Revista Académica:
CONTRIBUCIONES A LA ECONOMÍA
Grupo eumednet

Junio 2019 - ISSN: 1696-8360

# IMPORTANCIA DE LA NORMA ISO/EIC 27000 EN LA IMPLEMENTACION DE UN SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN

# IMPORTANCE OF ISO/ EIC 27000 STANDARD IN THE IMPLEMENTATION OF AN INFORMATION SECURITY MANAGEMENT SYSTEM

**M. en T.I. Gisela Regina Baena Cstro. ***
Centro Universitario Temascaltepec de la
Universidad Autonoma del Estado de Mexico.
gisela_baena_castro@hotmail.com

**M. en T.I. Rafael Valentin Mendoza Mendez. ****
Centro Universitario Temascaltepec de la
Universidad Autonoma del Estado de Mexico.
salascutemas@gmail.com

***Autor de Contacto*: Dr. Ernesto dorantes Joel Coronado. *****
Centro Universitario Temascaltepec de la
Universidad Autonoma del Estado de Mexico.
ernestodorantesc@hotmail.com

Para citar este artículo puede utilizar el siguiente formato:

Gisela Regina Baena, Rafael Valentín Mendoza Méndez y Ernesto dorantes Joel Coronado (2019): "Importancia de la norma ISO/EIC 27000 en la implementación de un sistema de gestión de la seguridad de la información", Revista contribuciones a la Economía (abril-junio 2019).
En línea: https://eumed.net/ce/2019/2/norma-iso-eic.html

RESUMEN

Las organizaciones dependen cada vez de la tecnología para garantizar el funcionamiento de sus procesos , y la información que se genera de sus actividades ha pasado a convertirse en su activo más valioso, por lo que no tomar medidas de seguridad para proteger ese activo le puede generar consecuencias importantes para la empresa y sus usuarios. Tal como lo menciona Joaquim Serrahima, en su libro titulado La amenaza digital: Conozca los riesgos informáticos que pueden arruinar su negocio.

> Las pérdidas de datos causadas por siniestros o incidentes son más comunes de lo que pueda pensar y en prácticamente todos los casos tienen consecuencias fatales ya que acostumbran a ser perdidas completas y, en muchos casos, incluyen la perdida de las copias de respaldo. (Serrahima, 2009)

Una amenaza informática se considera como toda circunstancia o un evento e inclusive una persona que tiene el potencial de efectuar un daño en un sistema, pudiendo ser este por sustracción de datos, destrucción, mostrar información clasificada, modificar sin autorización los datos de los registros de las bases de datos, siendo también cualquier vulnerabilidad o situación de riesgo de nuestro sistema de información que de nacimiento de cualquier vulnerabilidad que pueda ser aprovechada de manera ilícita. "Se denomina riesgo a la posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad". (Aguilera, 2010)

La compañía Symantec encargada de proveer producto y servicios de Ciberseguridad define una vulnerabilidad como:

> "Una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad (CIA) de los sistemas. Las vulnerabilidades pueden hacer lo siguiente:
>
> - Permitir que un atacante ejecute comandos como otro usuario.
> - Permitir a un atacante acceso a los datos, lo que se opone a las restricciones específicas de acceso a los datos.
> - Permitir a un atacante hacerse pasar por otra entidad.
> - Permitir a un atacante realizar una negación de servicio" (Symantec, 2017).

El periódico la expansión, de una nota tomada de la agencia de noticias Notimex menciona que los ataques cibernéticos dejan al año pérdidas de más de 24 millones de dólares en las empresas en México.

Ante esto se hace patente que la seguridad de los sistemas de información de las empresas ha dejado ser un lujo, para convertirse en una necesidad, esta implementación debe de ir acompañado de una metodología que proporcione una serie de lineamientos de forma metódica y lógica para disminuir y reducir de manera significativa el impacto de estos riegos que la empresa debe de conocer y afrontar de manera ordenada, por lo que estos procedimientos deben de ser adecuados a los que recomiendan los Sistemas de Gestión de la Seguridad basados en la norma ISO/IEC 27000 que proporciona un marco de gestión de los procesos orientados a la Seguridad de la Información dentro de las organizaciones.

