SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI)

nqa.

NEVER STOP IMPROVING

LA FAMILIA DE NORMAS DE SGSI

LA FAMILIA DE NORMAS DE SGSI

01. Información general
02. Normas que describen una visión general y la terminología
03. Normas que especifican los requisitos
04. Normas que describen guías o directrices generales
05. Normas que describen guías específicas o sectoriales

Información general

La familia de normas SGSI consiste en una serie de normas relacionadas entre sí, ya publicadas o en preparación, y que contiene una serie de importantes componentes estructurales.

Estos componentes se centran en normas para describir las **especificaciones de un SGSI (ISO/IEC 27001)**, los **requisitos para los organismos de certificación (ISO/IEC 27006)** que certifiquen el cumplimiento con la Norma ISO/IEC 27001, y un **marco de requisitos adicionales para implementaciones sectoriales específicas del SGSI (ISO/IEC 27009).**

Otras normas ofrecen guías para los diversos aspectos de la implementación de un SGSI, directrices para abordar un proceso genérico, así como directrices sectoriales específicas.

Información general

Cada grupo de normas de la familia de SGSI se describe indicando su tipo (o rol) dentro de la familia de SGSI y su número de referencia.

Los apartados a los que esto aplica son:

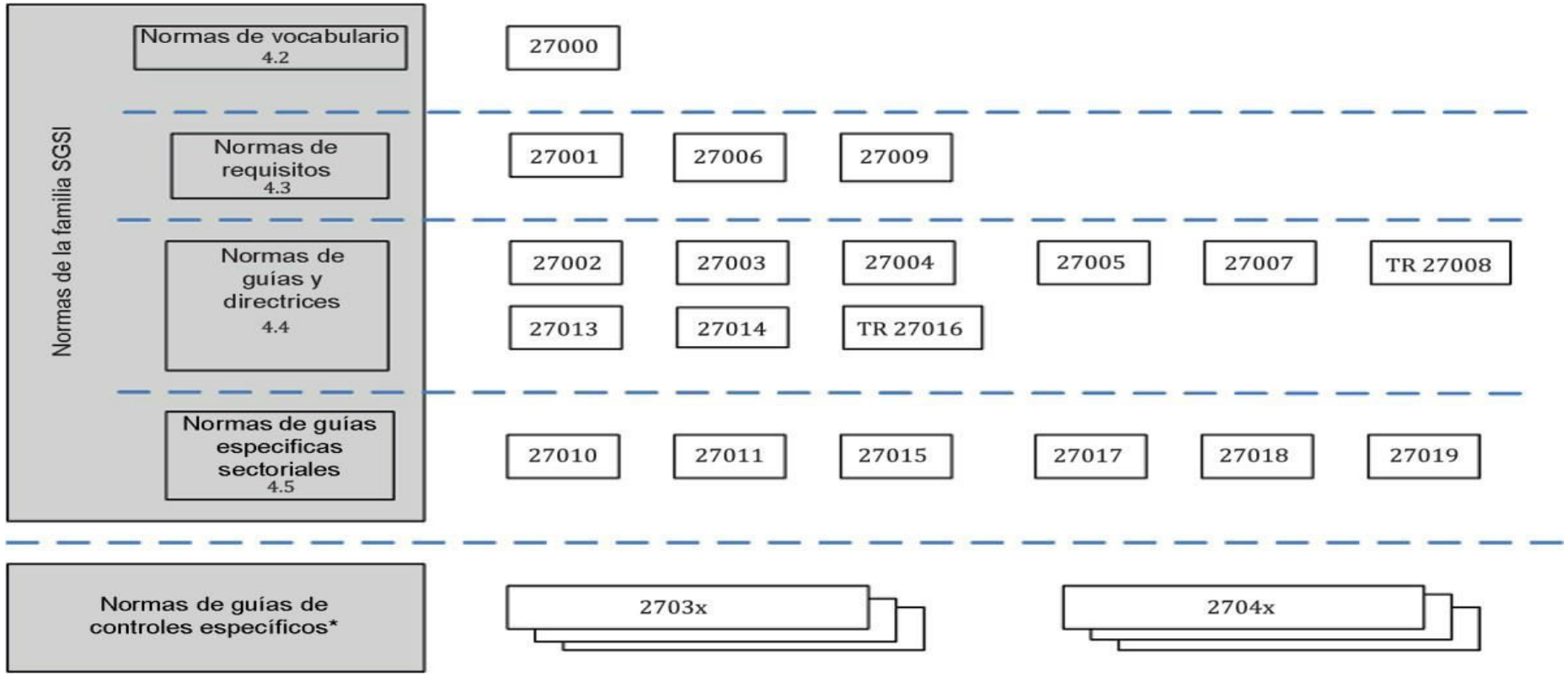
a) normas que describen una visión general y la terminología;

b) normas que especifican los requisitos;

c) las normas que describen guías o directrices generales ; o

d) normas que describen guías o directrices específicas sectoriales.

