Quito – Ecuador

NORMA
TÉCNICA
ECUATORIANA

NTE INEN-ISO/IEC 27000

Cuarta edición

TECNOLOGÍAS DE LA INFORMACIÓN — TÉCNICAS DE SEGURIDAD — SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – DESCRIPCIÓN GENERAL Y VOCABULARIO. (ISO/IEC 27000:2016, IDT)

INFORMATION TECHNOLOGY — SECURITY TECHNIQUES — INFORMATION SECURITY MANAGEMENT SYSTEMS — OVERVIEW AND VOCABULARY (ISO/IEC 27000:2016)

Correspondencia:

Esta Norma Técnica Ecuatoriana es una traducción idéntica de la Norma Internacional ISO/IEC 27000:2016.

ICS: 01.040.35;35.040

38
Páginas

Prólogo nacional

Esta Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27000, es una traducción idéntica de la Norma Internacional ISO/IEC 27000:2016, *Information technology — Security techniques — Information security management systems — Overview and vocabulary (ISO/IEC 27000:2016).* El Servicio Ecuatoriano de Normalización, INEN, es el responsable de la traducción de esta Norma Técnica Ecuatoriana, y de su adopción es el Comité Técnico de Normalización del INEN, "Tecnologías de la información".

Para el propósito de esta Norma Técnica Ecuatoriana se han hecho los siguientes cambios editoriales:

a) Las palabras "esta Norma Internacional" han sido reemplazadas por "esta norma nacional".

Índice página

Prólogo

ISO (Organización Internacional de Normalización) e IEC (la Comisión Electrotécnica Internacional) constituyen el sistema especializado para la normalización a nivel mundial. Los organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de normas internacionales a través de comités técnicos establecidos por las organizaciones respectivas para realizar acuerdos en los campos específicos de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en campos de interés mutuo. Otras organizaciones internacionales, públicas y privadas, en coordinación con ISO e IEC, también participan en el trabajo. En el campo de tecnologías de la información, ISO e IEC han establecido un comité técnico conjunto, el denominado ISO/IEC JTC 1.

Los procedimientos utilizados para desarrollar este documento y los destinados a su posterior mantenimiento se describen en las Directivas ISO/IEC, Parte 1. En particular, deben tenerse en cuenta los diferentes criterios de aprobación necesarios para los diferentes tipos de documentos. Este documento fue elaborado de acuerdo con las normas editoriales de las Directivas ISO/IEC, Parte 2 (ver www.iso.org/directives).

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento puedan estar sujetos a derechos de patente. ISO e IEC no deben asumir la responsabilidad por la identificación de cualquiera o todos los derechos de patente. Los detalles de cualquier derecho de patente identificados durante el desarrollo del documento estarán en la introducción y/o en la lista de ISO de las declaraciones de patentes recibidas (ver www.iso.org/patents).

Cualquier nombre comercial utilizado en el presente documento se da información para la comodidad de los usuarios y no constituye un endoso.

Para obtener una explicación sobre el significado de los términos y expresiones específicas, ISO relacionadas con la evaluación de la conformidad, así como información sobre el cumplimiento de ISO de los principios de la OMC en los Obstáculos Técnicos al Comercio (OTC) ver la siguiente URL: *Foreword - Supplementary information*

El comité responsable de este documento es ISO/IEC JTC 1, *Tecnologías de la información, SC 27, Técnicas de seguridad de TI*.

Esta cuarta edición anula y sustituye a la tercera edición (ISO/IEC 27000:2014) que ha sido revisada técnicamente.

Tecnologías de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Descripción general y vocabulario

0 Introducción

0.1 Descripción General

Las normas internacionales para los sistemas de gestión proporcionan un modelo a seguir para el establecimiento y operación de un sistema de gestión. Este modelo incorpora las características que los expertos acuerdan como un reflejo del estado del arte a nivel internacional. El subcomité SC27 del comité conjunto ISO/IEC JTC 1 cuenta con un grupo de expertos dedicado a la elaboración de normas internacionales sobre sistemas de gestión de seguridad de la información, también conocido como familia de normas de Sistemas de Gestión de Seguridad de la Información (SGSI).

