

Seguridad Informática

La seguridad informática es el conjunto de herramientas, normativas y métodos diseñados para proteger la información y los sistemas de computación de accesos no autorizados, daños o interrupciones. Su principal objetivo es preservar la confidencialidad, integridad y disponibilidad de los datos.

Tipos de malware

Conoce virus

Riesgos

Consejos simples para estar seguro.

Protegerme

Cuidado

Retarme

Ponerme a prueba

Sobre mi

Me gusta la programación. Disfruto mucho de crear cosas con código y resolver problemas. También me encanta aprender cada vez más; siempre estoy buscando algo nuevo que me ayude a mejorar.

La tecnología en general me apasiona, especialmente todo lo relacionado con redes, ciberseguridad y seguridad informática. Son áreas que me interesan mucho y en las que quiero seguir creciendo.

Actualmente estoy cursando 6to año en la EPET N°20, en Neuquén Capital, Argentina, y estoy por recibir el título de Técnico en Programación.

Motivo del proyecto

El motivo de este proyecto es poner en práctica mis conocimientos, animarme a equivocarme y aprender en el proceso. También quiero desafiar a buscar soluciones por mi cuenta, sin depender siempre de una guía.

Además, busco brindar información que considero realmente importante, sobre todo para quienes no están tan metidos en estos temas, pero que igual deberían tener en cuenta, porque todos somos vulnerables en el mundo digital.

Proyecto final desarrollado por Cristian Antinir - EPET N°20, Neuquén, Argentina.
Contacto: cristian.antinir.tech@gmail.com

Volver

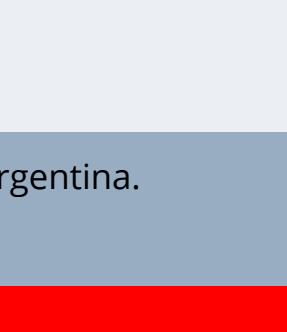
Tipos de malware

Inicio

Virus



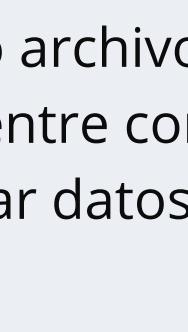
Troyano



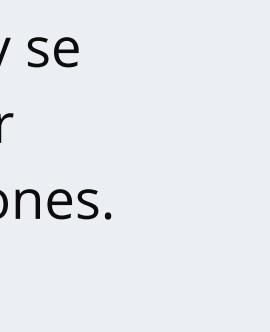
Ransomware



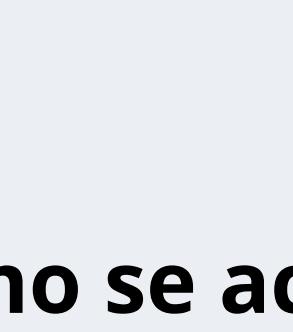
Gusano (Worm)



