# ISO/IEC 27000

**Jaime Damian Vasquez** **nickdamianvasquez@gmail.com**
*Facultad de Ingeniería y Arquitectura*
*Universidad Católica de Trujillo*
*Carretera Panamericana Norte Km. 555-Trujillo-Perú.*

**Resumen**

En la actualidad, las amenazas tecnológicas son una realidad cotidiana, especialmente en las organizaciones, que van desde virus hasta ataques sofisticados como los de día cero. Esto exige la implementación de controles de seguridad de la información para proteger los datos y recursos confidenciales, reduciendo la fricción de acceso de los usuarios ante amenazas. La dependencia de las Tecnologías de la Información y las Comunicaciones (TIC) en las organizaciones ha dado lugar a la necesidad de un Sistema de Gestión de Seguridad de la Información (SGSI) para garantizar la protección adecuada de la información y mantener niveles aceptables de riesgo. Las normas ISO/IEC 27000 definen la preservación de la confidencialidad, integridad y disponibilidad de la información. Este ensayo aborda la implementación de SGSI, la diferencia entre seguridad de la información y seguridad informática, y presenta las principales normas de la familia ISO/IEC 27000.

***Palabras clave:*** Cadena de Suministro, microempresas, crisis económica, estrategias

**Abstract**

Nowadays, technological threats are a daily reality, especially in organizations, ranging from viruses to sophisticated zero-day attacks. This necessitates the implementation of information security controls to protect confidential data and resources, reducing user access friction in the face of threats. The dependence on Information and Communication Technologies (ICT) in organizations has led to the need for an Information Security Management System (ISMS) to ensure the adequate protection of information and maintain acceptable levels of risk. ISO/IEC 27000 standards define the preservation of confidentiality, integrity, and availability of information. This essay addresses the implementation of ISMS, the distinction between information security and computer security, and presents the main standards in the ISO/IEC 27000 family.

***keywords:*** Amenazas tecnológicas, seguridad de la información, seguridad informática, Sistema de Gestión de Seguridad de la Información (SGSI), normas ISO/IEC 27000

## 1. Introducción

Hoy en día las amenazas tecnológicas son parte de nuestro día a día y más aún en las organizaciones, las cuales van desde diversas formas de virus, pasando por los recientes ataques de ransomware (Secuestro de datos), hasta amenazas sofisticadas como los ataques día cero (en inglés, zero-day attack (ataque contra una aplicación o sistema)). Lo cual requiere

la implementación de controles que puedan ser gestionados a través de un adecuado enfoque de seguridad de la información y de esta manera se protegerá los recursos y datos confidenciales con la finalidad de reducir la fricción de acceso de los usuarios mediante directivas dinámicas que escalan en tiempo real cuando se producen amenazas. La aparición de las Tecnologías de la Información y las Comunicaciones (TIC) y su nivel de dependencia por parte de las organizaciones y el uso adecuado de la información, dio inicio a la necesidad de una adecuada implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) que permita garantizar la adecuada protección de la información empresarial y mantener los niveles aceptables de riesgo de la información organizacional y de los dispositivos tecnológicos que permiten la recolección, procesamiento, acceso, intercambio, almacenamiento, transformación y adecuada presentación. Todo esto ha sido definido por la norma ISO/IEC 27000 como la preservación de la confidencialidad, integridad y disponibilidad de la información. Uno de los requisitos para implementar un SGSI (Sistema de Gestión de Seguridad de la Información), en una organización es conocer los estándares, su estructura y la relación existente entre cada uno de ellos. Las normas para implementar un SGSI corresponden a la serie ISO/IEC 27000 publicadas por la ISO y la Comisión Electrotécnica Internacional (IEC), compuesta por aproximadamente 17 normas.

Este ensayo tiene por finalidad argumentar la implementación de SGSI, la diferenciación entre seguridad de la información y seguridad informática, seguido de una explicación de las principales normas de la familia ISO/IEC 27000.

