TEMA 1: SEGURIDAD INFORMÁTICA

1. LA SEGURIDAD INFORMÁTICA

La seguridad informática intenta proteger el almacenamiento, procesamiento y transmisión de información digital.

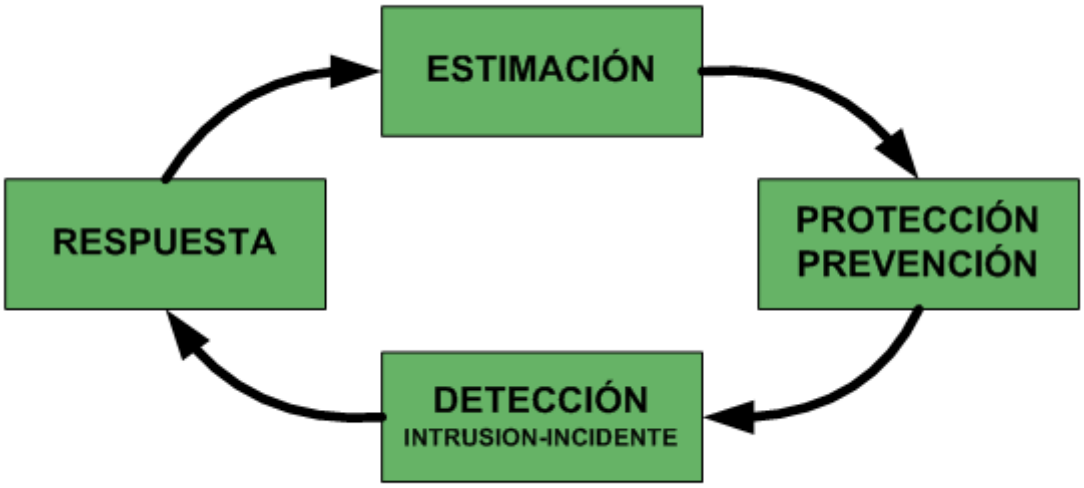
Medidas adoptadas para evitar el uso no autorizado, el mal uso, la modificación o la denegación del uso de conocimiento, hechos, datos o capacidades.

1.1 ¿QUE ES LA SEGURIDAD INFORMÁTICA?

La seguridad es el proceso consistente en mantener un nivel aceptable de riesgo percibido.

La seguridad es un proceso, no un estado final. Este proceso es cíclico y nos lleva por las siguientes etapas:

Estimación
Protección o **prevención**
Detección (intrusión, incidente)
Respuesta (parchear y continuar, perseguir y denunciar,…)



La seguridad es el proceso de mantener un nivel aceptable de riesgo percibido; se trata de un proceso y no de un estado.

1.2 ¿QUE ES EL RIESGO?

El riesgo es la posibilidad de sufrir daños o perdidas, una medida del peligro que corre un bien.

Riesgo = Amenaza * Vulnerabilidad * Valor del bien

El eslabón más débil en la seguridad son las personas.

El riesgo aumenta con el aumento del de cualquiera de estos parámetros. Si alguno de los parámetros (amenazas, vulnerabilidades, valor del bien) es muy alto el riesgo será muy alto.

Si conseguimos reducir mucho alguno o varios de estos parámetros el riesgo será muy bajo.

La seguridad completa es imposible, independientemente de la preocupación y el presupuesto; debemos desplegar la máxima seguridad posible con el presupuesto y la formación de los técnicos de los que disponemos.

AMENAZA

Alguien que tiene la capacidad de intención de aprovechar una vulnerabilidad de un cierto bien.

Amenazas no estructuradas

Amenazas estructuradas (organizadas, metódicas, dirigidas, concretas, subvencionadas, motivadas)

Análisis de amenazas: Estima las interacciones y capacidades de las amenazas.

VULNERABILIDAD

Debilidad de un bien que podría dar lugar a su explotación. Las vulnerabilidades llegan a los bienes a través de un diseño, implementación o mantenimiento deficientes.

Defecto que puede ser aprovechado por el atacante. **Malware**: programa que se aprovecha de un defecto para tomar el control de la máquina (**Exploit**) para los fines del atacante.

Vulnerabilidades reconocidas corregidas con un parche por el fabricante.
Vulnerabilidades reconocidas pero sin parche o con una solución “temporal” por parte del fabricante.
Vulnerabilidades no reconocidas o no conocidas por el fabricante.