Spyware



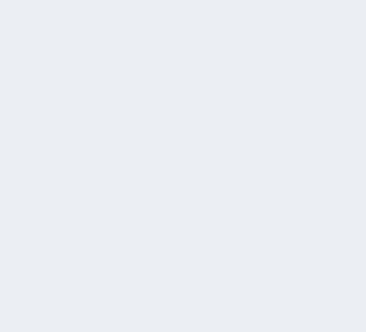
Adware



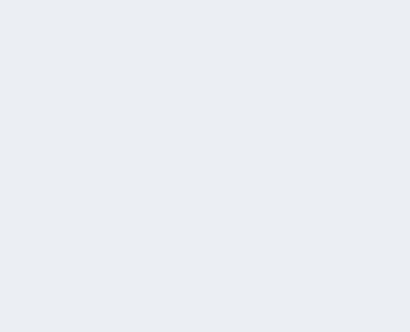
Rootkit



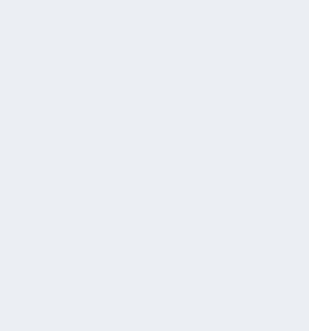
Keylogger



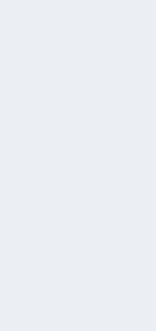
Botnet



Scareware



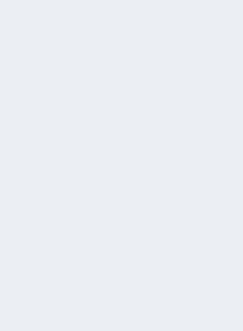
Backdoor



Exploit



Fileless malware



¿Qué es? 🤔

software malicioso (malware) que se adhiere a programas o archivos legítimos, se replica y se propaga entre computadoras para dañar sistemas, robar datos o interrumpir operaciones.

¿Cómo se activa? 😬

al ejecutar el archivo infectado y se pueden prevenir utilizando software antivirus, manteniendo el sistema actualizado, realizando copias de seguridad y adoptando prácticas de navegación seguras.

¿Que daños causa? 🔥

Pérdida o corrupción de datos.
Ralentización o bloqueo del sistema.
Robo de información personal o confidencial.
Acceso no autorizado a dispositivos.
Propagación a otros equipos en la red.

¿Cómo protegerse? 🛡️

Instala un antivirus confiable.
Mantén el software actualizado.
No abras correos sospechosos.
Navega en sitios seguros (HTTPS).

¿Cómo eliminarlo? ✗

Desconectarse de internet algo de texto.
Análisis con antivirus y anti-malware.
Actualizar el sistema y antivirus.
Eliminar archivos temporales.
Modo seguro.

Volver

Otros tipos

Inicio

Proyecto final desarrollado por Cristian Antinir - EPET N°20, Neuquén, Argentina.

Contacto: cristian.antinir.tech@gmail.com

Troyano

¿Qué es? 🤔

Es un tipo de malware que se oculta como un programa legítimo para engañar al usuario. Una vez instalado, permite acceso no autorizado al sistema.

¿Cómo se activa? 😕

El usuario descarga o ejecuta el archivo pensando que es seguro. Ej: cracks, juegos piratas, archivos adjuntos falsos, etc.

¿Que daños causa? 🔥

Robo de información personal
Control remoto del dispositivo
Instalación de más malware
Acceso a cámara, micrófono o archivos
Uso del equipo para ataques

¿Cómo protegerse? 🛡️

No descargar software pirata o desconocido
Usar antivirus y mantenerlo actualizado
Evitar correos y enlaces sospechosos
Revisar permisos al instalar programas

¿Cómo eliminarlo? ✗

Usa herramientas anti-troyanos (como Malwarebytes)
Ejecuta un análisis completo con antivirus
Revisa accesos remotos y desactívalos
Desconéctate de internet
Inicia en modo seguro
Cambia tus contraseñas

[Volver](#)

[Otros tipos](#)

[Inicio](#)

Proyecto final desarrollado por Cristian Antiñir – EPET N°20, Neuquén, Argentina.
Contacto: cristian.antinir.tech@gmail.com

Ransomware

¿Qué es? 🤔

Es un tipo de malware que bloquea el acceso a tus archivos o sistema y exige un pago (rescate) para liberarlos.

