¿Qué es ISO?

- ISO es una red de organismos nacionales de estandarización de más de 163 países
- Los resultados finales de los trabajos realizados por ISO son publicados como normas internacionales
- Se han publicado más de 21 000 normas desde 1947

Historia

En 1946, los delegados de 25 países se reunieron en Londres y decidieron crear una nueva organización internacional, cuyo objeto sería “facilitar la coordinación internacional y la unificación de estándares industriales”. La nueva organización inició oficialmente sus operaciones el 23 de febrero de 1947, en Ginebra, Suiza.

La Organización Internacional de Normalización (ISO) es una organización no gubernamental que tiene una posición especial entre el sector público y el sector privado. Entre sus miembros figuran organizaciones de estándares nacionales que a menudo forman parte de las estructuras de gobierno en sus países o que tienen el mandato de estos gobiernos.

Otros miembros pertenecen al sector privado, como las asociaciones nacionales de asociaciones de la industria.

Objetivos/Ventajas

El papel de la ISO es facilitar la coordinación internacional y la estandarización de las normas industriales. Para alcanzar estos objetivos, la ISO publica normas técnicas. Estas normas contribuyen al desarrollo, fabricación y entrega de productos y servicios que sean más eficaces, más seguros y más claros. Facilitan el comercio justo entre los países. Además, aportan una base técnica a los gobiernos para la legislación sobre salud, seguridad y medioambiente; y ayudan a transferir tecnologías a los países en desarrollo. Las Normas ISO se utilizan también para proteger a los consumidores y usuarios en general de productos y servicios. Estas normas se utilizan también para simplificar sus vidas.

Nota sobre la terminología: Dado que la Organización Internacional de Normalización tendría siglas diferentes en idiomas diferentes ("IOS" en inglés por "International Organization for Standardization", "OIN" en francés por "Organisation Internacionale de Normalisation"), sus fundadores decidieron darle también un nombre corto para todo uso. Eligieron "ISO", derivado del griego "isos", que significa "igual".

Fuente: www.iso.org

¿Cómo se desarrollan las normas ISO?

Las delegaciones nacionales de expertos de un comité se reúnen para tratar, debatir y discutir hasta llegar a un consenso sobre un borrador de acuerdo. Las “organizaciones de enlace” también participan en esta labor. En algunos casos, el trabajo avanzado dentro de estas organizaciones significa que ya se ha producido un sustancial desarrollo técnico y debate, lo que lleva a un cierto reconocimiento internacional y, en este caso, un documento puede ser presentado por “vía rápida” de procesamiento. En ambos casos, el documento resultante se distribuirá como un Proyecto de Norma Internacional (DIS) a todos los organismos miembros de ISO para votar y hacer comentarios.

Si el voto es a favor, el documento, con las eventuales modificaciones, se distribuye a los miembros de la ISO como Borrador Final de Estándar Internacional (FDIS). Si ese voto es positivo, el documento se publica como una Norma Internacional. (No hay un escenario FDIS en el caso de los documentos tramitados por el procedimiento de vía rápida del comité técnico conjunto ISO/IEC JTC 1, Tecnología de la información).

Todos los días laborables del año, un promedio de siete reuniones técnicas se llevan a cabo en todo el mundo. Entre reuniones, los expertos continúan el trabajo de desarrollo de las normas por correspondencia. Cada vez más, su trabajo se lleva a cabo por medios electrónicos, lo que acelera el desarrollo de normas y reduce los costos de viaje.

Principios Básicos – Normas ISO

Principios Básicos de las Normas ISO

1. **Representación igualitaria:** 1 voto por país
2. **Adhesión voluntaria:** ISO no tiene la autoridad para forzar la adopción de sus normas
3. **Orientación al negocio:** ISO sólo desarrolla las normas para las que existe una demanda del mercado.
4. **Enfoque de consenso:** Busca un amplio consenso entre las distintas partes interesadas
5. **Cooperación internacional:** Más de 163 países además de organismos de enlace

