



UANL




UNIVERSIDAD AUTÓNOMA DE NUEVO LEÓN



FIME

Catedrático: Norma Edith Marin Martinez

</ Redes y seguridad: sistemas distribuidos. />

	Nombre	Matricula	Carrera
	Guillermo Vladimir Flores Báez	2127967	ITS
	Diego Tristán Castro Franco	2109462	IAS
	Jorge Isaac De León Pérez	1932783	ITS

INTRODUCCION

En términos más técnicos, un virus informático es un tipo de programa o código malicioso escrito para modificar el funcionamiento de un equipo. Además, está diseñado para propagarse de un equipo a otro. Los virus se insertan o se adjuntan a un programa o documento legítimo que admite macros a fin de ejecutar su código. En el proceso, un virus tiene el potencial para provocar efectos inesperados o dañinos, como perjudicar el software del sistema, ya sea dañando o destruyendo datos.

Un virus informático, como un virus de gripe, está diseñado para propagarse de un host a otro y tiene la habilidad de replicarse. De forma similar, al igual que los virus no pueden reproducirse sin una célula que los albergue, los virus informáticos no pueden reproducirse ni propagarse sin programar, por ejemplo, un archivo o un documento.

VIRUS INFORMATICO

Un virus informático es un software que tiene por objetivo alterar el funcionamiento normal de cualquier tipo de dispositivo informático, sin el permiso o el conocimiento del usuario principalmente para lograr fines maliciosos sobre el dispositivo. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este mismo. Los virus pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo producen molestias o imprevistos.

[illegible]

PROPAGACION EN OTROS SISTEMAS OPERATIVOS

Los virus informáticos afectan en mayor o menor medida a casi todos los sistemas más conocidos y usados en la actualidad. Windows, MacOS, Linux... Cabe aclarar que un virus informático mayoritariamente atacará solo el sistema operativo para el que fue desarrollado, aunque ha habido algunos casos de virus multiplataforma.

MS-Windows, Android y IOS

- Su gran popularidad, como sistemas operativos, entre los computadores personales y dispositivos móviles. Se estima que, en 2007, un 90 % de ellos usaba Windows. Mientras que Android tiene una cuota de mercado de 80 % en 2015.
- La falta de seguridad en Windows (prioridad actual de Microsoft) hace muy fácil la “infección” del Ordenador al ser un sistema tradicionalmente muy permisivo con la instalación de programas ajenos a este, sin requerir ninguna autenticación por parte del usuario o pedirle algún permiso especial para ello en los sistemas más antiguos.

Unix y derivados

- Tradicionalmente los programadores y usuarios de sistemas basados en Unix han considerado la seguridad como una prioridad por lo que hay mayores medidas frente a virus, tales como la necesidad de autenticación por parte del usuario como administrador o robot para poder instalar cualquier programa adicional al sistema. En Windows esta prestación existe desde Windows Vista.
- Los directorios o carpetas que contienen los archivos vitales del sistema operativo cuentan con permisos especiales de acceso, por lo que no cualquier usuario o programa puede acceder fácilmente a ellos para modificarlos o borrarlos. Existe una jerarquía de permisos y accesos para los usuarios

TIPOS DE VIRUS

Existen diversos tipos de virus, varían según su función o la manera en que este se ejecuta en nuestra computadora alterando la actividad de la misma, entre los más comunes están:

- **Recycler:** Consiste en crear un acceso directo de un programa y eliminar su aplicación original, además al infectar un pendrive convierte a toda la información en acceso directo y oculta el original de modo que los archivos no puedan ser vistos, pero con la creación de un archivo batch que modifique los atributos de los archivos contenidos en el pendrive, estos podrían ser recuperados.
- **Troyano:** Consiste en robar información o alterar el sistema del hardware o en un caso extremo permite que un usuario externo pueda controlar el equipo.
- **Bombas lógicas:** Son programas que se activan al producirse un acontecimiento determinado. La condición suele ser una fecha (bombas de tiempo), una combinación de teclas, o ciertas condiciones técnicas (bombas lógicas). Si no se produce la condición permanece oculto al usuario.
- **Gusano:** Tiene la propiedad de duplicarse a sí mismo.



CARACTERISTICAS



Dado que una característica de los virus es el consumo de recursos, los virus ocasionan problemas tales como: pérdida de productividad, cortes en los sistemas de información o daños a nivel de datos.