¿Cómo se activa? 😕

Correos falsos con archivos adjuntos
Descargas de programas piratas
Vulnerabilidades del sistema
Enlaces maliciosos

¿Cómo protegerse? 🛡️

No abrir correos o archivos sospechosos
Realizar copias de seguridad frecuentes
Mantener el sistema y programas al día
No descargar software ilegal
Usar antivirus actualizado

¿Cómo eliminarlo? ✗

Restaurá archivos desde una copia de seguridad (si tenés)
Formateá si es necesario (como última opción)
Reforzá la seguridad para evitar reinfecciones
Escaneá con antivirus y anti-ransomware
Desconectá el equipo de internet
No pagues el rescate

[Volver](#)

[Otros tipos](#)

[Inicio](#)

Proyecto final desarrollado por Cristian Antiñir – EPET N°20, Neuquén, Argentina.
Contacto: cristian.antinir.tech@gmail.com

Gusano (Worm)

¿Qué es? 🤔

Es un malware que se copia a sí mismo y se propaga automáticamente por redes o dispositivos sin que el usuario lo abra.

¿Cómo se activa? 😕

Correos electrónicos con enlaces maliciosos
Se instala a través de redes vulnerables
Exploita fallos de seguridad en el sistema
Dispositivos USB infectados

¿Cómo protegerse? 🛡️

Escanear dispositivos externos antes de usarlos
Mantener el sistema y antivirus actualizados
No abrir correos o enlaces sospechosos
Usar firewall para proteger la redal

¿Cómo eliminarlo? ✗

Actualizá seguridad antes de reconectarte
Escaneá otros equipos conectados a la red
Ejecutá un análisis completo con antivirus
Eliminá archivos infectados detectados
Desconectá el equipo de la red
Iniciá en modo seguro

[Volver](#)

[Otros tipos](#)

[Inicio](#)

Proyecto final desarrollado por Cristian Antiñir – EPET N°20, Neuquén, Argentina.
Contacto: cristian.antinir.tech@gmail.com

Spyware

¿Qué es? 🤔

Es un software espía que se instala sin permiso y vigila lo que hacés en tu dispositivo, como contraseñas, clics o conversaciones.

¿Cómo se activa? 😕

Haciendo clic en anuncios o enlaces maliciosos
Con instaladores ocultos en software pirata
A través de archivos adjuntos en correos
Descargando apps o programas falsos

¿Que daños causa? 🔥

Robo de contraseñas y datos personales
Registro de tus actividades y sitios web
Venta de tu información a terceros
Acceso a tu cámara o micrófono

¿Cómo protegerse? 🛡️

Cuidá lo que compartís en formularios y redessconocido
No aceptes permisos innecesarios en apps
Usá antivirus y anti-spyware actualizados
Evitá descargar programas no confiables

¿Cómo eliminarlo? ✗

Revisá y eliminá extensiones o apps sospechosas
Ejecutá un escaneo con antivirus y anti-spyware
Activá la autenticación en dos pasos si podés
Iniciá el sistema en modo seguro
Cambiá todas tus contraseñas
Desconectá de internet

[Volver](#)

[Otros tipos](#)

[Inicio](#)

Proyecto final desarrollado por Cristian Antiñir – EPET N°20, Neuquén, Argentina.
Contacto: cristian.antinir.tech@gmail.com

Adware

¿Qué es? 🤔

Es un tipo de software que muestra publicidad no deseada en tu dispositivo. A veces viene incluido con programas gratuitos.

¿Cómo se activa? 😕

Mediante extensiones del navegador o apps no confiables
Al instalar programas gratuitos con adware incluido
Al hacer clic en anuncios engañosos

¿Que daños causa? 🔥

Possible recolección de datos sin permiso
Ralentiza el sistema y el navegador
Redirecciones a sitios peligrosos
Publicidad molesta y constante

¿Cómo protegerse? 🛡️

Evitá sitios web sospechosos o con exceso de pop-ups
Leé bien antes de instalar programas gratuitos
Usá antivirus y bloqueadores de anuncios
No instales extensiones desconocidas

¿Cómo eliminarlo? ✗

Revisá que no vuelva a instalarse automáticamente
Restablecé el navegador si sigue el problema
Escaneá el sistema con antivirus/anti-adware
Eliminá extensiones extrañas del navegador
Desinstalá programas sospechosos

[Volver](#)

[Otros tipos](#)

[Inicio](#)

Proyecto final desarrollado por Cristian Antiñir – EPET N°20, Neuquén, Argentina.
Contacto: cristian.antinir.tech@gmail.com

Rootkit

¿Qué es? 🤔

Es un malware avanzado que se oculta en el sistema operativo para permitir el control remoto del equipo sin que el usuario lo note.