Con el uso de las normas de la familia de SGSI, las organizaciones pueden desarrollar e implementar un marco para gestionar la seguridad de sus activos de información y preparar la evaluación independiente de su SGSI en materia de seguridad de la información por ejemplo para la información financiera, propiedad intelectual, la información del personal, o la información confiada a una organización por clientes o por terceros. Estas normas también pueden ser usadas por las organizaciones para prepararse ante una evaluación independiente de su SGSI aplicada a la protección de la información.

0.2 Familia de normas SGSI

La familia de normas de SGSI (ver capítulo 4) tiene como fin, ayudar a organizaciones de todo tipo y tamaño a implementar y operar un SGSI. La familia de normas SGSI incluye bajo el título general de: *Tecnologías de la información. Técnicas de seguridad* las siguientes normas internacionales (listadas en orden numérico):

- ISO/IEC 27000, *Sistemas de Gestión de Seguridad de la Información. Descripción general y vocabulario.*
- ISO/IEC 27001, *Sistemas de Gestión de Seguridad de la Información. Requisitos*.
- ISO/IEC 27002, *Código de práctica para los controles de seguridad de la información*.
- ISO/IEC 27003, *Guía para la implementación de los Sistemas de Gestión de Seguridad de la Información*.
- ISO/IEC 27004, *Gestión de seguridad de la información. Métricas*.
- ISO/IEC 27005, *Gestión de riesgos de seguridad de la información*.
- ISO/IEC 27006, *Requisitos para entidades que auditan y certifican Sistemas de Gestión de Seguridad de la información.*
- ISO/IEC 27007, *Guía para la auditoría de los Sistemas de Gestión de Seguridad de la Información.*
- ISO/IEC 27008, *Guía para los auditores de controles de seguridad de la información.*
- ISO/IEC 27010, *Gestión de seguridad de la información en comunicaciones intersectoriales e interorganizacionales.*
- ISO/IEC 27011 *Guía para la gestión de seguridad de la información para las organizaciones de telecomunicaciones basada en la ISO/IEC 27002.*

– ISO/IEC 27013 *Guía para la implementación integrada de ISO/IEC 27001 e ISO/IEC 20000-1.*

– ISO/IEC 27014 *Gobernanza de seguridad de la información.*

– ISO/IEC TR 27015 *Guía para la gestión de seguridad de la información para servicios financieros.*

– ISO/IEC TR 27016 *Gestión de seguridad de la información. Economía organizacional.*

– ISO/IEC TR 27017 *Gestión de seguridad de la información ISO/IEC 27017, Código de prácticas para el control de seguridad de la información en base a la ISO/IEC 27002 para los servicios en la nube*

– ISO/IEC TR 27018 *Gestión de seguridad de la información ISO/IEC 27018, Código de prácticas para la protección de la información personal identificable (PII) en nubes públicas en calidad de procesadores de PII*

– ISO/IEC TR 27019 *Gestión de seguridad de la información ISO/IEC 27019, directrices de gestión de seguridad de la información en base a la ISO/IEC 27002 para sistemas de control de procesos específicos de la industria de servicios públicos de energía*

NOTA El título general "*Tecnologías de la información*, *Técnicas de seguridad*" indica que estas normas han sido desarrolladas por el Subcomité SC 27, Técnicas de seguridad del Comité Técnico Conjunto ISO/IEC JTC 1, *Tecnologías de la información*.

Las normas internacionales que no están bajo el mismo título general también son parte de la familia de las normas de SGSI son:

– ISO/IEC 27799:2008, *Informática de la salud. Gestión de seguridad de la información en sanidad utilizando la ISO/IEC 27002.*

0.3 Objeto de esta norma nacional

Esta norma nacional ofrece una descripción general de los Sistemas de Gestión de Seguridad de la Información (SGSI), y define los términos relacionados.

NOTA El Anexo A aclara el uso de algunas formas verbales que se utilizan para expresar los requisitos y recomendaciones en la familia de normas de SGSI.

La familia de normas de SGSI cuenta con normas para:

a) definir los requisitos para un SGSI y para los organismos que certifiquen tales sistemas;

b) prestar apoyo directo, guía y/o interpretación detallada del conjunto de procesos para establecer, implementar, mantener y mejorar un SGSI;

c) directrices específicas del sector de dirección para el SGSI; y

d) sentar la base para la evaluación de la conformidad de un SGSI.

Los términos y definiciones contenidos en esta norma nacional

– cubren los términos y definiciones de uso común en la familia de normas de SGSI;

– no cubren todos los términos y las definiciones utilizados en la familia de normas de SGSI; y

– no limitan a que otras normas la familia de SGSI puedan definir nuevos términos para su uso.

Tecnologías de la información — Técnicas de seguridad — Sistemas de gestión de seguridad de la información – Descripción general y vocabulario

1 Objeto y campo de aplicación

Esta norma nacional proporciona una descripción general de los sistemas de gestión de seguridad de la información, así como los términos y definiciones de uso común en la familia de normas de SGSI. Esta norma nacional es aplicable a organizaciones de todo tipo y tamaño (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin ánimo de lucro).

2 Términos y definiciones

Para los fines de este documento, los siguientes términos y definiciones aplican.

2.1
control de acceso
medios para asegurar que el acceso a los activos está autorizado y restringido en función de los *requisitos* (2.63) de negocio y de seguridad

2.2
modelo analítico
algoritmo o cálculo que combina una o más *medidas base* (2.10) y/o *medidas derivadas* (2.22) con los *criterios de decisión asociados (2.21)*

2.3
ataque
tentativa de destruir, exponer, alterar, inhabilitar, robar o acceder sin autorización para hacer uso no autorizado de un activo

2.4
atributo
propiedad o característica de un *objeto* (2.55) que es cuantitativa o cualitativamente distinguible por medios humanos o automáticos.

[FUENTE: ISO/IEC 15939:2007, modificada - "entidad" ha sido sustituido por "objeto" en la definición.]

2.5
auditoría
proceso (2.61) sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en el que se cumplen los criterios de auditoría.

NOTA 1 a la entrada: Una auditoría puede ser interna (de primera parte), o externa (de segunda o tercera parte), y puede ser combinada (combinando dos o más disciplinas).

NOTA 2 a la entrada: “Evidencia de auditoría” y “criterios de auditoría” se definen en ISO 19011.

2.6

alcance de la auditoría

extensión y límites de una *auditoría* (2.5)

INFORMACIÓN COMPLEMENTARIA

Documento: NTE INEN-ISO/IEC 27000	**TÍTULO: TECNOLOGÍAS DE LA INFORMACIÓN — TÉCNICAS DE SEGURIDAD — SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – DESCRIPCIÓN GENERAL Y VOCABULARIO. (ISO/IEC 27000:2016, IDT))**	**Código ICS: 27.010**

ORIGINAL: Fecha de iniciación del estudio: 2016-02-5	REVISIÓN: La Subsecretaría de la Calidad del Ministerio de Industrias y Productividad aprobó este proyecto de norma Oficialización con el Carácter de Voluntaria por Resolución No.11 410 de 2011-12-29 publicado en el Registro Oficial Suplemento No. 699 de 2012-05-09 Fecha de iniciación del estudio: 2016-02-5

Fechas de consulta pública:

Comité Técnico de:
Fecha de iniciación: Fecha de aprobación:
Integrantes del Comité:

NOMBRES:	**INSTITUCIÓN REPRESENTADA:**

Otros trámites: Esta NTE INEN-ISO/IEC 27000:2016 reemplaza a la NTE INEN ISO/IEC 27000:2012.

La Subsecretaría de la Calidad del Ministerio de Industrias y Productividad aprobó este proyecto de norma

Oficializada como: Por Resolución No. Registro Oficial No.

Servicio Ecuatoriano de Normalización, INEN - Baquerizo Moreno E8-29 y Av. 6 de Diciembre
Casilla 17-01-3999 - Telfs: (593 2)3 825960 al 3825999
Dirección Ejecutiva: E-Mail: direccion@normalizacion.gob.ec
Dirección de Normalización: consultanormalizacion@normalizacion.gob.ec
Centro de Información: centrodeinformacion@normalizacion.gob.ec
URL:www.normalizacion.gob.ec