Título:	Norma ISO/IEC 27001:2013
Tipo:	Monografía
Autor:	Franklin Alexis Díaz Díaz
Fecha:	Diciembre 2018
Palabras claves:	Confidencialidad, integridad, disponibilidad
Aprobado por:	Decano de la Facultad de Ingeniería Mg. Ing. Enrique Durand Bazán
Firma:	

INTRODUCCIÓN

Las normas de la familia ISO/IEC 27000 constituyen un conjunto de estándares internacionales diseñados para ayudar a las organizaciones a gestionar de manera efectiva la seguridad de la información.

Estas normas proporcionan un marco integral que abarca desde la identificación y evaluación de riesgos hasta la implementación de controles específicos, garantizando así la confidencialidad, integridad y disponibilidad de la información. La serie ISO/IEC 27000 es particularmente relevante en un entorno digital donde las amenazas cibernéticas son cada vez más sofisticadas y frecuentes.

A través de la adopción de estas normas, las organizaciones no solo cumplen con requisitos legales y regulatorios, sino que también fortalecen su reputación y confianza ante clientes y socios.

Esta introducción a la familia ISO/IEC 27000, referente a la seguridad de la información, sienta las bases para comprender su estructura, objetivos y beneficios, así como su importancia en la gestión de la seguridad de la información en el mundo actual.

Normas ISO/IEC

La ISO (Internacional Organization for Standardization) es la Organización Internacional de Normalización, cuya principal actividad es la elaboración de normas técnicas internacionales. Tiene su sede principal en Ginebra, y es una federación de organismos nacionales entre los que se incluye a INACAL en el Perú.

Las normas ISO/IEC son un conjunto de normas reconocidas internacionalmente diseñadas para ayudar a las empresas a establecer niveles uniformes de gestión, prestación de servicios y desarrollo de productos en la industria.

ISO es una red de organismos nacionales de normalización de más de 160 países que publican normas internacionales. Desde 1947 se han publicado más de 19.000 normas.

Las normas ISO contienen instrucciones y recomendaciones para la correcta implementación de procesos y actividades en las organizaciones. Su objetivo es crear estándares reconocidos internacionalmente para garantizar que los productos y servicios que ofrece la empresa sean más eficientes, seguros y transparentes.

Además, las normas ISO proporcionan a los gobiernos la base técnica para la legislación sobre salud, seguridad y medio ambiente. También ayudan a transferir tecnología a los países en desarrollo y ayudan a proteger a los consumidores y usuarios en general.

Importancia de una norma estándar internacional

- Una norma ISO es un estándar internacional que refleja un conjunto de reglas orientadas a un determinado tipo de actividad, especificando qué objetivos y en qué tiempo deben alcanzarse, siguiendo un conjunto de instrucciones y cuya ejecución no está dada de antemano.
- Las normas ISO nos dicen qué, cuándo, qué o por qué y para qué, pero no nos dicen cómo.

Principales normas estándares ISO

Las 7 normas ISO principales en la actualidad son las siguientes:

1. ISO 9001

   Es la norma para implantar Sistemas de Gestión de la Calidad. De esta forma, las empresas pueden garantizar la calidad de los productos que ofrecen y sus procesos estandarizados.
2. ISO 27001

Es la norma relacionada con el Sistema de Gestión de la Seguridad de Información y Ciberseguridad. La certificación en ISO 27001 aporta mucho prestigio a una organización respecto del aseguramiento de la información.

3. ISO 22301

   Es la norma que garantiza el Sistema de Gestión de Continuidad de Negocio ante eventos que puedan poner en peligro la actividad de cualquier organización.

4. ISO 14001

   Es la norma para poner en marcha el Sistema de Gestión Medio Ambiental por excelencia. Las empresas preocupadas por el impacto ambiental de sus actividades implementan esta norma para garantizar unos procesos más sostenibles.

5. ISO 45001

   Siguiendo los requisitos de esta norma se puede implementar un Sistema de Gestión de Seguridad y Salud en el Trabajo. Es, por tanto, una guía de referencia para la gestión de riesgos laborales.