Una de las características es la posibilidad que tienen de diseminarse por medio de réplicas y copias. Las redes en la actualidad ayudan a dicha propagación cuando estas no tienen la seguridad adecuada.

Otros daños que los virus producen a los sistemas informáticos son la pérdida de información, horas de parada productiva, tiempo de reinstalación, etc.

Hay que tener en cuenta que cada virus plantea una situación diferente.

METODOS DE PROPAGACION

Existen dos grandes clases de contagio. En la primera, el usuario, en un momento dado, ejecuta o acepta de forma inadvertida la instalación del virus. En la segunda, el programa malicioso actúa replicándose a través de las redes. En este caso se habla de gusanos. En cualquiera de los dos casos, el sistema operativo infectado comienza a sufrir una serie de comportamientos anómalos o imprevistos. Dichos comportamientos pueden dar una pista del problema y permitir la recuperación de este.

Dentro de las contaminaciones más frecuentes por interacción del usuario están las siguientes:

- Mensajes que ejecutan automáticamente programas (como el programa de correo que abre directamente un archivo adjunto).
- Ingeniería social, mensajes como "ejecute este programa y gane un premio", o, más comúnmente: "Haz 2 clics y gana 2 tonos para móvil gratis".
- Entrada de información en discos de otros usuarios infectados.
- Instalación de software modificado o de dudosa procedencia.



METODO DE PROTECCION

ACTIVOS

- **Antivirus:** son programas que tratan de descubrir las trazas que ha dejado un software malicioso, para detectarlo y eliminarlo del dispositivo completamente, y en algunos casos contener o parar la contaminación.
- **Filtros de ficheros:** Consiste en generar filtros de ficheros dañinos si el computador está conectado a una red. Estos filtros pueden usarse, por ejemplo, en el sistema de correos o usando técnicas de firewall.
- **Actualización automática:** Consiste en descargar e instalar las actualizaciones que el fabricante del sistema operativo lanza para corregir fallos de seguridad y mejorar el desempeño.

Pasivos

Para no infectar un dispositivo, hay que:

- No instalar software de dudosa procedencia.
- No abrir correos electrónicos de desconocidos ni adjuntos que no se reconozcan.
- Usar un bloqueador de elementos emergentes en el navegador.
- Usar la configuración de privacidad del navegador.
- Activar el Control de cuentas de usuario.
- Borrar la memoria caché de Internet y el historial del navegador.

TIPOS DE INTRUSOS

¿Qué es un intruso?

Se podría resumir como persona o programa que intenta acceder a un sistema informático sin autorización, de estos intrusos en su mayoría se tratan de personas o programas con conocimientos muy amplios sobre ciberseguridad.

Algunos ejemplos de estos serían los ya conocidos hackers cuyo objetivo principal es comprender los sistemas y el funcionamiento de ellos. Buscan y descubren las debilidades de una computadora o red informática.

Entre las practicas más comunes los hackers inyectan un tipo de malware para comprometer sistemas o datos, ¿Pero ¿qué son los malware?



Es un término general para referirse a cualquier tipo de "malicious software" (software malicioso) diseñado para infiltrarse en su dispositivo sin su conocimiento y causar daños e interrupciones en el sistema o robar datos. Adware, spyware, virus, redes de robots (botnets), troyanos, gusanos, rootkits y ransomware

- **Virus:** Se adjunta a archivos existentes y se propaga cuando se ejecutan esos archivos.
- **Gusano (Worm):** Se propaga a través de redes informáticas y puede replicarse a sí mismo para infectar otros sistemas.
- **Troyano (Trojan):** Se hace pasar por un programa legítimo, pero realiza funciones maliciosas una vez instalado en un sistema.

