ser objetiva basándose en características técnicas medibles.

Complejidad	Simple y rápida de calcular mentalmente.	Compleja. Requiere calculadora y evaluar métricas Base, Temporales y de Entorno.
Uso actual	En desuso (Microsoft usa ahora *Bug Bar* / STRIDE).	**Estándar mundial** (NVD, CVE, proveedores de software).
Métrica "Discoverability"	La incluye (penaliza si es fácil de encontrar).	**No la incluye.** Asume que si la vulnerabilidad existe, será encontrada.

❖ ¿Cuál es más eficiente?

Después de ver ambas comparativas en la tabla anterior, si nos basamos en aspectos técnicos, podemos concluir que **CVSS** es más eficiente y robusta para la industria profesional.

Los motivos relevantes son:

1. **Estandarización:** CVSS permite que una vulnerabilidad en un router Cisco y una en un servidor Windows se midan con la misma vara. DREAD es demasiado subjetivo para esto.
2. **Contexto:** CVSS permite ajustar la puntuación según el entorno (Métricas de Entorno). Por ejemplo, una vulnerabilidad crítica puede bajar a media si el servidor está desconectado de internet. DREAD es más estático.
3. **Madurez:** DREAD es útil para una "lluvia de ideas" rápida entre desarrolladores, pero CVSS es necesario para informes de auditoría, cumplimiento normativo y priorización de parches en empresas.

2.4. Descripción de 5 vulnerabilidades detectadas

A continuación, se describen cinco vulnerabilidades identificadas durante las fases de análisis de vulnerabilidades y pentesting sobre las máquinas del laboratorio (VM-MT y VM-WIN).

1. **Backdoor en Servicio FTP (VSFTPD)**

    a. **Descripción de la vulnerabilidad:**

    Durante la fase de explotación con Metasploit, se identificó una versión específica del servicio FTP en la máquina objetivo. Esta versión contiene una puerta trasera ("backdoor") conocida que permite la ejecución remota de código sin autenticación válida.

    b. **Criticidad:**

    Crítica (CVSS v3 aprox: 9.8)

    c. **Aplicación o enlace afectado:**

    Servicio FTP (puerto 21) ejecutándose en la máquina VM-MT (Metasploitable).

    d. **Alcance del daño:**

    Compromiso total del sistema. Un atacante puede abrir una "shell" de comandos con privilegios de *root*, obteniendo control absoluto sobre el servidor, sus archivos y la red interna conectada.

2. **Desbordamiento de Búfer en aplicación "FTP Utility"**

    a. **Descripción de la vulnerabilidad:**

    Se instaló intencionadamente una versión vulnerable del software "FTP Utility" para realizar pruebas de concepto. Esta aplicación falla al manejar correctamente la entrada de datos, permitiendo un desbordamiento de memoria (Buffer Overflow) que puede ser explotado mediante Metasploit.

    b. **Criticidad:**

    Alta / Crítica.

c. **Aplicación o enlace afectado:**

Software FTP Utility instalado en la máquina VM-WIN (Windows 10).

d. **Alcance del daño:**

Ejecución remota de código. El atacante logra establecer una sesión *Meterpreter* (reverse_tcp o bind), lo que le permite controlar el sistema operativo Windows de la víctima, exfiltrar datos o escalar privilegios.

3. Exposición de Paneles de Administración (Tomcat)

a. **Descripción de la vulnerabilidad:**

Mediante el escaneo con la herramienta Nikto, se descubrió que el servidor web tiene expuestos los directorios de gestión por defecto sin restricciones de acceso adecuadas, como el "host manager" y la herramienta de administración.

b. **Criticidad:**

Alta

c. **Aplicación o enlace afectado:**

Servidor Apache Tomcat (puerto 8180) en la máquina VM-MT.

d. **Alcance del daño:**

Si las credenciales por defecto no han sido cambiadas, un atacante puede desplegar aplicaciones maliciosas (archivos .WAR), detener servicios o reconfigurar el servidor web completo.

4. Acceso no autorizado a Gestor de Base de Datos (phpMyAdmin)

a. **Descripción de la vulnerabilidad:**

El análisis de vulnerabilidades web (realizado con Nikto o Nmap) reveló la existencia y accesibilidad de la interfaz de gestión de bases de datos phpMyAdmin y directorios sensibles como "doc" a través del puerto 80.

b. **Criticidad:**

Media / Alta (dependiendo de la fortaleza de la contraseña).

c. **Aplicación o enlace afectado:**

Interfaz web phpMyAdmin (puerto 80) en VM-MT.

d. **Alcance del daño:**

Fuga de información sensible, manipulación, robo o borrado de las bases de datos alojadas en el servidor. Posibilidad de inyectar código si la configuración de la base de datos lo permite.

