Universidad Mariano Gálvez de Guatemala
Facultad de Ingeniería en sistemas
Curso: SEGURIDAD Y AUDITORÍA DE SISTEMAS
Ing. CARLOS EUGENIO GARZARO HIGUEROS

TAREA:

Norma 27000 y sus diferentes series

CARLOS DANIEL LÓPEZ HERNÁNDEZ
Carné: 5190-19-5203
Guatemala 17/08/2024

Contenido

Introducción

La Norma ISO/IEC 27000 es parte de una familia más amplia de estándares, conocida como la serie ISO/IEC 27000, que está diseñada para ayudar a las organizaciones a mantener la confidencialidad, integridad y disponibilidad de la información. Este conjunto de normas es desarrollado por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), y se centra en establecer, implementar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI).

Importancia de la Norma ISO/IEC 27000

La Norma ISO/IEC 27000 sirve como punto de partida para las organizaciones que buscan alinear sus prácticas de seguridad de la información con estándares internacionales reconocidos. Esta norma proporciona una terminología y una descripción general de los conceptos fundamentales de la serie ISO/IEC 27000, lo que facilita la comprensión y aplicación de las normas específicas que la componen.

Uno de los principales beneficios de adoptar la Norma ISO/IEC 27000 es que permite a las organizaciones demostrar su compromiso con la seguridad de la información, lo cual es crucial para generar confianza entre clientes, socios y partes interesadas. Además, proporciona una base para la evaluación de riesgos y la implementación de controles que se adaptan a las necesidades específicas de la organización, lo que contribuye a una gestión proactiva de la seguridad.

Resumen de NORMA 27000

En esta sección se detallan las distintas normas que conforman la serie ISO 27000 y se explica cómo una organización puede implementar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la ISO 27001, integrándolo con otras normas de la serie 27k, así como con otros sistemas de gestión.

Es importante destacar que los textos completos de estas normas no están disponibles de forma gratuita, ya que están protegidos por derechos de propiedad intelectual y deben ser adquiridos oficialmente.

Los documentos originales, que siempre se publican en inglés, pueden adquirirse en línea a través de la tienda virtual de la organización, donde es posible revisar la estructura del contenido y algunas páginas antes de realizar la compra.

En cuanto a las versiones en español, estas son elaboradas a partir de la traducción del original por las entidades nacionales responsables en cada país. Esto puede dar lugar a que las publicaciones traducidas estén disponibles en diferentes momentos, dependiendo del país, y que existan múltiples versiones en español del estándar, una por cada entidad nacional encargada. Además, algunas guías de la serie pueden no estar disponibles en español, según los criterios y recursos de cada entidad de normalización.

ISO/IEC 27000

Esta norma, publicada por primera vez el 1 de mayo de 2009, ha pasado por varias revisiones: una segunda edición el 1 de diciembre de 2012, una tercera el 14 de enero de 2014, y una cuarta en febrero de 2016. Proporciona una visión general de las normas que forman parte de la serie 27000, destacando el propósito y el alcance de cada una. Incluye todas las definiciones pertinentes a la serie y explica la importancia de implementar un Sistema de Gestión de Seguridad de la Información (SGSI). Además, ofrece una introducción a los SGSI y una descripción de los pasos clave para establecer, monitorizar, mantener y mejorar estos sistemas. Es importante notar que, en la última edición, se ha omitido el ciclo Plan-Do-Check-Act para evitar que se considere el único marco de referencia para la mejora continua. Aunque hay versiones traducidas al español, es fundamental verificar la versión que se descarga. El original en inglés y su traducción al francés en su edición de 2018 están disponibles para su descarga gratuita.

ISO / IEC 27001

Publicada el 15 de octubre de 2005, revisada el 25 de septiembre de 2013 y actualizada el 25 de octubre de 2022, esta norma es la principal de la serie y contiene los requisitos para el sistema de gestión de seguridad de la información (SGSI). Su origen se remonta a la norma BS 7799-2:2002, que ya ha sido anulada, y es la base para la certificación de los SGSIs por auditores externos. El Anexo A resume los objetivos de control y controles de la ISO 27002, los cuales las organizaciones pueden seleccionar para desarrollar su SGSI; aunque no es obligatorio implementar todos los controles, la organización debe justificar la no aplicabilidad de aquellos que no implementa.