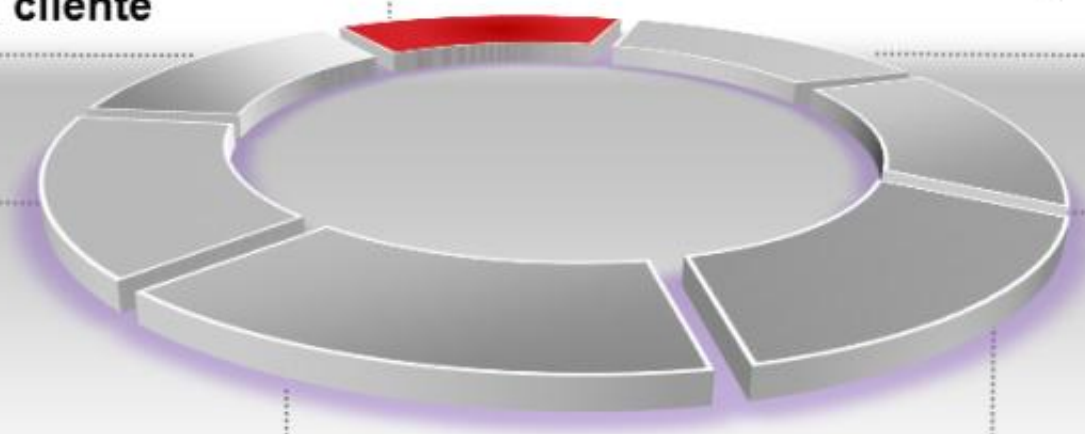
Principios básicos de la ISO

1. Representación igualitaria: Cada miembro de ISO (miembro de pleno derecho) tiene el derecho a participar en el desarrollo de cualquier norma que crea importante para la economía de su país. Cualquiera que sea el tamaño o la fuerza de la economía, cada miembro participante puede reclamar su derecho al voto. Las actividades de la ISO se realizan así en una estructura democrática donde los países miembros están en pie de igualdad en términos de su influencia en la orientación laboral.

2. Voluntario: La adopción de las normas ISO es voluntaria. Como organización no gubernamental, la ISO no tiene autoridad legal para su aplicación. Un porcentaje de las normas ISO — en particular las relacionadas con la salud, la seguridad y el medio ambiente – han sido adoptadas en varios países como parte del marco regulador, o cuando se indica en la legislación funcionando como base técnica. Esas adopciones son decisiones soberanas de las organizaciones reguladoras o los gobiernos.

La ISO no regula ni legisla. Sin embargo, a pesar de que las normas ISO son voluntarias, pueden convertirse en una exigencia del mercado, como es el caso con la norma ISO 9001 o con las dimensiones de los contenedores de mercancías, la trazabilidad de los alimentos, etc.

Los Siete Principios de Gestión de la ISO



Liderazgo

Participación y competencia de las personas

Enfoque en el cliente

Gestión de relaciones

Enfoque basado en procesos

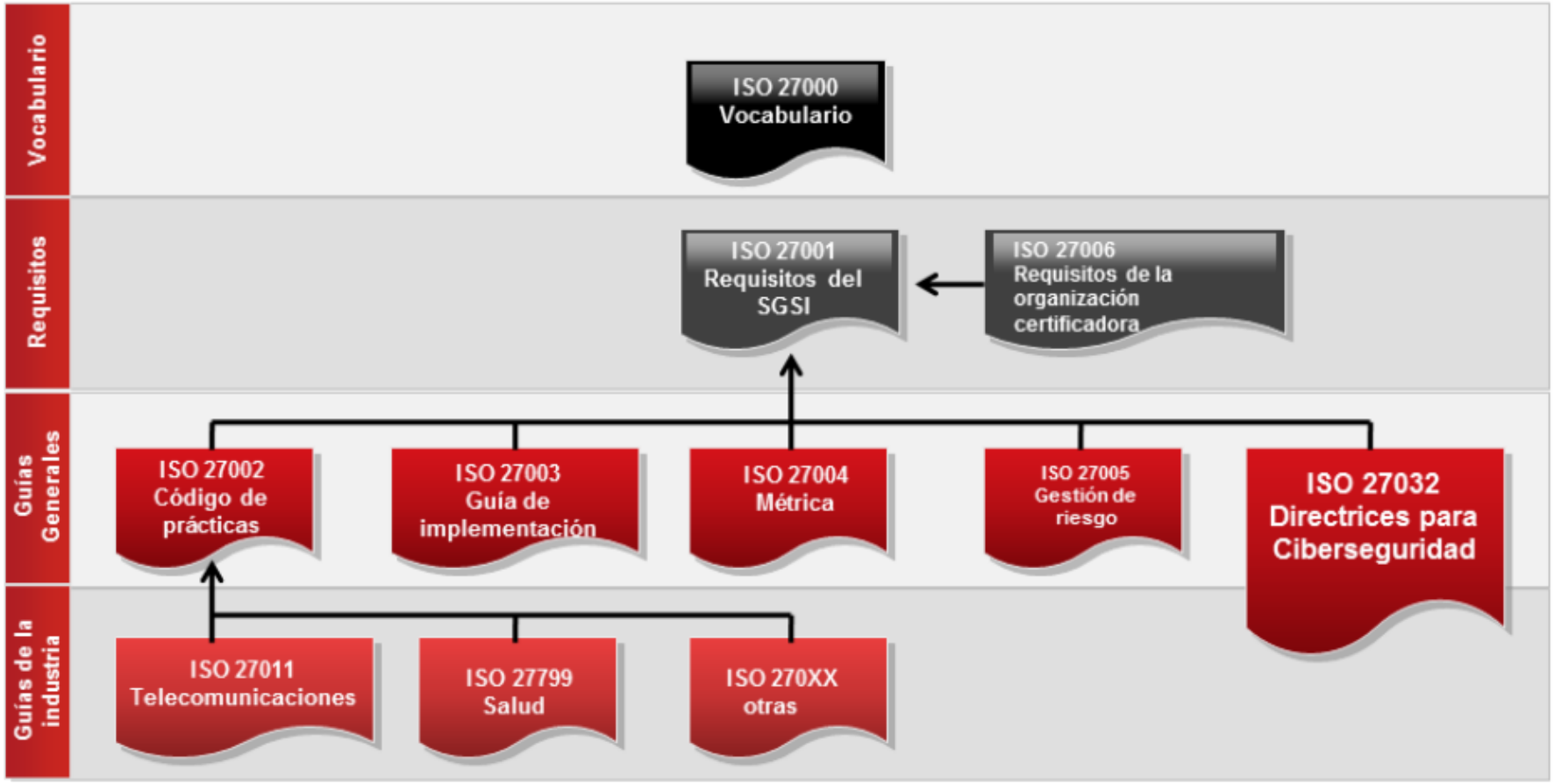
La toma de decisiones fundamentada

Mejora

Historia de la Norma ISO 27001

Fechas importantes

La familia ISO 27000



Resultante de reflexiones de grupos de trabajo internacionales dedicados al ámbito de la seguridad de la información, la familia ISO 27000 se está publicando gradualmente desde el año 2005. ISO 27001:2005 es la única norma certificable de la familia ISO 27000. Las demás normas son directrices.

- **ISO 27000:** Este estándar de seguridad de la información desarrolla los conceptos básicos, así como el vocabulario que se aplica en el análisis de un SGSI. Una copia gratuita de esta norma puede ser descargado desde el sitio de la ISO.
- **ISO 27001:** Esta norma de seguridad de la información define los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI).
- **ISO 27002 (anteriormente ISO 17799):** Guía de las mejores prácticas para la gestión de seguridad de la información. Esta norma define los objetivos y recomendaciones en materia de seguridad de la información y se anticipa a las preocupaciones globales de las organizaciones relacionadas con la seguridad de la información para sus actividades en general.
- **ISO 27003:** Guía para la implementación o la creación de un SGSI.
- **ISO 27004:** Guía de indicadores para facilitar la gestión del SGSI, proporciona un método para definir los objetivos para la implementación y de los criterios de eficacia, de las mediciones de seguimiento y evolución a través de todo el proceso.
- **ISO 27005:** Guía para la gestión de riesgos de seguridad de la información que cumple con los conceptos, modelos y procesos generales especificados en la norma ISO 27001.
- **ISO 27006:** Guía para las organizaciones que auditan y certifican los SGSI.
- **ISO 27007:** Directrices para la auditoría de sistemas de gestión de seguridad de la información
- **ISO 27008:** Directrices para los auditores de la seguridad de la información.
- **ISO 27011:** Directrices para el uso de la norma ISO 27002 en el sector de las telecomunicaciones.