5. Susceptibilidad a Ataques de Denegación de Servicio (SYN Flood)

a. **Descripción de la vulnerabilidad:**

El sistema objetivo no cuenta con mecanismos de protección (como *rate limiting* o *SYN cookies*) configurados en su pila TCP/IP. Esto permite que un atacante envíe un flujo masivo de paquetes SYN sin finalizar la conexión (usando hping3), agotando los recursos del sistema.

b. **Criticidad:**

Media (Afecta a la Disponibilidad).

c. **Aplicación o enlace afectado:**

Pila de red TCP/IP y servicios expuestos (Web/Apache) en VM-WIN.

d. **Alcance del daño:**

Interrupción del servicio. La máquina se vuelve inaccesible para los usuarios legítimos o deja de responder debido a la saturación de la tabla de conexiones, impidiendo la navegación o el acceso remoto.

2.5. Resumen estadístico de vulnerabilidades

El servicio está en riesgo debido a diversas vulnerabilidades de seguridad, cada una con diferentes niveles de criticidad.
En el entorno analizado (máquinas VM-MT (Metasploits) y VM-WIN (Windows)) se han identificado 5 vulnerabilidades principales, clasificadas de la siguiente forma:

- **2 vulnerabilidades Críticas**
- **2 vulnerabilidades Altas**

- **1 vulnerabilidad Media**

En total, el 80 % de las vulnerabilidades detectadas son de nivel Alto o Crítico, lo que indica un riesgo elevado para la confidencialidad, integridad y disponibilidad del sistema.

A continuación, se resumen las vulnerabilidades detectadas:

1. **Backdoor en Servicio FTP (VSFTPD) –**
   Criticidad: Crítica
   Indica que el servicio FTP está utilizando una versión de VSFTPD con una puerta trasera conocida, que permite la ejecución remota de código sin autenticación válida. Compromete por completo la máquina VM-MT, permitiendo obtener una shell con privilegios de root.

2. **Desbordamiento de Búfer en la aplicación "FTP Utility"** –
   Criticidad: Alta/Crítica
   Existe una versión vulnerable del software FTP Utility en VM-WIN que no gestiona correctamente la entrada de datos. Esto permite explotar un desbordamiento de memoria y conseguir ejecución remota de código mediante Metasploit, obteniendo una sesión Meterpreter sobre el sistema Windows.

3. **Exposición de Paneles de Administración (Apache Tomcat) –**
   Criticidad: Alta
   El servidor Tomcat de la máquina VM-MT tiene accesibles los paneles de administración y host manager mediante URLs por defecto. Si se mantienen credenciales por defecto o poco seguras, es posible desplegar aplicaciones maliciosas, detener servicios o reconfigurar el servidor.

4. **Acceso no autorizado a Gestor de Base de Datos (phpMyAdmin) –**
   Criticidad: Media/Alta
   Se ha detectado la interfaz phpMyAdmin accesible desde la red, junto a directorios sensibles como doc. Dependiendo de la fortaleza de las contraseñas y la configuración, puede permitir fuga de información, modificación o borrado de bases de datos y posibles ataques de inyección.

5. **Susceptibilidad a Ataques de Denegación de Servicio (SYN Flood) – Criticidad: Media**
   El sistema no tiene configurados mecanismos de protección específicos frente a SYN Flood (cómo rate limiting o SYN cookies). Un atacante puede enviar gran cantidad de paquetes SYN (por ejemplo, con hping3), saturando la tabla de conexiones y dejando los servicios de red inaccesibles.

2.6. Niveles de seguridad informática

A partir de las vulnerabilidades detectadas **(backdoor FTP, desbordamiento de búfer, paneles Tomcat expuestos, phpMyAdmin accesible y susceptibilidad a SYN Flood)**, se pueden relacionar los resultados con los siguientes estándares:

1. **ISO/IEC 27001**
   - **Descripción**: Estándar internacional para la gestión de la seguridad de la información mediante un Sistema de Gestión de Seguridad de la Información (SGSI).
   - **Relación con el proyecto:**
     - Las vulnerabilidades críticas detectadas muestran falta de controles básicos de gestión de vulnerabilidades, control de accesos, configuración segura de servicios y protección de la información.
   - **Conclusión:** El entorno analizado estaría en un nivel muy inicial de madurez respecto a los controles que propone ISO 27001.

2. **NIST Cybersecurity Framework**
   - **Descripción:** Marco de ciberseguridad basado en cinco funciones: Identificar, Proteger, Detectar, Responder y Recuperar.
   - **Relación con el proyecto:**
     - Se han realizado tareas de Identificar (vulnerabilidades) y se han probado ataques (parte de Proteger/Detectar desde el punto de vista didáctico), pero en un entorno real faltarían procesos claros

de Respuesta y Recuperación ante incidentes como una explotación de backdoor o un SYN Flood.

3. **COBIT (Control Objectives for Information and Related Technologies)**
   - **Descripción**: Marco de gestión y gobierno de TI que ayuda a alinear la tecnología con los objetivos del negocio, incluyendo gestión de riesgos y controles.

