# Módulo 4:

# Estándares de gestión de la seguridad de la información

Se da un repaso en este módulo a los principales estándares aceptados por la industria en el área de la seguridad de la información, las Normas ISO 27001 e ISO 27002, explicando los objetivos y los requisitos contenidos en estas dos normas.

El contenido de este módulo es:

- La organización ISO.
- Estándares en Seguridad de la Información: Las Normas ISO 27000.
- La Norma ISO 27001.
- La Norma ISO 27002.

## I. LA ORGANIZACIÓN ISO:

ISO (Organización Internacional de Estándares) es una organización especializada en el desarrollo y difusión de los estándares a nivel mundial.

Los miembros de ISO, son organismos nacionales que participan en el desarrollo de Normas Internacionales a través de comités técnicos establecidos para tratar con los campos particulares de actividad técnica. Los comités técnicos de ISO colaboran en los campos de interés mutuo con la IEC (International Electrotechnical Commission), la organización que a nivel mundial prepara y publica estándares en el campo de la electrotecnología. En el campo de tecnología de información, ISO e IEC han establecido unir un comité técnico, ISO/IEC JTC 1 (Join Technical Committee Nº1).

Los borradores de estas Normas Internacionales son enviados a los organismos de las diferentes naciones para su votación. La publicación, ya como una Norma Internacional, requiere la aprobación de por lo menos el 75% de los organismos nacionales que emiten su voto.

## II. LA FAMILIA DE LAS NORMAS ISO:

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares. Muchos de ellos no están aún publicados, pero la estructura ya está definida:

| LA FAMILIA DE LAS NORMAS ISO |
| --- |
| ▪ ISO/IEC27000 Sistemas de Gestión de Seguridad de la Información, Generalidades y vocabulario, publicada en Abril del 2009, en la que se recogen los términos y conceptos relacionados con la seguridad de la información, una visión general de la familia de estándares de esta área, una introducción a los SGSI, y una descripción del ciclo de mejora continua. |
| ▪ UNE-ISO/IEC 27001, Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. (ISO/IEC 27001:2005), publicada en el año 2007. Esta es la norma fundamental de la familia, ya que contiene los requerimientos del sistema de gestión de seguridad de la información y es la norma con arreglo a la cual serán certificados los SGSI de las organizaciones que lo deseen. |
| ▪ ISO/IEC27002, Tecnología de la Información. Código de buenas prácticas para la Gestión de la Seguridad de la Información, publicada en el año 2005. Esta guía de buenas prácticas describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. |
| ▪ ISO/IEC27003. Guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. |
| ▪ ISO27004: Estándar para la medición de la efectividad de la implantación de un SGSI y de los controles relacionados. |
| ▪ ISO/IEC27005:2008 Gestión del Riesgo en la Seguridad de la Información, publicada en el año 2008. Esta norma al pertenecer a la familia de las Normas 27000, se ajusta a las necesidades de las organizaciones que pretende realizar su análisis de riesgos en este ámbito y cumplir con los requisitos de la Norma ISO 27001. |
| ▪ ISO/IEC27006. Requisitos para las entidades que suministran servicios de auditoría y certificación de sistemas de gestión de seguridad de la información. Publicada en el año 2007. Recoge los criterios mediante los cuales una organización se puede acreditar para realizar esos servicios. |
| ▪ ISO/IEC27007. Guía para la realización de las auditorías de un SGSI. |

