

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 320 *Ciberseguridad y protección de datos  
personales*, cuya secretaría desempeña UNE.

**EXTRACTO DEL DOCUMENTO UNE-EN ISO/IEC 27000**

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.

## **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

© UNE 2021

Prohibida la reproducción sin el consentimiento de UNE.

Todos los derechos de propiedad intelectual de la presente norma son titularidad de UNE.

# Índice

Prólogo europeo .....	6
Declaración.....	6
Prólogo.....	7
0      Introducción.....	8
0.1    Visión de conjunto.....	8
0.2    Objeto del presente documento.....	8
0.3    Contenido de este documento.....	8
1      Objeto y campo de aplicación.....	9
2      Normas para consulta.....	9
3      Términos y definiciones.....	9
4      Sistemas de gestión de la seguridad de la información.....	19
4.1    General .....	19
4.2    ¿Qué es un SGSI?.....	20
4.2.1  Información y principios generales.....	20
4.2.2  Información .....	21
4.2.3  Seguridad de la información .....	21
4.2.4  Gestión.....	21
4.2.5  Sistema de gestión.....	22
4.3    Enfoque basado en procesos .....	22
4.4    ¿Por qué es importante un SGSI? .....	22
4.5    Establecer, supervisar, mantener y mejorar el SGSI.....	23
4.5.1  Visión general .....	23
4.5.2  Identificar los requisitos de seguridad de la información .....	24
4.5.3  Apreciación de los riesgos de seguridad de la información.....	24
4.5.4  Tratamiento de los riesgos de seguridad de la información .....	25
4.5.5  Seleccionar e implementar los controles.....	25
4.5.6  Supervisar, revisar, mantener y mejorar la eficacia de los SGSI.....	27
4.5.7  Mejora continua .....	27
4.6    Factores críticos de éxito de un SGSI.....	27
4.7    Beneficios de la familia de normas de SGSI.....	28
5      La familia de normas de SGSI .....	29
5.1    Información general.....	29
5.2    Norma que describe una visión general y una terminología: ISO/IEC 27000 (este documento) .....	30
5.3    Normas que especifican los requisitos .....	30
5.3.1  ISO/IEC 27001 .....	30
5.3.2  ISO/IEC 27006 .....	30
5.3.3  ISO/IEC 27009 .....	31
5.4    Normas que describen guías o directrices generales.....	31
5.4.1  ISO/IEC 27002 .....	31
5.4.2  ISO/IEC 27003 .....	31
5.4.3  ISO/IEC 27004 .....	32
5.4.4  ISO/IEC 27005 .....	32
5.4.5  ISO/IEC 27007 .....	32
5.4.6  ISO/IEC 27008 .....	32
5.4.7  ISO/IEC 27013 .....	33
5.4.8  ISO/IEC 27014 .....	33

5.4.9	ISO/IEC TR 27016.....	34
5.4.10	ISO/IEC 27021 .....	34
5.5	<b>Normas que describen guías específicas sectoriales.....</b>	<b>34</b>
5.5.1	ISO/IEC 27010 .....	34
5.5.2	ISO/IEC 27011 .....	35
5.5.3	ISO/IEC 27017 .....	35
5.5.4	ISO/IEC 27018 .....	35
5.5.5	ISO/IEC TR 27019.....	36
5.5.6	ISO 27799 .....	37
	<b>Bibliografía .....</b>	<b>38</b>

## 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.