   - **Relación con el proyecto:**
     - La existencia de servicios vulnerables y mal configurados (VSFTPD vulnerable, Tomcat y phpMyAdmin expuestos) indica una falta de control en la gestión de cambios, configuraciones y activos TI, que COBIT trata de regular.

4. **CIS Controls (Center for Internet Security Controls)**

   - **Descripción**: Conjunto de controles y buenas prácticas técnicas para reducir las amenazas más frecuentes.

   - Relación con el proyecto:

     - Varias vulnerabilidades se podrían mitigar aplicando controles como:
       - Inventario y control de activos de software.
       - Configuración segura de servidores.
       - Gestión continua de vulnerabilidades.
       - Protección de puertos, servicios y cortafuegos.

5. **PCI DSS (Payment Card Industry Data Security Standard)**

   - **Descripción**: Estándar para proteger datos de tarjetas de pago.

   - Relación con el proyecto:

     - Aunque el laboratorio no trata datos de tarjetas, sirve como ejemplo de lo estrictos que deben ser los controles cuando hay información sensible: servicios con backdoors, contraseñas débiles o paneles expuestos serían inaceptables.

6. **TCSEC (Trusted Computer System Evaluation Criteria)**

Este modelo clasifica los sistemas en clases de seguridad desde D (sin protección) hasta A1 (seguridad muy alta con verificación formal):

- Clase D: Controles mínimos, prácticamente sin seguridad real.
- Clase C1/C2: Seguridad básica y controlada frente a usuarios no autorizados.
- Clases B y A: Seguridad más estricta, etiquetado, controles formales y resistencia frente a ataques avanzados.

Dado que en el entorno analizado hay backdoors, paneles de administración expuestos y falta de protección DoS, el nivel global se situaría entre **Clase D y C1**, adecuado solo para un entorno de prácticas, pero no para producción.

2.7. Medidas de mitigación

En base a las vulnerabilidades detectadas, se pueden proponer las siguientes mejoras técnicas y organizativas para mitigar estas amenazas.

1. **Actualizaciones y parches de servicios vulnerables**
   Mantener actualizado el servicio FTP (VSFTPD) y la aplicación FTP Utility, sustituyendo versiones vulnerables por versiones corregidas o alternativas seguras (por ejemplo, SFTP).

   Relacionado con: backdoor en VSFTPD, desbordamiento de búfer en FTP Utility.

2. **Desinstalación de software innecesario o inseguro**
   Eliminar aplicaciones instaladas únicamente para pruebas que serían peligrosas en producción, como la versión vulnerable de FTP Utility.

3. **Hardening de servidores y aplicaciones web (Tomcat, phpMyAdmin)**
   Configurar correctamente Tomcat y phpMyAdmin:

   - Deshabilitar paneles de administración que no se utilicen.
   - Cambiar credenciales por defecto.
   - Limitar su acceso a redes internas o a través de VPN.

4. **Control de acceso y autenticación robusta**
   Establecer políticas de contraseñas seguras (longitud, complejidad, caducidad) y, si es posible, aplicar doble factor de autenticación para accesos críticos.

5. **Segmentación de red**
   Separar servicios de administración (Tomcat Manager, phpMyAdmin) de las

redes de usuarios normales, utilizando VLANs o redes diferentes, reduciendo el impacto de un posible ataque.

6. **Protección frente a ataques de Denegación de Servicio (DoS/SYN Flood)**
    - Activar SYN cookies.
    - Ajustar parámetros de la pila TCP/IP (número máximo de conexiones, tiempos de espera).
    - Configurar reglas de firewall para limitar el número de conexiones por IP.

7. **Gestión continua de vulnerabilidades**
   Realizar escaneos periódicos con herramientas de análisis de vulnerabilidades y revisar informes para aplicar correcciones antes de que puedan ser explotadas.

8. **Registro y monitorización de eventos**
   Habilitar logs en servicios como FTP, Tomcat, Apache y bases de datos, y revisar regularmente estos registros para detectar accesos sospechosos o intentos de explotación.

9. **Configuración segura de servidores en Internet**
   Minimizar la exposición de servicios, cerrando puertos que no son necesarios y evitando publicar paneles de administración directamente hacia Internet.

10. **Copias de seguridad y plan de recuperación**
    Mantener copias de seguridad periódicas de bases de datos y sistemas críticos para poder recuperar la información en caso de ataque exitoso.

11. **Educación y concienciación en seguridad**
    Formar a administradores y personal técnico en buenas prácticas de seguridad, gestión de contraseñas, hardening y respuesta a incidentes.

12. **Pruebas de penetración periódicas**
    Repetir pruebas de pentesting de forma regular para validar que las vulnerabilidades corregidas no reaparecen y que no surgen nuevas debilidades.

