



Comprar

norma española

UNE-ISO/IEC 27001

Noviembre 2014

TÍTULO

Tecnología de la información

Técnicas de seguridad

Sistemas de Gestión de Seguridad de la Información (SGSI)

Requisitos

Information technology. Security techniques. Information security management systems. Requirements.

Technologies de l'information. Techniques de sécurité. Systèmes de management de la sécurité de l'information. Exigences.

CORRESPONDENCIA

Esta norma es idéntica a la Norma Internacional ISO/IEC 27001:2013.

OBSERVACIONES

ANTECEDENTES

Esta norma ha sido elaborada por el comité técnico AEN/CTN 71 *Tecnología de la información*.

EXTRACTO DEL DOCUMENTO UNE-ISO/IEC 27001

Editada e impresa por AENOR
Depósito legal: M 32359:2014

© AENOR 2014
Reproducción prohibida

LAS OBSERVACIONES A ESTE DOCUMENTO HAN DE DIRIGIRSE A:

AENOR Asociación Española de
Normalización y Certificación

Génova, 6
28004 MADRID-España

info@aenor.es
www.aenor.es

Tel.: 902 102 201
Fax: 913 104 032

30 Páginas



Comprar

Índice

Prólogo.....	4
0	Introducción..... 5
0.1	Generalidades 5
0.2	Compatibilidad con otras normas de sistema de gestión..... 5
1	Objeto y campo de aplicación..... 5
2	Normas para consulta 6
3	Términos y definiciones..... 6
4	Contexto de la organización..... 6
4.1	Comprensión de la organización y de su contexto 6
4.2	Comprensión de las necesidades y expectativas de las partes interesadas..... 6
4.3	Determinación del alcance del sistema de gestión de seguridad de la información 6
4.4	Sistema de gestión de seguridad de la información 6
5	Liderazgo..... 7
5.1	Liderazgo y compromiso..... 7
5.2	Política 7
5.3	Roles, responsabilidades y autoridades en la organización..... 7
6	Planificación..... 8
6.1	Acciones para tratar los riesgos y oportunidades 8
6.2	Objetivos de seguridad de la información y planificación para su consecución 9
7	Soporte..... 10
7.1	Recursos 10
7.2	Competencia..... 10
7.3	Concienciación 11
7.4	Comunicación 11
7.5	Información documentada..... 11
8	Operación 12
8.1	Planificación y control operacional..... 12
8.2	Apreciación de los riesgos de seguridad de información 12
8.3	Tratamiento de los riesgos de seguridad de información 13
9	Evaluación del desempeño 13
9.1	Seguimiento, medición, análisis y evaluación 13
9.2	Auditoría interna 13
9.3	Revisión por la dirección..... 14
10	Mejora 14
10.1	No conformidad y acciones correctivas 14
10.2	Mejora continua..... 15
Anexo A (Normativo)	Objetivos de control y controles de referencia 16
Bibliografía.....	30



Comprar

1 Objeto y campo de aplicación

Esta norma internacional especifica los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de seguridad de la información en el contexto de la organización. Esta norma también incluye los requisitos para la apreciación y el tratamiento de los riesgos de seguridad de información a la medida de las necesidades de la organización. Los requisitos establecidos en esta norma internacional son genéricos y aplicables a todas las organizaciones, cualquiera que sea su tipo, tamaño o naturaleza. No se acepta la declaración de conformidad con respecto a esta norma internacional habiendo excluido alguno de los requisitos especificados en los capítulos 4 al 10.

2 Normas para consulta

Los documentos indicados a continuación, en su totalidad o en parte, son normas para consulta indispensables para la aplicación de este documento. Para las referencias con fecha, sólo se aplica la edición citada. Para las referencias sin fecha se aplica la última edición (incluyendo cualquier modificación de ésta).

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.*