

Técnicas de seguridad

Extensión de las Normas ISO/IEC 27001 e
ISO/IEC 27002 para la gestión de privacidad
de la información

Requisitos y directrices

(ISO/IEC 27701:2019)

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 27701

UNE-EN ISO/IEC 27701

Técnicas de seguridad
Extensión de las Normas ISO/IEC 27001 e ISO/IEC 27002 para la gestión
de privacidad de la información
Requisitos y directrices
(ISO/IEC 27701:2019)

Security techniques. Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management. Requirements and guidelines (ISO/IEC 27701:2019).

Techniques de sécurité. Extension d'ISO/IEC 27001 et ISO/IEC 27002 au management de la protection de la vie privée. Exigences et lignes directrices (ISO/IEC 27701:2019).

Esta norma es la versión oficial, en español, de la Norma Europea EN ISO/IEC 27701:2021, que a su vez adopta la Norma Internacional ISO/IEC 27701:2019.

EXTRACTO DEL DOCUMENTO UNE-EN ISO/IEC 27701

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	8
Declaración.....	8
Prólogo.....	9
0 Introducción	10
0.1 Generalidades	10
0.2 Compatibilidad con otras normas de sistemas de gestión	10
1 Objeto y campo de aplicación	11
2 Normas para consulta	11
3 Términos, definiciones y abreviaturas.....	11
4 Generalidades	12
4.1 Estructura de este documento	12
4.2 Aplicación de los requisitos de la Norma ISO/IEC 27001:2013	14
4.3 Aplicación de las directrices de la Norma ISO/IEC 27002:2013	14
4.4 Cliente	15
5 Requisitos específicos del SGPI relacionados con la Norma ISO/IEC 27001	16
5.1 Generalidades	16
5.2 Contexto de la organización.....	16
5.2.1 Comprensión de la organización y de su contexto	16
5.2.2 Comprensión de las necesidades y expectativas de las partes interesadas.....	17
5.2.3 Determinación del alcance del sistema de gestión de la seguridad de la información	17
5.2.4 Sistema de gestión de la seguridad de la información.....	17
5.3 Liderazgo	17
5.3.1 Liderazgo y compromiso.....	17
5.3.2 Política.....	17
5.3.3 Roles, responsabilidades y autoridades en la organización	17
5.4 Planificación	18
5.4.1 Acciones para tratar los riesgos y oportunidades.....	18
5.4.2 Objetivos de la seguridad de la información y planificación para su consecución.....	19
5.5 Soporte	19
5.5.1 Recursos.....	19
5.5.2 Competencia	19
5.5.3 Concienciación	19
5.5.4 Comunicación	19
5.5.5 Información documentada.....	19
5.6 Operación	20
5.6.1 Planificación y control operacional.....	20
5.6.2 Evaluación de los riesgos de seguridad de la información.....	20
5.6.3 Tratamiento de los riesgos de seguridad de la información	20
5.7 Evaluación del desempeño.....	20
5.7.1 Monitorización, medición, análisis y evaluación.....	20
5.7.2 Auditoría interna.....	20
5.7.3 Revisión por la dirección	20
5.8 Mejora.....	20