2.8. Informe técnico final consolidado

A continuación, se presenta un informe técnico final consolidado:

2.8.1. Vulnerabilidades detectadas en el entorno de laboratorio

Se han identificado 5 vulnerabilidades principales en las máquinas VM-MT y VM-WIN, destacando:

- Presencia de acceso por la puerta trasera en los servicios FTP (VSFTPD).
- Desbordamiento de búfer en FTP Utility que permite ejecución remota de código.
- Paneles de administración de Tomcat expuestos.
- Acceso a phpMyAdmin sin restricciones adecuadas.
- Falta de protección frente a SYN Flood que afecta a la disponibilidad.

La mayoría de estas vulnerabilidades permiten un alto grado de control sobre los sistemas.

2.8.2. Impacto sobre la confidencialidad, integridad y disponibilidad

- **Confidencialidad:**

- Se ve comprometida por la puerta de atrás de la herramienta FTP y por el acceso a phpMyAdmin, que permiten leer información sensible, ficheros del sistema y bases de datos.

- **Integridad:**

  - Las vulnerabilidades que permiten ejecución remota de código y acceso a paneles de administración permiten modificar configuraciones, bases de datos y contenidos, comprometiendo gravemente la integridad de la información.

- **Disponibilidad:**

  - La susceptibilidad a SYN Flood puede dejar servicios inaccesibles, afectando a los usuarios legítimos y a la continuidad del servicio.

2.8.3. Relación con marcos y niveles de seguridad

Comparando el estado actual con marcos como ISO/IEC 27001, NIST CSF y modelos como TCSEC, se concluye:

- El entorno presenta un nivel de seguridad bajo, gestión de vulnerabilidades y control de acceso poco desarrollados.

- Según **TCSEC**, el sistema se situaría entre clase D/C1, adecuado únicamente como entorno de prácticas y no como sistema de producción.

2.8.4. Recomendaciones prioritarias

1. Eliminar o actualizar servicios y aplicaciones vulnerables (VSFTPD vulnerable, FTP Utility).

2. Restringir y securizar paneles de administración (Tomcat, phpMyAdmin), cambiando credenciales por defecto y limitando el acceso por IP o VPN, llegando a segmentar la red por VLAN o deshabilitando el puerto de acceso a estos recursos.

3. Implementar medidas de protección frente a DoS/SYN Flood, ajustando la pila TCP/IP y configuración de firewalls.

4. Aplicar políticas de contraseñas seguras y revisar permisos de usuarios y servicios.

5. Establecer un proceso de gestión de vulnerabilidades y parches, con escaneos periódicos.

2.8.5. Conclusión

El análisis realizado demuestra que aunque el entorno es de laboratorio y está pensado para fines de producción, el riesgo técnico es muy elevado debido a la presencia de puertas traseras con acceso fácil, desbordamientos de búfer, paneles de administración expuestos y falta de protección frente a ataques de denegación de servicio.

La aplicación de las medidas propuestas (protección de la red, segmentación y gestión continua de vulnerabilidades) permitiría mejorar de forma significativa el nivel de seguridad, acercando el sistema a las buenas prácticas recomendadas por los principales estándares de seguridad informática.

3. Informe no técnico para gerencia

3.1. Plan de Seguridad Informática

En este apartado se muestran los diferentes puntos para tener en cuenta para la gestión de la seguridad dentro de la empresa mediante un plan de seguridad.

Objetivos principales que debe cumplir el plan de seguridad

Confidencialidad: El primer objetivo que marcamos en este plan es asegurar la confidencialidad de los datos, esto se conseguirá tomando las medidas de seguridad necesarias en los equipos e infraestructuras como pueden ser análisis periódicos con diferentes herramientas como las que hemos ido usando en productos anteriores.

Integridad: El siguiente objetivo que debemos tener en cuenta es el control de acceso de esta forma minimizamos la posibilidad de que usuarios no autorizados de dentro de la empresa o si algún usuario consiguiera entrar de forma no autorizada a la red de la empresa puedan acceder y modificar información que no debiera ser modificada.

Disponibilidad: El último objetivo, no es un objetivo tan relacionado con la seguridad, pero también en ciertos casos podría ayudar a cumplir los dos anteriores, en este caso se habla de la disponibilidad, cuanta más disponibilidad de equipos tengamos todo estará más controlado, ya que podremos trabajar con mucha más seguridad en lo que a integridad de la información se refiere.

Medidas a aplicar para cumplir estos objetivos

Gestión de accesos

Se usarán contraseñas para todos los accesos y en los accesos críticos se podrá usar una 2FA para el acceso.

Se asignan roles a los usuarios con listas de ACLs restrictivas en función del puesto en la empresa.

Protección de la red

Se segmentan las redes de las oficinas para evitar el intercambio de información entre ellas.

Se instalarán firewalls tanto de software en todos los equipos como de hardware en la entrada desde el ISP.

Protección de los equipos

Se mantendrán todos los equipos actualizados a las últimas versiones disponibles en cuanto a aplicaciones se refiere.

Adicionalmente al firewall en los equipos también se instalará software antivirus para una protección mayor contra amenazas.

