

# Multitarea: Redes y seguridad en sistemas distribuidos

Actividad Fundamental 4.

Alonso Ramírez Páez ITS 2127873

Emiliano Garcia Montemayor ITS 2003905

Natividad Aron De León Ramírez IAS 1855134

Daniel Aharon Sánchez González ITS 1967943

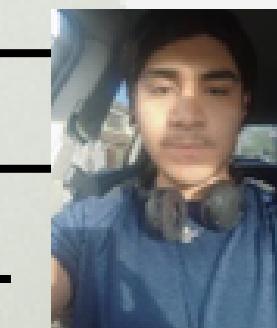
Carlos Gabriel Beas Gonzalez ITS 1940892

Javier López Pérez ITS 2127884

Rocío Guadalupe Sánchez Medrano IAS 1959446

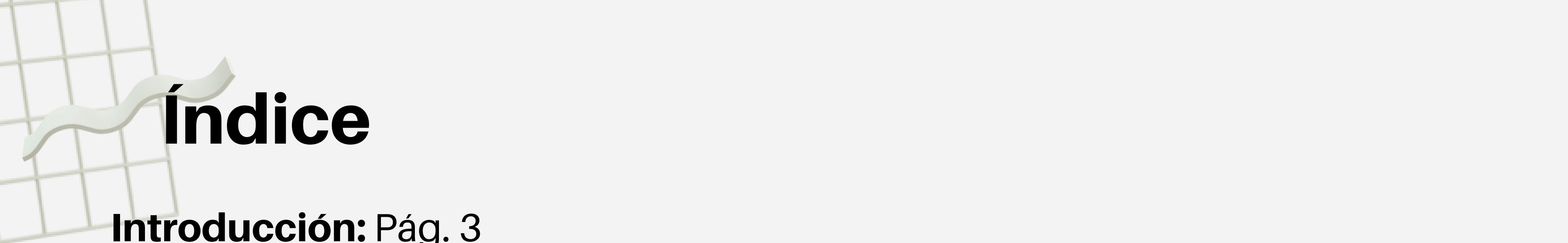
Sistemas Operativos.

Equipo 2



UANL FIME

A 22 de abril de 2024



# Índice

**Introducción:** Pág. 3

**Desarrollo:** Pág. 6

**Tipos de virus:** Pág. 7

**Tipos de intrusos:** Pág. 23

**Tipos de autentificaciones:** Pág. 31

**Niveles de seguridad:** Pág. 35

**Administración de riesgos:** Pág. 40

**Análisis de problemas y prevención de desastres:** Pág. 44

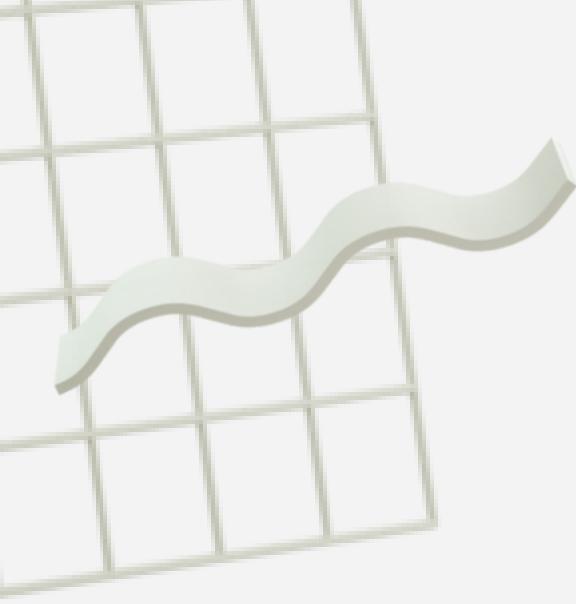
**Seguridad de hardware, software, archivos e información:** Pág. 50

**Conclusiones individuales:** Pág. 57

**Conclusión general:** Pág. 62

**Bibliografía:** Pág. 65





# **Introducción**

## **¿En qué consiste la seguridad informática?**





La seguridad informática se refiere a la protección de sistemas informáticos, redes y datos contra accesos no autorizados, uso indebido, daños o cualquier otra amenaza que pueda comprometer su integridad, confidencialidad o disponibilidad.



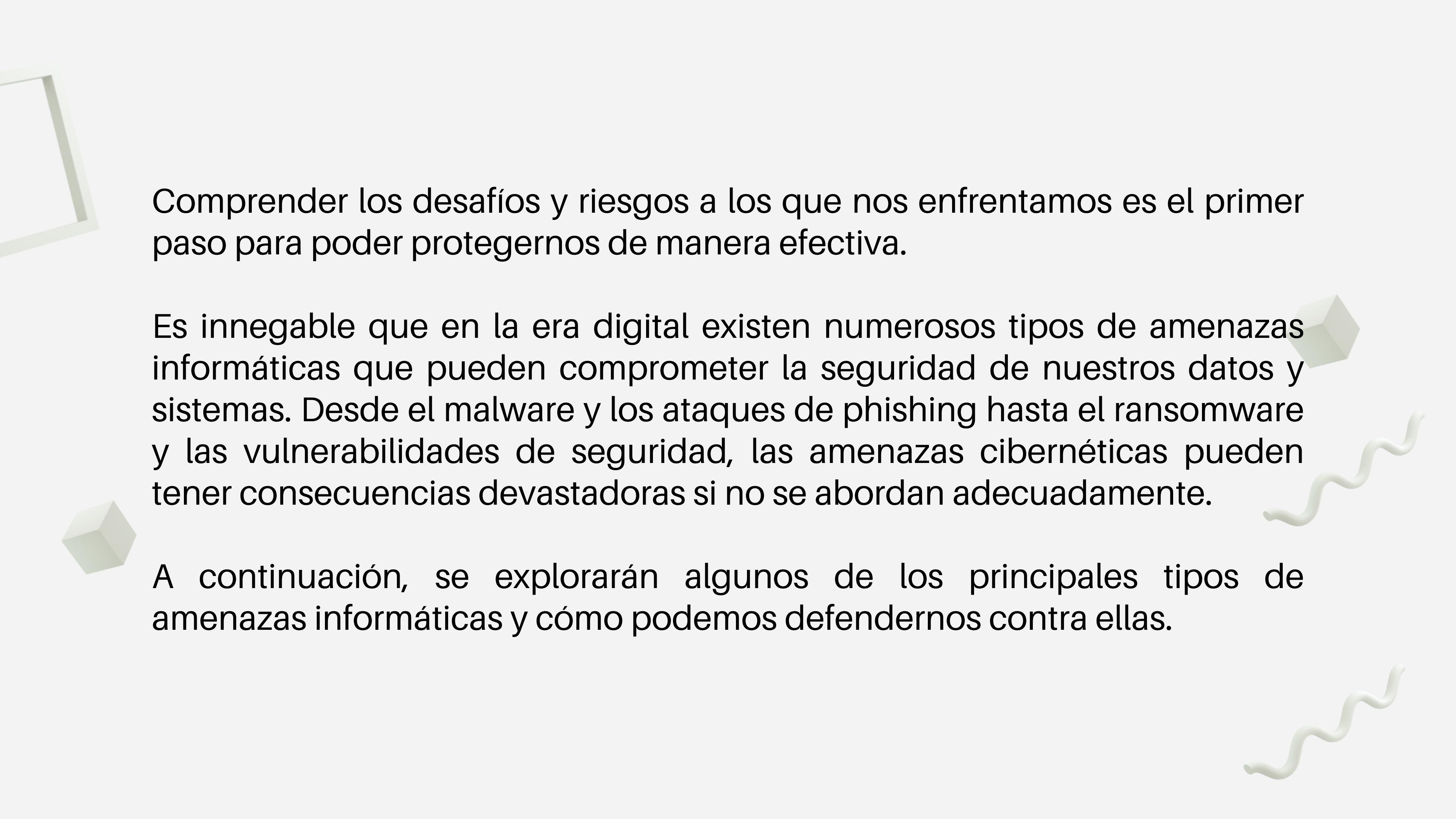
En la actualidad, la seguridad informática es de suma importancia debido al creciente riesgo de ciberataques y amenazas cibernéticas. Con la dependencia cada vez mayor de la tecnología en nuestra vida cotidiana y en el funcionamiento de las organizaciones, garantizar la seguridad de la información se ha convertido en una prioridad.



## Desarrollo

¿Qué tipos de amenazas existen, y  
cómo protegerse?





Comprender los desafíos y riesgos a los que nos enfrentamos es el primer paso para poder protegernos de manera efectiva.

Es innegable que en la era digital existen numerosos tipos de amenazas informáticas que pueden comprometer la seguridad de nuestros datos y sistemas. Desde el malware y los ataques de phishing hasta el ransomware y las vulnerabilidades de seguridad, las amenazas cibernéticas pueden tener consecuencias devastadoras si no se abordan adecuadamente.

A continuación, se explorarán algunos de los principales tipos de amenazas informáticas y cómo podemos defendernos contra ellas.

# Virus



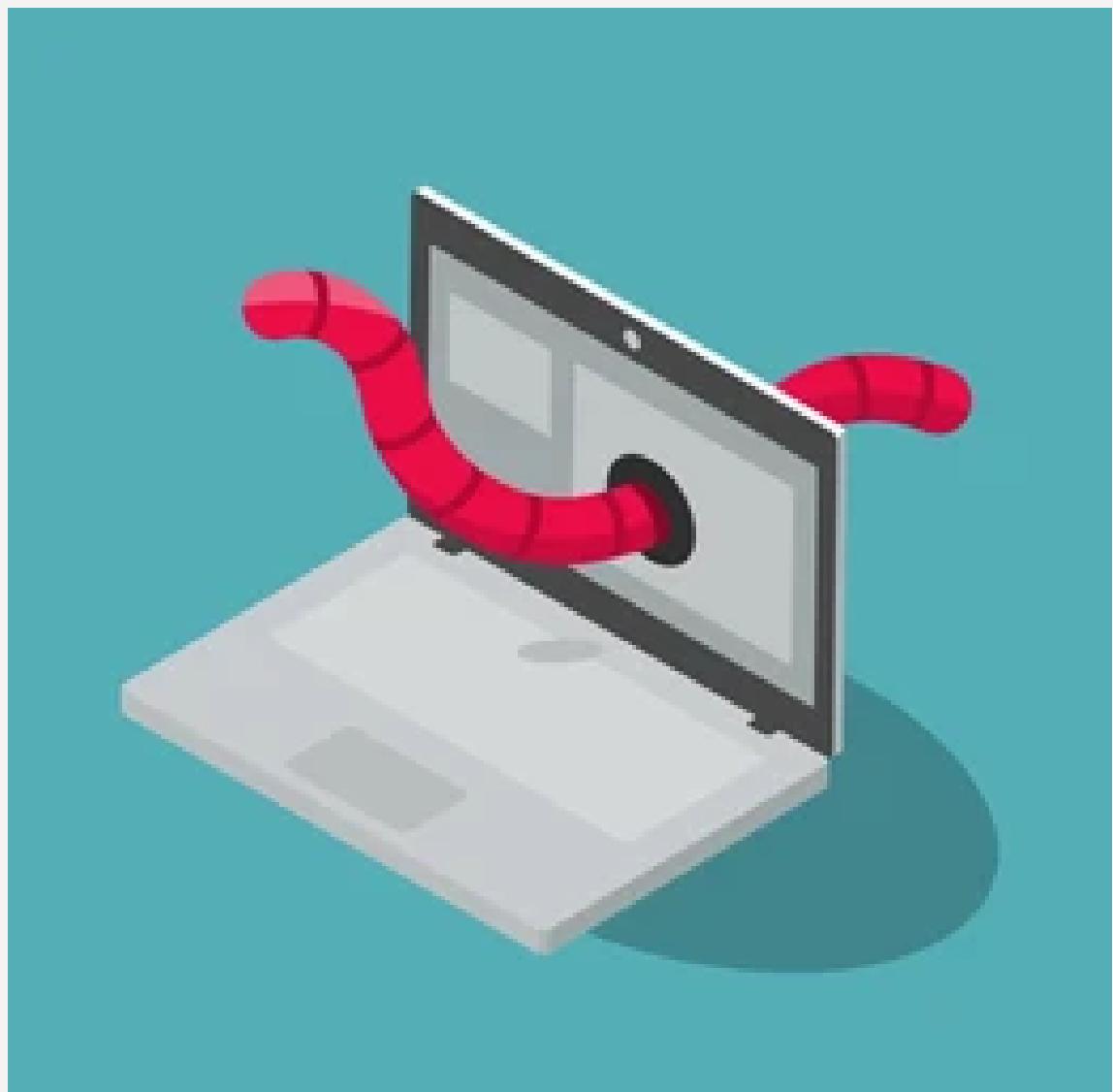
Un virus informático es un tipo de programa malicioso que altera el funcionamiento de un dispositivo y se propaga a otros. Se inserta en programas o documentos legítimos y puede causar daños, como dañar el software o destruir datos.

