**Malware**

Definición:

Conjunto de programas o códigos maliciosos cuyo objetivo es infiltrarse en un sistema informático para dañarlo, alterar su funcionamiento, robar información o dar acceso no autorizado al atacante. Incluye virus, gusanos, troyanos, ransomware, spyware, entre otros.

Noticia:

Interfaz de usuario gráfica

El contenido generado por IA puede ser incorrecto.

[Enlace](https://es.cointelegraph.com/news/modstealer-malware-crypto-wallets-fake-job-ads)

**Virus**

Definición:

Tipo de malware que se adhiere a programas o archivos legítimos y, al ser ejecutados, se replica e infecta otros archivos o sistemas. Suelen dañar datos, ralentizar equipos o incluso hacerlos inservibles. Requieren la acción del usuario (abrir un archivo, ejecutar un programa) para propagarse.

Noticia:

Diagrama

El contenido generado por IA puede ser incorrecto.

[Enlace](https://www.20minutos.es/tecnologia/ciberseguridad/malware-encontrado-77-apps-maliciosas-google-acaba-retirar_6239922_0.html)

**Gusanos**

Definición:

Malware autorreplicable que se propaga automáticamente a través de redes y dispositivos sin intervención del usuario. A diferencia de los virus, no necesitan un archivo anfitrión. Pueden saturar redes, consumir recursos y abrir puertas traseras para futuros ataques.

Noticia:

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

El contenido generado por IA puede ser incorrecto.

[Enlace](https://elpais.com/tecnologia/2009/01/19/actualidad/1232357280_850215.html)

**Troyanos**

Definición:

Programas que aparentan ser aplicaciones legítimas, pero contienen código malicioso. Suelen instalarse disfrazados de software útil o atractivo y, una vez dentro, permiten al atacante obtener acceso remoto, robar información o instalar más malware.

Noticia:



[Enlace](https://www.20minutos.es/tecnologia/ciberseguridad/nuevo-troyano-rat-on-transferencias-automaticas-dinero_6326216_0.html)

**Spyware**

Definición:

Software que recopila información del usuario sin su conocimiento ni consentimiento. Puede registrar hábitos de navegación, datos personales, contraseñas o información bancaria, transmitiéndola al atacante. Normalmente se instala junto a programas gratuitos o anuncios engañosos.

Noticia:



[Enlace](https://www.incibe.es/linea-de-ayuda-en-ciberseguridad/casos-reales/infeccion-por-spyware-en-una-guarderia-expone-datos-personales-de-menores)

**Adware**

Definición:

Aplicaciones que muestran publicidad invasiva en el dispositivo del usuario. Aunque no siempre son peligrosas, muchas veces recolectan datos de navegación o instalan anuncios no deseados, lo que compromete la privacidad y puede abrir la puerta a más malware.

Noticia:



[Enlace](https://www.europapress.es/portaltic/ciberseguridad/noticia-descubren-campana-adware-oculta-afecta-60000-aplicaciones-android-20230612173259.html)

**Ransomware**

Definición:

Tipo de malware que bloquea el acceso a los archivos o sistemas de la víctima mediante cifrado. Los atacantes exigen un rescate (normalmente en criptomonedas) para devolver el acceso. Es uno de los ataques más peligrosos y costosos para empresas y particulares.

Noticia:

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

[Enlace](https://www.splashtop.com/es/blog/the-5-most-devastating-ransomware-attacks-of-2021so-far)

**Phishing**

Definición:

Técnica de ingeniería social que consiste en enviar correos, mensajes o enlaces falsos que imitan a entidades legítimas (bancos, empresas, redes sociales) con el fin de engañar al usuario y robar credenciales, información bancaria o instalar malware.

Noticia:

Texto

El contenido generado por IA puede ser incorrecto.

[Enlace](https://www.lavelez.com.ar/technology/el-nuevo-ataque-de-phishing-apunta-a-los-usuarios-de-facebook-a-robar-credenciales-de-inicio-de-sesion/236362)

**Spear phishing**

Definición:

Variante del phishing más sofisticada, dirigida específicamente a una persona u organización. Se personaliza el mensaje (nombre, cargo, empresa) para aumentar las probabilidades de éxito del engaño.

Noticia:

Una captura de pantalla de un celular con texto e imagen

El contenido generado por IA puede ser incorrecto.

[Enlace](https://www.elconfidencial.com/tecnologia/2025-01-16/spear-phishing-expertos-seguridad-alertan-mensajes-fraudulentos-reales-1qrt_4044709)

**Whaling**

Definición:

Subtipo de spear phishing dirigido a altos ejecutivos o directivos de una empresa (“peces gordos”). El objetivo suele ser obtener información sensible de la compañía o autorización para transferencias de dinero.

