2. Amenazas

2.1. Tipos de amenazas

Existen 3 tipos de amenazas según su origen:

Amenazas Humanas

Tipos de amenazas humanas más habituales:

- Usuarios con conocimientos básicos
- Hackers
- Antiguos empleados de una Organización

Amenazas lógicas

- Software Malicioso
- Vulnerabilidades del software

Amenazas Físicas

- Fallos en los dispositivos
- Accidentes
- Catástrofes Naturales

2.2. Conductas de seguridad

Técnicas de seguridad activa

El fin de las medidas de seguridad activa es evitar daños a los sistemas informáticos.

Para ello podemos utilizar diferentes estrategias:

- Empleo de **contraseñas** adecuadas y seguras (elegir una contraseña segura, comprobar la seguridad de una contraseña)
- **Encriptación** de los datos (codificar la información con una contraseña, cualquier persona que la intercepte no pueda ver el mensaje original)
- El uso de **software de seguridad** informática
- Control de Acceso
- Firmas y certificados digitales
- Utilizar protocolos seguros como HTTPS

Enlaces:

- Comprobar si nuestros datos han sido comprometidos
- https://howsecureismypassword.net/

Técnicas o prácticas de seguridad pasiva

Su fin es minimizar los efectos causados por un accidente, un usuario o un malware.

Estrategias:

- Hardware adecuado frente a accidentes y averías (refrigeración del sistema, conexiones eléctricas adecuadas, etc.)
- Realización de copias de seguridad (**backup**) de los datos (en más de un soporte y en distintas ubicaciones físicas)
- Herramientas de Limpieza
- Sistemas de Alimentación Ininterrumpida (**SAI**)
- Sistemas Redundantes