VALOR DEL BIEN

Es una medida del tiempo y recursos necesarios para reemplazar un bien o para devolverle su estado anterior.

¿Qué protegemos? Equipos, aplicaciones y datos (almacenados y durante la comunicación). Equipos, aplicaciones, datos y comunicaciones.

1.3 HERRAMIENTAS Y TÉCNICAS DE SEGURIDAD

Es obvio que nadie puede depender de un solo tipo de seguridad para proteger la información de una organización. Tampoco puede confiar en un solo producto para proporcionar toda la seguridad a su computadora y a sus sistemas de red.

Los siguientes son algunos ejemplos de **herramientas** o **técnicas** que potencian o mejoran la seguridad informática en una organización.

SOFTWARE ANTIVIRUS

CONTROLES DE ACCESO

Debemos estar muy seguros de la identidad de la persona o sistema que desea acceder a nuestra información. Podemos clasificar las medidas de control de acceso según el sistema **Sabes – Tienes – Eres** (Algo que sabes, algo que tienes, algo que eres), la autenticación será mas fiable cuantos mas elementos utilice.

MUROS DE FUEGO – CORTAFUEGOS – FIREWALL

Dispositivos de control de acceso para la red que pueden ayudar a proteger la red interna de una organización contra ataques externos.
Productos de seguridad de frontera, lo cual significa que están en el límite entre la red interna y la red externa.

TARJETAS INTELIGENTES

La autenticación o validación de un individuo puede llevarse a cabo utilizando una combinación de algo que usted conoce, algo que usted tiene o algo que usted es.
Las tarjetas inteligentes (algo que usted tiene) pueden ser utilizadas para la autenticación y así pueden disminuir el riesgo de que alguien adivine la contraseña.
Ejemplo: tarjetas del banco.

BIOMÉTRICA

Cada método suele requerir de algún tipo de dispositivo para identificar las características humanas. Suelen ser dispositivos bastante sofisticados para detectar intentos de simulación.

- Huellas digitales
- Retina/iris
- Huellas de las palmas
- Geometría de las manos
- Geometría facial
- Voz

DETECCIÓN DE INTRUSIONES (IDS)

Idealmente no sería necesario proteger nuestros sistemas, podríamos identificar cuando alguien estuviese haciendo algo incorrecto y detenerlo.

ADMINISTRACIÓN DE POLÍTICAS

Política de copia de seguridad
Auditoría de seguridad internas y externas
Política de contraseñas y control de acceso
Planes de contingencia ante catastrofes
Monitorización y auditoría del sistema
Formación
Estándares y cumplimiento de la normativa (ISO/IEC 27002:2009)
Pruebas de carga
Alta disponibilidad

EXPLORACIÓN DE VULNERABILIDADES

Ayuda a una organización a identificar los puntos de entrada potenciales para los intrusos.
Deben implementarse medidas de seguridad inmediatamente después de identificar cada punto vulnerable.

CRIPTOGRAFÍA

Es el mecanismo principal para la seguridad de las comunicaciones.
Es un buen método para proteger la información en tránsito.
La criptografía puede proteger información que se encuentre almacenada mediante el cifrado de archivos.

MECANISMOS DE SEGURIDAD FÍSICA

Los empleados deben tener acceso a las computadoras y a la información para que la organización funcione.
Los mecanismos de seguridad física que se pueden poner en marcha deben permitir que algunas personas tengan acceso.
Normalmente los sistemas están conectados a la red, por tanto pueden sufrir ataques sin un acceso físico a las instalaciones.

2. OBJETIVOS DE LA SEGURIDAD INFORMÁTICA – SERVICIOS PROPORCIONADOS POR LA SEGURIDAD INFORMÁTICA

Seguridad informática:
Medidas adoptadas para evitar el uso no autorizado, el mal uso, la modificación o la denegación del uso de conocimiento, hechos, datos o capacidades.

2.1 CONFIDENCIALIDAD

Capacidad de garantizar que la información, almacenada en el sistema informático o transmitida por la red, solamente va a estar disponible para aquellas personas autorizadas a acceder a dicha información, es decir, que si los contenidos cayesen en manos ajenas, estas no podrían acceder a la información o a su interpretación.

