Norma Española

UNE-EN ISO/IEC 27000

Febrero 2019

Tecnología de la información

Técnicas de seguridad

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

Visión de conjunto y vocabulario

(ISO/IEC 27000:2016)

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

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

INGENIERIA DE SISTEMAS PARA LA DEFENSA DE ESPAÑA, S.A., S.M.E., M.P. - ISDEFE

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 27000:2016)

Information technology. Security techniques. Information security management systems. Overview and vocabulary (ISO/IEC 27000:2016).

Technologies de l'information. Techniques de sécurité. Systèmes de gestion de sécurité de l'information. Vue d'ensemble et vocabulaire (ISO/IEC 27000:2016).

Esta norma es la versión oficial, en español, de la Norma Europea EN ISO/IEC 27000:2017, que a su vez adopta la Norma Internacional ISO/IEC 27000:2016.

Esta norma anula y sustituye a las Normas UNE-ISO/IEC 27000:2012 y UNE-ISO/IEC 27000:2014.

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
Depósito legal: M 6847:2019

© UNE 2019
Prohibida la reproducción sin el consentimiento de UNE.
Todos los derechos de propiedad intelectual de la presente norma son titularidad de UNE.

NORMA EUROPEA
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN ISO/IEC 27000

Febrero 2017

ICS 01.040.35; 03.100.70; 35.030

Versión en español

Tecnología de la información
Técnicas de seguridad
Sistemas de Gestión de la Seguridad de la Información (SGSI)
Visión de conjunto y vocabulario
(ISO/IEC 27000:2016)

Information technology. Security techniques. Information security management systems. Overview and vocabulary (ISO/IEC 27000:2016).

Technologies de l'information. Techniques de sécurité. Systèmes de gestion de sécurité de l'information. Vue d'ensemble et vocabulaire (ISO/IEC 27000:2016).

Informationstechnik. Sicherheitsverfahren. Informationssicherheits-Managementsysteme. Überblick und Terminologie (ISO/IEC 27000:2016).

Esta norma europea ha sido aprobada por CEN el 2017-01-26.

Los miembros de CEN/CENELEC están sometidos al Reglamento Interior de CEN/CENELEC que define las condiciones dentro de las cuales debe adoptarse, sin modificación, la norma europea como norma nacional. Las correspondientes listas actualizadas y las referencias bibliográficas relativas a estas normas nacionales pueden obtenerse en el Centro de Gestión de CEN/CENELEC, o a través de sus miembros.

Esta norma europea existe en tres versiones oficiales (alemán, francés e inglés). Una versión en otra lengua realizada bajo la responsabilidad de un miembro de CEN/CENELEC en su idioma nacional, y notificada al Centro de Gestión de CEN/CENELEC, tiene el mismo rango que aquéllas.

Los miembros de CEN/CENELEC son los organismos nacionales de normalización y los comités electrotécnicos nacionales de los países siguientes: Alemania, Antigua República Yugoslava de Macedonia, 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, Rumanía, Serbia, Suecia, Suiza y Turquía.

CENTRO DE GESTIÓN DE CEN/CENELEC
Rue de la Science, 23, B-1040 Brussels, Belgium

© 2017 CEN/CENELEC. Derechos de reproducción reservados a los Miembros de CEN/CENELEC.

Índice

Prólogo europeo

El texto de la Norma ISO/IEC 27000:2016 ha sido elaborado por el Comité Técnico ISO/IEC JTC 1 *Tecnología de la información*, de la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) y se ha tomado como Norma EN ISO/IEC 27000:2017.

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 2017, y todas las normas nacionales técnicamente divergentes deben anularse antes de finales de agosto de 2017.

Se llama la atención sobre la posibilidad de que algunos de los elementos de este documento estén sujetos a derechos de patente. CEN y/o CENELEC no es(son) responsable(s) de la identificación de dichos derechos de patente.

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, Antigua República Yugoslava de Macedonia, 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, Rumanía, Serbia, Suecia, Suiza y Turquía.

Declaración

El texto de la Norma ISO 27000:2016 ha sido aprobado por CEN como Norma EN ISO/IEC 27000:2017 sin ninguna modificación.

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.

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.

La Norma ISO/IEC 27000 fue preparada por el Comité Técnico conjunto ISO/IEC JTC 1 *Tecnología de la Información,* SC 27 *Técnicas de seguridad*.

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

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 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 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 La familia de normas de SGSI

La familia de normas de SGSI (véase 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: *Tecnología de la información. Técnicas de seguridad* las siguientes normas internacionales (listadas en orden numérico):

- ISO/IEC 27000, *Sistemas de Gestión de la Seguridad de la Información (SGSI). Visión de conjunto y vocabulario.*
- ISO/IEC 27001, *Sistemas de Gestión de la Seguridad de la Información (SGSI). 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 la Seguridad de la Información (SGSI)*.
- 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 la Seguridad de la Información (SGSI).*
- ISO/IEC 27007, *Guía para la auditoría de los Sistemas de Gestión de la Seguridad de la Información (SGSI).*
- ISO/IEC 27008, *Guía para los auditores de controles de seguridad de la información.*
- ISO/IEC 27009, *Aplicación sectorial específica de ISO/IEC 27001. Requisitos.*
- 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 Norma 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 la 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 27017, *Código de práctica para los controles de seguridad de la información basados en ISO/IEC 27002 para servicios en la nube* (*cloud services).*

— ISO/IEC 27018, *Código de práctica para la protección de información de identificación personal (PII) en nubes públicas que actúan como procesadores de PII.*

— ISO/IEC 27019, *Directrices de gestión de seguridad de la información en base a la Norma ISO/IEC 27002 para sistemas de control de procesos específicos de la industria de servicios públicos de energía.*

NOTA El título general "*Tecnología de la información, Técnicas de seguridad*" indica que estas normas internacionales han sido desarrolladas por el Subcomité SC 27, *Técnicas de seguridad* del comité técnico conjunto ISO/IEC JTC 1, *Tecnología de la información*.

Las normas internacionales cuyo título general no es *Tecnología de la información. Técnicas de Seguridad*, pero que también son parte de la familia de las normas SGSI son:

– ISO/IEC 27799, *Informática sanitaria. Gestión de seguridad de la información en sanidad utilizando la Norma ISO/IEC 27002.*

0.3 Objeto de esta norma internacional

Esta norma internacional ofrece una visión general de los Sistemas de Gestión de la 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 e interpretación detallada del conjunto de procesos para establecer, implementar, mantener y mejorar un SGSI,

c) ofrecer directrices específicas de determinados sectores para un SGSI, y

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

Los términos y definiciones contenidos en esta norma internacional

– 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 de la familia de SGSI puedan definir nuevos términos para su uso.

1 Objeto y campo de aplicación

Esta norma internacional proporciona una visión general de los sistemas de gestión de la seguridad de la información, así como los términos y definiciones de uso común en la familia de normas de SGSI. Esta norma internacional 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, se aplican los términos y definiciones siguientes:

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

2.2 modelo analítico:
Algoritmo o cálculo que combina una o más *medidas básicas* (2.10) y/o *derivadas* (2.22) siguiendo los *criterios de decisión* asociados a las mismas (2.21).

2.3 ataque:
Tentativa de destruir, exponer, alterar, inhabilitar, robar o acceder sin autorización o hacer un 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.

[ISO/IEC 15939:2007, 2.2, modificado – "entidad" ha sido reemplazado 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 Una auditoría puede ser interna (realizada por la propia empresa), o externa (realizada por una tercera parte), y puede ser combinada (combinando dos o más disciplinas).

NOTA 2 "Evidencia de auditoría" y "criterios de auditoría" se definen en la Norma ISO 19011.

2.6 alcance de la auditoría:
Extensión y límites de una *auditoría* (2.5).

[ISO 19011:2011, 3.14, modificado – Se ha eliminado la NOTA 1]

2.7 autenticación:
Aportación de garantías de que son correctas las características que una entidad reivindica para sí misma.

2.8 autenticidad:
Propiedad consistente en que una entidad es lo que dice ser.

2.9 disponibilidad:
Propiedad de ser accesible y estar listo para su uso a demanda de una entidad autorizada.

2.10 medida básica:
Medida (2.47) definida por medio de un *atributo* (2.4) y el método para cuantificarlo.

[ISO/IEC 15939:2007, 2.3, modificado – Se ha eliminado la NOTA 2]

NOTA Una medida básica es funcionalmente independiente de otras *medidas* (2.47).

2.11 competencia:
Capacidad para aplicar conocimientos y habilidades con el fin de lograr los resultados previstos.

2.12 confidencialidad:
Propiedad de la información por la que se mantiene inaccesible y no se revela a individuos, entidades o *procesos* (2.61) no autorizados.

2.13 conformidad:
Cumplimiento de un *requisito* (2.63).

NOTA El término "conformance" es sinónimo, pero está en desuso.

2.14 consecuencia:
Resultado de un *suceso* (2.25) que afecta a los *objetivos* (2.56).

[Guía ISO 73:2009, 3.6.1.3, modificado]

NOTA 1 Un *suceso* (2.25) puede conducir a una serie de consecuencias.

NOTA 2 Una consecuencia puede ser cierta o incierta y normalmente es negativa en el contexto de la *seguridad de la información* (2.33).

NOTA 3 Las consecuencias se pueden expresar de forma cualitativa o cuantitativa.

NOTA 4 Las consecuencias iniciales pueden convertirse en reacciones en cadena.

2.15 mejora continua:
Actividad recurrente para mejorar el *desempeño* (2.59).

2.16 control:
Medida que modifica un *riesgo* (2.68).

[Guía ISO 73:2009, 3.8.1.1]

NOTA 1 Los controles incluyen cualquier *proceso* (2.61), *política* (2.60), dispositivo, práctica, u otras acciones que modifiquen un *riesgo* (2.68).

NOTA 2 Los controles no siempre pueden proporcionar el efecto de modificación previsto o asumido.

2.17 objetivo de control:
Declaración que describe lo que se quiere lograr como resultado de la implementación de *controles* (2.16).

2.18 corrección:
Acción para eliminar una *no conformidad* (2.53) detectada.

2.19 acción correctiva:
Acción para eliminar la causa de una *no conformidad* (2.53) y prevenir que vuelva a ocurrir.

2.20 datos:
Conjunto de valores asociados a *medidas básicas* (2.10), *medidas derivadas* (2.22) y/o *indicadores* (2.30).

[ISO/IEC 15939:2007, 2.4, modificado – Se ha eliminado la NOTA 1]

NOTA Esta definición sólo se aplica en el contexto de la Norma ISO/IEC 27004.

2.21 criterios de decisión:
Umbrales, objetivos o patrones que se utilizan para determinar la necesidad de una acción o de una mayor investigación, o para describir el nivel de confianza en un resultado determinado.

[ISO/IEC 15939:2007, 2.7]

2.22 medida derivada:
Medida (2.47) que se define en función de dos o más valores de *medidas básicas* (2.10).

[ISO/IEC 15939:2007, 2.8, modificado – Se ha eliminado la NOTA 1]

2.23 información documentada:
Información que una *organización* (2.57) tiene que controlar y mantener, y el medio en el que está contenida.

