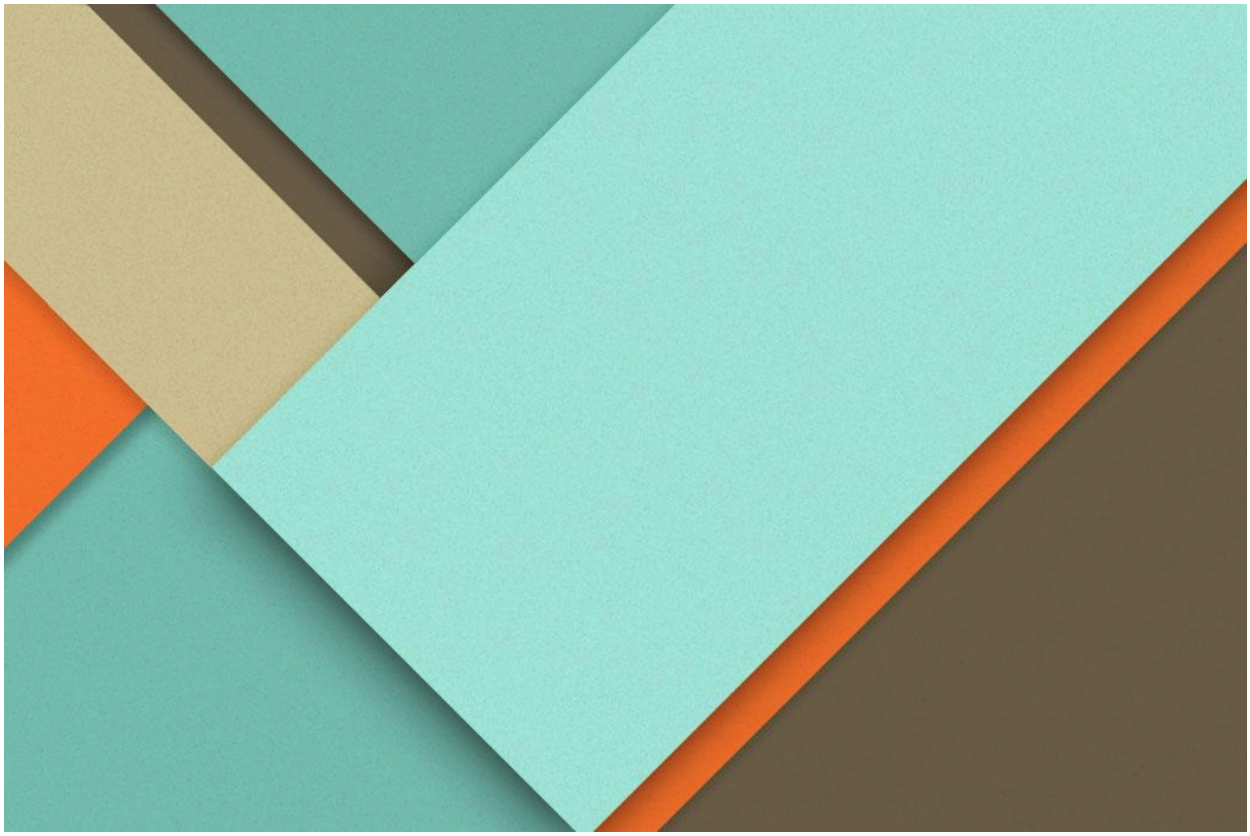

PEC1

26/01/2026

Manuel Pérez Romero

Ejercicio A: Pilares básicos de la seguridad informática

Los pilares de la seguridad de la información (la tríada CIA) son fundamentales para garantizar la protección de los datos. A continuación, presento un ejemplo detallado de cada uno:

1. Confidencialidad:

- **Ejemplo:** El uso de cifrado extremo a extremo en una aplicación de mensajería corporativa.
- **Explicación:** Este pilar asegura que la información solo sea accesible por personas autorizadas. Si un atacante intercepta los mensajes, solo verá datos cifrados ilegibles. La clave de descifrado solo reside en los dispositivos del emisor y receptor, cumpliendo así con el principio de privacidad.

2. Integridad:

- **Ejemplo:** El uso de funciones *hash* (como SHA-256) al descargar un software oficial o una actualización de sistema.
- **Explicación:** La integridad garantiza que la información no haya sido alterada de forma no autorizada. Si el *hash* del archivo descargado coincide con el proporcionado por el fabricante, tenemos la certeza de que el archivo es exacto al original y no ha sido modificado maliciosamente por un tercero.

3. Disponibilidad:

- **Ejemplo:** La implementación de un sistema de balanceo de carga y servidores en alta disponibilidad (clúster) para un servicio de banca online.
- **Explicación:** La disponibilidad asegura que los usuarios autorizados tengan acceso a la información y a los recursos cuando lo necesiten. Si un servidor falla, el sistema de respaldo entra en funcionamiento inmediatamente, evitando que el servicio caiga y que los clientes se queden sin acceso a sus cuentas.

Ejercicio B: Metodologías de gestión de riesgos no basadas en activos

Investigando metodologías que se alejan del enfoque tradicional centrado en el inventario de activos físico/lógicos, destaca **OCTAVE Allegro** (desarrollada por el SEI de la Universidad Carnegie Mellon).

- ### Características principales:
    1. Se centra en el **flujo de información** y cómo ésta es utilizada, almacenada y transportada.
    2. Prioriza los riesgos basándose en el impacto hacia la misión de la organización, no solo en la tecnología.
    3. Es más ágil y menos burocrática que las versiones anteriores de OCTAVE.

- ### Descripción del proceso:
    1. **Establecer criterios de medición:** Se definen qué impactos son aceptables para la organización.
    2. **Perfilado de contenedores:** Se identifican los "contenedores" (personas, sistemas, papel) donde reside la información crítica.
    3. **Identificación de amenazas:** Se analizan las amenazas en relación con esos contenedores.
    4. **Identificación y mitigación de riesgos:** Se evalúan las consecuencias de las amenazas y se seleccionan las medidas de control.

Ejercicio C: Debate sobre activos y normativa

¿Qué es realmente un activo? ¿Puede serlo un aire acondicionado?

- Un activo es cualquier cosa que tenga valor para la organización y que, por tanto, requiera protección. Sí, una consola de aire acondicionado **puede ser un activo**. Aunque no procesa datos directamente, es un "activo de soporte" crítico. Si el aire acondicionado falla en un CPD (Centro de Procesamiento de Datos), los servidores se sobrecalentarán y se apagará el servicio, afectando directamente a la **disponibilidad**.

¿Es obligatorio el uso de activos en la ISO 27001? ¿Podemos evaluar riesgos sin ellos?

- En la versión actual de la norma (ISO/IEC 27001:2022), el enfoque es más flexible. Aunque históricamente se ha basado en activos, la norma ahora pone el énfasis en la **identificación de riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad**. Por tanto, es posible (y a veces recomendable) realizar evaluaciones basadas en **procesos de negocio** o en escenarios de amenaza, siempre que el resultado permita aplicar los controles de seguridad necesarios de manera efectiva.