¿Cómo se activa? 😕

Por troyanos que descargan el rootkit en segundo plano
Mediante vulnerabilidades del sistema
Al instalar software pirata o infectado

¿Que daños causa? 🔥

Dificulta o impide su detección y eliminación
Robo de información sin ser detectado
Acceso total al sistema sin autorización
Instalación de otros malware

¿Cómo protegerse? 🛡️

Revisar comportamientos anormales del sistema
No descargar programas de fuentes dudosas
Usar antivirus con protección contra rootkits
Mantener el sistema operativo actualizado

¿Cómo eliminarlo? ✗

Usá herramientas específicas anti-rootkit (Ej: TDSSKiller, Malwarebytes)
Reforzá la seguridad antes de volver a usar el equipo normalmente
Restaurá desde una copia de seguridad limpia
A veces es necesario formatear el sistema
Ejecutá los análisis en modo seguro

[Volver](#)

[Otros tipos](#)

[Inicio](#)

Proyecto final desarrollado por Cristian Antiñir – EPET N°20, Neuquén, Argentina.
Contacto: cristian.antinir.tech@gmail.com

Keylogger

¿Qué es? 🤔

Es un tipo de malware que registra todo lo que escribís en el teclado, incluyendo contraseñas, chats y datos personales.

¿Cómo se activa? 😕

Mediante dispositivos físicos conectados al teclado
Al instalar programas falsos o crackeados
A través de troyanos u otros malware
Desde correos o enlaces maliciosos

¿Que daños causa? 🔥

Robo de contraseñas y cuentas
Suplantación de identidad
Acceso a datos bancarios
Pérdida de privacidad

¿Cómo protegerse? 🛡️

Activar la verificación en dos pasos en tus cuentas
Evitar descargar software pirata o desconocido
Usar antivirus y antikeyloggers actualizados
Revisar permisos de las apps instaladas

¿Cómo eliminarlo? ✗

Reinstalá el sistema si no se puede eliminar completamente
Cambiá todas tus contraseñas desde un dispositivo seguro
Revisá los procesos activos y programas sospechosos
Iniciá en modo seguro para facilitar la detección
Ejecutá un análisis con antivirus y antikeylogger

[Volver](#)

[Otros tipos](#)

[Inicio](#)

Proyecto final desarrollado por Cristian Antiñir - EPET N°20, Neuquén, Argentina.
Contacto: cristian.antinir.tech@gmail.com

Botnet

¿Qué es? 🤔

Es una red de dispositivos infectados (bots) que son controlados remotamente por un atacante, sin que el usuario lo sepa.

¿Cómo se activa? 😕

Una vez infectado, el dispositivo se conecta a la red del atacante
Mediante descargas engañosas o vulnerabilidades del sistema
A través de malware como troyanos o gusanos

¿Que daños causa? 🔥

Tu dispositivo se usa para ataques DDoS (derribar sitios web)
Robo de datos o envío masivo de spam
Aumento del uso de red sin razón
Robo de datos o envío masivo de spam

¿Cómo protegerse? 🛡️

Evitar hacer clic en enlaces o archivos sospechosos
No descargar software de fuentes no confiables
Usar antivirus y firewall actualizados
Mantener tu sistema y apps al día

¿Cómo eliminarlo? ✗

Restaurá o formateá si no se logra eliminar completamente
Eliminá procesos o archivos maliciosos detectados
Cambiá contraseñas desde un dispositivo seguro
Escaneá con antivirus y anti-botnet confiables
Desconectá el equipo de la red

[Volver](#)

[Otros tipos](#)

[Inicio](#)

Proyecto final desarrollado por Cristian Antiñir - EPET N°20, Neuquén, Argentina.
Contacto: cristian.antinir.tech@gmail.com

Scareware

¿Qué es? 🤔

Es un software falso que asusta al usuario con mensajes de alerta falsos, como "¡Tu equipo está infectado!", para que instale un programa o pague por una "solución".