6. ISO 37301

   Es una norma ISO del Sistema de Gestión de Compliance. Siguiendo sus directrices, una organización puede prevenir riesgos de incumplimiento legal. De esta forma, reduce sus posibilidades de ser multada o sancionada por los organismos reguladores.

7. ISO 31000

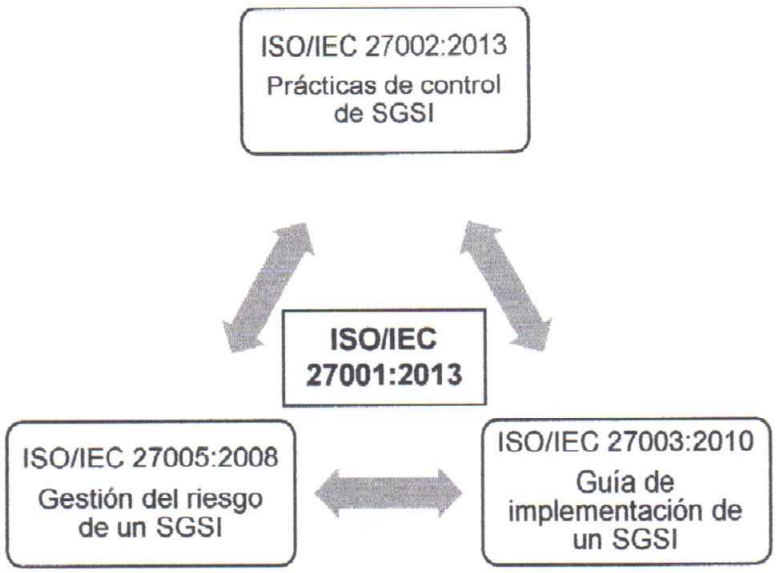
   Es la norma de referencia para implementar el pensamiento basado en riesgos en una organización. Gracias a ella, se reducen costos y se mitigan riesgos. Para su aplicación práctica, es ideal utilizar las técnicas y herramientas recogidas en ISO 31010.

Norma ISO/IEC 27001: 2013

- Es la norma internacional para los sistemas de gestión de la seguridad de la información (SGSI).
- Proporciona un marco robusto para proteger la información que se puede adaptar a organizaciones
  de todo tipo y tamaño.
- Es la única norma destinada a la certificación.
- La norma ISO-27002 proporciona las directrices para las normas de seguridad de la información de la organización y las prácticas de gestión de seguridad de la información, incluyendo la selección, implementación y gestión de los controles,

considerando el entorno de riesgos de seguridad de la información de la organización.

Normas intervinientes al implementar un SGSI basado en los estándares de la familia de normas ISO/IEC 27000