Autenticación: Intenta confirmar que una persona o máquina es quien dice ser, que no es un impostor.
Autorización: Una vez autenticado, los distintos usuarios de la información tendrán distintos privilegios sobre ella (solo lectura o lectura y modificación).
Cifrado: La información está cifrada para que no pueda ser útil para cualquiera que no supere la autenticación.
Protocolos AAA: Protocolos que ofrecen servicios de Autenticación, Autorización y Contabilización (Authentication, Authorization and Accounting en inglés).

2.1 DISPONIBILIDAD

Capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario con normalidad en el horario establecido.

2.1 INTEGRIDAD

Capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización. La información de la que disponemos es válida y consistente. Garantiza que los datos no han sido modificados sin el consentimiento de su propietario.

2.1 RESPONSABILIDAD – NO REPUDIO

Garantiza la identidad del autor de un documento digital y garantiza la participación de las partes en una comunicación, intenta evitar que cualquiera de ellas pueda negar la participación en esa relación. En toda comunicación existe un emisor y un receptor, por lo que podemos distinguir dos tipos de no repudio o responsabilidad:

(Identidad del emisor)No repudio de origen: garantiza que la persona que envía el mensaje no puede negar que es el emisor del mismo, ya que el receptor tendrá pruebas del envío.
(Identidad del receptor) No repudio de destino: El receptor no puede negar que recibió el mensaje, porque el emisor tiene pruebas de la recepción del mismo.
(Identidad del autor) Autoría: garantiza la identidad del autor de un contenido digital

3. PRINCIPIOS BÁSICOS DE SEGURIDAD

Conocer la forma en la que trabajan los hackers nos ayuda a prevenir y evitar sus ataques.

3.1 CARACTERÍSTICAS DE UN INTRUSO

ALGUNOS INTRUSOS SON MÁS LISTOS QUE NOSOTROS
MUCHOS INTRUSOS SON IMPREDECIBLES
LA PREVENCIÓN FRACASA EVENTUALMENTE

Si al menos algunos de los intrusos son más listos que nosotros, y no se puede predecir lo que harán, entonces van a encontrar alguna forma de atravesar nuestras defensas.

Este principio no significa que deban abandonarse los esfuerzos de prevención.

La prevención es un componente necesario, aunque no suficiente de la seguridad.

3.2 LAS FASES DE UN COMPROMISO

Si deseamos detectar las intrusiones, debemos comprender las acciones necesarias para comprometer un objetivo.

RECONOCIMIENTO
Proceso de validar la conectividad, enumerar los servicios y buscar aplicaciones vulnerables.

EXPLOTACIÓN
Abusar de los servicios de un blanco, subvertirlos o dañarlos.
Los abusos de servicio implican hacer uso ilegítimo de un modo legítimo de acceso.

REFUERZO
Se aprovecha del modo inicial de acceso no autorizado con objeto de ganar capacidades adicionales en el blanco.

CONSOLIDACIÓN
Se produce cuando el intruso se comunica con el servidor de la víctima a través de la puerta trasera (Ej. Un servicio de escucha al que se conecta el intruso).

PILLAJE
Ejecución del plan final del intruso (robo de información privada, construir una base para un ataque mas profundo dentro de la organización o cualquier otra cosa que desee el intruso).

3.3 REDES DEFENDIBLES

La **NSM Monitorización de Seguridad de Redes** es la recolección, análisis y notificaciones de indicaciones y advertencias con objeto de detectar entradas y responder a ellas.
La seguridad es el proceso de mantener un nivel aceptable de riesgo percibido; se trata de un proceso y no de un estado.
El riesgo es la posibilidad de sufrir daños o perdidas, una medida del peligro que corre un bien.
Para minimizar el riesgo, los defensores tienen que estas siempre vigilantes, implementando procedimientos de estimación, detección y respuesta.
Implementar con éxito un proceso de seguridad requiere mantener una red que pueda ser defendida.

Empresas propugnan la autodefensa digital basándose en los siguientes criterios:

LAS REDES DEFENDIBLES SE PUEDEN VIGILAR
Monitorizar.
Observar el tráfico que atraviesa las redes de la empresa.

LAS REDES DEFENDIBLES LIMITAN LA CAPACIDAD DE MANIOBRA DE LOS INTRUSOS

LAS REDES DEFENDIBLES OFRECEN UN NÚMERO MÍNIMO DE SERVICIOS
Siempre que sea posible despliegue sistemas operativos que permitan instalaciones mínimas.