¿Cómo se activa? 😕

A través de ventanas emergentes en sitios web
Mediante falsos antivirus o alertas del sistema
Al descargar software pirata o dudoso
En correos con mensajes alarmantes

¿Cómo eliminarlo? ✗

Limpiá el navegador y restablecé la configuración
Escaneá el equipo con antivirus real y actualizado
Cambiá contraseñas si diste información
Cerrá la alerta sin interactuar con ella
Desinstalá programas sospechosos

¿Cómo protegerse? 🛡️

Cerrar las ventanas emergentes con cuidado (no hacer clic en "Aceptar")
Evitar descargas de sitios no oficiales
No hacer clic en alertas sospechosas
Usar antivirus actualizado

¿Cómo eliminarlo? ✗

Limpiá el navegador y restablecé la configuración
Escaneá el equipo con antivirus real y actualizado
Cambiá contraseñas si diste información
Cerrá la alerta sin interactuar con ella
Desinstalá programas sospechosos

[Volver](#)

[Otros tipos](#)

[Inicio](#)

Proyecto final desarrollado por Cristian Antiñir - EPET N°20, Neuquén, Argentina.
Contacto: cristian.antinir.tech@gmail.com

Backdoor

¿Qué es? 🤔

Es un tipo de malware que crea una “puerta trasera” en tu sistema para que un atacante pueda acceder y controlarlo de forma remota, sin tu permiso.

¿Cómo se activa? 😕

Instalado manualmente por un atacante con acceso físico
En archivos descargados de fuentes no seguras
Aprovechando vulnerabilidades del sistema
A través de troyanos u otros virus

¿Que daños causa? 🔥

Instalado manualmente por un atacante con acceso físico
En archivos descargados de fuentes no seguras
Pérdida de dinero si el usuario paga
Ralentización del sistema

¿Cómo protegerse? 🛡️

Revisar los permisos y conexiones del sistema
No descargar software pirata o desconocido
Mantener el sistema siempre actualizado
Usar antivirus y firewall activos

¿Cómo eliminarlo? ✗

Restaurá o formateá si el sistema fue comprometido
Escaneá con antivirus y anti-malware actualizados
Iniciá en modo seguro para facilitar la detección
Cerrá accesos remotos sospechosos
Cambiá todas tus contraseñas

[Volver](#)

[Otros tipos](#)

[Inicio](#)

Proyecto final desarrollado por Cristian Antiñir – EPET N°20, Neuquén, Argentina.
Contacto: cristian.antinir.tech@gmail.com

Exploit

¿Qué es? 🤔

Es un programa o código que aprovecha fallos o vulnerabilidades en un sistema, aplicación o red para ejecutar acciones maliciosas sin permiso.

¿Cómo se activa? 😕

Usando software desactualizado con errores de seguridad
Mediante páginas web maliciosas
A través de redes sin protección
Al abrir archivos infectados

¿Que daños causa? 🔥

Instalación de malware (ransomware, troyanos, etc.)
Daños a la red o a otros dispositivos conectados
Control del sistema sin que lo sepas
Robo de información y accesos

¿Cómo protegerse? 🛡️

Mantener el sistema y programas actualizados
Usar antivirus con protección contra exploits
No abrir archivos de fuentes desconocidas
Evitar sitios web peligrosos o sin HTTPS