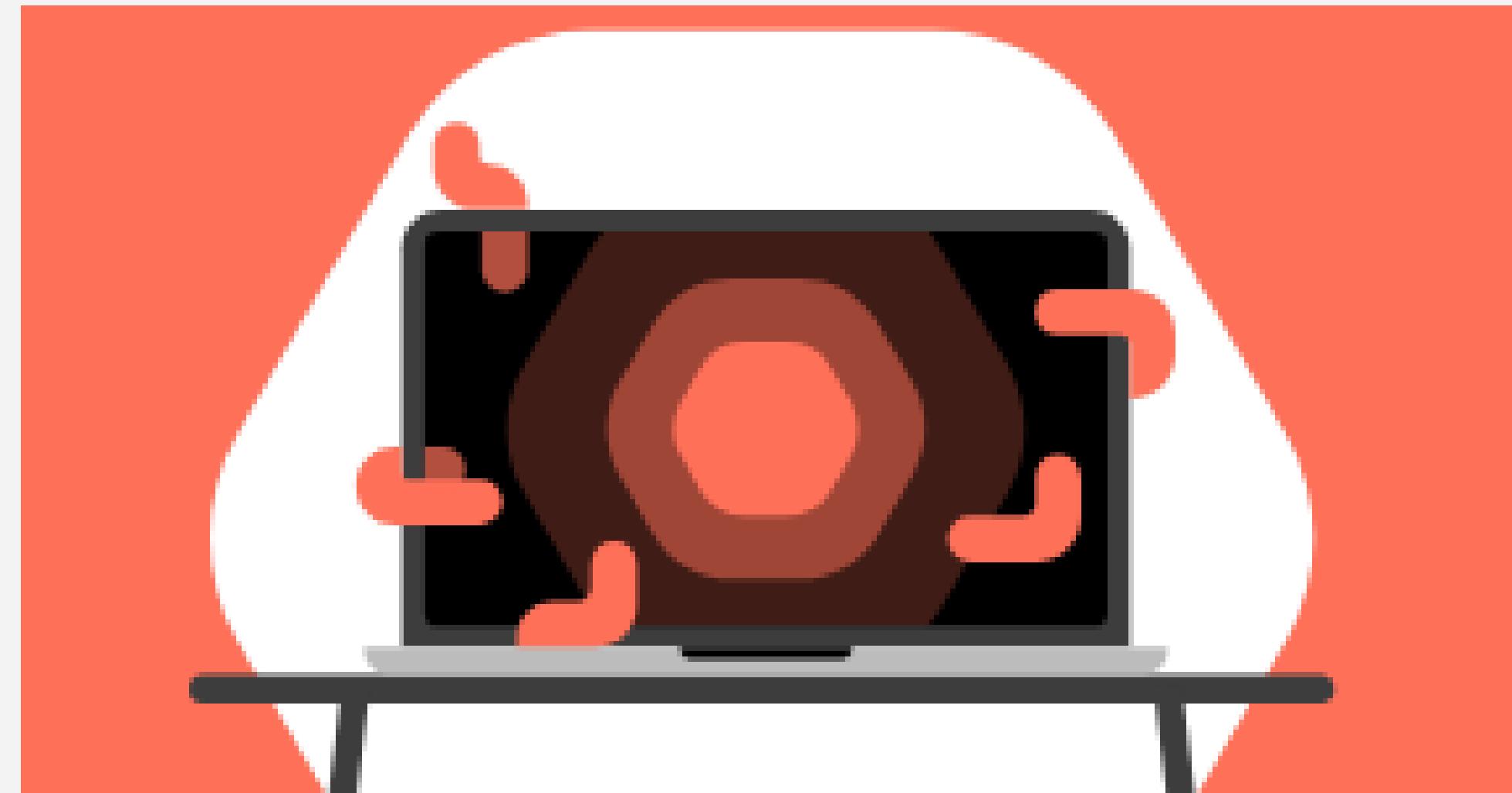
**Para protegerse es importante utilizar un software de seguridad completo.** Este tipo de software ofrece protección contra una variedad de amenazas, tanto existentes como nuevas. De la misma forma, proporciona una defensa más robusta y abarcativa.

# Gusanos

Los gusanos informáticos son programas maliciosos que se propagan de forma autónoma a través de redes informáticas, sin necesidad de intervención humana. **Se caracterizan por su capacidad de autoreplicación y rápida propagación**, lo que los hace especialmente peligrosos.

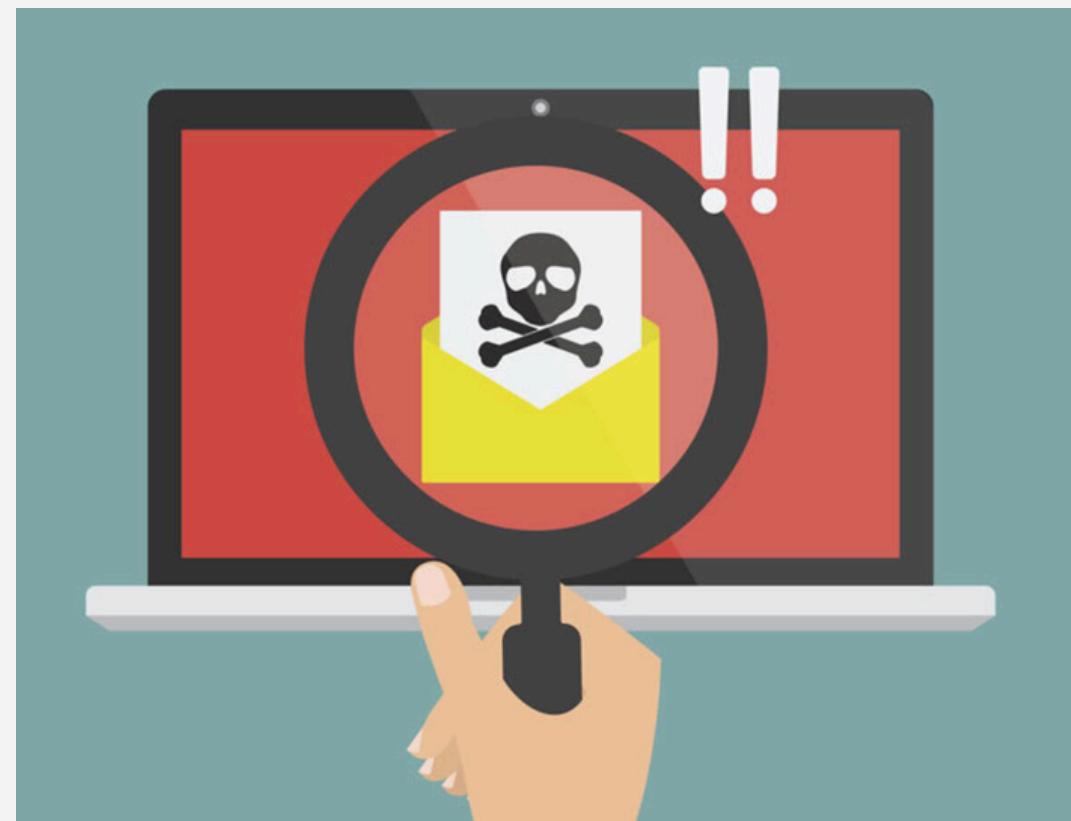
Pueden causar daños significativos, como la **eliminación de archivos o la corrupción de datos, y suelen aprovechar vulnerabilidades** en sistemas operativos objetivo. Algunos están diseñados para ocultarse y evitar la detección por parte del software de seguridad.





Es crucial protegerse contra ellos mediante la actualización de sistemas, el uso de software de seguridad y la promoción de la conciencia de seguridad entre los usuarios.

# Malware



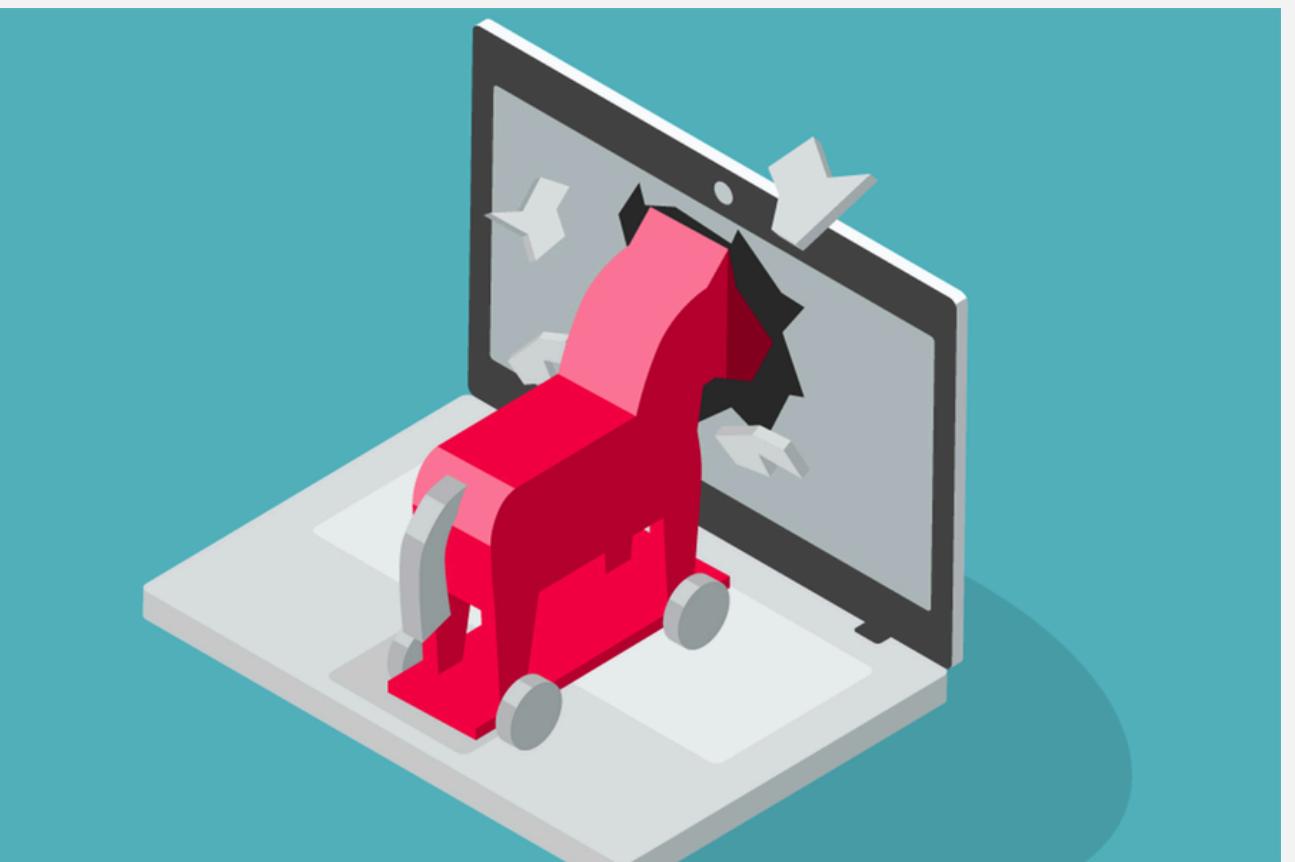
El malware es un término que hace referencia a cualquier programa malicioso diseñado para causar daño, robar información o realizar actividades no autorizadas en un sistema informático.

Puede presentarse de diversas formas y tener diferentes objetivos, pero su propósito común es **comprometer la seguridad y el funcionamiento de los sistemas informáticos y redes**.

# Troyanos

Los troyanos informáticos son programas maliciosos que se camuflan como software legítimo para engañar a los usuarios y obtener acceso no autorizado a sus sistemas. Requieren que el usuario los ejecute voluntariamente, generalmente sin darse cuenta de su naturaleza maliciosa.

Pueden hacerse pasar por aplicaciones populares o archivos multimedia, y se distribuyen a través de descargas de Internet o correos electrónicos. Una vez ejecutados, pueden robar información, instalar otro malware, o permitir el control remoto del sistema infectado.





Para protegerse contra los troyanos, es importante ser cauteloso al descargar software, mantener actualizado el software de seguridad y practicar la conciencia de seguridad en línea.

# Spyware



Tipo de software malicioso que recopila información sobre las actividades de un usuario en su dispositivo sin su consentimiento, comprometiendo su privacidad y seguridad.

Se distribuye a través de descargas de software gratuito, correos electrónicos con archivos adjuntos maliciosos, enlaces engañosos, entre otros.

Los datos recopilados pueden usarse para robar identidades, realizar fraudes financieros o enviar spam.

