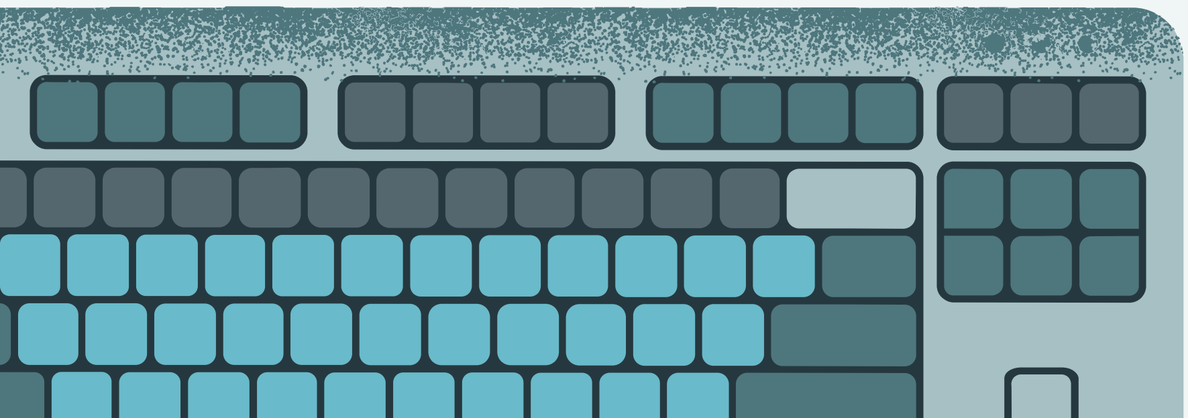
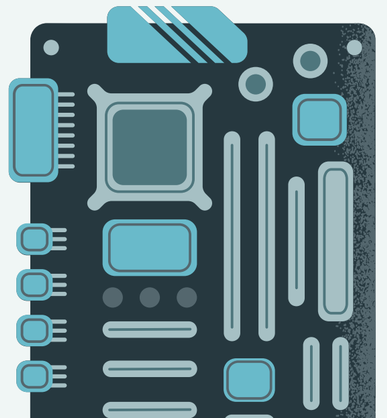
Ariadna Guerrero Angelina Navarro Julieta Berón
Colegio Del Prado Andrea Gómez 3 “A” 2024

