SEGURIDAD

Entendemos por **seguridad informática** el conjunto de acciones, herramientas y dispositivos cuyo objetivo es dotar a un sistema informático de integridad, confidencialidad y disponibilidad. Tenemos que ser conscientes de que las pérdidas de información no pueden venir sólo de ataques externos sino que pueden producirse por errores nuestros o por accidentes o averías en los equipos.

El elemento clave de un sistema de información son los datos y hay dos principales amenazas externas al software y a los datos:

* **Código malicioso**(malware)
* **Ingeniería social**

### **1. Código malicioso (malware)**

El código malicioso o malware, es un programa que tiene como objetivo introducirse y hacer daño en un ordenador sin que el usuario lo note.

Entre sus objetivos podemos señalar:

* Robar información, datos personales, claves, números de cuenta.
* Crear redes de ordenadores zombis, denominadas también botnet, para ser utilizadas en el envío masivo de spam, phising, realización de ataques de denegación de servicio.
* Cifrar el contenido de determinados archivos para solicitar el pago de una cantidad para solucionarlo (Ransomware).

# VÍDEO: [**Qué es el Malware**](https://www.youtube.com/watch?v=Md9ergKwZ3Y)

Hay diferentes tipos de malware entre los que podemos destacar los siguientes:

**Virus**

Es un código malicioso que tiene como objetivos alterar el funcionamiento de un ordenador sin el conocimiento del

usuario. Por lo general incorporan código infectado en archivos ejecutables activándose los virus cuando se ejecuta este archivo. En ese momento el virus se aloja en la memoria RAM y se apodera de los servicios básicos del sistema operativo. Cuando el usuario ejecuta otro archivo ejecutable, el virus alojado en la RAM lo infecta también para ir de esta manera replicándose.

**Gusanos**

Es un tipo de virus. La principal diferencia entre gusano y virus es que el gusano no necesita la intervención humana para ser propagado, lo hace automáticamente, no necesita alojarse en el código anfitrión, se propaga de modo autónomo, sin intervención de una persona que ejecute el archivo infectado. Suelen apropiarse de los servicios de transmisión de datos para controlarlo. Por lo general los gusanos consumen mucha memoria provocando que los equipos no funcionen adecuadamente. Uno de los sistemas que utiliza el gusano para propagarse es enviarse a sí mismo mediante correo electrónico a los contactos que se encuentran en el ordenador infectado.

**Troyanos**

Son programas aparentemente inofensivos que tienen una función no deseada. Son realmente un programa dañino con apariencia de software útil que puede acabar siendo una gran amenaza contra el sistema informático.

Ejemplos de virus que se pueden identificar como troyanos serían:

* **Puertas traseras** (backdoors): Modifican el sistema para permitir una puerta oculta de acceso al mismo de modo que el servidor toma posesión del equipo como si fuese propio lo que permite tener acceso a todos los recursos, programas, contraseñas, correo electrónico, unas veces en modo de vigilancia y otras para modificar la información y utilizarla con fines no lícitos.
* **Keyloggers:** Almacenan todas las pulsaciones del teclado que realiza el usuario. Se utilizan normalmente para robar contraseñas.
* **Spyware**: Envía información del sistema el exterior de forma automática. Es un código malicioso que, para instalarse en un ordenador, necesita la participación de un virus o troyano, aunque también puede estar oculto en los archivos de instalación de un programa normal. Su cometido es obtener información de los usuarios que utilizan ese ordenado. El objetivo más leve y más común es aportar los datos a determinadas empresas de márketing online que, con posterioridad y por diferentes medios, correo electrónico, pop-ups, enviarán publicidad al usuario sobre los temas que detectaron que les podían interesar.

Estos programas espía pueden indagar en toda la información existente en el equipo, como listas de contactos, información recibida, enviada, por ejemplo el DNI, números de tarjetas de crédito, cuentas bancarias, domicilios, teléfonos, software que tiene instalado, direcciones IP, servidores de internet que utiliza, páginas web que visita, tiempo de permanencia en un sitio web, etc. Por otra parte, el spyware puede servir como sistema de detección de delitos cometidos a través de internet, es muy representativa la utilización por la Policía española de código malicioso incorporado a fotos de menores que permite identificar casos de corrupción de menores y pederastia.

* **Adware**: Programas de publicidad que muestran anuncios, generalmente mediante ventanas emergentes o páginas del navegador.

**Bot malicioso**

También son conocidos como **robot web**, "bot" es la simplificación de robot, se trata de un programa que pretende emular el comportamiento humano. Hay bots con fines lúdicos, que buscan mantener un chat con una persona, ser contrincante en un juego o de rastreo como los que usan los buscadores google o yahoo que tienen como finalidad detectar el movimiento que se produce en los sitios webs a los que enlazan y ofrecen las novedades en las búsquedas de los usuarios. Los bots maliciosos son realmente troyanos de puerta trasera, con la particularidad de que se instalan en los equipos vulnerables mediante el sistema de rastreo en internet. Una vez infectado el equipo envía una señal a su creador y pasa a formar parte de una botnet o red de bots.

A los bots se les denomina zombis, pues cumplen las órdenes de los ciberdelincuentes que los crearon. Así pueden reenviar spam y virus, robar información confidencial o privada, enviar órdenes de denegación de servicio en internet o hacer clic automáticamente en anuncios publicitarios en la página web del ciberdelincuente que pagan por clic efectuado