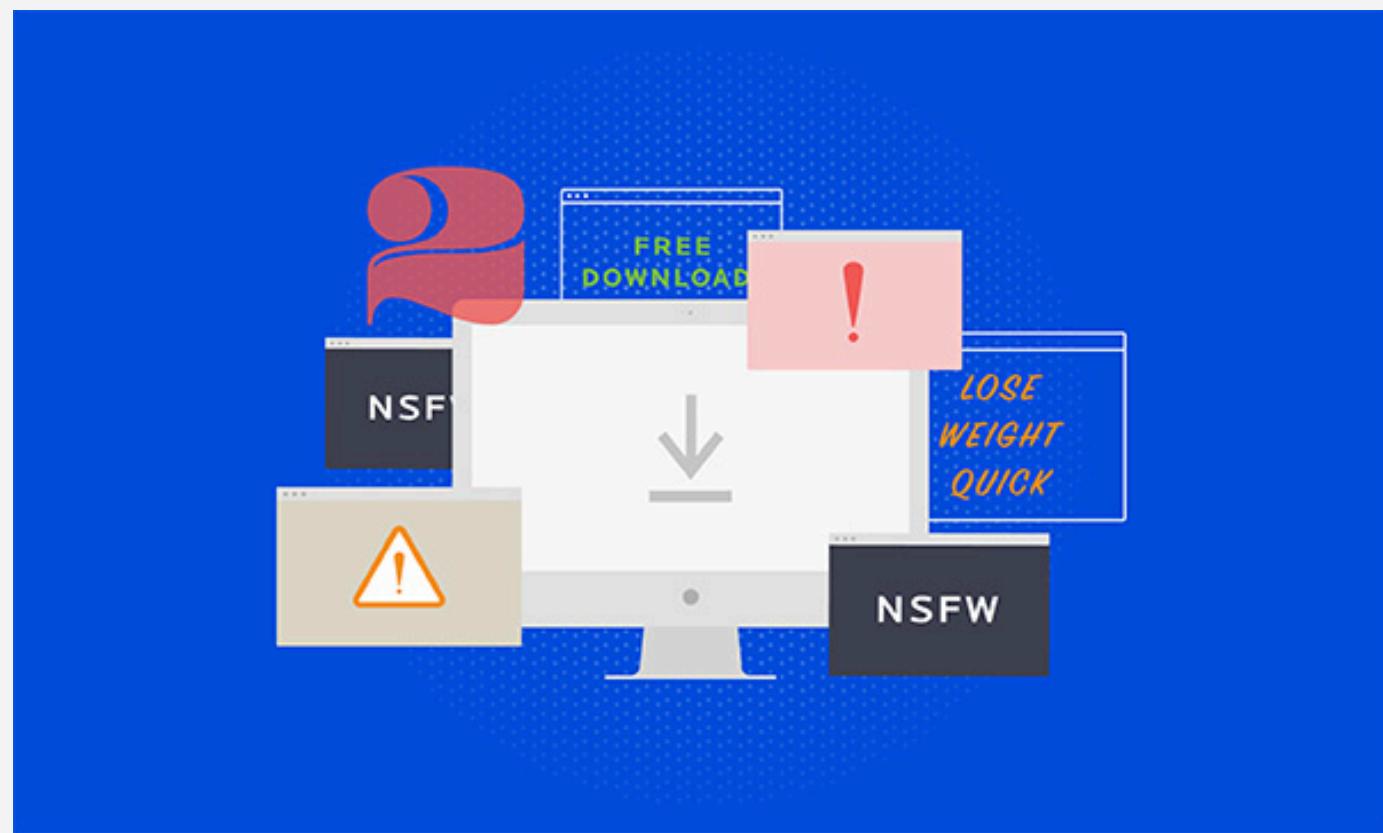


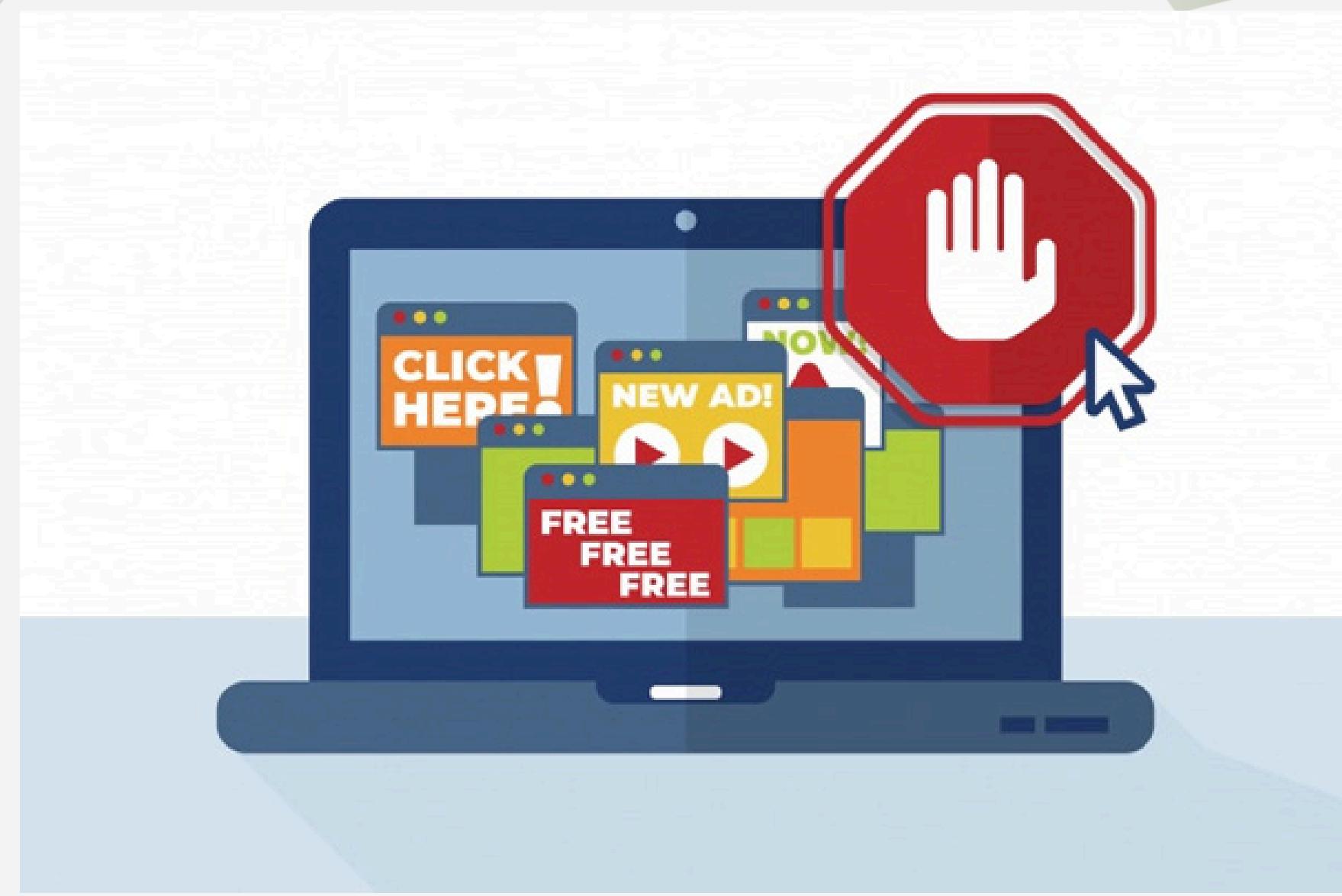
Para cuidarse, es crucial mantener actualizado el software de seguridad, utilizar software antivirus confiable, ser cauteloso al descargar software y educar a los usuarios sobre los riesgos del spyware.

# Adware

Software que muestra anuncios publicitarios no deseados en dispositivos informáticos, como computadoras, teléfonos inteligentes o tabletas. A diferencia de otros tipos de malware, el adware **no tiene la intención principal de dañar el sistema o robar datos del usuario, pero puede resultar molesto e intrusivo.**

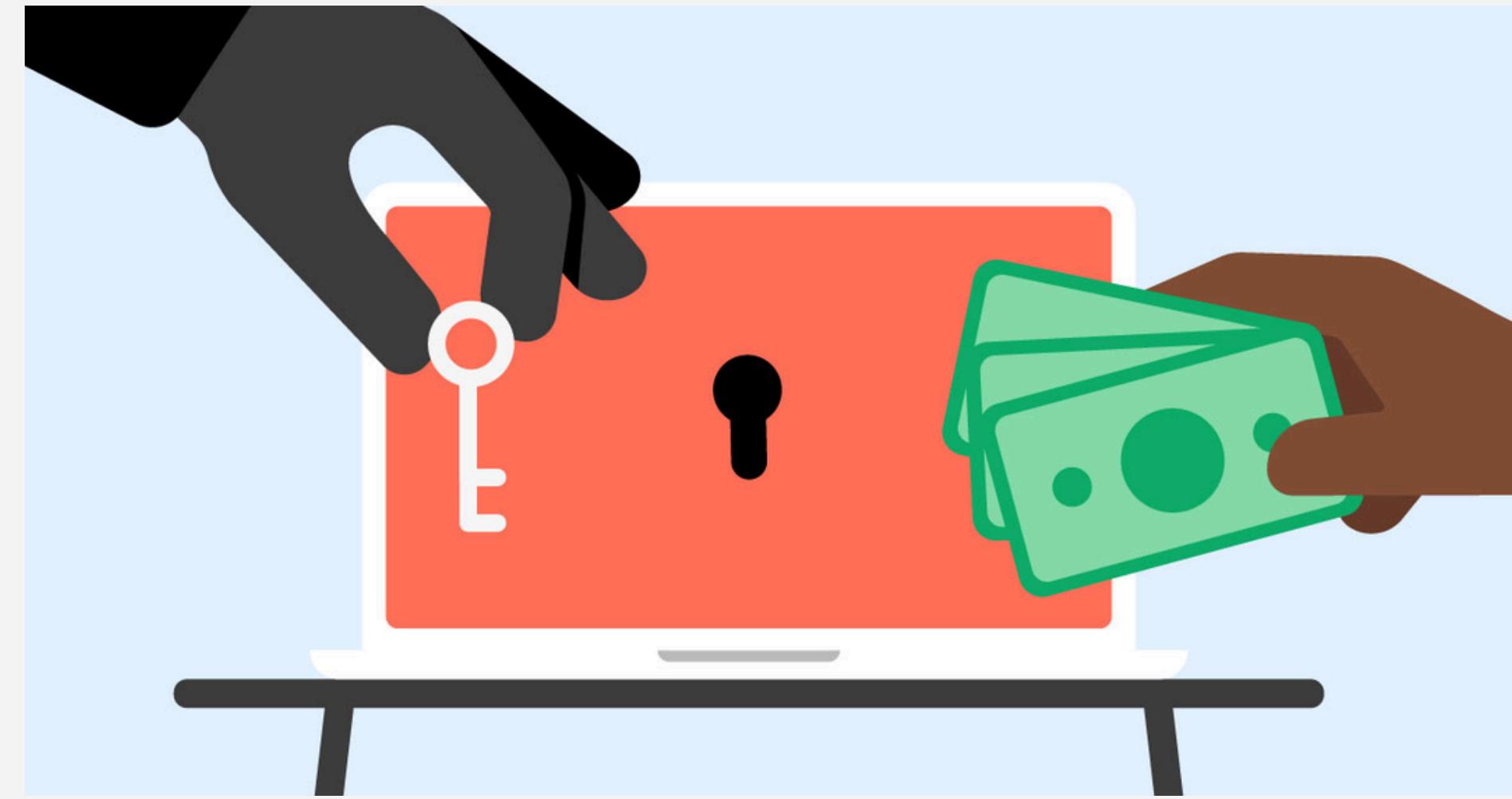
Se instala a menudo junto con otros programas gratuitos, consume recursos del sistema y puede ralentizar el rendimiento del dispositivo.





Aunque no suele ser tan peligroso como otros tipos de malware, la protección contra el adware requiere descargar software solo de fuentes confiables, leer detenidamente los términos de uso al instalar programas y utilizar software antivirus y antimalware actualizado.