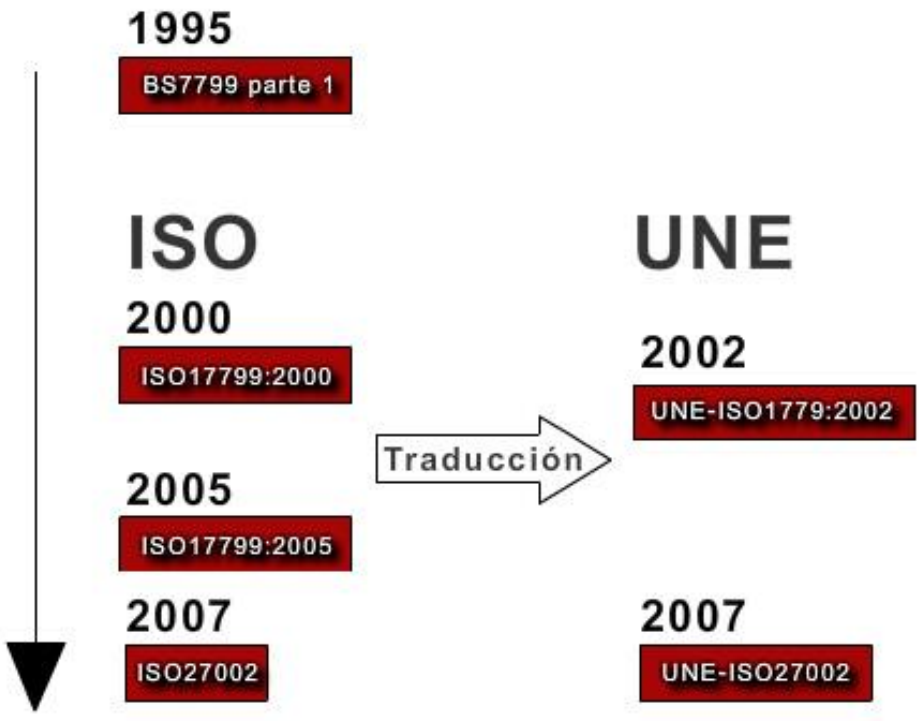
- ISO/IEC27011. Directrices para la seguridad de la información en organizaciones de telecomunicaciones utilizando la Norma ISO/IEC 27002. Contiene recomendaciones para empresas de este sector, facilitando el cumplimiento de la Norma ISO27001 y conseguir un nivel de seguridad aceptable.

- EN ISO27799. Gestión de la seguridad de la información sanitaria utilizando la Norma ISO/IEC27002 (ISO27799:2008). Vigente en nuestro país ya que ha sido ratificada por AENOR en agosto de 2008. Como en la anterior, es una guía sectorial que da cabida a los requisitos específicos de entorno sanitario.

## III. ORIGENES:

La Norma fue publicada como Norma Española en el año 2007, pero tiene una larga historia antes de llegar a este punto.

Ya en el año 1995 el British Standard Institute (BSI) publica la norma BS7799, un código de buenas prácticas para la gestión de la seguridad de la información.



A la vista de la gran aceptación de esta Norma, en 1998, el BSI publica la norma BS7799-2, Especificaciones para los sistemas de gestión de la seguridad de la información; se revisa en 2001. Tras una revisión de ambas Normas, la primera es adoptada como norma ISO en 2000 y denominada ISO/IEC 17799.

En 2002 la norma ISO se adopta como UNE sin apenas modificación (UNE 17799), y en 2004 se establece la norma UNE 71502, basada en BS7799-2, sin que haya un equivalente ISO.

A partir de julio de 2007 la ISO 17799:2005 adopta el nombre de ISO 27002 y en octubre de 2007 la norma ISO 27001 se adopta como UNE. Con la publicación de la UNE-ISO/IEC 27001, dejó de estar vigente la UNE 71502 y las empresas nacionales se certifican ahora únicamente con esta nueva norma (UNE-ISO/IEC 27001).

**Contenido de la UNE-ISO/IEC 27001**

La norma UNE-ISO/IEC 27001 especifica los requisitos para establecer, implantar, documentar y evaluar un Sistema de Gestión de la Seguridad de la Información (en adelante SGSI ) de acuerdo a la Norma ISO 27002 dentro del contexto de los riesgos identificados por la Organización.

Como otras Normas de gestión (ISO 9000, ISO 14001, etc.), los requisitos de esta Norma aplican a todo tipo de organizaciones, independientemente de su tipo, tamaño o área de actividad.

Asimismo está basada en un enfoque por procesos y en la mejora continua, por lo tanto es perfectamente compatible e integrable con el resto de sistemas de gestión que ya existan en la organización. La Norma asume que la organización identifica y administra cualquier tipo de actividad para funcionar eficientemente. Cualquier actividad que emplea recursos y es administrada para transformar entradas en salidas, puede ser considerada como un "proceso". A menudo, estas salidas son aprovechadas nuevamente como entradas, generando una realimentación de los mismos. Estos procesos se someten a revisiones para detectar fallos e identificar mejoras, por lo que se encuentran dentro de un proceso de mejora continua.

La Norma recoge:

- Los componentes del SGSI , es decir, en qué consiste la parte documental del sistema: qué documentos mínimos deben formar parte del SGSI , cómo se deben crear, gestionar y mantener y cuales son los registros que permitirán evidenciar el buen funcionamiento del sistema.

- Cómo se debe diseñar e implantar el SGSI.
- Define los controles de seguridad a considerar. Se requiere que se escojan los controles del Anexo A, que recoge todos los controles detallados en la Norma ISO/IEC 27002.
- Cómo debe realizarse la revisión y mejora del SGSI.

La ISO 27001 adopta un proceso para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI en una organización.

## IV. LA NORMA ISO 27002:

Esta norma contiene 11 capítulos de controles de seguridad que contienen un total de 133 controles de seguridad. Puede servir de guía práctica para la gestión de la seguridad de la información. No es una norma certificable.

Los objetivos de control contemplados en la Norma son:

1. Política de seguridad. Cuenta con dos controles: Documento de Política de seguridad y Revisión del Sistema.

2. Organización de la seguridad de la información, tienen 11 controles: Compromiso de la Dirección, Identificación de riesgos relacionados con terceras partes.

3. Gestión de activos, con 5 controles: Utilización aceptable de los activos, etiquetado y tratamiento de la Información.

4. Seguridad ligada a los Recursos Humanos con 9 controles: Análisis y selección, Retirada de los derechos de acceso.

5. Seguridad física y del entorno tiene 13 controles: Controles físicos de entrada, emplazamiento y protección de los equipos.

6. Gestión de comunicaciones y operaciones, con 32 controles es el capítulo más extenso y más técnico: Gestión de la Capacidad, Protección frente a código malicioso, Copias de seguridad, Registro de fallos.

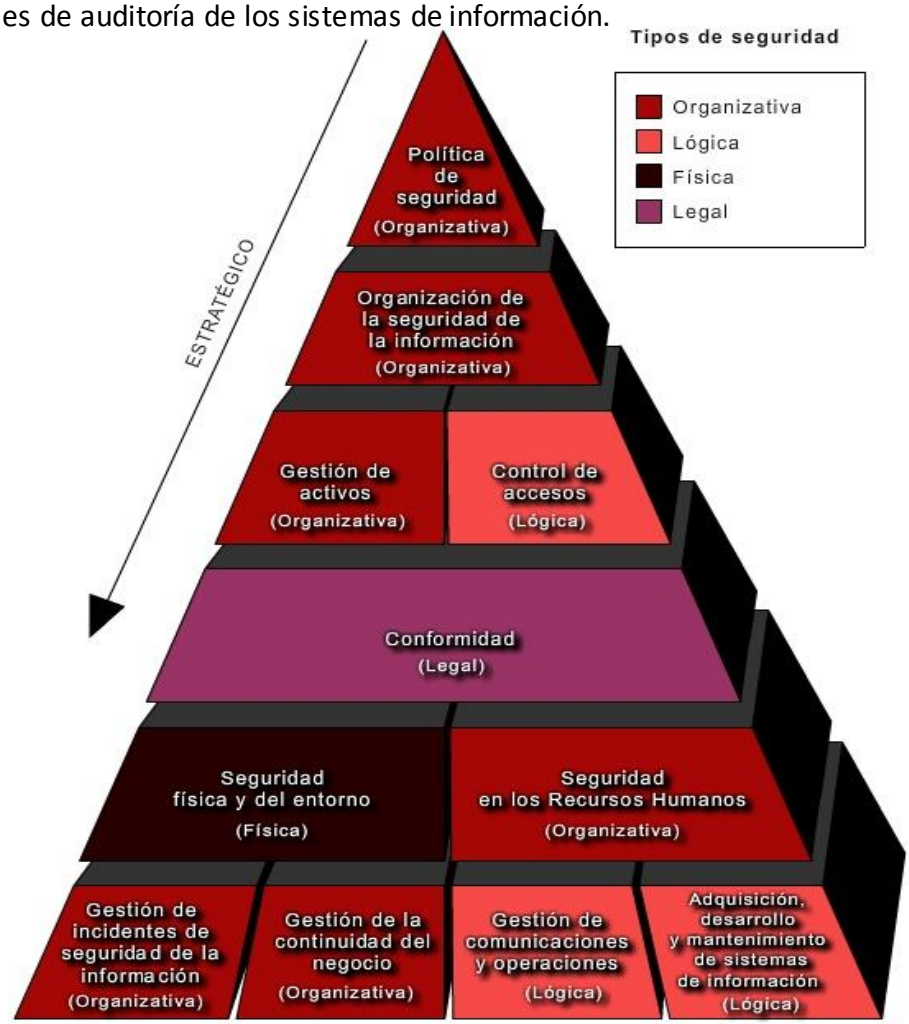
7. Control de acceso, cuenta con 25 controles: Gestión de contraseñas de usuarios Autenticación de usuarios para conexiones externas, Aislamiento de sistemas sensibles.

8. Adquisición, desarrollo y mantenimiento de SI, tiene 16 controles: Validación de datos de entrada, Control de acceso al código fuente de los programas, control de vulnerabilidades técnicas.

9. Gestión de incidentes de seguridad de la información, con sólo 5 controles: Informes de eventos de seguridad, Recogida de pruebas, es sin embargo uno de los aspectos claves en la gestión de la seguridad de la información.

10. Gestión de la continuidad del negocio, también con 5 controles: Evaluación de riesgos y continuidad del negocio Prueba, Mantenimiento y re-evaluación de los planes de continuidadEs uno de los requisitos fundamental para cualquier SGSI.

11. Conformidad, tienen 10 controles: Identificación de la legislación aplicable, Controles de auditoría de los sistemas de información.



La Norma contiene explicaciones exhaustivas de cómo se puede implantar cada uno de los controles, pero hay que tener en cuenta que no es una norma preceptiva sino informativa, por lo que la información que da puede y debe ser adaptada a las necesidades y situación específica de la organización. Debe evitarse caer en el error de tratar de seguir al pie de la letra las indicaciones que se dan, ya que pueden ser excesivamente complejas e innecesarias para muchas organizaciones.

## Evaluación Módulo 4

Marque la casilla con una X según la lectura del Módulo, la respuesta a cada pregunta es única:

1. Los estándares ISO son:

- [ ] Internacionales
- [ ] Nacionales
- [ ] De obligatorio cumplimiento

2. La Norma UNE/ISO-IEC 27001 contiene:

- [ ] Los requisitos para asegurar los sistemas de información
- [ ] Los requisitos de seguridad de cualquier organización
- [ ] Los requisitos para diseñar e implantar un SGSI

3. La Norma ISO/IEC 27002:

- [ ] Es certificable
- [ ] No certificable
- [ ] Depende del sector económico de la organización

4. Las medidas de seguridad del Anexo A de la Norma ISO/IEC 27001:

- [ ] Deben aplicarse todas
- [ ] Debe escogerse al menos una de cada epígrafe
- [ ] Deben escogerse las necesarias para la organización