Relaciones entre las normas de la familia SGSI



nqa.
NEVER STOP IMPROVING

* fuera del campo de aplicación de esta norma internacional

LA FAMILIA DE NORMAS DE SGSI

01. Información general
02. Normas que describen una visión general y la terminología
03. Normas que especifican los requisitos
04. Normas que describen guías o directrices generales
05. Normas que describen guías específicas o sectoriales

Normas que describen una visión general y la terminología

ISO/IEC 27000

Tecnologías de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Visión de conjunto y vocabulario.

Ámbito de aplicación: Esta norma internacional proporciona a organizaciones y personas:

a) una visión general de la familia de las normas SGSI;

b) una introducción a los sistemas de gestión de la seguridad de la información; y

c) los términos y las definiciones utilizadas en toda la familia de las normas de SGSI.

Objeto: Esta norma internacional describe los fundamentos de los sistemas de gestión de la seguridad de la información, que constituyen el objeto de la familia de las normas de SGSI, y define los términos relacionados.

LA FAMILIA DE NORMAS DE SGSI

01. Información general
02. Normas que describen una visión general y la terminología
03. Normas que especifican los requisitos
04. Normas que describen guías o directrices generales
05. Normas que describen guías específicas o sectoriales

Normas que describen una visión general y la terminología

ISO/IEC 27001

Tecnologías de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.

Ámbito de aplicación: Esta norma internacional especifica los requisitos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar el Sistema de Gestión de la Seguridad de la Información (SGSI) en el marco de los riesgos de negocio generales de la organización. Establece requisitos para la aplicación de los controles de seguridad adaptados a las necesidades de las organizaciones individuales o partes de la misma. Esta norma internacional es universal para todo tipo de organizaciones.

Objeto: La Norma ISO/IEC 27001 establece los requisitos normativos para el desarrollo y operación de un SGSI, incluyendo un conjunto de controles para el control y mitigación de los riesgos asociados con los activos de información que la organización trata de proteger mediante la operación de su SGSI. Las organizaciones que implementan un SGSI pueden hacer que se audite y certifique su conformidad. Los objetivos de control y controles del anexo A de la Norma ISO/IEC 27001 deben ser seleccionados en función de las necesidades, durante el proceso del SGSI para satisfacer los requisitos identificados. Los objetivos de control y controles que se enumeran en la tabla A.1 de la Norma ISO/IEC 27001 proceden directamente y están alineados con los que se enumeran en los capítulos 5 a 15 de la Norma ISO/IEC 27002.

Normas que describen una visión general y la terminología

ISO/IEC 27006

Tecnologías de la información. Técnicas de seguridad. Requisitos para entidades que auditan y certifican Sistemas de Gestión de la Seguridad de la Información (SGSI).

Ámbito de aplicación: Esta norma internacional especifica los requisitos y proporciona las directrices que han de cumplir las entidades que auditan y certifican un SGSI según la Norma ISO/IEC 27001, además de los requisitos contenidos en la Norma ISO/IEC 17021. Su intención principal es servir de apoyo para la acreditación de organismos de certificación que proporcionan servicios de certificación de SGSI según la Norma ISO/IEC 27001.

Objeto: La Norma ISO/IEC 27006 complementa a la Norma ISO/IEC 17021 al ofrecer los requisitos para que las organizaciones de certificación sean acreditadas de manera que éstas provean certificaciones de conformidad consistentes frente a los requisitos especificados en la Norma ISO/IEC 27001.

Normas que describen una visión general y la terminología

ISO/IEC 27009

Tecnología de la información - Técnicas de seguridad - Aplicación sectorial de la norma ISO/IEC 27001 – Requisitos

Ámbito de aplicación: Este documento define los requisitos para el uso de ISO/IEC 27001 en cualquier sector específico (campo, área de aplicación o sector de mercado). Explica cómo incluir requisitos adicionales a los de la norma ISO/IEC 27001, cómo perfeccionar cualquiera de los requisitos de la norma ISO/IEC 27001 y cómo incluir controles o conjuntos de controles además de la norma ISO/IEC 27001:2013, Anexo A.