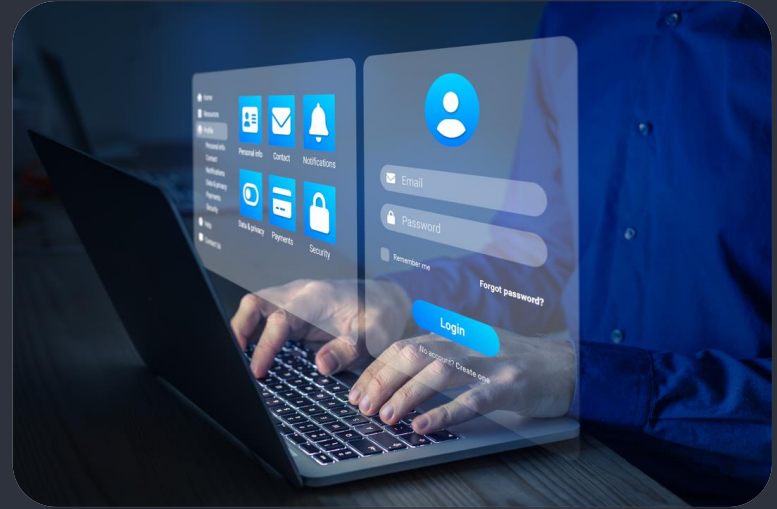
TIPOS DE MALWARE

- **Ransomware:** Encripta los archivos de la víctima y exige un rescate para desbloquearlos.
- **Spyware:** Monitorea las actividades del usuario sin su conocimiento, como la navegación web o la entrada de teclado, con fines de robo de información.
- **Adware:** Muestra anuncios no deseados en el sistema infectado, a menudo con el objetivo de generar ingresos para el creador del malware.
- **Rootkit:** Oculta la presencia de otros malware o actividades maliciosas en un sistema al nivel más profundo del sistema operativo.
- **Botnet:** Consiste en una red de computadoras infectadas controladas por un atacante, a menudo utilizado para llevar a cabo ataques coordinados como ataques de denegación de servicio (DDoS).

</ Que es la autenticación?

Es el proceso que usan las empresas para confirmar que solo las personas, servicios y aplicaciones adecuados con los permisos correctos pueden acceder a recursos de la organización. El proceso de autenticación incluye tres pasos principales:

1. **Identificación:** Los usuarios establecen quiénes son a través de un nombre de usuario, normalmente.
2. **Autenticación:** Normalmente, los usuarios prueban que son quienes dicen ser al escribir una contraseña (algo que, supuestamente, solo conoce el propio usuario).
3. **Autorización:** El sistema comprueba que los usuarios tengan permisos para el sistema al que intentan acceder.





Tipos de autenticaciones



Existen diferentes tipos de autenticación que se pueden utilizar para proteger sistemas y datos.

</ Autenticación de un solo factor (SFA).

Este es el método más básico de autenticación y se basa en un único factor, como una contraseña o un nombre de usuario. Si bien es simple de usar, también es el más vulnerable a ataques.

Características:

- El método de autenticación más básico.
- Se basa en un único factor, como una contraseña o un nombre de usuario.
- Es simple de usar, pero también es el más vulnerable a ataques.

Ejemplos:

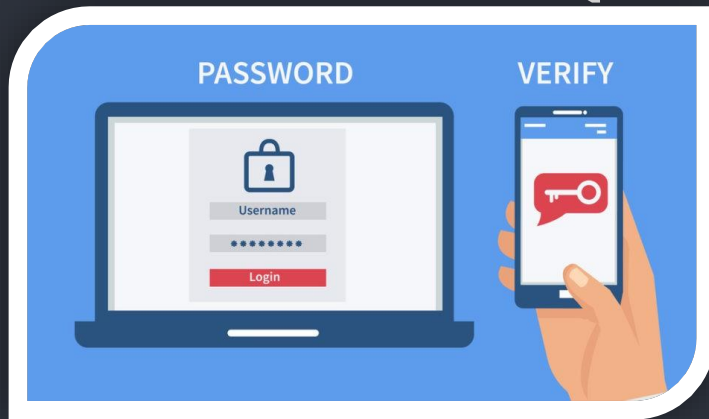
- Solo usar una contraseña para acceder a una cuenta.
- Usar el mismo nombre de usuario y contraseña para múltiples cuentas.



</ Autenticación de un dos factores (2FA).

La 2FA agrega una capa adicional de seguridad al requerir dos factores de autenticación, como una contraseña y un código enviado al teléfono del usuario.

Esto hace que sea mucho más difícil para los atacantes obtener acceso no autorizado.



Características:

- Agrega una capa adicional de seguridad al requerir dos factores de autenticación.
- Un factor suele ser algo que el usuario conoce, como una contraseña, y el otro factor suele ser algo que el usuario posee, como un teléfono móvil.
- Es más seguro que la SFA, pero aún puede ser vulnerable a ataques.