Desde el 12 de noviembre de 2014, esta norma se publicó en España como UNE-ISO/IEC 27001:2014. También está disponible en otros países de habla hispana, como Colombia, Chile y Uruguay, con sus respectivas denominaciones. El original en inglés y la traducción al francés pueden adquirirse en iso.org.

ISO /IEC 27002

Publicada el 1 de julio de 2007, esta norma renombró la ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe objetivos de control y controles recomendados en materia de seguridad de la información, aunque no es certificable. Contiene 39 objetivos de control y 133 controles, organizados en 11 dominios. La ISO 27001 incluye un anexo que resume los controles de la ISO 27002:2005. Publicada en España como UNE-ISO/IEC 27002:2009 el 9 de diciembre de 2009, también está disponible en español en otros países como Colombia, Venezuela, Argentina, Chile y Uruguay. La última actualización, del 15 de febrero de 2022, consta de 93 controles divididos en cuatro categorías: organización 37, personas 8, instalaciones físicas 14 y tecnología 34. Esta versión permite que cada organización desarrolle atributos específicos para los controles de seguridad, facilitando la integración de ISO 27001 con otros marcos de gestión y la adaptación de los controles a sectores específicos.

ISO / IEC 27003

Publicada el 1 de febrero de 2010 y actualizada el 12 de abril de 2017, esta guía no es certificable. Se centra en los aspectos críticos necesarios para el diseño e implementación exitosa de un Sistema de Gestión de Seguridad de la Información (SGSI) de acuerdo con la norma ISO/IEC 27001. Describe el proceso de especificación y diseño, desde la concepción hasta la implementación, así como la obtención de aprobación por parte de la dirección para llevar a cabo un SGSI. Tiene su origen en el anexo B de la norma BS 7799-2 y en una serie de documentos publicados por BSI con recomendaciones y guías de implementación.

ISO / IEC 27004

Publicada el 15 de diciembre de 2009 y revisada en diciembre de 2016, esta guía no es certificable. Se enfoca en el desarrollo y uso de métricas y técnicas de medición para evaluar la eficacia de un Sistema de Gestión de Seguridad de la Información (SGSI) y los controles implementados según la norma ISO/IEC 27001. La guía proporciona un marco para establecer indicadores clave de rendimiento (KPIs) que permiten a las organizaciones medir el desempeño de sus controles de seguridad, identificar áreas de mejora y asegurar que el SGSI cumpla con sus objetivos. Además, incluye recomendaciones sobre cómo interpretar los resultados obtenidos y ajustar las estrategias de seguridad en consecuencia para mantener la efectividad del SGSI a lo largo del tiempo.

ISO/IEC 27005

La cuarta edición, publicada en octubre de 2022, alinea la norma con la ISO 31000:2018, introduciendo un enfoque basado en eventos para la gestión de riesgos en seguridad de la información, en contraste con el enfoque clásico basado en activos. No es certificable y proporciona directrices para gestionar riesgos según ISO/IEC 27001.

ISO/IEC 27006:

Especifica requisitos para la acreditación de entidades que auditan y certifican sistemas de gestión de seguridad de la información (SGSI) según ISO 27001. Publicada inicialmente en 2007, con revisiones posteriores en 2011 y 2015, no es una norma de acreditación por sí misma, pero añade requisitos específicos a ISO/IEC 17021.

ISO/IEC TS 27006-2:2021

Publicada en junio de 2021, especifica requisitos y brinda orientación para organismos que certifican sistemas de gestión de información de privacidad (PIMS) según ISO/IEC 27701, en conjunto con ISO/IEC 27001 y ISO/IEC 27006. Es crucial para la acreditación de estos organismos.

ISO/IEC 27007

Esta guía de auditoría para SGSI, complementaria a la ISO 19011, fue publicada en noviembre de 2011, con revisiones en 2017 y 2020. No es certificable.

ISO/IEC TS 27008

Publicada como una especificación técnica en 2019 (sustituyendo a un informe técnico de 2011), esta guía no certificable ofrece orientación para la auditoría de controles seleccionados dentro de un SGSI.

ISO/IEC 27009

Publicada en 2016 y revisada en 2020, esta norma no certificable define requisitos para aplicar ISO/IEC 27001 en sectores específicos, permitiendo la personalización de controles y requisitos según las necesidades del sector.