# Ransomware

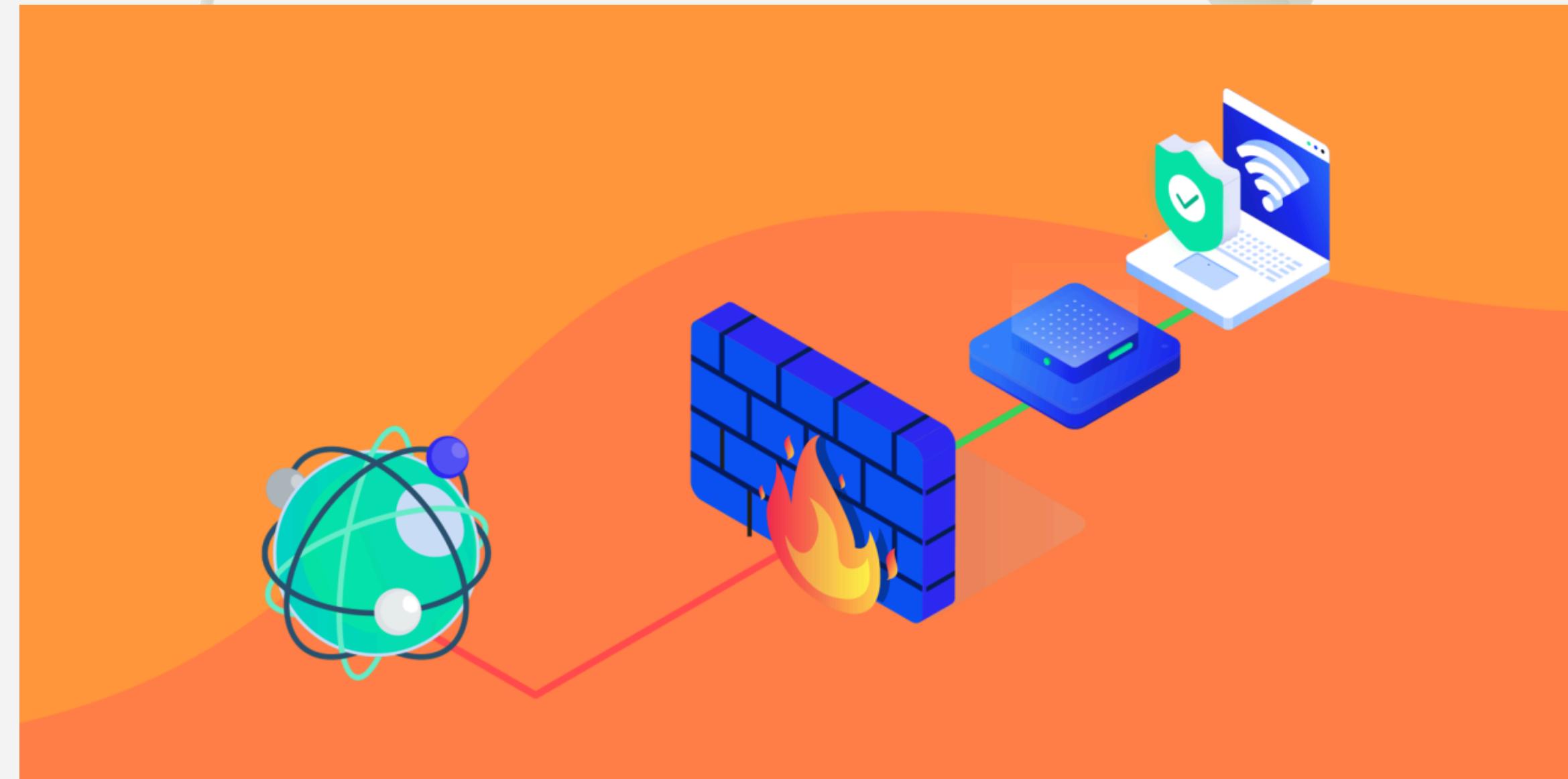


Malware que cifra los archivos en el sistema de la víctima y luego exige un pago de rescate, generalmente en criptomonedas, a cambio de proporcionar la clave de descifrado necesaria para restaurar el acceso a los archivos. Este tipo de ataque puede causar daños significativos al bloquear el acceso a datos críticos o confidenciales.

Algunas características clave del ransomware incluyen:



- Cifrado de archivos
- Notificación de rescate
- Demanda de pago en criptomonedas
- Plazos y amenazas
- Vectores de ataque
- Impacto devastador



Para protegerse contra el ransomware, es esencial mantener actualizado el software y los sistemas operativos, implementar medidas de seguridad como firewalls y antivirus, realizar copias de seguridad periódicas de los datos importantes y educar a los usuarios sobre prácticas de seguridad en línea.

# Pishing



El phishing es una táctica ciberdelictiva que busca obtener información confidencial mediante engaños y suplantación de identidad. Sus características clave son:

- **Correo electrónico fraudulento**
- **Engaño y manipulación con amenazas falsas o promesas de beneficios**
- **Enlaces y archivos maliciosos**
- **Consecuencias graves como pérdida de datos, robo de identidad, etc.**



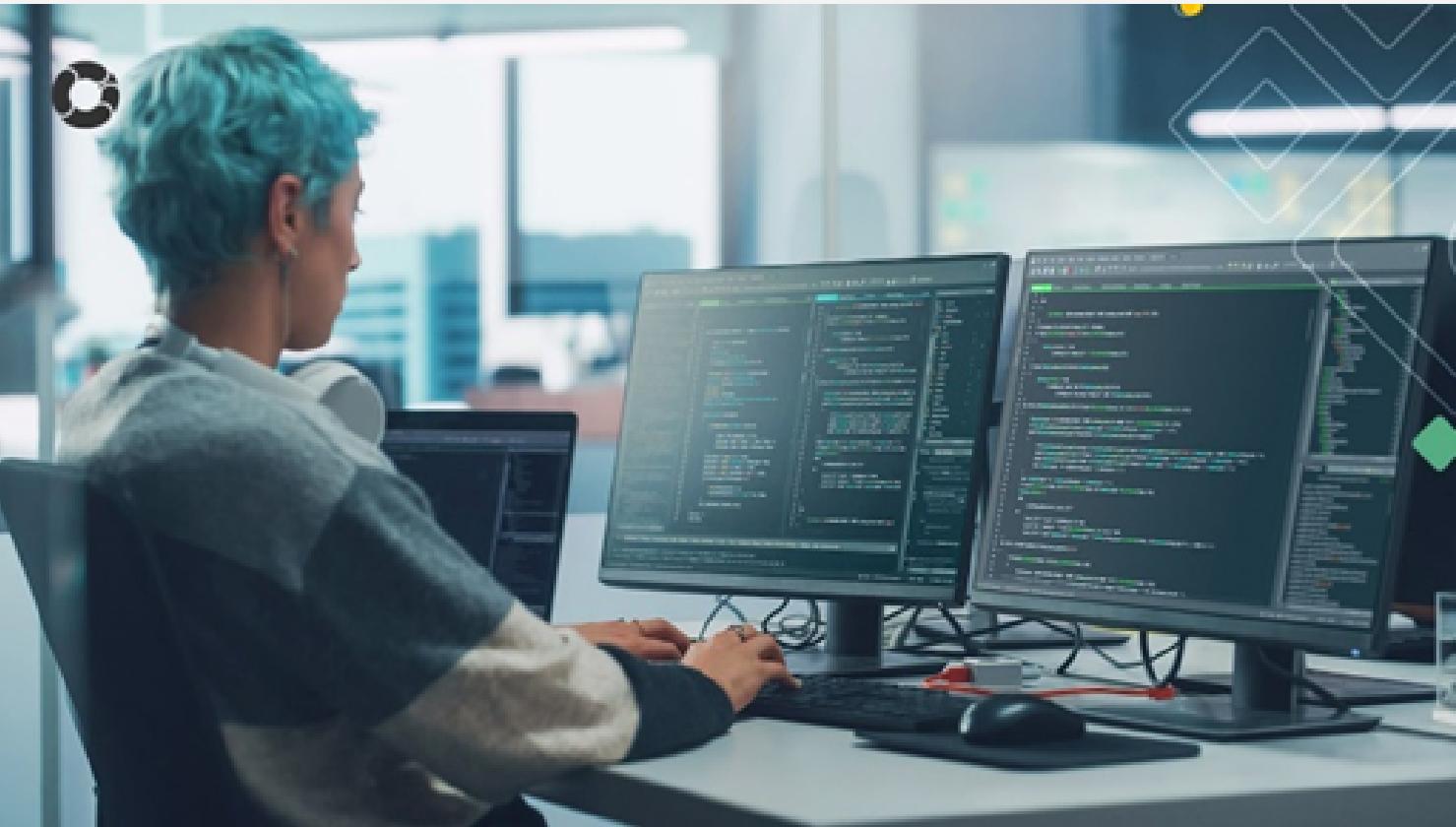
Para protegerse, se debe ser cauteloso con los correos electrónicos no solicitados, verificar la autenticidad de los remitentes y enlaces, evitar proporcionar información confidencial y mantener actualizado el software de seguridad

# Tipos de intrusos

Los intrusos informáticos son individuos o grupos que buscan comprometer la seguridad de sistemas informáticos con diversos objetivos, que van desde el robo de información hasta el sabotaje.

Estos intrusos pueden ser clasificados en diferentes tipos según sus intenciones y métodos de ataque. Entender quiénes son y cómo operan es crucial para implementar medidas efectivas de seguridad informática.

# Hacker



Los hackers son individuos con habilidades técnicas avanzadas que manipulan sistemas informáticos y redes por diversas razones.

Inicialmente, los hackers valoraban la programación como una forma de arte y abogaban por el libre flujo de información, creando lo que se conoce como Ética Hacker.

Figuras modernas como Richard Stallman y Steve Wozniak han contribuido significativamente al desarrollo de tecnologías clave como sistemas operativos y computadoras personales.

Los crackers son ciberdelincuentes que emplean habilidades técnicas para comprometer sistemas con intenciones maliciosas, como robo de datos o fraude.

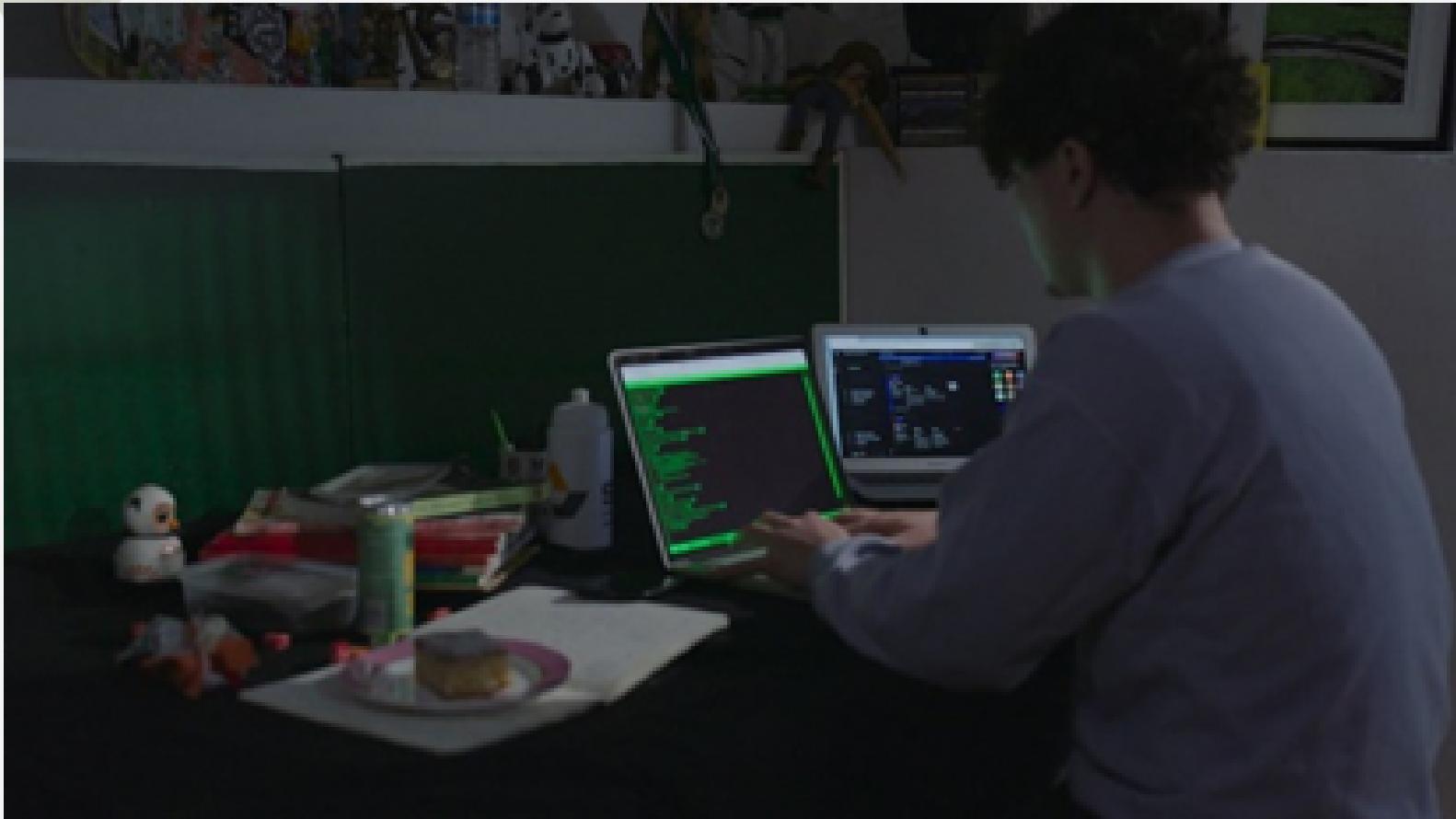
A diferencia de los hackers, que siguen la Ética Hacker y valoran el conocimiento, los crackers son vistos como individuos menos talentosos que simplemente hacen uso de herramientas sin entender su funcionamiento.

