**Hacker :** El término “hacker hacker” es un concepto que se refiere a una persona que explota vulnerabilidades en redes y sistemas informáticos para obtener acceso no autorizado o control sobre archivos digitales.

<https://www.significados.com/hacker/>

**Cracker:** En el contexto de la informática y la seguridad cibernética, un cracker se refiere a una persona que intenta acceder a un sistema informático sin autorización, con el objetivo de violar la seguridad de manera ilegal

<https://ayudaleyprotecciondatos.es/2021/10/18/cracker/>

**Newbie:** también llamados n00b, noob, nooblet o nub, es una jerga de informática y otras áreas utilizada para describir aquel individuo que es nuevo en algo. ...

<https://www.alegsa.com.ar/Dic/newbie.php#gsc.tab=0>

**Wannabe :** se refiere a una persona que quiere aparentar ser un hacker o un experto en seguridad informática, pero no tiene los conocimientos y habilidades reales para serlo.

<https://es.wikipedia.org/wiki/Wannabe>

**Grey Hat:** El término Grey Hat Hacker o hacker de sombrero gris en Internet se refiere a un hacker que a veces puede violar las leyes o los estándares éticos típicos, pero por lo general no tiene la intención maliciosa típica de un hacker de sombrero negro.

<https://www.deltaprotect.com/glosario/grey-hat-hacker>

**¿Qué problemas crees que podrían causarse por un uso inadecuado del software?**

Podrían suponer un riesgo para la salud el uso prolongado de software, ya que puede generar alteraciones físicas y psicológicas.

**Vulnerabilidades Tempest**

Las vulnerabilidades TEMPEST se refieren a las posibilidades de interceptar información confidencial o clasificada a través de emisiones electromagnéticas no intencionadas (EEM) generadas por equipos electrónicos y electrónicos. Estas emisiones pueden ser detectadas y analizadas para obtener información sensible.

Las vulnerabilidades TEMPEST se encuentran en:

Equipos electrónicos y electrónicos: Monitores LCD, impresoras, terminales y otros dispositivos que emiten radiaciones electromagnéticas no intencionadas.

Instalaciones: La falta de protección adecuada en las instalaciones puede permitir la interceptación de EEM.

Certificación: Aunque algunos dispositivos tienen certificación TEMPEST, esto no garantiza que sean completamente seguros.

Ejemplos de vulnerabilidades

Monitores LCD modernos emiten radiaciones electromagnéticas más bajas que los CRT, pero aún pueden ser vulnerables.

Las grandes multinacionales y gobiernos pueden ser objetivos prioritarios para ataques TEMPEST debido al valor del conocimiento de la información.

La falta de protección adecuada en las instalaciones puede permitir la interceptación de EEM.