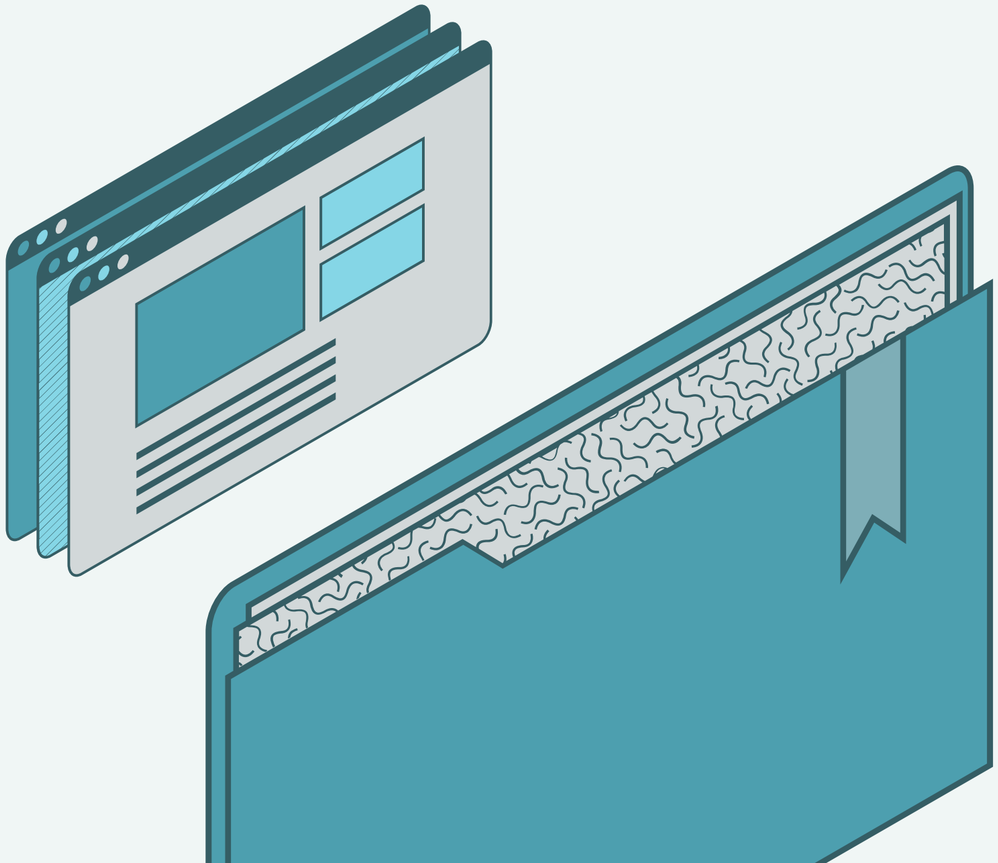
INFORMATICA

CIBERSEGURIDAD - VIRUS INFORMATICOS





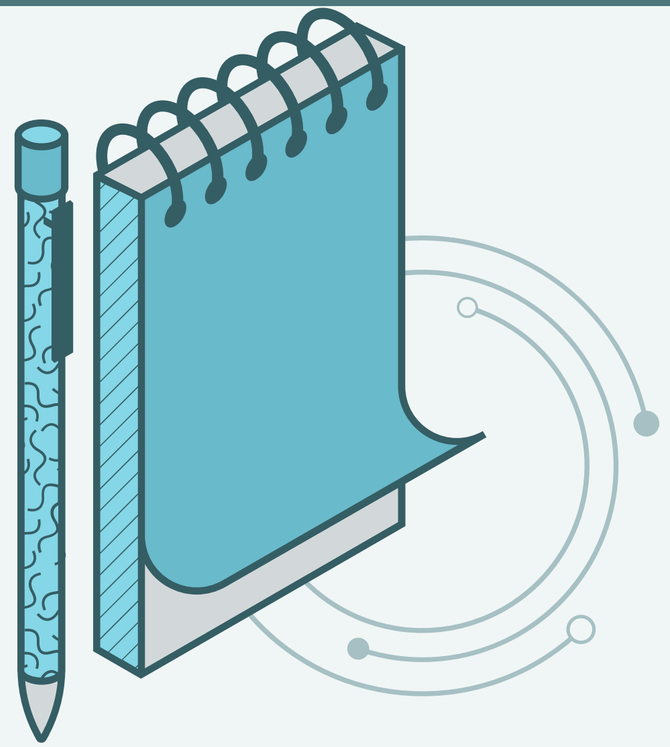

ÍNDICE



CIBERSEGURIDAD

¿Por qué es importante?

La ciberseguridad es vital para proteger la información, mantener la confianza y garantizar la operatividad y el crecimiento sostenible de organizaciones y personas en un mundo cada vez más digital.



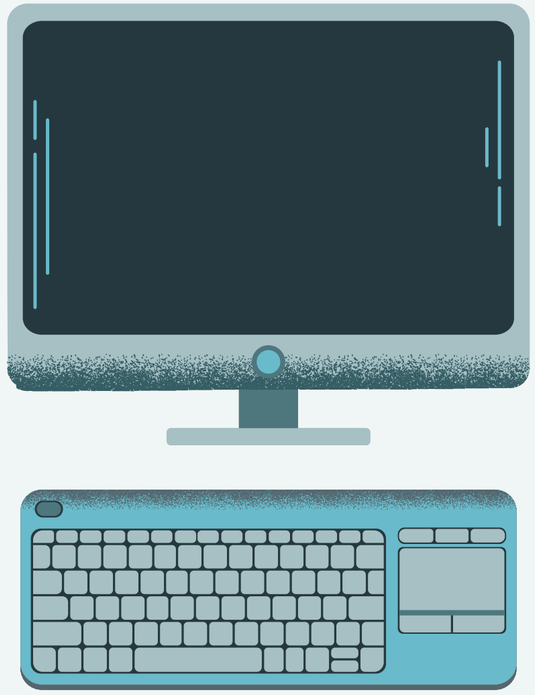
VIRUS INFORMATICOS

Son programas maliciosos diseñados para replicarse y propagarse de un sistema a otro. Su principal objetivo es dañar, alterar o robar información en dispositivos como computadoras, teléfonos móviles y otros sistemas electrónicos.

