Tema 2: Sistema de gestión de seguridad de la administración

Familia ISO/IEC 27000

Un sistema de gestión es una forma de hacer la gestión basándonos en una serie de documentación. Es un conjunto de elementos interrelacionados de una organización para establecer unos objetivos, así como los recursos y políticas para alcnazarlos. Los objetivos generalmente son los siguientes:

La familia 27000 es una serie de normas, donde la 27001 es la certificable.

- **ISO 27001**: Especifica los requisitos a cumplir para implantar un SGSI certificable conforme a la norma 27001.
- **ISO 27002**: Conjunto de controles que hay que valorar si es necesaria su aplicación o no
    - Consta de 93 controles en la versión actual.
        - Control de acceso de personal a espacios sensibles
        - Realización de copias de seguridad
        - Contratos de confidencialidad
        - Documento de salida que debe firmar del empleado
- **ISO 27003**: Guía de implementación de un SGSI.
- **ISO 27004**: Métricas y técnicas de medida
    - Cuantas incidencias hay
    - Medidas a tomar.
- **ISO 27005**: Consiste en como realizar un análisis de riesgos
- **ISO 27006**: Acreditaciós a cumplir por las organizaciones encargadas de realizar las auditorías
- **ISO 27007**: Como realizar una auditoría para realizar una certificación
- **ISO 27033**: Seguridad de redes
- **ISO 27035**: Seguridad de la información
- **ISO 27036**: Guía de cuatro partes de seguridad en la relación con proveedores (En desarrollo)

ISO/IEC 27001

Especifica los requisitos para especificar, manter y mejorar un SGSI.

Perspectivas

- Riesgo: Requisitos de protección y exposición al riesgo de los activos de la empresa y los istemas informáticos
    - Entorno = Riesgos: Reconocer los diferentes riesgos y metodologías para su gestión
- Cumplimiento:
    - Regulaciones externas establecidas por leyes, regulaciones y estándares.
    - Obligaciones contractuales
- Gobernanza: Alinear los objetivos de TI y seguridad de la información derivados de los objetivos generales de la empresa.

Fundamentos

- La seguridad total no existe
- La seguridad que se debe implementar depende de la organización y su entorno.
- La seguridad deja de ser solo una cuestión técnica para ser parte del plan de negocio.
- Se aplica a todos los niveles de la organización.
- Se introduce el análisis de Riesgo y un sistema de gestión orientado a la protección de la información
- Se define un conjunto de controles que no dejan nada al azar (ISO 27002)
- Asocia la gobernabilidad con la seguridad de la información.

Evolución

Comenzó a finales de los 90 con normas nacionales, tomándose como referencia la norma británica BS 7799-2 y fue evolucionando con los años:

- ISO/IEC 27001:2005
- ISO/IEC 27001:2013
- ISO/IEC 27001:2022 (Versión actual)

Estructura

1. Ámbitos de la norma
2. Alcance
3. Términos y definiciones de la norma 27001
4. contexto organizacional y de las partes interesadas
5. Liderazgo en seguridad de la información y apoyo de alto nivel para la política
6. Planificación de un sistema de gestión de seguridad de la información: Evaluación de riesgos y tratamiento de riesgos
7. Apoyar un sistema de gestión de seguridad de la información
8. Hacerun sistema de gestión de la seguridad de la información
9. Revisar el funcionamiento del sistema
10. Acciones correctivas
11. Anexo A: Lista de los controles y sus objetivos.

ISO 27001 y el Ciclo Deming (PDCA)

- Planificar (Establecer el SGSI)
- DO (Hacer)
- Check
- Act

ISO/IEC 27002

Esquema Nacional de Seguridad

From:
https://knoppia.net/ - **Knoppia**

Permanent link:
https://knoppia.net/doku.php?id=master_cs:gsi:tm2&rev=1758560019

Last update: **2025/09/22 16:53**