NOTA 1 La información documentada puede estar en cualquier formato y medio, y puede provenir de cualquier fuente.

NOTA 2 La información documentada puede hacer referencia a:

- el *sistema de gestión* (2.46), incluidos los *procesos* (2.61) relacionados,
- la información creada para que la *organización* (2.57) opere (documentación),
- la evidencia de los resultados alcanzados (registros).

2.24 eficacia:
Grado en el cual se realizan las actividades planificadas y se logran los resultados planificados.

2.25 evento:
Ocurrencia o cambio de un conjunto particular de circunstancias.

[equivalente a "suceso" en Guía ISO 73:2009, 3.5.1.3, modificado – Se ha eliminado la NOTA 4]

NOTA 1 Un evento puede ser único o repetirse, y se puede deber a varias causas.

NOTA 2 Un evento puede consistir en algo que no se llega a producir.

NOTA 3 Algunas veces, un evento se puede calificar como un "incidente" o un "accidente".

2.26 dirección ejecutiva:
Persona o grupo de personas en la(s) que los *órganos de gobierno* (2.29) han delegado la responsabilidad de implementar estrategias y políticas para alcanzar la misión de la *organización* (2.57).

NOTA La dirección ejecutiva a veces se llama *alta dirección* (2.84) y puede incluir directores generales, directores financieros, directores de la información, y otros roles similares.

2.27 contexto externo:
Entorno externo en el que la organización busca alcanzar sus *objetivos* (2.56).

[Guía ISO 73:2009, 3.3.1.1]

NOTA El entorno externo puede incluir lo siguiente:

- el entorno cultural, social, político, legal, regulatorio, financiero, tecnológico, económico, natural y competitivo, a nivel internacional, nacional, regional o local,
- los factores y las tendencias que tengan impacto sobre los *objetivos* (2.56) de la *organización* (2.57),
- las relaciones con las *partes interesadas* externas (2.82), sus percepciones y sus valores.

2.28 gobernanza de la seguridad de la información:
Sistema mediante el cual una *organización* (2.57) dirige y supervisa las actividades de *seguridad de la información* (2.33).

2.29 órgano de gobierno:
Conjunto de personas que responden de y rinden cuentas del *desempeño* (2.59) de la *organización* (2.57).

NOTA Algunas jurisdicciones, el órgano de gobierno puede ser el consejo de administración.

2.30 indicador:
Medida (2.47) que proporciona una estimación o una evaluación de determinados *atributos* (2.4) usando un *modelo analítico* (2.2) para satisfacer unas determinadas *necesidades de información* (2.31).

2.31 necesidades de información:
Conocimiento necesario para gestionar los *objetivos*, (2.56), las metas, el riesgo y los problemas.

[ISO/IEC 15939:2007, 2.12]

2.32 recursos (instalaciones) de tratamiento de información:
Cualquier sistema de tratamiento de la información, servicios o infraestructura, o los lugares físicos que los albergan.

2.33 seguridad de la información:
Preservación de la *confidencialidad* (2.12), la *integridad* (2.40) y la *disponibilidad* (2.9) de la información.

NOTA Pudiendo, además, abarcar otras propiedades, como la *autenticidad* (2.8), la responsabilidad, el *no repudio* (2.54) y la *fiabilidad* (2.62).

2.34 continuidad de la seguridad de la información:
Procesos (2.61) y procedimientos para asegurar la continuidad de las actividades relacionadas con la *seguridad de la información* (2.33).

2.35 evento o suceso de seguridad de la información:
Ocurrencia detectada en el estado de un sistema, servicio o red que indica una posible violación de la *política* (2.60) de *seguridad de la información* (2.33), un fallo de los *controles* (2.16), o una situación desconocida hasta el momento y que puede ser relevante para la seguridad.

2.36 incidente de seguridad de la información:
Evento singular o serie de *eventos de seguridad de la información* (2.35), inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la *seguridad de la información* (2.33).

2.37 gestión de incidentes de seguridad de la información:
Procesos (2.61) para la detección, notificación, evaluación, respuesta, tratamiento, y aprendizaje de *incidentes de seguridad de la información* (2.36).

2.38 colectivo que comparte información:
Grupo de *organizaciones* (2.57) que acuerdan compartir información.

NOTA Una *organización* (2.57) puede ser un individuo.

2.39 sistema de información:
Aplicaciones, servicios, activos de tecnologías de la información y otros componentes para manejar información.

2.40 integridad:
Propiedad de exactitud y completitud.

2.41 parte interesada:
Persona u *organización* (2.57) que puede afectar, estar afectada, o percibir que está afectada por una decisión o actividad.

2.42 contexto interno:
Entorno interno en el que la *organización* (2.57) busca alcanzar sus objetivos.

[Guía ISO 73:2009, 3.3.1.2]

NOTA El contexto interno puede incluir lo siguiente:

- el gobierno, la estructura de la organización, las funciones y la obligación de rendir cuentas,
- las *políticas* (2.60), los *objetivos* (2.56) y las estrategias que se establecen para conseguirlo,
- las capacidades, entendidas en términos de recursos y conocimientos (por ejemplo, capital, tiempo, personas, *procesos* (2.61), sistemas y tecnologías),
- los *sistemas de información* (2.39), los flujos de información y los *procesos* (2.61) de toma de decisiones (tanto formales como informales),
- las relaciones con, y las percepciones y los valores de las *partes interesadas* internas (2.82),
- la cultura de la *organización* (2.57),
- las normas, las directrices y los modelos adoptados por la *organización* (2.57),
- la forma y amplitud de las relaciones contractuales.

2.43 proyecto del SGSI:
Actividades estructuradas llevadas a cabo por una *organización* (2.57) para implementar un SGSI.

2.44 nivel de riesgo:
Magnitud de un *riesgo* (2.68) o combinación de riesgos, expresados en términos de la combinación de las *consecuencias* (2.14) y de su *probabilidad* (2.45).

[Guía ISO 73:2009, 3.6.1.8, modificado – Se ha eliminado “o combinación de riesgos” en la definición]

2.45 probabilidad (*likelihood*):
Posibilidad de que algún hecho se produzca.

[Guía ISO 73:2009, 3.6.1.1, modificado – Se han eliminado la NOTA 1 y 2]

2.46 sistema de gestión:
Conjunto de elementos de una *organización* (2.57) interrelacionados o que interactúan para establecer *políticas* (2.60), *objetivos* (2.56) y *procesos* (2.61) para lograr estos objetivos.

NOTA 1 Un sistema de gestión puede tratar una sola disciplina o varias disciplinas.

NOTA 2 Los elementos del sistema incluyen la estructura de la organización, los roles y las responsabilidades, la planificación, la operación.

NOTA 3 El alcance de un sistema de gestión puede incluir la totalidad de la organización, funciones específicas e identificadas de la *organización* (2.57), secciones específicas e identificadas de la *organización* (2.57), o una o más funciones dentro de un grupo de *organizaciones* (2.57).

2.47 medida:
Variable a la que se le asigna un valor como resultado de una *medición* (2.48).

[ISO/IEC 15939:2007, 2.15, modificado]

NOTA El término "medidas" se utiliza para hacer referencia conjuntamente a *medidas de base* (2.10), *medidas derivadas* (2.22), e *indicadores* (2.30).

2.48 medición:
Proceso (2.61) para determinar un valor.

NOTA En el contexto de *seguridad de la información* (2.33), el proceso (2.61) para determinar un valor requiere información sobre la *eficacia* (2.24) de un sistema de gestión (2.46) de *seguridad de la información* (2.33) y sus correspondientes *controles* (2.16) utilizando un *método de medición* (2.50), una *función de medición* (2.49), un *modelo analítico* (2.2), y unos *criterios de decisión* (2.21).

2.49 función de medición:
Algoritmo o cálculo realizado para combinar dos o más *medidas básicas* (2.10).

[ISO/IEC 15939:2007, 2.20]

2.50 método de medición:
Secuencia lógica de operaciones, descritas genéricamente, utilizada en la cuantificación de un *atributo* (2.4) con respecto a una *escala* (2.80) especificada.

[ISO/IEC 15939:2007, 2.22, modificado – Se ha eliminado la NOTA 2]

NOTA El tipo de método de medición depende de la naturaleza de las operaciones utilizadas para cuantificar un *atributo* (2.4). Se pueden distinguir dos tipos de la siguiente manera:

- subjetivo: la cuantificación se basa en el juicio humano,
- objetivo: la cuantificación se basa en reglas numéricas.

2.51 resultados de las mediciones:
Uno o más *indicadores* (2.30) y sus correspondientes interpretaciones que abordan una *necesidad de información* (2.31).

2.52 supervisión, seguimiento o monitorización (*monitoring*):
Determinación del estado de un sistema, un *proceso* (2.61) o una actividad.

NOTA 1 Para determinar el estado puede ser necesario verificar, supervisar u observar en forma crítica.

2.53 no conformidad:
Incumplimiento de un requisito (2.63).

2.54 no repudio:
Capacidad para corroborar que es cierta la reivindicación de que ocurrió un cierto *suceso* (2.25) o se realizó una cierta acción por parte de las entidades que lo originaron.

2.55 objeto:
Elemento caracterizado por medio de la *medición* (2.48) de sus *atributos* (2.4).

2.56 objetivo:
Resultado a lograr.

NOTA 1 Un objetivo puede ser estratégico, táctico u operativo.

NOTA 2 Los objetivos pueden referirse a diferentes disciplinas (como financieras, de seguridad y salud y ambientales) y se pueden aplicar en diferentes niveles (como estratégicos, para toda la organización, para proyectos, productos y *procesos* (2.61).

NOTA 3 Un objetivo se puede expresar de otras maneras, por ejemplo, como un resultado previsto, un propósito, un criterio operativo, un objetivo de *seguridad de la información* (2.33), o mediante el uso de términos con un significado similar (por ejemplo, finalidad o meta).

NOTA 4 En el contexto de *sistemas de gestión* (2.46) de la *seguridad de la información* (2.33), la organización establece los objetivos de *seguridad de la información* (2.33), en concordancia con la *política* (2.60) de *seguridad de la información* (2.33), para lograr resultados específicos.

2.57 organización:
Persona o grupo de personas que tienen sus propias funciones con responsabilidades, autoridades y relaciones para el logro de sus *objetivos* (2.56).

NOTA El concepto de organización incluye, pero no se limita a, empresarios unipersonales, empresas, corporaciones, firmas, autoridades, asociaciones, etc., en sí mismas, parcialmente o grupos de ellas, sean públicas o privadas.

2.58 contratar externamente (verbo):
Establecer un acuerdo mediante el cual una *organización* (2.57) externa realiza parte de una función o *proceso* (2.61) de una *organización* (2.57).

NOTA 1 Una organización externa está fuera del alcance del *sistema de gestión* (2.46), aunque la función o *proceso* (2.61) contratado externamente forme parte del alcance.

2.59 desempeño:
Resultado medible.

NOTA 1 El desempeño se puede relacionar con hallazgos cuantitativos o cualitativos.

NOTA 2 El desempeño se puede relacionar con la gestión de actividades, *procesos* (2.61), productos (incluidos servicios), sistemas u *organizaciones* (2.57).