VIRUS INFORMATICOS

PHISHING

- Definición: Técnica de engaño para obtener información sensible haciéndose pasar por una entidad confiable.
- Características: Correos electrónicos fraudulentos, enlaces maliciosos, apariencia de legitimidad.
- Causas: Desconocimiento del usuario, falta de formación en ciberseguridad.
- Prevención: Capacitación a usuarios, verificación de fuentes y autenticación en dos pasos.



ESCANEO DE PUERTOS

- Definición: Técnica para identificar puertos abiertos en un sistema con el fin de encontrar vulnerabilidades.
- Características: Uso de herramientas automatizadas, puede ser parte de un ataque más complejo.
- Causas: Intención de vulnerar un sistema o red.
- Prevención: Uso de firewalls, monitoreo de tráfico y políticas de seguridad adecuadas.

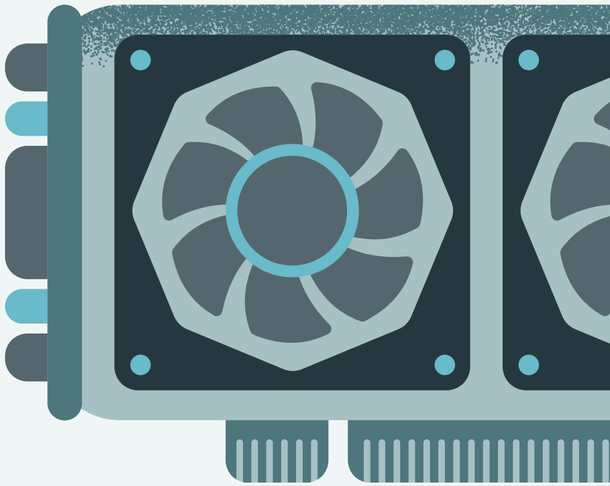
VIRUS INFORMATICOS

Criptografía

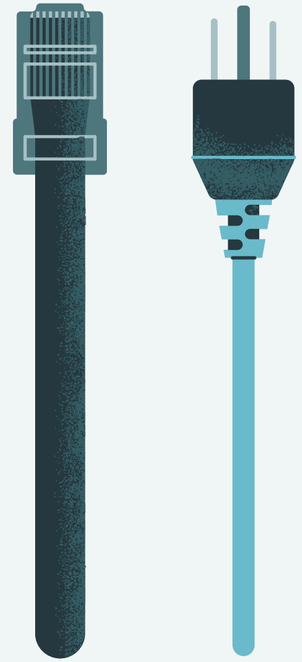
Definición: **Técnica de codificación de información para protegerla de accesos no autorizados.**
Características**: Uso de algoritmos, claves públicas y privadas.**
Causas: **Necesidad de proteger datos sensibles.**
Prevención**: Aplicar métodos de cifrado robustos y actualizaciones periódicas de algoritmos.**

Backdoors

Definición**: Métodos ocultos para eludir la autenticación y acceder a sistemas.**
Características**: Instalación silenciosa, puede ser parte de malware.**
Causas: **Vulnerabilidades en software o intenciones maliciosas de desarrolladores.**
Prevención: **Actualización regular de software y auditorías de seguridad.**



VIRUS INFORMÁTICOS



RAMSOMWARE

Definición: Tipo de malware que cifra archivos y solicita un rescate para liberarlos.
Características: Criptografía fuerte, demanda de pago en criptomonedas.
Causas: Descargas maliciosas, correos de phishing.
Prevención: Copias de seguridad regulares, software antivirus y educación sobre seguridad.