LAS REDES DEFENDIBLES SE PUEDEN MANTENER ACTUALIZADAS

3.4 ATAQUES Y ATACANTES

3.4.1 TIPOS DE ATAQUES

ROBO, INUNDACIÓN, INCENDIO, DESASTRE...
INTERRUPCIÓN
INTERCEPTACIÓN
FABRICACIÓN
INGENIERÍA SOCIAL
PHISHING
KEYLOGERS
STEALERS
FUERZA BRUTA
POR DICCIONARIO
SPOOFING
SNIFFING
DoS – DENEGACIÓN DE SERVICIO
DDoS – DENEGACIÓN DE SERVICIO DISTRIBUIDO
VIRUS

GUSANOS
TROYANOS
BACKDOOR – PUERTA TRASERA
DRIVE-BY DOWNLOADS
ROOTKITS
HIJACKERS
BOTNETS – ZOMBIES
ROGUE SOFTWARE
RANSOMWARE – CRIPTOVIRUS – SECUESTRADORES
ADWARE
DIALERS
SPYWARE

3.4.2 TIPOS DE ATACANTES Y LOS BUENOS

HACKER: Expertos informáticos con curiosidad por conocer vulnerabilidades de los sistemas informáticos.
CRACKER
PHEAKERS
SCRIPT KIDDIE – LAMMERS
PROGRAMADORES DE MALWARE – PROGRAMADORES DE VIRUS
SNIFFERS
CARDERS
CIBERTERRORISTA

ANALISTA DE SEGURIDAD - TÉCNICO DE SISTEMAS: Expertos informáticos con curiosidad por conocer vulnerabilidades de los sistemas informáticos y corregirlas.

4. CLASIFICACIÓN DE LAS SEGURIDAD INFORMÁTICA

Es posible que muchas de las herramientas y técnicas de seguridad no se ajusten claramente a la clasificación siguiente, en ese caso las clasificaremos como “mixtas”.Herramientas o técnicas que implementan seguridad física y lógica o seguridad activa y pasiva a la vez.

4.1 SEGURIDAD FÍSICA Y LÓGICA

Tipos de seguridad en función del recurso que protegemos.

4.1.1 SEGURIDAD FÍSICA

La seguridad física es aquella que trata de **proteger el hardware** (los equipos informáticos, el cableado...) de los posibles desastres naturales (terremotos, tifones...), de incendios, inundaciones, sobrecargas eléctricas, robos,...

Posibles amenazas al hardware:

Incendios
Inundaciones
Robos
Señales electromagnéticas
Apagones
Sobrecargas eléctricas
Desastres naturales

4.1.2 SEGURIDAD LÓGICA

La seguridad lógica protege el software de los equipos informáticos, es decir, las aplicaciones y los datos de usuario, de robos, de perdida de datos, entrada de virus informáticos, modificaciones no autorizadas de los datos, ataques desde la red...

Posibles amenazas al software:

Robo
Pérdida de información
Pérdida de integridad en la información
Entrada de virus
Ataques desde la red
Modificaciones no autorizadas

Comprobación de la integridad de los ficheros del sistema:

Para un buen funcionamiento de nuestro sistema operativo resulta conveniente verificar periódicamente la integridad de los archivos de sistema. En Windows se nos simplifica la labor utilizando desde el menú Inicio/Ejecutar el comando ***sfc /scannow***. Se nos abrirá la ventana "Protección de archivos de Windows" y verificará que los archivos protegidos de nuestro sistema se encuentran intactos y en sus versiones originales.

Pendiente Linux?

4.2 SEGURIDAD ACTIVA Y PASIVA

El criterio de clasificación es el momento en el que se ponen en marcha las medidas de seguridad.

4.2.1 SEGURIDAD ACTIVA

La seguridad activa la podemos definir como el conjunto de medidas que previenen e intentan evitar los daños en los sistemas informáticos.

Uso de contraseñas
Listas de control de acceso
Cifrado
Uso de software de seguridad informática
Firmas y certificados digitales
Sistemas de ficheros con tolerancia a fallos
Cuotas de disco

4.2.1 SEGURIDAD PASIVA

La seguridad pasiva complementa a la seguridad activa y se encarga de minimizar los efectos que haya ocasionado algún percance.

