INFORMÁTICA Y COMUNICACIONES
G.S. Administración de Sistemas Informáticos en Red

La seguridad y la alta disponibilidad

Fernando Fernández Fidalgo

EDITORIAL SINTESIS

La seguridad y la alta disponibilidad

Fernando Fernández Fidalgo

EDITORIAL SINTESIS

© Fernando Fernández Fidalgo

© EDITORIAL SÍNTESIS, S. A.
Vallehermoso, 34. 28015 Madrid
Teléfono 91 593 20 98
www.sintesis.com

ISBN: 978-84-1357-437-0
Depósito Legal: M-13.734-2025

Impreso en España - Printed in Spain

Reservados todos los derechos. Está prohibido, bajo las sanciones penales y el resarcimiento civil previstos en las leyes, reproducir, registrar o transmitir esta publicación, íntegra o parcialmente, por cualquier sistema de recuperación y por cualquier medio, sea mecánico, electrónico, magnético, electroóptico, por fotocopia o por cualquier otro, sin la autorización previa por escrito de Editorial Síntesis, S. A.

ÍNDICE

Presentación 8

1. Adopción de pautas de seguridad informática RA1

Resultado de aprendizaje y criterios de evaluación 10
Objetivos de Desarrollo Sostenible 10
Mapa conceptual 11
Glosario 12
Punto de partida 12
1.1. Introducción 13
1.2. Pilares fundamentales de la seguridad informática: fiabilidad, confidencialidad, integridad y disponibilidad 13
1.2.1. La paradoja de la seguridad 18
1.3. Elementos vulnerables en el sistema informático 19
1.4. Análisis de las principales vulnerabilidades de un sistema informático 20
1.4.1. Vulnerabilidades más comunes 21
1.4.2. Herramientas de análisis de vulnerabilidades 21
1.5. Amenazas 22
1.5.1. Tipos de amenazas 22
1.5.2. Estadísticas 24
1.6. Seguridad física y ambiental 25
1.6.1. Ubicación y protección física de los equipos y servidores 25
1.6.2. Sistemas de alimentación ininterrumpida (SAI) 25
1.6.3. Estructura física y componentes de un SAI 26
1.7. Seguridad lógica 27
1.7.1. Criptografía 27
1.7.2. Listas de control de acceso (ACL) 29
1.7.3. Establecimiento de políticas de contraseñas 31
1.7.4. Utilización de sistemas biométricos de identificación 32
1.7.5. Políticas de almacenamiento 33
1.7.6. Copias de seguridad e imágenes de respaldo 33

1.7.7. Medios de almacenamiento 35
1.7.8. Recuperación de datos 36
1.7.9. Realización de auditorías de seguridad 38
1.8. Análisis forense en sistemas informáticos 40
1.8.1. Objetivo del análisis forense 40
1.8.2. Recogida y análisis de evidencias 40
1.8.3. Herramientas del análisis 41
Ideas clave 44
Aplica lo aprendido 45
Solución del punto de partida 46
Práctica profesional 47
Ponte a prueba 48

2. Implantación de mecanismos de seguridad activa RA2

Resultado de aprendizaje y criterios de evaluación 50
Objetivos de Desarrollo Sostenible 50
Mapa conceptual 51
Glosario 52
Punto de partida 52
2.1. Introducción 53
2.2. Ataques y contramedidas en sistemas personales 53
2.2.1. Clasificación de los ataques 53
2.2.2. Anatomía de ataques y análisis de software malicioso 54
2.2.3. Herramientas preventivas 55
2.2.4. Herramientas paliativas 56
2.2.5. Actualización de sistemas y aplicaciones 58
2.3. Seguridad en la conexión con redes públicas 58
2.3.1. Identificación digital 58
2.3.2. Firma electrónica y certificado digital 59
2.3.3. Publicidad y correo no deseado 60
2.3.4. Otros 61
2.4. Elaboración de un manual de seguridad y planes de contingencia 62
2.5. Seguridad en la red corporativa 65
2.5.1. Monitorización del tráfico en redes 65
2.5.2. Seguridad en los protocolos para comunicaciones inalámbricas 67
2.5.3. Riesgos potenciales de los servicios de red 68
2.5.4. Intentos de penetración 69
2.5.5. Sistemas de detección de intrusiones 70
Ideas clave 72
Aplica lo aprendido 73
Solución del punto de partida 74
Práctica profesional 75
Ponte a prueba 76

3. Implantación de técnicas de acceso remoto. Seguridad perimetral RA3

Resultado de aprendizaje y criterios de evaluación 78
Objetivos de Desarrollo Sostenible 78
Mapa conceptual 79
Glosario 80
Punto de partida 80
3.1. Introducción 81
3.2. Elementos básicos de la seguridad perimetral 81
3.2.1. *Router* frontera 81
3.2.2. Cortafuegos 82
3.2.3. Redes privadas virtuales (VPN) 85
3.2.4. Perímetros de red 86
3.3. Políticas de defensa en profundidad 87
3.3.1. Defensa perimetral 87
3.3.2. Defensa interna 89
3.3.3. Factor humano 90
3.4. Cifrado y tipos de VPN 91
3.4.1. Beneficios y desventajas con respecto a las líneas dedicadas 92
3.4.2. Técnicas de cifrado 92
3.4.3. Tipos de VPN 96
3.5. Servidores de acceso remoto 99
3.5.1. Protocolos de autenticación 100
3.5.2. Configuración de parámetros de acceso 101
3.5.3. Servidores de autenticación 102
Ideas clave 106
Aplica lo aprendido 107
Solución del punto de partida 108
Práctica profesional 109
Ponte a prueba 110

4. Instalación y configuración de cortafuegos RA4

Resultado de aprendizaje y criterios de evaluación 112
Objetivos de Desarrollo Sostenible 112
Mapa conceptual 113
Glosario 114
Punto de partida 114
4.1. Introducción 115
4.2. Utilización de cortafuegos 115
4.2.1. Filtrado de paquetes de datos 116
4.2.2. Ubicación de cortafuegos 118
4.2.3. Reglas de filtrado de cortafuegos 121
4.3. Pruebas de funcionamiento 122

4.3.1. Herramientas de sondeo 123
4.3.2. Pasos para realizar un sondeo 125
4.4. Registros de sucesos de un cortafuegos 126
4.5. Tipos de cortafuegos 127
4.5.1. Cortafuegos integrados en los sistemas operativos 128
4.5.2. Cortafuegos libres y propietarios 130
4.5.3. Cortafuegos hardware 133
Ideas clave 134
Aplica lo aprendido 135
Solución del punto de partida 136
Práctica profesional 137
Ponte a prueba 138