2.60 política:
Intenciones y dirección de una *organización* (2.57), como las expresa formalmente su *alta dirección* (2.84).

2.61 proceso:
Conjunto de actividades interrelacionadas o que interactúan, que transforma elementos de entrada en elementos de salida.

2.62 fiabilidad:
Propiedad relativa a la consistencia en el comportamiento y en los resultados deseados.

2.63 requisito:
Necesidad o expectativa que está establecida, generalmente implícita u obligatoria.

NOTA 1 "Generalmente implícita" significa que es una costumbre o práctica común en la *organización* (2.57) y en las partes interesadas, que la necesidad o expectativa que se considera está implícita.

NOTA 2 Un requisito especificado es el que está declarado, por ejemplo, en *información documentada* (2.23).

2.64 riesgo residual:
Riesgo (2.68) remanente después del *tratamiento del riesgo* (2.79).

NOTA 1 El riesgo residual puede contener *riesgos* (2.68) no identificados.

NOTA 2 El riesgo residual también se puede conocer como "riesgo retenido".

2.65 revisión:
Actividad que se realiza para determinar la idoneidad, la adecuación y la *eficacia* (2.24) del tema estudiado para conseguir los *objetivos* (2.54) establecidos.

[Guía ISO 73:2009, 3.8.2.2, modificado – Se ha eliminado la NOTA 1]

2.66 objeto en revisión:
Elemento específico que está siendo revisado.

2.67 objetivo de la revisión:
Declaración que describe lo que se quiere lograr como resultado de una *revisión* (2.65).

2.68 riesgo:
Efecto de la incertidumbre sobre la consecución de los objetivos.

[Guía ISO 73:2009, 1.1, modificado]

NOTA 1 Un efecto es una desviación, positiva y/o negativa, respecto a lo previsto.

NOTA 2 La incertidumbre es el estado, incluso parcial, de deficiencia en la información relativa a la comprensión o al conocimiento de un *suceso* (2.25), de sus *consecuencias* (2.14) o de su *probabilidad* (2.45).

NOTA 3 Con frecuencia, el riesgo se caracteriza por referencia a *sucesos* (2.25) potenciales y a sus *consecuencias* (2.14) o una combinación de ambos.

NOTA 4 Con frecuencia, el riesgo se expresa en términos de combinación de las *consecuencias* (2.14) de un *suceso* (2.25) (incluyendo los cambios en las circunstancias) y de su *probabilidad* (2.45).

NOTA 5 En el contexto de *sistemas de gestión* (2.46) de la *seguridad de la información* (2.33), los riesgos de *seguridad de la información* (2.33) se pueden expresar como el efecto de la incertidumbre sobre los *objetivos* (2.56) de *seguridad de la información* (2.33).

NOTA 6 El riesgo de *seguridad de la información* (2.33) se relaciona con la posibilidad de que las *amenazas* (2.83) exploten *vulnerabilidades* (2.89) de un activo o grupo de activos de información y causen daño a una *organización* (2.57).

2.69 aceptación del riesgo:
Decisión informada en favor de tomar un *riesgo* (2.68) particular.

[Guía ISO 73:2009, 3.7.1.6]

NOTA 1 La aceptación del riesgo puede tener lugar sin que exista *tratamiento del riesgo* (2.79) o durante el *proceso* (2.61) de *tratamiento del riesgo* (2.79).

NOTA 2 Los *riesgos* (2.68) aceptados son objeto de *seguimiento* (2.52) y de *revisión* (2.65).

2.70 análisis del riesgo:
Proceso (2.61) que permite comprender la naturaleza del *riesgo* (2.68) y determinar el *nivel de riesgo* (2.44).

[Guía ISO 73:2009, 3.6.1]

NOTA 1 El análisis del riesgo proporciona las bases para la *evaluación del riesgo* (2.74) y para tomar las decisiones relativas al *tratamiento del riesgo* (2.79).

NOTA 2 El análisis del riesgo incluye la estimación del riesgo.

2.71 apreciación del riesgo:
Proceso (2.61) global que comprende la *identificación del riesgo* (2.75), el *análisis del riesgo* (2.70) y la *evaluación del riesgo* (2.74).

[Guía ISO 73:2009, 3.4.1]

2.72 comunicación y consulta del riesgo:
Procesos (2.61) iterativos y continuos que realiza una organización para proporcionar, compartir u obtener información y para establecer el diálogo con las *partes interesadas* (2.82), en relación con la gestión del *riesgo* (2.68).

NOTA 1 La información puede corresponder a la existencia, la naturaleza, la forma, la *probabilidad* (2.45), la importancia, la evaluación, la aceptabilidad y el tratamiento de la gestión del *riesgo* (2.68).

NOTA 2 La consulta constituye un *proceso* (2.51) de comunicación informada de doble sentido entre una *organización* (2.57) y sus *partes interesadas* (2.82), sobre una cuestión antes de tomar una decisión o determinar una orientación sobre dicha cuestión. La consulta es:

- un *proceso* (2.61) que impacta sobre una decisión a través de la influencia más que por la autoridad, y
- una contribución para una toma de decisión, y no una toma de decisión conjunta.

2.73 criterios de riesgo:
Términos de referencia respecto a los que se evalúa la importancia de un *riesgo* (2.68).

[Guía ISO 73:2009, 3.3.1.3]

NOTA 1 Los criterios de riesgo se basan en los objetivos de la organización, y en el *contexto externo* (2.27) e *interno* (2.42).

NOTA 2 Los criterios de riesgo se pueden obtener de normas, leyes, *políticas* (2.60) y otros *requisitos* (2.63).

2.74 evaluación del riesgo:
Proceso (2.61) de comparación de los resultados del *análisis de riesgo* (2.70) con los *criterios de riesgo* (2.73) para determinar si el *riesgo* (2.68) y/o su magnitud son aceptables o tolerables.

[Guía ISO 73:2009, 3.7.1]

NOTA La evaluación del riesgo ayuda a la toma de decisiones sobre el *tratamiento del riesgo* (2.79).

2.75 identificación del riesgo:
Proceso (2.61) que comprende la búsqueda, el reconocimiento y la descripción de los *riesgos* (2.68).

[Guía ISO 73:2009, 3.5.1]

NOTA 1 La identificación del riesgo implica la identificación de las fuentes de riesgo, los *sucesos* (2.25), sus causas y sus *consecuencias* (2.14) potenciales.

NOTA 2 La identificación del riesgo puede implicar datos históricos, análisis teóricos, opiniones informadas y de expertos, así como necesidades de las *partes interesadas* (2.82).

2.76 gestión del riesgo:
Actividades coordinadas para dirigir y controlar una *organización* (2.57) en lo relativo al *riesgo* (2.68).

[Guía ISO 73:2009, 2.1]

2.77 proceso de gestión del riesgo:
Aplicación sistemática de *políticas* (2.60), procedimientos y prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, e identificación, análisis, evaluación, tratamiento, seguimiento y revisión del *riesgo* (2.68).

[Guía ISO 73:2009, 3.1, modificado – Se ha añadido la NOTA 1]

NOTA La Norma ISO/IEC 27005 utiliza el término '*proceso*' (2.61) para describir la gestión integral del riesgo. Los elementos dentro del *proceso* (2.61) de *gestión del riesgo* (2.76) se denominan 'actividades'.

2.78 dueño del riesgo:
Persona o entidad que tiene la responsabilidad y autoridad para gestionar un *riesgo* (2.68).

[Guía ISO 73:2009, 3.5.1.5]

2.79 tratamiento del riesgo:
Proceso (2.61) destinado a modificar el *riesgo* (2.68).

[Guía ISO 73:2009, 3.8.1, modificado – "decisión" ha sido reemplazada por "elección" en la NOTA 1]

NOTA 1 El tratamiento del riesgo puede implicar lo siguiente:

- evitar el *riesgo* (2.68), decidiendo no iniciar o continuar con la actividad que motiva el *riesgo* (2.68),
- aceptar o aumentar el *riesgo* (2.68) con objeto de buscar una oportunidad,
- eliminar la fuente de *riesgo* (2.68),
- cambiar la *probabilidad* (2.45),
- cambiar las *consecuencias* (2.14),
- compartir el *riesgo* (2.68) con otra u otras partes [incluyendo los contratos y la financiación del riesgo],
- mantener el *riesgo* (2.68) en base a una decisión informada.

NOTA 2 Los tratamientos del riesgo que conducen a *consecuencias* (2.14) negativas, en ocasiones se citan como "mitigación del riesgo", "eliminación del riesgo", "prevención del riesgo" y "reducción del riesgo".

NOTA 3 El tratamiento del *riesgo* (2.68) puede originar nuevos riesgos o modificar los *riesgos* (2.68) existentes.

2.80 escala:
Conjunto ordenado de valores, continuo o discreto, o un conjunto de categorías a las que se asigna el *atributo* (2.4).

[ISO/IEC 15939:2007, 2.35, modificado]

NOTA El tipo de escala depende de la naturaleza de la relación entre los valores de la escala. Comúnmente se identifican cuatro tipos de escala de la siguiente manera:

- nominal: los valores de *medición* (2.48) son categorías,

- ordinal: los valores de *medición* (2.48) son categorías ordenadas,
- intervalo: los valores de las *mediciones* (2.48) se ajustan a rangos de valores cuantitativos del *atributo* (2.4),
- proporción: los valores de las *mediciones* (2.48) son relativos y proporcionales al valor de otro *atributo* (2.4), correspondiendo el valor cero al valor cero del atributo.

Estos son sólo ejemplos de tipos de escala.

2.81 norma de implementación de la seguridad:
Documento que especifica las formas autorizadas para satisfacer las necesidades de seguridad.

2.82 parte interesada:
Persona u *organización* (2.57) que puede afectar, estar afectada, o percibir que está afectada por una decisión o actividad.

[Guía ISO 73:2009, 3.2.1.1, modificado – Se ha eliminado la NOTA 1]

2.83 amenaza:
Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una *organización* (2.57).

2.84 alta dirección:
Persona o grupo de personas que dirigen y controlan una *organización* (2.57) al más alto nivel.

NOTA 1 La alta dirección tiene el poder para delegar autoridad y proporcionar recursos dentro de la *organización* (2.57).

NOTA 2 Si el alcance del *sistema de gestión* (2.46) comprende sólo una parte de una *organización* (2.57), entonces "alta dirección" se refiere a quienes dirigen y controlan esa parte de la *organización* (2.57).

2.85 entidad de confianza para la comunicación de información:
Organización (2.57) independiente que sustenta el intercambio de información dentro de un *colectivo que comparte información* (2.38).

2.86 unidad de medida:
Cantidad concreta, definida y adoptada por convenio, con la cual se comparan otras cantidades de la misma naturaleza a fin de expresar su magnitud en relación a dicha cantidad.

[ISO/IEC 15939:2007, 2.40, modificado]

2.87 validación:
Confirmación mediante la aportación de evidencia objetiva de que se han cumplido los *requisitos* (2.63) para una utilización o aplicación específica prevista.

[ISO 9000:2015, 3.8.12, modificado]

2.88 verificación:
Confirmación mediante la aportación de evidencia objetiva de que se han cumplido los *requisitos* (2.63) especificados.