¿Cómo eliminarlo? ✗

Restaurá el sistema desde un punto seguro si es necesario
Cambiá contraseñas si hubo acceso no autorizado
Actualizá el sistema operativo y todo el software
Escaneá el sistema con antivirus/anti-exploit
Eliminá archivos o programas sospechosos

[Volver](#)

[Otros tipos](#)

[Inicio](#)

Proyecto final desarrollado por Cristian Antiñir – EPET N°20, Neuquén, Argentina.
Contacto: cristian.antinir.tech@gmail.com

Fileless malware

¿Qué es? 🤔

Es un tipo de malware que no se guarda como archivo en el disco, sino que se ejecuta directamente en la memoria RAM, lo que lo hace más difícil de detectar.

¿Cómo se activa? 😕

Aprovechando herramientas legítimas como PowerShell o WMI
A través de enlaces maliciosos o macros en documentos
Usando vulnerabilidades del sistema o software
Mediante scripts en sitios web infectados

¿Que daños causa? 🔥

Difícil de detectar con antivirus tradicionales
Instalación de otros tipos de malware
Robo de datos sin dejar rastros
Control remoto del sistema

¿Cómo protegerse? 🛡️

Usar antivirus con protección en tiempo real contra amenazas en memoria
Mantener el sistema y software siempre actualizados
No abrir documentos sospechosos (Word, Excel, etc.)
Desactivar macros por defecto

¿Cómo eliminarlo? ✗

Escaneá el sistema con antivirus especializado (con detección en memoria)
Revisá procesos sospechosos en ejecución (RAM)
Reforzá la seguridad para evitar reinfección
Restaurá el sistema desde un punto seguro
Reiniciá en modo seguro

[Volver](#)

[Otros tipos](#)

[Inicio](#)

Proyecto final desarrollado por Cristian Antiñir – EPET N°20, Neuquén, Argentina.
Contacto: cristian.antinir.tech@gmail.com

Riesgo de malware !

[Inicio](#)

El malware, en sus distintas formas, representa un riesgo constante para usuarios y organizaciones. Su capacidad para infiltrarse sin ser detectado lo convierte en una amenaza difícil de prevenir si no se toman las medidas adecuadas.

Los efectos pueden ir desde una simple molestia hasta consecuencias graves como el robo de datos sensibles, el secuestro de archivos, la pérdida de dinero o el control remoto del dispositivo afectado.

Además, muchos tipos de malware se propagan fácilmente en redes, lo que amplifica el daño a otros sistemas conectados. Estar informado y protegido es clave para reducir este riesgo.

¿Cómo protegerme? ✓

[Inicio](#)

La mejor defensa contra el malware es la prevención. Mantén siempre tu sistema operativo, navegadores y aplicaciones actualizados. Muchas amenazas se aprovechan de errores ya corregidos, por eso es clave instalar las actualizaciones de seguridad.

Usa un antivirus confiable y evita hacer clic en enlaces sospechosos o abrir archivos de remitentes desconocidos. Desconfía de correos, mensajes o ventanas emergentes que te pidan datos personales o contraseñas.

Además, haz copias de seguridad regularmente y utiliza contraseñas seguras y únicas para cada cuenta. Con hábitos simples, puedes reducir drásticamente el riesgo de infección.

¿Realmente aprendí?

¿Qué hace un keylogger?

- Limpia archivos duplicados
- Registra lo que escribes en el teclado
- Cifra tus archivos
- Elimina virus automáticamente



[Inicio](#)

[Siguiente](#)

¿Realmente aprendí?

¿Qué buena práctica ayuda a protegerte del malware?

- Usar antivirus y hacer copias de seguridad
- Compartir contraseñas
- Ignorar actualizaciones del sistema
- Descargar archivos de cualquier sitio



Inicio

Siguiente

¿Realmente aprendí?

¿Cuál de estos malware
puede secuestrar tus
archivos y pedir un rescate?

- Adware
- Ransomware
- Spyware
- Rootkit



[Inicio](#)

[Siguiente](#)