Se realizarán auditorías periódicas con herramientas de seguridad como pueden ser Nessus u OpenVAS para la búsqueda de vulnerabilidades que puedan ir apareciendo.

Copias de Seguridad

Se realizarán copias de seguridad locales y en la nube en función de las necesidades para preservar los datos y su integridad.

Adicionalmente, periódicamente se realizarán pruebas de restauración para ver la eficacia e integridad de estas copias realizadas periódicamente.

Plan de respuesta a incidentes

Se realizará un plan de respuesta claro para todos los empleados de la empresa para saber como actuar en caso de detectar algún fallo o vulnerabilidad en la empresa.

3.2. Mapa de Red con Equipamiento de Seguridad

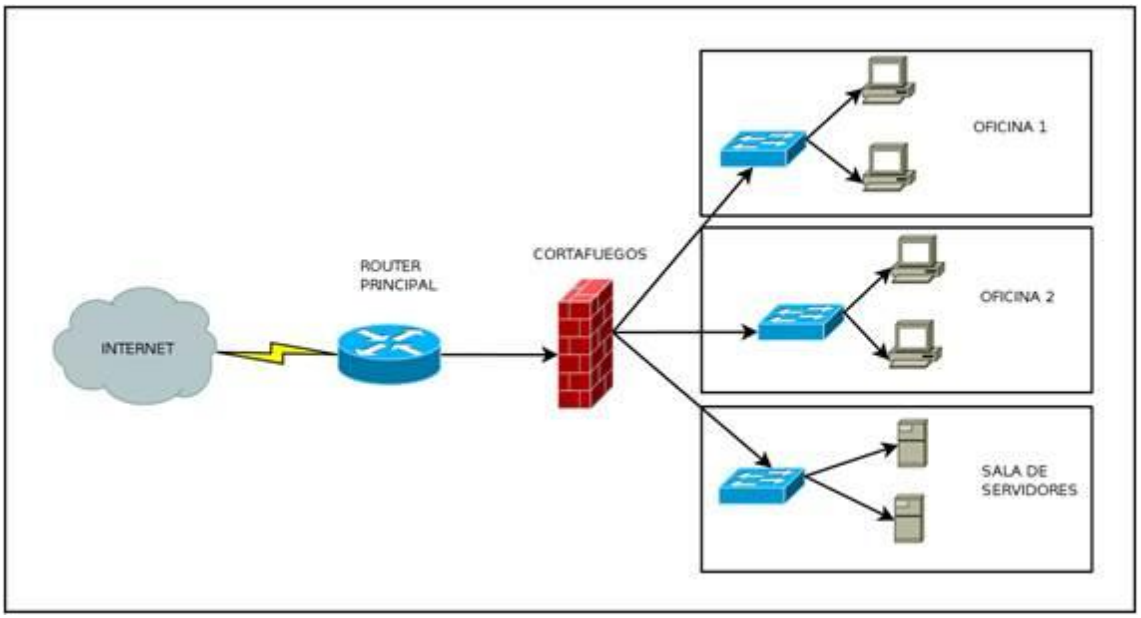
En este apartado se muestra la infraestructura básica de la red de la empresa.

Para la conexión a internet encontramos el router del ISP.

El primer elemento que nos encontramos después del router principal es el Firewall.

A partir de este firewall se conectaría a un switch el cual se encargaría de distribuir al resto de las oficinas, este switch no se encuentra en el diagrama expuesto, ya que es una versión simplificada del diagrama real

Finalmente se representa de una forma básica como son las diferentes salas que se encuentran en la empresa, como se puede observar no existen conexiones a las salas sin pasar por el firewall. Dentro de cada sala se encuentra un switch para realizar las conexiones de red de los equipos.



3.3. Cuadro Comparativo de Herramientas de Prevención de Ataques

Herramienta	Funciones Principales	Ventajas	Limitaciones	Donde se debe Instalar
Antivirus*	Detecta y elimina virus conocidos	Bajo coste de mantenimiento	Protección básica, solo detecta virus ya conocidos.	Se instalará en todos los equipos
Antimalware*	Bloquea software malicioso en los equipos	Analiza el comportamiento del software	Precio elevado según las funciones deseadas.	Servidores y estaciones criticas para la empresa.
Antispyware*	Previene el robo de información	Protege credenciales e información sensible en los equipos.	Poca efectividad contra malware más complejo.	PCs de empleados y dispositivos móviles
Firewall software	Filtra tráfico en cada equipo	Altas opciones de filtrado y configuración	Difícil de configurar	En todos los equipos como complemento al firewall perimetral
IDS (Intrusion Detection System)	Detecta y bloquea intrusiones no autorizadas	Bloquea ataques no autorizados	Requiere un mantenimiento constante.	Servidores y red corporativa
SIEM (Security Information and Event Management)	Centraliza las alertas de todos los softwares y equipos	Centraliza toda la seguridad	Coste elevado	Servidores encargados de la gestión de la seguridad

* En ciertos casos estos bien en el mismo paquete de software disminuyendo así las limitaciones entre ellos.