[ISO 9000:2015, 3.8.4]

NOTA También podría llamarse prueba de conformidad.

2.89 vulnerabilidad:
Debilidad de un activo o de un *control* (2.16) que puede ser explotada por una o más *amenazas* (2.83).

3 Sistemas de gestión de la seguridad de la información

3.1 General

Las organizaciones de todo tipo y tamaño:

a) recogen, procesan, almacenan y transmiten información;

b) reconocen que la información y los procesos, sistemas, redes y personas relacionados con ella son activos importantes para el logro de los objetivos de la organización;

c) se enfrentan a una variedad de riesgos que puedan afectar el funcionamiento correcto de los activos; y

d) dirigen su exposición al riesgo mediante la implementación de controles de seguridad de la información.

Toda la información guardada y procesada por una organización está expuesta a ataques, errores, riesgos naturales (por ejemplo, inundaciones o incendios), etc. y está expuesta a vulnerabilidades inherentes en su uso. El término "seguridad de la información" generalmente se basa en el hecho de que la información se considera un activo que tiene valor y, como tal, requiere una protección adecuada contra la pérdida de su disponibilidad, confidencialidad e integridad. La habilitación de una información precisa y completa, y disponible de manera oportuna a las personas autorizadas es un catalizador de la eficiencia empresarial.

La protección de los activos de información mediante la definición, implementación, mantenimiento y mejora de la seguridad de la información de forma eficaz es esencial para permitir que una organización logre sus objetivos, y mantenga y mejore el cumplimiento de la legislación y su imagen. Estas actividades coordinadas dirigidas hacia la implementación de controles adecuados y el tratamiento de los riesgos inaceptables en seguridad de la información son generalmente conocidas como los elementos de gestión de la seguridad de la información.

Debido a que los riesgos asociados a la seguridad de la información y la eficacia de los controles cambian según las circunstancias, las organizaciones necesitan:

a) controlar y evaluar la eficacia de las medidas y procedimientos aplicados;

b) identificar los riesgos emergentes que deben tratarse; y

c) seleccionar, implementar y mejorar los controles según sea necesario.

Para relacionar y coordinar dichas actividades relativas a la seguridad de la información, cada organización necesita establecer su política y sus objetivos para la seguridad de la información, y lograr estos objetivos de manera efectiva mediante el uso de un sistema de gestión.

3.2 ¿Qué es un SGSI?

3.2.1 Información y principios generales

Un SGSI (Sistema de Gestión de la Seguridad de la Información) consiste en un conjunto de políticas, procedimientos, guías y sus recursos y actividades asociados, que son gestionados de manera colectiva por una organización. Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información de una organización para alcanzar los objetivos de negocio. Este enfoque está basado en una apreciación del riesgo y en los niveles de aceptación del riesgo de la organización diseñados para tratar y gestionar con eficacia los riesgos. El análisis de los requisitos para la protección de los activos de información y la aplicación de controles adecuados para garantizar la protección de estos activos de información, según sea necesario, contribuye a la exitosa implementación de un SGSI. Los siguientes principios fundamentales también pueden contribuir a la implementación exitosa de un SGSI:

a) la conciencia de la necesidad de seguridad de la información;

b) la asignación de responsabilidades en seguridad de la información;

c) la incorporación del compromiso de la Dirección y los intereses de las partes interesadas;

d) la mejora de los valores sociales;

e) apreciaciones de riesgos para determinar los controles adecuados para alcanzar niveles aceptables de riesgo;

f) la seguridad incorporada como un elemento esencial de los sistemas y redes de información;

g) la prevención y detección activas de incidentes de seguridad de la información;

h) el garantizar una aproximación exhaustiva a la gestión de la seguridad de la información; y

i) la evaluación continua de la seguridad de la información y la realización de modificaciones cuando corresponda.

3.2.2 La información

La información es un activo que, al igual que otros activos importantes del negocio, es esencial para el negocio de una organización y, por consiguiente necesita ser debidamente protegida. La información puede ser almacenada en muchas formas, incluyendo: formato digital (por ejemplo, ficheros almacenados en medios electrónicos u ópticos), formato material (por ejemplo, en papel), así como la información intangible que forma parte del conocimiento de los empleados. La información puede ser transmitida por diversos medios: mensajería, comunicación electrónica o verbal. Independientemente del formato o del medio por el cual se transmite la información, es necesaria siempre una protección adecuada.

La información de una organización depende de la tecnología de la información y de las comunicaciones. Esta tecnología es un elemento esencial en cualquier organización y ayuda a facilitar la creación, transformación, almacenamiento, transmisión, protección y destrucción de información. Cuando el entorno del negocio se amplía, y se vuelve global e interconectado, lo mismo ocurre con la obligación de proteger la información ya que esta información queda ahora sujeta a una variedad más amplia de amenazas y vulnerabilidades.

3.2.3 La seguridad de la información

La seguridad de la información asegura la confidencialidad, la disponibilidad y la integridad de la información. Con el objetivo de garantizar el éxito empresarial sostenido, así como su continuidad, y minimizar consecuencias de incidentes de seguridad de la información, la seguridad de la información conlleva la aplicación y la gestión de controles adecuados que implican la consideración de una amplia gama de amenazas.

La seguridad de la información se consigue mediante la implementación de un conjunto de controles aplicables, seleccionados a través del proceso de gestión de riesgos que se haya elegido y gestionado por medio de un SGSI, empleando políticas, procesos, procedimientos, estructuras organizativas, software y hardware para proteger los activos de información identificados. Estos controles necesitan ser especificados, implementados, monitorizados, revisados y mejorados cuando sea necesario, para garantizar que la seguridad y los objetivos de negocio y de seguridad específicos se cumplan. Estos controles de seguridad de la información deben integrarse de forma coherente con los procesos de negocio de una organización.

3.2.4 La gestión

La gestión implica actividades para dirigir, controlar y mejorar de manera continua la organización dentro de las estructuras adecuadas. Las actividades de gestión incluyen la acción, la forma, o la práctica de la organización, el manejo, dirección, supervisión y control de los recursos. Las estructuras de gestión se extienden desde una única persona en una organización pequeña hasta jerarquías de gestión compuestas por muchos individuos en las grandes organizaciones.

En términos de un SGSI, la gestión implica la supervisión y la toma de las decisiones necesarias para alcanzar los objetivos de negocio mediante la protección de los activos de información de la organización. La gestión de la seguridad de la información se expresa a través de la formulación y el uso de las políticas de seguridad de la información, normas, procedimientos y guías, que luego son aplicadas en toda la organización por parte de todos los individuos vinculados con la organización.

3.2.5 El sistema de gestión

Un sistema de gestión utiliza un marco de recursos para alcanzar los objetivos de una organización. El sistema de gestión incluye la estructura organizativa, las políticas, la planificación de actividades, responsabilidades, prácticas, procedimientos, procesos y recursos.

En términos de seguridad de la información, un sistema de gestión permite a una organización:

a) satisfacer los requisitos de seguridad de los clientes y otras partes interesadas;

b) mejorar los planes y actividades de la organización;

c) cumplir con los objetivos de seguridad de información de la organización;

d) cumplir con las regulaciones, leyes y obligaciones sectoriales; y

e) gestionar los activos de información de una manera organizada que facilita la mejora continua y la adaptación a las actuales metas de la organización y a su entorno.

3.3 El enfoque basado en procesos

Las organizaciones necesitan identificar y gestionar numerosas actividades con el fin de funcionar de manera eficaz y eficiente. Cualquier actividad que utilice recursos necesita gestionarse para permitir la transformación de entradas en salidas empleando un conjunto de actividades interrelacionadas o que interactúan; esto también se conoce como un proceso. La salida de un proceso puede ser directamente la entrada a otro proceso y, en general esta transformación se lleva a cabo en condiciones planificadas y controladas. La aplicación de un sistema de procesos dentro de una organización, junto con la identificación e interacciones de estos procesos, y su gestión, puede ser referida como un “enfoque basado en procesos".

3.4 ¿Por qué es importante un SGSI?

Como parte del SGSI de una organización, los riesgos asociados con los activos de información de una organización necesitan ser tratados. Lograr la seguridad de la información requiere la gestión del riesgo, y engloba los riesgos relacionados con amenazas físicas, humanas y tecnológicas asociados con todas las formas de información, ya sean internas o utilizadas por la organización.

Se espera que la adopción de un SGSI sea una decisión estratégica para una organización y es necesario que esta decisión se integre a la perfección, de una manera proporcional y actualizada de acuerdo con las necesidades de la organización.

El diseño e implementación del SGSI de una organización están influenciados por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos de negocio, los empleados y el tamaño y estructura de la organización. El diseño y operación de un SGSI necesita reflejar los intereses y requisitos de seguridad de la información de todas las partes interesadas de la organización, incluyendo clientes, proveedores, socios, accionistas y otros terceros pertinentes.

En un mundo interconectado, la información y sus procesos relacionados, los sistemas y las redes constituyen activos críticos del negocio. Las organizaciones y sus sistemas y redes de información se enfrentan a amenazas de seguridad provenientes de una amplia gama de fuentes, incluyendo el fraude asistido por ordenadores, espionaje, sabotaje, vandalismo, incendios e inundaciones. El daño a los sistemas y las redes de información causados por códigos maliciosos, la piratería informática, y los ataques de denegación de servicio cada vez son más comunes, más ambiciosos, y más sofisticados.

Un SGSI es importante tanto para empresas públicas como empresas del sector privado. En cualquier industria, un SGSI es un elemento facilitador que apoya el comercio electrónico y es esencial para las actividades de gestión de riesgos. La interconexión de las redes públicas y privadas y el hecho de compartir activos de información aumenta la dificultad de controlar el acceso y manejo de la información. Además, la distribución de dispositivos móviles con capacidad de almacenamiento que contienen activos de información puede debilitar la eficacia de los controles tradicionales. Cuando las organizaciones adoptan e implementan la familia de normas de SGSI, se puede demostrar a los socios del negocio y a otras partes interesadas la capacidad de aplicar, de forma coherente y mutuamente reconocible, los principios de la seguridad de la información.

La seguridad de la información no siempre se tiene en cuenta en el diseño y desarrollo de los sistemas de información. Además, la seguridad de la información es a menudo considerada como una solución técnica. Sin embargo, la seguridad que puede lograrse a través de medios técnicos es limitada, y puede ser ineficaz sin el apoyo de una gestión y unos procedimientos adecuados en el contexto de un SGSI. Integrar la seguridad en un sistema de información después de que se haya producido un hecho puede ser complejo y costoso. Un SGSI implica identificar qué controles están actualmente funcionando y requiere una planificación cuidadosa y la atención a los detalles. A modo de ejemplo, los controles de acceso, que pueden ser de carácter técnico (lógico), físico, administrativo (gestión) o una combinación de los anteriores, proporcionan un medio para garantizar que el acceso a los activos de información este autorizado y restringido en función de la organización y de sus requisitos de seguridad.

La implementación exitosa de un SGSI es importante para proteger los activos de información que permita a una organización:

a) lograr una mayor confianza en que sus activos de información están adecuadamente protegidos contra los riesgos de seguridad de la información de forma continua;

b) mantener un marco estructurado y global para identificar y apreciar los riesgos de seguridad de la información, seleccionar y aplicar los correspondientes controles, y medir y mejorar su eficacia;

c) mejorar de manera continua su entorno de seguridad; y

d) lograr un cumplimiento eficaz de las obligaciones legales y reglamentarias.

