GLOSARIO DE CIBERSEGURIDAD

DAW2

CRISTIAN MATEOS VEGA

Contenido

- **Análisis Forense**
  Proceso de investigar incidentes de seguridad recopilando y analizando evidencias digitales de lo ocurrido. Incluye la preservación de pruebas, reconstrucción de eventos y generación de informes que pueden ser utilizados en procesos legales o internos.

- **Amenazas**
  Posibles peligros que pueden explotar vulnerabilidades para dañar sistemas, robar información, interrumpir servicios o comprometer la seguridad. Pueden ser internas (empleados malintencionados) o externas (hackers, malware).

- **Antimalware**
  Software diseñado para detectar, bloquear y eliminar programas maliciosos como virus, gusanos, troyanos, spyware, adware y ransomware. Suele incluir funciones de análisis en tiempo real y escaneo programado.

- **Antivirus**
  Tipo de antimalware enfocado en detectar y eliminar virus informáticos. También puede proteger contra otras amenazas si incluye funciones adicionales como protección web.

- **Auditoría**
  Revisión sistemática de sistemas, redes y procesos para evaluar su seguridad, cumplimiento normativo y eficiencia operativa. Puede ser interna o externa, y suele generar recomendaciones de mejora.

- **Autenticación Multifactor (MFA)**
  Método de verificación de identidad que requiere dos o más factores: algo que sabes (contraseña), algo que tienes (token, móvil) y algo que eres (huella digital, reconocimiento facial). Aumenta significativamente la seguridad frente a accesos no autorizados.

- **Ciclo de vida de la información**
  Etapas por las que pasa la información desde su creación hasta su eliminación segura. Incluye: creación, almacenamiento, uso, intercambio, archivo y destrucción. Cada etapa debe gestionarse con medidas de seguridad adecuadas.

- **Ciclo de vida de un incidente:**
  - **Detección**

    Identificación de una posible amenaza mediante alertas, monitoreo o reportes.
  - **Análisis**

    Evaluación del alcance, impacto y origen del incidente.
  - **Contención**

    Acciones inmediatas para limitar la propagación del daño.
  - **Erradicación**

    Eliminación completa de la amenaza y sus vectores de ataque.
  - **Recuperación**

    Restauración de sistemas y servicios afectados, asegurando su integridad.
  - **Aprendizaje**

    Documentación y análisis post-incidente para mejorar la respuesta futura y prevenir recurrencias.

- **Cifrar**
  Transformar datos en un formato ilegible mediante algoritmos criptográficos, de modo que solo puedan ser leídos por quienes posean la clave adecuada. Es esencial para proteger la confidencialidad en comunicaciones y almacenamiento.

- **Confidencialidad**
  Principio de seguridad que garantiza que la información solo sea accesible a personas autorizadas. Se logra mediante controles de acceso, cifrado y políticas de privacidad.

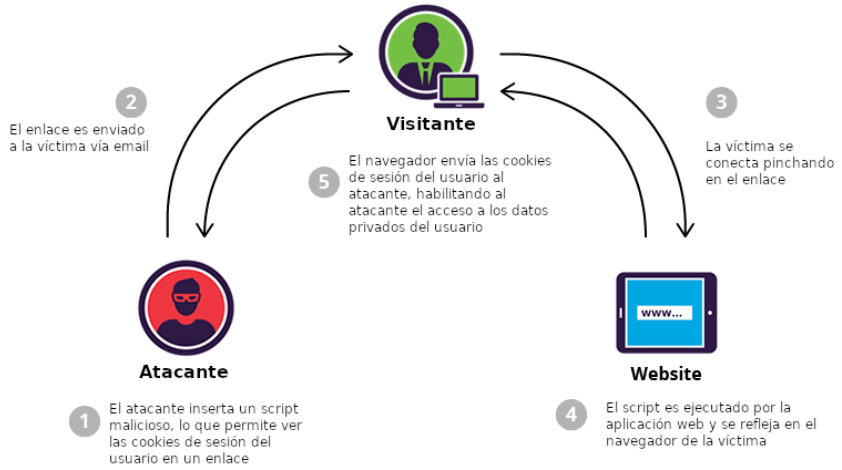
- **Cortafuegos**

  Software o hardware que controla el tráfico de red para bloquear accesos no autorizados y permitir comunicaciones legítimas. Actúa como una barrera entre redes internas y externas.