Palabras Clave: ISO, SGSI, Seguridad Informatica, Riesgos Informaticos, ISO/IEC 27000

ABSTRACT

Organizations depend on technology every time to ensure the functioning of their processes, and the information generated from their activities has become their most valuable asset, so not taking security measures to protect that asset can generate important consequences for the company and its users. As mentioned by Joaquim Serrahima, in his book entitled The digital threat: Know the computer risks that can ruin your business.

Losses of data caused by accidents or incidents are more common than you may think and in almost all cases have fatal consequences as they tend to be lost completely and, in many cases, include the loss of backup copies. (Serrahima, 2009)

A computer threat is considered as any circumstance or event and even a person who has the potential to do a damage in a system, this may be by subtraction of data, destruction, display classified information, modify without authorization the data of the records of the databases, being also any vulnerability or risk situation of our information system that of birth of any vulnerability that can be exploited in an illicit way. "Risk is called the possibility of a threat materializing or not taking advantage of a vulnerability." (Aguilera, 2010)

The Symantec company in charge of providing Cybersecurity products and services defines a vulnerability as:

"A vulnerability is a flawed state in a computer system (or set of systems) that affects the confidentiality, integrity and availability (CIA) properties of the systems. The vulnerabilities can do the following:

• Allow an attacker to execute commands as another user.

• Allow an attacker access to data, which is contrary to specific restrictions on access to data.

• Allow an attacker to impersonate another entity.

• Allow an attacker to perform a denial of service "(Symantec, 2017).

The expansion newspaper, from a note taken from the Notimex news agency, mentions that cyber attacks leave more than 24 million dollars in losses per year in companies in Mexico.

Given this it becomes clear that the security of the information systems of companies has been a luxury, to become a necessity, this implementation must be accompanied by a methodology that provides a series of guidelines in a methodical and logical way to reduce and significantly reduce the impact of these risks that the company must know and deal with in an orderly manner, so these procedures must be appropriate to those recommended by the Safety Management Systems based on ISO / IEC 27000 which provides a management framework for the processes aimed at guaranteeing Information Security within organizations.

Key Words: ISO, ISMS, Computer Security, Computer Risks, ISO / IEC 27000.

INTRODUCCION

Una de las principales preocupaciones de las organizaciones públicas, que han realizado un esfuerzo e inversión en la implementación de sus sistemas de información automatizados en la mejora de sus servicios, trabajar en la implementación de una cultura de seguridad de su información, es proporcionar un marco de trabajo que le permita asegurar la no interrupción de sus procesos informáticos, minimizando así el impacto de los riesgos, e identificándolos para asegurar la protección de su información.

> Los riesgos a que está expuesta la información, se conocen como físicos y lógicos. Los riesgos físicos son el daño que puede sufrir el hardware y en general las instalaciones del centro o área de computo de la empresa. “Todos los riesgos lógicos han sido creados y siguen siendo creados por personas que tienen la intención de dañar o robar información de los sistema informáticos empresariales…”. (Baca, 2016)
>
> Dado que la información es uno de los activos más importantes de toda organización, requiere junto a los procesos y sistemas que la manejan, ser protegidos convenientemente frente a amenazas que puedan poner en peligro la continuidad de los niveles de competitividad, rentabilidad y conformidad legal necesarios para alcanzar los objetivos de la organización. (Ofiseg Consulting, S.L., 2010).

En contemplación de lo anterior se puede observar que es obligatorio que las empresas lleven a cabo la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) con el fin de manejar estos riesgos bajo una normativa que regule estas actividades de manera lógica y sistemática con el fin de garantizar la efectividad de sus implementaciones y esto se logra mediante el apoyo de los estándares internacionales sobre la Seguridad de la Información ISO. Siendo las normas ISO normas o estándares que son establecidas por la Organización Internacional para la Estandarización (ISO), y la Comisión Electrotécnica Internacional (IEC), que son las encargadas de crear e implementar estándares y la manera en que estas deben implementarse a través de guías, en los sistemas de gestión que son aplicables a cualquier organización nacionales o internacionales.

