

# TALLER DE CIBERSEGURIDAD

APRENDE A VIVIR EN UN MUNDO  
CIBERINSEGURO:



Málaga 2023  
[www.digitechfp.com](http://www.digitechfp.com)

Alberto Ruiz Rodriguez

# HAY DOS GRANDES VERDADES EN EL UNIVERSO

- 1º QUE TODOS VAMOS A MORIR.
- 2º QUE TODOS VAMOS A SER HACKEADOS AL MENOS UNA VEZ EN LA VIDA.

Y DEL PRIMER PUNTO NO ESTOY TOTALMENTE SEGURO.



# INDICE

1. Primera parte: Cuales son la amenazas, quienes son los que nos atacan, porque lo hacen.
2. Segunda parte: Como actúan los cibercriminales.
3. Tercera parte: Como detectar si hemos sido atacados. Como podemos protegernos.



# Primera parte:

# Cuales son la amenazas, quienes son los que nos atacan, porque lo hacen.



# LAS AMENAZAS TECNOLÓGICAS.

“En 1989, el famoso experto en seguridad de Internet *Gene Spafford* dijo que «el único sistema verdaderamente seguro es el que se apaga, se coloca en un bloque de hormigón y se sella en una habitación revestida de plomo con guardias armados, y aún así tengo mis dudas».

Es cierto para los ordenadores independientes y para los ordenadores integrados conectados a Internet y que están en todas partes. Hace poco, **Rod Beckstrom**, exdirector del Centro Nacional de Seguridad Cibernética, lo resumió de esta manera:

- 1) Cualquier cosa conectada a Internet puede ser pirateada;
- 2) Todo se está conectando a Internet;
- 3) Como resultado, todo se vuelve vulnerable.”

BRUCE SCHNEIER “HAZ CLIC AQUÍ PARA MATARLOS A TODOS” 2018



## LAS AMENAZAS TECNOLÓGICAS

Robo de datos

Fraude

Fakenews

Pérdida de información

Extorsión

Suplantación de identidad

Problemas en la cadena de suministros

Accidentes

# ¿Qué es la ciberseguridad?

- La ciberseguridad se refiere a **la protección de los sistemas informáticos**, redes, dispositivos y datos de amenazas y ataques cibernéticos. La ciberseguridad es importante porque los sistemas informáticos y las redes son vulnerables a diversas amenazas, como virus informáticos, malware, phishing, ataques de denegación de servicio, robo de identidad, piratería informática y otros ataques cibernéticos..

## ¿porque es tan importante hoy en día?



# ¿Somos vulnerables?

- **Una vulnerabilidad** (en términos de informática) es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas.

## ¿Cuáles son nuestras vulnerabilidades?

Importante !

**LOS CIBERDELINCUENTES APROVECHAN ESTAS VULNERABILIDADES QUE SON DE DISTINTOS TIPOS Y PONEN EN RIESGO A LA EMPRESA, ORGANIZACIONES Y LAS PERSONAS.**



# EJEMPLOS DE VULNERABILIDADES

**Formulario web que no comprueba los parámetros introducidos por el usuario.**

**Mala ubicación de un servidor de base de datos dentro de la red corporativa.**

**Hardware obsoleto y sistemas operativos sin actualizar.**

**Ausencia de copias de seguridad.**

**Cuentas de usuario mal configuradas.**



# EJEMPLOS DE VULNERABILIDADES PERSONALES

**No poner ningún sistema de seguridad para entrar en nuestros dispositivos móviles.**

**Contraseñas débiles.**

**Ofrecer información personal en redes sociales.**

**No tener cuidado a la hora de darnos de alta en sitios web.**

**No cambiar las contraseñas NUNCA.**



# CICLO DE VIDA DE UNA VULNERABILIDAD

## 1 Detección de la vulnerabilidad

Detección y descripción de la vulnerabilidad. .

## 4 muerte de la vulnerabilidad

Generación de un parche de actualización o de nueva versión del código para impedir el uso malicioso de la vulnerabilidad.

## 2 Explotando la vulnerabilidad. Somos atacados.

Explotación de la vulnerabilidad del sistema (desarrollo de exploits o ataque).

## 3 Solucionado el problema.

Solución al problema.



# VULNERABILIDAD DE ZERO-DAY

- . Se conoce como **vulnerabilidad de zero day o 0-day** (vulnerabilidad de día 0) a la situación que aparece cuando sólo una persona (o muy pocas personas) **conocen una vulnerabilidad** y están en una situación de ventaja para poder explotarla.
- . Es decir, la persona que ha encontrado la vulnerabilidad no la ha hecho pública, de modo que ni el fabricante ni los administradores/usuarios son conocedores del problema.



# Quienes son los que nos atacan

Desmintiendo mitos:

## ¡NI TODOS LOS HACKERS SON CIBERDELINCUENTES. NI TODOS LOS CIBERDELINCUENTES SON HACKERS

**1.Hacker:** un hacker es una persona que tiene habilidades avanzadas en el uso de la tecnología y utiliza esas habilidades para explorar, probar y mejorar la seguridad de los sistemas informáticos. Los hackers pueden ser sombrero negro, sombrero gris o sombrero blanco, según sus intenciones.

**2.Lamers:** un lamer es alguien que tiene conocimientos limitados de informática y tecnología, pero que pretende ser un hacker o tiene una actitud arrogante hacia los demás usuarios de tecnología.

**3.Cracker:** un cracker es una persona que utiliza habilidades informáticas avanzadas para violar la seguridad de sistemas informáticos, dispositivos o redes con el fin de obtener acceso no autorizado o realizar actividades ilegales. Los crackers son diferentes de los hackers en que sus intenciones suelen ser maliciosas.

**4.Ciberespías:** los ciberespías son personas que utilizan la tecnología para espiar a individuos, empresas, organizaciones o países con el fin de obtener información confidencial. Los ciberespías pueden ser individuos o pueden trabajar para gobiernos o empresas.

**5.Ciberdelincuentes:** los ciberdelincuentes son personas que utilizan la tecnología para cometer delitos, como el robo de información personal o financiera, el secuestro de datos, el phishing, el malware y otros tipos de ataques cibernéticos.

**6.Cibermafia:** la cibermafia es un grupo de ciberdelincuentes que trabajan juntos en actividades ilegales y delictivas en línea, como el robo de información financiera, el fraude en línea y el robo de identidad.

**7.Ciberhacktivismo:** el ciberhacktivismo es el uso de técnicas de hacking y tecnología para promover una causa social o política. Los ciberhacktivistas utilizan la tecnología para llamar la atención sobre problemas sociales y políticos y para promover el cambio social.

Algunos grupos que se han destacado en el mundo de la seguridad informática son Anonymous, LulzSec, APT28, Fancy Bear, entre otros.



# Espionaje industrial, espionaje político y la ciberguerra

- El espionaje industrial, el espionaje político y la ciberguerra son formas de uso malintencionado de la tecnología en el ámbito político y empresarial. Aquí hay algunas definiciones y ejemplos:
  1. **Espionaje industrial:** el espionaje industrial es el uso de la tecnología y otros medios para obtener información confidencial de empresas y organizaciones competidoras, con el fin de obtener una ventaja competitiva. Por ejemplo, puede incluir el robo de secretos comerciales, el sabotaje de procesos de producción o el espionaje de planes de negocios.
  2. **Espionaje político:** el espionaje político es el uso de la tecnología y otros medios para obtener información confidencial de gobiernos y organizaciones políticas extranjeras, con el fin de obtener una ventaja geopolítica o militar. Por ejemplo, puede incluir el robo de secretos militares, la interferencia en elecciones y la infiltración de organizaciones políticas.
  3. **Ciberguerra:** la ciberguerra es un conflicto cibernético entre dos o más naciones que involucra la destrucción de sistemas informáticos críticos, la interrupción de servicios esenciales y la obtención de información confidencial. Las ciberguerras pueden ser utilizadas en combinación con conflictos armados convencionales. Ejemplos incluyen los ataques a la red eléctrica ucraniana por parte de Rusia en 2015 y los ataques a los sistemas informáticos de Irán por parte de Estados Unidos e Israel en 2010.
- Algunos países que se han destacado por su actividad en estos temas **incluyen China, Rusia, Corea del Norte, Irán, Estados Unidos y varios países de la Unión Europea.** Sin embargo, es importante señalar que cualquier país con capacidad tecnológica avanzada y una presencia en línea significativa podría participar en estas actividades.

# Rusia y la guerra de Ucrania

## ¿Se está reagrupando Rusia para una nueva ciberguerra?



- En 2023, Rusia ha aumentado sus ataques de espionaje, tomando como objetivo organizaciones de al menos 17 países europeos, en su mayor parte agencias gubernamentales. Además, los ataques con malware Wiper continúan en Ucrania.
- También seguimos monitorizando el desarrollo y despliegue de nuevas variantes de ransomware. En noviembre de 2022, Microsoft y otras empresas de seguridad identificaron una nueva variante, llamada Sullivan y desplegada contra objetivos ucranianos, además del [ransomware Prestige](#) que Rusia lanzó en Polonia y Ucrania en octubre de 2022. Nuestro análisis sugiere que Rusia continuará llevando a cabo ataques de espionaje contra Ucrania y sus aliados, además de ataques destructivos dentro y, potencialmente, fuera de Ucrania, tal y como se hizo con Prestige.
- La ofensiva híbrida rusa también ha incluido sofisticadas operaciones de influencia. Por ejemplo, la maquinaria de propaganda de Moscú recientemente marcó como objetivo a los refugiados ucranianos en Europa, en un intento de que fueran deportados y reclutados por el ejército ucraniano.
- Las operaciones de influencia alineadas con Rusia también han logrado subir la tensión en Moldavia. Los medios rusos promovieron protestas apoyadas por un partido político prorruso que animaba a los ciudadanos a reclamar al gobierno que pagase la factura de la energía en invierno. Otra campaña alineada con Rusia, llamada “Moldova Leaks”, publicó supuestas filtraciones de políticos moldavos, una más de las operaciones híbridas *hack-and-leak* (literalmente, hackear y filtrar) dirigidas a socavar la confianza de los ciudadanos europeos en sus gobiernos.
- Estos son solo algunos de los puntos más relevantes del nuevo informe [Microsoft Threat Intelligence](#) sobre la actividad rusa. El informe destaca otras amplias, e importantes, tendencias.

Fuente: <https://news.microsoft.com/es-es/2023/03/17/se-esta-reagrupando-rusia-para-una-nueva-ciberguerra/>



# El caso de Israel y la capacidad nuclear de IRÁN

- El incidente del pendrive es el ataque cibernetico conocido como "**Stuxnet**", que se descubrió en 2010 y se cree que retrasó el programa nuclear de Irán varios años.
- Stuxnet fue un **virus informático** diseñado específicamente para atacar el programa nuclear iraní. Se cree que fue desarrollado conjuntamente por Estados Unidos e Israel, aunque ninguno de los dos países ha confirmado oficialmente su participación.
- El virus se propagó a través de una serie de dispositivos USB infectados que fueron introducidos en las computadoras de las instalaciones nucleares iraníes. Una vez dentro del sistema, el virus se encargaba de dañar las centrifugadoras utilizadas en el proceso de enriquecimiento de uranio.
- El ataque fue muy sofisticado y se cree que implicó el uso de técnicas de ingeniería inversa para comprometer el software utilizado en las instalaciones nucleares. Se considera uno de los primeros casos conocidos de un ataque cibernetico con capacidad para causar daño físico en el mundo real.
- El incidente de Stuxnet fue una clara señal de la creciente importancia de la ciberguerra en el ámbito de la seguridad nacional e internacional. Desde entonces, ha habido varios otros incidentes de ciberguerra relacionados con el programa nuclear de Irán, así como en otros ámbitos geopolíticos.



## Ciberhacktivimos: ANONYMUS



- **Anonymous** es un grupo internacional de hackers y activistas cibernéticos que se definen a sí mismos como defensores de la libertad de expresión, la privacidad en línea y la transparencia gubernamental. El grupo se formó en 2003 y es conocido por sus operaciones de hacktivismo, en las que utilizan técnicas de hacking para **acceder y divulgar información de organizaciones gubernamentales y corporaciones**. También han llevado a cabo protestas y manifestaciones en línea, así como acciones de caridad. Anonymous es un grupo descentralizado y sin líderes formales, por lo que las acciones de sus miembros no están coordinadas ni autorizadas por una figura central.



# Hacker y los sombreros

El término "hacker" se popularizó en la década de 1960 en el Instituto de Tecnología de Massachusetts (MIT), donde los estudiantes se referían a sí mismos como "hackers" para describir a aquellos que realizaban modificaciones ingeniosas y creativas en el software y hardware de las computadoras



## Hacker sombrero negro (Black hat hacker):

- Este término se utiliza para describir a los hackers que utilizan sus habilidades para violar la seguridad de los sistemas informáticos con fines maliciosos o ilegales. Los hackers sombrero negro pueden realizar acciones como el robo de información, la interrupción de servicios en línea, la instalación de malware o virus, y otros tipos de ataques cibernéticos.



## Hacker sombrero gris (Gray hat hacker):

- Este término se utiliza para describir a los hackers que realizan acciones ilegales o no autorizadas en sistemas informáticos, pero sin intenciones maliciosas. Los hackers sombrero gris pueden probar la seguridad de un sistema o sitio web, o incluso proporcionar información sobre vulnerabilidades a los propietarios del sistema. Aunque suelen tener buenas intenciones, sus acciones aún pueden ser ilegales y conllevan riesgos.