5.8.1	No conformidad y acciones correctivas.....	20
5.8.2	Mejora continua.....	21
6	Guía específica del SGPI relacionadas con la Norma ISO/IEC 27002.....	21
6.1	Generalidades	21
6.2	Políticas de seguridad de la información.....	21
6.2.1	Directrices de gestión de la seguridad de la información	21
6.3	Organización de la seguridad de la información	22
6.3.1	Organización interna	22
6.3.2	Los dispositivos móviles y el teletrabajo	23
6.4	Seguridad relativa a los recursos humanos	23
6.4.1	Antes del empleo	23
6.4.2	Durante el empleo.....	23
6.4.3	Finalización del empleo o cambio en el puesto de trabajo.....	24
6.5	Gestión de activos	24
6.5.1	Responsabilidad sobre los activos	24
6.5.2	Clasificación de la información	25
6.5.3	Gestión de los soportes.....	25
6.6	Control de acceso	26
6.6.1	Requisitos de negocio para el control de acceso	26
6.6.2	Gestión de acceso de usuario.....	27
6.6.3	Responsabilidades del usuario	28
6.6.4	Control de acceso a sistemas y aplicaciones	28
6.7	Criptografía.....	29
6.7.1	Controles criptográficos.....	29
6.8	Seguridad física y del entorno.....	29
6.8.1	Áreas seguras	29
6.8.2	Seguridad de los equipos	30
6.9	Seguridad de las operaciones	31
6.9.1	Procedimientos y responsabilidades operacionales	31
6.9.2	Protección contra el <i>software</i> malicioso (<i>malware</i>)	32
6.9.3	Copias de seguridad	32
6.9.4	Registro, monitorización y supervisión	33
6.9.5	Control del <i>software</i> en explotación	34
6.9.6	Gestión de la vulnerabilidad técnica	34
6.9.7	Consideraciones sobre la auditoría de sistemas de información.....	34
6.10	Seguridad de las comunicaciones	34
6.10.1	Gestión de la seguridad de redes.....	34
6.10.2	Intercambio de información	35
6.11	Adquisición, desarrollo y mantenimiento de los sistemas de información.....	35
6.11.1	Requisitos de seguridad en los sistemas de información	35
6.11.2	Seguridad en el desarrollo y en los procesos de soporte.....	36
6.11.3	Datos de prueba.....	38
6.12	Relación con proveedores	38
6.12.1	Seguridad en las relaciones con proveedores	38
6.12.2	Gestión de la provisión de servicios del proveedor	39
6.13	Gestión de incidentes de seguridad de la información.....	39
6.13.1	Gestión de incidentes de seguridad de la información y mejoras.....	39
6.14	Aspectos de la seguridad de la información para la gestión de la continuidad del negocio	42
6.14.1	Continuidad de la seguridad de la información	42
6.14.2	Redundancias	42
6.15	Cumplimiento.....	43
6.15.1	Cumplimiento de los requisitos legales y contractuales.....	43
6.15.2	Revisiones de la seguridad de la información	44

7	Guía adicional de la Norma ISO/IEC 27002 para el responsable del tratamiento de IIP	44
7.1	Generalidades	44
7.2	Condiciones para la recogida y tratamiento	45
7.2.1	Identificar y documentar la finalidad	45
7.2.2	Identificar bases legitimadoras	45
7.2.3	Determinar cuándo y cómo se debe obtener el consentimiento	46
7.2.4	Obtener y registrar el consentimiento	46
7.2.5	Evaluar el impacto de la privacidad	47
7.2.6	Contratos con encargados del tratamiento de IIP	48
7.2.7	Corresponsables del tratamiento de IIP	48
7.2.8	Registros de actividades del tratamiento de IIP	49
7.3	Obligaciones hacia los interesados.....	50
7.3.1	Determinar y cumplir las obligaciones con los interesados	50
7.3.2	Determinar la información a facilitar a los interesados	50
7.3.3	Proporcionar información a los interesados.....	51
7.3.4	Proporcionar un mecanismo para modificar o retirar el consentimiento	51
7.3.5	Proporcionar un mecanismo para oponerse al tratamiento de IIP	52
7.3.6	Acceso, rectificación y/o supresión	53
7.3.7	Obligaciones de los responsables del tratamiento de IIP de informar a terceros	53
7.3.8	Proporcionar una copia de la IIP tratada	54
7.3.9	Gestión de solicitudes	54
7.3.10	Toma de decisiones automatizadas.....	55
7.4	Privacidad desde el diseño y privacidad por defecto.....	55
7.4.1	Limitar la recogida de IIP	55
7.4.2	Limitar el tratamiento	56
7.4.3	Exactitud y calidad.....	56
7.4.4	Objetivos de minimización de IIP.....	56
7.4.5	Anonimización de la IIP y eliminación al final del tratamiento	57
7.4.6	Archivos temporales	58
7.4.7	Plazo de conservación	58
7.4.8	Eliminación	58
7.4.9	Control de transmisiones de IIP	59
7.5	Intercambio, transferencia y comunicación de IIP	59
7.5.1	Identificar las bases para la transferencia de IIP entre jurisdicciones	59
7.5.2	Países y organizaciones internacionales a los que se puede transferir IIP	60
7.5.3	Registros de transferencia de IIP	60
7.5.4	Registros de comunicación de IIP a terceros.....	60
8	Guía adicional de la Norma ISO/IEC 27002 para el encargado del tratamiento de IIP	61
8.1	Generalidades	61
8.2	Condiciones de recogida y tratamiento	61
8.2.1	Acuerdo con el cliente.....	61
8.2.2	Finalidades de la organización.....	61
8.2.3	Uso de marketing y publicidad	62
8.2.4	Instrucción infractora.....	62
8.2.5	Obligaciones del cliente	63
8.2.6	Registros de actividades del tratamiento de IIP.....	63
8.3	Obligaciones hacia los interesados.....	63
8.3.1	Obligaciones hacia los interesados.....	63
8.4	Privacidad desde el diseño y privacidad por defecto.....	64
8.4.1	Archivos temporales	64