Ejemplos:

- Usar una contraseña y un código enviado al teléfono móvil para acceder a una cuenta.
- Usar una contraseña y una huella dactilar para desbloquear un dispositivo.

</ Autenticación multifactor (MFA).

La MFA va más allá de la 2FA al requerir tres o más factores de autenticación. Esto puede incluir elementos que el usuario posee, como una tarjeta inteligente o una llave de seguridad, o características biométricas, como una huella dactilar o un escaneo facial. La MFA es el método de autenticación más seguro.

Características:

- El método de autenticación más seguro.
- Requiere tres o más factores de autenticación.
- Los factores pueden incluir algo que el usuario conoce, algo que el usuario posee y algo que el usuario es.
- Es muy difícil de eludir, incluso para atacantes sofisticados.

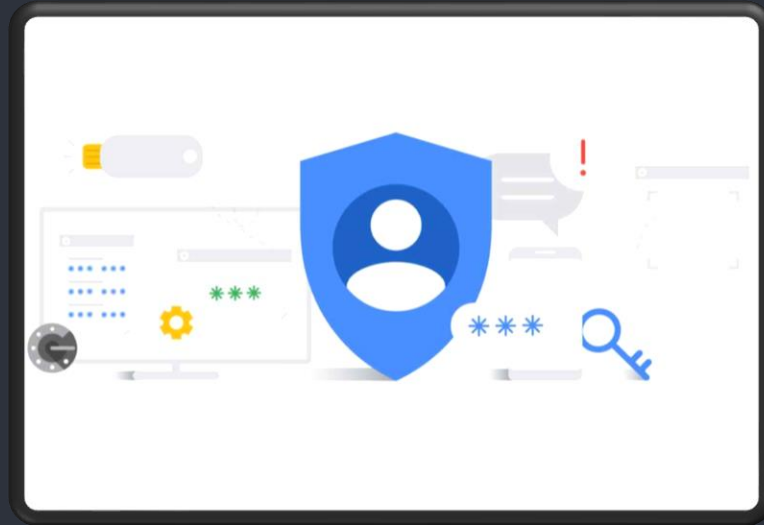
Ejemplos:

- Usar una contraseña, un código enviado al teléfono móvil y una huella dactilar para acceder a una cuenta bancaria.
- Usar una contraseña, una tarjeta inteligente y un escaneo facial para acceder a una red corporativa.





Niveles de Seguridad



</ Niveles de seguridad para Usuarios.

Contraseñas seguras

- Es importante utilizar contraseñas seguras y únicas para cada cuenta.
- Las contraseñas deben tener al menos 12 caracteres de largo y contener una combinación de letras mayúsculas, minúsculas, números y símbolos.

Software antivirus y anti-malware

- Es importante tener instalado y actualizado un software antivirus y anti-malware en su computadora.
- Este software puede ayudar a proteger su computadora contra virus, gusanos, troyanos y otro malware.

Actualizaciones de software

- Asegúrese de mantener su software actualizado, incluido su sistema operativo, navegador web y software de seguridad.
- Las actualizaciones de software a menudo contienen parches de seguridad que pueden ayudar a proteger su computadora contra vulnerabilidades conocidas.

1 0 1 1 0 1 1 0 1 1 0 1 1 0 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 1 0 1 1 0 1 1 0 1 1 1 1 1 0 1

</ Niveles de seguridad para Usuarios.

Tenga cuidado con lo que hace clic

- Tenga cuidado con los enlaces y archivos adjuntos en los correos electrónicos y -mensajes de redes sociales.
- No haga clic en enlaces ni descargue archivos adjuntos de personas que no conoce.

Sea consciente de las estafas de phishing

- Las estafas de phishing son intentos de engañarlo para que revele su información personal o financiera.
- Tenga cuidado con los correos electrónicos, sitios web y llamadas telefónicas que parecen provenir de organizaciones legítimas.

</ Niveles de seguridad para Redes.

Firewalls

Los firewalls son barreras que ayudan a proteger las redes de intrusos no autorizados.
Los firewalls pueden bloquear el tráfico no deseado y evitar que los ataques lleguen a las computadoras de la red.

Sistemas de detección de intrusiones (IDS)

Los IDS monitorean el tráfico de la red en busca de actividades sospechosas.
Si se detecta una actividad sospechosa, el IDS puede alertar a los administradores de la red para que investiguen.