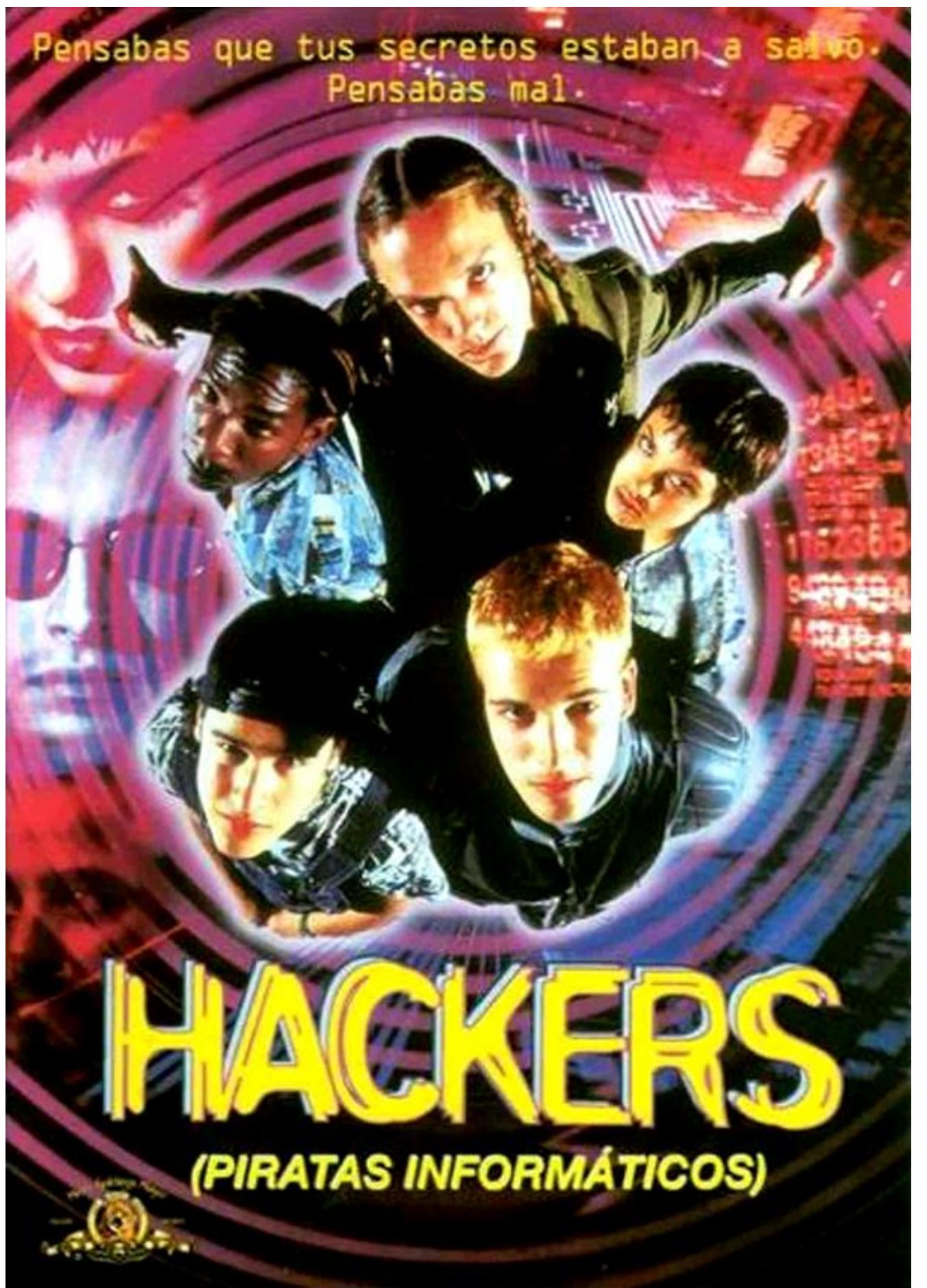


## Hacker sombrero blanco (White hat hacker):

- Este término se utiliza para describir a los hackers que utilizan sus habilidades para proteger sistemas informáticos y redes de posibles amenazas. Los hackers sombrero blanco trabajan para empresas o organizaciones y realizan pruebas de seguridad para identificar vulnerabilidades y fortalecer la seguridad. A diferencia de los hackers sombrero negro y gris, las acciones de los hackers sombrero blanco son legales y éticas, y su objetivo es mejorar la seguridad de los sistemas informáticos en lugar de dañarlos.

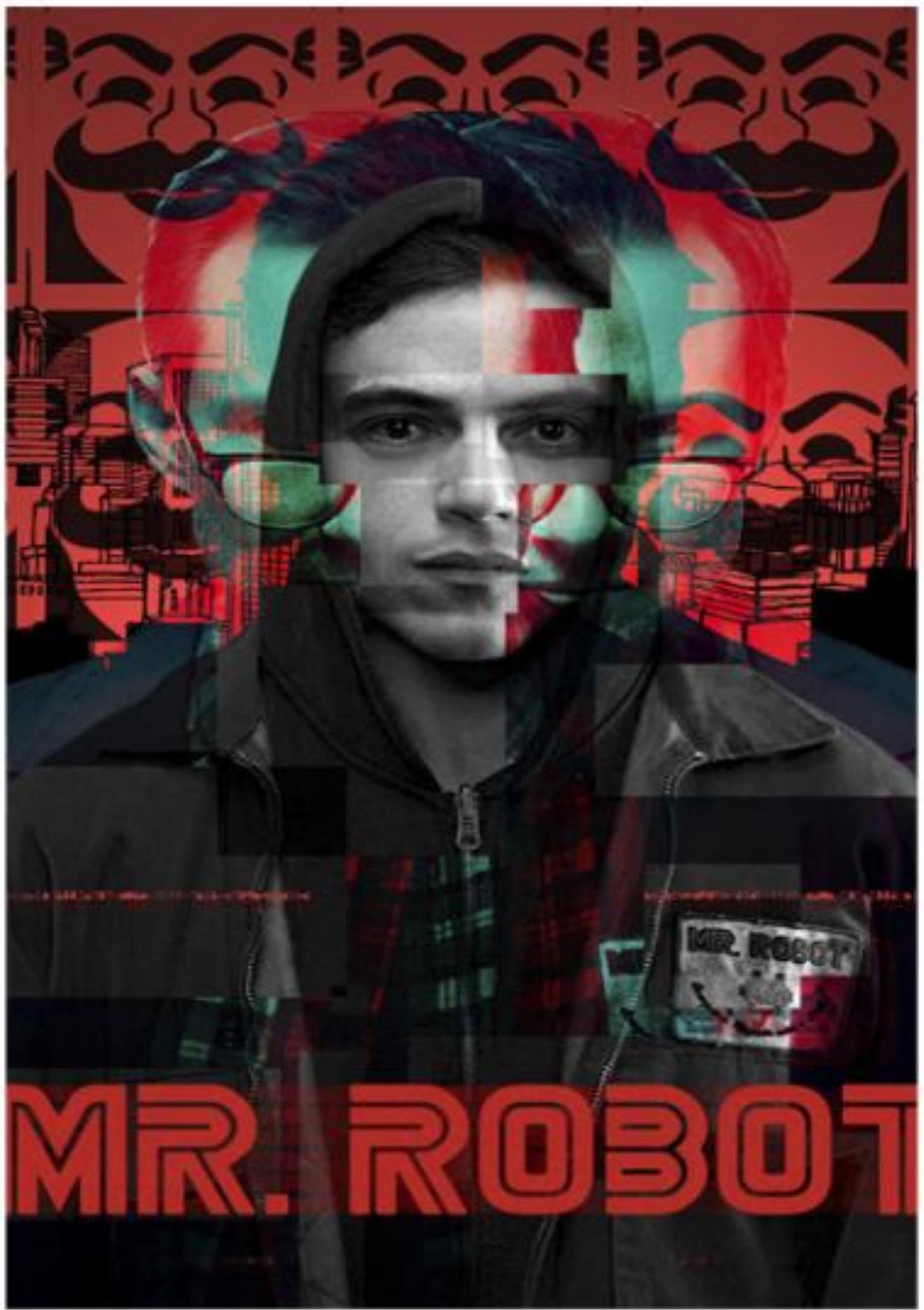


- Película Hacker



Un grupo de adolescentes cuya afición es piratear sistemas informáticos por diversión descubren los planes de un hacker para cometer un delito, y deciden tomar parte en ellos. 1995

- Mister Robot



Elliot Alderson, un brillante programador con problemas de ansiedad social, trabaja como ingeniero de ciberseguridad de día y como justiciero de noche. Su vida da un giro cuando unos ciberterroristas lo reclutan. 2019



# ¿Por qué nos atacan?

- 1. Lucro económico:** los ciberdelincuentes pueden llevar a cabo ataques con el fin de obtener beneficios económicos, como el robo de información financiera, la extorsión de empresas y el rescate de datos.
- 2. Espionaje:** los gobiernos y otros grupos pueden llevar a cabo ataques para recopilar información confidencial de otras naciones o empresas.
- 3. Activismo político:** los grupos de hacktivistas pueden llevar a cabo ataques para protestar o hacer campaña por una causa política o social.
- 4. Sabotaje:** los ataques pueden ser llevados a cabo con el fin de dañar la reputación de una empresa, interferir con sus operaciones o causar daños físicos.
- 5. Experimentación:** los hackers pueden realizar ataques como una forma de probar sus habilidades técnicas y demostrar su destreza.
- 6. Venganza:** los ataques pueden ser llevados a cabo como un acto de venganza contra una empresa o individuo específico.



Desmintiendo otro mito



- No soy tan importante como para que me ataquen, tengo un dispositivo electrónico, sea una Tablet, móvil portátil. para ver series, películas, escribir algún documento, mis redes sociales, el banco, hacienda.

## ¡Todo somos posibles víctimas!

Solución: Vuelvo a lo analógico.



No, eso es otro error, no es cuestión de no usar los medios tecnológicos es simplemente tener cuidado, igual que cerramos la puerta de casa, o tenemos una puerta blindada, alarma en el coche, etc. **PRECAUCIÓN AMIGO CIBERNAUTA, NO MIEDO.**



# Como nos atacan

**1.Phishing:** los ciberdelincuentes pueden enviar correos electrónicos o mensajes falsos que parecen legítimos con el fin de engañar a los usuarios para que revelen información confidencial como contraseñas, números de tarjetas de crédito, entre otros.

**2.Malware:** los ciberdelincuentes pueden distribuir software malicioso, como virus, troyanos o ransomware, que se instala en el sistema de la víctima para robar información o dañar el sistema.

**3.Atajes de fuerza bruta:** los ciberdelincuentes pueden utilizar programas para intentar adivinar contraseñas y obtener acceso a sistemas o cuentas protegidas.

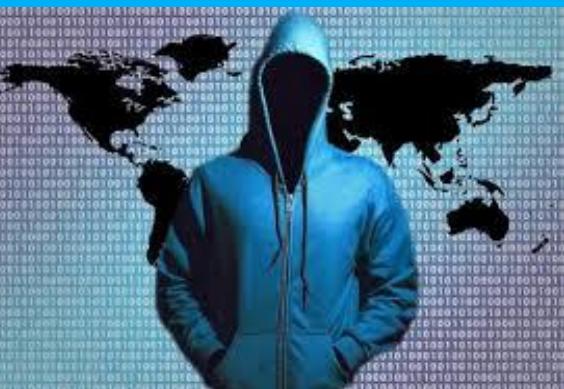
**4.Ingeniería social:** los ciberdelincuentes pueden utilizar técnicas de manipulación psicológica para engañar a los usuarios para que revele información confidencial.

**5. Ataques de denegación de servicio (DDoS):** los ciberdelincuentes pueden inundar un sitio web o un sistema con tráfico malicioso para sobrecargar el sistema y dejarlo inoperable.

**6. Ataques de red:** los ciberdelincuentes pueden escanear una red en busca de vulnerabilidades y explotarlas para obtener acceso no autorizado a sistemas o información.



# Segunda parte: Como actúan los ciberdelincuentes.

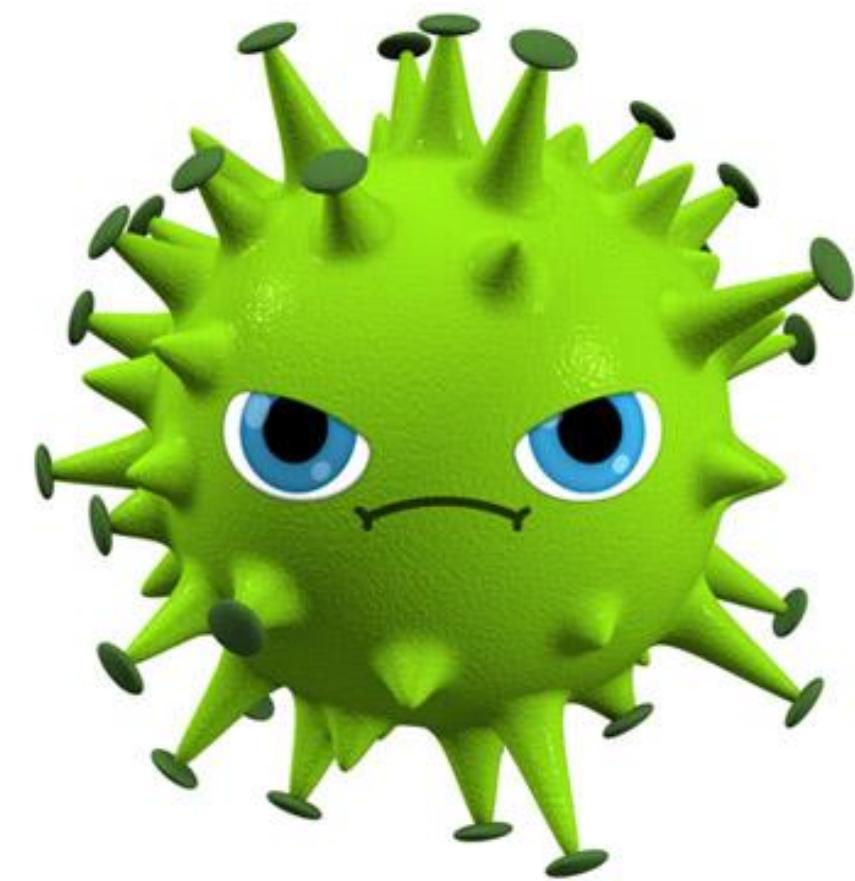


# Virus informáticos y malware en general.

**1. Formas de actuar y técnicas de los ciberdelincuentes**

**2. Malware.**

**3. Patrones de ataques.**



# 1. Formas de actuar y técnicas de los ciberdelincuentes:

**1 Anonimato:**



Ocultan su identidad. Borran las huellas.