8.4.2	Devolución, transferencia o eliminación de IIP	64
8.4.3	Controles de transmisión de IIP	65
8.5	Intercambio, transferencia y comunicación de IIP	65
8.5.1	Identificación de las bases para la transferencia de IIP entre jurisdicciones	65
8.5.2	Países y organizaciones internacionales a los que se puede transferir IIP	66
8.5.3	Registros de comunicación de IIP a terceros	66
8.5.4	Notificación de solicitudes de comunicación de IIP	67
8.5.5	Comunicaciones de IIP legalmente vinculantes	67
8.5.6	Comunicación de subencargados del tratamiento de IIP	67
8.5.7	Contratación de un subencargado del tratamiento de IIP	68
8.5.8	Cambio de subencargado del tratamiento de IIP	68
Anexo A (Normativo)	Objetivos de control y controles específicos del SGPI (responsable del tratamiento de IIP)	71
Anexo B (Normativo)	Objetivos de control y controles específicos del SGPI (encargados del tratamiento de IIP)	75
Anexo C (Informativo)	Correspondencia con la Norma ISO/IEC 29100	78
Anexo D (Informativo)	Correspondencia con el Reglamento General de Protección de Datos	81
Anexo E (Informativo)	Correspondencia con las Normas ISO/IEC 27018 e ISO/IEC 29151	85
Anexo F (Informativo)	Cómo aplicar las Normas ISO/IEC 27701, ISO/IEC 27001 e ISO/IEC 27002	88
Bibliografía		91

1 Objeto y campo de aplicación

Este documento especifica los requisitos y proporciona una guía para implementar, mantener y mejorar continuamente un Sistema de Gestión sobre la Privacidad de la Información (SGPI) como una extensión de las Normas ISO/IEC 27001 e ISO/IEC 27002 para la gestión de la privacidad en el contexto de la organización.

Este documento especifica los requisitos relacionados con el SGPI y proporciona orientación para los responsables del tratamiento y encargados del tratamiento que tienen la responsabilidad y la obligación de rendir cuentas sobre el tratamiento de IIP.

Este documento es aplicable a todos los tipos y tamaños de organizaciones, tanto de carácter público como privado, así como a entidades gubernamentales y organizaciones sin ánimo de lucro que son responsables del tratamiento de y/o encargados del tratamiento que tratan IIP dentro de un SGPI.

2 Normas para consulta

En el texto se hace referencia a los siguientes documentos de manera que parte o la totalidad de su contenido constituyen requisitos de este documento. Para las referencias con fecha, solo se aplica la edición citada. Para las referencias sin fecha se aplica la última edición (incluida cualquier modificación de esta).

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 27001:2013, *Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.*

ISO/IEC 27002:2013, *Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información.*

ISO/IEC 29100, *Tecnología de la información. Técnicas de seguridad. Marco de privacidad.*