ISO/IEC 27010

Publicada en 2012 y revisada en 2015, es una guía para la gestión de la seguridad de la información compartida entre organizaciones o sectores, aplicable a intercambios sensibles en sectores críticos. Actualmente está en proceso de revisión.

ISO/IEC 27011

Publicada en 2008 y revisada en 2016, esta norma es una guía de implementación de seguridad de la información en el sector de telecomunicaciones, basada en ISO/IEC 27002 y también conocida como ITU-T X.1051.

ISO/IEC 27013

Publicada en 2012 y revisada en 2015 y 2021, es una guía para la implementación integrada de ISO/IEC 27001 (gestión de seguridad de la información) e ISO/IEC 20000-1 (gestión de servicios TI).

ISO/IEC 27014

Esta guía de gobierno corporativo para la seguridad de la información, ciberseguridad y privacidad, fue publicada en 2013 y actualizada en 2020.

ISO/IEC TR 27015

Publicada en 2012, esta guía, que no será actualizada, está orientada al sector financiero y de seguros para la implementación de SGSI, complementando la ISO/IEC 27002:2005.

ISO/IEC TR 27016

Publicada en 2014, es una guía que aborda los aspectos financieros de la seguridad de la información.

ISO/IEC 27017

Publicada en 2015, esta norma es una guía de seguridad para Cloud Computing, alineada con ISO/IEC 27002 y con controles específicos para entornos de nube. Es posible certificarla junto con un SGSI basado en ISO/IEC 27001.

ISO/IEC 27018

Publicada en 2014 y revisada en 2019, es un código de buenas prácticas para la protección de datos en servicios de Cloud Computing, con posibilidad de certificación junto con un SGSI según ISO/IEC 27001.

ISO/IEC TR 27019

Publicada en 2013 y actualizada en 2017, es una guía para la industria de la energía, alineada con ISO/IEC 27002:2013, que abarca la seguridad de sistemas de control de procesos específicos del sector.

ISO/IEC 27021

Publicada en 2017, esta norma específica los requisitos de competencia para profesionales que lideran o participan en la implementación y mantenimiento de procesos de SGSI según ISO/IEC 27001.

ISO/IEC 27022

Publicada en 2021, define un modelo de referencia de procesos para la gestión de seguridad de la información, guiando a los usuarios de ISO/IEC 27001 en la incorporación de un enfoque basado en procesos.

ISO/IEC TR 27023

Publicada en 2015, esta guía no certificable ofrece correspondencias entre las versiones 2013 de las normas ISO/IEC 27001 y ISO/IEC 27002, facilitando la transición desde las versiones de 2005.

ISO/IEC TR 27024

En desarrollo, este documento enumera leyes y reglamentos relevantes de diferentes países o regiones en materia de seguridad de la información.

ISO/IEC 27028

En desarrollo, servirá como guía para el desarrollo y aplicación de atributos en los controles indicados en ISO/IEC 27002:2022.

ISO/IEC 27029

En desarrollo, cubrirá la relación de la norma ISO/IEC 27002 con otros estándares ISO e IEC.

ISO/IEC 27031

Publicada en 2011, es una guía no certificable que apoya la adecuación de las tecnologías de información y comunicación (TIC) para la continuidad del negocio.

ISO/IEC 27032

Publicada en 2012, proporciona orientación para la mejora de la ciberseguridad, abordando la seguridad de la información, redes, internet e infraestructuras críticas, estableciendo un marco para la colaboración en la solución de problemas de ciberseguridad.

ISO/IEC 27033

Norma dedicada a la seguridad en redes, consiste en 6 partes publicadas entre 2009 y 2016, abordando conceptos generales, directrices de diseño, escenarios de referencia, seguridad en gateways, VPNs y redes IP wireless.

ISO/IEC 27034

Norma en 7 partes, publicada entre 2011 y 2018, dedicada a la seguridad en aplicaciones informáticas, abordando desde conceptos generales hasta la seguridad para aplicaciones de uso específico.

ISO/IEC 27035

Publicada en 2011, esta norma en 3 partes aborda la gestión de incidentes de seguridad de la información, con guías para la elaboración de planes de respuesta y operaciones en la respuesta a incidentes.

ISO/IEC 27036

Guía en 4 partes publicada entre 2014 y 2023, aborda la seguridad en las relaciones con proveedores, cubriendo conceptos generales, requisitos comunes, seguridad en la cadena de suministro TIC y entornos de servicios Cloud.