Conjunto de discos redundantes
SAI
Realización de copias de seguridad

4.3 ALTA DISPONIBILIDAD

Alta disponibilidad (High Availability) es la capacidad de que aplicaciones y datos se encuentre operativos para los usuarios autorizados en todo momento 24 * 7 (o en el horario acordado) y **sin interrupciones**, debido principalmente a su carácter crítico.

Tipo de interrupciones:

Previstas: se realizan cuando paralizamos el sistema para realizar cambios o mejoras en nuestro hardware o software

Imprevistas: suceden por acontecimientos imprevistos (apagón, error de hardware/software, problemas de seguridad, desastre natural, virus,...)

ENLACES INTERESANTES - BIBLIOGRAFÍA

Seguridad informática (Wikipedia)

Alta disponibilidad (Wikipedia)

Intypedia – Information security encyclopedia

OSI – Oficina de Seguridad del Internauta

INCIBE – Instituto Nacional de Ciberseguridad

"Fundamentos de seguridad de redes" – Eric Maiwald – Editorial Mc Graw Hill – ISBN 970-10-4624-2

"El Tao de la monitorización de seguridad en redes – Richard Bejtlich – Editorial Pearson Educación – ISBN 84-205-4600-3

"Seguridad informática – Jose Fabián Roa Buendía – Editorial Mc Graw Hill – ISBN 978-84-481-8396-7

(Entretenimiento) Chema Alonso hacker y cómico

EJERCICIOS

1. Explica los **servicios que proporciona la seguridad informática**. Nombra dos técnicas de seguridad que proporcionan cada uno de los servicios,

2. Explica los **servicios que ofrece la seguridad informática**.

3. Explica para que sirve la **seguridad informática**.

4. Define el concepto de **riesgo de un sistema informático**, cuáles son los aspectos que influyen en el aumento del riesgo percibido de un sistema informático.

5. Explica la relación entre la **seguridad informática** y el **riesgo** de un sistema informático.

6. Explica el concepto de **confidencialidad** como servicio de la seguridad informática y, en tu opinión, cuáles son la técnicas de seguridad informática mas adecuadas para garantizar la confidencialidad de los datos de un sistema informático.

7. Explica el concepto de **disponibilidad** como servicio de la seguridad informática y, en tu opinión, cuáles son la técnicas de seguridad informática mas adecuadas para garantizar la disponibilidad de un sistema informático.

8. Explica el concepto de **integridad** como servicio de la seguridad informática y, en tu opinión, cuáles son la técnicas de seguridad informática mas adecuadas para garantizar la integridad de los datos de un sistema informático.

9. Explica el concepto de **responsabilidad** como servicio de la seguridad informática y, en tu opinión, cuáles son la técnicas de seguridad informática mas adecuadas para garantizar la responsabilidad en un sistema informático.

10. Explica la diferencia entre **Vulnerabilidad** y **Amenaza** en un sistema informático.

11. Explica en que consiste el concepto de **Alta Disponibilidad (High Availability)** en seguridad informática.

12. Enumera y describe las **características de una red defendible** (Red de Área Local – LAN).

13. Explica las **fases de un compromiso (ataque) a un sistema informático**.

14. Describe el concepto de **seguridad pasiva** de un sistema informático. Describe dos herramientas o técnicas de seguridad pasiva que conozcas explicando sus características y en qué condiciones debemos utilizarlos.

15. Explica dos **técnicas o herramientas de seguridad pasiva** que consideres importantes.

16. Describe el concepto de **seguridad activa** de un sistema informático. Describe dos herramientas o técnicas de seguridad pasiva que conozcas explicando sus características y en qué condiciones debemos utilizarlos.

17. Explica dos **técnicas o herramientas de seguridad activa** que consideres importantes.

18. Describe el concepto de **seguridad física** de un sistema informático. Describe dos herramientas o técnicas de seguridad pasiva que conozcas explicando sus características y en qué condiciones debemos utilizarlos.

19. Explica dos **técnicas o herramientas de seguridad física** que consideres importantes.

20. Describe el concepto de **seguridad lógica** de un sistema informático. Describe dos herramientas o técnicas de seguridad pasiva que conozcas explicando sus características y en qué condiciones debemos utilizarlos.

21. Explica dos **técnicas o herramientas de seguridad lógica** que consideres importantes.

22. Explica todas las **técnicas de seguridad activa** que implementarías en la red local de una pequeña empresa (dos servidores, 5 puestos clientes y una conexión ADSL a Internet).

