TCPR7TRIM2- Seguridad e Integridad Digital

Objetivo:

- Identificar las medidas de seguridad que protegen y mantienen la información íntegra, estable y funcional, a través del estudio de software malicioso y riesgos virtuales.

Parte 1. Parte Teórica.

I. Identifica cada riesgo virtual con su concepto correspondiente:

1. Software que daña el acceso a un servicio o alterar la integridad de la información.	Virus
2. Se autoinstala para rastrear actividad personal del usuario sobre sus preferencias y gustos de navegación, para después enviarla a terceros para poder ofrecer servicios	Perfil falso
3. Es un acoso que una persona o grupo hace a alguien más, a través de la tecnología y el internet.	Spyware
4. Es un malware disfrazado de una aplicación o programa inofensivo o legitimo	Grooming
5. Software no deseado que envía información publicitaria, en forma de ventanas emergentes	Adware
6. Es un acoso o chantaje por parte de un adulto hacia un menor, por medio de la tecnología y el internet	Troyano
7. Es cuando una persona se hace pasar por alguien más	Ciberbullying

II. Anota dentro de cada afirmación, si es verdadera (V) o falsa (F).

1. Malware se refiere a códigos que normalmente dañan sistemas informáticos	
2. Al actualizar tu sistema operativo, ayudas a mejorar tu protección de equipo.	
3. Las amenazas son mejoras en la seguridad que permiten acceder a un sistema.	
4. Se llama "Hackear" cuando alguien ingresa sin permiso y de manera forzada a nuestros dispositivos.	
5. Si compartes tu contraseña con tus amigos y familiares cercanos, disminuyes el riesgo de pérdida de información.	