3.4. Auditoría y previsión de costes

A partir de los análisis realizados en los productos anteriores, se ha llevado a cabo una auditoría técnica orientada a evaluar el estado actual de los servicios informáticos utilizados en la empresa, identificar sus principales debilidades y proponer mejoras que permitan una puesta en producción segura, estable y eficiente.
Esta auditoría sigue los criterios propios de la auditoría informática: revisión del estado actual, detección de debilidades, análisis del impacto y emisión de recomendaciones concretas orientadas a la mejora continua.

Situación Actual de los Servicios Analizados

Los resultados previos evidenciaron diversos riesgos y carencias en la infraestructura tecnológica, entre los que destacan:

Vulnerabilidades críticas en servidores

- Servicios desactualizados (FTP, SMB, Apache, Tomcat).
- Credenciales por defecto en aplicaciones internas.
- Exposición de puertos y servicios sin medidas de protección.

Falta de seguridad en la red interna

- Ausencia de firewall avanzado.
- Tráfico sin filtrar y sin segmentación.
- Ausencia de un sistema de detección de intrusiones (IDS/IPS).

Protección insuficiente en los equipos

- Carencia de herramientas corporativas de antivirus y antimalware.
- Configuraciones inseguras y riesgo elevado de ataques de ransomware.

Riesgos asociados a errores humanos

- Uso de contraseñas débiles.
- Accesos no controlados.

Ausencia de un sistema sólido de copias de seguridad

- Riesgo real de pérdida de datos críticos.

Debilidades Detectadas

Del análisis se desprende la existencia de las siguientes debilidades principales:

1. **Riesgo elevado de intrusión externa** por la falta de protección perimetral y puertos vulnerables expuestos.
2. **Riesgo de infección por malware** por la falta de herramientas corporativas de protección.
3. **Inestabilidad operativa** derivada de servicios no actualizados.
4. **Ausencia de protocolos internos de seguridad** (PSI, control de accesos, gestión de credenciales).

5. **Deficiencias en la continuidad de negocio** por la falta de backups y recuperación ante desastres.
6. **Escasa monitorización**, lo que dificulta detectar incidentes antes de que generen un impacto.

Estas debilidades comprometen la integridad del sistema, la disponibilidad de los servicios y la protección de los datos personales.

Propuestas de Mejora

Las mejoras recomendadas se dividen en cinco áreas estratégicas:

Seguridad perimetral

- Implantación de un **firewall UTM profesional**.
- Creación de redes segmentadas (VLANs) para separar zonas críticas: desarrollo, servidores, oficinas, invitados.
- Configuración de reglas restrictivas para evitar accesos no autorizados.

Beneficio: protección frente a ataques externos y reducción del riesgo de intrusiones.

Seguridad en servidores y servicios

- Actualización completa del sistema operativo y servicios vulnerables.
- Eliminación o desactivación de protocolos inseguros (FTP, Telnet).
- Aplicación de medidas de hardening en todos los servidores.
- Revisión periódica de permisos y configuraciones.

Beneficio: reducción drástica de vulnerabilidades y mejora en la estabilidad operativa.

Seguridad en los equipos del personal

- Instalación de antivirus y antimalware corporativo.
- Implementación de autenticación multifactor (2FA).
- Restricción de dispositivos USB.
- Configuración de políticas de uso seguro.

Beneficio: menor probabilidad de infecciones y accesos indebidos.

Monitorización y detección temprana

- Instalación de un sistema IDS/IPS para supervisar el tráfico en tiempo real.
- Configuración de alertas automáticas ante comportamientos sospechosos.
- Revisión semanal de logs y eventos.

Beneficio: detección de ataques antes de que afecten a los servicios.

Copias de seguridad y continuidad de negocio

- Implementación de un NAS empresarial.
- Copias automáticas diarias, semanales y mensuales.
- Cifrado de backups y almacenamiento redundante.

- Pruebas de recuperación trimestrales.

Beneficio: protección contra ransomware, fallos técnicos y pérdida de datos.

Previsión de Costes Económicos

A continuación se presenta una estimación económica para la puesta en producción segura de los servicios, adaptada al tamaño estándar de una PIME tecnológica.