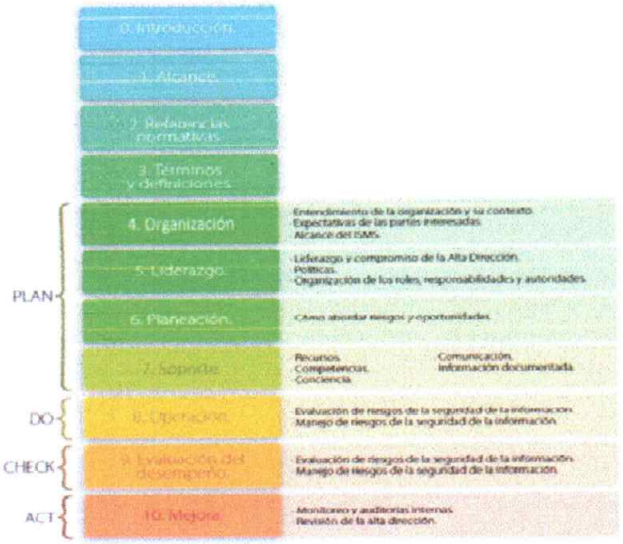


1. ISO/IEC 27001:2013 Sistemas de Gestión de Seguridad de la Información.
   - Las secciones 1 a 3 son introductorias y propias de la norma (no son obligatorias para la implementación).
   - Especifica los requisitos de gestión de un SGSI (Cláusula 4 a 10)
   - Los requisitos (cláusulas) son escritos utilizando el verbo "deberán" en imperativo
   - Anexo A: 14 cláusulas de control que contienen 35 objetivos de control y 114 controles (v.2013)
   - Una organización puede ser certificada en esta norma
2. ISO/IEC 27002:2013 Código de Buenas Prácticas para Controles de seguridad de la Información.
   - Guía para el código de prácticas para los controles de la seguridad de la información (Documento de referencia)
   - Un control es "una medida que modifica el riesgo"
   - Está compuesto de 14 cláusulas, 35 objetivos de control y 114 controles (v.2013)
   - Una organización no puede ser certificada en esta norma

3. ISO/IEC 27003:2010 Guía para la Implementación de los Sistemas de Gestión de Seguridad de Información.
   - Guía para el código de prácticas para la implementación de un SGSI
   - Documento de referencia para ser utilizado con las normas ISO 27001 e ISO 27002
   - Consta de 9 cláusulas que definen 28 etapas para implementar un SGSI
   - La certificación con esta norma no es posible
4. ISO/IEC 27005:2018 Gestión de Riesgos de Seguridad de Información.
   - Especifica el proceso de la gestión de riesgos de un SGSI
   - Proporciona directrices y lineamientos de métodos y técnicas de evaluación de riesgos de seguridad de la información como soporte de la ISO/IEC 27001.
   - Una organización no puede ser certificada en esta norma

Estructura Operativa de un Sistema de Gestión de Seguridad de la Información bajo la ISO 27001

1. Cláusulas de requisitos
   - Definen todas las actividades necesarias para implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).
   - Para estar alineada con el estándar, una organización debe cumplir con las cláusulas 4 a la 10 -en la versión de 2013.
2. Controles de seguridad
   - Un control es descrito como "una "medida que modifica el riesgo".
   - Son descritos en el Anexo A del documento, los cuales describen una lista de 114 controles de seguridad agrupados en 35 objetivos de control, que a su vez están considerados en 14 dominios para la versión de 2013.

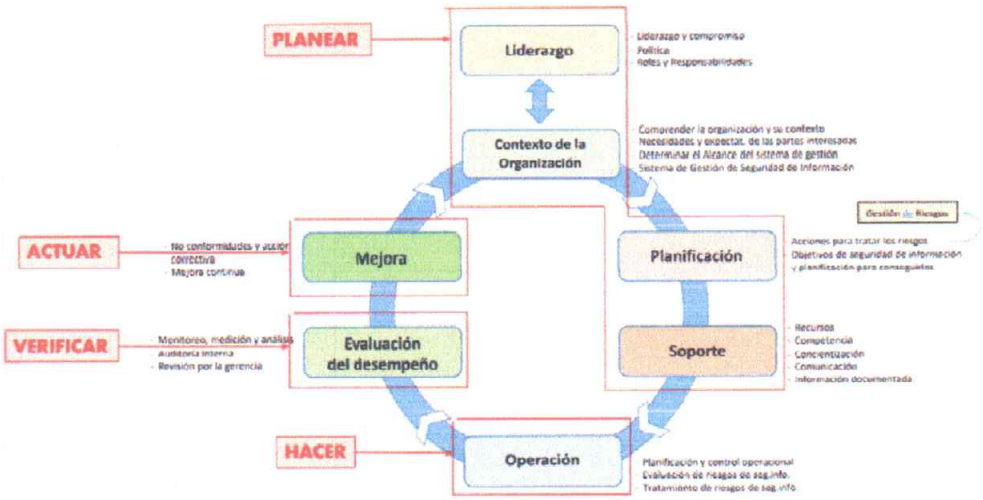


Estructura de la ISO 27001

Teniendo en cuenta las 07 cláusulas de implementación del SGSI, podemos concluir lo siguiente:

- El eje central de ISO 27001 es la gestión de riesgos que permitirá proteger la confidencialidad, integridad y disponibilidad (tríada CID) de la información en una empresa.
- Esto se logra investigando cuáles son los potenciales problemas que podrían afectar la información (evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (tratamiento de riesgos).
- Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.
- Las medidas de seguridad (o controles) que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos).
- Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software, pero los utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará relacionada con determinar las reglas organizacionales (por ejemplo, redacción de documentos) necesarias para prevenir violaciones de la seguridad.
- Como este tipo de implementación demandará la gestión de múltiples políticas, procedimientos, personas, bienes, etc., ISO 27001 ha detallado cómo amalgamar todos estos elementos dentro del sistema de gestión de seguridad de la información (SGSI).

- Por eso, la gestión de la seguridad de la información no se acota solamente a la seguridad de TI (por ejemplo, firewall, antivirus, etc.), sino que también tiene que ver con la gestión de procesos, de los recursos humanos, con la protección jurídica, la protección física, etc.



Metodología de Implementación de un SGSI – ISO 27001

1. Ciclo 1: Establecer el SGSI (Plan)
   1.1. Establecer la organización del SGSI
   1.2. Identificar los riesgos
   1.3. Analizar y evaluar los riesgos
   1.4. Objetivos de control y controles deben seleccionarse para cumplir con los requerimientos identificados en el proceso de análisis y tratamiento de riesgo
2. Ciclo 2: Implementar y operar el SGSI (Do)
   2.1. Implementar los controles seleccionados para cumplir los objetivos de control
3. Ciclo 3: Monitorear y revisar el SGSI (Check)
   3.1. Llevar a cabo revisiones regulares de la efectividad del SGSI
4. Ciclo 4: Mantener y mejorar el SGSI (Act)
   4.1. Implementar las mejoras identificadas en el SGSI

NTP-ISO/IEC 27001:2014

Es el complemento de la norma ISO de Seguridad de la Información para Perú. Norma técnica peruana elaborada con la finalidad de brindar los requisitos necesarios para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de seguridad de información; así mismo, los requerimientos para la implementación de

controles de seguridad para las necesidades de una organización, un sector de esta, o un proceso, según el alcance del SGSI. De igual forma se establece la documentación exigida para su certificación en el caso del cumplimiento de todos los requisitos. Así mismo, en el Anexo A de la mencionada norma se establece los controles que deben ser implementados en la organización para garantizar la seguridad de información. (NTP-ISO/IEC27001-2014, 2014).

Oficial de Seguridad de Información en las Organizaciones

- El CISO (Chief Information Security Officer / Oficial de Seguridad de la Información) es un ejecutivo de alto nivel responsable de alinear las iniciativas de seguridad con los programas corporativos y los objetivos de negocio, garantizando que los bienes y tecnologías de la información están adecuadamente protegidos.
- El rol del CISO no solamente debe tener experiencia y competencia en la materia, sino también contar con habilidades blandas (inteligencia emocional) necesarias para entender la visión de negocio y saber interrelacionarse con las diferentes áreas de la compañía.

BIBLIOGRAFÍA

Calder, A. (2017). ISO27001/ISO27002: una Guía de Bolsillo. Alemania: Walter de Gruyter GmbH.

Calder, A. (2009). Information Security Based on ISO 27001/ISO 27002. Países Bajos: Van Haren Publishing.

Chopra, A., Chaudhary, M. (2019). Implementing an Information Security Management System: Security Management Based on ISO 27001 Guidelines. Alemania: Apress.

Fernandez Climent, E. (2024). Iso/Iec 27001: 2022 Paso a Paso: Implementación, Auditoría y Mejora Continua. (n.p.): Amazon Digital Services LLC - Kdp.

Gómez Fernández, L., Andrés, A., Andrés Álvarez, A. (2012). Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. España: AENOR.

Kenyon, B. (2019). ISO 27001 Controls: A Guide to Implementing and Auditing. Reino Unido: ITGP.

Watkins, S. (2022). Iso/iec 27001:2022: An Introduction to Information Security and the ISMS Standard. Alemania: Walter de Gruyter GmbH.