## 2. Análisis

Las normas ISO son normas o estándares de seguridad establecidas por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) que se encargan de establecer estándares y guías relacionados con sistemas de gestión y aplicables a cualquier tipo de organización internacionales y mundiales, con el propósito de facilitar el comercio, facilitar el intercambio de información y contribuir a la transferencia de tecnologías. Las series 27000 están orientadas al establecimiento de buenas prácticas en relación con la implantación, mantenimiento y gestión del Sistema de Gestión de Seguridad de la Información (SGSI) o por su denominación en inglés Information Security Management System (ISMS). Estas guías tienen como objetivo establecer las mejores prácticas en relación con diferentes aspectos vinculados a la gestión de la seguridad de la información, con una fuerte orientación a la mejora continua y la mitigación de riesgos. En la actualidad es relativamente fácil para una persona tener acceso a herramientas informáticas que le permiten acceder a información confidencial de una organización ya que esto generalmente ésta es transmitida por redes de datos e internet. Los avances tecnológicos, la facilidad de uso, disponibilidad en el mercado y la alta capacidad de cómputo de los equipos informáticos han contribuido a la globalización de la economía y por lo tanto a realizar negocios de distintas formas ya no tradicionales, ahora se realizan mediante compras en tiendas virtuales o comercio electrónico, inclusive entre países lejanos y de diferentes culturas alrededor del planeta. Sin embargo, esta situación y sus características también han facilitado que se presenten ataques hacia la información corporativa, los cuales han sido materializados de una forma más sofisticada y cada vez exigen menor conocimiento del atacante gracias a las herramientas disponibles para este fin.

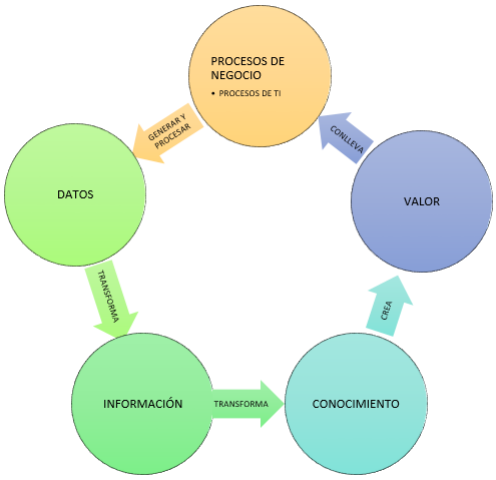


Figura 1: Ciclo de la ainformación

Tradicionalmente, se afirma que las organizaciones están inundadas por datos, los cuales, en ocasiones, no se aprovechan de forma adecuada como insumo para la generación de información que sirva de base para convertirla en conocimiento y, a partir de allí, incorporarla en sus diferentes estrategias organizacionales, para garantizar ciertos niveles de competitividad en el mercado.

Entre lo que cabe recalcar existen diferentes tipos de normas de seguridad y unas de las principales son las ISO 27000, la 27001 y también esta principal es la de la OSHA 18000. Iniciando por la norma de seguridad ISO 27000, es una de las estandarizaciones que recoge un extenso número de normas de la familia de ISO. La familia ISO 27000 contiene un conjunto de estándares de buenas prácticas para el establecimiento, implementación, mantenimientos y mejoras de SGSI. Esto nos permita evaluar todo tipo de riesgo o amenazas susceptibles de poner en peligro la información de una organización tanto propia como datos de terceros. Asimismo, nos permite establecer controles y estrategias más adecuadas para eliminar o minimizar dichos peligros. Además, que los pilares principales de esta familia son las normas 27001 y la 27002. La principal diferencia entre estas dos normas, es que 27001 se basa en una gestión de la seguridad de forma continua apoyada en la identificación de los riesgos de forma continuada en el tiempo. En cambio, 27002, es una mera guía de buenas prácticas que escribe una serie de objetivos de control y gestión que deberían ser perseguidos por las organizaciones.

La norma técnica ISO/IEC 27000 está enfocada en procesos, toda la organización se ve involucrada en su implementación en lo que a cada una le corresponde de tal manera que la suma de cada uno de los esfuerzos individuales, apoyados por la gestión y dirección de las personas que lideran el proceso, termine formando un SGSI que logre ejecutar todas las actividades de administración de riesgos incluyendo la creación de medidas ante tales riesgos y los controles para evaluar la efectividad de tales medidas [ISO]. La familia de normas ISO/IEC 27000 son de aplicación voluntaria pero su uso a nivel mundial facilita las relaciones comerciales entre compañías internacionales y aumenta la competitividad en el mercado, también ayuda a mejorar la calidad y productos ofrecidos ya que este estándar internacional

provee un modelo para establecer, implementar, operar y mantener un SGSI (Sistema de Gestión de Seguridad de la Información), basado en los objetivos de la compañía, requisitos, requerimientos y expectativas de seguridad independiente del tamaño, estructura y razón de ser del negocio. El ISO/IEC 27000 contiene términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión [ISO].