Equipamiento físico

Elemento	**Coste aproximado**
Firewall UTM profesional	800 – 1.500 €
Switch gestionable 24 puertos	250 – 450 €
Puntos WiFi profesionales (2 uds.)	250 – 350 €
NAS empresarial	400 – 700 €
Discos duros para NAS (2×4 TB)	200 – 300 €
SAI/UPS para proteger servidores	150 – 250 €

Subtotal equipamiento: 2.000 – 3.500 €

Software y licencias

Software	**Coste anual aproximado**
Antivirus corporativo	150 – 300 €/año
Antimalware / Anti-ransomware	200 – 400 €/año
Gestor de contraseñas	100 – 200 €/año
Copia en la nube (backup off-site)	150 – 300 €/año

Subtotal anual: 600 – 1.200 €/año

Servicios profesionales

Servicio	Coste aproximado
Implantación del firewall y segmentación de red	300 – 600 €
Hardening de servidores	200 – 500 €
Configuración de copias de seguridad	150 – 300 €
Auditoría externa de seguridad	400 – 800 €
Formación en ciberseguridad	150 – 300 €

Subtotal servicios: 1.200 – 2.500 €

Coste Total Estimado

- **Coste inicial de implantación: 4.000 – 7.000 €**
- **Coste anual de mantenimiento: 600 – 1.200 €**

La auditoría evidencia que, aunque la empresa cuenta con recursos tecnológicos funcionales, existen carencias significativas en materia de seguridad. Las mejoras propuestas y su correspondiente inversión económica permiten:

- Reducir el riesgo de ciberataques.
- Proteger los datos de clientes, empleados y usuarios de las aplicaciones.
- Garantizar la disponibilidad de los servicios.
- Cumplir con las normativas vigentes de protección de datos.
- Modernizar la infraestructura tecnológica.

3.5. Normativa legal y RGPD

Introducción

La empresa analizada es una PIME tecnológica dedicada al desarrollo de aplicaciones móviles para Android e iOS. Debido a su actividad, trata datos personales de clientes, usuarios de las aplicaciones, proveedores y empleados. Por este motivo, está obligada a cumplir con el **Reglamento General de Protección de Datos (RGPD)** y la **Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de Derechos Digitales (LOPDGDD)**.

El objetivo de esta propuesta es establecer las obligaciones legales que debe aplicar la empresa y las directrices prácticas para garantizar un tratamiento seguro y conforme

a la ley, teniendo en cuenta su tamaño y su actividad.

Marco Normativo de Referencia

RGPD (Reglamento UE 2016/679)

Es la norma principal que regula la protección de datos personales y establece:

- Requisitos de seguridad técnica.
- Obligaciones de transparencia e información.
- Derechos de los usuarios.
- Responsabilidades del Responsable del Tratamiento.
- Notificación de brechas de seguridad.

LOPDGDD (Ley Orgánica 3/2018)

Complementa y desarrolla el RGPD en España, añadiendo:

- Derechos digitales en el entorno laboral.
- Regulación de videovigilancia y geolocalización.
- Normas sobre el tratamiento de datos de empleados.

Real Decreto 1720/2007

Aunque parcialmente derogado, mantiene en vigor artículos relacionados con:

- Gestión documental.
- Medidas organizativas internas no incompatibles con el RGPD.

ENS (Esquema Nacional de Seguridad – RD 311/2022)

No es obligatorio para PIMEs privadas, pero sus principios sirven de guía para:

- Clasificación de información.
- Controles de seguridad.
- Gestión de riesgos y continuidad.

Datos que trata la empresa

Debido a su actividad, la empresa procesa:

- **Datos identificativos**: nombres, correos, teléfonos.
- **Datos técnicos**: direcciones IP, identificadores de dispositivos móviles.
- **Datos de uso de apps**: estadísticas, comportamiento en la aplicación.
- **Datos laborales internos**: nóminas, contratos, horarios.
- **Datos de clientes y proveedores**.

Esta categoría de datos obliga a implementar medidas de seguridad adecuadas al riesgo, según el art. 32 del RGPD.

Obligaciones Legales que Debe Cumplir la Empresa

Registro de Actividades de Tratamiento (RAT)

La empresa debe documentar todos los tratamientos de datos personales indicando:

- Finalidades del tratamiento.
- Base jurídica (contrato, consentimiento, interés legítimo…).
- Plazos de conservación.
- Cesiones a terceros y transferencias internacionales.
- Sistemas utilizados (apps, servidores, software).

Este documento debe mantenerse actualizado y disponible para inspección.

Información al Usuario y Políticas de Privacidad

Cada aplicación móvil debe incluir una **política de privacidad clara**, que explique:

- Qué datos se recogen.
- Para qué se utilizan.
- Durante cuánto tiempo se conservan.
- Qué derechos tiene el usuario.
- Cómo puede ejercerlos.

La información debe ser transparente y fácil de entender.

Obtención del Consentimiento

El RGPD exige consentimiento explícito cuando:

- Se usan datos de localización.
- Se accede a cámara, micrófono, galería o sensores del móvil.
- Se envían notificaciones personalizadas.
- Se utilizan SDKs o herramientas de analítica de terceros.

El consentimiento debe ser:

- Claro
- Informado
- Reversible
- Específico para cada finalidad

Encargados del Tratamiento

La empresa debe firmar contratos RGPD con proveedores que traten datos en su nombre, como:

- Servicios de hosting o servidores.
- Plataformas de analítica móvil (Firebase, Google Analytics).
- Sistemas de mensajería push.

