Norma Española

UNE-EN ISO/IEC 27000

Diciembre 2021
Versión corregida, Septiembre 2024

Tecnología de la información

Técnicas de seguridad

Sistemas de Gestión de la Seguridad de la Información (SGSI)

Visión de conjunto y vocabulario

(ISO/IEC 27000:2018)

Esta norma ha sido elaborada por el comité técnico CTN-UNE 320 *Ciberseguridad y protección de datos personales*, cuya secretaría desempeña UNE.

EXTRACTO DEL DOCUMENTO UNE-EN ISO/IEC 27000

Asociación Española de Normalización
Calle de Génova, 6
28004 Madrid. España
915 294 900
info@une.org – www.une.org

UNE-EN ISO/IEC 27000

Tecnología de la información
Técnicas de seguridad
Sistemas de Gestión de la Seguridad de la Información (SGSI)
Visión de conjunto y vocabulario
(ISO/IEC 27000:2018)

Information technology. Security techniques. Information security management systems. Overview and vocabulary (ISO/IEC 27000:2018).

Technologies de l'information. Techniques de sécurité. Systèmes de management de la sécurité de l'information. Vue d'ensemble et vocabulaire (ISO/IEC 27000:2018).

Esta norma es la versión oficial, en español, de la Norma Europea EN ISO/IEC 27000:2020, que a su vez adopta la Norma Internacional ISO/IEC 27000:2018.

Esta norma anula y sustituye a la Norma UNE-EN ISO/IEC 27000:2019.

Esta versión corregida de la Norma UNE-EN ISO/IEC 27000:2021 incorpora las siguientes correcciones:

Apartado 4.2.1, primer párrafo, primera frase, se añade la expresión " ….con el objetivo de proteger los activos de la información"

Apartado 4.2.5, punto e), se elimina al final de la frase "y a su entorno"

Apartado 4.4, primer párrafo, primera frase, se elimina la expresión "Como parte del SGSI de una organización,"

Apartado 4.4, tercer párrafo, primera frase, se corrige la expresión " …., los procesos de negocio, los empleados y el tamaño…" para leer "…los procesos de negocio empleados y el tamaño…"

Apartado 4.4, punto a), se corrige la expresión "… protegidos contra los riesgos de seguridad de la información de forma continua;" por "… protegidos contra las amenazas de forma continua;"

Apartado 4.5.2, punto b), se corrige para leer "las necesidades de negocio para el tratamiento, el almacenamiento y la comunicación de la información"

Apartado 5.1, primer guion, se sustituye la expresión "las especificaciones" por "los requisitos"

EXTRACTO DEL DOCUMENTO UNE-EN ISO/IEC 27000

Las observaciones a este documento han de dirigirse a:

Asociación Española de Normalización
Génova, 6
28004 MADRID-España
Tel.: 915 294 900
info@une.org
www.une.org

Índice

Prólogo europeo

El texto de la Norma ISO/IEC 27000:2018 del Comité Técnico ISO/IEC JTC 1 *Tecnología de la información*, de la Organización Internacional de Normalización (ISO), ha sido adoptado como Norma EN ISO/IEC 27000:2020 por el Comité Técnico CEN/CLC/JTC 13 *Ciberseguridad y protección de datos*, cuya Secretaría desempeña DIN.

Esta norma europea debe recibir el rango de norma nacional mediante la publicación de un texto idéntico a ella o mediante ratificación antes de finales de agosto de 2020, y todas las normas nacionales técnicamente divergentes deben anularse antes de finales de agosto de 2020.

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento estén sujetos a derechos de patente. CEN no es responsable de la identificación de dichos derechos de patente.

Esta norma anula y sustituye a la Norma EN ISO/IEC 27000:2017.

De acuerdo con el Reglamento Interior de CEN/CENELEC, están obligados a adoptar esta norma europea los organismos de normalización de los siguientes países: Alemania, Austria, Bélgica, Bulgaria, Chipre, Croacia, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Islandia, Italia, Letonia, Lituania, Luxemburgo, Malta, Noruega, Países Bajos, Polonia, Portugal, Reino Unido, República Checa, República de Macedonia del Norte, Rumanía, Serbia, Suecia, Suiza y Turquía.

Declaración

El texto de la Norma ISO/IEC 27000:2018 ha sido aprobado por CEN como Norma EN ISO/IEC 27000:2020 sin ninguna modificación.

Prólogo

ISO (Organización Internacional de Normalización) es una federación mundial de organismos nacionales de normalización (organismos miembros de ISO). El trabajo de elaboración de las Normas Internacionales se lleva a cabo normalmente a través de los comités técnicos de ISO. Cada organismo miembro interesado en una materia para la cual se haya establecido un comité técnico, tiene el derecho de estar representado en dicho comité. Las organizaciones internacionales, gubernamentales y no gubernamentales, vinculadas con ISO, también participan en el trabajo. ISO colabora estrechamente con la Comisión Electrotécnica Internacional (IEC) en todos los temas de normalización electrotécnica.

En la Parte 1 de las Directivas ISO/IEC se describen los procedimientos utilizados para desarrollar este documento y aquellos previstos para su mantenimiento posterior. En particular debería tomarse nota de los diferentes criterios de aprobación necesarios para los distintos tipos de documentos ISO. Este documento ha sido redactado de acuerdo con las reglas editoriales de la Parte 2 de las Directivas ISO/IEC (véase 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 no asume la responsabilidad por la identificación de alguno o todos los derechos de patente. Los detalles sobre cualquier derecho de patente identificado durante el desarrollo de este documento se indicarán en la Introducción y/o en la lista ISO de declaraciones de patente recibidas (véase www.iso.org/patents).

Cualquier nombre comercial utilizado en este documento es información que se proporciona para comodidad del usuario y no constituye una recomendación.

Para una explicación de la naturaleza voluntaria de las normas, el significado de los términos específicos de ISO y las expresiones relacionadas con la evaluación de la conformidad, así como la información acerca de la adhesión de ISO a los principios de la Organización Mundial del Comercio (OMC) respecto a los Obstáculos Técnicos al Comercio (OTC), véase www.iso.org/iso/foreword.html.

Este documento ha sido elaborado por el Comité Técnico ISO/IEC JTC 1, *Tecnología de la información*, Subcomité SC 27, *Ciberseguridad y Protección de la Privacidad*.

Esta quinta edición anula y sustituye a la cuarta edición (ISO/IEC 27000:2016) que ha sido revisada técnicamente. Los cambios principales en comparación con la edición previa son los siguientes:

- la Introducción ha sido reformulada;
- se han eliminado algunos términos y definiciones;
- el capítulo 3 se ha alineado con la estructura de alto nivel para el SMS;
- el capítulo 5 se ha actualizado para reflejar los cambios en las normas correspondientes;
- se han eliminado los anexos A y B.

0 Introducción

0.1 Visión de conjunto

Las normas internacionales para los sistemas de gestión proporcionan un modelo a seguir para la implementación y operación de un sistema de gestión. Este modelo incorpora las características que los expertos acuerdan como un reflejo del estado más avanzado a nivel internacional. El subcomité SC 27 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 la seguridad de la información, también conocido como familia de normas de Sistemas de Gestión de la 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 la 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 Objeto del presente documento

La familia de normas del SGSI incluye normas que:

a) definen los requisitos para un SGSI y para los que certifican esos sistemas;

b) proporcionan apoyo directo, guía detallada y/o interpretación para el proceso general de establecimiento, implementación, mantenimiento y mejora de un SGSI;

c) abordan las directrices específicas del sector para el SGSI; y

d) abordar la evaluación de la conformidad para el SGSI.

0.3 Contenido de este documento

En este documento se utilizan las siguientes formas verbales:

– “debe/n” indica un requisito;

– “debería/n” indica una recomendación;

– “puede/n” indica que algo es permisible, o una posibilidad o capacidad.

La información marcada como "NOTA" sirve de referencia para comprender o clarificar el requisito correspondiente. Las "notas de entrada" utilizadas en el capítulo 3 proporcionan información adicional que complementa los datos terminológicos y pueden contener disposiciones relativas al uso de un término.

1 Objeto y campo de aplicación

Este documento proporciona una visión general de los sistemas de gestión de la seguridad de la información (SGSI). También proporciona los términos y definiciones de uso común en la familia de normas de SGSI. Este documento es aplicable a organizaciones de todo tipo y tamaño (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin ánimo de lucro).

Los términos y definiciones que figuran en el presente documento

– abarcan los términos y definiciones comúnmente utilizados en la familia de normas de SGSI;

– no abarcan todos los términos y definiciones aplicados dentro de la familia de normas de SGSI; y

– no limitan la familia de normas de SGSI en la definición de nuevos términos de uso.

2 Normas para consulta

No existen normas para consulta en este documento.