Noticia:

Interfaz de usuario gráfica, Texto

El contenido generado por IA puede ser incorrecto.

[Enlace](https://enthec.com/whaling)

**Doxing**

Definición:

Práctica maliciosa que consiste en investigar, recopilar y difundir públicamente datos personales o privados de una persona sin su consentimiento. Suele usarse como forma de acoso o intimidación.

Noticia:

Interfaz de usuario gráfica, Texto

El contenido generado por IA puede ser incorrecto.

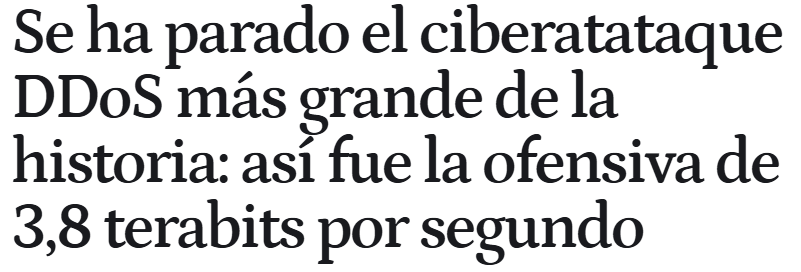
[Enlace](https://elpais.com/mexico/2024-02-27/que-es-el-doxing-la-violencia-digital-contra-las-candidatas-claudia-sheinbaum-y-xochitl-galvez.html)

**Ataques de denegación de servicio DoS y DDoS**

Definición:

Consisten en saturar un servidor, red o servicio con una avalancha de peticiones hasta hacerlo inaccesible para los usuarios legítimos. En el caso de los ataques DDoS, la sobrecarga proviene de múltiples dispositivos infectados en diferentes ubicaciones.

Noticia:



[Enlace](https://www.elespanol.com/omicrono/software/20241004/parado-ciberatataque-ddos-grande-historia-ofensiva-terabits-segundo/890911320_0.html)

**Man-in-the-middle**

Definición:

Ataque en el que el ciberdelincuente se coloca entre dos partes que se comunican (usuario y servidor, por ejemplo) para interceptar, espiar o modificar la información sin que ninguna de las dos lo detecte. Es común en redes Wi-Fi públicas inseguras.

Noticia:



[Enlace](https://cadenaser.com/castillayleon/2025/07/24/la-policia-nacional-ha-identificado-a-los-autores-de-una-estafa-man-in-the-middle-radio-palencia)

**Spoofing**

Definición:

Suplantación de identidad digital. El atacante falsifica direcciones IP, correos electrónicos, páginas web o identidades para hacerse pasar por una fuente confiable y engañar a la víctima.

Noticia:

Texto

El contenido generado por IA puede ser incorrecto.

[Enlace](https://www.libertaddigital.com/ciencia-tecnologia/internet/2025-06-12/la-policia-advierte-del-spoofing-la-nueva-estafa-telefonica-con-la-que-pueden-vaciarte-la-cuenta-bancaria-en-minutos-7263966)

**Sniffing**

Definición:

Técnica que consiste en interceptar y analizar el tráfico de red para capturar información sensible, como contraseñas, correos o datos bancarios. Se realiza con herramientas llamadas *sniffers* y suele aprovechar redes sin cifrado.

Noticia:

Texto

El contenido generado por IA puede ser incorrecto.

[Enlace](https://cybersecuritynews.es/que-es-y-como-protegerse-de-un-ataque-de-sniffing)

**Inyección SQL**

Definición:

Vulnerabilidad que ocurre cuando una aplicación web no valida correctamente las entradas del usuario. El atacante puede insertar comandos SQL maliciosos en formularios o URLs para acceder, modificar o eliminar datos de la base de datos.

Noticia:

Imagen que contiene Texto

El contenido generado por IA puede ser incorrecto.

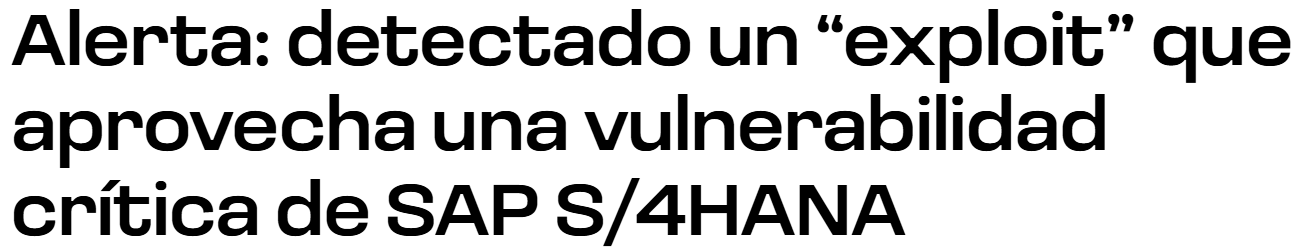
[Enlace](https://www.europapress.es/portaltic/ciberseguridad/noticia-identifican-vulnerabilidad-grave-inyeccion-sql-complemento-wp-automatic-wordpress-20240426114224.html)

**Exploit de vulnerabilidades**

Definición:

Programas o técnicas que aprovechan fallos o errores de seguridad en sistemas operativos, aplicaciones o dispositivos para obtener acceso no autorizado, elevar privilegios o ejecutar código malicioso.

