Estructura de la Norma ISO 27002:2022

La nueva versión de la norma ISO 27002 tiene la siguiente estructura:

Introducción: contextualiza el valor de la información para las organizaciones, cómo es alcanzada la seguridad de la información a través de la implementación de un conjunto de controles de seguridad, los requerimientos de seguridad de la información que debe determinar una organización, la determinación de controles para proteger la información, consideraciones del ciclo de vida de la información (desde su creación hasta su eliminación) y la relación de esta norma con otras normas (especialmente de la familia ISO/IEC 2700).

- **Cláusula 1 – Alcance**: indica que este documento está diseñado para que las organizaciones lo utilicen como referencia para la selección de controles en el proceso de implantación de un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001.
- **Cláusula 2 – Referencias normativas:** no hay referencias normativas en esta norma.
- **Cláusula 3 – Términos, definiciones y términos abreviados**: relaciona un conjunto de términos, definiciones y abreviaturas que aplican en el contexto de esta norma.
- **Cláusula 4 – Estructura del documento**: determina las cláusulas, temas y atributos, y diseño de estructura de cada control incluido en la norma.
- **Cláusulas 5 a 8:** establece nombre de control, tabla de atributos, propósito, guía de implementación y otra información (si aplica) para controles de seguridad:
- Organizacionales (Cláusula 5).

- Personas (Cláusula 6).
- Físicos (Cláusula 7).
- Tecnológicos (Cláusula 8).
- **Anexo A:** Este anexo proporciona una tabla para demostrar el uso de los atributos como forma de crear diferentes vistas de los controles.
- **Anexo B**: Correspondencia entre ISO/IEC 27002:2022 con ISO/IEC 27002:2013
- **Bibliografía**: Relación de otras normas y documentos usados en esta norma.

Principales novedades de la norma ISO 27002:2022

Los principales cambios de la norma ISO27001:2022 frente a la versión anterior son:

1. **Cambio en el nombre de la norma**: Se ha eliminado el término "*Código de prácticas*" del nombre de la nueva norma ISO 27002. Su nombre actual es "***Seguridad de la información, ciberseguridad y protección de la privacidad – Controles de seguridad de la información***", lo cual refleja un contexto más amplio y que incluye ahora la prevención, detección y respuesta a ciberataques, así como la protección de los datos.

2. **Cambios en controles de seguridad**: La norma ISO 27002:2013 contenía 114 controles (divididos en 14 Anexos). La versión 2022 contiene 93 controles, divididos en 4 cláusulas que se enfocan hacia el contexto de aplicación del control así:
   - Controles Organizativos: 37 controles
   - Controles de Personas: 8 controles
   - Controles Físicos: 14 controles
   - Controles Tecnológicos: 34 controles

   De los 93 controles actuales:
   - 58 se han actualizado
   - 24 representan la fusión de controles anteriores
   - 11 se han introducido como nuevos controles

   Este nuevo enfoque conlleva también la desaparición del concepto "objetivo de control", aunque se incluye un atributo que permite la clasificación específica del control en uno o más de 15 categorías establecidas, como se indica en el siguiente apartado.

3. **Estructura de atributos de controles:** cada uno de los 93 controles contiene una estructura de atributos particular que determina:
    - **Tipo de control**: atributo para ver los controles desde la perspectiva de cuándo y cómo el control modifica el riesgo con respecto a la ocurrencia de un incidente de seguridad de la información identificando si es Preventivo, Detectivo o Correctivo.
    - **Propiedades de seguridad de la información**: atributo para ver los controles desde la perspectiva de qué características de la información el control contribuirá a preservar: Confidencialidad, Integridad o Disponibilidad.
    - **Conceptos de Ciberseguridad**: atributo para ver los controles desde la perspectiva de la asociación de los controles a los conceptos de ciberseguridad definidos en el marco de ciberseguridad descrito en ISO/IEC TS 27110 y usado en otros marcos de trabajo como NIST-Cibersecurity Framework: Identificar, Proteger, Detectar, Responder, Recuperar.
    - **Capacidades Operativas**: atributo para ver los controles desde la perspectiva del profesional de las capacidades de seguridad de la información. Los valores de este atributo son:
        - Gobernanza,
        - Gestión de activos,
        - Protección de la información,
        - Seguridad de los recursos humanos,
        - Seguridad física,

- Seguridad de sistemas y redes,
- Seguridad de las aplicaciones,
- Configuración segura,
- Gestión de la identidad y del acceso,
- Gestión de amenazas y vulnerabilidades,
- Continuidad,
- Seguridad de las relaciones con los proveedores,
- Cumplimiento legal,
- Gestión de eventos de seguridad de la información
- Aseguramiento de la información

- **Dominios de Seguridad**: atributo que permite ver los controles desde la perspectiva de cuatro dominios de seguridad de la información: Gobernanza y ecosistema, Protección, Defensa, Resiliencia

---

Se pide:

1. Describir un control de la ISO 27002-2022.
2. Los términos para definir se encuentran en el documento **controles**. El docente asignará a cada alumno un control.
3. Cada alumno buscará información del control asignado en la norma ISO 27002-2022 y elaborará una descripción de este, indicando la variación respecto a la versión anterior de la norma
4. El alumno debe elaborar un documento explicando el control asignado
5. Cada alumno explicará los términos asignados en clase.