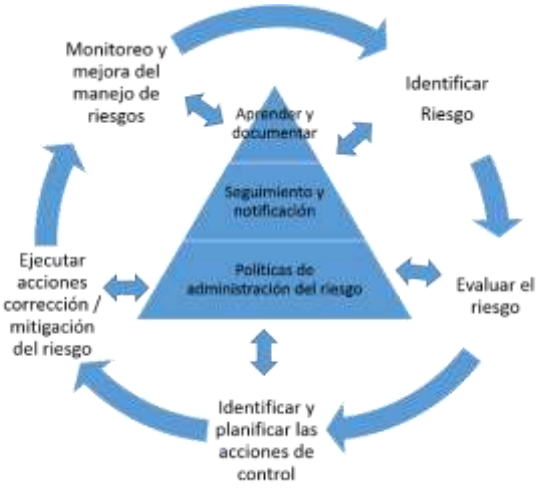

*Figura 1 : Ciclo de identificación, planificación y manejo del riesgo, elaboración propia.*

*Figura 1: Ciclo de identificación, planificación y manejo del riesgo, elaboración propia.*

En apoyo de la adopción de un Sistema de Gestión de Seguridad de la Información existe la norma ISO 27000 que se desarrolló para ser un conjunto de estándares internacionales sobre la Seguridad de la Información, esta norma presenta una serie de procedimientos de buenas prácticas para establecer, mantener y optimar al mismo tiempo que estandariza estos procedimientos para normar los Sistemas de Gestión de la Seguridad de la Información.

> La serie de normas ISO/IEC 27000 se denomina << requisitos para la especificación de sistemas de gestión de la seguridad de la información (SGSI)>>, proporciona un marco de estandarización para la seguridad de la información para que sea aplicado en una organización o empresa y comprende un conjunto de normas sobre las siguientes materias:
>
> - Sistemas de gestión de la seguridad de la información.
> - Valoración de riesgos.
> - Controles.” (ISOTools, 2015)

Un Sistema de Gestión de Seguridad de Información (SGSI) debe descansar en tres objetivos fundamentales que garanticen los datos que maneja y estos son:

- La Confidencialidad.
- La Integridad
- La Disponibilidad.

En lo que se conoce como el triángulo de la seguridad de los datos con el acrónimo de CID, Confidencialidad, Integridad y Disponibilidad:


*Figura 2: Triángulo de la Seguridad de la Información: Elaboración propia*

Donde la

- **Confidencialidad:** Debe garantizar que el acceso al sistema está limitado solamente a los usuarios que tengan el nivel de autorización pertinente, evitando así que la información importante pueda ser accesado por alguien que no tiene el nivel de acceso autorizado.

La OCDE (Organización para la Cooperación y el Desarrollo Económico), en sus Directrices para la Seguridad de los Sistemas de Información define la confidencialidad como << el hecho de que los datos o información estén únicamente al alcance del conocimiento de las personas, entidades o mecanismos autorizados, en los momentos autorizados y de una manera autorizada>>. (Aguilera, 2010).

- **Integridad:** Esta debe asegurar que los registros del sistema solo pueden modificarse, o eliminarse por usuarios que cuenten con el nivel de autorización requerido, así esta asegura que no se realicen modificaciones por usuarios no autorizados, que no se lleven a cabo modificaciones por usuarios o procesos que no tengan autorización, manteniendo así la integridad de estos tal como fue generada. "Integridad: La propiedad de salvaguardar la exactitud e integridad de los activos" (Alberto, 2005).
- **Disponibilidad:** Esta es la característica de los sistemas que le condiciona que la información debe de estar a disposición de quienes tengan el nivel de acceso a ella, pudiendo ser otro proceso o una persona que necesite hacer uso de esta. Sin importar que existan interrupciones de energía, fallos de los medios de almacenamiento u otro hardware o por la aplicación de la alguna actualización para corregir algún bug del sistema. "Se trata de identificar los riesgos, cuantificar su probabilidad e impacto, y analizar medidas que los eliminen –lo que generalmente no es posible- o que disminuyan la probabilidad que ocurran los hechos o mitiguen el impacto" (Mario G.Piattini, 2001).