5. Instalación y configuración de servidores proxy RA5

Resultado de aprendizaje y criterios de evaluación 140
Objetivos de Desarrollo Sostenible 140
Mapa conceptual 141
Glosario 142
Punto de partida 142
5.1. Introducción 143
5.2. Tipos de proxy 143
5.2.1. Proxy de reenvío o proxy directo *(forward proxy)* 143
5.2.2. Proxy inverso *(reverse proxy)* 144
5.2.3. Proxy transparente 144
5.2.4. Proxy anónimo 145
5.2.5. Proxies encadenados 145
5.3. Instalación de servidores proxy 146
5.3.1. Instalación en sistemas basados en Linux 147
5.3.2. Instalación en Windows 149
5.3.3. Instalación en macOS 152
5.4. Instalación y configuración de clientes proxy 153
5.4.1. Configuración manual en navegadores 153
5.4.2. Configuración automática mediante scripts PAC 154
5.4.3. Configuración en sistemas operativos 155
5.4.4. Configuración avanzada con autenticación 158
5.5. Configuración del almacenamiento en la caché de un proxy 160
5.5.1. Configuración básica de la caché en Squid 161
5.5.2. Monitoreo y mantenimiento de la caché 162
5.5.3. Configuración avanzada de la caché 164
5.5.4. Consideraciones para un almacenamiento en caché eficiente 165
5.6. Configuración de filtros 165
5.6.1. Configuración de filtros en Squid 166
5.6.2. Configuración de filtros en otros proxies 168

5.6.3. Pruebas y mantenimiento de los filtros 169
5.6.4. Consideraciones de buenas prácticas 170
5.7. Métodos de autenticación en un proxy 172
5.8. Proxies inversos 175
5.8.1. Configuración de un proxy inverso 176
5.8.2. Balanceo de carga con proxy inverso 178
5.8.3. Seguridad y pruebas de un proxy inverso 181
5.8.4. Documentación de configuración 183
5.9. Proxies encadenados 183
5.9.1. Arquitectura de proxies encadenados 185
5.9.2. Implementación de proxies encadenados 185
5.9.3. Ventajas y desafíos de los proxies encadenados 189
5.9.4. La red TOR: enrutamiento distribuido para anonimato 190
5.9.5. Solución de problemas 192
5.9.6. Documentación 195
5.10. Pruebas de funcionamiento 198
5.10.1. Tipos de pruebas. 199
5.10.2. Proceso de pruebas de funcionamiento 200
5.10.3. Herramientas gráficas 201
Ideas clave 208
Aplica lo aprendido 209
Solución del punto de partida 210
Práctica profesional 211
Ponte a prueba 212

6. Implantación de soluciones de alta disponibilidad RA6

Resultado de aprendizaje y criterios de evaluación 214
Objetivos de Desarrollo Sostenible 214
Mapa conceptual 215
Glosario 216
Punto de partida 216
6.1. Introducción 217
6.2. Definición y objetivos 217
6.3. Análisis de configuraciones de alta disponibilidad 219
6.3.1. Funcionamiento ininterrumpido 220
6.3.2. Integridad de datos y recuperación de servicio 221
6.3.3. Servidores redundantes 222
6.3.4. Sistemas de clústeres 223
6.3.5. Balanceadores de carga 224
6.4. Soluciones de alta disponibilidad basadas en virtualización 225
6.5. Virtualización de sistemas 229
6.6. Configuración y utilización de máquinas virtuales 232
6.6.1. Alta disponibilidad y virtualización 232

6.6.2. Simulación de servicios con virtualización 233
6.6.3. Servicios reales con virtualización 234
6.7. Análisis de la actividad del sistema virtualizado 234
6.7.1. Pruebas de carga 235
6.7.2. Modelos predictivos y análisis de tendencias 237
Ideas clave 240
Aplica lo aprendido 241
Solución del punto de partida 242
Práctica profesional 243
Ponte a prueba 244

7. Legislación y normas sobre seguridad RA7

Resultado de aprendizaje y criterios de evaluación 246
Objetivos de Desarrollo Sostenible 246
Mapa conceptual 247
Glosario 248
Punto de partida 248
7.1. Introducción 249
7.2. Legislación sobre protección de datos 250
7.2.1. Reglamento General de Protección de Datos (RGPD) 250
7.2.2. Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD) 252
7.3. Legislación sobre servicios digitales 254
7.4. Normas ISO sobre gestión de seguridad de la información 256
7.4.1. Normas ISO/IEC 27000 256
7.4.2. Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) 259
7.4.3. Otros estándares internacionales relevantes: NIST 261
7.5. Organismos de gestión de incidencias 263
Ideas clave 268
Aplica lo aprendido 269
Solución del punto de partida 270
Práctica profesional 271
Ponte a prueba 272

2 Implantación de mecanismos de seguridad activa

RESULTADO DE APRENDIZAJE Y CRITERIOS DE EVALUACIÓN

RA2. Implanta mecanismos de seguridad activa, seleccionando y ejecutando contramedidas ante amenazas o ataques al sistema.