TROYANO

Definición: Malware que se presenta como un programa legítimo pero causa daño o permite acceso no autorizado.
Características: Engañoso, se infiltra sin que el usuario lo note.
Causas: Descargas de software no confiable.
Prevención: Uso de antivirus, escaneo de archivos y precaución al descargar.

VIRUS INFORMÁTICOS

SNIFFING

Definición: Monitoreo del tráfico de red para capturar datos sensibles.
Características: Análisis de paquetes, puede ser pasivo o activo.
Causas: Redes inseguros o mal configuradas.
Prevención: Cifrado de datos en tránsito y uso de redes seguras.

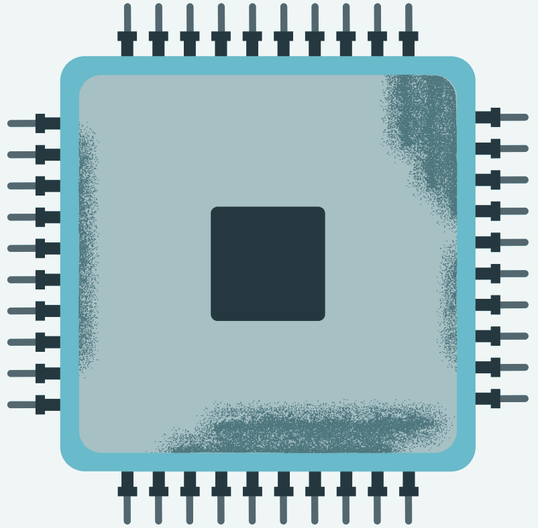
CODIGO MALICIOSO

Definición: Software diseñado para dañar o infiltrarse en sistemas.
Características: Variedad de tipos (virus, gusanos, ransomware), efectos perjudiciales.
Causas: Descargas de fuentes no confiables, vulnerabilidades.
Prevención: Antivirus actualizado, formación de usuarios y cuidado en descargas.

DAÑOS FÍSICOS AL EQUIPO

Definición: Daños causados a hardware que afectan su funcionamiento.
Características: Puede ser intencional (vandalismo) o accidental (fallos eléctricos).
Causas: Desastres naturales, manipulación indebida.
Prevención: Mantenimiento regular, protección física y copias de seguridad
.

VIRUS INFORMATICOS



DAÑOS FISICOS AL EQUIPAMIENTO

Alteraciones o deterioros que afectan la integridad física de un dispositivo, máquina o sistema, impedendo su funcionamiento correcto.

Tipos de daños físicos:

1. **Mecánicos: Desgaste, rotura o deformación de componentes.**
2. **Eléctricos: Cortocircuitos, sobrecalentamiento, descargas eléctricas.**
3. **Térmicos: Sobrecalentamiento, quemaduras, daños por temperatura.**
4. **Físicos: Golpes, caídas, vibraciones, humedad.**

HACKERS

Un hacker es un individuo que utiliza sus habilidades y conocimientos en informática y seguridad para acceder, modificar, controlar o dañar sistemas informáticos, redes, dispositivos o datos sin autorización.