- **Cortafuegos basados en host**
  Instalados en dispositivos individuales para protegerlos de accesos no deseados.

- **Cortafuegos basados en red**
  Protegen una red completa, filtrando el tráfico entre segmentos o hacia Internet.

- **Cross-Site Scripting (XSS)**
  Ataque que inyecta scripts maliciosos en sitios web vulnerables. El código se ejecuta en el navegador de otros usuarios, permitiendo robo de cookies, redirecciones o manipulación de contenido.



- **Datos sensibles**
  Información confidencial que, si se divulga, puede causar perjuicios a individuos o entidades. Incluye contraseñas, datos bancarios, información médica, identificadores personales (como DNI o dirección), y secretos empresariales. Su protección es esencial para evitar fraudes, suplantación de identidad o pérdidas económicas.

- **DDoS**
  Ataque coordinado desde múltiples dispositivos que sobrecarga un servidor, red o servicio con tráfico masivo, provocando su caída o inaccesibilidad. Es común en sabotajes digitales y extorsiones.

- **Diagnóstico de fallos**
  Proceso técnico que busca identificar, analizar y documentar las causas de errores, fallos o comportamientos anómalos en sistemas informáticos. Es clave para la resolución de problemas y la mejora continua de la seguridad.

- **Disponibilidad**
  Principio de la seguridad informática que asegura que los sistemas, servicios y datos estén accesibles para los usuarios autorizados cuando los necesiten.

- **DoS**
  Ataque que busca interrumpir el funcionamiento normal de un sistema o red mediante el envío masivo de solicitudes desde una única fuente, provocando saturación y caída del servicio.

- **Esquema Nacional de Seguridad (ENS)**
  Marco regulatorio español que establece los principios, requisitos y medidas paragarantizar la protección de la información en el sector público y en entidades que colaboran con él. Incluye niveles de seguridad, auditorías y certificaciones.

- **Estrategias Proactivas**
  Conjunto de medidas anticipadas que buscan prevenir incidentes de seguridad antes de que ocurran. Incluyen análisis de riesgos, simulacros, formación, actualizaciones constantes y vigilancia activa.

- **Exploit**
  Fragmento de código o técnica que aprovecha una vulnerabilidad específica en software, hardware o sistemas para ejecutar acciones maliciosas, como obtener acceso no autorizado, escalar privilegios o ejecutar malware.

- **Filtrado de Puertos y Protocolos**
  Técnica de seguridad que regula el tráfico de red permitiendo o bloqueando el acceso a determinados puertos (como el 80 para HTTP) y protocolos (como TCP/IP), según políticas definidas. Es esencial en firewalls y routers.

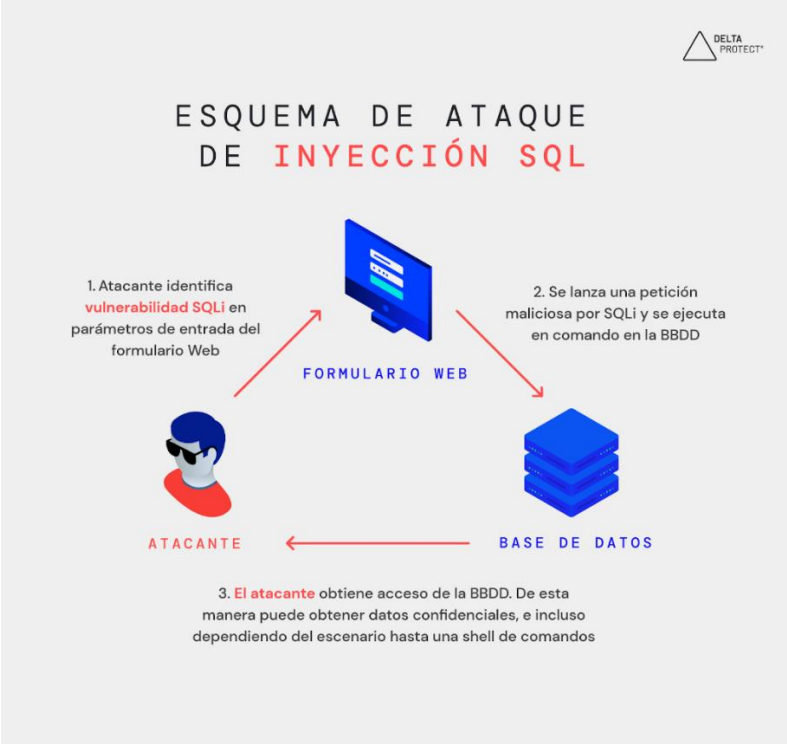
- **IDS/IPS**
  Sistemas que monitorizan el tráfico de red o actividad del sistema. IDS detecta y alerta sobre posibles intrusiones; IPS va un paso más allá y bloquea automáticamente el tráfico malicioso.

- **Incidentes de seguridad**
  Eventos que afectan negativamente la confidencialidad, integridad o disponibilidad de la información. Pueden incluir accesos no autorizados, pérdida de datos, infecciones por malware o ataques externos.

- **Indicadores de compromiso (IoC)**
  Rastros digitales que evidencian una posible intrusión o ataque. Incluyen direcciones IP sospechosas, cambios no autorizados en archivos, patrones de tráfico inusuales, o presencia de malware.

- **Ingeniería Social**
  Técnica de manipulación psicológica que busca engañar a personas para que revelen información confidencial o realicen acciones inseguras. Ejemplos comunes son el phishing o el baiting.

- **Inyección SQL**
  Ataque que consiste en insertar código SQL malicioso en formularios web o entradas de usuario para acceder, modificar o eliminar datos de una base de datos. Es una de las vulnerabilidades más comunes en aplicaciones web mal protegidas.



- **Integridad**
  Principio que garantiza que los datos no han sido modificados, alterados o destruidos de forma no autorizada. Es fundamental para asegurar la veracidad y fiabilidad de la información.

- **ISO/IEC 27001**
  Norma internacional que define los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Ayuda a proteger información mediante controles organizativos y técnicos.

- **Man-in-the-Middle**
  Ataque en el que un tercero intercepta la comunicación entre dos partes sin que estas lo sepan. Puede modificar, robar o redirigir la información transmitida. Es común en redes Wi-Fi públicas sin cifrado.

- **Monitoreo**
  Vigilancia continua de sistemas, redes y aplicaciones para detectar comportamientos anómalos, accesos no autorizados o fallos. Es clave para la detección temprana de amenazas y la respuesta rápida.

- **Permisos**
  Derechos asignados a usuarios o procesos para acceder, modificar o ejecutar recursos dentro de un sistema. Una gestión adecuada de permisos minimiza el riesgo de accesos indebidos.

- **Políticas de acceso**
  Conjunto de reglas que determinan quién puede acceder a qué recursos, en qué condiciones y con qué nivel de privilegio. Se basan en roles, horarios, ubicaciones, autenticación y otros factores.

- **Propuestas de mejora**
  Sugerencias técnicas u organizativas que buscan reforzar la postura de seguridad tras auditorías, análisis de riesgos o incidentes. Pueden incluir nuevas herramientas, formación, cambios en procesos o actualizaciones.

- **Ransomware**
  Tipo de malware que cifra los archivos de un sistema y exige un pago (rescate) para liberarlos. Puede propagarse por correos maliciosos, vulnerabilidades o descargas fraudulentas.

- **Reglas de Firewall**
  Conjunto de instrucciones que definen cómo debe actuar un cortafuegos ante diferentes tipos de tráfico. Permiten o bloquean conexiones según IP, puerto, protocolo, origen o destino.

- **Reglamento General de Protección de Datos**
  Ley europea que regula el tratamiento de datos personales, garantizando derechos como el consentimiento, el acceso, la rectificación y el olvido. Afecta a todas las entidades que gestionan datos de ciudadanos europeos.

- **Registro de Incidencias**
  Documento o sistema que recopila información detallada sobre incidentes de seguridad: fecha, tipo, impacto, respuesta aplicada y medidas correctivas. Es esencial para análisis forense y mejora continua.

- **Roles**
  Categorías que agrupan usuarios según sus funciones y responsabilidades. Cada rol tiene permisos específicos que definen qué acciones puede realizar dentro de un sistema (ej. administrador, auditor, usuario).

- **Routers**
  Dispositivos que conectan diferentes redes y dirigen el tráfico de datos entre ellas. También pueden incluir funciones de seguridad como NAT, firewall y VPN.

- **Vulnerabilidades**
  Debilidades en software, hardware o procesos que pueden ser explotadas por atacantes para comprometer la seguridad. Su gestión incluye identificación, evaluación, corrección y monitoreo.