ISO/IEC 27037

Publicada en 2012, proporciona directrices para la identificación, recopilación, consolidación y preservación de evidencias digitales en dispositivos electrónicos.

ISO/IEC 27038

Publicada en 2014, es una guía de especificación para la seguridad en la redacción digital.

ISO/IEC 27039

Publicada en 2015, ofrece una guía para la selección, despliegue y operación de sistemas de detección y prevención de intrusión (IDS/IPS).

ISO/IEC 27040

Publicada en 2015, esta guía se centra en la seguridad en medios de almacenamiento.

ISO/IEC 27041

Publicada en 2015, es una guía para garantizar la idoneidad y adecuación de los métodos de investigación en seguridad de la información.

ISO/IEC 27042

Publicada en 2015, ofrece directrices para el análisis e interpretación de evidencias digitales.

ISO/IEC 27043

Publicada en 2015, desarrolla principios y procesos de investigación para la recopilación de evidencias digitales.

ISO/IEC 27045-46

En desarrollo desde 2018, estas normas cubrirán procesos de seguridad y privacidad en sistemas de big data.

ISO/IEC 27050

Norma en 4 partes, desarrollada entre 2016 y 2021, aborda la gestión de información almacenada en dispositivos electrónicos, desde su identificación hasta la producción de ESI (información electrónicamente almacenada) en procesos legales.

Conclusión

La familia de normas ISO/IEC 27000 se erige como un marco integral y robusto para la gestión de la seguridad de la información. Estas normas proporcionan una guía esencial para las organizaciones que buscan proteger sus activos de información de amenazas cada vez más sofisticadas y variadas, a la vez que aseguran la confidencialidad, integridad y disponibilidad de los datos. A lo largo de su evolución, la serie ISO/IEC 27000 ha respondido a la creciente complejidad del entorno tecnológico y de amenazas, ofreciendo enfoques específicos y adaptables para diferentes industrias y escenarios.

Además del núcleo de la serie, existen numerosas normas adicionales que amplían y complementan las directrices establecidas por ISO/IEC 27001 y 27002. Por ejemplo, ISO/IEC 27005 se enfoca en la gestión de riesgos de la seguridad de la información, proporcionando un marco para identificar, evaluar y tratar riesgos de manera efectiva. Otras normas, como ISO/IEC 27017 y 27018, abordan desafíos específicos, como la seguridad en la computación en la nube y la protección de datos personales en estos entornos, ofreciendo controles adicionales y específicos para mitigar riesgos asociados a estos entornos modernos.

Auditoría, Certificación y Cumplimiento

La serie también incluye normas como ISO/IEC 27006 y 27007, que proporcionan directrices para la acreditación de organismos de certificación y la auditoría de un SGSI, respectivamente. Estas normas aseguran que los procesos de certificación y auditoría sean consistentes y fiables, fortaleciendo la confianza en la validez de las certificaciones otorgadas bajo ISO/IEC 27001. Esto es crucial en un entorno donde la confianza en los sistemas de información es fundamental para las operaciones comerciales y la reputación organizacional.

Bibliografías

ISOS 27000 SITIO WEB DE TODAS LAS ISOS

https://www.iso27000.es/iso27000.html

ISO - International Organization for Standardization

Título: ISO/IEC 27000 Information security management

URL: https://www.iso.org/isoiec-27001-information-security.html

Descripción: Sitio oficial de ISO que proporciona información sobre la serie ISO/IEC 27000, incluyendo las normas y guías para la gestión de la seguridad de la información.

BSI Group

Título: Information Security Management System (ISMS) Standards

URL: https://www.bsigroup.com/en-GB/standards/iso-iec-27001-information-security/

Descripción: Ofrece una visión general de las normas ISO/IEC 27000, con detalles sobre la implementación y certificación del Sistema de Gestión de Seguridad de la Información.

International Electrotechnical Commission (IEC)

Título: ISO/IEC 27001 Information Security Management Systems

URL: https://www.iec.ch/standards-dev/resources/publications/isoiec-27001

Descripción: Proporciona información sobre la norma ISO/IEC 27001 y su relación con otras normas en la serie ISO/IEC 27000.

NIST - National Institute of Standards and Technology

Título: Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations

URL: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Descripción: Aunque no es específicamente sobre ISO/IEC 27000, este documento del NIST está alineado con las normas ISO/IEC 27001 y puede proporcionar contexto adicional sobre controles de seguridad.