SPOOFING

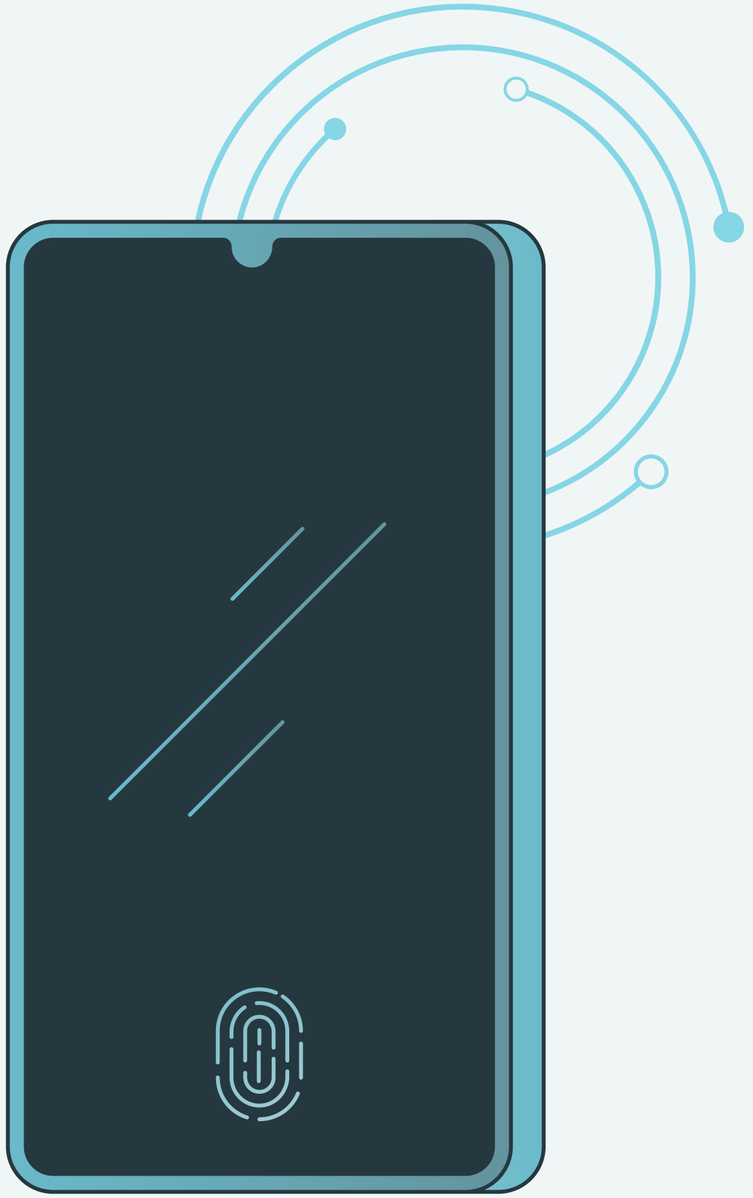
El spoofing es un tipo de robo de identidad que ocurre en los medios digitales y electrónicos. A través de esta práctica ilegal, las personas extraen información sensible de sus víctimas, la cual aprovechan para cometer crímenes. El spoofing debe su nombre al término en inglés spoof, que significa suplantación.

