**Confidencialidad**

* **Significa:** Proteger la información para que **solo personas autorizadas** puedan acceder a ella.
* **Objetivo:** Evitar el **acceso no autorizado** a datos sensibles.
* **Ejemplos:**
  + Uso de contraseñas o cifrado.
  + Restricción de accesos a archivos confidenciales.
  + Autenticación de usuarios.

**🛡️ Integridad**

* **Significa:** Asegurar que la información esté **completa, exacta y sin alteraciones** no autorizadas.
* **Objetivo:** Garantizar que los datos no sean **modificados de forma indebida**.
* **Ejemplos:**
  + Controles de versión.
  + Sumas de verificación (checksum).
  + Auditorías de cambios.

**⚙️ Disponibilidad**

* **Significa:** Asegurar que la información esté **accesible cuando se necesite** por los usuarios autorizados.
* **Objetivo:** Evitar interrupciones que impidan el acceso a sistemas o datos.
* **Ejemplos:**
  + Servidores con alta disponibilidad.
  + Copias de seguridad (backups).
  + Protección contra ataques de denegación de servicio (DDoS).

**En un hospital:**

**1. Disponibilidad – La más crítica en situaciones de emergencia**

* **¿Por qué?** Porque los médicos necesitan **acceso inmediato** a historiales clínicos, resultados de exámenes, medicamentos, etc. para **salvar vidas**.
* **Ejemplo:** Si el sistema cae en plena cirugía o emergencia, podría ser fatal.

**2. Integridad**

* **¿Por qué?** Es vital que la información **no esté alterada o equivocada**. Una dosis mal registrada o una alergia modificada por error puede poner en peligro al paciente.
* **Ejemplo:** Un cambio no detectado en el grupo sanguíneo de un paciente puede tener consecuencias graves.

**3. Confidencialidad**

* **¿Por qué?** Aunque es muy importante (protección de la privacidad del paciente), en el contexto hospitalario **salvar vidas y tratar correctamente al paciente es la prioridad**, por lo que podría tener un nivel de urgencia menor frente a los dos anteriores.
* **Ejemplo:** Se necesita asegurar que solo el personal autorizado vea el historial, pero si se trata de una emergencia, el acceso debe ser rápido.

**🧾 Resumen en orden de prioridad en un hospital:**

| **Prioridad** | **Pilar** | **Motivo principal** |
| --- | --- | --- |
| 1️⃣ | **Disponibilidad** | El acceso inmediato puede salvar vidas |
| 2️⃣ | **Integridad** | Los datos incorrectos pueden ser mortales |
| 3️⃣ | **Confidencialidad** | Importante, pero se puede comprometer en emergencia |

**En una empresa de electrónica:**

**1. Confidencialidad – La más importante**

* **¿Por qué?** Esta empresa maneja **propiedad intelectual**: diseños de circuitos, prototipos, patentes, estrategias comerciales, etc. Si esa información se filtra o se roba, **la competencia podría copiar sus productos**.
* **Ejemplo:** Si los planos de un nuevo microchip caen en manos de un competidor, pueden lanzar una copia antes que la empresa original.

**2. Integridad**

* **¿Por qué?** Es fundamental que los planos, especificaciones técnicas, datos de producción o configuraciones **no sean alterados**. Un error puede causar **fallos en el producto** o **pérdidas millonarias**.
* **Ejemplo:** Si el archivo con los parámetros de una máquina se modifica por accidente o sabotaje, se pueden fabricar lotes defectuosos.

**3. Disponibilidad**

* **¿Por qué?** Aunque importante, **la empresa puede tolerar una interrupción temporal** si los datos están seguros. Lo prioritario es que los datos estén **correctos y protegidos**.
* **Ejemplo:** Un apagón o mantenimiento puede ser asumido si no se compromete la integridad ni se filtra información.

**🧾 Resumen en orden de prioridad en una empresa de electrónica:**

| **Prioridad** | **Pilar** | **Motivo principal** |
| --- | --- | --- |
| 1️⃣ | **Confidencialidad** | Protege patentes, diseños y secretos comerciales |
| 2️⃣ | **Integridad** | Evita errores técnicos costosos y fallos |
| 3️⃣ | **Disponibilidad** | Aceptable en ciertos casos si los datos están seguros |

DEFINISION Y EJEMPLOS

GUSANO: Es un softare malicioso que actúa automáticamente, se eplica e infecta todo el sistema y daña los datos

* EJEMPLO: Se difunde a través de redes de computadoras, aprovechando vulnerabilidades de software o conexiones de red

TROYANO: Es un software disfrasado que al momento de abrilo por el usuario se destapa como un virus que ataca al sistema y a la maquina

* EJEMPLO: Descargas un "juego gratis" desde una página sospechosa. Al ejecutarlo, se instala un troyano que permite al atacante entrar a tu computadora y copiar tus archivos personales.

RANSOMWARE: Es un malware que bloquea el acceso a tu sistema o cifra tus archivos y luego exige un rescate (ransom) en dinero (normalmente en criptomonedas) para restaurar el acceso.

* Ejemplo: Recibes un archivo por correo que parece una factura. Al abrirlo, el ransomware cifra todos tus documentos y aparece un mensaje diciendo: "Paga 500 USD en Bitcoin en 72 horas o perderás tus archivos para siempre."

SPYWARE: Es un software malicioso que espía al usuario sin su consentimiento, recolectando información como contraseñas, historial de navegación, correos o incluso grabaciones de audio/video.

* Ejemplo: Instalas una extensión de navegador dudosa y, sin saberlo, está capturando todas tus contraseñas y enviándolas al atacante.



