# Código malicioso ¿Qué es y qué tipos hay?



El código malicioso es lo que vulgarmente conocemos como **virus o** [**malware**](https://www.ymant.com/servicios-informaticos/seguridad/)**.**

Las empresas destinan un gran esfuerzo en luchar contra estas amenazas, por eso es importante saber cuáles son las más comunes y en que nos afecta como usuarios.

Se debe tener especial atención por parte de las empresas en asegurar que sus herramientas y dispositivos aseguren una integridad, confidencialidad y disponibilidad de los datos. No olvidemos que los datos de una empresa son lo que garantizan la continuidad de la misma. Una pérdida o robo de los mismos, perjudicaría gravemente a la empresa afectando tanto a su reputación como a la actividad normal de su empresa, pudiendo significar incluso el cierre del negocio.

## **¿Qué es el código malicioso o malware?**

Son programas que tienen como objetivo acceder a tu sistema sin que detectes su presencia.

En función de la intención del Cracker, el programa podría:

* Robar credenciales, datos bancarios, información…
* Creación de redes con ordenadores botnet.
* Cifrado del contenido. Con esto se intenta que los usuarios paguen un rescate por sus datos.

## **¿Qué tipos de código malicioso existen?**

### Virus

Tiene como objetivo alterar el funcionamiento de los equipos infectados, su modo de actuar es mediante la ejecución del código, alojarse en la memoria RAM. Por lo que son realmente dañinos a la hora de consumir recursos de nuestro equipo, provocando una pérdida de productividad o daños a nuestros datos.

### Gusanos

También conocidos como Worms tienen como peculiaridad replicarse a sí mismo sin la necesidad de una persona. Estos se adhieren a la memoria RAM y ocasionan problemas debido a que al multiplicarse consumen recursos. Son capaces de auto propagarse por medio de la red.

### Troyanos

Los troyanos son denominados así por el hecho de aparentar un software inofensivo para el usuario, pero que al ejecutarlo permite al atacante hacerse con el acceso al equipo infectado. Estos por lo general no provocan daños al sistema, pero se usan para el robo de datos y credenciales personales.

### Keyloggers

Son software con intención de registrar las pulsaciones realizadas en el teclado, de esta forma el registro de lo que escribimos es enviado al delincuente, lo que pone en peligro contraseñas importantes como: números de tarjetas bancarias u información privada.

### Spyware

Estos programas recopilan información de tu equipo sin el consentimiento del propietario, estos softwares utilizan CPU y memoria RAM. Entre sus funciones reduce el rendimiento del sistema, enseñan anuncios de programas (por lo que en ocasiones se les denomina adwares), abren ventanas emergentes, instalan otros programas…

### Bots maliciosos

Son considerados como troyanos de puerta trasera, se instalan en equipos vulnerables mediante un sistema de rastreo en internet, una vez infectado el equipo, los ordenadores forman parte de una botnet y cumplen las órdenes de los ciberdelincuentes.

### Virus de macros

Estos virus usan documentos de Word o Excel para ejecutar macros en nuestra biblioteca de macros y acabará ejecutándose en diferentes documentos que se abran con la aplicación.

De esta forma se puede infectar equipos mediante documentos aparentemente normales como un Word, Excel, Access y similares.

Sus efectos suelen ser desde el robo de los contactos de correo electrónico, hasta borrar tus datos. Estas son las principales amenazas de lo que conocemos como código malicioso, para evitar ser víctima de estos [malwares](https://es.wikipedia.org/wiki/Malware) siempre debemos tomarnos la seguridad informática en serio y contar con elementos como firewalls y antivirus. Además de asegurarnos de que contamos con una buena formación en seguridad informática.