**LOS VIRUS INFORMÁTICOS.**

**¿Qué es un virus informático?**

Los virus son programas informáticos que tienen como objetivo alterar el funcionamiento del computador, sin que el usuario se dé cuenta.

Estos, por lo general, infectan otros archivos del sistema con la intención de modificarlos para destruir de manera intencionada archivos o datos almacenados en tu computador.
Aunque no todos son tan dañinos. Existen unos un poco más inofensivos que se caracterizan únicamente por ser molestos.

**Métodos de infección:**

Hay muchas formas con las que un computador puede infectarse con virus. Por ejemplo:
Mensajes dejados en redes sociales como Twitter o **Facebook**.
**Archivos adjuntos** en los mensajes de **correo electrónico**.

- Sitios web sospechosos.
- Insertar USBs, infectados.
- Descarga de aplicaciones o programas de internet.
- Anuncios publicitarios falsos.

**¿Cómo infecta un virus el computador?**

- El usuario instala un programa infectado en su computador. La mayoría de las veces se desconoce que el archivo tiene un virus.
- El archivo malicioso se aloja en la memoria RAM de la computadora, así el programa no haya terminado de instalarse.
- El virus infecta los archivos que se estén usando en ese instante.
- Cuando se vuelve a prender el computador, el virus se carga nuevamente en la memoria RAM y toma control de algunos servicios del sistema operativo, lo que hace más fácil su replicación para contaminar cualquier archivo que se encuentre a su paso.

**Algunos virus más conocidos.**

- Troyanos
- Gusanos
- Spyware
- Ransonware
- Botnets
- Apps maliciosas
- Adware

……

**Nota: Deben copiar en el cuaderno solo esta primera página.**

Tarea: Realizar un resumen en hojas sueltas que contenga SÓLO TRES páginas.

- Pág.1 La presentación,
- Pág.2 Un resumen del contenido de LOS VIRUS, que copian en el cuaderno
- Pág.3 El desarrollo de uno de los virus descritos más abajo.

Las hojas, pueden ser con líneas o sin líneas.

# ¿Cuáles son los principales tipos de *malware*?

**Veamos los principales tipos de virus y *malware* que podemos encontrarnos:**

## *Adware*

Es aquel software que ofrece publicidad no deseada o engañosa. Estos anuncios pueden aparecer en el navegador con pop-ups o ventanas con gran contenido visual, e incluso audios.
Se reproducen de manera automática con el fin de generar ganancias económicas a los creadores. En ocasiones este software provoca que el buscador predilecto del usuario sea cambiado por otro, generando errores en las búsquedas deseadas y entorpeciendo la experiencia de navegación del usuario.
**¿Cómo nos protegemos?** Evitemos abrir enlaces de descarga de páginas poco fiables y, cuando instalemos software, debemos revisar los pasos para que no se nos instale ningún buscador, programa o complemento sin que nos demos cuenta.

## *Spyware*

Este tipo de virus se encarga de recopilar de manera fraudulenta la información sobre la navegación del usuario, además de datos personales y bancarios. Un ejemplo de este tipo de virus son los *Keyloggers*, los cuales monitorizan toda nuestra actividad con el teclado (teclas que se pulsan), para luego enviarla al ciberdelincuente.

**¿Cómo nos protegemos?** El primer paso y más importante será la instalación y actualización de un buen sistema antivirus. Otra forma de protegernos es evitar conectar dispositivos desconocidos, como USB o discos duros externos.

## Gusanos

Este virus está creado con la capacidad de replicarse entre ordenadores. A menudo causa errores en la red, como consecuencia de un consumo anormal del ancho de banda ocasionado por este *malware*.

Los ciberdelincuentes suelen usar nombres llamativos en los enlaces para que este virus sea descargado como, por ejemplo, las palabras: sexo, apuestas, regalo o premio.
**¿Cómo nos protegemos?** Al igual que para los gusanos y resto de virus detallados, es importante tener actualizado nuestro sistema y sus defensas para estar protegidos y evitar se infectados, así como desactivar la función de “autoejecutar” los discos externos (memorias USB o discos duros). Si el antivirus está actualizado, también identificará y eliminará este tipo de amenazas que intenten colarse en nuestros dispositivos.

## Troyano

Este tipo de virus se presenta como un software legítimo, pero que, al ejecutarlo, le permite al atacante tomar el control del dispositivo infectado. Como consecuencia, nuestra información personal se encontraría en permanente riesgo, a merced del atacante para robar todo lo que quisiera de nuestros equipos infectados.
**¿Cómo nos protegemos?** Además de todas las medidas anteriores, como tener actualizado el sistema operativo y el antivirus, y analizar los dispositivos USB que se vayan a conectar a nuestro equipo, debemos tener mucho cuidado cuando navegamos por Internet, ya que pueden acabar instalándose algún archivo infectado o al acceder a páginas web fraudulentas.

## *Ransomware*

*Malware* que toma por completo el control del dispositivo bloqueando o cifrando la información del usuario para, a continuación, pedir dinero a cambio de liberar o descifrar los ficheros del dispositivo. Este software malicioso se transmite en el dispositivo, tal y como lo hace un gusano o un troyano. Pueden llegar camuflados en adjuntos de correos electrónicos o en páginas web poco fiables que nos inviten a descargar algún archivo bajo una apariencia inofensiva. También se aprovechan frecuentemente de fallos de seguridad del sistema operativo o incluso de aplicaciones.

**¿Cómo nos protegemos?** Mucho cuidado con los correos electrónicos maliciosos con algún adjunto. La mayoría de los ataques por *ransomware* se producen cuando el usuario ejecuta un archivo infectado. También es recomendable realizar copias de seguridad para que, en caso de infección, dispongamos de una copia de nuestros datos en otro lugar de almacenamiento.

### *Botnets*

Son redes de dispositivos infectados que los ciberdelincuentes utilizan para lanzar ataques, como el envío masivo de correos spam, ataques de denegación de servicio o DDoS, robos de credenciales, etc. Una vez que un dispositivo está infectado, entrará a formar parte de la red de *botnets* cuyo objetivo es seguir expandiéndose.

**¿Cómo nos protegemos?** Lo principal es hacer un buen uso de los dispositivos cuando nos conectamos a la red, teniendo un sistema actualizado con programas antivirus instalados, utilizando credenciales robustas y cambiando las contraseñas regularmente y no entrando en páginas web que puedan ser poco fiables. Otra fuente de infección son los correos maliciosos.

### Apps maliciosas

Cuando instalamos una app en nuestro dispositivo móvil, esta nos pide concederle una serie de permisos. A veces, estos permisos no tienen relación con la funcionalidad de la app o descargamos una app poco fiable que acaba por infectar nuestro dispositivo, tomar control y robar la información que tenemos almacenada en él como contactos, credenciales, imágenes, vídeos, etc.

**¿Cómo nos protegemos?** Cuando se trata de descarga de apps, lo primero que debemos tener en cuenta es utilizar tiendas oficiales. Además, debemos revisar las valoraciones y comentarios de otros usuarios e información del desarrollador. Al instalarla, nos pedirá aceptar una serie de permisos, que no debemos dar a no ser que esté relacionado con la función de la app. Por ejemplo, nunca le daríamos permiso a una app "Linterna" para acceder a nuestros contactos ¿verdad?

**¿Cómo puedo saber si mi dispositivo está infectado?**

Los ciberdelincuentes han logrado crear virus con capacidad de colarse y ocultarse en nuestros dispositivos de diferentes maneras. Hay algunas **pistas que pueden ayudarnos a identificar si nuestro dispositivo ha sido infectado**, tanto si es un ordenador sobremesa o portátil, como si es un dispositivo móvil:

**10 Síntomas de un equipo infectado**

**¡Mi móvil está poseído!**

Por suerte, **contamos con la ayuda de nuestro antivirus que, siempre y cuando lo mantengamos debidamente actualizado, detectará y eliminará una gran cantidad de este tipo de amenazas.** Aun así, este filtro no es infalible y puede que no detecte el 100% de los *malware* que tratan de infectarnos, por tanto, es posible que en un momento dado necesitemos ponernos manos a la obra para desinfectarlo. De manera adicional, tenemos a nuestra disposición herramientas y servicios gratuitos como "Conan mobile (móviles Android)" y el "Servicio Antibotnet". Utilicémoslos para protegernos de las distintas amenazas, ¡son gratuitos!

Finalmente, si nuestros equipos están infectados y no sabemos qué hacer, podemos pedir ayuda a INCIBE a través del teléfono gratuito y confidencial: 017. Los operadores nos indicarán cómo proceder.