ISO 27001

- Especifica los requisitos de gestión de un SGSI

  (Cláusula 4 a 10)
- Los Requisitos (cláusulas) son escritos utilizando el verbo “deben” en imperativo
- Anexo A: 14 cláusulas que contienen 35 objetivos de control y 114 controles
- La organización puede ser certificada en esta norma


INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2005-06-15

Information technology — Security techniques — Information security management systems — Requirements

Reference number
ISO/IEC 27001:2005(E)

© ISO/IEC 2005

ISO 27001:

- Un conjunto de requisitos normativos para el establecimiento, implementación, operación, supervisión y revisión para actualizar y mejorar un Sistema de Gestión de Seguridad de la información (SGSI);
- Un conjunto de requisitos para seleccionar controles de seguridad a la medida de las necesidades de cada organización, basado en las mejores prácticas de la industria.
- Un sistema de gestión que se integra en el marco de riesgo global asociado a la actividad de la organización;
- Un proceso reconocido internacionalmente, definido y estructurado para gestionar seguridad de la información;
- Un estándar internacional para adaptarse a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro...), de todos los tamaños en todas las industrias.

ISO 27001 27001, cláusula 0.1: Generalidades

Esta Norma Internacional ha sido preparada para proveer requisitos para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un sistema de gestión de seguridad de la información (SGSI). La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica de una organización. El diseño y la implementación del SGSI de una organización dependen de las necesidades y objetivos de cada organización, así como de sus requisitos de seguridad, sus procesos utilizados, y el tamaño y estructura de la organización. Es previsible que todos estos factores cambien con el tiempo.

El sistema de gestión de seguridad de la información mantiene la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión de riesgos y da la confianza a las partes interesadas de que los riesgos son manejados adecuadamente.

Es importante que el sistema de gestión de seguridad de la información sea parte de, y esté integrado con, los procesos y la estructura de gestión en general de la organización y que la seguridad de la información sea considerada en el diseño de los procesos, los sistemas de información y controles. Es de esperar que la aplicación de un sistema de gestión de seguridad de la información será escalado de acuerdo con las necesidades de la organización.

Esta Norma Internacional puede ser utilizada por partes internas y externas para evaluar la capacidad de la organización para satisfacer los requisitos propios de seguridad de la información de la organización.

ISO 27032

- Guía de buenas prácticas para las partes involucradas en el Ciberespacio
- Explicación de la interrelación entre la Ciberseguridad y otros tipos de seguridad
- Un Marco de Referencia para que las partes involucradas puedan colaborar en la resolución de los asuntos de Ciberseguridad
- La organización no puede obtener una certificación sobre este estándar


INTERNATIONAL STANDARD

ISO/IEC 27032

First edition
2012-07-16

Information technology — Security techniques — Guidelines for cybersecurity

Technologies de l'information — Techniques de sécurité — Lignes directrices pour la cybersécurité

Reference number
ISO/IEC 27032:2012(E)

© ISO/IEC 2012

ISO 27002

- Guía para el código de prácticas para los controles de la seguridad de la información (documento de referencia)
- Cláusulas escritas utilizando el verbo “debería”
- Compuesto de 14 cláusulas, 35 objetivos de control y 114 controles
- Una organización no puede ser certificada en esta norma

ISO 27002:

- Revisada en 2005, ISO 17799 es una guía de las mejores prácticas de gestión de seguridad de la información. En 2007, se convirtió en la norma ISO 27002 para integrarse a la familia de la norma ISO 27000. En 2013, se publica la segunda edición de la norma ISO 27002 .
- Esta norma internacional proporciona una lista de los objetivos y controles de seguridad generalmente practicados en la industria.
- En particular las cláusulas 5 a 18 prestan un asesoramiento específico y una guía para la aplicación de las mejores prácticas para apoyar los controles especificados en el Anexo A de la norma ISO 27001 (cláusula A.5 a A.18).

ISO 27009+

Dentro de la serie 27000, la ISO 27009 y los números siguientes están reservados para la creación de normas enfocadas a dominios específicos:

- Para las industrias:
  - Telecomunicaciones
  - Salud
  - Finanzas y seguros...
- Para sectores específicos relacionados con seguridad de la información:
  - Seguridad de las aplicaciones
  - Seguridad cibernética
  - Gestión de incidentes de seguridad
  - Protección de la privacidad