Normas serie ISO 27000: La serie de normas internacionales ISO/IEC 27000 ofrecen una serie de recomendaciones de mejores prácticas, para la gestión de la seguridad de la información, y esta puede ser aplicada en cualquier organización sin importar el tamaño que tenga, está orientada a que estas puedan mantener un Sistema de Gestión de la Seguridad, la cual está compuesta de las siguientes normas que se pueden observar en la siguiente tabla, y de las cuales más adelante solo se harán la descripción de la 27001,27002, 27003, 27004 y 27005 al ser las que se encuentran relacionadas más íntimamente con la puesta en marcha de un SGSI.

*Tabla 1: Componentes de la familia de la norma 27000, elaboración propia.*

| Familia de normas 27000 | |
|---|---|
| ***NORMA ISO*** | ***CONTENIDO*** |
| **ISO 27000** | Estándar que contiene las definiciones y los términos que se usan en toda la familia de normas de la ISO 27000. |
| **ISO 27001** | Norma que contiene y provee los requisitos del SGSI , enumera los objetivos de control en su implementación del SGSI. |
| **ISO 27002** | Provee un manual de buenas prácticas para gestionar |

| | |
|---|---|
| | la seguridad de la información. No es una norma certificable. |
| **SO 27003** | Provee una serie de directrices para la implementación del SGSI, y sirve de soporte para la 27001, no es una norma certificable. |
| **ISO 27004** | Proporciona una guía, para la creación y uso de métricas y metodologías de medida aplicadas a determinar la eficacia del SGSI. No es una norma certificable. |
| **ISO 27005** | Proporciona directrices para gestionar el riesgo en la Seguridad Informática, dando soporte a la 27001 en el proceso de gestión de riesgos. |
| **ISO 27006** | Norma que proporciona los requisitos para la acreditación de organismos que acreditan y auditan los sistemas de gestión de seguridad de la información. |
| **ISO 27007** | Manual que proporciona los lineamientos para auditar los Sistemas de Gestión de Seguridad de la Información. |
| **ISO 27011** | Guía de administración de la seguridad en la gestión de telecomunicaciones. |
| **ISO 27031** | Norma que hace una descripción de procesos y los métodos necesarios para señalar e identificar los aspectos que sirvan en la implantación de las TICs con el fin de garantizar la continuidad del negocio. |
| **ISO 27032** | Proporciona un marco de trabajo seguro para el intercambio de información, manejo de incidentes y coordinación con el fin de hacer más seguros los procesos. |
| **ISO 27033** | Norma orientada a la administración de la seguridad de las redes de datos de las organizaciones contemplando los apartados de la gestión de su seguridad, el diseño de la arquitectura de su seguridad, marcos de referencias, uso de Gateway, Control en el acceso remoto, uso de VPNs y del diseño e implementación de la seguridad en las redes. |
| **ISO 27034** | Norma que proporciona una guía de seguridad de las aplicaciones. |
| **ISO 27799** | Norma que proporciona un estándar de la Gestión de |

| | |
|---|---|
| | Seguridad de la Información en el sector sanitario, estableciendo controles y buenas prácticas que deben implementar las empresas del sector sanitario. |

DESCRIPCIÓN

Procederemos a describir sólo aquellas de mayor importancia en la implementación del Sistema de Gestión de Seguridad de la Información (SGSI).