23. Explica todas las **técnicas de seguridad pasiva** que implementarías en la red local de una pequeña empresa (dos servidores, 5 puestos clientes y una conexión ADSL a Internet).

24. Explica todas las **técnicas de seguridad física** que implementarías en la red local de una pequeña empresa (dos servidores, 5 puestos clientes y una conexión ADSL a Internet).

25. Explica todas las **técnicas de seguridad lógica** que implementarías en la red local de una pequeña empresa (dos servidores, 5 puestos clientes y una conexión ADSL a Internet).

26. Explica la diferencia entre **seguridad física y seguridad lógica** poniendo además 2 ejemplos de herramientas de cada uno de estos tipos de seguridad informática.

27. Explica la diferencia entre **seguridad activa y seguridad pasiva** poniendo además 2 ejemplos de herramientas de cada uno de estos tipos de seguridad informática.

28. Describe cinco **técnicas de seguridad** que consideres imprescindibles en un equipo que va a utilizar una persona en su casa con conexión a Internet a través de una linea ADSL (**Configuración de seguridad para un hogar**). Indica cuales técnicas son imprescindibles y cuales opcionales.

29. Describe **cinco técnicas de seguridad** que consideres **imprescindibles para una empresa pequeña** (5 empleados con un ordenador cada uno , un servidor y una red local conectada a Internet con un router ADSL) (Configuración de seguridad para una pequeña empresa). Indica cuales técnicas son imprescindibles y cuales opcionales.

30. Analiza la **red Wi-Fi de tu casa** y valora las técnicas de seguridad que tienes implementadas y los problemas de seguridad que has sufrido.

31. Analiza y comenta los **recursos compartidos disponibles en la red** de tu casa entre los dispositivos conectados a esta red.

32. Localiza y visita las siguientes web´s:

INCIBE: Instituto Nacional de Ciberseguridad

OSI: Oficina de Seguridad del Internauta

33. Diccionario de seguridad:

Seguridad informática
Riesgo
Amenaza
    Amenazas físicas: atacan al hardware.
    Amenazas lógicas: atacan a los programas.
    Amenazas que atacan a los datos y las comunicaciones:
        Interrupción
        Interceptación
        Modificación
        Fabricación
Ataque
Impacto
Vulnerabilidad
Día cero
Tiempo de reacción
Hacker
Intruso
Confidencialidad
Integridad
Disponibilidad
High Avability – Alta Disponibilidad
Responsabilidad
No repudio
Fiabilidad
Autenticación
Cifrar
Descifrar
Criptografía
Cifrado Simétrico
Cifrado Asimétrico
Certificado de seguridad
Autoridad de certificación
Firma digital
Firma electrónica – DNI electrónico
ACL – Lista de Control de Acceso
Password – política de contraseñas – complejidad de la contraseña
Fuerza bruta – fortaleza de una contraseña
Rainbow Table
CPD
SAI
Grupo electrógeno
Sistema biométrico de identificación
IDS
Firewall – Cortafuegos
Proxy
Copia de seguridad
Completa
Diferencial
Incremental
Política de copia de seguridad
RAID
Imagen del sistema
Recuperación de datos
Análisis forense
Borrado seguro
Auditoría de seguridad
COBIT
ISO 27002
ISO 27001
Test de intrusión
Malware
Ingeniería social
Ataque DoS – Denegación de Servidio
Ataque de modificación
Suplantación
Monitorización
Bug
Caballo de Troya – Troyano
Backdoors
Bomba lógica
Virus
Gusano
Spyware
Cookies
Parche – Actualización del software
Bot
Redes zombies: Botnet
Hackismo
Wikileaks
APT - Advanced Persistent Threat – Amenaza Persistente Avanzada
Stuxnet
Koobface
Administración remota segura

HTTPS	VLAN
SFTP	VPN
FTPS	WPA
SSL/TLS	Portal cautivo
IPSec	

Avanzado

34. Integridad de los archivos del sistema

35. Localiza y prueba un **escáner de vulnerabilidades del sistema**.

36. Localiza y prueba un **software de detección de intrusos en la red** (**NIDS**) para descubrir dispositivos conectados en tu misma red y los recursos compartidos e información que has podido obtener de estos dispositivos.