Sistemas de prevención de intrusiones (IPS)

Los IPS son similares a los IDS, pero también pueden tomar medidas para bloquear el tráfico malicioso.
Esto puede ayudar a prevenir que los ataques lleguen a las computadoras de la red.

1 0 1 1 0 1 1 0 1 1 0 1 1 0 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 1 0 1 1 0 1 1 0 1 1 1 1 1 0 1

</ Niveles de seguridad para Redes.

Redes privadas virtuales (VPN)	Las VPN encriptan el tráfico de la red, lo que lo hace más seguro. Esto es especialmente importante cuando se usa una red Wi-Fi pública, ya que estas redes a menudo no son seguras.
Segmentación de red	La segmentación de red divide una red en segmentos más pequeños, lo que dificulta que los atacantes se muevan por la red si logran obtener acceso a un segmento.
Control de acceso basado en roles (RBAC)	El RBAC restringe el acceso a los recursos de la red en función del rol del usuario. Esto ayuda a garantizar que los usuarios solo puedan acceder a los recursos que necesitan para hacer su trabajo

1 0 1 1 0 1 1 0 1 1 0 1 1 0 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 1 0 1 1 0 1 1 0 1 1 1 1 1 0 1

</ Niveles de seguridad para Empresas.

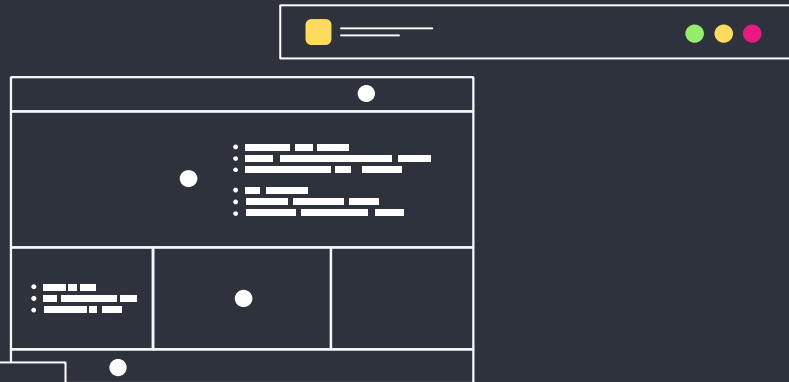
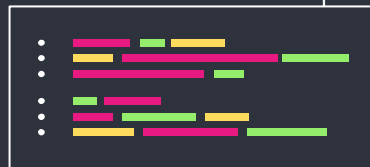
Políticas de seguridad	Las políticas de seguridad establecen las reglas y procedimientos que los empleados deben seguir para proteger la información y los sistemas de la empresa
Conciencia de seguridad	Es importante capacitar a los empleados sobre seguridad para que puedan identificar y evitar amenazas.
Pruebas de penetración	Las pruebas de penetración son simulaciones de ataques que pueden ayudar a identificar vulnerabilidades en los sistemas de la empresa.
Plan de respuesta a incidentes	Un plan de respuesta a incidentes describe los pasos que se deben seguir si ocurre una violación de seguridad.

1 0 1 1 0 1 1 0 1 1 0 1 1 0 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 1 0 1 1 0 1 1 0 1 1 1 1 1 0 1

</ Conclusiones

Guillermo Vladimir Flores Báez - 212767:

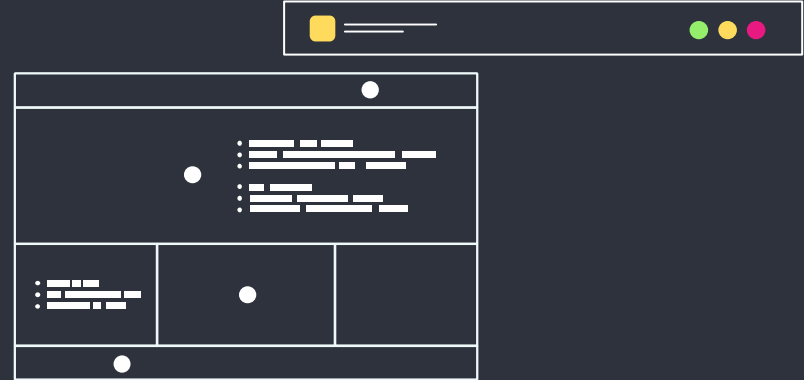
En conclusion, la seguridad es un tema importante que debe considerarse en todos los niveles, desde usuarios hasta grandes empresas. Al comprender las amenazas y tomar las medidas adecuadas para protegerse, puede ayudar a mantener sus sistemas y datos seguros.



</ Conclusiones

Jorge Isaac De León Pérez-1932783

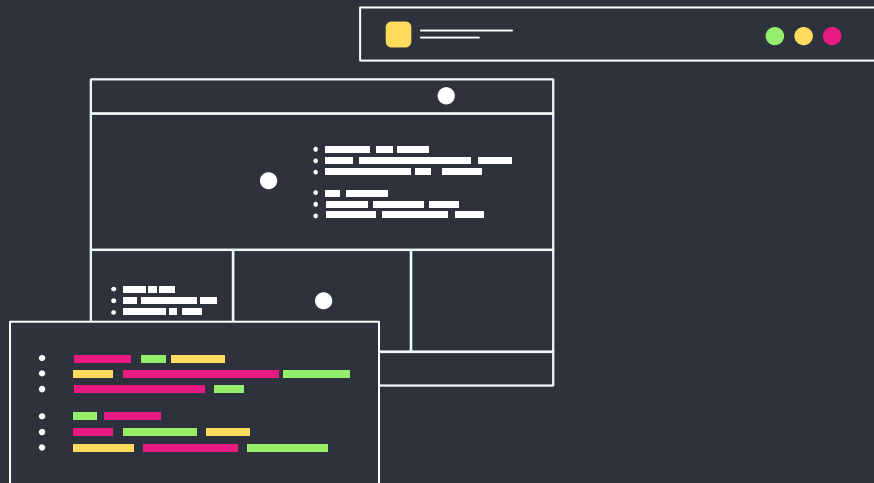
En conclusión, se debe tener mucho cuidado a la hora de la ciberseguridad, ya que algún tipo de malware que nos infecte la computadora podría hacer uso de los datos personales y podría robar información sobre cuentas bancarias y de más información y mas hoy en día debemos estar más atentos ya que no solo se puede ser vulnerado en una computadora sino también por medio de phishing etc. cada vez es más fácil aplicar medidas de seguridad.



</ Conclusiones

Diego Tristan Castro Franco-2109462

En conclusión, se debe tener un extremo cuidado con los virus en los dispositivos porque es algo que daña en el sistema operativo, archivos, documentos por eso se debe tener una copia de todo lo que tengamos en nuestra computadora y para prevenirlo hay que tener un antivirus o de lo contrario hasta podría un virus dañar nuestro disco duro y no podríamos utilizar nuestra computadora con frecuencia



</ Referencias

- Bessa, A. (21 de Abril de 2023). Alura Latam. Obtenido de <https://www.aluracursos.com/blog/tipos-de-autenticacion>
- Chavez, J. J. (29 de Octubre de 2022). Deltaprotect. Obtenido de <https://www.deltaprotect.com/blog/seguridad-de-la-red>
- IBM. (13 de Abril de 2021). IBM. Obtenido de <https://www.ibm.com/docs/es/i/7.4?topic=authority-security-levels>
- Microsoft. (s.f.). Microsoft. Obtenido de <https://www.microsoft.com/es-es/security/business/security-101/what-is-authentication>



- Colaboradores de Wikipedia. (2024, 10 abril). *Hacker*. Wikipedia, la Enciclopedia Libre. <https://es.m.wikipedia.org/wiki/Hacker>
- Belcic, I. (2023, 25 junio). *¿Qué es el malware y cómo protegerse de los ataques? ¿Qué Es el Malware y Cómo Protegerse de los Ataques?* <https://www.avast.com/es-es/c-malware>
- Szell, C. (2024, 2 febrero). Intrusos informáticos: Hackers y Crackers – Conecta Magazine. *Conecta Magazine*. <https://www.conectasoftware.com/magazine/hackers-crackers-no-galletas-definiendo-tipos-intrusos/>
- Norton. (2023, 6 marzo). *¿Qué es un virus informático?* <https://mx.norton.com/blog/malware/what-is-a-computer-virus#:~:text=En%20t%C3%A9rminos%20m%C3%A1s%20t%C3%A9cnicos%2C%20un,fin%20de%20ejecutar%20su%20c%C3%B3digo.>