# 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

## 1. Alcance

Este documento establece los requisitos para elaborar un sistema de gestión de la información, incluyendo requisitos para la evaluación y tratamiento de riesgos. Cualquier requisito excludio debe ser justificado y aceptado por los auditores. Esta parte tiene en cuenta los controles genéricos, estos

controles deben ser conocidos.

## 2. Referencias normativas

Se referencian las normativas usadas como la 27001.

## 3. Términos y definiciones

Terminos y definiciones relevantes en el contexto

## 4. Contexto de la organiación

Cubre varios puntos:

- 4.1 Organización: estuctura organizativa
- 4.2 Partes interesadas: Personas o organizaciones que pueden influir en la seguridad de la información
    - Clientes
    - Empleados
    - Proveedores
    - Accionistas
- 4.3 Determinación de alcance del SGSI
    - Las cuestiones internas y externas del 4.1
    - Los requisitos del 4.2
    - Las interfaces y dependencias entre actividades realizadas por la organización y las realizadas por otras organizaciones.
- 4.4 SGSI
    - La organización debería establecer, implementar, mantener y mejorar de forma contínua el SGSI.

## 5. Liderazgo

- 5.1. Liderazgo y compromiso:
    - La alta dirección debe demostrar liderazgo y compromiso con respecto al SGSI
- 5.2 Política
    - La alta dirección define una política de seguridad de la información que:
        - Sea apropiada para el propósito de la organización
        - Incluya información de los objetivos de seguridad da la información
        - Compromiso de mejora contínua
        - Compromiso para satisfacer los requisitos
    - La política de seguridad de la información debe:
        - Estar disponible como información documentada
        - Ser comunicada dentro de la organización
        - Estar disponible para las partes interesadas
- 5.3 Funciones, responsabilidades y autoridades de la organización
    - Es responsabilidad de la alta dirección garantizar que las funciones, responsabilidades y

autoridades se deleguen y comuniquen de manera efectiva.
    - La alta dirección debe asignar la responsabilidad para:
        - Asegurar que la SGSI es conforme con los requisitos de la ISO 27001
        - Informar sobre los resultados del SGSI a la alta dirección

## 6. Plan

### 6.1 Acciones para abordar riesgos y oportunidades

- 6.1.1 General:
    - La organización debe planear:
        - Las acciones para abordar los riesgos y oportunidades
        - Como integrar e implementar las acciones en procesos del SGSI
        - Evaluar la eficacia de dichas acciones
- 6.1.2 Evaluación de reisgos de seguridad de la información
    - Establezca y mantenga criterios de riesgo incluyendo:
        - El criterio de aceptación de riesgo
        - Criterios para realizar evaluaciones de riesgos de seguridad de la información
    - Asegura la reproducibilidad de las evaluaciones con resultados consistentes, válidos y comparables
    - Identifique los riesgos de seguridad de la información y alos propietarios de los riesgos
    - Analice los riesgos de seguridad de la información, considerando las consecuencias potenciales y la probabilidad de ocurrencia para determinar el nivel de riesgo.
        - Un análisis de riesgos puede ser desarrollado con cualquier tipo de metodología siempre y cuando sea completa y metódica, siendo el resultado final:
            - Clara identificación, definición y descripción de los activos
    - Evalue los riesgos de seguridad de la información, comparando los resultados del análisis de riesgo con el criterio de aceptación y priorizando los riesgos analizados para el tratamiento del riesgo.
- 6.1.3 Tratamiento de riesgos de seguridad de la información
    - Selecciona las opciones de tratamiento de riesgo
    - Determinar todos los controles necesarios para implementar las opciones de tratamiento
    - Comparar los controles determinados con los disponibles en el “Anexo A” y verificar que no se han omitido riesgos necesarios.
    - Reproducir la declaración de aplicailidad (SOA)
        - Controles necesarios
        - Justifiación de su inclusión
        - Si los controles necesarios están o no implementados
        - La justificación de su exclusión.
    - Formular el plan de tratamiento de riesgos (RTP)
    - Obtener la aprobación del propietario de riesgo para el RTP y aceptación de riesgos residuales

# ISO/IEC 27002

# Esquema Nacional de Seguridad