ISO 27001, Norma certificable que tiene su origen en la norma británica BS 7799-2 elaborara con el fin de poder certificar los Sistemas de Gestión de Seguridad de la Información, es un estándar internacional que permite el aseguramiento, confidencialidad e integridad de los datos y de la información, así como del sistema que la procesa, especificando los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información conocido como un SGSI, "La norma ISO 27001 se ha impuesto como referencia en materia de seguridad de los sistemas de información, principalmente para la aplicación de un sistema de gestión de seguridad de la información …" (Carpentier, 2016). Esta norma sigue el enfoque o ciclo Deming PDCA que consiste en Planificar, Hacer, Verificar y Actuar. Entre las actividades a desarrollar en su implantación se encuentran:

1. Definir el alcance del Sistema de Gestión de Seguridad de la Información.
2. Definir Políticas de Seguridad.
3. Identificar los riesgos.
4. Definir los procedimientos para la administración del riesgo.
5. Identificar una metodología para el Análisis y Gestión del Riesgo.
6. Definir métricas para medir la eficiencia de los controles.
7. Desarrollo de programas de Cultura de la seguridad informática.
8. Administración de los recursos y operaciones.
9. Otros.

En la actualidad podemos observar que las empresas y organizaciones enfrentan a diario riesgos e inseguridad en sus datos que provienen de los nuevos negocios y tecnologías relacionadas con la información que los miembros de estas deben manejar. Es aquí que la norma ISO 27001 provee un marco de trabajo para evaluar estos riesgos y ayudar a establecer una serie de controles y estrategias para proveer protección a los flujos de información de estas teniendo como principal propósito establecer, implantar, mantener y mejorar de forma permanente la seguridad de la información en las empresas, pero no debemos perder vista que "Si bien la ISO 27001 es la norma en base a la cual se certifica por auditores externos, a la empresa u organización a los Sistemas de Gestión de Seguridad de la Información de la misma. Aunque el hecho de estar certificado en ISO 27001 no prueba que la organización sea 100% segura" (López, 2015).

ISO 27002 es una norma que sirve de apoyo de la 27001, proveyendo una guía de buenas prácticas en la implementación e controles que puedan garantizar gracias a estas la seguridad de la información, antes conocida como ISO 17799, y basada en la norma británica BS 7799, siendo conformada por 14 dominios principales que son los siguientes:

1. Políticas de Seguridad.
2. Organización de la Seguridad de la Información.
3. Seguridad de los Recursos Humanos.
4. Gestión de Activos.
5. Control de Accesos
6. Cifrado.
7. Seguridad Física y Ambiental.
8. Seguridad de las Operaciones.
9. Seguridad de las Comunicaciones.
10. Adquisición de Sistemas.
11. Relaciones con los proveedores.
12. Gestión de Incidencias.
13. Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio.
14. Conformidad.

ISO 27003 Si bien la norma ISO 27002 es una guía de buenas prácticas en la implementación de controles, la ISO 27003 establece un marco de trabajo con el propósito de conseguir una aprobación de implantar un Sistema de Gestión de Seguridad de la Información (SGSI), pudiendo ser usada por aquellos administradores de tecnologías de las empresas que deseen implantar un SGSI, en conformidad con el estándar ISO 27 001 proporcionando una serie de directrices para realizarlo, que ayudan a la delimitación del SGSI además de la planeación, diseño y ejecución de distintos planes en su implementación, su contenido se refiere a:

1. Alcance.
2. Referencias Normativas.
3. Términos y Definiciones.
4. Estructura de esta Norma.
5. Obtención de la aprobación de la alta dirección para iniciar un SGSI.
6. Definición del alcance del SGSI, límites y políticas.
7. Evaluación de requerimientos de seguridad de la Información.
8. Evaluación de Riesgos y Plan de tratamiento de riesgos.
9. Diseño del SGSI.

Así como los siguientes anexos:

- Anexo A, un checklist de la implementación del SGSI.

- Anexo B, donde se comprueban las responsabilidades y roles de seguridad de la información.
- Anexo C, donde se muestra información sobre las auditorías internas.
- Anexo D, la estructura de las políticas de seguridad.
- Anexo E, donde se presenta el monitoreo y seguimiento del SGSI.