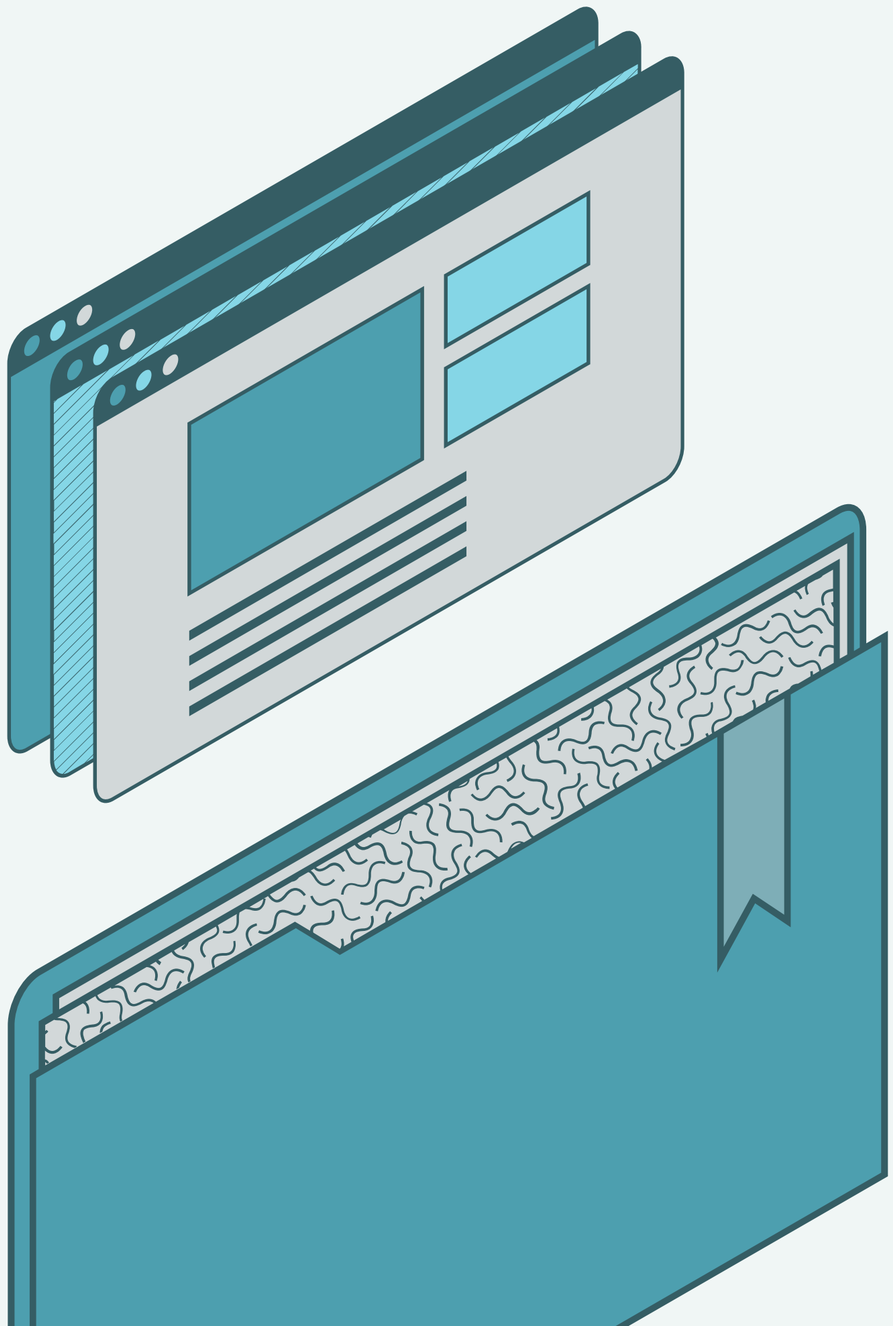
EXPLOIT

Código, técnica o herramienta que aprovecha una vulnerabilidad o debilidad en un sistema informático, software o hardware para acceder, controlar, dañar o obtener información confidencial sin autorización.

VIRUS INFORMATICOS

- **Eavesdropping:** Escucha secreta o interceptación no autorizada de conversaciones, comunicaciones electrónicas o datos transmitidos entre dos o más partes.
- **Ataques de Contraseñas :** Técnicas maliciosas utilizadas para obtener o descubrir contraseñas de acceso a sistemas, redes, aplicaciones o cuentas de usuario, con el fin de comprometer la seguridad y autorizar accesos no autorizados.
- **Denegación de Servicio:** Ataque cibernético que sobrecarga un sistema, red o aplicación con una cantidad masiva de solicitudes, tráfico o peticiones, con el objetivo de hacer que sea inaccesible o dejar de funcionar, negando el servicio a los usuarios legítimos.
- **Fraude Informático:** Utilización de tecnologías de la información y comunicación (TIC) para realizar actividades ilícitas, engañosas o fraudulentas, con el objetivo de obtener beneficios económicos, información confidencial o ventajas injustas.





