Glosario de Términos

Jesús Temprano Gallego

DAW2

Ultima revisión: 29/10/2025

Contenido

Amenazas

Cualquier situación, acción o evento que **pueda** causar daño a los sistemas, datos o redes de un equipo u organización.

Antimalware

Software diseñado para detectar, prevenir y eliminar programas maliciosos como virus, troyanos, spyware, ransomware, etc.

Antivirus

Tipo de antimalware especializado en detectar y eliminar virus informáticos, aunque muchos antivirus modernos también protegen contra otros tipos de malware.

Análisis forense

Proceso de investigar incidentes de seguridad en un equipo o red para identificar qué ocurrió, cómo ocurrió y quién fue responsable, preservando evidencia digital.

Auditoría

Revisión sistemática de sistemas, redes y procedimientos de seguridad para verificar que cumplan con normas, políticas y buenas prácticas.

Autenticación Multifactor (MFA)

Método de seguridad que requiere más de un tipo de verificación para acceder a un sistema, como una contraseña + código enviado al móvil.

Ciclo de vida de la información

Etapas por las que pasa la información desde que se crea hasta que se elimina, incluyendo creación, almacenamiento, uso, compartición, archivado y destrucción.

Ciclo de vida de un incidente: detección, análisis, contención, erradicación, recuperación y aprendizaje

Proceso que sigue un equipo de seguridad para manejar un incidente:

- **Detección**: Identificar que ha ocurrido un incidente.
- **Análisis**: Determinar la causa y el alcance del incidente.
- **Contención**: Limitar el daño y evitar que se propague.
- **Erradicación**: Eliminar la amenaza de los sistemas afectados.
- **Recuperación**: Restaurar los sistemas y datos a un estado normal.
- **Aprendizaje**: Revisar el incidente para mejorar la seguridad y prevenir futuros problemas.

Cifrar

Transformar datos en un formato ilegible para que solo puedan ser leídos por personas autorizadas usando claves de descifrado.

Confidencialidad

Principio de seguridad que asegura que la información solo sea accesible para quienes tienen autorización, evitando accesos no autorizados.

Cortafuegos

Dispositivo o software especializado en impedir la comunicación. Controla el tráfico de red entre diferentes redes, permitiendo o bloqueando el acceso según reglas de seguridad.

Cortafuegos: basados en red y cortafuegos basados en host

- **Basados en red**: Protegen toda una red, filtrando el tráfico que entra y sale a nivel de red.
- **Basados en host**: Protegen un equipo específico, controlando el tráfico hacia y desde ese equipo.

Cross-Site Scripting (XSS)

Vulnerabilidad de seguridad en aplicaciones web donde un atacante inserta código malicioso (normalmente JavaScript) que se ejecuta en el navegador de otros usuarios.

Datos sensibles

Información que requiere protección especial porque su divulgación puede causar daño, como datos personales, financieros o de salud.

DDoS

Ataque que busca saturar un servidor o red enviando gran cantidad de tráfico desde múltiples equipos, provocando que deje de funcionar.

Diagnóstico de fallos

Proceso de identificar y analizar problemas en sistemas, redes o equipos para encontrar su causa y solucionarlos.

Disponibilidad

Principio de seguridad que garantiza que los sistemas, servicios y datos estén accesibles y operativos cuando los usuarios autorizados los necesiten.

DoS

Ataque que busca interrumpir el funcionamiento de un equipo o servicio enviando solicitudes excesivas desde un solo origen.

Esquema Nacional de Seguridad (ENS)

Conjunto de normas y medidas de seguridad que deben seguir las administraciones públicas en España para proteger la información y los sistemas.

Estrategias proactivas

Medidas de seguridad que se toman antes de que ocurra un incidente para prevenir ataques o problemas, como análisis de vulnerabilidades o actualizaciones periódicas.

Exploits

Programas o fragmentos de código que aprovechan vulnerabilidades en sistemas, aplicaciones o redes para realizar acciones no autorizadas.

Filtrado

Proceso de examinar y controlar el tráfico de red o información según ciertas reglas para permitir o bloquear el acceso.

Firewall

Sinónimo de cortafuegos; dispositivo o software que protege redes o equipos controlando el tráfico según reglas de seguridad.

IDS/IPS

- **IDS (Intrusion Detection System)**: Sistema que detecta actividades sospechosas o intrusiones en una red o equipo.
- **IPS (Intrusion Prevention System)**: Similar al IDS, pero además bloquea automáticamente las amenazas detectadas.

Incidentes de seguridad

Eventos que afectan la seguridad de la información o sistemas, como ataques, accesos no autorizados o fallos de software.

Indicadores de compromiso (IoC)

Señales o evidencias que indican que un sistema o red ha sido comprometido por un ataque o malware.

Integridad

Principio de seguridad que asegura que la información no sea alterada, modificada o destruida de forma no autorizada.

Inyección SQL

Vulnerabilidad donde un atacante inserta código SQL malicioso en una aplicación para acceder o manipular la base de datos sin permiso.

ISO/IEC 27001

Norma internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI) en una organización.

Man-in-the-Middle

Ataque en el que un atacante intercepta y, a veces, modifica la comunicación entre dos partes sin que ellas lo sepan.

Monitoreo

Supervisión continua de sistemas, redes o aplicaciones para detectar problemas, anomalías o posibles ataques.

Permisos

Derechos asignados a usuarios o programas que determinan qué acciones pueden realizar sobre archivos, carpetas o recursos del sistema.

Políticas de acceso

Conjunto de reglas que definen quién puede acceder a qué recursos, en qué condiciones y con qué nivel de privilegio.

Propuestas de mejora

Sugerencias o acciones planificadas para aumentar la seguridad, eficiencia o rendimiento de los sistemas informáticos.

Protocolos

Conjuntos de reglas que determinan cómo se comunican los dispositivos en una red (por ejemplo, HTTP, TCP/IP, FTP).

Proxy

Dispositivo o software especializado en mediar la comunicación entre un equipo y otro servidor o Internet. Recibe las solicitudes de un equipo y las envía al destino final, permitiendo controlar el tráfico, filtrar contenido y proteger la identidad del usuario.

Puertos

Puntos lógicos que permiten a un ordenador o servidor identificar y gestionar diferentes tipos de tráfico de red o servicios (por ejemplo, puerto 80 para HTTP).

Ransomware

Tipo de malware que bloquea o cifra los archivos de un equipo y exige un pago (rescate) para recuperarlos.

Registro de incidencias

Documento o sistema donde se anotan todos los incidentes de seguridad detectados, su causa, impacto y las acciones tomadas para resolverlos.

Reglamento General de Protección de Datos (RGPD)

Ley europea que protege los datos personales de los ciudadanos, regulando cómo las organizaciones pueden recopilarlos, usarlos y almacenarlos.

Reglas

Conjunto de condiciones o instrucciones que determinan cómo deben actuar los sistemas de seguridad, como cortafuegos o antivirus, para permitir o bloquear acciones.

Roles

Conjuntos de permisos o funciones asignados a un usuario dentro de un sistema, que determinan qué acciones puede realizar (por ejemplo, administrador, usuario, invitado).

Routers

Dispositivo o software especializados en comunicar. Dirigen el tráfico de datos entre diferentes redes, como entre una red local (LAN) y una conexión a Internet.

Vulnerabilidades

Fallos o debilidades en sistemas, programas o redes que pueden ser aprovechados por atacantes para causar daño o acceder sin permiso.