Seguridad de la información:

- Proceso que elimina riesgos. La información es el recurso más valioso.
- Estrategias que cubren los procesos de negocios de una organización.

Seguridad informática:

- Seguridad técnica de los sistemas informáticos.
- Concepto más restrictivo.

Perspectivas:

1) Legal → regulación nacional e internacional. (protección de privacidad, derechos de propiedad intelectual, protección de datos).
2) Técnica → desarrollo, análisis, configuración y despliegue (hardware y software).
3) Organizativa → análisis de riesgo, seguridad fundamental para el negocio (políticas, procedimientos, guías, procesos y controles)

   ¿Qué hay que proteger? Para ello, la perspectiva legal y organizativa.

   ¿Por qué y de qué proteger? Perspectiva legal y organizativa.

   - Evitar la violación de la privacidad de las personas.
   - Evitar las posibles vulnerabilidades que el negocio tenga.

   ¿Cómo proteger? Perspectiva técnica.

   - Realizar controles, auditorías y revisiones.
   - Salvaguardas en base a las amenazas.

1. Integridad, confidencialidad y disponibilidad

Principios de seguridad:

Confidencialidad:

- Protege la filtración de información a terceros intencionado o no.
- Respeto de la privacidad.

Integridad:

- Protege la información de modificaciones no autorizadas.

Disponibilidad:

- Permite que la información sea accesible por las personas que tengan que acceder a ellas.

2. Identificación, Autentificación, Accountability y Autorización.

Principios de la Seguridad:

Identificación

- Proceso que permite la identificación de los usuarios. (Tarjetas de autentificación, usuarios y claves).

Autentificación

- Comprobación por parte del responsable del usuario. (comprueba si es o no el usuario).

Contabilidad

- Capacidad de los sistemas de hacer seguimiento de las acciones y procesos de los sistemas y usuarios.

Autorización

- Derechos y permisos de los individuos para acceder a los recursos del sistema. (lectura y escritura, roles).

3. introducción a los sistemas de gestión de la seguridad de la información

Clasificación de la información.

Sin clasificar:

- Información no clasificada.
- La difusión de esta información no afecta a la confidencialidad.

Sensible pero no clasificada:

- Información con un impacto menor si se difunde.

Confidencial.

- Si se filtra la información puede ser perjudicial.

Secreta

- Difusión → muy grave.

Uso público →difusión pública.

Uso interno → solo se puede difundir internamente

La seguridad implica a las personas.

Ingeniería social →arte de engañar y manipular a las personas para que revelen información confidencial (phishing).

La política general de seguridad establece los objetivos de las políticas funcionales que se implantan mediante;

- Estándares →obligatorios, especifican el uso de tecnologías y métodos.
- Directrices → no son obligatorias, son recomendaciones.
- Procedimientos → descripción de pasos o procesos para realizar una tarea.
- Líneas base. → descripción de configuración de elementos de seguridad.

Sistema de Gestión de la seguridad de la información. SGSI.

¿Qué es? ¿Por qué está formado? à Es un marco de trabajo, donde se pretende la confidencialidad, integridad y disponibilidad de la información mediante la implantación, seguimiento, auditoría y mejora de controles, formado por:

- Normativa.
- Procedimientos y guías.
- Documentación, personas y controles.
- Recursos y actividades asociadas.

(se basa también en el análisis de riesgos con el objetivo de tratar y gestionar de manera eficiente los mismos).

Modelo PDCA