VIRUS INFORMATICOS

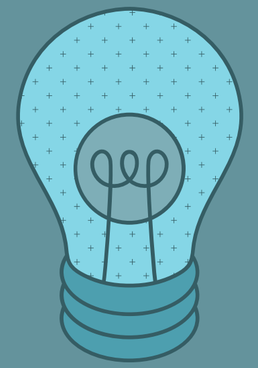
01. Malware

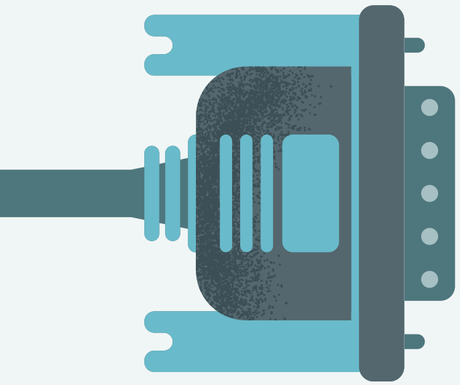
es un término que abarca cualquier tipo de software malicioso diseñado para dañar o explotar cualquier dispositivo, servicio o red programable.
Características de un malware
Es diseñado intencionalmente. ...
Engloba a cualquier clase de software malicioso.
Realiza acciones sin el consentimiento del usuario.
Existen muchos vectores de ataque de malware: descargar e instalar un programa infectado, hacer clic en un vínculo infectado, abrir un archivo adjunto de un correo electrónico malicioso o incluso utilizar medios físicos corruptos, como una memoria USB infectada.
Lo evitamos instalando un antivirus

02. Software ilegal

El concepto de software ilegal o pirata se refiere a la falsificación o copia no autorizada de un programa informático con derechos de autor registrados, que no cuenta con la correspondiente licencia para su uso de manera legal.
Características
Las posibilidades de infectar un equipo con virus son mayores. ...
Acceso denegado a actualizaciones y mejoras
El software malicioso puede entrar en su sistema de varias maneras. Puede provenir de hacer clic en vínculos maliciosos, descargar archivos infectados o abrir archivos adjuntos de correo electrónico de remitentes desconocidos
En ese caso, las leyes del copyright son el único método para proteger su software de un uso ilegal

VIRUS INFORMATICO





SOFTWARE ILEGAL

El concepto de software ilegal o pirata se refiere a la falsificación o copia no autorizada de un programa informático con derechos de autor registrados, que no cuenta con la correspondiente licencia para su uso de manera legal.
Características Las posibilidades de infectar un equipo con virus son mayores
Acceso denegado a actualizaciones y mejoras
El software malicioso puede entrar en su sistema de varias maneras. Puede provenir de hacer clic en vínculos maliciosos, descargar archivos infectados o abrir archivos adjuntos de correo electrónico de remitentes desconocidos
En ese caso, las leyes del copyright son el único método para proteger su software de un uso ilegal

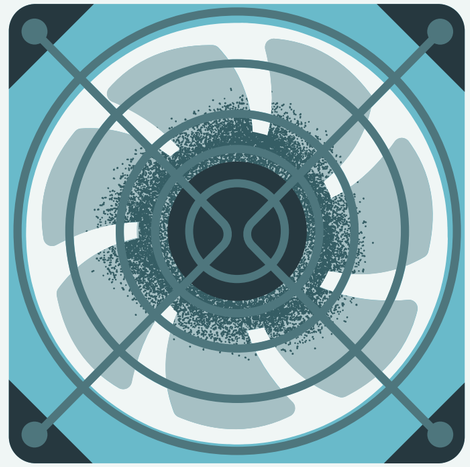
ADWARE

Un adware es un tipo de programa publicitario malicioso
El adware puede bloquear programas o congelar el dispositivo.
, se aconseja utilizar soluciones antimalware, bloqueadores de publicidad, mantener el software actualizado y evitar enlaces y archivos sospechosos
Ser intrusivo: El adware tiene la capacidad de mostrar anuncios publicitarios de manera constante, incluso cuando el usuario no está navegando en internet

TRASHING

El trashing es la acción de obtener información a través de archivos y documentos desechados o descartados; con la finalidad de cometer fraudes y robos de identidad.
El trashing es una técnica utilizada por los ciberdelincuentes para obtener información confidencial de las personas
Para evitar el trashing físico, lo mejor es asegurarte de destruir adecuadamente tus documentos usando destructoras de papel o con empresas especializadas