Mientras los hackers tienen un enfoque más ético y creativo en su actividad, los crackers se centran en actividades ilegales y a menudo buscan beneficios financieros rápidos.

# Cracker



# Script Kiddies



Son individuos con habilidades técnicas limitadas que utilizan herramientas y scripts predefinidos, desarrollados por otros, para llevar a cabo ataques informáticos sin comprender completamente el funcionamiento de las técnicas que utilizan.

A menudo, aprovechan herramientas y documentación disponible en Internet, pero carecen de habilidades para desarrollar sus propias herramientas o entender los aspectos más profundos de la seguridad informática. Aunque pueden causar problemas, suelen ser descuidados en sus acciones y dejan huellas digitales fácilmente identificables.

Representan una amenaza significativa para la seguridad informática de una organización, ya que tienen acceso legítimo a los sistemas y redes y pueden abusar de este acceso para actividades maliciosas.

Pueden ser empleados, contratistas o socios comerciales con privilegios de acceso.

Las contramedidas incluyen la instalación de sistemas de detección y alarma, así como la implementación de medidas físicas de seguridad.

## Intrusos internos



# Hacktivistas



El hacktivismo combina la protesta política con la piratería informática en el ciberespacio, buscando influir tanto en la vida virtual como en la realidad fuera de línea.

Surge de la intersección entre el hacking, las sociedades digitales y la protesta social moderna.

Los hacktivistas buscan garantizar la libertad y el acceso a la información en Internet, creando herramientas para mantener el ciberespacio como un lugar de información libre y seguro.



Este movimiento refleja una política informativa que fluye con la virtualidad y desafía la censura estatal en línea.

Los actores respaldados por el estado, como los gobiernos y agencias de inteligencia, representan una seria amenaza en ciberseguridad debido a sus amplios recursos y herramientas avanzadas.

Realizan operaciones ciberneticas con diversos objetivos políticos, militares o económicos, como el espionaje y la desinformación.

Para protegerse contra ellos, las organizaciones y gobiernos deben implementar medidas avanzadas de seguridad, fortalecer la infraestructura crítica y cooperar internacionalmente en ciberseguridad.

# Estado-Nación o actores respaldados por el estado

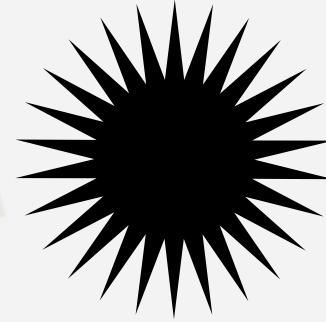


# Tipos de autentificaciones

La confidencialidad intenta que la información solo sea utilizada por las personas o máquinas debidamente autorizadas. Para garantizar la confidencialidad necesitamos disponer de tres tipos de mecanismos:

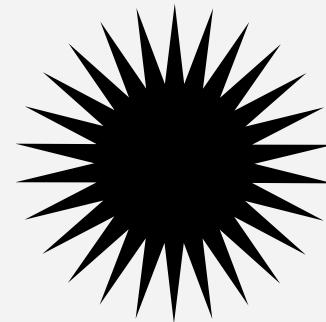
- Autenticación
- Autorización
- Cifrado





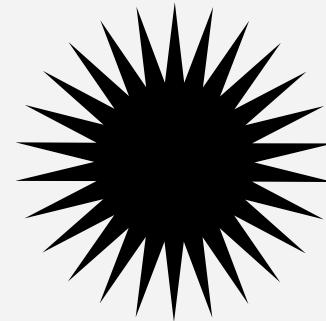
## Autenticación:

La autenticación intenta confirmar que una persona o máquina es quien dice ser, que no estamos hablando con un impostor.



Autorización. Una vez autenticado, los distintos usuarios de la información tendrán distintos privilegios sobre ella.

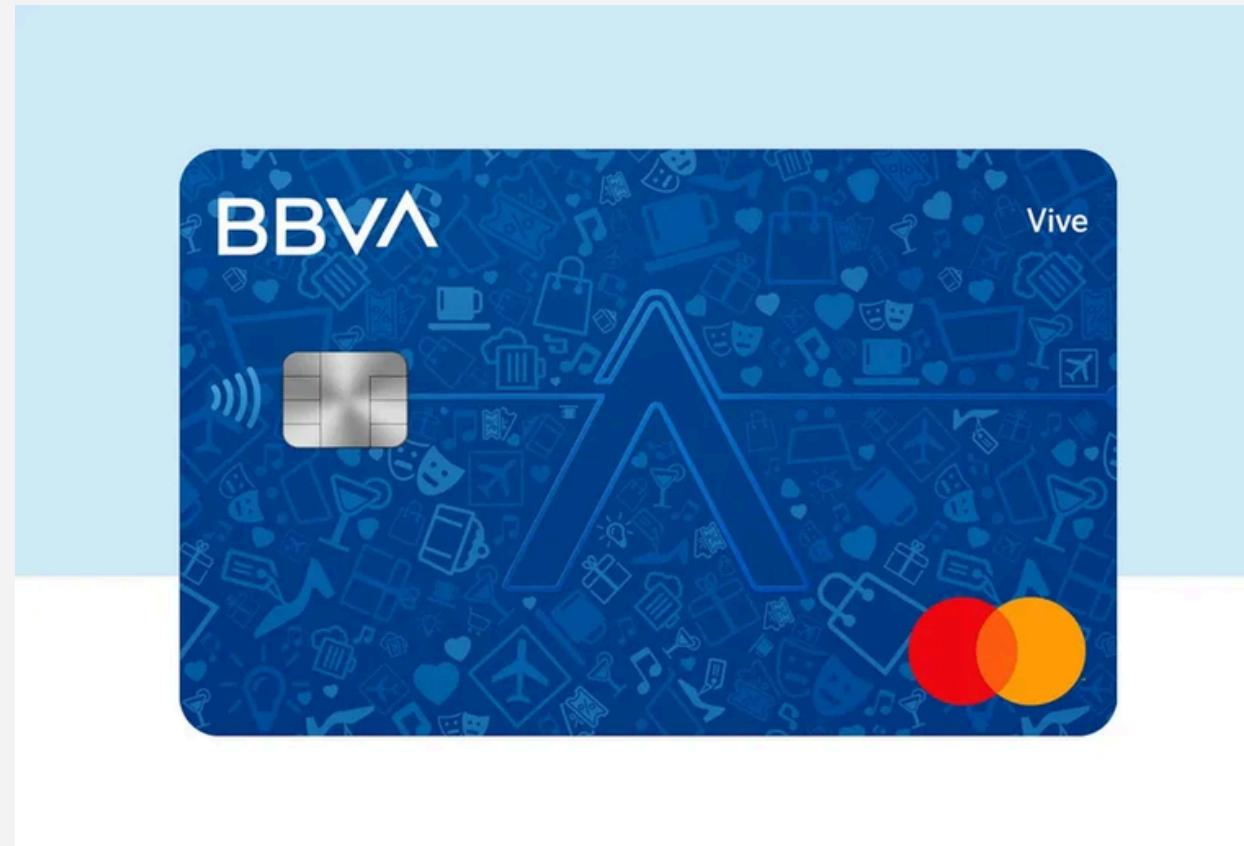
Básicamente dos: solo lectura, o lectura y modificación.



Cifrado. La información estará cifrada para que sea inútil para cualquiera que no supere la autenticación.



# Ejemplos del mundo real



Para entrar a un estadio de fútbol se necesita una entrada (autenticación); pero unos irán a tribuna y otros a un palco VIP (autorización).

Para sacar dinero de un cajero necesitas una tarjeta y el PIN de esa tarjeta (autenticación). Al recoger un envío certificado necesitas llevar el DNI, para que comprueben que eres tú (autenticación).

En los parques temáticos hay que llevar una entrada (autenticación) y, si pagas un poco más, tienes un fast-pass para no hacer cola en las atracciones (autorización). El objetivo de la integridad es que los datos queden almacenados tal y como espera el usuario: que no sean alterados sin su consentimiento. Un ejemplo sería el identificador de la cuenta bancaria, que tiene cuatro grupos de números:

La autenticación es especialmente importante en temas de seguridad. Debemos estar muy seguros de la identidad de la persona o sistema que solicita acceder a nuestra información. Un esquema muy utilizado para analizar la autenticación es clasificar las medidas adoptadas según tres criterios:

Algo que sabes. Para acceder al sistema necesitas conocer alguna palabra secreta: la típica contraseña.

Algo que tienes. En este caso es imprescindible aportar algún elemento material: generalmente una tarjeta.

Algo que eres. El sistema solicita reconocer alguna característica física del individuo (biometría): huella dactilar, escáner de retina, reconocimiento de voz, etc.



# Niveles de seguridad

La seguridad informática es una preocupación cada vez más importante en el mundo digital actual. A medida que la tecnología avanza y las amenazas ciberneticas se vuelven más sofisticadas, es crucial comprender y aplicar diferentes niveles de seguridad para proteger la información y los sistemas.

En este contexto, se distinguen tres niveles principales de seguridad: a nivel de usuario, a nivel de redes y a nivel de empresas y organizaciones. Cada uno de estos niveles aborda diferentes aspectos.

# Nivel de seguridad del usuario

A nivel de usuario, la seguridad informática se centra en proteger la información personal y los dispositivos utilizados en la vida diaria.



Los usuarios deben tomar medidas para proteger sus contraseñas, mantener su software actualizado y ser cautelosos al interactuar con correos electrónicos y sitios web sospechosos.

El uso de software antivirus y la educación sobre prácticas de seguridad en línea son fundamentales para prevenir ataques cibernéticos y proteger la privacidad.

# Nivel de seguridad de red

A nivel de redes, la seguridad informática implica proteger la infraestructura de comunicaciones, como routers, switches y servidores, así como los datos que se transmiten a través de ellas.

Se utilizan medidas como firewalls, cifrado de datos, autenticación de usuarios y detección de intrusiones para garantizar la integridad, confidencialidad y disponibilidad de la red.

Es importante no dejarse llevar por la confianza excesiva en la seguridad de la red y mantener una actitud vigilante y proactiva frente a posibles amenazas.



# Nivel de seguridad empresarial



A nivel empresarial, la seguridad informática es fundamental para proteger los activos digitales, la información confidencial y la reputación de la empresa.

Esto implica implementar políticas y procedimientos de seguridad, utilizar herramientas avanzadas de protección y capacitar al personal en prácticas de seguridad cibernética.

Además, las empresas deben realizar evaluaciones regulares de riesgos y estar preparadas para responder de manera efectiva a incidentes de seguridad.



La colaboración con expertos en ciberseguridad y el seguimiento de las mejores prácticas del sector son clave para mantener la integridad y la continuidad del negocio.