Noticia:



[Enlace](https://www.computerworld.es/article/4052127/alerta-detectado-un-exploit-que-aprovecha-una-vulnerabilidad-critica-de-sap-s-4hana.html)

**Zero-day exploits**

Definición:

Exploits que atacan vulnerabilidades recién descubiertas y que todavía no han sido corregidas por el fabricante. Son especialmente peligrosos porque no existen parches ni defensas inmediatas contra ellos.

Noticia:

Texto

El contenido generado por IA puede ser incorrecto.

[Enlace](https://www.welivesecurity.com/es/investigaciones/vulnerabilidad-zero-day-winrar-explotada-activamente)

**Botnets**

Definición:

Redes de computadoras, servidores o dispositivos IoT infectados con malware y controlados de forma remota por un atacante. Se usan para enviar spam, lanzar ataques DDoS o distribuir más malware de manera masiva.

Noticia:

Texto

El contenido generado por IA puede ser incorrecto.

[Enlace](https://www.welivesecurity.com/es/investigaciones/vulnerabilidad-zero-day-winrar-explotada-activamente)

**Keylogger**

Definición:

Programa o dispositivo que registra en secreto todas las teclas que pulsa un usuario. Se usa para robar contraseñas, mensajes o cualquier dato que se escriba en el teclado.

Noticia:

Imagen que contiene Texto

El contenido generado por IA puede ser incorrecto.

[Enlace](https://www.incibe.es/empresas/blog/cuidado-keylogger-podria-estar-registrando-tus-contrasenas)

**CryptoJacking**

Definición:

Uso no autorizado de la capacidad de procesamiento de un dispositivo para minar criptomonedas en beneficio del atacante. Suele ejecutarse en segundo plano, ralentizando el sistema y aumentando el consumo eléctrico.

Noticia:

Enlace

**Clickjacking**

Definición:

Ataque en el que se manipula la interfaz de una página web para que el usuario haga clic en botones ocultos o disfrazados. Así, puede autorizar transferencias, activar la cámara o instalar malware sin darse cuenta.

Noticia:

Enlace

**Drive-by-attack**

Definición:

Infección que se produce automáticamente al visitar una página web comprometida. El usuario no necesita hacer clic ni descargar nada; basta con acceder a la web para que se instale el malware.

Noticia:

Enlace

**Pharming**

Definición:

Manipulación de sistemas DNS o configuraciones de red para redirigir al usuario a páginas falsas, aunque escriba la dirección correcta. Se utiliza para robar credenciales bancarias o información personal.

Noticia:

Enlace

**Ataque de ingeniería social**

Definición:

Conjunto de técnicas que manipulan psicológicamente a las personas para que revelen información confidencial, den acceso a sistemas o realicen acciones inseguras. Ejemplo: llamadas de falsos técnicos de soporte.

Noticia:

Enlace

**Ataque aplicaciones móviles**

Definición:

Explotación de vulnerabilidades en apps de smartphones o tablets. Pueden incluir malware oculto en aplicaciones, robo de datos personales, acceso a la cámara o el micrófono, o control remoto del dispositivo.

Noticia:

Enlace

**ACTIVIDAD 2 DEFINICIONES**

**1. Encriptación**

Proceso que transforma datos legibles (texto plano) en un formato ilegible (texto cifrado) mediante algoritmos matemáticos y una clave. Su objetivo es proteger la confidencialidad de la información para que solo pueda ser entendida por quien posea la clave correcta para descifrarla.

* **AES (Advanced Encryption Standard):** Algoritmo de cifrado simétrico muy usado en discos duros y comunicaciones.
* **RSA:** Cifrado asimétrico utilizado para proteger claves y datos en HTTPS.
* **Signal Protocol:** Protocolo de cifrado de extremo a extremo usado en apps como WhatsApp y Signal.

**2. Firmas y certificados digitales**

* **Firma digital:** mecanismo criptográfico que garantiza que un mensaje o archivo no ha sido alterado y que proviene realmente del remitente. Funciona usando claves privadas para firmar y claves públicas para verificar la autenticidad.
* **Certificado digital:** documento electrónico emitido por una Autoridad de Certificación (CA) que asocia una identidad (persona, empresa, web) con una clave pública. Sirve para confirmar que la clave pública realmente pertenece a quien dice ser.
  + **Firma digital PDF (Adobe Sign):** Garantiza que el documento no ha sido modificado desde que se firmó.
  + **Certificado SSL/TLS:** Usado en sitios web
  + **DNIe (Documento Nacional de Identidad electrónico – España):** Permite firmar trámites legales online.

**3. Hashing**

Proceso que toma datos de cualquier tamaño y los transforma en una cadena de longitud fija mediante una función matemática llamada “función hash”.

* Es **unidireccional** (no puede revertirse para obtener el dato original).
* Se usa para verificar integridad (si algo cambia, el hash cambia), almacenar contraseñas de forma segura o firmar digitalmente archivos.
  + **SHA-256:** Usado en blockchain (Bitcoin) para proteger bloques y transacciones.
  + **MD5:** Antes se usaba para verificar integridad de archivos descargados (aunque hoy se considera inseguro).
  + **bcrypt:** Algoritmo seguro para almacenar contraseñas en bases de datos.

**4. Auditorías en control de versiones**

Práctica de revisar y analizar el historial de cambios en un sistema de control de versiones (como Git) para asegurar que el código cumple estándares de seguridad, calidad y responsabilidad.

* Permite rastrear quién hizo cada cambio, cuándo y por qué.
* Ayuda a detectar código malicioso, errores introducidos, y garantiza la trazabilidad.
  + **Revisión de commits en GitHub:** Detectar si alguien subió credenciales a un repositorio público.
  + **Herramientas como SonarQube:** Analizan la calidad y seguridad del código en repositorios.
  + **Uso de git blame:** Saber quién y cuándo introdujo una línea de código problemática.

**5. Mecanismos de autenticación robustos**

Métodos de verificación de identidad diseñados para ser seguros y difíciles de vulnerar.

* Incluyen autenticación multifactor (MFA), uso de contraseñas fuertes, autenticación biométrica (huella, rostro), tokens físicos (YubiKey) o códigos de un solo uso (OTP).
* Objetivo: asegurarse de que solo usuarios legítimos acceden a sistemas críticos.
  + **Autenticación en dos pasos (2FA) de Google:** Código SMS o app Authenticator además de la contraseña.
  + **YubiKey:** Llave física que añade un segundo factor de autenticación.
  + **Face ID (Apple):** Reconocimiento facial como segundo factor de seguridad.

**6. Sistemas de control de accesos**

Conjunto de políticas y tecnologías que regulan qué usuarios pueden acceder a qué recursos dentro de un sistema.

* Modelos comunes:
  + DAC (Discretionary Access Control): el dueño decide quién accede.
  + MAC (Mandatory Access Control): el acceso depende de reglas estrictas definidas por el sistema.
  + RBAC (Role-Based Access Control): permisos según el rol del usuario (admin, editor, lector).
  + **Permisos de archivos en Linux:** Lectura/escritura/ejecución para usuario, grupo y otros.
  + **RBAC en AWS IAM:** Roles y políticas para limitar acceso a servicios en la nube.
  + **Control de acceso en Active Directory (Windows):** Administrar qué usuarios acceden a carpetas o recursos de red.

**7. No repudio**

Propiedad de un sistema que garantiza que un usuario **no puede negar haber realizado una acción** o haber enviado un mensaje.

* Se logra combinando cifrado, firmas digitales y registros seguros.
* Importante en transacciones electrónicas y documentos legales para asegurar que nadie pueda negar su participación.
* Ejemplo: al firmar un contrato digitalmente, el emisor no puede negar después haberlo firmado.
  + **Factura electrónica firmada digitalmente:** El emisor no puede negar haber enviado la factura.
  + **Correo certificado electrónico (Burofax online):** Garantiza que el mensaje fue enviado y recibido.
  + **Blockchain (Bitcoin/Ethereum):** Las transacciones quedan registradas y no pueden negarse ni alterarse.

**1. Autenticidad**

**Definición:**  
Propiedad que garantiza que algo **es realmente lo que dice ser** y que **proviene de la fuente legítima**. En el contexto digital, asegura que un mensaje, archivo, documento o usuario no ha sido falsificado ni suplantado.

* Se logra mediante **firmas digitales**, **certificados**, y mecanismos de **autenticación segura**.

**2. Trazabilidad**

**Definición:**  
Capacidad de **seguir el historial completo de un elemento o acción**, desde su origen hasta su estado actual. Permite saber **quién hizo qué, cuándo y cómo**, para asegurar transparencia, auditoría y control.

* Es esencial en seguridad informática, control de calidad y sistemas de gestión.