Seguridad en sistemas informaticos: Todo sistema que procese, almacene o transmita información tiene que cumplir una serie de requisitos.

1) Ha de preservar la información frente a alteraciones tanto fortuitas como deliberadas, debidas a fallos en el software o en el hardware, provocadas por agentes externos —incendios, interrupciones en el suministro eléctrico, etc. -- o por los propios usuarios.
2) En segundo lugar, es necesario evitar accesos no autorizados tanto al sistema como a su contenido.
3) El sistema debe garantizar que la información esté disponible cuando sea necesario

   Estos tres requerimientos quedan recogidos en los conceptos de integridad, confidencialidad y disponibilidad de la información respectivamente, y son los que hacen que podamos considerar seguro a un sistema.

   Por lo tanto, garantizar la seguridad de un sistema informático es un objetivo mucho más amplio y complejo que la simple protección de los datos mediante técnicas criptográficas. De hecho, hemos de tener en cuenta múltiples factores, tanto internos como externos.

Tipos de Sistemas según su conexión a redes:

1. Sistemas aislados:
   No tienen conexión a redes. Son muy pocos hoy en día. Su seguridad depende de controles físicos (cerraduras, cámaras) y del manejo correcto de los privilegios de los usuarios.

2. Sistemas interconectados:
   Son los más comunes. Están conectados a redes constantemente (como computadoras, celulares o consolas). Esto hace que la gestión de la seguridad sea más compleja y desafiante.

Principales aspectos de la seguridad en sistemas informáticos:

1. Seguridad física:
   Protege los soportes físicos de la información (no la info en sí). Incluye:
   - **Prevención de incendios y fallos eléctricos.**
   - **Medidas contra ataques físicos o terroristas.**
   - **Backups y control de acceso físico a los equipos.**
2. Seguridad en canales de comunicación:
   Los canales no suelen ser seguros, ya que están fuera de nuestro control. Por eso se deben aplicar mecanismos de protección, incluso en entornos hostiles o manipulados.
3. Control de acceso a los datos:

   Solo los usuarios autorizados deben acceder a la información. Esto requiere:
   - **Asignar privilegios individualizados.**
   - **Usar técnicas como el cifrado para proteger datos, incluso si alguien accede físicamente al dispositivo.**
4. Autenticación:

   Es necesario verificar la identidad:
   - **De los usuarios.**
   - **De los dispositivos.**
   - **De la información transmitida.**
     El objetivo es evitar suplantaciones de identidad.
5. No repudio:
   Garantiza que el emisor de un mensaje no pueda negar su autoría, lo cual es vital en contratos y transacciones.
6. **Anonimato:**
   Permite proteger la identidad de los usuarios en

situaciones sensibles (como votaciones o denuncias).
⚠️ Aunque **también puede usarse para actividades ilegales, lo que genera debates y dificultades para implementarlo en la industria.**