**2 Controlan remotamente:**



Convierten tu dispositivo en un bouncer o equipo zombie, controlándolo sin que te des cuenta y lo usan para atacar a otros o para minería de Bitcoin Para ello usan un troyano.

**3 Utilizan un proxy o una red VPN :**



Para esconder la identidad del atacante. (Un proxy es un equipo informático que hace de intermediario entre las conexiones de un cliente y un servidor de destino, filtrando todos los paquetes entre ambos) O el uso de redes privadas virtuales o VPN. Que hacen difícil el rastreo

**4 Uso de la deep web**



También denominada o Internet Profunda, gracias a proyectos como TOR, que garantiza también el anonimato. También se usa una red servidores TOR que son servidores anónimos y que ocultan la identidad e IP del atacante.



# Tipos de ataques



**1. Interrupción:** Un recurso del sistema o de la red, deja de estar disponible debido al ataque.

**Por ejemplo** no podemos acceder a internet provocado por un virus o Malware.

**2. Modificación:** La información de la que se dispone, es modificada sin autorización y por lo tanto

deja de ser válida. Roban nuestras credenciales, estas son modificadas y no podemos entrar en un sistema

**Por ejemplo** roban nuestro acceso a programas de gestión de la empresa.

**3. Fabricación:** Consiste en crear un producto que sea difícil de distinguir del autentico y que es

utilizado para hacerse con la información confidencial de los usuarios.

**Por ejemplo** nos envían un email haciéndose pasar por un banco para robar nuestros datos.

**4. Intercepción:** El intruso accede a la información de nuestros equipos, o a la información que enviamos por la red. Consiguen nuestros datos de correo y el atacante puede ver todos nuestros correos sin que nos percatemos de ello.



# Eventos-ataques e incidentes de seguridad

## 1. Evento de seguridad

Ejemplo:

- Un servidor es escaneado para encontrar sus vulnerabilidades.
- Los datos de un cliente son modificados sin autorización.
- Un usuario es suplantado en una red social.
- Un proceso industrial (fabricación de un medicamento) es interrumpido.

Un evento de seguridad de la información indica que el sistema, la seguridad o los servicios de red y de infraestructura han sido comprometidos o vulnerados. Esto indica que los controles implementados han fallado y/o que no se ha seguido la política de seguridad de la información de la organización.

## 2. Ataque

Ejemplos:

Una vulnerabilidad de un sistema operativo es empleada para que un malware escale privilegios y se ejecute con permisos de administrador.

Un sniffer de red es empleado para espiar el tráfico y obtener la contraseña de un usuario.

Un campo de un formulario web es empleado para realizar una consulta SQL en una base de datos y descargar un fichero sin autorización.

El **ataque** empieza antes, cuando se utiliza algún tipo de herramienta para explotar una vulnerabilidad y termina un poco más tarde, cuando gracias a la acción realizada sobre el objetivo se produce un resultado concreto.

## 3. Incidente de seguridad

Ejemplos:

Un terrorista manipula el sistema de control de un pozo petrolífero y genera un desastre medioambiental.

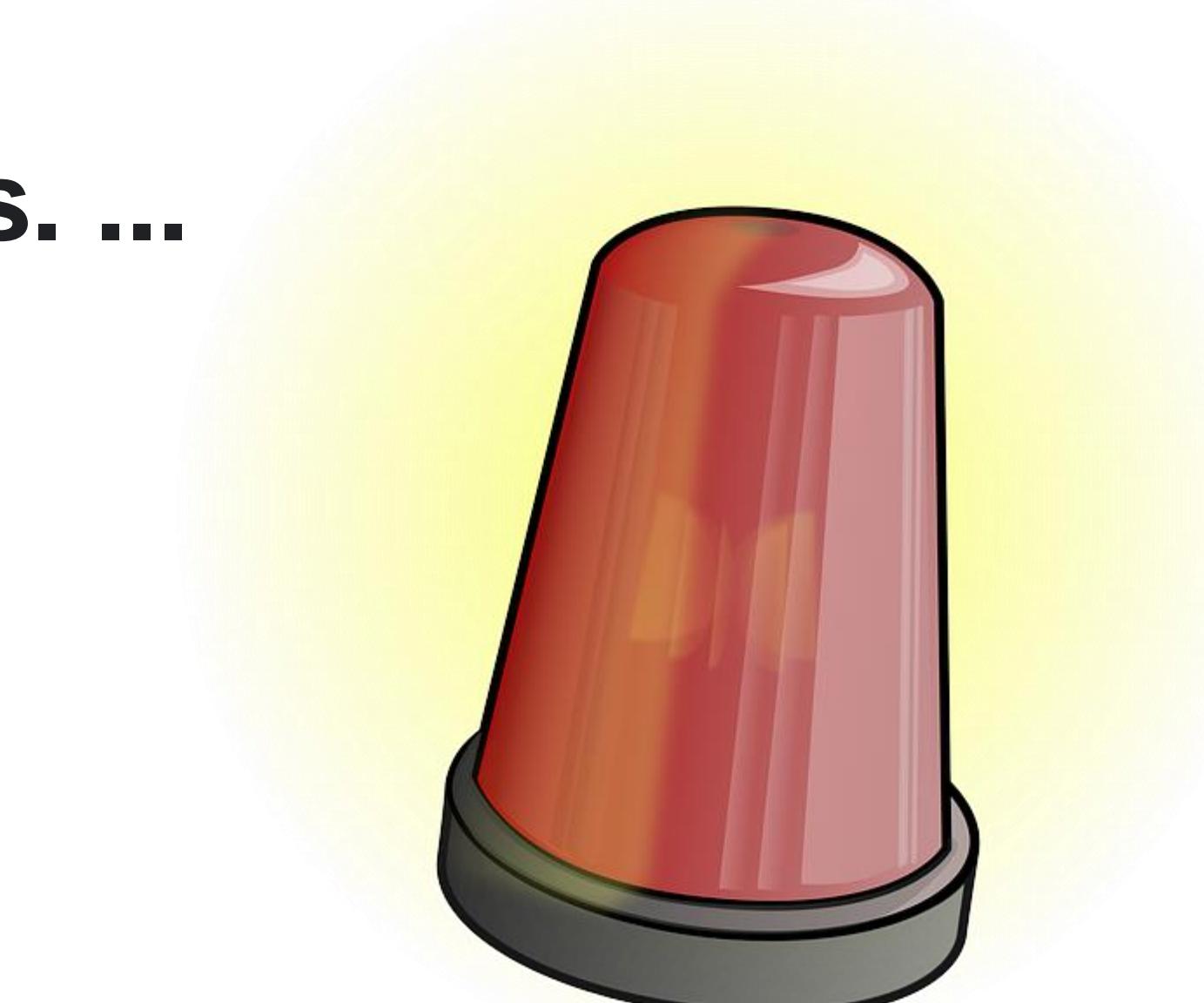
Un estudiante de informática se descarga un kit de exploits e intenta realizar una denegación de servicio en la página web de su universidad.

El **incidente** es cuando la seguridad de un sistema ha sido comprometida, y ha resultado en robo de información o pérdida de datos.



# Cómo detectar incidentes de seguridad

- 1. Comportamiento inusual de cuentas de usuario privilegiadas. ...**
- 2. Empleados no autorizados que intentan acceder a servidores y datos. ...**
- 3. Anomalías en el tráfico de la red de salida. ...**
- 4. Tráfico enviado hacia o desde lugares desconocidos. ...**
- 5. Consumo excesivo. ...**
- 6. Cambios en la configuración.**



AulaFacil.com



# ¿QUE ES UN MALWARE?

**Se llama malware, del inglés malicious software, programa malicioso, programa maligno, badware, código maligno, software maligno, software dañino o software malintencionado a cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.** [Wikipedia](#)



# Algunos tipos de malware

- **Virus.** Se incorporan a los programas existentes y se activan cuando el usuario abre el programa. ...
- **Gusanos.** ...
- **Troyanos.** ...
- **Spyware.** ...
- **Herramientas de administración remota (RAT)** ...
- **Ransomware.** ...
- **Rogueware.** ...
- **Malware polimórfico.**

## Desmontando mitos

¿Un virus informático puede afectar al ser humano?



Por supuesto... que NOOOOOOOOOOOOOOO



# VIRUS

- Un virus o virus informático<sup>-1</sup> 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. 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.



**!!!!El término correcto es Malware no hablar solo de virus, virus es un tipo de MALWARE!!!**



# Historia de los virus para escépticos.

- Los virus informáticos son programas maliciosos que se replican y propagan en sistemas informáticos con el objetivo de causar daño o robar información. Los primeros virus informáticos se desarrollaron en la **década de 1970** y eran relativamente simples en comparación con los virus modernos. A medida que la tecnología avanzó, también lo hicieron los virus, y hoy en día existen diversas formas de malware que pueden causar daño a los sistemas informáticos.
- El primer virus informático conocido fue llamado "**Creeper**" y se desarrolló en 1971. Este virus se propagaba a través de una red de computadoras ARPANET y mostraba el mensaje "Soy la enredadera, ¡atrápame si puedes!" en las pantallas de las computadoras infectadas. El primer virus que se propagó ampliamente a través de la red fue el virus "**Morris**" en 1988, que se propagó a través de la red ARPANET y afectó a miles de computadoras en todo el mundo.
- A medida que las computadoras personales se volvieron más populares en la década de 1990, también lo hicieron los virus informáticos. Los virus se propagaban a través de discos infectados, correos electrónicos maliciosos y descargas de software infectado. Los virus como "**Melissa**" y "**ILOVEYOU**" se propagaron rápidamente a través de correo electrónico y causaron grandes daños en sistemas informáticos en todo el mundo.
- En la década de 2000, el malware se volvió más sofisticado y peligroso. El malware como el troyano "**Zeus**" se utilizó para robar información financiera de empresas y particulares, mientras que los virus de tipo "**gusano**" como "**Conficker**" se propagaron a través de redes y sistemas sin la necesidad de la interacción del usuario.
- El ransomware es una forma relativamente nueva de malware que se ha vuelto cada vez más común en los últimos años. El ransomware es un tipo de malware que cifra los archivos de la víctima y exige un rescate para descifrarlos. Ejemplos de ransomware incluyen "**WannaCry**" y "**NotPetya**", que afectaron a empresas y organizaciones en todo el mundo en 2017.
- En general, la historia de los virus informáticos ha sido una carrera armamentista entre los cibercriminales y los expertos en seguridad cibernética. A medida que los virus se han vuelto más sofisticados, también lo han hecho las herramientas y tecnologías utilizadas para combatirlos. Es importante que los usuarios tomen medidas preventivas para protegerse contra los virus, como mantener su software de seguridad actualizado y ser conscientes de los correos electrónicos y descargas sospechosas.



## GUSANOS-WORMS

**Un gusano informático es un malware que se replica para propagarse a otras computadoras. Este software malicioso suele utilizar una red informática para propagarse, aprovechando las fallas de seguridad en la computadora de destino para acceder a ella.**

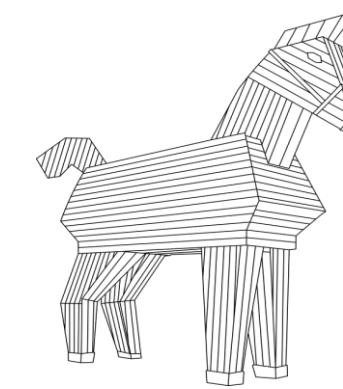


Una vez que un gusano infecta un sistema, puede llevar a cabo diversas acciones maliciosas, como robar información confidencial, degradar el rendimiento del sistema, instalar software malicioso adicional o crear "puertas traseras" para permitir el acceso remoto no autorizado. Los gusanos

también pueden consumir recursos valiosos del sistema, como el ancho de banda de la red, lo que puede afectar negativamente el rendimiento de los sistemas y la red.

Además, los gusanos pueden ser diseñados para propagar otros tipos de malware, como troyanos o ransomware, lo que puede causar daños aún mayores





# TROYANOS

En informática, se denomina caballo de Troya, o troyano, a un malware que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado. A los troyanos de acceso remoto también se les denomina **Backdoor o puerta trasera. Los hay que son de tipo espionaje, bancarios, o de cifrado (Ransomware)**

## Troyanos de descarga:

Son aplicaciones de software que no pueden dañar al equipo anfitrión por sí mismos, si éste no se conecta a Internet. Su código de carga se conecta a Internet, y luego facilita la instalación de otras aplicaciones (exploits, por ejemplo).

## Troyanos de destrucción de datos:

Están diseñados específicamente para borrar por completo o corromper los datos almacenados en el sistema, ya sean archivos del sistema operativo o datos del usuario.

## Troyanos de denegación de servicio (DoS):

Están diseñados para impedir o detener el funcionamiento normal de un sitio web, u otro recurso de red, inundándolo con más tráfico del que es capaz de manejar.

## Troyanos Rogue Ware

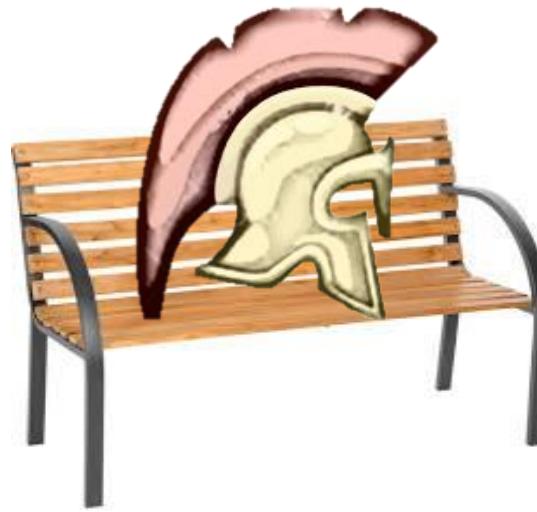
Son aplicaciones que advierten a los usuarios de infecciones que no existen con el fin de engañarles para que compren la versión "completa" de un producto anti-malware ficticio.

## Desactivadores de antivirus:

Son troyanos que, una vez en el ordenador anfitrión, tratan de detener o de convertir en inútiles las aplicaciones antivirus o los firewalls de host sin el consentimiento del usuario.



# Troyanos bancarios



- Los troyanos bancarios son una de las especies de malware de mayor prevalencia en la actualidad. Los autores de este tipo de malware (mayoritariamente brasileños y rusos en la actualidad) tienen como objetivo mantener las infecciones vivas y sin ser detectadas durante un tiempo suficiente para que puedan **robar datos bancarios** de sistemas de banca on-line, sistemas de pago electrónico y tarjetas de débito o crédito. Todos los datos robados son **enviados a los atacantes mediante diferentes protocolos** (HTTP, FTP, IRC, etc.) y pueden ser explotados directamente por estos atacantes o vendidos en el mercado negro. Día tras día, víctimas inocentes son hackeadas y sus **cuentas bancarias vaciadas**.
- ¿Qué técnicas emplean los troyanos para robar información bancaria? Casi siempre incorporan **keyloggers**, pero también **capturan formularios y pantallas**, realizan **redirecciones** (a servidores controlados por los atacantes, esto se suele denominar pharming).



# MALWARE PARA OBTENER BENEFICIOS ECONOMICOS

## 1. Spyware:

Malware cuya funcionalidad es espiar al usuario/equipo infectado. Suelen incorporar keyloggers, grabadores de escritorio, software para activar la webcam, etc.



## 2. Adware:

En este caso la funcionalidad es mostrar publicidad de manera agresiva.



## 3. Keyloggers:

Se trata de un malware que se encarga de registrar las pulsaciones en el teclado permitiendo el acceso a contraseñas u otro tipo de información privada



## 4. Stealers:

Los stealers roban la información privada que se encuentra guardada en el equipo. Al ejecutarse comprueban los programas instalados en el equipo y si tienen contraseñas o credenciales almacenadas, por ejemplo en los navegadores web y se la envían al atacante



## 5. Ransomware:

Conocido como malware "secuestrador" Se trata de malware que hace inaccesibles archivos de utilidad para el usuario, se habla de ransomware criptográfico cuando para ello se cifran estos archivos. Se pide un rescate para poder liberar/descriptar los archivos,



# Saber más: Ramsonware:

- Los ataques con Ramsonware se están volviendo más agresivos, no solo encriptan la información a cambio de un rescate, también está robando información confidencial, incluso con la amenaza de publicarla o bien de venderla al mejor postor.



# EJEMPLO DE RANSOMWARE: LA PESADILLA DEL SIGLO XXI



1º Pagar no es la solución, ya que ocurre con frecuencia que el atacante no da la clave de descriptación.

2º Incluso aunque te dieran la clave, lo habitual es que sigan teniendo el control del sistema y en cualquier otro momento te vuelvan a extorsionar, o peor aún vendan el acceso a tu sistema a otros ciberdelincuentes o mafias y recibas ataques varias veces a lo largo de un año.

3º Hay seguros que cubren incluso la extorsión, lo que ha hecho es aumentar este tipo de delitos.

4º Se está dando el caso que la impunidad de estos ciberdelincuentes, les permite anunciarse e incluso poner un teléfono de atención al cliente en caso de no saber como realizar el pago.



# Casos famosos de Ransomware

1. WannaCry: Este ransomware se propagó a través de una vulnerabilidad en el protocolo de red SMB de Microsoft en mayo de 2017, afectando a empresas y organizaciones en más de 150 países. Se estima que WannaCry infectó a más de 200,000 sistemas y causó daños económicos por valor de miles de millones de dólares.
2. NotPetya: Este ransomware apareció en junio de 2017 y se propagó a través de una actualización falsa del software de contabilidad ucraniano. Afectó a empresas en todo el mundo, pero especialmente en Ucrania, y causó daños económicos por valor de miles de millones de dólares.
3. Locky: Este ransomware apareció por primera vez en 2016 y se propagó a través de correos electrónicos de phishing. Afectó a empresas de todo el mundo y se estima que causó daños económicos por valor de cientos de millones de dólares.
4. Ryuk: Este ransomware se detectó por primera vez en agosto de 2018 y se propagó a través de correos electrónicos de phishing y vulnerabilidades en los sistemas de red. Se ha utilizado para atacar a empresas y organizaciones en todo el mundo, incluyendo hospitales y empresas de fabricación, y ha causado daños económicos significativos.
5. DarkSide: Este ransomware apareció en 2020 y se utilizó para atacar a la empresa de energía Colonial Pipeline en Estados Unidos en mayo de 2021. El ataque provocó una interrupción en el suministro de combustible en la costa este de Estados Unidos y se pagó un rescate de 4.4 millones de dólares para recuperar los datos.



# Casos de Ransomware en España



- 1. El ataque a SEPE:** En marzo de 2021, el Servicio Público de Empleo Estatal (SEPE) de España sufrió un ataque de ransomware que dejó a la organización sin acceso a sus sistemas informáticos durante varios días. El ataque afectó a los servicios de empleo en todo el país y se sospecha que pudo ser perpetrado por un grupo de ciberdelincuentes rusos.
- 2. El ataque a Everis:** En septiembre de 2019, la empresa de servicios de consultoría tecnológica Everis sufrió un ataque de ransomware que afectó a sus sistemas informáticos en España y otros países. Los atacantes exigieron un rescate en criptomonedas para desbloquear los sistemas.
- 3. El ataque a Redes Energéticas Nacionales (REN):** En diciembre de 2020, la empresa española REN sufrió un ataque de ransomware que afectó a su red de telecomunicaciones. Aunque la empresa aseguró que no se produjo una interrupción en el suministro de energía, el ataque demuestra la vulnerabilidad de las infraestructuras críticas a este tipo de amenazas.
- 4. El ataque a la Universidad de Málaga:** En agosto de 2020, la Universidad de Málaga sufrió un ataque de ransomware que afectó a sus sistemas informáticos y obligó a la organización a suspender las clases en línea durante varios días.



[Iniciar sesión](#)



**Smartphones, móviles y tablets**  
Durabilidad, Innovación, Fiabilidad  
esprinet® Consiguelo en Esprinet, mayorista oficial de Crosscall



GARANTÍA DEL FABRICANTE  
**5 AÑOS**



---

[Números anteriores](#)
[Revista Digital](#)
[IT Webinars](#)
[IT Televisión](#)
[IT Whitepapers](#)
[Almacenamiento IT](#)
[Discover Micro Focus](#)

[Impresión Digital](#)
[Content Marketing](#)
[TI para empresa](#)
[IT Trends](#)
[Opinión](#)
[Ofertas de Empleo TI](#)

Negocio Cloud RentableBuscar

# 9 de cada 10 empresas españolas fueron atacadas por ransomware en 2022

Seguridad 01 MAR 2023

```
settings: {path: "page/postcode"},  
a.user.postcode"}  
ore/src/lib/dat  
b/dataElement  
e/src/lib/d  
\\/(apps  
Code.js",  
.js", sett  
settings:  
a.product  
rc/lib/d  
case l:re  
n undefin  
idow.perform  
""}, "tool
```





DMI Computer  
www.dmi.es

KIOXIA

Juntos compartimos.

USB 2.0



# Ataque de ransomware a compañía de oleoducto afecta el suministro de combustible en Estados Unidos

17 estados afectados declararon estado de emergencia luego de que Colonial Pipeline, la compañía de oleoducto más importante del país, se viese obligada a la interrupción sus sistemas para intentar controlar el ataque.

# CODIGO POLIMORFICO

Un **código polimórfico** es aquel que sirve para **mutarse a si mismo** mientras mantiene su funcionalidad original intacta. Esta técnica es usada por el malware para ocultar su presencia y evitar ser descubierto. Lo que hacen es utilizar técnicas de ofuscación de código y encriptación. Esta técnica de ofuscación sirve para que el programa sea difícil de leer y comprender.



## BOTNETS-sistema de control hacker

- Botnet es un término que hace referencia a un conjunto o red de robots informáticos o bots, que se ejecutan de manera autónoma y automática. El artífice de la botnet puede controlar todos los ordenadores/servidores infectados de forma remota.



# INGENIERIA SOCIAL Y EL FACTOR HUMANO

¿Sabías que los ataques de ingeniería social suponen el 93% de las brechas de seguridad?



Según la investigación anual de Verizon sobre brechas de datos, los ataques de ingeniería social son responsables del **93%** de las brechas de datos que tienen éxito. Posibles escenarios y mensajes que puede recibir. Verizon es una empresa estadounidense de telecomunicaciones que ofrece servicios de telefonía, internet y televisión. Fundada en 1983, Verizon es una de las empresas de telecomunicaciones más grandes del mundo, con presencia en más de 150 países.



# ¿QUÉ ES LA INGENIERÍA SOCIAL?

DESCUIDO

MALA FE

## ¿Qué es?

- Esta es una mezcla entre ciencia, psicología y arte, por la que se intenta influir o manipular a una persona para que lleve a cabo acciones o facilite información confidencial, normalmente en contra de sus intereses.

## ¿Cómo funciona?

- Habitualmente de técnicas psicológicas que **combinadas** con ciertas **habilidades sociales** se aprovechan de la buena (o mala) fe de las personas de dentro de una organización, para que realicen determinadas acciones (como por ejemplo instalar software malicioso) u obtener de ellas información o acceso a zonas restringidas, y poder así llevar a cabo un ataque con éxito. También se conoce como “hackear a la persona” (human hacking).
- Un atacante externo puede aprovechar los descuidos o la escasa formación de un empleado para acceder a la información suficiente para realizar un ataque con éxito. También puede ser directamente el propio empleado (insider) el que de forma consciente (ya sea por venganza, por dinero, por coacción, etc.) proporcione la información al atacante o incluso lleve él mismo a cabo el ataque.



## INGENIERIA SOCIAL

# No presenciales:

Contacto con empleados, normalmente realizando algún tipo de suplantación por teléfono (vishing), correo electrónico (phishing), mensajería instantánea, etc.



# Presenciales:

Búsqueda en la basura (dumpster diving), seguimiento de personas y vehículos, vigilancia de salas y edificios, generación de situaciones de crisis, presión psicológica, soborno, chantaje o extorsión, etc.



# INGENIERIA SOCIAL: Y LLEGÓ LA INTELIGENCIA ARTIFICIAL. UN NUEVO DESAFIO



La técnica que describe se conoce como "Deepfake", que es una técnica de inteligencia artificial que se utiliza para crear contenido de audio y video falso e hiperrealista que parece ser auténtico. Los Deepfakes a menudo se utilizan en la ingeniería social y en campañas de desinformación para engañar a las personas y hacerles creer cosas que no son ciertas.

En el contexto empresarial, los Deepfakes pueden ser utilizados para suplantar la identidad de un ejecutivo o jefe de la empresa y engañar a los empleados o clientes para que tomen medidas que podrían ser perjudiciales para la empresa.

Es importante que las empresas sean conscientes de esta técnica y tomen medidas para protegerse contra ella, como la formación de los empleados sobre los riesgos de la ingeniería social y el uso de medidas de autenticación de la identidad, como el uso de contraseñas seguras y la autenticación de dos factores.



# Los 4 casos famosos de suplantación de identidad o deepfake: Tom Cruise y Zuckerberg figuraron

Directivos de empresas, presidentes y personas famosas fueron víctimas de la herramienta de inte

9 Dic, 2022

Escuchar

Compartir

PUBI



# Fraude del CEO: qué es y cómo las organizaciones pueden reconocer esta estafa

¿Qué es el fraude del CEO, por qué es tan frecuente y cómo pueden las organizaciones reconocer y defenderse de estas estafas?



Gabrielle Ladouceur Despins

4 May 2020 - 02:16PM



# ¿QUE ES EL PHISING?

Consiste en el envío masivo de comunicaciones (normalmente correos electrónicos) desde lo que parece un origen de confianza, con el aspecto de un escrito real en el que requiere al receptor que facilite determinada información, bien respondiendo al email, bien conectándose a una página web que parece real donde introducirá sus datos. El éxito del phishing se basa en el **envío masivo** y la probabilidad, dado que el número de víctimas potenciales es muy grande, es muy probable que alguna de ellas caiga en la trampa y facilite esa información que el atacante tan amablemente solicita.

## ¿Qué significa el smishing?

El **smishing** es una técnica **que** consiste en el envío de un SMS por parte de un ciberdelincuente a un usuario simulando ser una entidad legítima -red social, banco, institución pública, etc. -con el objetivo de robarle información privada o realizarle un cargo económico.

## ¿Qué significa el vishing?

Fraude por llamada telefónica, también suplantación por voz.

### Ejemplo

Se ha iniciado sesión desde un nuevo dispositivo, si no reconoce dicha acción, verifique inmediatamente en <https://seguridad-unicaja-online.co>



# TIPOS DE PHISING

## Spear-phishing:

Variante que perfecciona y personaliza la comunicación (la traducción sería pesca con arpón), adaptándola a cada individuo, gracias a un análisis previo de la empresa, los nombres de los empleados/jefes/personal de servicio técnico, nombres de clientes, etc.

En definitiva, cualquier información que pueda ser útil para hacer más creíble la comunicación que va a recibir la víctima.

Los envíos no son masivos como los mencionados anteriormente, sino muy dirigidos a un **grupo de posibles víctimas** concretas.

## Whaling:

Tiene como objetivo los directivos de la empresa, de manera que al igual que con el spear-phishing se personalizan mucho más las comunicaciones que se envían en lugar de hacer envíos masivos. Este tipo de técnica suele tener una alta probabilidad de éxito ya que los **directivos** no suelen asistir a las sesiones de concienciación o de formación que se organizan para los empleados.

## Watering-holes

(la traducción sería abrevaderos) es otra de las técnicas que, aunque no explota directamente el factor humano, sí que se suele emplear conjuntamente con técnicas de recogida de información como las comentadas anteriormente.

**Se trata de averiguar primero qué páginas o sitios web suelen visitar los empleados de la empresa objetivo, para infectar alguna de ellas con malware o con algún exploit específico**



# Ejemplo de phising

**NETFLIX**

Su elección > Cuenta > Actualizar > Confirmación

## Actualice su información de pago hoy

La nueva forma de pago se utilizará a partir del próximo periodo de facturación. Lo pagaremos suscripción mensual el primer dia de cada periodo de facturación.

---

Primer nombre\*

Apellido\*



# PELIGRO WILL ROBINSON



- En la actualidad las técnicas de phishing se están haciendo peligrosamente complejas, a través de aplicaciones se roban credenciales y se entra anónimamente en el correo de la víctima, realizando el atacante un análisis de los correos para realizar una personalización que es fácil caer, incluso se analiza la forma de escribir, los contactos o información relevante para enviar a otras víctimas correos del tipo:

## Ejemplo

“Hola Javier, como te dije la última vez, te envío de nuevo la factura rectificada”, se envía un fichero adjunto, que parece un PDF y si la persona se lo descarga ya lo tenemos infectado.



## 6. Robo de identidad y credenciales.

1. El robo de identidad se produce cuando alguien usa su información personal o financiera sin su permiso.
2. Le podrían robar su nombre y domicilio, su tarjeta de crédito o los números de su cuenta bancaria, su número de Seguro social o los números de su cuenta de seguro médico. Y los ladrones podrían usar esos datos para
3. Comprar cosas con sus tarjetas de crédito
4. Obtener tarjetas de crédito nuevas bajo su nombre
5. Abrir una cuenta de servicio de teléfono, electricidad o gas bajo su nombre
6. Robarle su declaración de impuestos
7. Usar su seguro de salud para obtener atención médica
8. Hacerse pasar por usted si los arrestan
9. Usar las redes sociales de manera fraudulenta.



[Suplantación de identidad y secuestro de cuentas: ¿cómo actuar? | Oficina de Seguridad del Internauta \(osi.es\)](#)



ACTUALIDAD

## Alerta por un fraude a clientes de Bankia-Caixabank: así puede evitarse

Varios clientes han alertado de llamadas o mensajes pidiendo que se compruebe información, alegando un falso cargo o haciendo referencia a un fallo en la seguridad.

---

As.com

Actualizado a: 29 de agosto de 2021 08:06 CEST



AD

➤ Suscríbete a  
nuestra newsletter

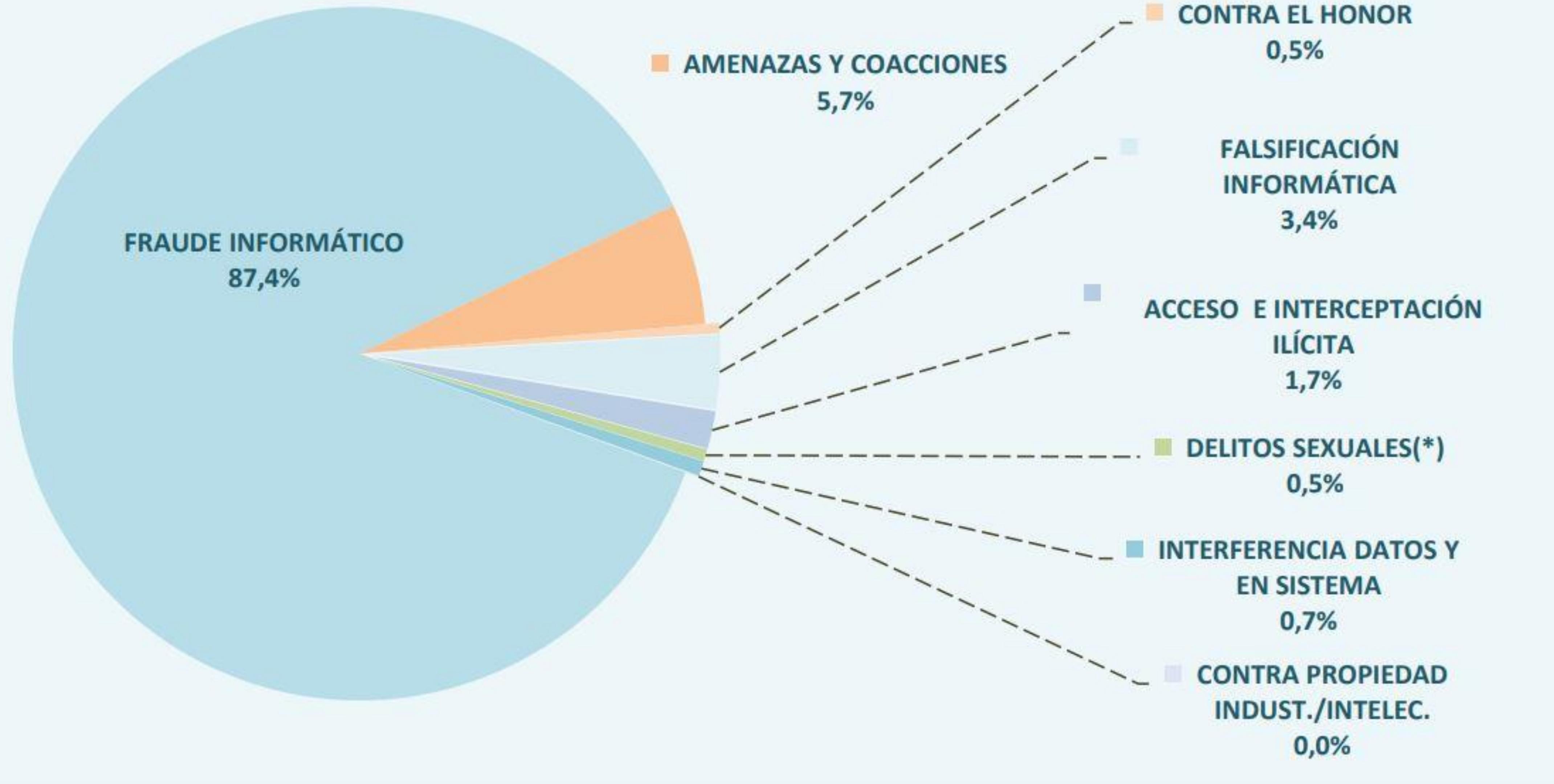


# Ataque por fuerza bruta

- Un **ataque de fuerza bruta** es un intento de descifrar una contraseña o nombre de usuario, de buscar una página web oculta o de descubrir la clave utilizada para cifrar un mensaje, que consiste en aplicar el método de prueba y error **con** la esperanza de dar **con** la combinación correcta finalmente.



# Gráfico principales ataques

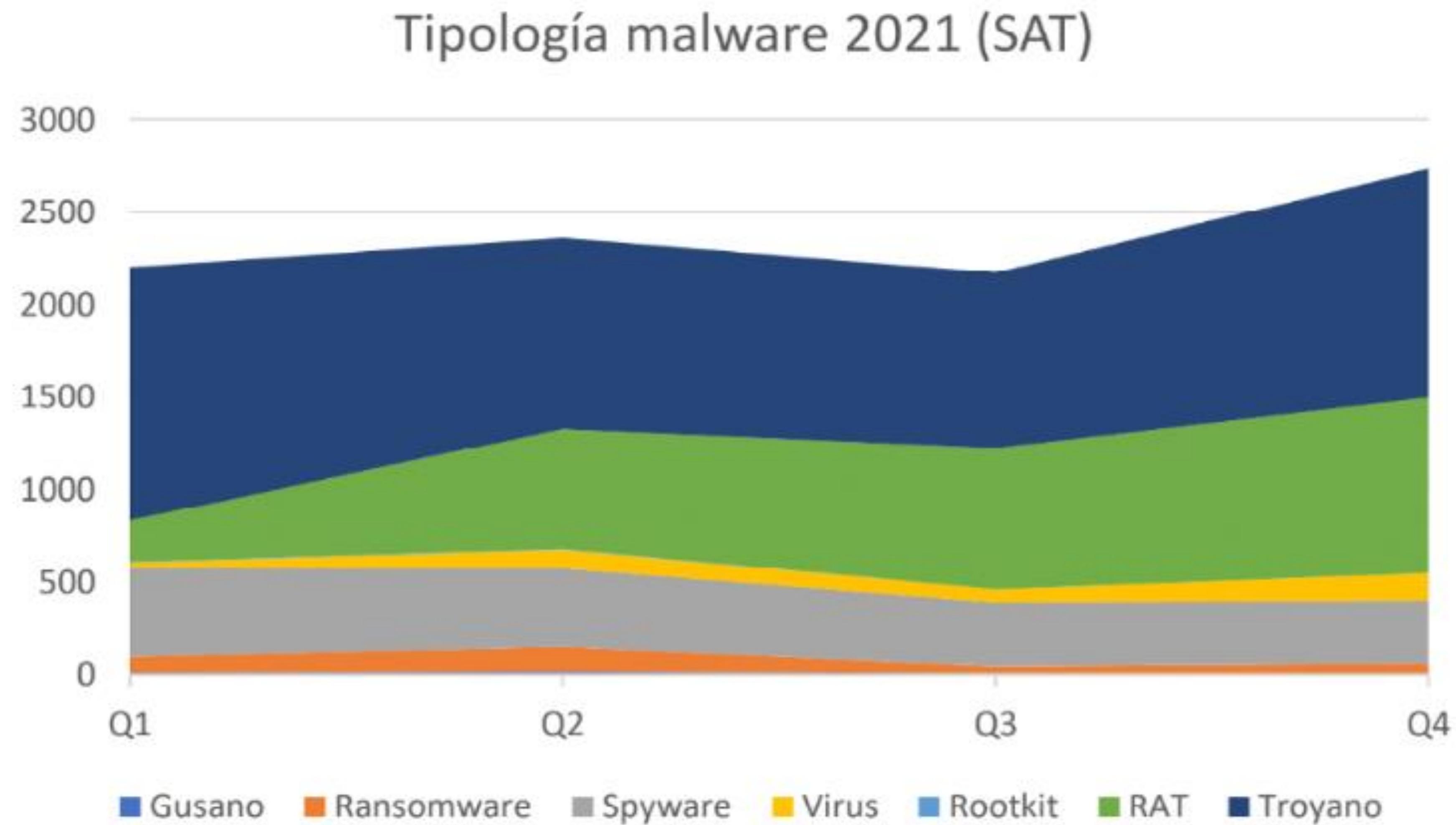


DATOS DEL AÑO 2021

[https://administracionelectronica.gob.es/pae/Home/pae\\_Actualidad/pae\\_Noticias/Anio2022/Noviembre/Noticia-2022-11-04-Informe-Panorama-Amenazas-ciberseguridad-2022.html#.ZDvje\\_ZBxD8](https://administracionelectronica.gob.es/pae/Home/pae_Actualidad/pae_Noticias/Anio2022/Noviembre/Noticia-2022-11-04-Informe-Panorama-Amenazas-ciberseguridad-2022.html#.ZDvje_ZBxD8)



# Tipos de ataques 2021



## Otros Patrones de ataques

- Denegacion de servicios (Dos o Ddos)
- Man in the middle
- Inyección SQL.



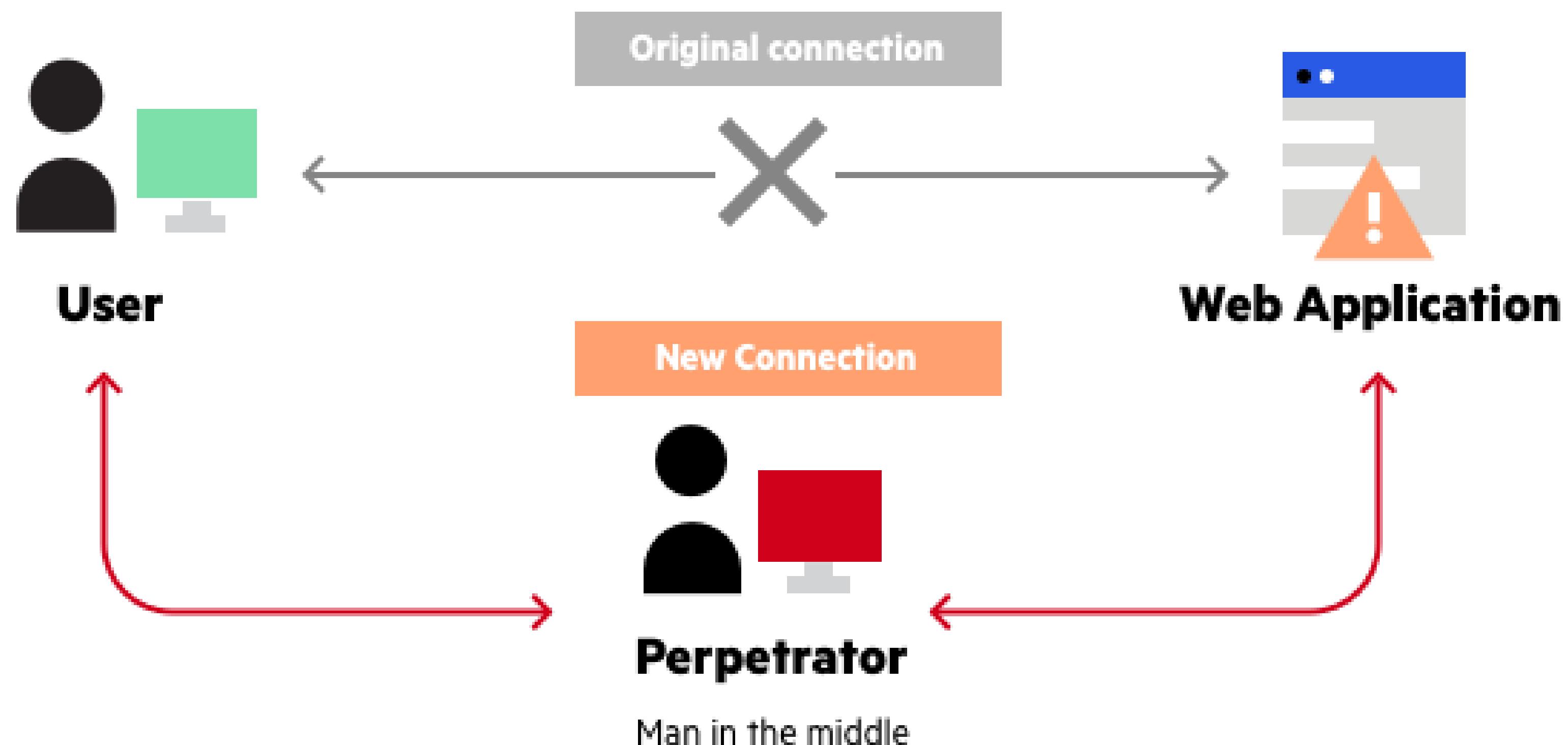
# Denegaciones de servicios

- En seguridad informática, un ataque de denegación de servicio, llamado también ataque **DoS**, es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.
- Un **ataque DDoS** tiene como objetivo inhabilitar un servidor, un servicio o una infraestructura. ... Durante un **ataque DDoS**, se envían simultáneamente múltiples solicitudes desde distintos puntos de la red. La intensidad de este «fuego cruzado» compromete la estabilidad, y, en ocasiones, la disponibilidad del servicio.



# ATAQUE MAN IN THE MIDDLE

- Por otro lado, un ataque de MitM es un tipo de ataque en el que un atacante intercepta la comunicación entre dos partes legítimas, para monitorear, manipular o injectar información en la comunicación sin que las partes lo sepan. Los vectores de ataque comunes para los ataques de MitM incluyen el uso de ARP spoofing, DNS spoofing, SSL stripping y otros.



# ATAQUE MAN IN THE MIDDLE: COMO SE LLEVA A CABO

- El ataque MitM se lleva a cabo generalmente en una red no segura o en una red Wi-Fi pública. Por ejemplo, un atacante podría configurar una red Wi-Fi falsa en un lugar público y nombrarla de forma similar a una red Wi-Fi legítima, como la del café local. Cuando los usuarios se conectan a la red falsa, toda su comunicación puede ser interceptada y manipulada por el atacante.
- Otro ejemplo de ataque MitM es cuando un atacante intercepta una conexión HTTPS cifrada, que normalmente se considera segura, utilizando técnicas de suplantación de certificados, por ejemplo, para engañar a un usuario y hacer que piense que está interactuando con un sitio web legítimo cuando en realidad está comunicándose con un sitio malicioso.



# Ataque de Inyección de SQL

- Ataque de Inyección de SQL: Este tipo de ataque aprovecha una vulnerabilidad en una aplicación web para injectar código malicioso en una base de datos, lo que puede permitir al atacante acceder a información confidencial.



## ¿Qué es Spoofing y sniffing)

- El "**spoofing**" es una técnica en la que un atacante falsifica su dirección IP, dirección MAC o algún otro identificador de red para engañar a la víctima y hacerle creer que el ataque proviene de una fuente confiable. El objetivo del spoofing puede ser ocultar la identidad del atacante o engañar a la víctima para que revele información confidencial.
- Por otro lado, el "**sniffing**" es una técnica en la que un atacante intercepta y lee el tráfico de red para obtener información confidencial, como contraseñas, nombres de usuario, información de tarjetas de crédito, etc. El sniffing se realiza mediante herramientas de software que capturan los paquetes de datos que circulan a través de la red y los analizan para extraer información útil.

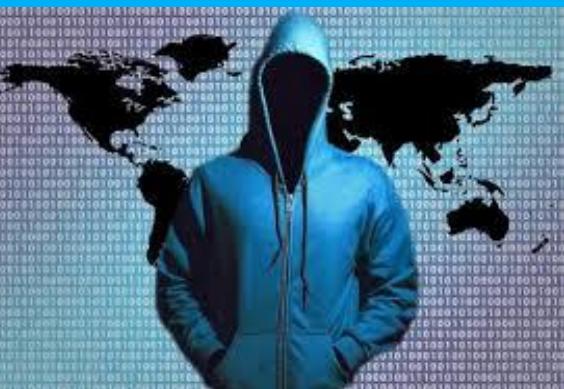
En cuanto a las aplicaciones que realizan estas técnicas, hay muchas herramientas de software disponibles en línea que pueden ser utilizadas para llevar a cabo ataques de spoofing y sniffing. Por ejemplo, el spoofing se puede realizar con herramientas como Nmap, Hping, Scapy, mientras que el sniffing se puede realizar con herramientas como Wireshark, tcpdump, Ettercap, entre otras.







Tercera parte:  
Como detectar si hemos sido atacados.  
Como podemos protegernos.



- 1º Riegos a los que nos enfrentamos.
- 2º Como prevenir un ciberataque.
- 3º Como protegernos de los ataques por ingeniería social.
- 4º Estos sitios web de pueden ayudar.
- 4º Herramientas para protegernos: los antivirus.
- 5º Actualizar los sistemas operativos, navegadores, app, aplicaciones.
- 6º Herramientas de análisis del tráfico de red.
- 7º Sistemas operativos para realizar Hacking ético.
- 8º Encriptación.
- 9º El futuro, que podemos esperar.



¿Cuáles son los riesgos a los que me puedo enfrentar?

1. Buscar por internet, a través de redes sociales.
2. Llamadas haciéndose pasar por otras personas.
3. Buscando en la mesa del usuario en una oficina.
4. Poner contraseñas sin apenas seguridad.
5. Hablar en voz alta y decirle a otro usuario la contraseña. O tenerla en un posit a la vista
6. Poner la contraseña y no mirar si detrás hay alguien mirando.
7. No proteger la cámara web o el micrófono.
8. No cambiar la contraseña cada poco tiempo.



# EL PROBLEMA DEL TOKEN ON AUTH

Podríamos definirlo como un conjunto de permisos que damos porque están almacenados en nuestro usuario y contraseña,  
como ejemplo

Cuando ingresamos en una web y no queremos definir nuestro usuario  
optamos  
por las opciones que vemos abajo

Ingrasa tu código de sección de 6 letras

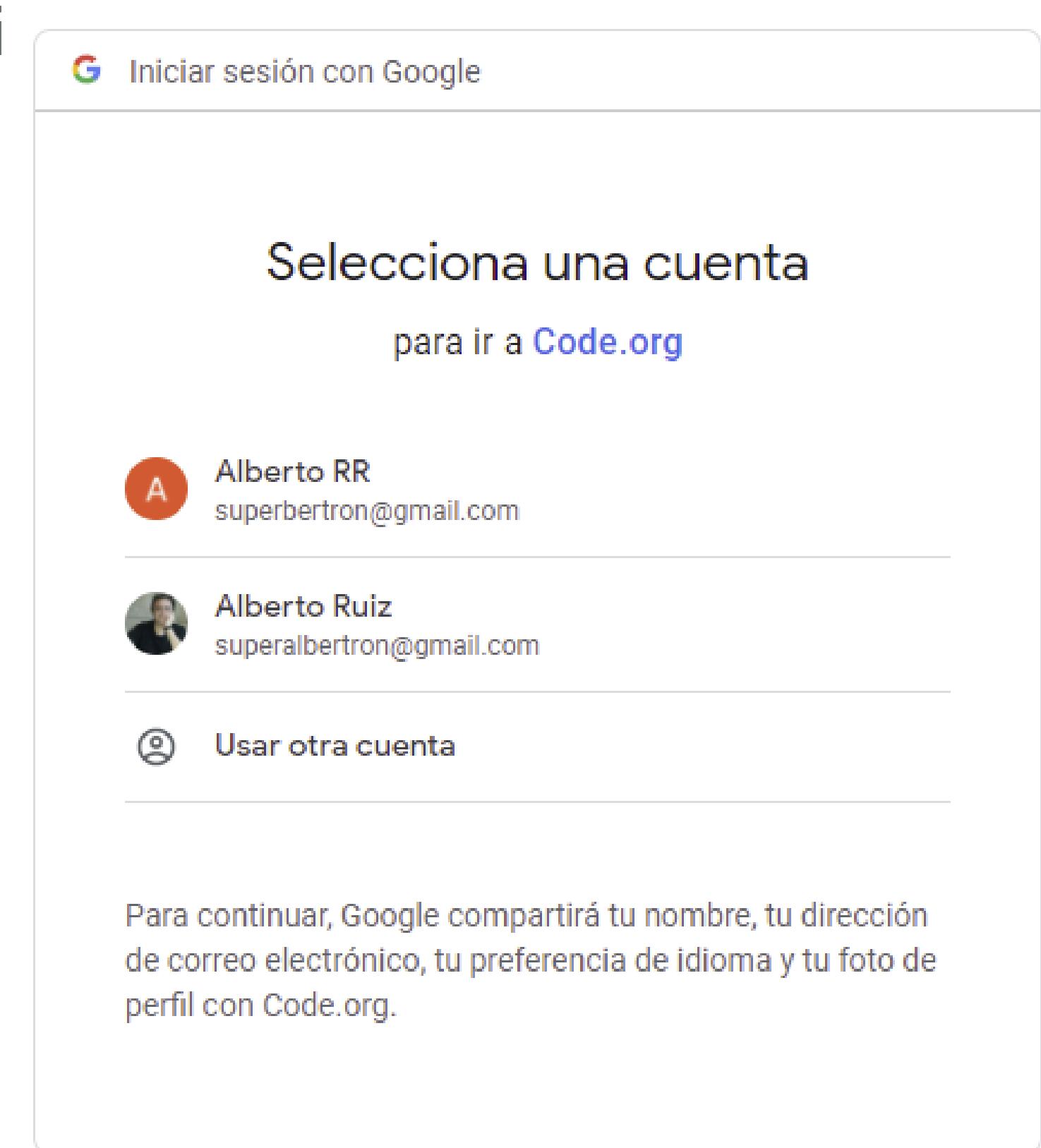
Código de sección (ABCDEF)

Go

**Continuar con Cuenta de Google**

**Continuar con Facebook**

**Continuar con Cuenta de Microsoft**



Español (España) ▾

Ayuda

Privacidad

Términos



Cuidado



- Debemos asegurarnos de que la **web sea lícita**, aunque el consejo es que demos de alta un correo y no usemos las opciones de Token porque le estamos dando acceso a información de nuestros contactos, etc.
- Hay Phishing tan efectivo que cuando le damos **el token**, de manera lícita pues la web que nos aparece es por ejemplo de Hotmail, después nos redirige a una web ilícita donde previamente nos ha robado nuestro Token, y pueden entrar de manera anónima a nuestro correo electrónico.



## Como protegernos ante ataques de ingeniería social

- **Nunca compartas tus contraseñas con nadie.** Asegúrate de utilizar contraseñas seguras que contengan una combinación de letras, números y símbolos. También puedes utilizar un administrador de contraseñas para generar y almacenar contraseñas seguras.
- **No reveles información personal o confidencial:** No reveles información personal o confidencial, como tu número de seguro social o información bancaria, a menos que estés seguro de la identidad de la persona o entidad que te lo solicita.

**Verifica la identidad del remitente:** Si recibes un correo electrónico o una llamada telefónica que solicita información personal o financiera, verifica la identidad del remitente. No hagas clic en enlaces sospechosos o descargas archivos adjuntos desconocidos.

**Capacita a tus empleados:** Si eres dueño de una empresa, capacita a tus empleados en técnicas de seguridad y educación en ciberseguridad para que estén preparados para detectar y prevenir ataques por ingeniería social.



# ¡¡¡Los incidentes de CIBERSEGURIDAD, deben denunciarse!!!!

**1. Identifica el tipo de incidente:** Identifica el tipo de incidente de ciberseguridad que has sufrido, como un ataque de phishing, un robo de identidad o un ataque de malware.

**2. Toma medidas inmediatas:** Toma medidas inmediatas para limitar el impacto del incidente. Por ejemplo, si crees que tu cuenta ha sido comprometida, cambia todas tus contraseñas y cierra la sesión en todos los dispositivos.

**3. Recopila evidencia:** Recopila toda la evidencia relevante, como correos electrónicos de phishing, capturas de pantalla, registros de actividad y cualquier otro tipo de información que pueda ayudar a las autoridades a investigar el incidente.

**4. Contacta con las autoridades:** Contacta con las autoridades pertinentes, como la policía local, la Guardia Civil o la Agencia Española de Protección de Datos (AEPD), y presenta tu denuncia. Puedes presentar la denuncia en línea o en persona en una comisaría o en la sede de la AEPD.

**5. Proporciona toda la información relevante:** Proporciona toda la información relevante sobre el incidente, incluyendo detalles sobre el tipo de ataque, la fecha y la hora, la naturaleza de la información comprometida y cualquier otra información que pueda ayudar a las autoridades a investigar el incidente.

**6. Sigue el progreso de la denuncia:** Sigue el progreso de la denuncia y colabora con las autoridades en todo lo posible. Es posible que te pidan más información o que necesiten que les proporciones acceso a tus dispositivos o cuentas para investigar el incidente.



# Pasos para prevenir un ciberataque

1. **Proteger los equipos.** Cualquier dispositivo electrónico que se tenga en casa o la oficina debe estar completamente actualizado. ...
2. **Contraseñas fuertes.** ...
3. **Utilizar protocolos de seguridad.** ...
4. **Comprobar la autenticidad de enlaces y perfiles.** ...
5. **Evitar dar datos personales.** ...
6. **No descargar contenido pirata.** ...
7. **Realizar una copia de seguridad.**
8. **Comprobar que las fuentes de los correos son fidedignas.**
9. **Nunca compartas tus claves de acceso.**
10. **Activa la verificación en dos pasos.**
11. **Instalar y mantener actualizado tu antivirus.**



# Pasos para prevenir un ciberataque

11. **No aceptes a desconocidos en redes sociales ni en otros medios.**
12. **Comparte información y archivos solo con gente y por canales de confianza.**
13. **No uses redes publicas para información importante**
14. **Uso únicamente de herramientas reconocidas por la empresa.**
15. **Control de la seguridad perimetral.**
16. **Establecer firewall para evitar la propagación.**
17. **Cifrado de dispositivos.**
18. **Gestión de accesos e identidades.**
19. **Usar certificados digitales.**
20. **Configurar la seguridad en los navegadores.**



## Web importantes

- [INCIBE | INSTITUTO NACIONAL DE CIBERSEGURIDAD](#)
- [www.osi.es OFICINA DE SEGURIDAD DEL INTERNAUTA](#)
- [CCN-CERT \(cni.es\) CENTRO CRIPTOGRAFICO NACIONAL](#)
- [CVE - Common Vulnerabilities and Exposures \(CVE\) \(mitre.org\)](#)  
VULNERABILIDADES



# Antivirus

Un antivirus es un programa diseñado para detectar, prevenir y eliminar software malicioso o virus informáticos. Los virus informáticos son programas diseñados para dañar, interferir o tomar el control de un sistema informático sin el consentimiento del usuario.

Existen diferentes tipos de antivirus, entre ellos:

Antivirus basados en firma: estos antivirus comparan el software malicioso conocido con los archivos en el sistema. Si se detecta un virus, el antivirus lo elimina o lo pone en cuarentena.

Antivirus basados en comportamiento: estos antivirus monitorean el comportamiento del software y detectan actividades sospechosas, como la creación de archivos o la modificación del registro de Windows.



## Antivirus: opciones

- 1. Protección en tiempo real:** esta opción permite al antivirus detectar y bloquear cualquier amenaza en tiempo real mientras se navega por Internet o se usa el ordenador.
- 2. Escaneo programado:** esta opción permite al usuario programar el antivirus para que realice escaneos automáticos en un horario predefinido, lo que ayuda a mantener el sistema protegido sin necesidad de realizar un análisis manual.
- 3. Análisis completo del sistema:** esta opción permite al usuario realizar un análisis completo del sistema para detectar cualquier amenaza existente en el ordenador.
- 4. Protección de correo electrónico:** esta opción permite al antivirus proteger la bandeja de entrada de correo electrónico del usuario, detectando y bloqueando mensajes de correo electrónico maliciosos.
- 5. Protección de la navegación:** esta opción permite al antivirus bloquear sitios web maliciosos y proteger contra phishing y otros tipos de ataques en línea.
- 6. Protección de dispositivos móviles:** algunos antivirus también ofrecen protección para dispositivos móviles, como smartphones y tablets, protegiendo contra aplicaciones maliciosas y otras amenazas.
- 7. Firewall:** algunos antivirus incluyen un firewall integrado para proteger contra ataques de red y otras amenazas.



## Que es un FIREWALL

Un firewall (o cortafuegos) es un componente de seguridad de red que se utiliza para controlar y filtrar el tráfico de red que entra y sale de una red informática. El firewall actúa como una barrera entre la red interna y externa, permitiendo únicamente el tráfico autorizado y bloqueando cualquier tráfico no autorizado.

El firewall puede estar integrado en un dispositivo de red, como un router, o puede ser un software que se ejecuta en un servidor o en un dispositivo de usuario final. El firewall utiliza una serie de reglas y políticas para determinar qué tráfico se permite y qué tráfico se bloquea.



Entre los antivirus más destacados se encuentran:

**Norton Antivirus:** es un antivirus de pago que ofrece protección en tiempo real, detección de malware avanzado y una amplia gama de funciones de seguridad.

**Kaspersky Antivirus:** es otro antivirus de pago que ofrece una excelente protección contra virus, spyware, malware y otras amenazas en línea.

**Windows Defender:** es el antivirus incorporado en Windows 10. Ofrece protección en tiempo real y se actualiza automáticamente.



# Windows Defender



Aunque Windows Defender es una opción sólida para la protección antivirus, es importante tener en cuenta que puede no ser suficiente para proteger contra todas las amenazas en línea. Por lo tanto, se recomienda complementar la protección con otro software de seguridad de terceros para obtener una protección más completa.

**1. Protección en tiempo real:** Windows Defender monitorea continuamente el sistema en busca de amenazas en tiempo real, detectando y eliminando cualquier malware o virus que se encuentre.

**2. Escaneo programado:** Windows Defender permite al usuario programar escaneos automáticos en un horario predefinido, lo que ayuda a mantener el sistema protegido sin necesidad de realizar un análisis manual.

**3. Análisis completo del sistema:** Windows Defender permite al usuario realizar un análisis completo del sistema para detectar cualquier amenaza existente en el ordenador.

**4. Protección de correo electrónico y navegación:** Windows Defender protege contra phishing y otros tipos de ataques en línea, y también puede escanear correos electrónicos en busca de archivos maliciosos.

**5. Protección de dispositivos externos:** Windows Defender puede escanear dispositivos externos, como unidades USB, para detectar y eliminar amenazas.

**6. Control de aplicaciones y navegación:** Windows Defender también puede controlar y bloquear aplicaciones y sitios web específicos que puedan representar una amenaza para el sistema.

**7. Firewall de Windows:** además de la protección antivirus, Windows Defender también incluye el Firewall de Windows, que ayuda a proteger contra ataques de red y otras amenazas.





## En un dispositivo móvil no es necesario un antivirus

Sí, es recomendable tener un antivirus instalado en tu smartphone, especialmente si usas tu dispositivo para realizar transacciones bancarias, compras en línea, acceder a correos electrónicos y otras actividades que puedan involucrar información sensible.

2.Norton Mobile Security: Este antivirus ofrece protección contra virus, malware, spyware y phishing, además de herramientas antirrobo y bloqueo de llamadas y mensajes de texto no deseados.

1.Bitdefender Mobile Security: Esta aplicación proporciona protección en tiempo real contra virus y malware, así como funciones adicionales como protección de la privacidad y antirrobo.

2.Kaspersky Mobile Antivirus: Este antivirus ofrece protección contra virus, malware y spyware, además de protección de la privacidad y herramientas antirrobo.



# Gestores de contraseñas seguras

- 1. Cifrado de extremo a extremo:** Un buen gestor de contraseñas debe tener cifrado de extremo a extremo para proteger tus contraseñas. Esto significa que tus contraseñas se cifran en tu dispositivo antes de ser enviadas a los servidores del gestor de contraseñas. De esta manera, sólo tú tienes acceso a tus contraseñas.
- 2. Autenticación de dos factores:** Un buen gestor de contraseñas debe tener autenticación de dos factores para proteger tus datos. Esto significa que además de tu contraseña principal, también necesitarás introducir un código de seguridad adicional para acceder a tus contraseñas.
- 3. Generación de contraseñas fuertes:** Un buen gestor de contraseñas debe ser capaz de generar contraseñas fuertes y únicas para cada cuenta que tengas. Estas contraseñas deben ser largas, complejas y difíciles de adivinar.
- 4. Sincronización multiplataforma:** Un buen gestor de contraseñas debe ser capaz de sincronizarse en diferentes plataformas y dispositivos. Esto significa que puedes acceder a tus contraseñas desde cualquier dispositivo con conexión a Internet.
- 5. Copia de seguridad y restauración:** Un buen gestor de contraseñas debe tener un sistema de copia de seguridad y restauración para evitar la pérdida de tus contraseñas en caso de un fallo técnico.
- 6. Auditoría de seguridad:** Un buen gestor de contraseñas debe tener auditoría de seguridad, lo que significa que se realizan regularmente pruebas de seguridad para garantizar que tu información se mantenga segura.

Algunos ejemplos de gestores de contraseñas seguros son **LastPass, Dashlane, 1Password y KeePass**. Es importante investigar y elegir una herramienta que se adapte a tus necesidades y que tenga características de seguridad sólidas.



# Configuración de autenticación en dos pasos: Gmail



- 1º Inicia sesión en tu cuenta de Gmail.
- 2º Haz clic en el icono de tu cuenta (en la esquina superior derecha) y selecciona "Cuenta de Google".
- 3º En la página de "Inicio de sesión y seguridad", desplázate hacia abajo y busca la sección "Verificación en dos pasos".
- 4º Haz clic en "Configuración" y sigue las instrucciones en pantalla para configurar la autenticación de dos pasos.
- 5º Elige el método de verificación que prefieras. Puedes recibir un mensaje de texto con un código, usar una aplicación de autenticación, o utilizar una llave de seguridad física.

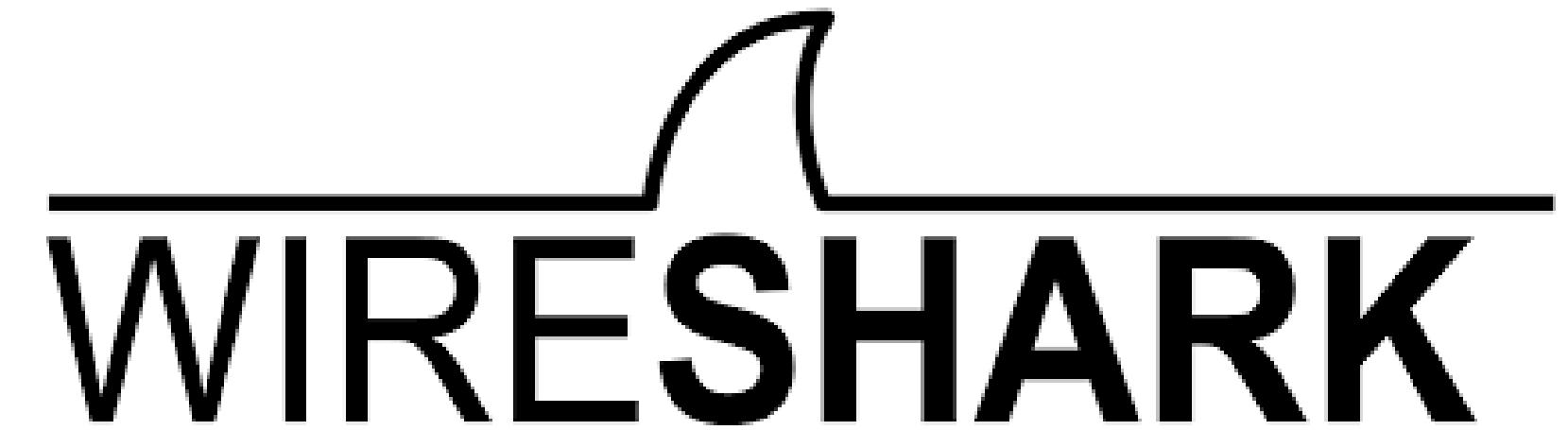


# Herramientas para analizar vulnerabilidades

- **Nessus:** Nessus es una herramienta de escaneo de vulnerabilidades muy popular y ampliamente utilizada.
- **OpenVAS:** OpenVAS es una herramienta de escaneo de vulnerabilidades de código abierto que es capaz de realizar pruebas en una amplia variedad de sistemas y aplicaciones, incluyendo sistemas operativos, aplicaciones web y dispositivos de red.
- **Qualys:** Qualys es una plataforma de seguridad en la nube que ofrece un conjunto de herramientas de seguridad, incluyendo un escáner de vulnerabilidades que puede detectar y priorizar vulnerabilidades en sistemas operativos, aplicaciones web y dispositivos de red.
- **Retina:** Retina es una herramienta de escaneo de vulnerabilidades que es capaz de identificar vulnerabilidades en sistemas operativos, aplicaciones web y bases de datos. También ofrece la capacidad de generar informes detallados sobre las vulnerabilidades encontradas.



# Wireshark



Wireshark es una herramienta de análisis de protocolos de red, que permite capturar y examinar el tráfico de red en tiempo real. Wireshark se utiliza comúnmente para analizar problemas de red, depurar problemas de conectividad, y para detectar y solucionar problemas de seguridad en la red. Entre las características más importantes de Wireshark se incluyen:

- 1. Captura de tráfico en tiempo real:** Wireshark es capaz de capturar y examinar el tráfico de red en tiempo real, lo que permite ver el flujo de datos en la red en tiempo real.
- 2. Análisis de protocolos:** Wireshark puede analizar y decodificar diferentes protocolos de red, como TCP, UDP, HTTP, FTP, SSH, DNS, entre otros. Esto permite identificar problemas de protocolo en la red.
- 3. Filtro y búsqueda de paquetes:** Wireshark permite filtrar y buscar paquetes específicos en la captura de tráfico, lo que facilita la búsqueda de información específica en la red.
- 4. Análisis de seguridad:** Wireshark puede ser utilizado para detectar y analizar amenazas de seguridad en la red, incluyendo el análisis de tráfico malicioso y la identificación de posibles vulnerabilidades en la red.



# Instrucciones en Windows y Linux para monitorizar la red

En **cmd** en Windows podemos usar netstat, nos da información sobre las conexiones entrantes y salientes

En **PowerShell**, puedes utilizar el cmdlet "Get-NetTCPConnection" para mostrar información sobre las conexiones de red activas. Sigue estos pasos para hacerlo:

- 1.Abre PowerShell. Puedes buscar PowerShell en el menú de inicio o presionando la tecla de Windows + R y escribiendo "powershell" y luego presionando Enter.
- 2.Una vez en PowerShell, escribe "Get-NetTCPConnection" y presiona Enter. Esto mostrará una lista de conexiones de red activas en tu computadora, junto con información sobre el estado de la conexión, el puerto utilizado, la dirección IP remota y local, entre otros datos.
- 3.Si deseas ver las conexiones que están utilizando un puerto específico, escribe "Get-NetTCPConnection | Where-Object {\$\_.LocalPort -eq <numero de puerto>}" y presiona Enter. Esto mostrará una lista de conexiones que utilizan el número de puerto especificado.

En **Linux**, puedes utilizar el comando "netstat" para mostrar información sobre las conexiones de red activas. Sigue estos pasos para hacerlo:

- 1.Abre la terminal en Linux. Puedes hacerlo buscando "Terminal" en el menú de aplicaciones o utilizando el atajo de teclado Ctrl+Alt+T.
- 2.Una vez en la terminal, escribe "netstat" y presiona Enter. Esto mostrará una lista de conexiones de red activas en tu computadora, junto con información sobre el estado de la conexión, el puerto utilizado, la dirección IP remota y local, entre otros datos.
- 3.Si deseas ver solo las conexiones activas en un momento determinado, escribe "netstat -a" y presiona Enter. Esto mostrará una lista de conexiones activas y escuchando en todos los puertos.
- 4.Si deseas ver las conexiones que están utilizando un puerto específico, escribe "netstat -an | grep <numero de puerto>" y presiona Enter. Esto mostrará una lista de conexiones que utilizan el número de puerto especificado.



# Que es el hacking ético

- El hacking ético (también conocido como **pentesting o testing de penetración**) es una técnica utilizada por profesionales de seguridad informática para identificar y evaluar las vulnerabilidades en un sistema o red de computadoras de manera legal y ética.
- Los hackers éticos **utilizan técnicas similares a las de los hackers malintencionados**, pero con la intención de descubrir y reportar las debilidades del sistema, en lugar de explotarlas con fines maliciosos. Esto se hace para ayudar a las organizaciones a protegerse contra futuros ataques, fortalecer su seguridad informática y garantizar la privacidad y protección de los datos de los usuarios.
- El proceso de hacking ético **generalmente implica la realización de pruebas de penetración controladas** y supervisadas en las que se simulan ataques informáticos para identificar posibles vulnerabilidades en los sistemas. Una vez identificadas, las vulnerabilidades se informan a la organización, lo que les permite tomar medidas para remediar los problemas y mejorar su seguridad informática.
- **El hacking ético es una práctica legal y ética**, siempre y cuando se realice con el consentimiento del propietario de la red o sistema que se está probando. Además, se espera que los hackers éticos respeten la privacidad y confidencialidad de los datos de la organización y que sigan las mejores prácticas de seguridad y ética profesional.



Un honeypot es un **sistema informático diseñado para ser atacado o comprometido**, con el fin de detectar, monitorear y analizar las tácticas y técnicas utilizadas por los atacantes. Un honeypot puede simular una variedad de sistemas y servicios, como servidores web, bases de datos y dispositivos de red.

Un honeypot **se configura para parecer atractivo para los atacantes**, con la intención de atraerlos y mantenerlos ocupados mientras se registran sus acciones y se analizan sus técnicas. Los honeypots también pueden utilizarse para engañar y desviar a los atacantes de los sistemas y recursos reales, reduciendo así el riesgo de daño real.

Existen diferentes tipos de honeypots, que se clasifican según su función y nivel de interacción con los atacantes.

- **Los honeypots de bajo interacción** simulan sistemas y servicios a un nivel superficial.
- **los honeypots de alta interacción** simulan sistemas y servicios a un nivel más profundo, lo que permite a los investigadores recopilar más información sobre las tácticas y técnicas utilizadas por los atacantes.

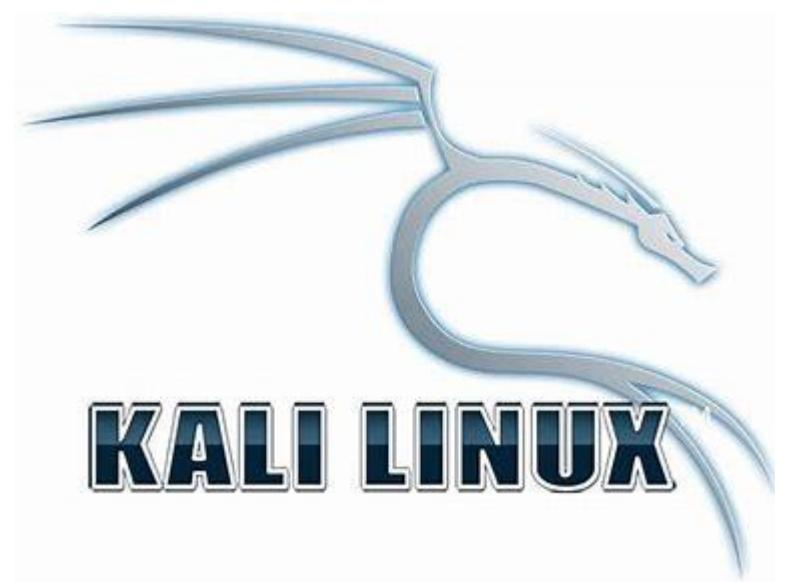
Los honeypots pueden ser una herramienta valiosa para los investigadores de seguridad y los equipos de respuesta a incidentes, ya que pueden proporcionar información valiosa sobre las amenazas y ayudar a mejorar la postura de seguridad de una organización al identificar y abordar las vulnerabilidades explotadas por los atacantes.



# Sistemas operativos que se usan para hacking ético

No existe un sistema operativo específico para hacking ético, pero hay algunos sistemas operativos que se utilizan con frecuencia en este campo debido a su capacidad para realizar pruebas de penetración y evaluaciones de seguridad. A continuación, te menciono algunos de los sistemas operativos más comunes para hacking ético:

- 1. Kali Linux:** Kali Linux es una distribución de Linux basada en Debian diseñada específicamente para realizar pruebas de penetración y evaluaciones de seguridad. Viene preinstalado con herramientas de hacking y pentesting, como Nmap, Metasploit Framework, Wireshark, entre otras.
- 2. Parrot Security OS:** Parrot Security OS es otra distribución de Linux basada en Debian, que se centra en la seguridad y privacidad de la información. Viene preinstalado con una gran cantidad de herramientas de seguridad y hacking, como Metasploit, Nmap, Aircrack-ng, entre otros.
- 3. BackBox:** BackBox es una distribución de Linux basada en Ubuntu que se centra en la seguridad de la información y el hacking ético. También viene preinstalado con una gran cantidad de herramientas de seguridad y hacking, como Metasploit, Nmap, Hydra, entre otros.
- 4. BlackArch:** BlackArch es una distribución de Linux basada en Arch Linux, que se centra en la seguridad de la información y el hacking ético. Viene preinstalado con más de 2000 herramientas de seguridad y hacking.





- Parrot Security OS es una distribución de Linux basada en Debian, que se enfoca en la seguridad y privacidad de la información. Es un sistema operativo diseñado para realizar pruebas de penetración, evaluaciones de seguridad y análisis forense. Además, también se puede utilizar como un sistema operativo diario para realizar tareas cotidianas.

**1. Metasploit Framework:** una de las herramientas más populares para pruebas de penetración, que permite a los usuarios identificar y explotar vulnerabilidades en sistemas informáticos.

**2. Nmap:** una herramienta de exploración de redes que permite a los usuarios descubrir dispositivos conectados a una red y obtener información detallada sobre ellos.

**3. Wireshark:** una herramienta de análisis de tráfico de red que permite a los usuarios capturar y analizar el tráfico de red en tiempo real.

**4. Aircrack-ng:** una herramienta para pruebas de penetración inalámbrica que permite a los usuarios monitorear y analizar redes inalámbricas y recuperar contraseñas WEP y WPA.

**5. John the Ripper:** una herramienta de cracking de contraseñas que permite a los usuarios probar la fortaleza de las contraseñas y descifrarlas si es posible.

**6. Hydra:** una herramienta de ataque de fuerza bruta que permite a los usuarios probar la fortaleza de las contraseñas en servicios como FTP, SSH y Telnet.

**7. Burp Suite:** una herramienta de pruebas de seguridad web que permite a los usuarios probar la seguridad de las aplicaciones web y encontrar vulnerabilidades como inyecciones SQL y XSS.



# Que es la encriptación

Hay varios sistemas de encriptación que se utilizan comúnmente, algunos de los más conocidos son:

**1. AES (Advanced Encryption Standard):** es uno de los algoritmos de encriptación más utilizados en todo el mundo. Fue adoptado por el gobierno de los Estados Unidos como el estándar de encriptación en 2002 y se utiliza para proteger datos sensibles en todo tipo de sistemas.

**2. RSA:** es un algoritmo de encriptación de clave pública que se utiliza para cifrar y descifrar mensajes. Se basa en el uso de dos claves diferentes: una clave pública que se comparte con otros usuarios para encriptar mensajes y una clave privada que se utiliza para descifrar los mensajes encriptados.

**3. Blowfish:** es un algoritmo de encriptación de clave simétrica que se utiliza ampliamente en sistemas operativos y software de seguridad. Fue diseñado por Bruce Schneier en 1993 y utiliza bloques de 64 bits para encriptar datos.

**4. Twofish:** es otro algoritmo de encriptación de clave simétrica que fue diseñado como una alternativa más segura al algoritmo Blowfish. Fue uno de los cinco finalistas en la competencia AES y es utilizado en varios sistemas de seguridad.

**5. DES (Data Encryption Standard):** es un algoritmo de encriptación de clave simétrica que fue desarrollado por IBM en la década de 1970 y utilizado por el gobierno de los Estados Unidos. Aunque es menos seguro que los estándares de encriptación modernos, aún se utiliza en algunos sistemas.



## El futuro, que podemos esperar.

Algunas de las tendencias clave que se espera que moldeen el futuro de la ciberseguridad incluyen:

- 1. Inteligencia artificial y aprendizaje automático:** se espera que estas tecnologías se utilicen cada vez más para identificar y mitigar amenazas de seguridad cibernética. La inteligencia artificial y el aprendizaje automático pueden ser utilizados para detectar patrones de tráfico inusual, identificar malware y analizar grandes conjuntos de datos para encontrar vulnerabilidades de seguridad.
- 2. Internet de las cosas (IoT):** con el aumento del número de dispositivos conectados a internet, se espera que la seguridad de IoT se convierta en una preocupación cada vez mayor. Se necesitarán soluciones de seguridad que puedan proteger los dispositivos IoT de manera efectiva y prevenir el acceso no autorizado.
- 3. Ciberseguridad en la nube:** se espera que el uso de servicios en la nube siga aumentando, lo que requerirá soluciones de seguridad que puedan proteger los datos almacenados en la nube y prevenir ataques a los servidores de la nube.
- 4. Amenazas avanzadas persistentes (APT):** estas amenazas están diseñadas para eludir la detección y permanecer en un sistema durante un período prolongado. Se espera que la lucha contra estas amenazas se vuelva cada vez más sofisticada a medida que los atacantes busquen formas de eludir las soluciones de seguridad.
- 5. Regulación de ciberseguridad:** se espera que los gobiernos y las organizaciones de todo el mundo adopten nuevas regulaciones para mejorar la ciberseguridad y proteger los datos. Las organizaciones también tendrán que cumplir con nuevas leyes y regulaciones, lo que requerirá una mayor inversión en ciberseguridad.



A woman with long dark hair, wearing a plaid shirt, is smiling and holding a smartphone in her right hand. She is wearing white headphones around her neck. The background is blurred, showing what appears to be an office or library setting.

# GRACIAS

Digitechfp: Alberto R,

Nombre ciudad  
[www.digitechfp.com](http://www.digitechfp.com)