La norma ISO 27000 es un ciclo de mejora continua para la gestión de la seguridad de la información en la cual permitirá ayudar a las organizaciones a mantenerse actualizadas y adaptarse a todos los cambios en el entorno de seguridad de la información [Moya]. La seguridad de información en las empresas cuenta con algunos de los sistemas de gestión de seguridad en la cual han sido implementados de acuerdo a algunos requerimientos de la empresa u organización de la norma ISO 27000, su implementación es otorgada a las organizaciones o empresas en la que su ventaja es la de asegurar su información este protegida de la mejor manera posible [Ortuño].

Las ventajas de implementar la norma ISO 27000 en una organización es, que ayuda a las empresas a implementar una excelente gestión de seguridad de la información, siendo efectivo y eficiente, proporciona una estructura clara para una mejor gestión de seguridad, protege la información de la empresa y reduce los riesgos que existan de la seguridad y ataques cibernéticos, permite a las empresas cumplir con todos los reglamentos y aumenta la confianza y credibilidad de los clientes [ISOTools Excellence]. Así mismo las desventajas de implementar la norma ISO 27000 en una organización es, que podría ser costosa y requiere de recursos muy grandes, se puede tornar un poco difícil para entender y aplicar en las empresas u organizaciones, la norma ISO 27000 lleva tiempo y requiere gran cantidad de esfuerzo y dedicación, no se encuentra garantizada con la protección de la información y tiene procesos constantes de evolución y actualizaciones [ISOTools Excellence].

La norma ISO 27000 dentro de un plan de gestión de seguridad de la información, se encuentra certificada después de una auditoría. La empresa debe contar con un sistema de gestión de seguridad de información, su implementación deberán realizarlo durante 3 meses con anticipación, estas auditorías se deben considerar elementos como la política de seguridad, la asignación de responsabilidades de seguridad y la educación y capacitación en seguridad [Sánchez].

Con la ISO 27001 se deben implementar diversos tipos de controles en una organización, para tener la seguridad de la información sin ningún tipo de alteración y que este se mantenga intacta y le de tranquilidad a los usuarios que trabajen con la herramienta, esto para evitar que por un solo correo spam una empresa pueda llegar a la banca rota [ISO].

## 3. Conclusiones

La norma ISO 27000 es una herramienta valiosa para mejorar la gestión de la seguridad de la información de la organización, al implementar esta norma dentro de la misma puede tener una mejora de su capacidad de proteger sus activos de información y reduciendo el riesgo de incidentes con respecto a su seguridad, y por ende podrá tener un buen impacto positivo y de mucha confianza con el cliente y la reputación de la organización.

La seguridad de la información es un aspecto que debe ser parte de la cultura organizacional, es inherente que las actividades de parte humana ya sea con cursos, seminarios y

talleres no bastan, hay que profundizar en las personas de la organización, la necesidad y beneficios de dicha cultura estratégica, así como los riesgos de no tenerla.

La norma ISO 27001, pretende establecer una metodología cuyo objetivo es preservar la confidencialidad, integridad y disponibilidad de la información.

## Referencias


ISO. (2021). ISO/IEC 27000 - Information security management systems – Overview and vocabulary. https://www.iso.org/standard/74126.html

ISO. (2021). ISO/IEC 27001 - Information security management systems – Requirements. https://www.iso.org/standard/54534.html

ISO. (2021). ISO/IEC 27002 - Information security management systems – Code of practice for information security controls. https://www.iso.org/standard/54533.html

ISO. (2021). ISO/IEC 27000 - Information security management systems – Overview and vocabulary. https://www.iso.org/standard/74126.html

Moya, J. (2016). La norma ISO 27001 y la seguridad de la información. https://revistas.um.es/analitica/article/view/261651/0

Ortuño, E. (2017). Norma ISO 27001: Ventajas y desventajas en su implementación. https://www.isotools.org/2017/12/19/norma-iso-27001-ventajas-desventajas-implementacion/

ISOTools Excellence. (s.f.). Ventajas y desventajas de implementar la norma ISO 27001 en una organización. https://www.isotools.org/2019/11/12/ventajas-desventajas-de-implementar-la-norma-iso-27001-en-una-organizacion/

Sánchez, J. (2017). Implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001 en la empresa EMTUSA. https://digitum.um.es/digitum/bitstream/10201/52053/1/Tesis