3.5 Establecer, supervisar, mantener y mejorar el SGSI

3.5.1 Información general

Una organización necesita llevar a cabo los siguientes pasos en el establecimiento, supervisión, mantenimiento y mejora de su SGSI:

a) identificar los activos de información y sus correspondientes requisitos de seguridad (véase 3.5.2);

b) apreciar los riesgos de seguridad de la información (véase 3.5.3) y tratar los riesgos de seguridad de la información (véase 3.5.4);

c) seleccionar e implementar los controles pertinentes para gestionar los riesgos inaceptables (véase 3.5.5);

d) supervisar, mantener y mejorar la eficacia de los controles de seguridad asociados con los activos de información de la organización (véase 3.5.6).

Para garantizar que el SGSI esté protegiendo eficazmente los activos de información de la organización de forma permanente, es necesario que se repitan continuamente los pasos (a) a (d) para identificar cambios en los riesgos, o en las estrategias de la organización, o en los objetivos de negocio.

3.5.2 Identificar los requisitos de seguridad de la información

Dentro de la estrategia general y los objetivos de negocio de la organización, de su tamaño y de su situación geográfica, los requisitos de seguridad de la información pueden ser identificados a través del conocimiento y entendimiento de los siguientes:

a) los activos de información identificados y su valor;

b) las necesidades de negocio para el tratamiento y almacenamiento de la información;

c) las medidas legislativas, reglamentarias y los requisitos contractuales.

Llevar a cabo una metódica apreciación de los riesgos asociados con los activos de información de la organización implica un análisis de las amenazas a los activos de información, los factores de vulnerabilidad ante la probabilidad de materialización de una amenaza a los activos de información, y el impacto potencial de cualquier incidente de seguridad de la información sobre los activos de información. Se espera que el gasto incurrido en los correspondientes controles de seguridad sea proporcionado con respecto al impacto percibido por las organizaciones en caso de materialización del riesgo.

3.5.3 Apreciación de los riesgos de seguridad de la información

Gestionar los riesgos de seguridad de información requiere unos métodos adecuados de apreciación y de tratamiento del riesgo que pueden incluir una estimación de los costes y beneficios, de los requisitos legales, de los aspectos sociales, económicos y ambientales, de las preocupaciones de las partes interesadas, las prioridades, y de otros datos y variables según el caso.

La apreciación de los riesgos debería identificar, cuantificar y priorizar riesgos en base a los correspondientes criterios de aceptación de riesgos y objetivos de la organización. Los resultados deberían orientar y determinar las decisiones apropiadas para definir las acciones y prioridades para la gestión de los riesgos de seguridad de información, y para la aplicación de controles pertinentes de seguridad para proteger contra estos riesgos.

La apreciación de riesgos debería incluir un enfoque sistemático de estimación de la magnitud de los riesgos (análisis de riesgos) y el proceso de comparación de los riesgos estimados con respecto a los criterios de riesgos para poder determinar la importancia de los riesgos (evaluación del riesgo).

La apreciación de riesgos debería modelarse de manera periódica para contemplar los cambios en los requisitos de seguridad de la información y en la situación del riesgo, por ejemplo, en los activos, amenazas, vulnerabilidades, impactos, en la evaluación del riesgo, y cuando ocurra un cambio significativo. Esta apreciación de riegos debería ser llevada a cabo de una manera metódica capaz de producir resultados comparables y reproducibles.

La apreciación de los riesgos de seguridad de la información debería tener claramente definido un alcance para poder ser eficaz y debería incluir interrelaciones con apreciaciones de riesgos de otras áreas, si es aplicable.

La Norma ISO/IEC 27005 proporciona directrices para la gestión de riesgos de seguridad de la información, incluyendo asesoramiento sobre la apreciación del riesgo, el tratamiento del riesgo, la aceptación del riesgo, la comunicación del riesgo, el seguimiento y supervisión del riesgo y la revisión del riesgo. Se incluyen también ejemplos de metodologías de apreciación del riego.

3.5.4 Tratamiento de los riesgos de seguridad de la información

Antes de abordar el tratamiento de un riesgo, la organización debería decidir los criterios para determinar cuándo se pueden o no aceptar los riesgos. Se pueden aceptar riesgos si, por ejemplo, se aprecia que el riesgo es bajo o bien que el coste de su tratamiento, en caso de producirse, es asumible para la organización. Dichas decisiones deberían quedar registradas.

Para cada uno de los riesgos identificados después de llevar a cabo la apreciación de riesgos, es necesario tomar una decisión sobre su tratamiento.

Las posibles opciones para el tratamiento de los riesgos incluyen las siguientes:

a) la aplicación de los controles apropiados para reducir los riesgos;

b) el conocimiento y aceptación objetiva de los riesgos, siempre que se satisfagan de una manera clara la política de la organización y los criterios de aceptación del riesgo;

c) la evitación de los riesgos, no permitiendo aquellas acciones que podrían provocar la ocurrencia del riesgo;

d) la compartición de los riesgos con terceras partes, por ejemplo con entidades aseguradoras o bien con los proveedores.

Para aquellos riesgos para los que la decisión de tratamiento es la aplicación de los correspondientes controles, dichos controles deberían ser seleccionados e implementados.

3.5.5 Seleccionar e implementar los controles

Una vez que hayan sido identificados los requisitos de seguridad de la información (véase 3.5.2), y que hayan sido determinados y apreciados los riesgos de seguridad de la información asociados a los activos de información identificados (véase 3.5.3), y las decisiones que hayan sido tomadas para el tratamiento de los riesgos de seguridad de la información (véase 3.5.4)), deben seleccionarse e implementarse los controles adecuados para reducir los riesgos.

Los controles deberían asegurar que los riesgos de la seguridad de la información se reducen a un nivel aceptable para la organización teniendo en cuenta lo siguiente:

a) los requisitos y obligaciones derivados de la regulación y legislación nacional e internacional;

b) objetivos de la organización;

c) requisitos y obligaciones operacionales;

d) el coste derivado de la implantación y operación de las medidas de reducción de los riesgos, y su mantenimiento en proporción a los requisitos y obligaciones de la organización;

e) sus objetivos para controlar, evaluar y mejorar la eficiencia y eficacia de los controles de seguridad de la información como apoyo a los objetivos de la organización. La selección e implantación de los controles debería quedar documentada dentro de la declaración de aplicabilidad para ayudar al cumplimiento de los requisitos;

f) la necesidad de equilibrar la inversión en la implantación y operación de los controles contra las posibles pérdidas resultantes de la ocurrencia de incidentes de seguridad de la información.

Los controles especificados en la Norma ISO/IEC 27002 se reconocen como las mejores prácticas aplicables para la mayoría de las organizaciones y son fácilmente adaptables a organizaciones de diferente tamaño y grado de complejidad. Otras normas de la familia de normas de SGSI proporcionan directrices para la selección y aplicación de los controles de la Norma ISO/IEC 27002 para el sistema de gestión de la seguridad de la información.

Los controles de seguridad de la información deberían considerarse en la fase de diseño y en la especificación de los requisitos de los sistemas y proyectos. El no hacerlo así, puede ocasionar costes adicionales y una menor eficacia de la solución, y puede ser, en el peor de los casos, imposible el conseguir una adecuada seguridad. Los controles pueden ser seleccionados de la Norma ISO/IEC 27002, o de otros conjuntos de controles, o bien pueden diseñarse nuevos controles para cumplir con necesidades específicas de la organización. Es necesario llamar la atención sobre el hecho de que algunos controles pueden no ser aplicables a todos los sistemas o entornos de información, y pueden por tanto no ser practicables para todas las organizaciones.

En ocasiones, lleva tiempo implementar un conjunto de controles seleccionado, y durante ese tiempo el nivel de riesgo puede hacerse mayor que el nivel tolerado en el largo plazo. Los criterios de riesgo deberían cubrir la tolerabilidad de los riesgos en el corto plazo, mientras son implementados los controles de seguridad. Las partes interesadas deberían estar informadas de los niveles de riesgo que se estiman o anticipan en los diferentes espacios de tiempo durante el periodo de implementación progresiva de los controles.

Se debería tener en cuenta que ningún conjunto de controles puede conseguir una completa seguridad de la información. Se deberían implantar acciones de gestión adicionales para controlar, evaluar y mejorar la eficiencia y eficacia de los controles para ayudar a alcanzar los objetivos de la organización.

La selección e implantación de los controles debería quedar documentada dentro de la declaración de aplicabilidad para ayudar al cumplimiento de los requisitos.

3.5.6 Supervisar, revisar, mantener y mejorar la eficacia de los SGSI

Una organización necesita mantener y mejorar el SGSI mediante el seguimiento, la supervisión y la evaluación del desempeño respecto a la política y los objetivos de la organización, y notificar los resultados a la dirección para su revisión. Esta revisión del SGSI comprobará que el SGSI incluye controles específicos que son adecuados para tratar los riesgos que están dentro del alcance del SGSI. Además proporcionará evidencias de verificación y trazabilidad de las acciones correctivas, preventivas y de mejora sobre la base de los registros de las áreas supervisadas.

3.5.7 Mejora continua

El objetivo de la mejora continua de un SGSI es aumentar la probabilidad de conseguir los objetivos relativos a la preservación de la confidencialidad, disponibilidad e integridad de la información. El núcleo de la mejora continua es descubrir oportunidades para la mejora y no asumir que las actividades de gestión existentes son suficientemente buenas o tan buenas como podrían ser.

Las acciones para la mejora incluyen las siguientes:

a) análisis y evaluación de la situación existente para identificar áreas de mejora;

b) establecimiento de objetivos para la mejora;

c) búsqueda de posibles soluciones para conseguir los objetivos;

d) evaluación de dichas soluciones y selección de las mismas;

e) implementación de la solución seleccionada;

f) medición, verificación, análisis y evaluación de los resultados de la implementación para determinar que los objetivos se han cumplido;

g) formalización de los cambios.

Los resultados son revisados, según sea necesario, para determinar oportunidades adicionales de mejora. En este sentido, la mejora es una actividad continua, es decir, las acciones se repiten con frecuencia. La respuesta de los clientes y de otras partes interesadas, las auditorías y la revisión del sistema de gestión de la seguridad de la información, pueden también ser utilizadas para identificar oportunidades de mejora.

3.6 Factores críticos de éxito de un SGSI

Un gran número de factores son fundamentales para la implementación exitosa de un SGSI que permita a una organización cumplir con sus objetivos de negocio. Algunos ejemplos de factores críticos de éxito son los siguientes:

a) que la política, los objetivos y actividades de seguridad de la información estén alineadas con los objetivos;

b) un enfoque y un marco para el diseño, ejecución, seguimiento, mantenimiento y mejora de la seguridad de la información en consonancia con la cultura de la organización;

c) el apoyo visible y el compromiso de todos los niveles de la Dirección, especialmente de la alta Dirección;

d) el conocimiento y entendimiento de los requisitos de protección de los activos de información obtenido mediante la aplicación de la gestión del riesgo de la seguridad de la información (véase la Norma ISO/IEC 27005);

e) un programa efectivo de concienciación, formación y educación sobre seguridad de la información, informando a todos los empleados y otras partes pertinentes de sus obligaciones en seguridad de la información establecidas en las políticas de seguridad de la información, normas, etc., y motivarlos a actuar en consecuencia;

f) un proceso efectivo de gestión de incidentes de seguridad de la información;

g) un enfoque efectivo de gestión de la continuidad del negocio;

h) un sistema de medición utilizado para evaluar el desempeño en la gestión de la seguridad de la información y para proporcionar sugerencias de mejora.