Objeto: ISO/IEC 27009 garantiza que los requisitos adicionales o matizados no entren en conflicto con los requisitos de ISO/IEC 27001.

LA FAMILIA DE NORMAS DE SGSI

01. Información general
02. Normas que describen una visión general y la terminología
03. Normas que especifican los requisitos
04. Normas que describen guías o directrices generales
05. Normas que describen guías específicas o sectoriales

Normas que describen guías o directrices generales

- ✓ ISO/IEC 27002
- ✓ ISO/IEC 27003
- ✓ ISO/IEC 27004
- ✓ ISO/IEC 27005
- ✓ ISO/IEC 27007
- ✓ ISO/IEC TS 27008
- ✓ ISO/IEC 27013
- ✓ ISO/IEC 27014
- ✓ ISO/IEC TR 27016

Normas que describen guías o directrices generales

ISO/IEC 27002

Tecnologías de la información. Técnicas de seguridad. Código de práctica para los controles de seguridad de la información.

Ámbito de aplicación: Esta norma internacional proporciona una lista de objetivos de control comúnmente aceptados así como las mejores prácticas en controles de seguridad que deben utilizarse como guía de aplicación para su selección e implementación para lograr la seguridad de la información.

Objeto: La Norma ISO/IEC 27002 proporciona directrices para la implementación de los controles de seguridad de la información. En concreto, los capítulos 5 a 18 proporcionan asesoramiento y orientación específicos para la puesta en marcha de las mejores prácticas en la implementación de los controles especificados en los capítulos A.5 a A.18 del anexo A de la Norma ISO/IEC 27001.

Normas que describen guías o directrices generales

ISO/IEC 27003

Tecnología de la información. Técnicas de seguridad. Guía para la implementación de los Sistemas de Gestión de la Seguridad de la Información (SGSI).

Ámbito de aplicación: Esta norma internacional proporciona orientación para la implementación práctica e información adicional para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un SGSI según la Norma ISO/IEC 27001.

Objeto: La Norma ISO/IEC 27003 proporciona un enfoque basado en procesos orientado a la implementación con éxito del SGSI según la Norma ISO/IEC 27001.

Normas que describen guías o directrices generales

ISO/IEC 27004

Tecnología de la información. Técnicas de seguridad. Gestión de Seguridad de la Información. Métricas.

Ámbito de aplicación: Esta norma internacional proporciona orientación y asesoramiento sobre el desarrollo y uso de las métricas con el fin de evaluar la eficacia del SGSI, de los objetivos de los controles y controles usados para aplicar y administrar la seguridad de la información, tal como se especifica en la Norma ISO/IEC 27001.

Objeto: La Norma ISO/IEC 27004 proporciona un marco de métricas que permite una evaluación de la eficacia del SGSI de acuerdo con la Norma ISO/IEC 27001.

Normas que describen guías o directrices generales

ISO/IEC 27005

Tecnologías de la información. Técnicas de seguridad. Gestión de riesgos de seguridad de la información.

Ámbito de aplicación: Esta norma internacional proporciona directrices para la gestión de riesgos de seguridad de la información. El enfoque descrito en esta norma internacional apoya los conceptos generales que se especifican en la Norma ISO/IEC 27001.

Objeto: La Norma ISO/IEC 27005 proporciona directrices sobre la aplicación de un enfoque de gestión de riesgos orientado a procesos para ayudar en la aplicación de manera satisfactoria y al cumplimiento de los requisitos de gestión de riesgos de seguridad de la Norma ISO/IEC 27001.

Normas que describen guías o directrices generales

ISO/IEC 27007

Tecnologías de la información. Técnicas de seguridad. Guía para la auditoría de los Sistemas de Gestión de la Seguridad de la Información (SGSI).

Ámbito de aplicación: Esta norma internacional ofrece orientación sobre la realización de auditorías de SGSI, así como sobre la competencia de los auditores del sistema de gestión de la seguridad de la información, además de las directrices contenidas en la Norma ISO 19011, que es aplicable a los sistemas de gestión en general.

Objeto: La Norma ISO/IEC 27007 proporciona directrices a las organizaciones que tienen que realizar auditorías internas o externas de un SGSI así como directrices para gestionar un programa de auditoría de SGSI según los requisitos especificados en la Norma ISO/IEC 27001.

Normas que describen guías o directrices generales

ISO/IEC TS 27008

Tecnologías de la información. Técnicas de seguridad. Guía para los auditores de controles de seguridad de la información.