ISO 27004 Es una norma no certificable que fue publicada en 2010, y revisada y actualizada el 12 de abril del 2016, es una norma orientada a medir y evaluar la eficiencia de la Seguridad de la Información, y tiene como objetivo medir y evaluar los resultados de la ISO 27001. La ISO 27004 muestra que las medidas que necesitemos implementar, dependerán del tamaño y que tan compleja sea la organización, del nivel de integración que deseemos de la relación seguridad-información y sobre todo la relación costo-beneficio que estemos dispuestos solventar. En la introducción del documento de esta norma se puede leer "El empleo de este estándar permitirá a las organizaciones dar respuesta a los interrogantes de cuan efectivo y eficiente es el SGSI y que niveles de implementación y madurez han sido alcanzados." De esta manera se puede observar que su importancia reside en la capacidad de "medir los controles", y de esta manera detectar si un control no puede ser medido no tiene ninguna aportación al SGSI.

Las etapas que propone son las siguientes:

1. Elegir los objetivos y procedimientos de medición, ya que las empresas deben medir los alcances y efectividad de los métodos, en este punto sólo se consideran los que han sido documentados de manera permanente, un ejemplo serían los controles, el desempeño, etc. Por lo que las empresas deben definir lo que se debe medir y su alcance.
2. Selección de valores base, que deben ser establecidos para cada objeto que se esté midiendo, ya que estos marcan una referencia de partida para la medición de estos objetivos o procedimientos.
3. Recopilación de datos precisos que deben ser dimensionados, se pueden implementar procedimientos programados de recogida de datos, para que esto se haga de manera normalizada y poder presentar informes.
4. Desarrollo de un sistema de medición ya que esta norma ISO 27004 presenta una secuencia metódica y lógica de operaciones en diferentes facetas del objeto a medir, se hace uso de indicadores como fuentes de información para mejorar los Sistemas de Información de Seguridad de la Información.
5. Interpretación de los valores medidos que, mediante procedimientos y uso de tecnologías para su análisis y entendimiento, se debe identificar las diferencias entre los valores de inicio y los obtenidos en tiempo real.

6. Información de los valores obtenidos en la medición al SGSI a la parte interesada, pudiendo ser un reporte con forma de gráficos, cuadros de mando operacionales u cualquier otro medio de fácil manejo y entendimiento.

ISO 27005 es una norma que fue publicada por primera vez en el 2008 y revisada en el 2011, y que contiene diferentes recomendaciones que se encargan de la gestión de riesgos de la Seguridad de la Información. La norma ISO 27005 es el estándar internacional que se ocupa de la gestión de los riesgos relativos a la seguridad de información. La norma suministra las directrices para la gestión de riesgos, apoyándose fundamentalmente en los requisitos sobre esta cuestión definidos en la ISO 27001 (ISOTools, 2015).

Se centra en la Gestión de Riesgos dejando a un lado el análisis de los mismos, ya que estos pueden impactar en los objetivos de las organizaciones y en sus metas. El fin que persigue es el de minimizar el impacto que pueda ocasionar al ser vulnerado sus protocolos de seguridad o un fallo del uso de las tecnologías de la Información, que les puedan suponer pérdidas financieras, que se vea afectada su imagen, o en algún problema a nivel operativo o de toma de decisiones. Si bien no existe un método que garantice la gestión correcta de riesgos su utilidad se ve reflejada al proporcionar un proceso metódicamente estructurado, de carácter sistemático basado en un riguroso análisis de riesgos para la creación de un plan de contingencia que permita tratarlos cuando estos ocurran, pudiendo ser aplicaciones sin parches de seguridad, sistemas operativos vulnerables, aplicaciones con bugs, uso de tecnologías de datos obsoletas lo que las haría vulnerables o mala gestión de la infraestructura de Tecnología, entre otros.

## CONCLUSIONES

Al Implementar un Sistema de gestión de Seguridad de la Información, es importante que deba hacerse de una manera estricta y metódica, por cualquier empresa que desee implementar controles que le ayuden a proteger su Sistema de Gestión de la Información que maneja en cada uno de sus procesos y así poder garantizar la confidencialidad, disponibilidad y su integridad de un de sus activos mas importantes , que es la información que procesa consume, procesa y produce, situación que sólo puede darse al ser esta manejada dentro de un marco de trabajo institucional que garantice su seguridad sin importar que esta se procese en un medio físico o lógico.

Con los avances tecnológicos al alcance de todos, surgen por parte de delincuentes informáticos constantemente nuevos métodos para comprometer la seguridad de la información que genera almacena o intercambia una empresa u organización, lo que las debe llevar a la implementacion de un Sistema de Gestion de la Seguridad de sus Sistemas de Información, una necesidad cada vez más evidente para la implementación de una estrategia orientada a la seguridad de los Sistemas de Información con los que esta interactuando con el fin de prevenir y administrar los riesgos informáticos a los que se puede ver expuesta. Para llevar a cabo esto mensionado es importante realizarlo con el apoyo de una norma ISO de esta area ya que aportaria a la empresa

una serie de procedimientos que ayudan a que regular el funcionamiento de las distintas areas de estas, al proveer un idioma de calidad comun.

La norma ISO/IEC 27000 son un conjunto de estándares que fueron y están siendo desarrolladas por la International Organization for Standardization (ISO) y la International Electrotechnical Commission (IEC), con el fin de proporcionar un marco de trabajo y administración de la seguridad de la información, para que esta pueda ser utilizada por cualquier organización sea esta pública, privada micro, mediana o grande.

Siendo de todas ellas la norma ISO/IEC 27001 como la principal al ser la única certificable pudiendo ser aplicada a cualquier organización sin importar su giro, tamaño, privada o pública aportando una metodología orientada a la puesta en funcionamiento del SGSI (Sistema de Gestión de la Seguridad de la Información) al implementar controles para ello.

Esta puede ser aplicada para resolver problemas dentro de las empresas que no tenga claro quien toma desiciones sobre sobre ciertos activos de informacion, quien tiene acceso a ellos o quien autoriza el acesso a los sistemas informaticos de la empresa.


*Figura 3: ISO 27001 y componentes principales, elaboración propia.*

En definitiva lleva a la empresa a establecer una cultura del a seguridad, ayudandole a establecer planes de contingencia, que le ayudan a reducir el impacto de los riesgos que de no administrarlos pueden convertirse en serias amenazas que afecten la continuidad del negocio de la empresa, lo que podría llevar a reclamaciones de clientes, demandas y perdidas de distintas oportunidades de negocio en el mercado.

Por último cabe mencionar que aquellas empresas que quieran beneficiarse de la implementación de la norma ISO 27001, como una diferenciación y ventaja competitiva con respecto a sus competidores, o moverse comercialmente en un mercado internacional deben certificarse en esta.

REFERENCIAS


Aguilera, P. (2010). *Seguridad informática, Ciclos Formativos.* Madrid: Editex.

Alberto G. P. (2005). *Análisis del Riesgo y el Sistema de Gestión de Seguridad de la Información: El Enfoque ISO 27001:2005.* Obtenido de http://www.iso27000.es/download/Analisis_del_Riesgo_y_el_ISO_27001_2005.pdf

Baca, G. (2016). *Introducción a la seguridad informática.* México: Grupo Editorial Patria.

Carpentier, J. F. (2016). *La seguridad informática en la PYME: Situación actual y mejores prácticas.* Ediciones ENI.

ISOTools (5 de 10 de 2015).Cómo implantar eficazmente la norma ISO 27005. Obtenido de https://www.isotools.org/2015/10/05/como-implantar-eficazmente-la-norma-iso-27005/

López, A. (2015). *Guía para gestionar los datos personales.* Madrid: Colección Alianza Formación Gestión.

Ofiseg Consulting, S.L. (2010). *¿Qué es un SGSI?.* Obtenido de http://www.ofisegconsulting.com/iso27000.htm

Piattini, M. (2001). *Auditoría Informática, Un enfoque práctico.* Madrid, España: Alfaomega Grupo Editor, S.A. de C.V.

Serrahima, J. (2009). *La amenaza digital: Conozca los riesgos informáticos que pueden arruinar su negocio.* Barcelona: Profit Editorial.

Symantec. (2017). *Glosario de Seguridad 101*. Obtenido de https://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad