Tema 7: seguridad

Introducción

Un técnico de TI es responsable de la seguridad de los datos y el equipo informático en una organización. Debe entender las amenazas a equipos físicos y a datos.

Malware

Software desarrollado por ciberdelincuentes para realizar actos maliciosos. Se instala sin el conocimiento del usuario.

Una vez que esta instalado en un host puede cambiar configuraciones, eliminar archivos, recopilar información o abrir ventanas.

Llega a un ordenador a través de sitios web infectados, USB encontrado en la calle, descargar programas “gratis”…

Los sistemas no compatibles (no se ha actualizado) y heredados (el proveedor ya no brinda soporte) son especialmente vulnerables a esto.

Depende el objetivo existen varios tipos de malware:

* **Virus**: requieren la acción humana para propagarse. Este se oculta al adjuntarse al código del ordenador, el software o los documentos. Cuando se abre se ejecuta e infecta el ordenador.

Pueden modificar archivos, causar problemas de arranque, capturar información, acceder a cuentas de correo o también permanecer inactivo hasta ser invocado por el atacante.

* **Troyanos**
* **Adware**
* **Ransomware**
* **Rootkit**
* **Spyware**
* **Gusano**

Programas anti-malware

Antivirus falsos

Actualizaciones de archivos de firma

Remedio de sistemas infectados

Ataques de ingeniería social

Procedimientos de seguridad