Ámbito de aplicación: Este informe técnico proporciona directrices sobre la revisión de la implementación y operación de controles incluyendo la comprobación de la conformidad técnica de los controles del sistema de información, y de la conformidad con las normas de seguridad de la información establecidas en una organización.

Objeto: Este informe técnico proporciona un enfoque de los controles de seguridad de la información, incluyendo la conformidad técnica con la implementación de la norma de seguridad de la información que se haya establecido en la organización. Este informe no pretende ser una guía específica de la conformidad respecto a mediciones, apreciación del riesgo o auditoría del SGSI como se especifica respectivamente en las Normas ISO/IEC 27004, ISO/IEC 27005 o ISO/IEC 27007. Tampoco está dirigido a la auditoría de los sistemas de gestión.

Normas que describen guías o directrices generales

ISO/IEC 27013

Tecnologías de la información. Técnicas de seguridad. Guía para la implementación integrada de ISO/IEC 27001 e ISO/IEC 20000-1.

Ámbito de aplicación: Esta norma internacional proporcionará directrices para la implementación integrada de las Normas ISO/IEC 27001 e ISO/IEC 20000-1 para las organizaciones que tengan intención de:

a) implementar la Norma ISO/IEC 27001 cuando ya tienen implementada la Norma ISO/IEC 20000-1, o viceversa;

b) implementar conjuntamente las Normas ISO/IEC 27001 e ISO/IEC 20000-1;

c) integrar las implementaciones existentes de los sistemas de gestión de ISO/IEC 27001 e ISO/IEC 20000-1.

Esta norma Internacional se enfoca exclusivamente en la implementación integrada de un sistema de gestión de la seguridad de la información (SGSI) según se especifica en la Norma ISO/IEC 27001 y un sistema de gestión de servicios (SGS) según se especifica en la Norma ISO/IEC 20000-1.

Objeto: Proporcionar a las organizaciones un mejor entendimiento de las características, similitudes y diferencias entre las Normas ISO/IEC 27001 e ISO/IEC 20000-1 para ayudar en la planificación de un sistema integrado de gestión conforme a ambas normas internacionales.

Normas que describen guías o directrices generales

ISO/IEC 27014

Tecnologías de la información. Técnicas de seguridad. Gobernanza de la seguridad de la información.

Ámbito de aplicación: Esta norma internacional proporcionará directrices sobre los principios y procesos para el gobierno de la seguridad de la información, mediante las cuales las organizaciones pueden evaluar, dirigir y controlar la gestión de la seguridad de la información.

Objeto: La seguridad de la información se ha convertido en un asunto clave para las organizaciones. No solo han aumentado los requisitos regulatorios, sino que el fallo de las medidas de seguridad en las organizaciones puede tener un impacto directo en la reputación de una organización. Por ello, se requiere a los órganos de gobierno, como parte de sus responsabilidades de gobierno, el tener una cada vez mayor vigilancia de la seguridad de la información para asegurar que se consiguen los objetivos de la organización.

Normas que describen guías o directrices generales

ISO/IEC TR 27016

Tecnologías de la información. Técnicas de seguridad. Gestión de seguridad de la información. Economía organizacional.

Ámbito de aplicación: Este informe técnico proporcionará una metodología que permita a las organizaciones un mejor entendimiento desde un punto de vista económico, de cómo valorar de manera precisa los activos de información identificados, valorar los riegos potenciales para dichos activos, apreciar el valor que los controles de protección de la información proporcionan a dicho activos y determinar el nivel óptimo de recursos a aplicar para proporcionar seguridad a los activos de información.

Objeto: Este informe técnico complementará la familia de normas de SGSI, proporcionando un punto de vista económico a la protección de los activos de información de una organización en el contexto del entorno social en el que opera la organización y proporcionando directrices de cómo aplicar criterios de economía organizacional a la seguridad de la información a través del uso de modelos y ejemplos.

LA FAMILIA DE NORMAS DE SGSI

01. Información general
02. Normas que describen una visión general y la terminología
03. Normas que especifican los requisitos
04. Normas que describen guías o directrices generales
05. Normas que describen guías específicas o sectoriales

Normas que describen guías específicas o sectoriales

- ✓ ISO/IEC 27010
- ✓ ISO/IEC 27011
- ✓ ISO/IEC TR 27015
- ✓ ISO/IEC 27018
- ✓ ISO/IEC 27799

Normas que describen guías o directrices generales

ISO/IEC 27010

Tecnologías de la información. Técnicas de seguridad. Gestión de seguridad de la información en comunicaciones intersectoriales e interorganizacionales.

