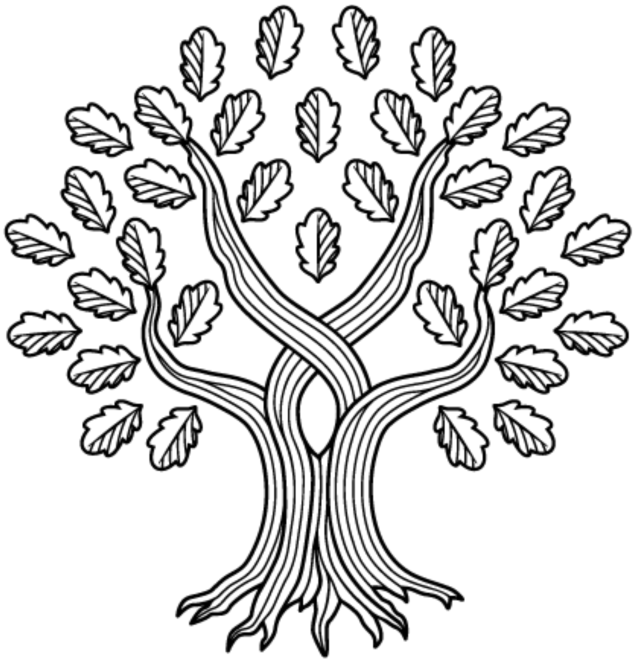
Práctica 2: ISO/IEC 27000:2018

Universidad Panamericana

Cibserseguridad

Ago 25, 2023



Osornio López Daniel Alejandro
0244685@up.edu.mx

Índice

1 Introducción

1.1 Qué es ISO/IEC

La Organización Internacional de Normalización (ISO) es una organización no gubernamental que reúne a organismos nacionales de normalización de todo el mundo. Estos organismos trabajan juntos para desarrollar normas internacionales que se apliquen a una amplia gama de productos, servicios y sistemas. [1]

Las normas ISO son voluntarias, pero se utilizan ampliamente en todo el mundo. Ayudan a garantizar que los productos y servicios sean seguros, de alta calidad y compatibles entre sí. También pueden ayudar a las empresas a ahorrar dinero y a aumentar su competitividad. [1]

La ISO colabora estrechamente con la Comisión Electrotécnica Internacional (IEC) en el desarrollo de normas electrotécnicas. [1]

1.2 ISMS

ISO/IEC JTC 1/SC 27 desarrolla normas internacionales de sistemas de gestión para la seguridad de la información, también conocidas como la familia de normas de sistemas de gestión de seguridad de la información (ISMS). [1]

Las organizaciones de todo tipo pueden aplican la familia de normas ISMS para implementae un marco (*framework*) para la gestión de la seguridad de la información.

1.3 ISO/IEC 27000:2018

El documento ISO/IEC 27000:2018 introduce la familia de normas ISMS. [1]

La familia ISMS no es más que un conjunto de estándares inter-relacionados, se dividen principalmente en aquellos que describen el vocabulario estándard, aquellos que cubren los estándares de requerimientos (27001, 27006, 270099), las guías estándares (27008, 27007, 27021, 27005, TR 27016, 27004, 27003, 27014, 27013, 27002), las guías específicas de sector (27010, 27011, 27017, 27018, 27019) y finalmente las guias específicas de control (2703x y 2704x) [1]

Los siguientes puntos de este apunte de investigación son todos estándares parte de la familia de normas de sistemas de gestión de seguridad de la información (ISMS).

2 Soporte y Control

2.1 ISO/IEC 27002

Code of practice for information security controls

ISO/IEC 27002 es una norma que proporciona un conjunto de controles de seguridad de la información que se pueden utilizar como una guía para implementar controles de seguridad de la información en los sistemas de información.

La norma no es certificable, pero las organizaciones pueden utilizarla como una referencia para implementar controles de seguridad de la información que sirvan para las necesidades de la misma.

2.2 ISO/IEC 27003

Information Security Management - Guidance

El documento ISO/IEC 27003 se puede describir sencillamente como uno que da explicaciones y funge como guía para la implementación del ISO/IEC 27001:2013, el cual, recordemos, trata sobre los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar ISMS.

2.3 ISO/IEC 27004

Monitoring, measurement, analysis and evaluation

El ISO/IEC 27004 es un documento que provee guias para que las organizaciones puedan evaluar la efectividad de los ISMS para poder satisfacer los discutido en el ISO/IEC 27001:2013. El documento se enfoca principalmente en el monitoreo y medición de la efectividad, incluyendo los procesos y controles involucrados en el ISMS y a cómo analizar e interpretar los resultados.

2.4 ISO/IEC 27005

Information Security Risk Management

El ISO/IEC 27005 da guias para evaluar y manejar el riesgo que tiene la seguridad de la información, se describe cómo realizarlo y guia en el proceso para implementarlo para satisfacer lo discutido en el ISO/IEC 27001

3 Controles por Sector

3.1 ISO/IEC 27010

Information security management for inter-sector and inter-organizational communications

El documento ISO/IEC 27010 proporciona directrices sobre cómo implementar, mantener y mejorar la seguridad de la información en las comunicaciones entre organizaciones. Las directrices se aplican a todos los tipos de intercambio y compartición de información sensible, tanto pública como privada, a nivel nacional e internacional, dentro del mismo sector o mercado o entre sectores.

