Seguridad de la Información

Es el conjunto de medidas y estrategias implementadas para proteger la información de organizaciones, empresas o individuos contra accesos no autorizados, pérdidas, modificaciones o robos.

Ciclo de Vida de la Información

- **Creación:** Generación de información.
- **Almacenamiento:** Guardar datos en sistemas o soportes.
- **Uso:** Acceso y utilización de la información.
- **Compartir:** Distribuir datos con usuarios autorizados.
- **Archivado:** Conservación a largo plazo.
- **Eliminación:** Descarte de información al final de su vida útil.

Confidencialidad, Integridad y Disponibilidad (CIA)

- **Confidencialidad:** Garantizar que la información solo sea accesible por usuarios autorizados.
- **Integridad:** Asegurar que los datos no sean modificados, alterados o corrompidos de manera no autorizada.
- **Disponibilidad:** Asegurar que la información esté disponible y accesible para los usuarios autorizados cuando sea necesario.

Sistema de Gestión de Seguridad de la Información (ISMS)

Es un enfoque integral y estructurado para manejar la

seguridad de la información. Se basa en un ciclo continuo de planificación, implementación, monitoreo y mejora.

Riesgos y Amenazas para la Información

- **Riesgos:** Posibilidad de pérdida o daño a la información y sus activos asociados.
- **Amenazas:** Posibles eventos o situaciones que pueden dañar, destruir, divulgar o manipular la información de manera no autorizada.

Las amenazas pueden ser internas (errores humanos, accidentes) o externas (ciberataques, malware). Identificar, evaluar y mitigar estos riesgos es fundamental para mantener la seguridad de la información.

Gestión de Riesgos de Seguridad de la Información

Consiste en identificar, evaluar y controlar los riesgos potenciales para la información. Esto incluye:

- Análisis de riesgos.
- Implementación de controles de seguridad.
- Monitoreo y revisión continua para mantener la protección de la información.