# ¿Qué es la administración de riesgos?

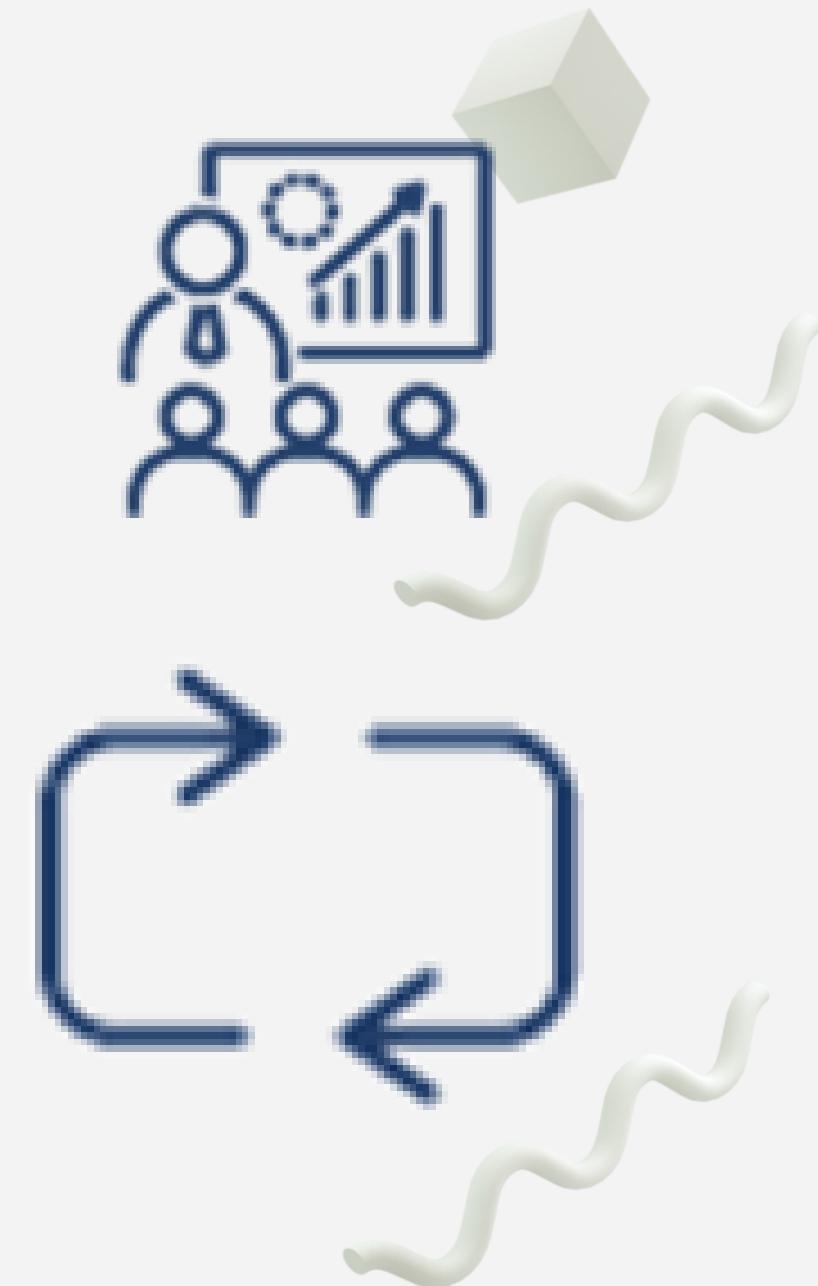


La administración de riesgos es un enfoque sistemático para gestionar las amenazas que pueden comprometer los activos de información de una organización. Estas amenazas incluyen desde ciberataques hasta incumplimientos normativos, representando riesgos para la continuidad operativa, la estabilidad financiera y la reputación de la organización.

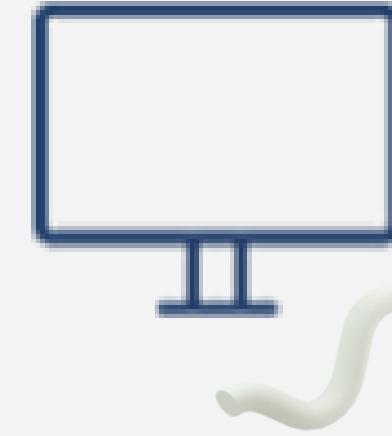
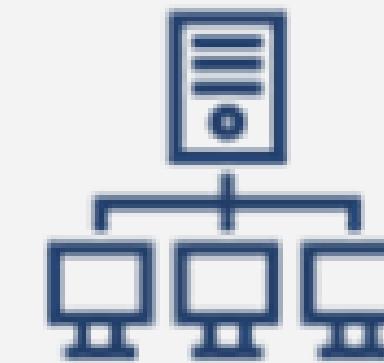
# Proceso de administración de riesgos

El Marco de Ciberseguridad del NIST ofrece pautas para comprender, gestionar y reducir los riesgos de ciberseguridad en las organizaciones. Se compone de cinco pasos:

- 1. Identificación:** haga una lista de todos los equipos, programas software y datos que use, incluyendo computadoras portátiles, teléfonos inteligentes, tablets y dispositivos utilizados en puntos de venta.
- 2. Protección:** controlar el acceso a la red y los dispositivos, utilizar programas de seguridad, cifrar datos, realizar copias de seguridad, actualizar regularmente la seguridad y capacitar al personal en ciberseguridad.



- 3. Detección:** monitorear la red y los dispositivos para detectar acceso no autorizado, revisar la red en busca de conexiones no autorizadas y investigar actividades inusuales.
- 4. Respuesta:** implementar un plan de notificación, mantener las operaciones comerciales, reportar el ataque, investigar y contener el ataque, actualizar las políticas de ciberseguridad y prepararse para eventos inesperados.
- 5. Recuperación:** reparar y restaurar equipos y partes de la red afectados, mantener informados a los empleados y clientes sobre las actividades de respuesta y recuperación.



# Importancia de la gestión proactiva de riesgos

La gestión proactiva de riesgos es esencial en la actualidad, ya que nos permite identificar errores y aciertos que podrían afectar el éxito de los proyectos y de la organización.

Ayuda a establecer sistemas de alerta temprana, priorizar lo que debe abordarse primero y desarrollar estrategias para alinear los riesgos con la cultura organizacional.

Además, permite resolver problemas antes de que ocurran y establecer las mejores prácticas para el futuro.

# Análisis de problemas y prevención de desastres

## 1. Identificación de posibles problemas de seguridad

Los problemas de seguridad en la seguridad informática son situaciones, debilidades o brechas que pueden ser explotadas por individuos malintencionados o programas maliciosos para comprometer la confidencialidad, integridad o disponibilidad de los sistemas y datos de una organización. Estos problemas pueden surgir por diversas razones, incluyendo fallos en la configuración, errores de diseño, falta de actualizaciones de seguridad, acciones de usuarios no autorizados, o incluso vulnerabilidades inherentes en el software o hardware utilizado.

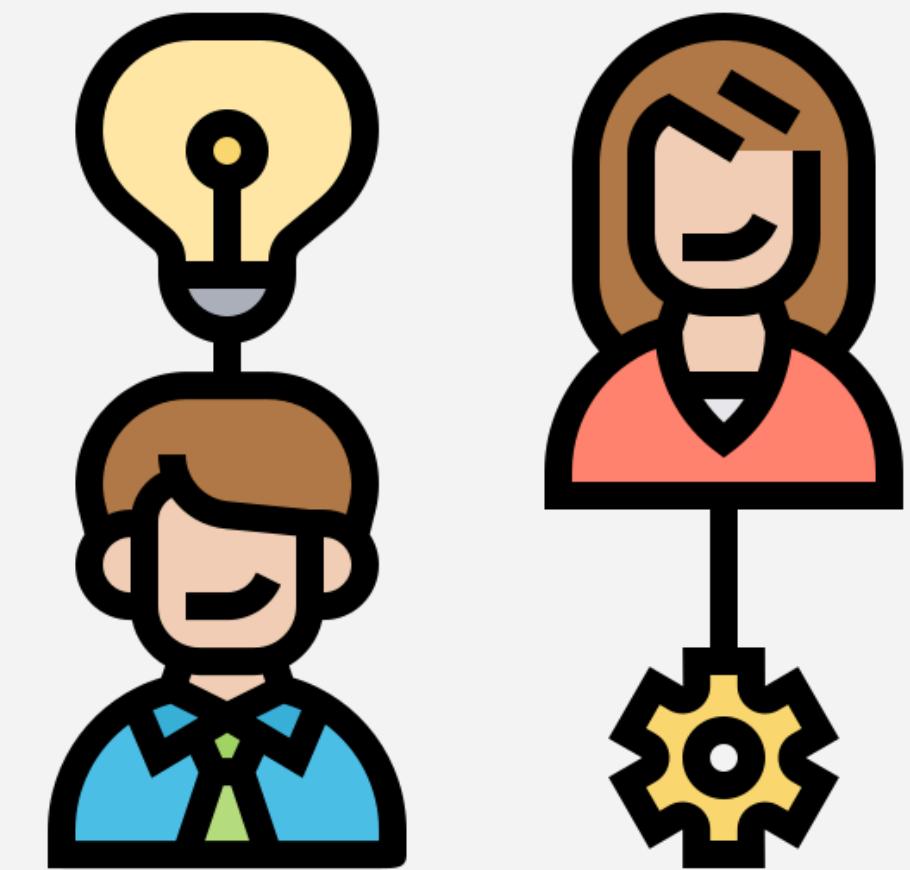
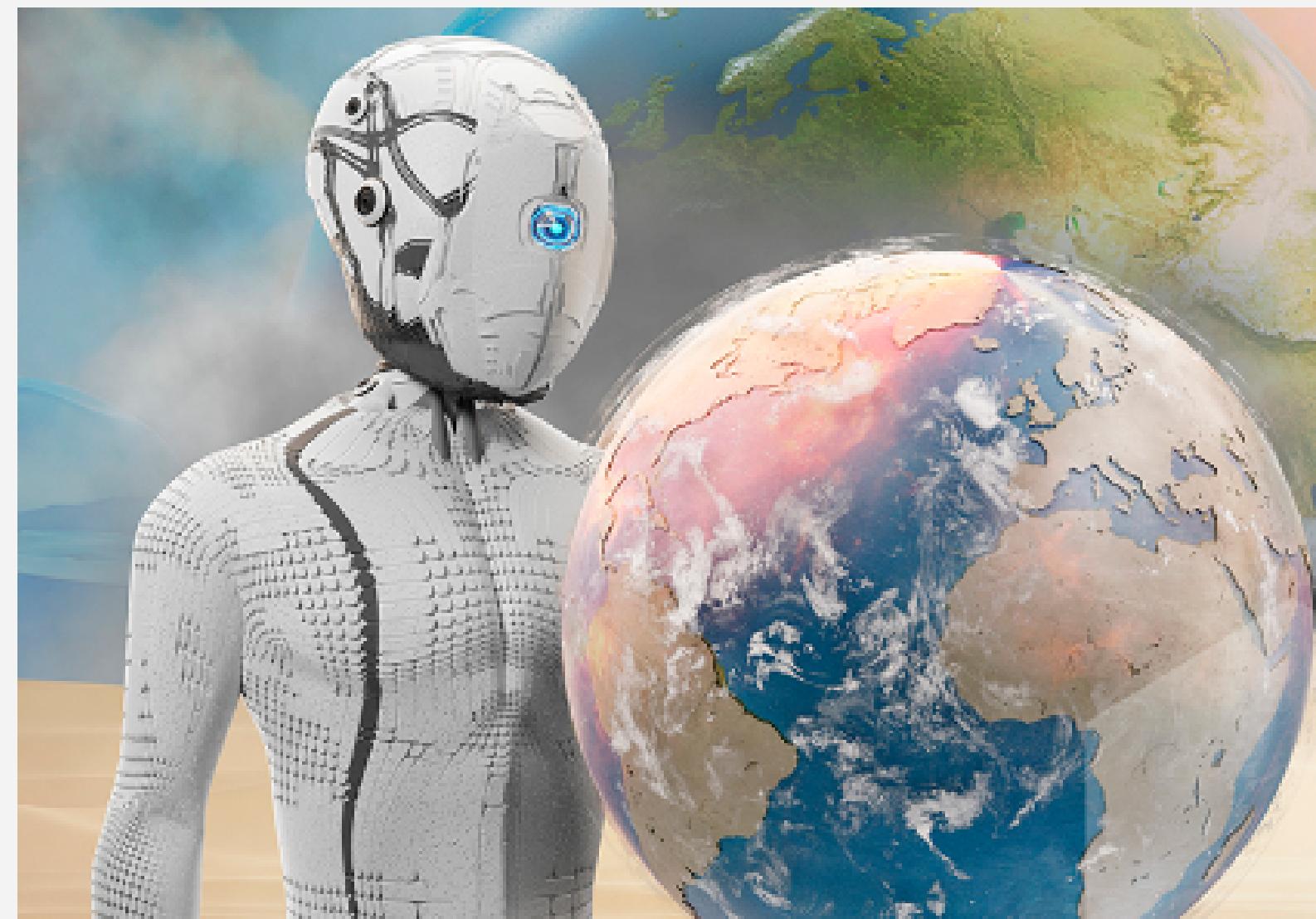


Para identificar los posibles problemas de seguridad implicará un proceso de evaluación constante y proactivo para detectar vulnerabilidades y amenazas potenciales. Es por eso que debemos de llevar a cabo los siguientes puntos si queremos lograr dicha tarea:

- **Realizar auditorías de seguridad:** Realizar auditorías regulares de seguridad para evaluar el estado de la infraestructura, los sistemas y las aplicaciones en busca de posibles brechas o vulnerabilidades.
- **Aplicar un análisis de vulnerabilidades:** Utilizar herramientas de escaneo de vulnerabilidades para identificar debilidades en sistemas y aplicaciones, como configuraciones incorrectas, software desactualizado o puertos abiertos.
- **Efectuar un monitoreo de registros:** Analizar registros de actividad y eventos de seguridad para detectar comportamientos anómalos o actividades sospechosas que puedan indicar una intrusión o un ataque en curso.

## 2. Estrategia de prevención y mitigación de desastres

Prevenir riesgos laborales debe entenderse cómo la manera de mejorar la productividad dentro de tu empresa, pero sobre todo de cuidar lo más valioso: el talento humano. Lamentablemente la mayoría de las empresas en nuestro país enfocan sus recursos exclusivamente a mantener o acrecentar su infraestructura dejando a un lado lo más valioso que tienen como organización: el talento humano.





Está demostrado que cuidar la salud, bienestar y condiciones de trabajo no solo ayuda a lograr compromiso y calidad en el desempeño de las diferentes actividades del equipo, sino que nos lleva a prevenir aquellos riesgos que en un caso extremo podrían causar la quiebra de nuestro negocio. Según datos de la Organización Internacional del Trabajo actualmente 2.3 millones de trabajadores fallecen cada año por accidentes y enfermedades. Desde el punto de vista económico esto tiene grandes repercusiones ya que representa alrededor de cuatro puntos del PIB mundial.

A partir de una importante consultoría aquí a continuación se presentarán cinco consejos que se deberían de tomar en cuenta para cuidar a una empresa de un riesgo, pero sobre todo a los empleados y colaboradores de cualquier tipo de desastre:

- **Crear una atmósfera segura para todos.** Lo primero es establecer las responsabilidades y compromisos que tiene cada miembro de la organización. Es indispensable el involucramiento de todos los integrantes y el asesoramiento en expertos en higiene y seguridad laboral.
- **Dimensionar riesgos.** Identificar los alcances e implicaciones de cada error que se cometa. Despertar conciencia. La idea no es iniciar una cacería de brujas en contra de los culpables sino evitar que siquiera existan situaciones de riesgo para todos. A partir de esto cada puesto contara con medidas de seguridad especiales dentro de su programa.
- **Capacitar para situaciones de emergencia.** No solo hablamos de la capacitación sobre las actividades básicas del puesto sino de las medidas a seguir ante cualquier percance. Mantener la calma será lo primero, pero ciertamente será más fácil cuando se sepa sobre primeros auxilios y de los diferentes manuales de acción ante cada situación atípica.

- **Dar mantenimiento a máquinas y herramientas que se manejen diariamente.** Olvidarse de esto es más común de lo que parece, pues confiarnos en la vida útil de los equipos no es buena idea. Las revisiones continuas tanto de personal interno como externo nos ayudaran a tener mayor tranquilidad en las operaciones de la empresa.



- **Gestión de parches.** Mantener actualizados los sistemas y aplicaciones con los últimos parches de seguridad para corregir vulnerabilidades conocidas y reducir el riesgo de explotación por parte de los atacantes.



# Seguridad de hardware, software, archivos e información.

## Seguridad de hardware

La seguridad de hardware se refiere a las medidas tomadas para proteger los componentes físicos de los sistemas informáticos y dispositivos electrónicos, así como los datos y procesos que se ejecutan en ellos. Los riesgos en la seguridad de hardware incluyen acceso físico no autorizado, manipulación o alteración de componentes, y amenazas en el firmware o periféricos.

# Métodos para proteger el hardware



**Uso de contraseñas o autenticación biométrica:** Protege el acceso a los dispositivos mediante contraseñas seguras o métodos biométricos como huellas dactilares o reconocimiento facial.

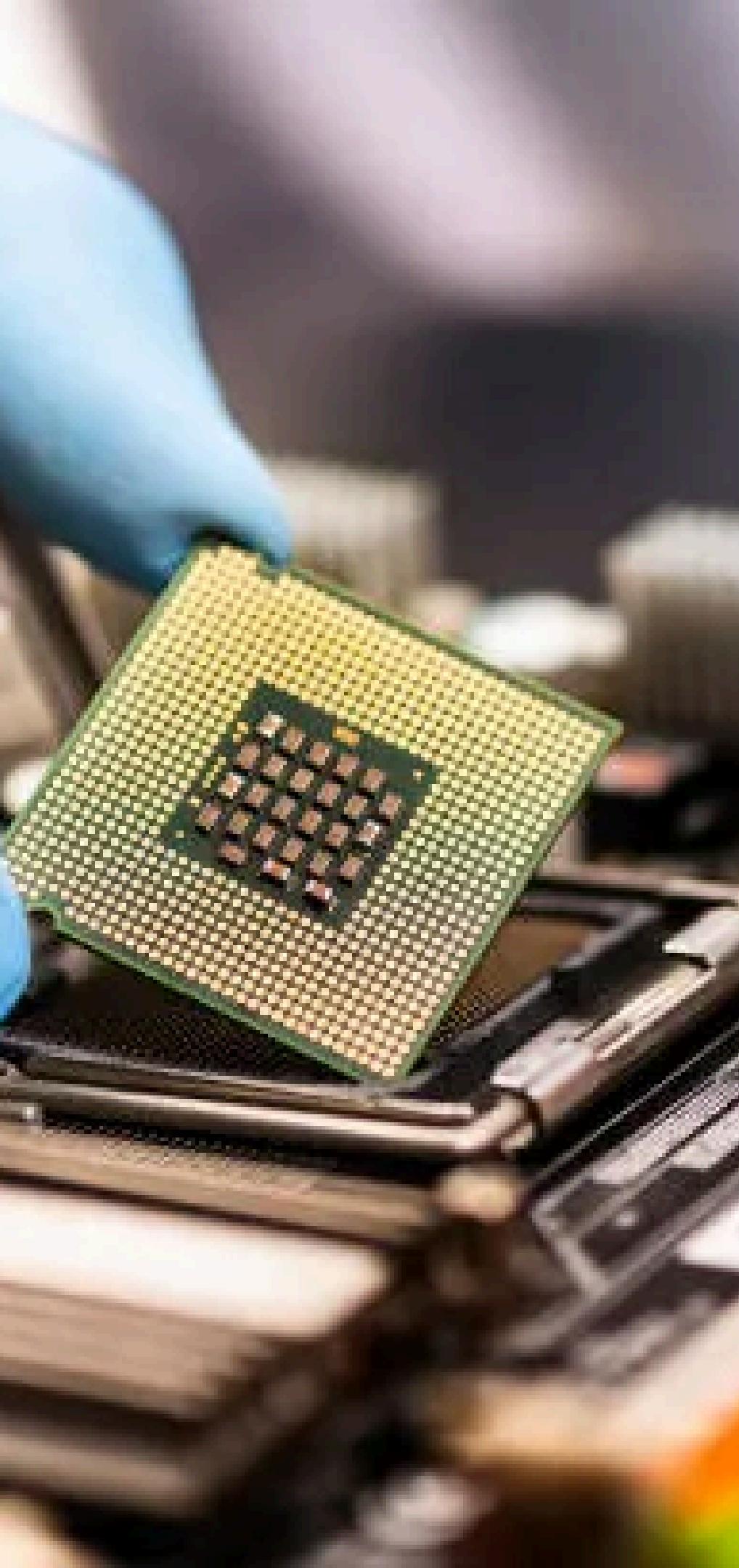
- **Secure Boot (Arranque seguro):** Verifica la integridad del firmware y garantiza que solo se inicie software de confianza en el dispositivo.

**Módulos TPM (Trusted Platform Module):** Utiliza chips de seguridad para almacenar claves de cifrado y realizar operaciones criptográficas, protegiendo los datos.

**Control de acceso físico:** Limita el acceso físico a los dispositivos con cerraduras, tarjetas de acceso o cámaras de seguridad, y políticas basadas en roles.

**Protección contra manipulación:** Emplea etiquetas de seguridad y dispositivos a prueba de manipulaciones para prevenir o detectar alteraciones en el hardware.

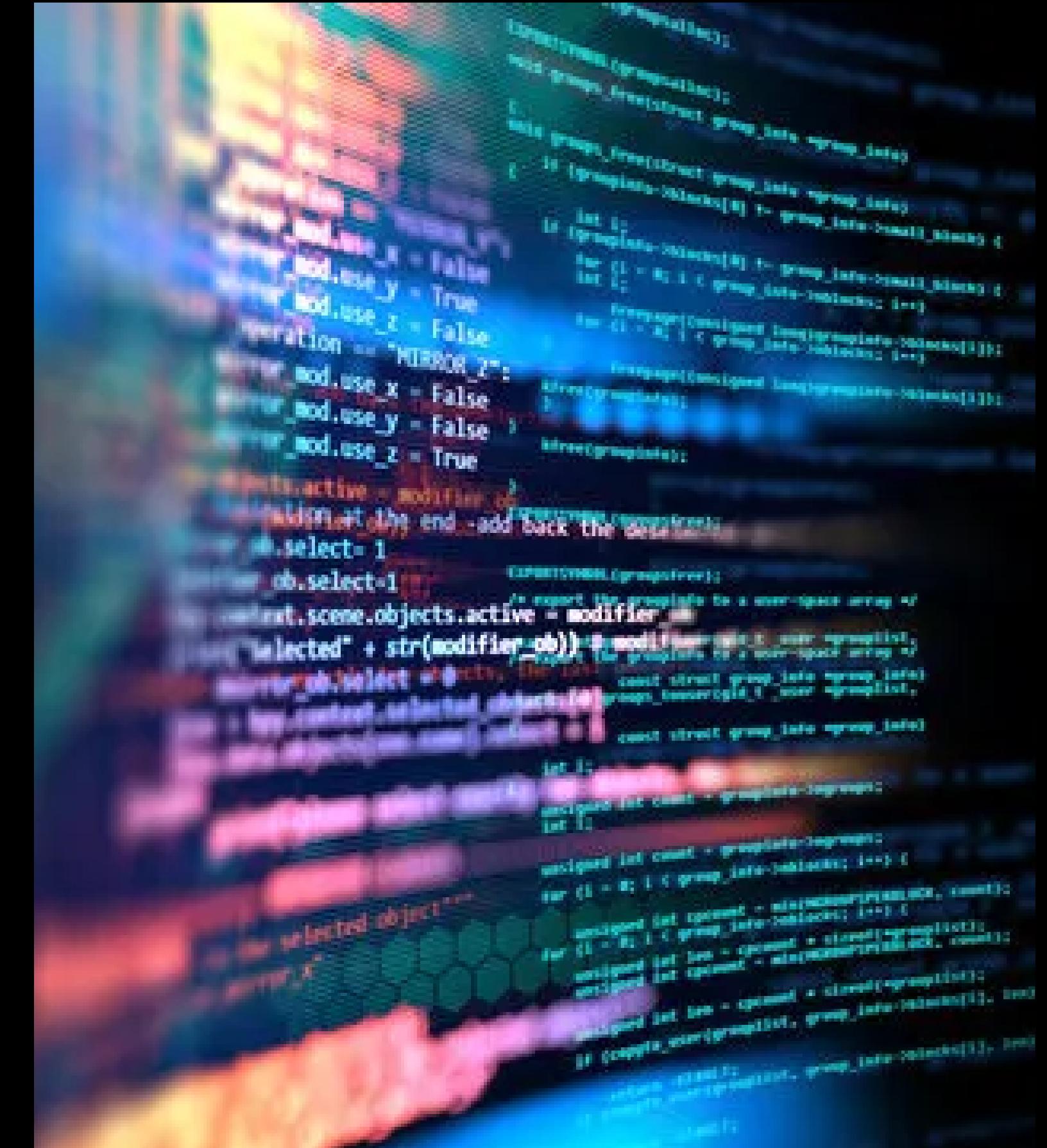
**Seguridad de firmware:** Actualiza el firmware regularmente para proteger contra vulnerabilidades y verifica su integridad.



# Seguridad del Software

---

La seguridad de software se centra en proteger las aplicaciones y programas informáticos contra amenazas y vulnerabilidades que puedan ser explotadas por atacantes. El objetivo es garantizar que el software funcione de manera segura, fiable y sin riesgos para los usuarios ni para el sistema.





# Las formas más eficientes de protegerte son:

- Mantener el Software Actualizado.
- Utilizar Herramientas de Seguridad, como antivirus y firewalls.
- Autenticación Fuerte utilizando verificación en dos pasos o similares.
- Educación y Concienciación de que hay que formas de ser hackeados y que nos roben información, para poder protegernos
- Realizar copias de seguridad periódicas de los datos importantes para prevenir pérdidas

# Seguridad en archivos e información

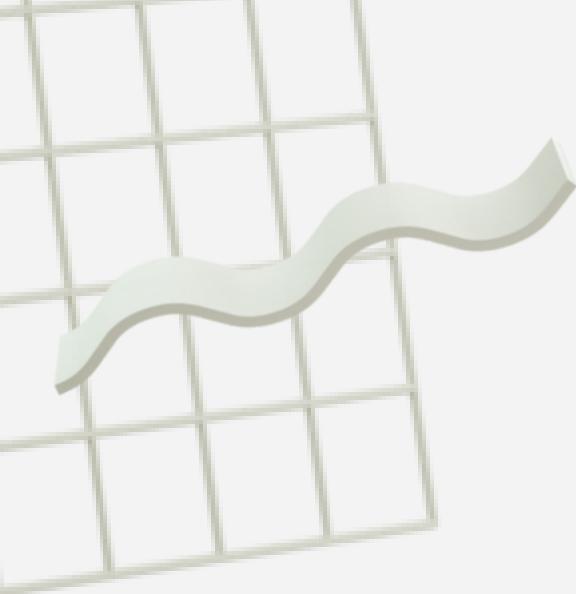
La seguridad de archivos e información es un aspecto crítico de la seguridad informática que se enfoca en proteger los datos almacenados en dispositivos de almacenamiento, archivos, bases de datos y otros formatos digitales. El objetivo es garantizar que los datos permanezcan seguros y accesibles solo para personas autorizadas. Esto implica la confidencialidad de la información, asegurándose de que solo quienes tienen los permisos adecuados puedan acceder a los datos; la integridad de la información, evitando modificaciones no autorizadas; y la disponibilidad, asegurando que los datos estén accesibles cuando se necesiten.



# Cifrado

El cifrado es un proceso que convierte datos legibles en datos codificados, o texto cifrado, utilizando una clave y un algoritmo de cifrado. El objetivo es proteger la confidencialidad de los datos tanto en tránsito (cuando los datos se envían a través de redes) como en reposo (cuando los datos se almacenan). Los algoritmos de cifrado pueden ser simétricos o asimétricos: el cifrado simétrico utiliza la misma clave para cifrar y descifrar datos, mientras que el cifrado asimétrico utiliza un par de claves, una pública y una privada. El cifrado asegura que solo las personas autorizadas con la clave adecuada puedan descifrar y acceder a los datos cifrados, proporcionando una capa esencial de seguridad para proteger información confidencial.





# **Conclusiones individuales**





## **Alonso Ramírez Páez 2127873 ITS**

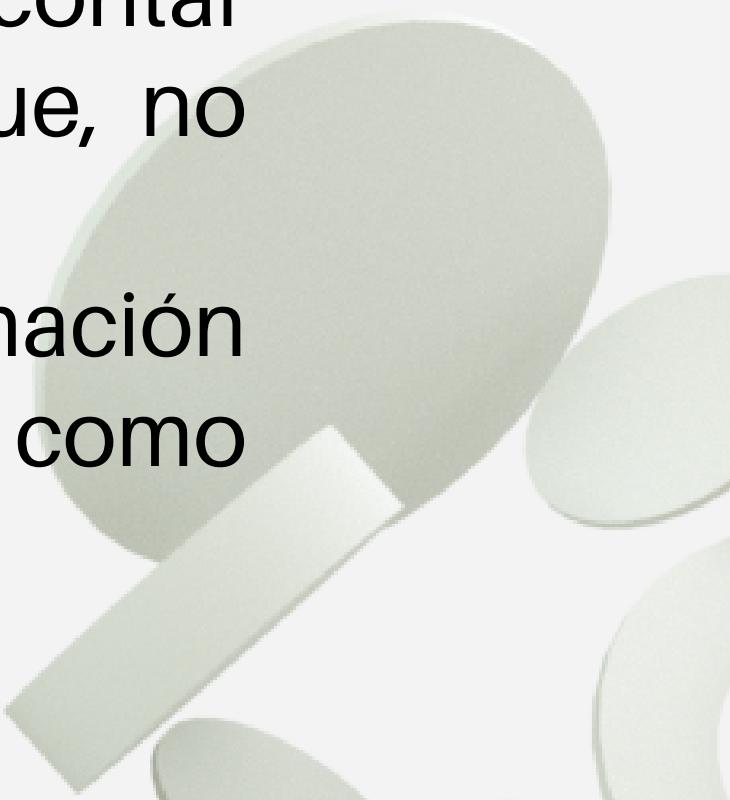
La seguridad informática es esencial en el mundo digital actual. Se trata de proteger nuestra información en internet para evitar problemas. Para lograrlo, necesitamos usar medidas de seguridad adecuadas y estar alerta ante posibles riesgos. Todos debemos tomar precauciones y aprender sobre cómo protegernos en línea para evitar problemas futuros.

## **Daniel Aharon Sánchez González 1967943 ITS**

Es importante tener en consideración siempre nuestra seguridad y saber cómo cuidarla.

Ante estos grandes avances de la tecnología es importante siempre contar con algo que pueda proteger nuestra información personal, ya que, no queremos que alguien robe nuestra información personal.

Debemos siempre seguir medidas de protección para nuestra información para así evitar que gente mala pueda obtener información personal como nombre, apellido, contraseñas, etc.



## **Emiliano García Montemayor 2003905 ITS**

La autenticación es un elemento vital en la seguridad de la información. Su objetivo principal es garantizar que la persona o sistema que intenta acceder a nuestros datos sea realmente quien dice ser. Para lograr esto, existen diferentes tipos de autenticación que se basan en algo que sabes, algo que tienes o algo que eres.

El hecho de autenticar correctamente a los usuarios es esencial para mantener la confidencialidad de la información. Una vez que se ha autenticado a un usuario, se pueden establecer diferentes niveles de autorización para acceder a la información, como solo lectura o lectura y modificación.

## **Javier López Pérez 2127884 ITS**

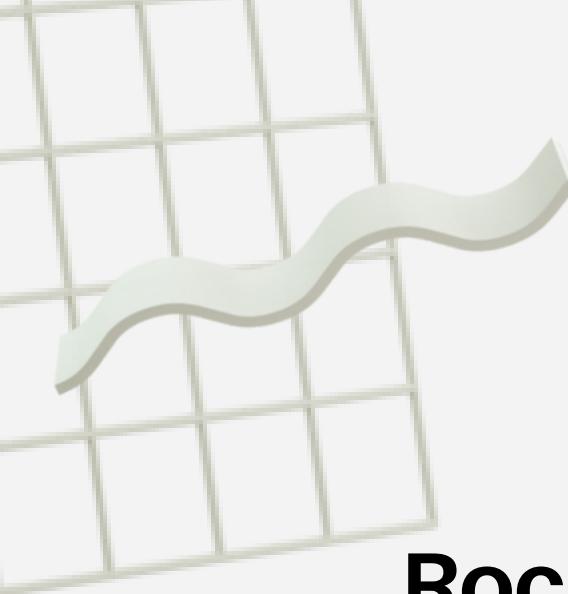
Dado que existen diferentes muchos tipos de virus informáticos, cada uno con sus propios métodos y riesgos asociados, es posible que puedan asustar, pero con precaución y medidas de seguridad adecuadas, podemos proteger nuestros dispositivos y datos. Es importante estar al tanto de los riesgos y tomar medidas para mantenernos seguros en línea.

## **Natividad Aron De León Ramírez 1855134 IAS**

Como conclusión, cabe resaltar que la identificación de posibles problemas de seguridad en seguridad informática requiere un enfoque multifacético que incluya evaluaciones regulares, monitoreo constante, actualizaciones de seguridad, educación de usuarios y preparación para responder a incidentes de seguridad, para de esta manera llevar a cabo satisfactoriamente la manera de trabajo de un grupo en determinada empresa u organización.

## **Carlos Gabriel Beas González 1940892 ITS**

Los niveles de seguridad a son cruciales para proteger contra amenazas y garantizar la integridad, confidencialidad y disponibilidad de la información y los recursos del sistema. A nivel de usuario, las prácticas seguras como el uso de contraseñas fuertes, autenticación de dos factores y la precaución al interactuar en línea son esenciales para evitar ataques de phishing y malware. En cuanto a la seguridad de redes, el uso de firewalls, cifrado de datos en tránsito, y monitoreo continuo ayuda a prevenir intrusiones y ataques externos. En conjunto, estos niveles de seguridad complementarios forman una defensa en profundidad que protege a los usuarios, redes y organizaciones frente a amenazas cibernéticas.



## **Rocío Guadalupe Sánchez Medrano 1959446 IAS**

Mi conclusión se enfoca en el tema que abordé, el cual fue los intrusos informáticos, los cuales cada tipo tiene un impacto único en nuestra era digital y requiere enfoques específicos de prevención. Comprender estas habilidades es fundamental para desarrollar estrategias de defensa efectivas. La colaboración entre expertos en seguridad y profesionales tecnológicos es crucial para promover un entorno digital más seguro y resiliente.





# Conclusión general

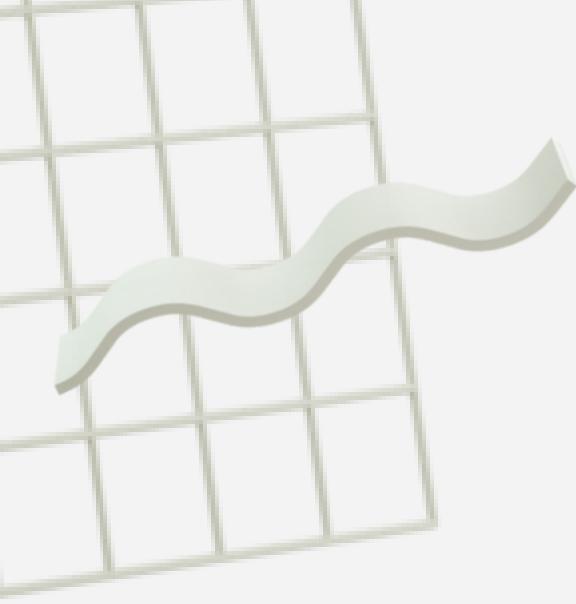




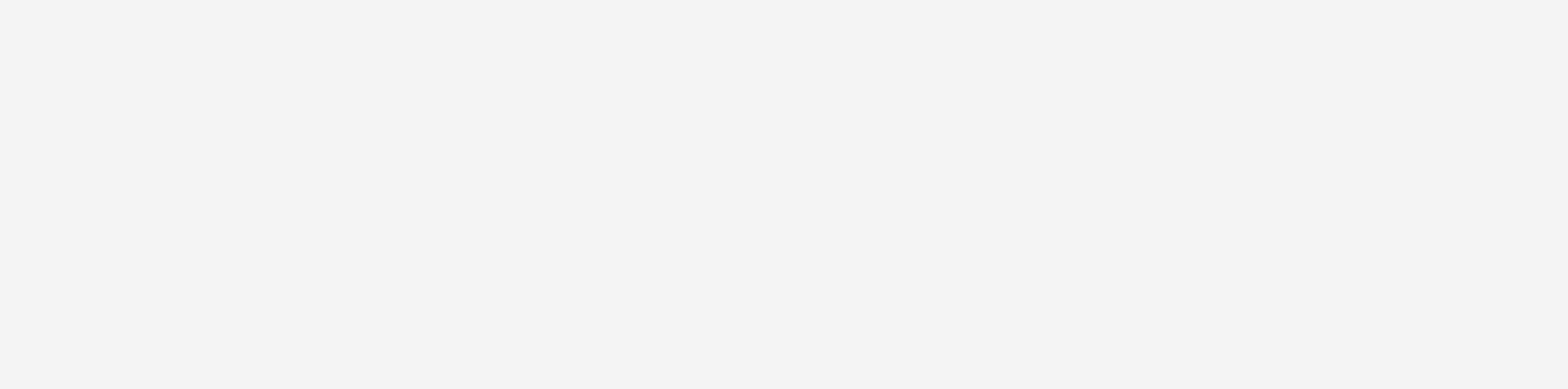
Nunca podemos confiarnos completamente cuando se trata de seguridad informática. Siempre debemos estar alerta y tomar medidas proactivas para proteger nuestros datos y sistemas contra posibles amenazas.



Mantenernos al tanto de las últimas amenazas y adoptar buenas prácticas de seguridad nos ayuda a mantenernos seguros en línea.



**Gracias por tomarse el  
tiempo de leer**



# Bibliografía

- Erickson, J. (2008). Hacking the art of exploitation (2nd Edition).
- Beaver, K. (2008). Hacking for dummies (3rd Edition). Wiley Publishing, Inc.
- G. Gelles, M. (2014). Insider Threat Prevention, detection, mitigation, and deterrence (Edition unavailable). Elsevier Science.
- Jordan, T., & Taylor, P. (2002). Hacktivism and cyberwars. Taylor & Francis e-Library.
- Ramos, M. D. P. A., & Hurtado, A. G. C. (2011). Seguridad informática y más conceptos. Editorial Paraninfo.
- Urbina, G. B. (2017). Introducción a la seguridad informática. Grupo editorial PATRIA.
- Marrero Travieso, Y. (2003). La Criptografía como elemento de la seguridad informática. Acimed, 11(6), 0-0.
- Aldeco Perez, R., Gallegos García, G., & Rodríguez Henríquez, L. (Eds.). (2020). Introducción a la ciberseguridad y sus aplicaciones en México (1.a ed.). ACADEMIA MEXICANA DE COMPUTACIÓN, A. C.  
<https://amexcomp.mx/media/publicaciones/intro-ciberseguridad-apps-en-mex-2020.pdf>