3.2 ISO/IEC 27011

Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations

Muy relacionado al ISO/IEC 27010, el ISO/IEC 27011 proporciona directrices sobre cómo implementar controles de seguridad de la información en las organizaciones de telecomunicaciones.

3.3 ISO/IEC 27013

Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

El ISO/IEC 27013 brinda orientación sobre la implementación e integración de los ISMS y los sistemas de gestión de servicios (SMS). La norma puede ser utilizada por las organizaciones de todos los tamaños y sectores, tanto por organizaciones que desean implementar un ISMS o un SMS, o por las organizaciones que ya tienen un ISMS o un SMS y desean integrarlos.

3.4 ISO/IEC 27015

Information security management guidelines for financial services

El ISO/IEC TR 27015:2012 proporciona una guía de seguridad de la informacón que complementan los controles de seguridad de la información definidos en ISO/IEC 27002:2005 para iniciar, implementar, mantener y mejorar la seguridad de la información dentro de las organizaciones que brindan servicios financieros. [2]

Este documento específicamente no venía definido en el ISO/IEC 27000:2018 [1].

3.5 ISO/IEC 27017

Code of practice for information security controls based on ISO/IEC 27002 for cloud services

El ISO/IEC 27017 da guias para controles de seguridad de la información basado en el ISO/IEC 27002 para servicios en la nube, provee información adicional relevante para los controles especificados en el ISO/IEC 27002 asi como controles adicionales con guías de implementación relacionadas a los servicios en la nube.

3.6 ISO/IEC 27019

Information security controls for the energy utility industry

El ISO/IEC 27019 da orientación sobre los controles de seguridad de la información que se pueden utilizar en los sistemas de control de procesos de la industria de servicios de energía. La norma puede ser utilizada por las organizaciones de todos los tamaños y sectores de la industria de servicios de energía.

El documento incluye procesos de control centralizados y descentralizados, monitoreo y automatización y programación de sistemas, dispositivos como PLCs, teconología de comunicación,

infraestructura de medición, y demás temas relacionados a la industria de la energía, lo que hace sentido teniendo en cuenta la presencia del IEC en el comité que desarrolla la norma.

4 Auditoría y Certificación

4.1 ISO/IEC 27006

Requirements for bodies providing audit and certification of information security management systems

Es una guía para las organizaciones que brindan auditoría y certificación de ISMS. El documento establece los requisitos que deben cumplir estas organizaciones para que sus auditorías y certificaciones sean fiables y de alta calidad.

4.2 ISO/IEC 27007

Guidelines for information security management systems auditing

El ISO/IEC 27007 es una norma que proporciona orientación sobre la auditoría de los ISMS. Las organizaciones puden usar el documento para auditar sus propios ISMS, o por las auditoras externas para auditar los ISMS de otras organizaciones.

4.3 ISO/IEC 27008

Guidelines for auditors on information security controls

El ISO/IEC 27008 es un documento guia para las organizaciones que desean revisar sus controles de seguridad de la información. El documento proporciona orientación sobre cómo seleccionar los controles adecuados, cómo evaluar su cumplimiento y cómo tomar medidas correctivas cuando sea necesario.

No está enfocado a servir como guia para certificar si una organización cumple o no con las especificaciones de medición o análisis de riesgo asi como en la asesoría de ISMS.

4.4 ISO/IEC 27009

Sector-specific application of ISO/IEC27001 — Requirements

El ISO/IEC 27009 es una norma que puede ser utilizada para adaptar la ISO/IEC 27001 a un sector específico. Esto permite a las organizaciones incluir requisitos adicionales, refinar los requisitos existentes, o incluir controles o conjuntos de controles que sean específicos para su sector.

5 Economía y Gobernabilidad

5.1 ISO/IEC 27014

Governance of information security

El documento ISO/IEC 27014 brinda los principios y procesos de governanza de la seguridad de la información. Se trata de un proceso que ayuda a las organizaciones a gestionar sus riesgos de seguridad de la información. El documento proporciona orientación sobre cómo establecer un *framework* de gobernanza de la seguridad de la información, cómo implementarlo y cómo evaluar su eficacia.

5.2 ISO/IEC 27016

Information security management — Organizational economics

El ISO/IEC 27016 explica la metodología para tener una forma de evaluar los riesgos de seguridad de la información y de determinar el nivel de protección adecuado para los activos de información. La metodología puede ser utilizada por las organizaciones de todos los tamaños y sectores.

Se incluye el cómo valorar los riesgos potenciales para los activos de información, apreciar el valor que ofrecen los controles de protección de la información a estos activos, y determinar el nivel óptimo de recursos que se debe invertir para protegerlos.

6 Conclusión

El ISO/IEC 27000:2018 es un documento que explica el resto de normativas de la familia 27000 para los Sistemas gestores de la seguridad de la información (ISMS), en la familia de estándares se tocan temas sobre requisitos, guías de implementación, asesoría, governanza y estrategias de gestión para todo tipo de organizaciones que permiten tener un manejo adecuado de los *activos* de información, cosa que es siempre deseable por su importancia.

Queda claro después de ver el documento que es un esfuerzo de toda la organización necesario para proteger a los terceros que interactúan con la organización y sus servicios.

Bibliografía

[1] *Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary*, ISO/IEC JTC 1/SC 27.

[2] "SO/IEC TR 27015:2012. Information technology — security techniques — information security management guidelines for financial services," ISO/IEC JTC 1/SC 27. https://www.iso.org/standard/43755.html