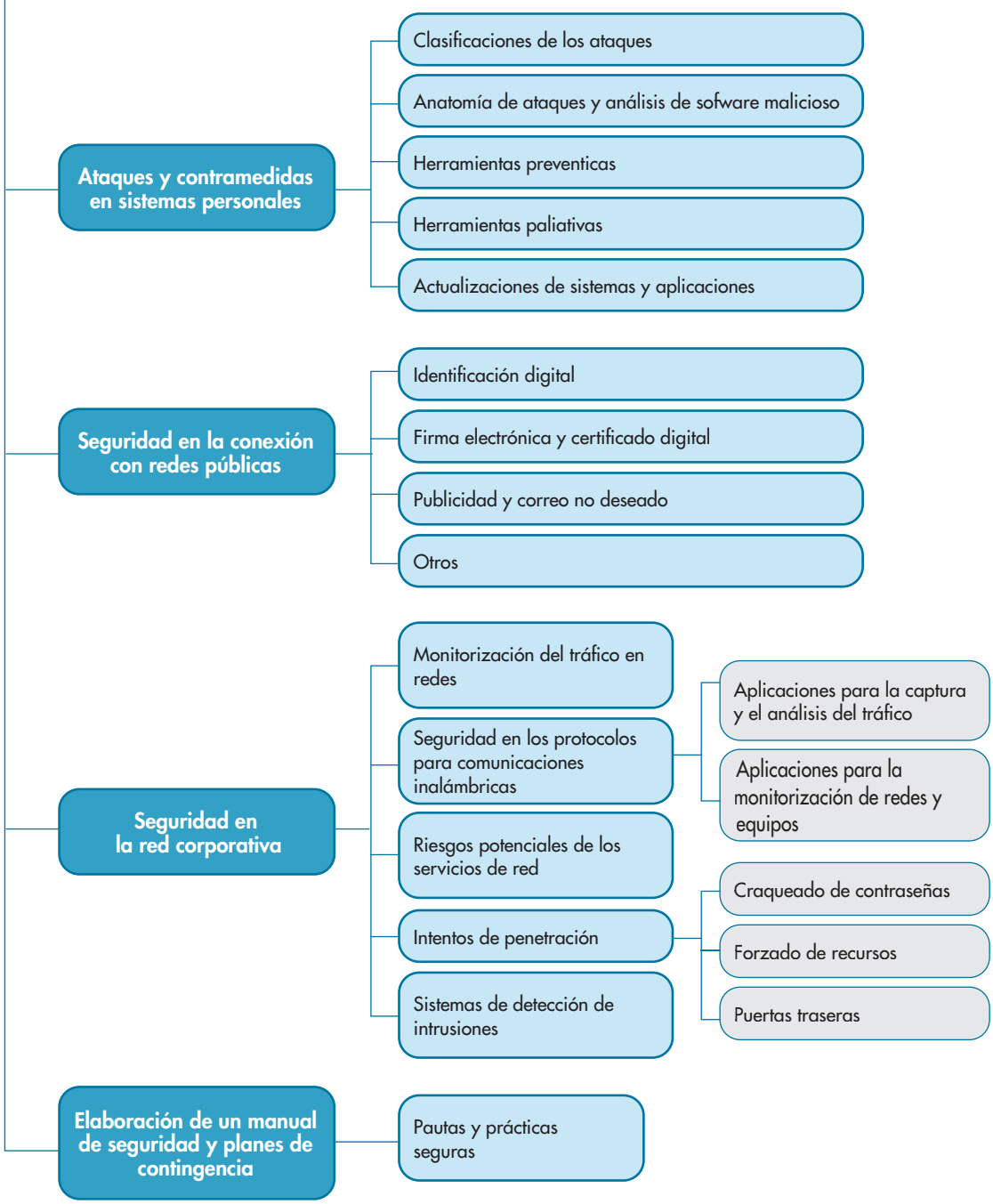
a) Clasifica los principales tipos de amenazas lógicas contra un sistema informático.
b) Verifica el origen y la autenticidad de las aplicaciones instaladas en un equipo, así como el estado de actualización del sistema operativo.
c) Identifica la anatomía de los ataques más habituales, así como las medidas preventivas y paliativas disponibles.
d) Analiza diversos tipos de amenazas, ataques y software malicioso, en entornos de ejecución controlados.
e) Implanta aplicaciones específicas para la detección de amenazas y la eliminación de software malicioso.
f) Utiliza técnicas de cifrado, firmas y certificados digitales en un entorno de trabajo basado en el uso de redes públicas.
g) Evalúa las medidas de seguridad de los protocolos usados en redes inalámbricas.
h) Reconoce la necesidad de inventariar y controlar los servicios de red que se ejecutan en un sistema.
i) Describe los tipos y características de los sistemas de detección de intrusiones.

Objetivos de Desarrollo Sostenible

En este capítulo se va a trabajar el ODS 9.

MAPA CONCEPTUAL

IMPLANTACIÓN DE MECANISMOS DE SEGURIDAD ACTIVA



GLOSARIO

Ataque de fuerza bruta. Método de ataque que intenta todas las combinaciones posibles de una contraseña hasta encontrar la correcta.

***Backdoor* (puerta trasera).** Método de acceso no autorizado al sistema que evade medidas de seguridad convencionales.

***Botnet*.** Red de dispositivos y sistemas conectados a Internet que se utilizan para realizar ataques distribuidos, enviar *spam* y robar datos.

Cortafuegos. Sistema que regula el tráfico de red entrante y saliente según reglas de seguridad predefinidas.

IDS (sistema de detección de intrusiones). Herramienta que monitoriza la red o sistemas para detectar actividades sospechosas.

***Malware*.** Software malicioso diseñado para dañar o infiltrarse en sistemas.

***Pentesting* (pruebas de penetración).** Análisis de seguridad que busca vulnerabilidades en sistemas y redes simulando ataques.

***Phishing*.** Tipo de ataque en el que el atacante se hace pasar por una entidad confiable para obtener información sensible.

***Proxy*.** Servidor que actúa como intermediario entre el usuario y el servidor destino para filtrar el tráfico.

PUNTO DE PARTIDA

Implantación de seguridad activa en TechGuard

La empresa TechGuard ha experimentado un aumento en incidentes relacionados con ataques dirigidos a sistemas personales y en conexiones inseguras en redes públicas. Los fallos en la actualización de sistemas, la configuración inadecuada de herramientas preventivas y paliativas, y la falta de un manual de seguridad han provocado vulnerabilidades críticas. Ante esta situación, se plantea la necesidad de implantar mecanismos de seguridad activa que garanticen la protección de la información y optimicen el funcionamiento operativo.

La dinámica será la siguiente:

- *Reflexión individual:* cada alumno identificará qué tipos de ataques (como *phishing*, *malware* o intentos de intrusión) pueden afectar los sistemas personales y las redes, y reflexionará sobre las contramedidas que se podrían implementar.
- *Investigación inicial:* se investigará en fuentes especializadas sobre la clasificación de ataques, la anatomía de los mismos y las herramientas tecnológicas disponibles para prevenir y paliar incidencias, así como la importancia de actualizar sistemas y aplicaciones.

– *Debate en grupo:* se organizará un debate para compartir hallazgos y discutir la eficacia de las diferentes herramientas preventivas y paliativas, considerando casos reales y analizando las mejores prácticas en la elaboración de manuales y planes de contingencia.

