Universidad Nacional Experimental Del Táchira
Vicerrectorado Académico
Decanato De Docencia
Departamento De Informática
Seminario

Familia de estándares ISO 27000

Elaborado por:

- Tyson Cardelli C.I.: 23.542.402
- Carlos Rangel C.I.: 21.003.721
- Arturo Bernal C.I.: 19.925.695
- Leydy Moreno C.I.: 24.743.325

Julio de 2016

Familia de Estándares ISO/IEC 27000

A través del tiempo las organizaciones se han preocupado cada vez más en satisfacer las necesidades de los clientes. Esta constante búsqueda para alcanzar la calidad dejaba la interrogante ¿Cuando mi producto es lo suficientemente bueno?. De allí surgió la necesidad de contar con estándares universales.

La organización internacional para estandarización ISO (International Organization for Standardization) es una organización mundial que agrupa a representantes de cada uno de los organismos nacionales para la estandarización cuyo objetivo es desarrollar estándares que faciliten las relaciones internacionales.

Si hablamos de la ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO e IEC (International Electrotechnical Commission) que garantizan un esquema de seguridad de la información adaptable a cualquier compañía

A continuación se hace una breve descripción de la familia de estándares ISO-27000 haciendo referencia al alcance y al propósito de cada una de ellas:

Estandar ISO-27000

La norma fue publicada inicialmente el 1ero de mayo del 2009 el alcance de la ISO-27000 abarca una visión general de las normas de la ISO-27000. Además en ella podemos encontrar una introducción bastante completa acerca de lo que es un sistema de seguridad de la información y un vocabulario empleado en la familia de estándares. El Propósito de publicación de esta norma es describir los aspectos fundamentales acerca de seguridad de la información los cuales están sujetos a los conceptos de un SGSI y toda la familia de estándares en general.

Estándar ISO-27001

Es considerada la norma principal de la serie, esto es debido a que enmarcado en la ISO-27001 las organizaciones pueden optar por su certificación. Es importante mencionar que el alcance de esta norma abarca los requerimientos mínimos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un sistema de seguridad de la información. Además la norma toma en cuenta los riesgos a los que está sujeto el negocio, sin tener en cuenta su tipo, tamaño o naturaleza ,aspecto fundamental en la seguridad de la información. Por lo tanto el propósito de la norma es establecer una normativa estándar para el desarrollo y operación de un SGSI mostrando además controles que logren minimizar los riesgos.

Estàndar ISO-27002

Esta norma menciona los controles a aplicar en lo concerniente a la seguridad de la información, el alcance de esta norma es proporcionar una guía de controles recomendados para mitigar los riesgos. Contiene 39 objetivos de control con 133 controles agrupados en 11 dominios. Igualmente la ISO-27001 contiene un anexo que presenta los controles de la ISO-27002, el propósito de esta norma es orientar sobre la aplicación de los controles basado en buenas prácticas

Estándar ISO/IEC 27004

Esta norma no es certificable, sin embargo, presenta un sistema de métricas e indicadores.
Alcance: Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI, objetivos de control y controles que se utilizan para implementar y administrar la seguridad de la información según ISO/IEC 27001.
Propósito: Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Check” del ciclo de Deming.

Estándar ISO/IEC 27005 :

Esta norma Otorga una guía de análisis de gestión de tu riesgos aplicados específicamente a los SGSI. Al igual que la norma 27004 no es certificable.
Alcance: Presenta las pautas para la gestión del riesgo en la seguridad de la información sobre los conceptos generales definidos en la norma ISO/IEC 27001.
Propósito: Esta norma está diseñada ayudar a la aplicación exitosa de la seguridad de la información basada en un enfoque de gestión de riesgos.

Estándar ISO/IEC 27006

Contiene especificaciones para los organismos certificadores de los sistemas de gestión de la seguridad de la información.
Alcance: enmarcan los requisitos específicos a cumplir para la acreditación de entidades auditoras y certificadoras de los SGSI.
Propósito: Añade a ISO/IEC 17021 los requisitos específicos relacionados con ISO 27001:2005, en otras palabras, ayuda a interpretar los criterios de acreditación de dicha norma cuando se aplican a entidades de certificación de ISO 27001.

Estándar ISO/IEC 27007

Es una guía para auditar específicamente SGSI, qué aplica como complemento a lo especificado en ISO 19011.
Alcance: específica directrices para auditar los SGSI, en las normas generales contenidas en la ISO 19011, así como también provee información sobre las conductas internas y externas a auditar.

Propósito: Orientar sobre la auditoría de sistemas de gestión de la seguridad de la información, así como orientación de las competencias de los auditores

Estándar ISO-27006

Menciona los requisitos para la acreditación de entidades de auditoría y certiicaciòn de los sistemas de gestión de seguridad de la información, fue publicada en su primera edición el 1 de Marzo de 2007. El alcance de esta norma tiene como objeto proporcionar una guía para todos aquellos organismos que realizan auditoría y certificación de un SGSI de acuerdo con la ISO-27001. Por lo tanto el propósito de la publicaciòn de esta norma fue presentar un estàndar de los requerimientos por medio de los cuales se puede acreditar una organización.

Estándar ISO-27008:

Este estándar busca dar orientación a los auditores sobre la revisión de los controles relacionados con la seguridad de la información. Basándose en un patrón de revisión establecido por la misma organización.

Estándar ISO-27013:

proporciona una guía para facilitar la integración de las normas ISO-27001 e ISO 20000-1 en una organización donde previamente exista al menos alguna de las dos. Ayudando a la organización en la comprensión de las características, similitudes y diferencias de ambas normas

Estándar ISO-27014:

Dado que la seguridad de la información es un factor clave para el desarrollo de sus actividades y su imagen ante sus clientes, este estándar establece los principios básicos para la gestión de la seguridad de la información que toda organización debe cumplir.

Estándar ISO-27016:

Este estándar establece por medio de un informe una metodología que permite a cualquier organización conocer con precisión el valor de sus activos de información y el valor de los riesgos sobre esos activos. Todo con la finalidad de dar una orientación sobre cuánto debería invertir en un SGSI.

Estándar ISO-27010

Esta norma internacional establece una serie de directrices para orientar a las organizaciones sobre qué controles implementar para mejorar la seguridad de la difusión de información sensible que se realiza de forma inter-organizacional.

Existen normas que se adaptan al contexto de las organizaciones y son complemento para otras normas, entre ellas se encuentran:

Estándar ISO-27011

Esta norma está orientada únicamente a aquellas organizaciones en el ámbito de las telecomunicaciones que ya posean una adaptación de la norma ISO-27002. Encargándose de establecer una serie de pautas a este tipo de organizaciones.

Estándar ISO-27015

Esta norma va dirigida a aquellas organizaciones que prestan servicios de carácter financiero. Es un suplemento para ayudar en la implantación del estándar ISO-27001:2005 tanto en el diseño como en los controles definidos.

Estándar ISO-27799

Esta norma va dirigida a todas aquellas organizaciones dedicadas al área de la salud que están implantando la ISO 27002:2005.

La información que manejan las organizaciones del sector sanitario debe cumplir ciertos criterios en cuanto a su integridad, disponibilidad y accesibilidad, allí es donde esta norma resulta importante ya que se encarga de establecer unas pautas únicas para la protección de la información, por ejemplo los datos de pacientes.