VIRUS INFORMATICOS



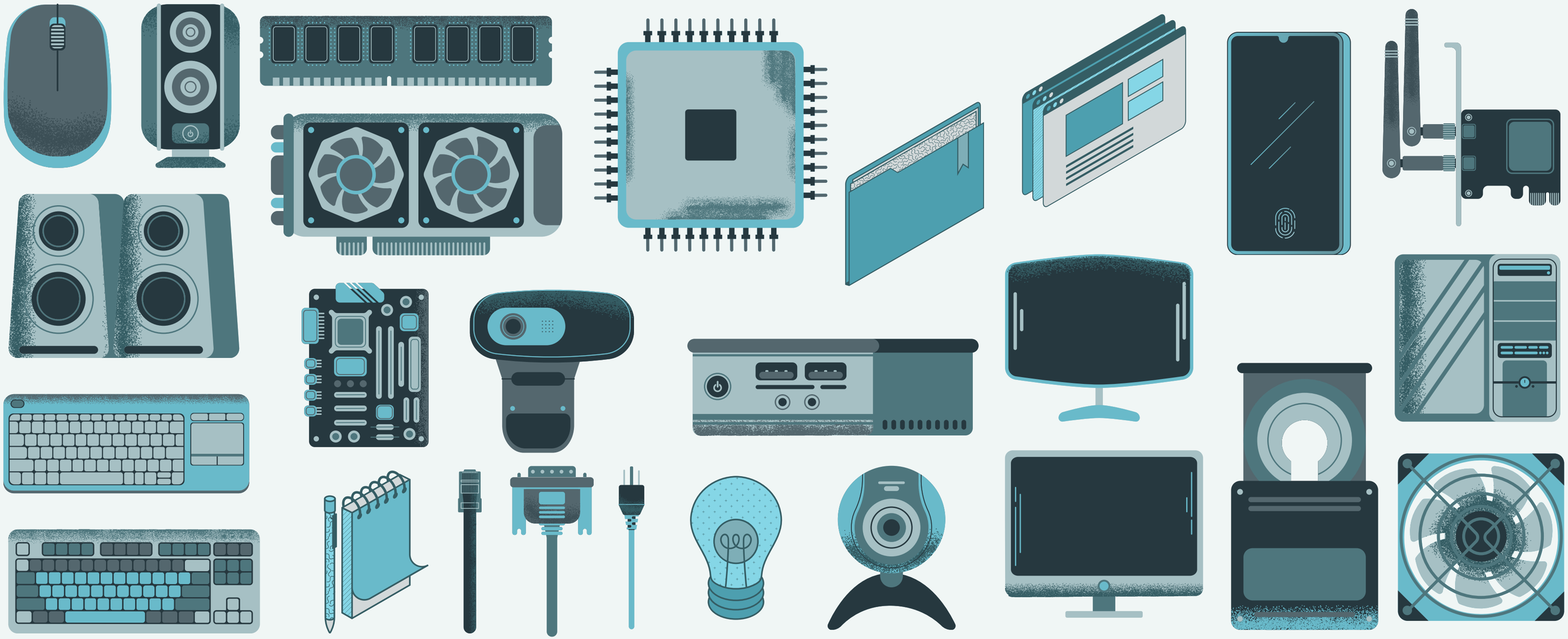
CIBERATAQUE

Un ciberataque es un conjunto de acciones dirigidas contra sistemas de información, como pueden ser bases de datos o redes computacionales, con el objetivo de perjudicar a personas, instituciones o empresas.
Pueden causar tiempo de inactividad, pérdida de datos y pérdida de dinero.
Instala también antivirus y programas de antimalware. Utiliza buenas contraseñas:
Un ciberataque es cualquier esfuerzo intencional para robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a una red, sistema informático o dispositivo digital.

WHITE HAT HACKER O HACKER

El término White Hat Hacker o hacker de sombrero blanco en Internet se refiere a un hacker ético, o un experto de seguridad informática
detectar problemas de seguridad y ayudar a las organizaciones a resguardarse de los hackers peligrosos.
Hackers éticos. - Detectan fallos y/o vulnerabilidades en sistemas para informarlos y así mejorar la seguridad informática. - No tienen intención de generar daños. - Están autorizados por la organización, entidad y/o gobierno.
taque
Protección sofisticada, seguridad avanzada: ofrece Symantec hoy.una protección avanzada para toda la cadena de ataque. Aprovecha los beneficios.

RECURSOS



www.unsitiogenial.es

MUCHAS GRACIAS