2.1. Introducción

En este capítulo se estudiarán las medidas de seguridad activa que se pueden implementar para proteger sistemas personales y redes frente a amenazas y ataques informáticos. Los estudiantes aprenderán tanto a identificar y clasificar los tipos de ataques más comunes como a implementar herramientas de protección y mitigación, así como a gestionar actualizaciones y configurar el acceso seguro a redes públicas. Además, se abordarán conceptos clave para la creación de manuales de seguridad y planes de contingencia, esenciales para mantener la integridad y disponibilidad de los sistemas.

2.2. Ataques y contramedidas en sistemas personales

Para asegurar un sistema informático personal, es imprescindible comprender los tipos de ataques que pueden comprometer su seguridad. Esta sección analizará la clasificación de los ataques, los métodos comunes y las herramientas para prevenir y mitigar posibles vulnerabilidades.

2.2.1. Clasificación de los ataques

Existen diversas formas de clasificar los ataques, pero generalmente se dividen en:

– *Ataques de ingeniería social*. Son métodos de manipulación psicológica que buscan obtener acceso o información mediante el engaño. Ejemplos comunes incluyen *phishing*, *vishing* y ataques de tipo *baiting*.
– *Ataques de malware.* Consisten en la utilización de software malicioso para dañar o tomar el control del sistema de un usuario. Incluyen virus, gusanos, troyanos, *ransomware* y *spyware.*
– *Ataques de fuerza bruta y craqueo de contraseñas.* Implican la utilización de herramientas automatizadas para descifrar contraseñas mediante pruebas exhaustivas. Son comunes en ataques de red y en sistemas que no han implementado restricciones de intentos fallidos y autenticación multifactor. Ejemplos son los ataques con diccionario o ataques al hash de la contraseña.
– *Ataques de denegación de servicio (DoS) y distribuidos (DDoS).* Consisten en saturar un sistema o red con tráfico innecesario hasta que sus recursos se agotan, volviéndolo inaccesible para usuarios legítimos (figura 2.1).
– *Ataques de interceptación (Man-in-the-Middle, MitM; en castellano, hombre en el medio).* En estos, el atacante intercepta y potencialmente altera la comunicación entre dos partes sin que estas lo sepan.

ACTIVIDAD PROPUESTA 2.1

Investiga tres ejemplos reales de cada uno de los tipos de ataques descritos en este apartado. Explica cómo afectaron a las víctimas y con qué herramientas y protocolos se podrían haber prevenido.

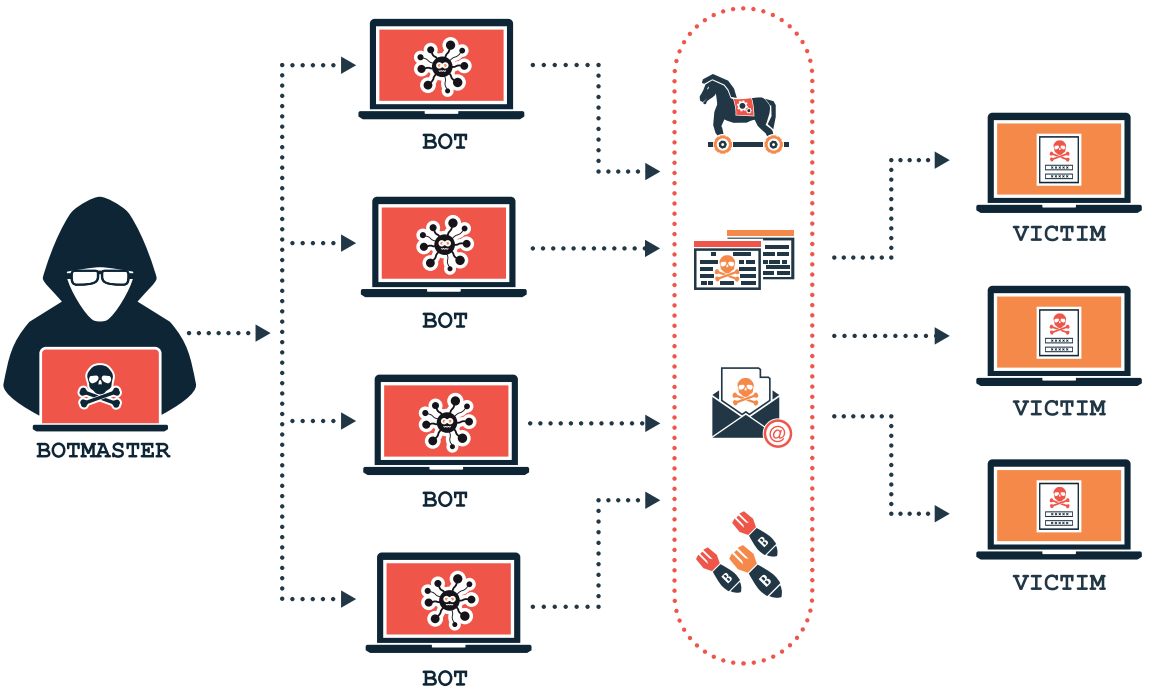


Figura 2.1. Diagrama de funcionamiento de un ataque DDoS desde una *botnet*.

2.2.2. Anatomía de ataques y análisis de software malicioso

Cuando un sistema es atacado con *malware*, suele suceder lo siguiente:

1. *Infección inicial*. El *malware* entra en el sistema, ya sea mediante un archivo adjunto en un correo, un enlace malicioso o la descarga de un archivo comprometido.
2. *Expansión*. Una vez dentro, el *malware* intenta extenderse dentro del sistema o hacia otros dispositivos conectados en la red. Los gusanos, por ejemplo, se replican y diseminan automáticamente.
3. *Ejecución de la carga útil*. En esta fase, el *malware* realiza la acción maliciosa para la cual fue diseñado, ya sea cifrar archivos (en caso de *ransomware*), robar datos o espiar las actividades del usuario.
4. *Evasión y persistencia*. Muchos tipos de *malware* incluyen mecanismos para evitar la detección y mantenerse activos incluso después de que el sistema sea reiniciado.

ACTIVIDAD PROPUESTA 2.2

Realiza un análisis básico de *malware* utilizando una herramienta como VirusTotal para examinar un archivo sospechoso. Describe los resultados y las clasificaciones de riesgo que da la herramienta.

2.2.3. Herramientas preventivas

Para prevenir ataques en sistemas personales, existen herramientas de seguridad que permiten reducir el riesgo de infección y la posibilidad de accesos no autorizados. A continuación, se detallan algunas de las herramientas más importantes y sus configuraciones en distintos sistemas operativos.

a) Instalación y configuración en Windows:

- *Antivirus y antimalware.* Windows cuenta con Windows Defender, pero es recomendable complementarlo con herramientas como Malwarebytes. Se deben configurar para realizar análisis periódicos y activar el escudo en tiempo real.
- *Firewall (cortafuegos).* Windows integra un *firewall* que debe estar activo en todo momento. En la configuración avanzada se pueden definir reglas específicas para el tráfico entrante y saliente.
- *Actualizaciones automáticas.* Es fundamental que Windows Update esté activo para asegurar que el sistema siempre tenga los últimos parches de seguridad.

b) Instalación y configuración en Linux:

- *ClamAV.* En Linux, ClamAV es un antivirus que ofrece una buena protección. Aunque los ataques de virus son menos comunes, su uso sigue siendo recomendado en entornos multiusuario.
- *Firewall (cortafuegos).* Iptables permite definir reglas de cortafuegos personalizadas para bloquear puertos y proteger servicios. También se puede utilizar `ufw` (*uncomplicated firewall*, en castellano, cortafugos 'descomplicado') o su versión con interfaz gráfica, `gufw`.
- *SELinux/AppArmor.* Ambas son herramientas de seguridad que añaden capas de control sobre las aplicaciones que se ejecutan en el sistema, limitando los permisos.

ACTIVIDAD RESUELTA 2.1

Configura un servidor web con ufw que permita tráfico HTTP (puerto 80) y HTTPS (puerto 443), pero bloquee todo el tráfico no autorizado.

Solución:

Paso	Comando
Habilitar UFW	`sudo ufw enable`
Permitir puertos HTTP y HTTPS	`sudo ufw allow 80` `sudo ufw allow 443`
Permitir SSH desde una IP específica (por seguridad)	`sudo ufw allow from 192.168.1.10 to any port 22`
Verificar la configuración	`sudo ufw status`
Bloquear todo el tráfico restante	`sudo ufw default deny incoming`

c) Instalación y configuración en macOs:

- *XProtect*. Es el antivirus integrado en macOs, que se actualiza automáticamente y protege contra amenazas conocidas.
- *Firewall (cortafuegos)*. En las opciones de seguridad y privacidad, se puede activar el *firewall* y definir permisos para aplicaciones específicas.
- *Gatekeeper*. Este sistema evita la ejecución de aplicaciones de desarrolladores no autorizados, minimizando el riesgo de instalar software malicioso.

ACTIVIDAD PROPUESTA 2.3

Configura el *firewall* en cada uno de los sistemas operativos mencionados que tengas disponibles y establece reglas para bloquear el tráfico entrante desde puertos no seguros. Al terminar, documenta los pasos realizados.

2.2.4. Herramientas paliativas

Las herramientas paliativas son aquellas que ayudan a reducir el impacto de un ataque una vez que este ya se ha producido. Aunque no previenen el ataque inicial, permiten mitigar el daño y facilitar la recuperación del sistema. Por ejemplo, una de las medidas es guardar copias de datos importantes siguiendo la regla de 3, 2, 1 (figura 2.2).

a) Herramientas paliativas en Windows:

- *Restauración del sistema*. Permite recuperar el estado del sistema a un punto anterior a la infección o problema.

- *Copia de seguridad* (backup). Windows incluye la posibilidad de hacer copias de seguridad automáticas de archivos importantes, así como copias de imagen del sistema para restauración completa.
- *Herramientas de diagnóstico.* Utilidades como el Visor de eventos ayudan a identificar posibles fuentes de problemas y rastrear actividades sospechosas.

b) Herramientas paliativas en Linux:

- *Backup (rsync).* Rsync permite sincronizar y realizar copias de seguridad de los archivos importantes en diferentes ubicaciones, facilitando la recuperación tras un ataque.
- *Logs del sistema.* En Linux, los registros se encuentran en la carpeta /var/log, y su análisis es esencial para entender cómo se produjo el ataque y qué áreas fueron comprometidas.
- *Chroot jail.* Chroot permite ejecutar aplicaciones en un entorno restringido, lo cual minimiza el daño que pueden causar al sistema en caso de infección.

c) Herramientas paliativas en macOs:

- *Time Machine.* Es la herramienta de *backup* de macOs, que permite restaurar archivos o todo el sistema a un estado previo.
- *Log console* (consola de registro). macOs tiene una consola de registro que ayuda a monitorear eventos y detectar actividades anómalas.
- *Modo seguro (Safe Boot).* Permite iniciar el sistema solo con los controladores básicos y ayuda a eliminar archivos maliciosos o a restaurar configuraciones.

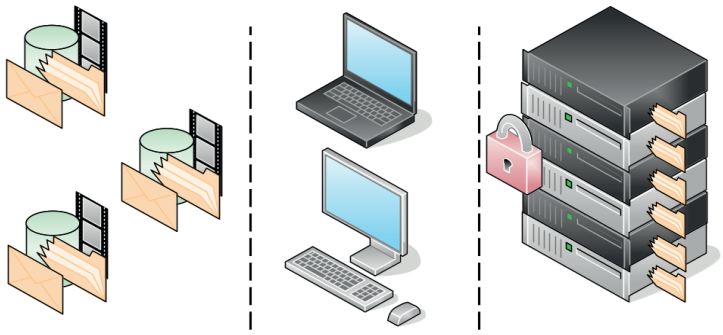


Figura 2.2. Representación de la regla de 3, 2, 1 aplicada al almacenamiento de datos.

ACTIVIDAD PROPUESTA 2.4

Configura y prueba una herramienta paliativa en cada sistema operativo que tengas al alcance. Simula una situación de recuperación y documenta el proceso.

2.2.5. Actualización de sistemas y aplicaciones

Mantener el sistema operativo y las aplicaciones actualizadas es una de las medidas de seguridad más efectivas contra vulnerabilidades conocidas. Las actualizaciones corrigen errores y fallos de seguridad que podrían ser explotados por atacantes.

- *Windows.* Las actualizaciones se gestionan desde Windows Update. Es recomendable activar las actualizaciones automáticas.
- *Linux*. Las distribuciones basadas en Debian, como Ubuntu, utilizan el gestor de paquetes apt o apt-get:

```
apt-get update && apt-get upgrade -y
```

  Otras distribuciones usan herramientas como yum o dnf.
- *macOs.* Las actualizaciones se gestionan a través de la App Store o el panel de preferencias del sistema. Se recomienda mantener las actualizaciones automáticas activas.

ACTIVIDAD PROPUESTA 2.5

Realiza una actualización completa del sistema operativo y una aplicación en cada plataforma disponible. Verifica que la actualización ha corregido vulnerabilidades conocidas y documentar el proceso.

2.3. Seguridad en la conexión con redes públicas

En este apartado se explorarán los riesgos y las medidas de seguridad al conectarse a redes públicas. Las redes públicas, como las de cafeterías, aeropuertos o centros comerciales, suelen ser menos seguras que las privadas, ya que están disponibles para cualquiera y no siempre cuentan con una protección adecuada. Esto convierte a los usuarios en posibles blancos de atacantes. Veremos los conceptos de identificación digital, firma electrónica y certificado digital, y abordaremos prácticas seguras para evitar el correo no deseado, publicidad no solicitada y otras amenazas.

2.3.1. Identificación digital

La identificación digital permite verificar la identidad de un usuario o sistema en línea. Este proceso es fundamental para autenticar conexiones, validar permisos de acceso y proteger datos personales.

Los métodos más comunes de identificación digital son los siguientes:

- *Autenticación basada en contraseñas.* El método más común, aunque menos seguro. Los usuarios deben utilizar contraseñas robustas y cambiarlas periódicamente.
- *Autenticación multifactor* (MFA). Incluye un segundo método de verificación, como un código enviado por SMS o la sincronización con una aplicación.
- *Certificados digitales.* Son documentos electrónicos que validan la identidad del usuario o sistema. Funcionan con un par de claves, una pública y otra privada, y son emitidos por una autoridad de certificación (CA). (Se amplía este concepto en los apartados 2.3.2 y 3.4.2).

ACTIVIDAD PROPUESTA 2.6

Configura una MFA en una cuenta personal de correo electrónico y documenta el proceso. ¿Cómo mejora esta medida la seguridad de la cuenta frente a ataques?

Estas son las acciones para la implementación de una identificación segura:

- Configurar contraseñas fuertes que combinen letras, números y caracteres especiales.
- Activar la autenticación multifactor cuando sea posible, especialmente en cuentas de correo electrónico y aplicaciones bancarias.
- Usar un gestor de contraseñas cifrado para almacenar de manera segura todas las credenciales de acceso.

SABÍAS QUE...

La ONU planteó los Objetivos de Desarrollo Sostenible en 2015 con la intención de que todos los países diesen pasos en la erradicación de la pobreza, el crecimiento económico y la protección del medio ambiente. Entre estos objetivos está el ODS 9: Industria, innovación e infraestructuras, que busca mejorar la capacidad tecnológica y el acceso a las tecnologías de la información de los sectores industriales, especialmente en los países en desarrollo. Para ello, las medidas de seguridad para acceder a redes públicas son fundamentales.

2.3.2. Firma electrónica y certificado digital

La firma electrónica y el certificado digital son componentes esenciales de la seguridad en línea, ya que permiten validar la identidad y la integridad de los documentos.

- *Firma electrónica.* Es un conjunto de datos que se añaden a un documento para identificar al firmante y garantizar que no ha sido modificado. Existen varios niveles de firma electrónica, desde la simple (sin validación) hasta la cualificada (verificada por una entidad acreditada).

Es muy útil en transacciones comerciales y firmas de documentos oficiales, con la Administración, en el entorno digital.

– *Certificado digital*. Un certificado digital es emitido por una CA (autoridad de certificación), que verifica la identidad del titular y genera una clave criptográfica única para ese usuario o empresa.

Los certificados digitales son usados tanto en sitios web (indicados por el protocolo HTTPS) como en la firma de documentos y correos electrónicos.

ACTIVIDAD PROPUESTA 2.7

La Administración pública española utiliza el certificado FNMT (Fábrica Nacional de Moneda y Timbre) para la identificación de personas y la firma de documentos oficiales en línea (figura 2.3). El uso de este certificado permite realizar trámites como la declaración de impuestos de manera segura.

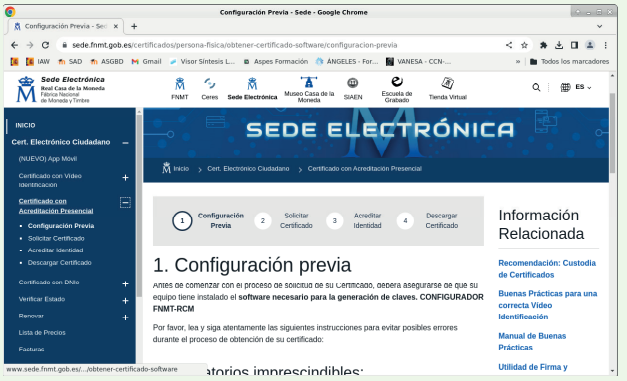


Figura 2.3. Página web de la FNMT sobre la configuración previa sobre el certificado ciudadano.

Investiga los pasos para obtener un certificado digital en el sitio web de la FNMT (Fábrica Nacional de Moneda y Timbre) y lista los documentos necesarios. Explora las aplicaciones prácticas de dicho certificado en la vida cotidiana.

2.3.3. Publicidad y correo no deseado

La publicidad y el correo no deseado (*spam*) representan una amenaza para la seguridad del usuario. El correo no deseado es a menudo el medio por el cual los atacantes difunden *malware*, lanzan campañas de *phishing* o recolectan información de los usuarios (figura 2.4).

Las amenazas más comunes en la publicidad y el correo no deseado son:

– *Phishing*. Suplantación de identidad mediante correos fraudulentos que buscan obtener información personal o financiera.

- *Malware oculto en enlaces o archivos adjuntos.* Muchas veces, los correos no deseados contienen archivos que infectan el sistema al abrirlos.
- *Recolección de datos.* Los atacantes pueden usar formularios o enlaces engañosos para recopilar datos de los usuarios.

Las contramedidas y buenas prácticas para evitarlos son las siguientes:

- *Filtros de correo.* Configurar filtros antispam en el cliente de correo o en el servidor.
- *Evitar abrir correos de remitentes desconocidos*. Es recomendable no abrir correos, especialmente aquellos que contienen enlaces o adjuntos, de remitentes desconocidos.
- *Navegación segura*. Evitar hacer clic en enlaces de sitios poco confiables y mantener siempre actualizado el navegador y el sistema operativo.

Figura 2.4. Amenazas en la publicidad y el *spam.*

CASO PRÁCTICO 2.1

Supón que trabajas en el departamento de seguridad de una empresa y te llega la petición de otro empleado para que le configures los filtros de su correo electrónico para reducir la cantidad de correos no deseados en la bandeja de entrada. Escribe un mail en el que expliques el proceso que tiene que hacer para diferentes servicios de mensajería y explícale cuál es el impacto de esta medida en su seguridad personal.

2.3.4. Otros

Además de las amenazas ya mencionadas, existen otras prácticas y precauciones a tener en cuenta cuando se navega en redes públicas:

1. *Evitar realizar transacciones sensibles.* Al conectarse a una red pública, es preferible no realizar transacciones bancarias ni introducir información personal sensible.
2. *Uso de VPN.* Una red privada virtual (*Virtual Private Network*, VPN) cifra la conexión entre el usuario y el servidor, lo cual aumenta la seguridad al ocultar la actividad en línea y proteger la privacidad del usuario.

3. *Desactivar el uso compartido de archivos.* Cuando se usa una red pública, desactivar las funciones de compartición de archivos y acceso remoto reduce la exposición a ataques.
4. *Configuración de* firewall. Configurar el *firewall* en el sistema operativo para restringir el tráfico entrante y evitar accesos no autorizados.

ACTIVIDAD PROPUESTA 2.8

Instala y configura una VPN en un dispositivo personal. Analiza cómo el uso de una VPN contribuye a proteger la conexión en una red pública. Si no te es posible utilizar una VPN, documenta el proceso de cómo se llevaría a cabo la instalación y la configuración.

2.4. Elaboración de un manual de seguridad y planes de contingencia

La creación de un manual de seguridad es esencial para establecer pautas y prácticas que minimicen el riesgo de incidentes. Un plan de contingencia, por su parte, es un protocolo que permite actuar rápidamente ante un incidente de seguridad para minimizar el impacto en el sistema (figura 2.5).

Un manual de seguridad debe incluir los siguientes contenidos:

1. *Definición de objetivos y alcance.* Es fundamental delimitar también las áreas de aplicación y los roles de cada usuario.
2. *Medidas preventivas.* Estas incluyen la implementación de contraseñas robustas, el uso de autenticación multifactor, y la capacitación continua en prácticas de seguridad para los usuarios.
3. *Procedimientos ante incidentes.* Debe definir claramente incluso los contactos de emergencia y las responsabilidades de cada miembro del equipo.
4. *Plan de recuperación*. Es crucial definir los pasos para restablecer el sistema y asegurar la integridad de los datos tras un incidente. Esto incluye el uso de copias de seguridad y herramientas de recuperación de sistemas.

En los cuadros 2.1 y 2.2 tienes unos ejemplos de un manual de seguridad y de un plan de contingencia.

CASO PRÁCTICO 2.2

Desarrolla el borrador de un plan de contingencia para una pequeña empresa. Incluye en él los pasos que habrá que seguir en el caso de una infección por *malware* y los métodos para restaurar la operación normal.

Cuadro 2.1. Ejemplo de manual de seguridad

1. Objetivos y alcance	Objetivo principal	Garantizar la protección de la información sensible y la disponibilidad de los sistemas informáticos de la empresa.
	Alcance	Este manual se aplica a todos los sistemas, redes, dispositivos y usuarios de la empresa, incluyendo empleados, proveedores y colaboradores externos. Cada usuario tiene roles y niveles de acceso que determinan sus responsabilidades dentro del sistema.
2. Medidas preventivas	Contraseñas robustas	Todas las contraseñas deben tener al menos 12 caracteres y combinar letras mayúsculas, minúsculas, números y caracteres especiales. Se requiere cambiar las contraseñas cada 90 días.
	Autenticación multifactor (MFA)	Para todos los accesos remotos y sistemas críticos se implementa MFA, que añade una segunda capa de seguridad mediante un código enviado al dispositivo móvil del usuario.
	Control de acceso	Se emplea una política de listas blancas, donde únicamente se permite la ejecución de aplicaciones aprobadas y verificada la autenticidad de cada una.
	Capacitación continua	Todos los empleados deben completar un curso anual de concienciación en ciberseguridad, que cubre temas como el reconocimiento de correos de *phishing* y la importancia de no compartir credenciales.
3. Procedimientos ante incidentes	Identificación de incidentes	Todo incidente debe ser informado inmediatamente al responsable de seguridad de la información (RSI), quien evaluará el impacto y la naturaleza del problema.
	Notificación de emergencia	En caso de brecha de seguridad, se debe comunicar a todos los afectados (usuarios y departamentos) siguiendo el protocolo establecido. Las notificaciones se envían mediante un sistema de alerta y correo electrónico.
	Aislamiento de sistemas comprometidos	El RSI puede decidir aislar sistemas afectados de la red para contener el incidente.
	Registro de eventos	Se documenta cada incidente en el registro de seguridad, detallando el tipo de amenaza, su origen, las medidas de contención adoptadas y los posibles efectos.
4. Plan de recuperación	Restauración de sistemas	Una vez resuelto el incidente, los administradores seguirán el proceso de restauración mediante las copias de seguridad más recientes, asegurándose de que la integridad de los datos no se haya visto comprometida.
	Verificación de integridad	Todo sistema restaurado se somete a un análisis de integridad para asegurar que no existan elementos residuales de software malicioso.
	Evaluación post-incidente	Tras la recuperación, el equipo de seguridad realiza una evaluación detallada del incidente para mejorar los procedimientos preventivos y documentar las lecciones aprendidas.

Cuadro 2.2. Ejemplo de plan de contingencia

1. Evaluación de riesgos	Análisis de sistemas críticos	Se identifican los sistemas esenciales para la continuidad operativa de la empresa, como el servidor de archivos, el servidor de aplicaciones y el sistema de gestión de clientes.
	Evaluación de amenazas potenciales	Incluye amenazas físicas (incendios, inundaciones) y amenazas lógicas (ataques de *malware*, suplantación de identidad y fallos de hardware).
2. Plan de acción ante incidentes de seguridad	Paso 1: Identificación del incidente	Ante cualquier anomalía, el personal de soporte debe investigar inmediatamente la causa del problema.
	Paso 2: Aislamiento del problema.	Se desconectan los sistemas comprometidos para evitar la propagación del problema.
	Paso 3: Comunicación	El equipo de seguridad informa a todos los departamentos relevantes y a los directivos sobre el incidente y las medidas que se están tomando.
3. Procedimiento de recuperación	Copias de seguridad	Las copias de seguridad completas del sistema se realizan diariamente y se almacenan en un servidor remoto y seguro.
	Restauración de sistemas	En caso de pérdida de datos, se emplean las copias de seguridad para restaurar la última versión válida del sistema. Se priorizan los sistemas críticos para reducir al mínimo la interrupción de la actividad.
	Verificación de sistemas restaurados	Tras restaurar los sistemas, se verifica que los datos restaurados estén completos y libres de *malware* antes de reanudar las operaciones.
4. Revisión y mejora del plan	Cada incidente debe ser revisado, y el plan de contingencia actualizado para integrar mejoras basadas en las lecciones aprendidas y las nuevas amenazas identificadas en el entorno de seguridad.	

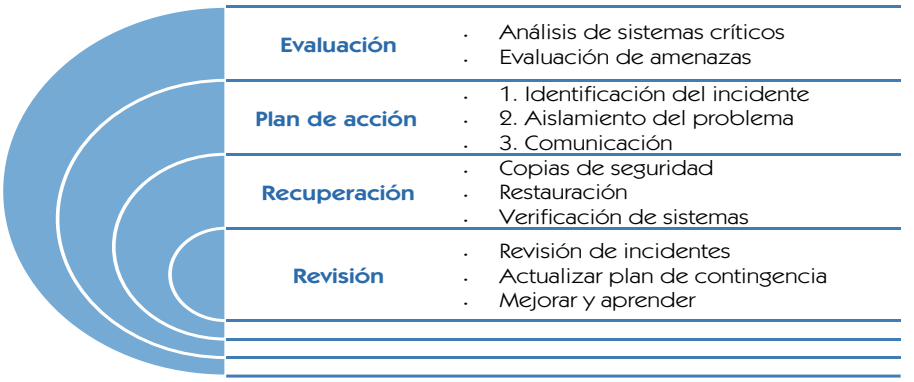


Figura 2.5. Claves del plan de contingencia.

2.5. Seguridad en la red corporativa

La seguridad en la red corporativa es un pilar fundamental en la protección de los sistemas informáticos de una organización (figura 2.6). Dado que en un entorno corporativo existen múltiples dispositivos conectados y un tráfico de datos constante, las vulnerabilidades pueden aumentar considerablemente. En esta sección, veremos cómo proteger y monitorizar el tráfico en redes, asegurar los protocolos de comunicación inalámbrica, identificar riesgos en los servicios de red, y estudiar los sistemas de detección de intrusiones.

Figura 2.6. NOC, *Network Operation Center*, centro de operaciones de red con las pantallas que monitorizan la red.

2.5.1. Monitorización del tráfico en redes

La monitorización del tráfico en redes permite detectar patrones sospechosos o intrusiones. Es un paso clave para garantizar que la información que circula por la red está protegida y para responder rápidamente ante posibles amenazas.

A) Aplicaciones para la captura y análisis del tráfico

La captura de tráfico consiste en recolectar datos que circulan por la red para analizarlos y detectar posibles irregularidades. Este proceso requiere de aplicaciones especializadas que pueden instalarse en diferentes sistemas operativos.

- *En Windows.* Una de las herramientas más utilizadas es Wireshark, un analizador de paquetes que permite ver todo el tráfico que circula en la red. Este programa es ideal para identificar problemas de red o ataques sospechosos.
- *En Linux*. Linux cuenta con herramientas potentes como `tcpdump` y `nmap`, además de Wireshark que cuenta con GUI. Tcpdump captura paquetes y permite realizar análisis detallados, mientras que Nmap escanea puertos y proporciona información sobre el tráfico y posibles vulnerabilidades (figura 2.7).
- *En macOs.* Wireshark también está disponible para macOs y es una opción preferida en este sistema. Además, Little Snitch es una herramienta popular que permite monitorear las conexiones entrantes y salientes en tiempo real.

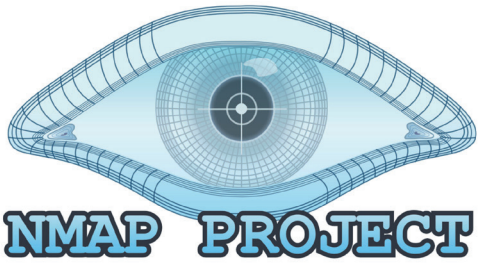


Figura 2.7. Logo de la aplicación Nmap, Nmap Project®.

ACTIVIDAD RESUELTA 2.2

Analiza el tráfico HTTP (puerto 80) en la interfaz eth0, capturando solo 20 paquetes y guardando la captura en un archivo para su análisis posterior.

Solución:

Paso	Comando
Capturar el tráfico en tiempo real	`sudo tcpdump -i eth0 port 80 -c 20 -w http_trafico.pcap`
Analizar el archivo guardado.	`sudo tcpdump -r http_trafico.pcap`
Filtrar tráfico HTTP con detalles adicionales (en hexadecimal y ASCII)	`sudo tcpdump -i eth0 port 80 -X -c 10`

ACTIVIDAD RESUELTA 2.3

Realiza un escaneo completo con nmap de un servidor en la red local para identificar servicios, versiones y posibles vulnerabilidades en los puertos comunes.

Solución:

Paso	Comando
Realizar un escaneo rápido de los puertos más comunes.	`nmap -F 192.168.1.1`
Escanear todos los puertos en el host para identificar posibles servicios adicionales.	`nmap -p- 192.168.1.1`
Obtener información detallada de los servicios y versiones en los puertos abiertos.	`nmap -sV 192.168.1.1`
Detectar el sistema operativo del servidor.	`nmap -O 192.168.1.1`
Realizar un escaneo intensivo y guardar los resultados en un archivo para su análisis.	`nmap -A -oN escaneo_intensivo.txt 192.168.1.1`

B) Aplicaciones para la monitorización de redes y equipos

La monitorización de redes y equipos permite obtener información en tiempo real sobre el estado de la infraestructura, facilitando la detección y resolución de problemas.

– *En Windows.* PRTG Network Monitor es una aplicación que permite monitorear el tráfico de red, servidores, dispositivos y aplicaciones. Se usa para generar informes detallados y alertas en caso de actividad inusual.