Estos contratos aseguran que el proveedor cumple también con el RGPD.

Seguridad Técnica y Organizativa (art. 32 RGPD)

La empresa debe aplicar medidas adecuadas a su nivel de riesgo:

Medidas técnicas:

- Cifrado de datos en tránsito (HTTPS).
- Cifrado de datos sensibles almacenados.
- Control de accesos por roles.
- Antivirus y antimalware.
- Sistemas de copias de seguridad.
- Firewall y segmentación de red.
- Autenticación multifactor en servicios internos.

Medidas organizativas:

- Políticas de seguridad por escrito.
- Procedimientos internos de gestión de incidencias.
- Control de acceso físico a servidores.
- Formación periódica en protección de datos.

Evaluaciones de Impacto (EIPD)

Obligatorias cuando las apps realizan:

- Perfilados complejos.
- Tratamiento sistemático de datos de localización.
- Recogida masiva de datos de usuarios.

La empresa debe evaluar los riesgos previamente y documentar cómo los reducirá.

Derechos de los Usuarios

Debe habilitar mecanismos gratuitos y sencillos para que cualquier usuario pueda ejercer:

- Acceso
- Rectificación
- Supresión
- Portabilidad
- Oposición
- Limitación del tratamiento

Las respuestas deben darse en un máximo de 1 mes.

Notificación de Brechas de Seguridad

Si ocurre un incidente que afecte a los datos personales:

- Debe notificarse a la AEPD en **menos de 72 horas**.
- Si es grave, también a los usuarios afectados.
- Debe existir un registro interno de brechas.

Directrices RGPD Específicas Para una Empresa Tecnológica

Debido al tipo de empresa, se aplican las siguientes directrices adicionales:

Privacidad desde el Diseño y por Defecto

Cada nueva aplicación desarrollada debe integrar la privacidad desde el primer momento:

- Minimización de datos.
- Configuraciones seguras por defecto.
- Solo se recogen los datos estrictamente necesarios.

Seguridad en APIs y comunicaciones

- Uso obligatorio de cifrado TLS.
- Autenticación fuerte en API y paneles admin.
- Revisiones de código y test de penetración.

Gestión segura del ciclo de vida del software

- Control de versiones.
- Encriptación de tokens y claves API.
- Eliminación de datos obsoletos.
- Pruebas de seguridad previas a la publicación.

Almacenamiento local seguro en la app

- Evitar almacenamiento en texto plano.
- Uso de KeyStore / Secure Enclave.

Control de terceros

Revisión exhaustiva de:

- SDKs externos
- Bibliotecas publicitarias
- Proveedores con acceso a datos

Recomendación Final

La empresa debe implantar un **Sistema de Gestión de Protección de Datos** que combine:

- Documentación legal actualizada
- Medidas técnicas efectivas
- Formación continua
- Auditorías periódicas

Cumplir el RGPD no es solo una obligación legal, sino una oportunidad para:

- Aumentar la confianza del usuario
- Mejorar la imagen corporativa
- Reducir riesgos de sanciones

- Asegurar que las aplicaciones móviles se desarrollan de forma responsable y segura

4. Bibliografía

- Burgos Salazar, J., & Campos, P. G. (s.f.). *Modelo para seguridad de la información en TIC* (paper13.pdf). Universidad del Bío-Bío.
- ENISA – European Union Agency for Cybersecurity. (2025). *About ENISA.* https://www.enisa.europa.eu/about-enisa
- Exploit Database. (2025). *Exploit 39215.* https://www.exploit-db.com/exploits/39215
- FIRST – Forum of Incident Response and Security Teams. (2025). *CVSS.* https://www.first.org/cvss/
- FIRST – Forum of Incident Response and Security Teams. (2025). *CVSS v3.1.* https://www.first.org/cvss/v3-1/
- Greenbone Networks. (2025). *Greenbone Community Edition.* https://www.greenbone.net/en/community-edition/
- INCIBE – Instituto Nacional de Ciberseguridad. (2025). *Conócenos.* https://www.incibe.es/conocenos
- López Viñas, D. (s.f.). *Auditoría informática* (P08/B0587/01928). Universitat Oberta de Catalunya.
- Microsoft. (2025). *Threat modeling for drivers.* https://learn.microsoft.com/en-us/windows-hardware/drivers/driversecurity/threat-modeling-for-drivers
- Metodología PSI – Proyecto de Seguridad Informática. (s.f.). *Metodología para la elaboración de Políticas de Seguridad de la Información*.
- NIKTO Project. (2025). *Nikto2 Web Scanner.* https://cirt.net/Nikto2
- OWASP Foundation. (2025). OWASP. https://owasp.org/
- OWASP Foundation. (2025). OWASP Top Ten. https://owasp.org/www-project-top-ten/
- Rapid7. (2025). Metasploit Framework Documentation. https://docs.metasploit.com/