Un SGSI aumenta la probabilidad de que una organización alcance de forma coherente los factores críticos de éxito para proteger sus activos de información.

3.7 Beneficios de la familia de normas de SGSI

Los beneficios de implementar un SGSI principalmente consisten en una reducción de los riesgos asociados a la seguridad de la información (es decir, reduciendo la probabilidad y/o el impacto causado por los incidentes de seguridad de la información). De una forma más específica, los beneficios que para una organización produce la adopción exitosa de la familia de normas SGSI son los siguientes:

a) un apoyo al proceso de especificar, implementar, operar y mantener un SGSI, global, eficiente en costes, integrado y alineado que satisfaga las necesidades de la organización en diferentes operaciones y lugares;

b) una ayuda para la dirección en la estructuración de su enfoque hacia la gestión de la seguridad de la información, en el contexto de la gestión y gobierno del riesgo corporativo, incluidas las acciones de educación y formación en una gestión holística de la seguridad de la información a los propietarios del negocio y del sistema;

c) la promoción de buenas prácticas de seguridad de la información, aceptadas a nivel mundial, de una manera no preceptiva, dando a las organizaciones la flexibilidad para adoptar y mejorar los controles aplicables, respetando sus circunstancias específicas y para mantenerlos de cara a futuros cambios internos y externos; y

d) disponer de un lenguaje común y una base conceptual para la seguridad de la información, haciendo más fácil confiar a los socios de un negocio si este es conforme a un SGSI, especialmente si requieren la certificación conforme a la Norma ISO/IEC 27001 por un organismo de certificación acreditado;

e) aumentar la confianza en la organización por las partes interesadas;

f) satisfacer necesidades y expectativas sociales;

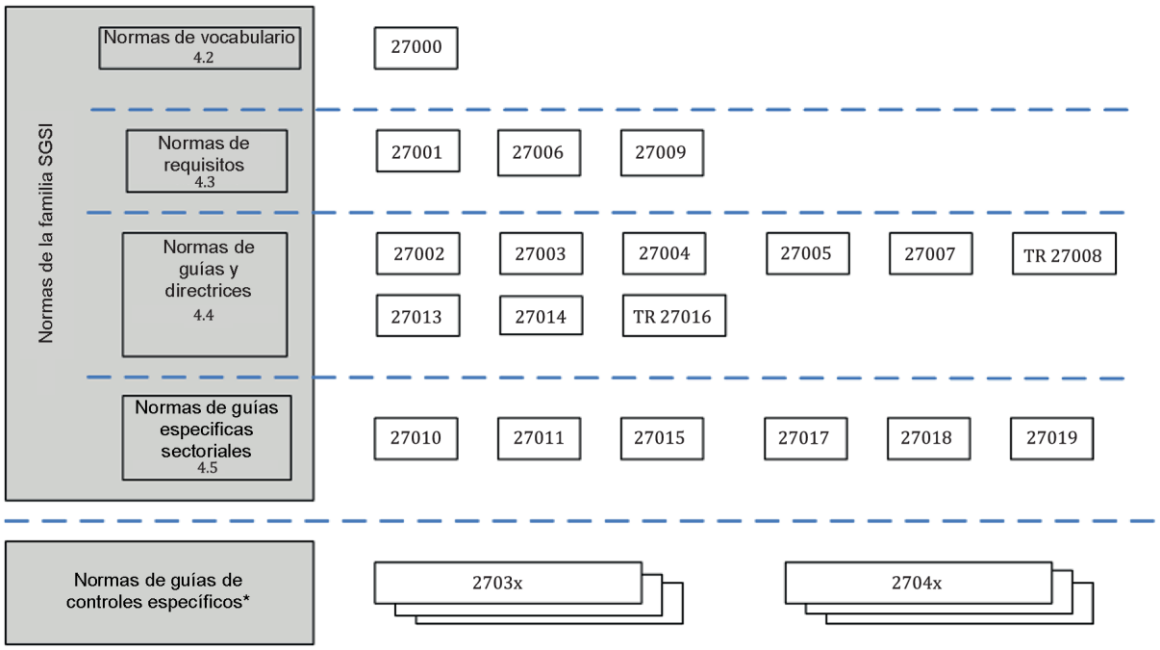
g) una más eficaz gestión desde un punto de vista económico de las inversiones en seguridad de la información.

4 La familia de normas de SGSI

4.1 Información general

La familia de normas SGSI consiste en una serie de normas relacionadas entre sí, ya publicadas o en preparación, y que contiene una serie de importantes componentes estructurales. Estos componentes se centran en normas para describir las especificaciones de un SGSI (ISO/IEC 27001), los requisitos para los organismos de certificación (ISO/IEC 27006) que certifiquen el cumplimiento con la Norma ISO/IEC 27001, y un marco de requisitos adicionales para implementaciones sectoriales específicas del SGSI (ISO/IEC 27009). Otras normas ofrecen guías para los diversos aspectos de la implementación de un SGSI, directrices para abordar un proceso genérico, así como directrices sectoriales específicas.

Las relaciones entre las normas de la familia SGSI se ilustran en la figura 1.



* fuera del campo de aplicación de esta norma internacional

Figura 1 – Relaciones entre las normas de la familia SGSI

Cada grupo de normas de la familia de SGSI se describe indicando su tipo (o rol) dentro de la familia de SGSI y su número de referencia. Los apartados a los que esto aplica son:

a) normas que describen una visión general y la terminología (véase 4.2);

b) normas que especifican los requisitos (véase 4.3);

c) las normas que describen guías o directrices generales (véase 4.4); o

d) normas que describen guías o directrices específicas sectoriales (ver 4.5).

4.2 Normas que describen una visión general y la terminología

4.2.1 ISO/IEC 27000 (esta norma internacional)

Tecnologías de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Visión de conjunto y vocabulario.

Ámbito de aplicación: Esta norma internacional proporciona a organizaciones y personas:

a) una visión general de la familia de las normas SGSI;

b) una introducción a los sistemas de gestión de la seguridad de la información; y

c) los términos y las definiciones utilizadas en toda la familia de las normas de SGSI.

Objeto: Esta norma internacional describe los fundamentos de los sistemas de gestión de la seguridad de la información, que constituyen el objeto de la familia de las normas de SGSI, y define los términos relacionados.

4.3 Normas que especifican los requisitos

4.3.1 ISO/IEC 27001

Tecnologías de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.

Ámbito de aplicación: Esta norma internacional especifica los requisitos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar el Sistema de Gestión de la Seguridad de la Información (SGSI) en el marco de los riesgos de negocio generales de la organización. Establece requisitos para la aplicación de los controles de seguridad adaptados a las necesidades de las organizaciones individuales o partes de la misma. Esta norma internacional es universal para todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin ánimo de lucro).

Objeto: La Norma ISO/IEC 27001 establece los requisitos normativos para el desarrollo y operación de un SGSI, incluyendo un conjunto de controles para el control y mitigación de los riesgos asociados con los activos de información que la organización trata de proteger mediante la operación de su SGSI. Las organizaciones que implementan un SGSI pueden hacer que se audite y certifique su conformidad. Los objetivos de control y controles del anexo A de la Norma ISO/IEC 27001 deben ser seleccionados en función de las necesidades, durante el proceso del SGSI para satisfacer los requisitos identificados. Los objetivos de control y controles que se enumeran en la tabla A.1 de la Norma ISO/IEC 27001 proceden directamente y están alineados con los que se enumeran en los capítulos 5 a 15 de la Norma ISO/IEC 27002.

4.3.2 ISO/IEC 27006

Tecnologías de la información. Técnicas de seguridad. Requisitos para entidades que auditan y certifican Sistemas de Gestión de la Seguridad de la Información (SGSI).

Ámbito de aplicación: Esta norma internacional especifica los requisitos y proporciona las directrices que han de cumplir las entidades que auditan y certifican un SGSI según la Norma ISO/IEC 27001, además de los requisitos contenidos en la Norma ISO/IEC 17021. Su intención principal es servir de apoyo para la acreditación de organismos de certificación que proporcionan servicios de certificación de SGSI según la Norma ISO/IEC 27001.

Objeto: La Norma ISO/IEC 27006 complementa a la Norma ISO/IEC 17021 al ofrecer los requisitos para que las organizaciones de certificación sean acreditadas de manera que éstas provean certificaciones de conformidad consistentes frente a los requisitos especificados en la Norma ISO/IEC 27001.

4.4 Normas que describen guías o directrices generales

4.4.1 ISO/IEC 27002

Tecnologías de la información. Técnicas de seguridad. Código de práctica para los controles de seguridad de la información.

Ámbito de aplicación: Esta norma internacional proporciona una lista de objetivos de control comúnmente aceptados así como las mejores prácticas en controles de seguridad que deben utilizarse como guía de aplicación para su selección e implementación para lograr la seguridad de la información.

Objeto: La Norma ISO/IEC 27002 proporciona directrices para la implementación de los controles de seguridad de la información. En concreto, los capítulos 5 a 18 proporcionan asesoramiento y orientación específicos para la puesta en marcha de las mejores prácticas en la implementación de los controles especificados en los capítulos A.5 a A.18 del anexo A de la Norma ISO/IEC 27001.

4.4.2 ISO/IEC 27003

Tecnología de la información. Técnicas de seguridad. Guía para la implementación de los Sistemas de Gestión de la Seguridad de la Información (SGSI).

Ámbito de aplicación: Esta norma internacional proporciona orientación para la implementación práctica e información adicional para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un SGSI según la Norma ISO/IEC 27001.

Objeto: La Norma ISO/IEC 27003 proporciona un enfoque basado en procesos orientado a la implementación con éxito del SGSI según la Norma ISO/IEC 27001.

4.4.3 ISO/IEC 27004

Tecnología de la información. Técnicas de seguridad. Gestión de Seguridad de la Información. Métricas.

Ámbito de aplicación: Esta norma internacional proporciona orientación y asesoramiento sobre el desarrollo y uso de las métricas con el fin de evaluar la eficacia del SGSI, de los objetivos de los controles y controles usados para aplicar y administrar la seguridad de la información, tal como se especifica en la Norma ISO/IEC 27001.

Objeto: La Norma ISO/IEC 27004 proporciona un marco de métricas que permite una evaluación de la eficacia del SGSI de acuerdo con la Norma ISO/IEC 27001.

4.4.4 ISO/IEC 27005

Tecnologías de la información. Técnicas de seguridad. Gestión de riesgos de seguridad de la información.

Ámbito de aplicación: Esta norma internacional proporciona directrices para la gestión de riesgos de seguridad de la información. El enfoque descrito en esta norma internacional apoya los conceptos generales que se especifican en la Norma ISO/IEC 27001.

Objeto: La Norma ISO/IEC 27005 proporciona directrices sobre la aplicación de un enfoque de gestión de riesgos orientado a procesos para ayudar en la aplicación de manera satisfactoria y al cumplimiento de los requisitos de gestión de riesgos de seguridad de la Norma ISO/IEC 27001.

4.4.5 ISO/IEC 27007

Tecnologías de la información. Técnicas de seguridad. Guía para la auditoría de los Sistemas de Gestión de la Seguridad de la Información (SGSI).

Ámbito de aplicación: Esta norma internacional ofrece orientación sobre la realización de auditorías de SGSI, así como sobre la competencia de los auditores del sistema de gestión de la seguridad de la información, además de las directrices contenidas en la Norma ISO 19011, que es aplicable a los sistemas de gestión en general.

Objeto: La Norma ISO/IEC 27007 proporciona directrices a las organizaciones que tienen que realizar auditorías internas o externas de un SGSI así como directrices para gestionar un programa de auditoría de SGSI según los requisitos especificados en la Norma ISO/IEC 27001.

4.4.6 ISO/IEC 27008

Tecnologías de la información. Técnicas de seguridad. Guía para los auditores de controles de seguridad de la información.

Ámbito de aplicación: Este informe técnico proporciona directrices sobre la revisión de la implementación y operación de controles incluyendo la comprobación de la conformidad técnica de los controles del sistema de información, y de la conformidad con las normas de seguridad de la información establecidas en una organización.

Objeto: Este informe técnico proporciona un enfoque de los controles de seguridad de la información, incluyendo la conformidad técnica con la implementación de la norma de seguridad de la información que se haya establecido en la organización. Este informe no pretende ser una guía específica de la conformidad respecto a mediciones, apreciación del riesgo o auditoría del SGSI como se especifica respectivamente en las Normas ISO/IEC 27004, ISO/IEC 27005 o ISO/IEC 27007. Tampoco está dirigido a la auditoría de los sistemas de gestión.

4.4.7 ISO/IEC 27013

Tecnologías de la información. Técnicas de seguridad. Guía para la implementación integrada de ISO/IEC 27001 e ISO/IEC 20000-1.

Ámbito de aplicación: Esta norma internacional proporcionará directrices para la implementación integrada de las Normas ISO/IEC 27001 e ISO/IEC 20000-1 para las organizaciones que tengan intención de:

a) implementar la Norma ISO/IEC 27001 cuando ya tienen implementada la Norma ISO/IEC 20000-1, o viceversa;

b) implementar conjuntamente las Normas ISO/IEC 27001 e ISO/IEC 20000-1;

c) integrar las implementaciones existentes de los sistemas de gestión de ISO/IEC 27001 e ISO/IEC 20000-1.

Esta norma Internacional se enfoca exclusivamente en la implementación integrada de un sistema de gestión de la seguridad de la información (SGSI) según se especifica en la Norma ISO/IEC 27001 y un sistema de gestión de servicios (SGS) según se especifica en la Norma ISO/IEC 20000-1.

Objeto: Proporcionar a las organizaciones un mejor entendimiento de las características, similitudes y diferencias entre las Normas ISO/IEC 27001 e ISO/IEC 20000-1 para ayudar en la planificación de un sistema integrado de gestión conforme a ambas normas internacionales.

4.4.8 ISO/IEC 27014

Tecnologías de la información. Técnicas de seguridad. Gobernanza de la seguridad de la información.

Ámbito de aplicación: Esta norma internacional proporcionará directrices sobre los principios y procesos para el gobierno de la seguridad de la información, mediante las cuales las organizaciones pueden evaluar, dirigir y controlar la gestión de la seguridad de la información.

Objeto: La seguridad de la información se ha convertido en un asunto clave para las organizaciones. No solo han aumentado los requisitos regulatorios, sino que el fallo de las medidas de seguridad en las organizaciones puede tener un impacto directo en la reputación de una organización. Por ello, se requiere a los órganos de gobierno, como parte de sus responsabilidades de gobierno, el tener una cada vez mayor vigilancia de la seguridad de la información para asegurar que se consiguen los objetivos de la organización.

4.4.9 ISO/IEC TR 27016

Tecnologías de la información. Técnicas de seguridad. Gestión de seguridad de la información. Economía organizacional.

Ámbito de aplicación: Este informe técnico proporcionará una metodología que permita a las organizaciones un mejor entendimiento desde un punto de vista económico, de cómo valorar de manera precisa los activos de información identificados, valorar los riegos potenciales para dichos activos, apreciar el valor que los controles de protección de la información proporcionan a dicho activos y determinar el nivel óptimo de recursos a aplicar para proporcionar seguridad a los activos de información.

Objeto: Este informe técnico complementará la familia de normas de SGSI, proporcionando un punto de vista económico a la protección de los activos de información de una organización en el contexto del entorno social en el que opera la organización y proporcionando directrices de cómo aplicar criterios de economía organizacional a la seguridad de la información a través del uso de modelos y ejemplos.

4.5 Normas que describen guías específicas sectoriales

4.5.1 ISO/IEC 27010

Tecnologías de la información. Técnicas de seguridad. Gestión de seguridad de la información en comunicaciones intersectoriales e interorganizacionales.

Ámbito de aplicación: Esta norma internacional proporciona directrices adicionales a las dadas en la familia de normas ISO/IEC 27000 para la implementación de la gestión de la seguridad en entornos donde diferentes comunidades comparten información, y proporciona controles y directrices específicos relativos al comienzo, implementación, mantenimiento y mejora de la seguridad de la información para las comunicaciones inter sectoriales e inter organizacionales.

Objeto: Esta norma internacional se aplica a todo tipo de intercambio o compartición de información sensible, ya sea de ámbito público o privado, a nivel nacional o internacional, dentro del mismo sector industrial o de mercado, o entre diferentes sectores. En particular, es aplicable a los intercambios y compartición de información relativa a la provisión, mantenimiento y protección de una infraestructura crítica de un estado o de una organización.

4.5.2 ISO/IEC 27011

Tecnologías de la información. Técnicas de seguridad. Guía para la gestión de seguridad de la información para las organizaciones de telecomunicaciones basada en la Norma ISO/IEC 27002.

Ámbito de aplicación: Esta norma internacional proporciona directrices de apoyo a la aplicación de los controles de Seguridad de la Información en las organizaciones de telecomunicaciones.

Objeto: la Norma ISO/IEC 27011 permite a las organizaciones de telecomunicaciones el cumplimiento de los requisitos básicos de gestión de seguridad de la información de confidencialidad, integridad, disponibilidad y cualquier otra propiedad de seguridad relevante.

4.5.3 ISO/IEC TR 27015

Tecnologías de la información. Técnicas de seguridad. Guía para la gestión de seguridad de la información para servicios financieros.

Ámbito de aplicación: Este informe técnico proporciona directrices adicionales a las dadas en la familia de Normas ISO/IEC 27000, para el inicio, implementación, mantenimiento y mejora de la seguridad de la información en organizaciones que proveen servicios financieros.

Objeto: Este informe técnico es un suplemento especializado de las Normas ISO/IEC 27001 e ISO/IEC 27002 para su uso en organizaciones que prestan servicios financieros, con objeto de servir de apoyo a:

a) el inicio, implementación, mantenimiento, y mejora de un sistema de gestión de la seguridad de la información basado en la Norma ISO/IEC 27001;

b) el diseño e implementación de los controles definidos en la Norma ISO/IEC 27002 o en este informe técnico.

4.5.4 ISO/IEC 27017

Tecnologías de la información. Técnicas de seguridad. Código de práctica para los controles de seguridad de la información basado en la Norma ISO/IEC 27002 para servicios en la nube (cloud services).

Ámbito de aplicación: la Norma ISO/IEC 27017 proporciona directrices para los controles de seguridad de la información aplicables a la prestación y utilización de servicios en la nube, proporcionando:

– guía de implementación adicional para los controles relevantes especificados en ISO/IEC 27002;

– controles adicionales con guías de implementación que se relacionan específicamente con los servicios en la nube.

Objeto: Esta Norma Internacional proporciona controles y guía de implementación tanto para los proveedores de servicios en la nube como para los clientes de servicios en la nube.

4.5.5 ISO/IEC 27018

Tecnologías de la información. Técnicas de seguridad. Código de práctica para la protección de información de identificación personal (PII) en nubes públicas que actúan como procesadores de PII.

Ámbito de aplicación: La Norma ISO/IEC 27018 establece objetivos de control, controles y directrices comúnmente aceptados para implementar medidas para proteger la información de identificación personal (PII) de acuerdo con los principios de privacidad de la Norma ISO/IEC 29100 para el entorno de computación en nube pública (cloud computing).

Objeto: Esta norma internacional es aplicable a organizaciones, incluidas empresas públicas y privadas, entidades gubernamentales y organizaciones sin fines de lucro, que proporcionan servicios de procesamiento de información como procesadores de PII a través de computación en la nube (cloud computing) bajo contrato con otras organizaciones. Las directrices de esta Norma Internacional también pueden ser relevantes para las organizaciones que actúan como controladores de PII; sin embargo, los controladores de PII pueden estar sujetos a legislaciones, regulaciones y obligaciones adicionales de protección de PII, que no se aplican a los procesadores de PII, y estos no están cubiertos en esta Norma Internacional.

4.5.6 ISO/IEC TR 27019

Tecnologías de la información. Técnicas de seguridad. Directrices de gestión de seguridad de la información basadas en ISO/IEC 27002 para sistemas de control de procesos específicos de la industria de servicios públicos de energía.

Ámbito de aplicación: La Norma ISO/IEC TR 27019 proporciona directrices sobre los controles de seguridad de la información a ser implementadas en los sistemas de control de procesos utilizados por la industria de servicios públicos de energía para controlar y monitorear la generación, transmisión, almacenamiento y distribución de energía eléctrica, gas y calor en combinación con el control de procesos de soporte.

- la tecnología de control, supervisión y automatización de procesos central y distribuida, respaldada por TI, así como los sistemas de TI utilizados para su funcionamiento, como los dispositivos de programación y parametrización;

- controladores digitales y componentes de automatización, como dispositivos de control y de campo o controladores lógicos programables (PLC), incluidos sensores digitales y elementos de actuador;

- todos los sistemas informáticos de soporte adicionales utilizados en el dominio de control de procesos, por ejemplo, para tareas de visualización de datos complementarias y para fines de control, monitoreo, archivo de datos y documentación;

- la tecnología de comunicaciones general utilizada en el dominio de control de procesos, por ejemplo, redes, telemetría, aplicaciones de telecontrol y tecnología de control remoto;

- dispositivos de medida y medición digitales, por ejemplo, para medir el consumo de energía, la generación o los valores de emisión;

- los sistemas de protección y de seguridad digital, por ejemplo, relés de protección o PLC de seguridad;

- componentes distribuidos de futuros entornos de redes inteligentes (smart grid);

- todos los software, firmware y aplicaciones instalados en los sistemas anteriormente mencionados.

Objeto: Además de los objetivos y medidas de seguridad que se establecen en la Norma ISO/IEC 27002, este Informe Técnico proporciona directrices para los sistemas utilizados por las empresas de servicios públicos de energía y los proveedores de energía en los controles de seguridad de la información que abordan otros requisitos especiales.

4.5.7 ISO 27799

Informática sanitaria. Gestión de seguridad de información en sanidad utilizando la Norma ISO/IEC 27002.

Ámbito de aplicación: Esta norma internacional proporciona directrices de apoyo a la aplicación de un Sistema de Gestión de la Seguridad de la Información (SGSI) en las organizaciones del ámbito sanitario.

Objeto: la Norma ISO/IEC 27799 proporciona a las organizaciones sanitarias una adaptación de la Norma ISO/IEC 27002 con guías específicas para el sector de sanidad y que son adicionales a las directrices proporcionadas para el cumplimiento de los requisitos del anexo A de la Norma ISO/IEC 27001.

Anexo A (Informativo)

Formas verbales para la expresión de las disposiciones

Nadie está obligado a aplicar las normas de la familia de normas de SGSI. Sin embargo esta obligación puede venir impuesta, por ejemplo, por vía legislativa, regulatoria o por un contrato entre partes. Con el fin de poder solicitar el cumplimiento de un documento, el usuario necesita ser capaz de identificar los requisitos necesarios que debe cumplir. El usuario también tiene que ser capaz de distinguir estos requisitos de las recomendaciones de otras normas donde hay una cierta libertad de elección.

La siguiente tabla aclara de qué manera un documento de la familia de normas de SGSI debe ser interpretado según las expresiones verbales utilizadas, es decir diferenciando aquellas que expresan requisitos o recomendaciones.

La tabla está basada en las provisiones de las Directivas de ISO/IEC, parte 2:2011, *Reglas para la estructura y elaboración de normas internacionales*, anexo H.

INDICACIÓN	**EXPLICACIÓN**
Requisito	los términos "debe", “se requiere”, “es necesario”, “es esencial” y “sólo está permitido” y "no debe", “no está permitido”, “no hay que…”, “no (verbo infinitivo)” indican que los requisitos tienen que cumplirse estrictamente para mostrar conformidad con el documento, no permitiéndose desviaciones
Recomendación	los términos "debería", “es conveniente”, “se recomienda” y "no se debería", “no se recomienda”, “no es conveniente” indican que se recomienda una de entre varias posibilidades como la adecuada, sin mencionar ni excluir a otras, o que una determinada actuación es preferible, pero no se requiere necesariamente, o que (en forma negativa) una cierta posibilidad o actuación no está recomendada pero sin quedar prohibida
Autorización	los términos "puede" “está permitido”, “es permisible” y "no es necesario", “no hace falta”, “no se requiere” indican una línea de actuación permitida dentro de los límites del documento
Posibilidad	los términos "puede", “ser capaz de”, “estar en posición de”, “existe la posibilidad de“, “es posible” y "no puede", “no ser capaz de”, “no tener capacidad de” indican la posibilidad de que algo ocurra

Anexo B (Informativo)

Términos y propietario del término

B.1 Propietario del término

El "propietario del término" en la familia de normas ISO/IEC 27000 es la norma que inicialmente define el término. El "propietario del término" es también el responsable del mantenimiento de la definición, y por tanto de:

- su provisión;
- su revisión;
- su actualización; y
- su retirada.

NOTA 1 La Norma ISO/IEC 27000 nunca es propietaria de ninguno de los términos que contiene.

NOTA 2 Las Normas ISO/IEC 27001 e ISO/IEC 27006, en calidad de normas con carácter normativo (conteniendo requisitos), siempre prevalecen frente a otra norma "propietaria del término".

B.2 Términos usados en estas normas internacionales donde se recogen

B.2.1 ISO/IEC 27001

auditoría	2.5	medición	2.48
disponibilidad	2.9	supervisión, seguimiento o monitorización	2.52
competencia	2.11	no conformidad	2.53
confidencialidad	2.12	objetivo	2.56
conformidad	2.13	organización	2.57
mejora continua	2.15	contratar externamente (verbo)	2.58
control	2.16	desempeño	2.59
corrección	2.18	política	2.60
acción correctiva	2.19	proceso	2.61
información documentada	2.23	requisito	2.63
eficacia	2.24	revisión	2.65
seguridad de la información	2.33	riesgo	2.68

integridad	2.40	dueño del riesgo	2.78
parte interesada	2.41	alta dirección	2.84
sistema de gestión	2.46		

B.2.2 ISO/IEC 27002

control de acceso	2.1	evento o suceso de seguridad de la información	2.35
ataque	2.3	incidente de seguridad de la información	2.36
autenticación	2.7	gestión de incidentes de seguridad de la información	2.37
autenticidad	2.8	sistema de información	2.39
objetivo de control	2.17	no repudio	2.54
recursos (instalaciones) de tratamiento de información	2.32	fiabilidad	2.62
continuidad de la seguridad de la información	2.34		

B.2.3 ISO/IEC 27003

proyecto de SGSI	2.43

B.2.4 ISO/IEC 27004

modelo analítico	2.2	función de medición	2.49
atributo	2.4	método de medición	2.50
medida básica	2.10	resultados de las mediciones	2.51
datos	2.20	objeto	2.55
criterios de decisión	2.21	escala	2.80
medida derivada	2.22	unidad de medida	2.86
indicador	2.30	validación	2.87
necesidades de información	2.31	verificación	2.88
medida	2.47		

B.2.5 ISO/IEC 27005

consecuencia	2.14	comunicación y consulta del riesgo	2.72
suceso	2.25	criterios de riesgo	2.73
contexto externo	2.27	evaluación del riesgo	2.74
contexto interno	2.42	identificación del riesgo	2.75
nivel de riesgo	2.44	gestión del riesgo	2.76
probabilidad (likelihood)	2.45	proceso de gestión del riesgo	2.77
riesgo residual	2.64	tratamiento del riesgo	2.79
aceptación del riesgo	2.69	amenaza	2.83
análisis del riesgo	2.70	vulnerabilidad	2.89
apreciación del riesgo	2.71		

B.2.6 ISO/IEC 27006

documentos de certificación

marca

B.2.7 ISO/IEC 27007

alcance de la auditoría	2.6

B.2.8 ISO/IEC TR 27008

objeto en revisión	2.66	norma de implementación de la seguridad	2.81
objetivo de la revisión	2.67		

B.2.9 ISO/IEC 27010

colectivo que comparte información	2.38	entidad de confianza para la comunicación de información	2.85

B.2.10 ISO/IEC 27011

colocación	instalaciones de telecomunicación
centro de comunicación	organizaciones de telecomunicación

comunicaciones esenciales
no revelación de las comunicaciones
información personal
llamada prioritaria
aplicaciones de telecomunicaciones
negocio de telecomunicaciones
sala de equipo de telecomunicaciones
registros de telecomunicación
servicios de telecomunicación
cliente del servicio de telecomunicación
usuario del servicio de telecomunicación
instalaciones terminales
usuario

B.2.11 ISO/IEC 27014

dirección ejecutiva	2.26	órgano de gobierno	2.29
gobernanza de la seguridad de la información	2.28	parte interesada	2.82

B.2.12 ISO/IEC TR 27015

servicios financieros

B.2.13 ISO/IEC TR 27016

pérdida anual esperada
valor directo
comparativa económica
factor económico
justificación económica
valor añadido económico
economía
valor esperado
valor extendido
valor indirecto
economía de la seguridad de la información
gestión de la seguridad de la información (GSI)
pérdida
valor de mercado
valor actual neto
beneficio no económico
valor actual
coste de oportunidad
valor de oportunidad
requisitos regulatorios
retorno de la inversión
valor social
valor
valor en riesgo

B.2.14 ISO/IEC TR 27017

capacidad

violación de datos

multi-tenencia segura

máquina virtual

B.2.15 ISO/IEC TR 27018

violación de datos

información de identificación personal, PII

controlador PII

PII principal

procesador PII

procesamiento de PII

proveedor de servicios de nube pública

B.2.16 ISO/IEC TR 27019

apagón

Equipo de Respuesta a Emergencias Informáticas (CERT)

infraestructura crítica

depuración

distribución

instalación de equipos de energía

suministro de energía

utilidad de energía

Interfaz Hombre Máquina (HMI)

mantenimiento

PLC

sistema de control de procesos

Seguridad

sistemas de seguridad

red inteligente

Declaración de Aplicabilidad (SOA)

sistema de transmisión

Bibliografía

[1] ISO/IEC 17021, *Conformity assessment. Requirements for bodies providing audit and certification of management systems.*

[2] ISO 9000:2015, *Quality management systems. Fundamentals and vocabulary.*

[3] ISO 19011:2011, *Guidelines for auditing management systems.*

[4] ISO/IEC 27001, *Information technology. Security techniques. Information security management systems. Requirements.*

[5] ISO/IEC 27002, *Information technology. Security techniques. Code of practice for information security controls.*

[6] ISO/IEC 27003, *Information technology. Security techniques. Information security management system implementation guidance.*

[7] ISO/IEC 27004, *Information technology. Security techniques. Information security management. Measurement.*

[8] ISO/IEC 27005, *Information technology. Security techniques. Information security risk management.*

[9] ISO/IEC 27006, *Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems.*

[10] ISO/IEC 27007, *Information technology. Security techniques. Guidelines for information security management systems auditing.*

[11] ISO/IEC TR 27008, *Information technology. Security techniques. Guidelines for auditors on information security controls.*

[12] ISO/IEC 27009, *Information technology. Security techniques. Sector-specific application of ISO/IEC 27001. Requirements.*

[13] ISO/IEC 27010, *Information technology. Security techniques. Information security management for inter-sector and inter-organizational communications.*

[14] ISO/IEC 27011, *Information technology. Security techniques. Information security management guidelines for telecommunications organizations based on ISO/IEC 27002.*

[15] ISO/IEC 27013, *Information technology. Security techniques. Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1.*

[16] ISO/IEC 27014, *Information technology. Security techniques. Governance of information security.*

[17] ISO/IEC TR 27015, *Information technology. Security techniques. Information security management guidelines for financial services.*

[18] ISO/IEC TR 27016, *Information technology. Security techniques. Information security management. Organizational economics.*

[19] ISO/IEC 27017, *Information technology. Security techniques. Code of practice for information security controls based on ISO/IEC 27002 for cloud services.*

[20] ISO/IEC 27018, *Information technology. Security techniques. Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.*

[20] ISO/IEC 27019, *Information technology. Security techniques. Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry.*

[21] ISO 27799, *Health informatics. Information security management in health using ISO/IEC 27002.*

[22] ISO Guide 73:2009, *Risk management. Vocabulary.*

[23] ISO/IEC 15939:2007, *Systems and software engineering. Measurement process.*

[24] ISO/IEC 20000-1:2011, *Information technology. Service management. Part 1: Service management system requirements.*

Para información relacionada con el desarrollo de las normas contacte con:

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

Para información relacionada con la venta y distribución de las normas contacte con:

AENOR INTERNACIONAL S.A.U.
Tel.: 914 326 000
normas@aenor.com
www.aenor.com

UNE NormalizaciónEspañola organismo de normalización español en: