

SEGURIDAD INFORMÁTICA

Conceptos básicos

Seguridad informática

- Consiste en asegurar que los recursos informáticos de una organización se usen adecuadamente, y sólo pueda acceder personal autorizado y con los permisos adecuados
- Para que un sistema informático se considere seguro, debe tener 4 características:
 - **Integridad:** la información sólo puede modificarla quien esté autorizado
 - **Confidencialidad:** la información sólo puede leerla el personal autorizado
 - **Disponibilidad:** la información debe estar disponible cuando se necesita
 - **Irrefutabilidad:** que no se pueda negar quién accedió o modificó una información

Tipos de amenazas y ataques

- Una **amenaza** es un evento que puede causar daños o pérdidas en un sistema informático
- Un **ataque** es una amenaza que ya ha ocurrido
- Los tipos más comunes son:
 - **Ingeniería social**: consiste en robar información directamente de las personas. Por ejemplo, haciéndose pasar por alguien (de un banco, por ejemplo) para pedirle información privada (número de tarjeta, o de cuenta). Se puede hacer por teléfono o por e-mail
 - **Virus, gusanos y troyanos**: son programas que se instalan en nuestro ordenador, y pueden dañarlo, o enviar a otros ordenadores información nuestra
 - **Spyware y adware**: los programas spyware reúnen información nuestra (contraseñas, etc) y la envían a otros lugares. Los adware envían información sobre webs que visitamos, etc, para que nos envíen publicidad después
 - **SPAM**: correo no deseado, que puede contener virus u otras amenazas, y nos satura las cuentas de correo electrónico

Medidas de seguridad

- Para hacer frente a esas amenazas, podemos tomar algunas medidas (aunque ninguna es 100% eficaz):
 - **Actualizar el software:** muchos programas dan parches y actualizaciones cada cierto tiempo para corregir defectos
 - **Usar antivirus:** para combatir virus, gusanos y troyanos. Existen gratuitos y de pago, y también existen online o instalables.
 - **Ejemplos:** AVG, Avast, Panda, Nod32, etc.
 - **Usar programas anti-spyware:** para eliminar el spyware y el adware
 - **Ejemplos:** Spybot Search & Destroy, Spyware Doctor, etc.
 - **Usar cortafuegos o firewalls:** son programas (e incluso dispositivos hardware) que controlan todo el tráfico que entra y sale de una red
 - Permite prohibir que se ejecuten algunas aplicaciones, o que se accede a algunas webs
 - **Ejemplos:** ZoneAlarm, BitDefender, Outpost, etc