Ámbito de aplicación: Esta norma internacional proporciona directrices adicionales a las dadas en la familia de normas ISO/IEC 27000 para la implementación de la gestión de la seguridad en entornos donde diferentes comunidades comparten información, y proporciona controles y directrices específicos relativos al comienzo, implementación, mantenimiento y mejora de la seguridad de la información para las comunicaciones inter sectoriales e inter organizacionales.

Objeto: Esta norma internacional se aplica a todo tipo de intercambio o compartición de información sensible, ya sea de ámbito público o privado, a nivel nacional o internacional, dentro del mismo sector industrial o de mercado, o entre diferentes sectores. En particular, es aplicable a los intercambios y compartición de información relativa a la provisión, mantenimiento y protección de una infraestructura crítica de un estado o de una organización.

Normas que describen guías o directrices generales

ISO/IEC 27011

Tecnologías de la información. Técnicas de seguridad. Guía para la gestión de seguridad de la información para las organizaciones de telecomunicaciones basada en la Norma ISO/IEC 27002.

Ámbito de aplicación: Esta norma internacional proporciona directrices de apoyo a la aplicación de los controles de Seguridad de la Información en las organizaciones de telecomunicaciones.

Objeto: la Norma ISO/IEC 27011 permite a las organizaciones de telecomunicaciones el cumplimiento de los requisitos básicos de gestión de seguridad de la información de confidencialidad, integridad, disponibilidad y cualquier otra propiedad de seguridad relevante.

Normas que describen guías o directrices generales

ISO/IEC TR 27015

Tecnologías de la información. Técnicas de seguridad. Guía para la gestión de seguridad de la información para servicios financieros.

Ámbito de aplicación: Este informe técnico proporciona directrices adicionales a las dadas en la familia de Normas ISO/IEC 27000, para el inicio, implementación, mantenimiento y mejora de la seguridad de la información en organizaciones que proveen servicios financieros.

Objeto: Este informe técnico es un suplemento especializado de las Normas ISO/IEC 27001 e ISO/IEC 27002 para su uso en organizaciones que prestan servicios financieros, con objeto de servir de apoyo a:

a) el inicio, implementación, mantenimiento, y mejora de un sistema de gestión de la seguridad de la información basado en la Norma ISO/IEC 27001;

b) el diseño e implementación de los controles definidos en la Norma ISO/IEC 27002 o en este informe técnico.

Normas que describen guías o directrices generales

ISO/IEC 27017

Tecnologías de la información. Técnicas de seguridad. Código de práctica para los controles de seguridad de la información basado en la Norma ISO/IEC 27002 para servicios en la nube (cloud services).

Ámbito de aplicación: la Norma ISO/IEC 27017 proporciona directrices para los controles de seguridad de la información aplicables a la prestación y utilización de servicios en la nube, proporcionando:

a) guía de implementación adicional para los controles relevantes especificados en ISO/IEC 27002;

b) controles adicionales con guías de implementación que se relacionan específicamente con los servicios en la nube.

Objeto: Esta Norma Internacional proporciona controles y guía de implementación tanto para los proveedores de servicios en la nube como para los clientes de servicios en la nube.

Normas que describen guías o directrices generales

ISO/IEC 27018

Tecnologías de la información. Técnicas de seguridad. Código de práctica para la protección de información de identificación personal (PII) en nubes públicas que actúan como procesadores de PII.

Ámbito de aplicación: La Norma ISO/IEC 27018 establece objetivos de control, controles y directrices comúnmente aceptados para implementar medidas para proteger la información de identificación personal (PII) de acuerdo con los principios de privacidad de la Norma ISO/IEC 29100 para el entorno de computación en nube pública (cloud computing).

Objeto: Esta norma internacional es aplicable a organizaciones, incluidas empresas públicas y privadas, entidades gubernamentales y organizaciones sin fines de lucro, que proporcionan servicios de procesamiento de información como procesadores de PII a través de computación en la nube (cloud computing) bajo contrato con otras organizaciones. Las directrices de esta Norma Internacional también pueden ser relevantes para las organizaciones que actúan como controladores de PII; sin embargo, los controladores de PII pueden estar sujetos a legislaciones, regulaciones y obligaciones adicionales de protección de PII, que no se aplican a los procesadores de PII, y estos no están cubiertos en esta Norma Internacional.

Cierre del contenido

NEVER STOP IMPROVING