Unión Internacional de Telecomunicaciones

UIT-T X.1054

(04/2021)

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad de la información y de las redes – Gestión de la seguridad

Seguridad de la información, ciberseguridad y protección de la privacidad – Gobernanza de la seguridad de la información

Recomendación UIT-T X.1054

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	**X.1050–X.1069**
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD (1)	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web (1)	X.1140–X.1149
Seguridad de las aplicaciones	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1319
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Correo certificado	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1350–X.1369
Seguridad en los sistemas de transporte inteligente (STI)	X.1370–X.1399
Seguridad de tecnología de libro mayor distribuido (DLT)	X.1400–X.1429
Seguridad de las aplicaciones (2)	X.1450–X.1459
Seguridad de la web (2)	X.1470–X.1489
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
Ciberdefensa	X.1590–X.1599
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699
COMUNICACIÓN CUÁNTICA	
Terminologías	X.1700–X.1701
Generador de números aleatorio cuántico	X.1702–X.1709
Marco de seguridad QKDN	X.1710–X.1711
Diseño de seguridad para QKDN	X.1712–X.1719
Técnicas de seguridad para QKDN	X.1720–X.1729
SEGURIDAD DE LOS DATOS	
Seguridad de los macrodatos	X.1750–X.1759
Protección de los datos	X.1770–X.1789
SEGURIDAD DE IMT-2020	X.1800–X.1819

Para más información, véase la Lista de Recomendaciones del UIT-T.

NORMA INTERNACIONAL ISO/CEI 27014
RECOMENDACIÓN UIT-T X.1054

Seguridad de la información, ciberseguridad y protección de la privacidad – Gobernanza de la seguridad de la información

Resumen

La Recomendación UIT-T X.1054 | Norma Internacional ISO/CEI 27014 proporciona orientación sobre la gobernanza de la seguridad de la información.

La seguridad de la información es una cuestión fundamental para las organizaciones, sobre todo por los rápidos adelantos en las metodologías y tecnologías de ataque y el consecuente aumento de la presión reglamentaria.

Cuando fracasan los controles de seguridad de la información en una organización, las consecuencias pueden ser muy negativas, tanto para la propia organización como para sus interesados, en particular puede generar desconfianza.

La gobernanza de la seguridad de la información consiste en utilizar recursos para garantizar la aplicación efectiva de la seguridad de la información y garantizar que:

- se observen las directrices relativas a la seguridad de la información; y
- el órgano rector reciba informes fiables y pertinentes sobre las actividades relacionadas con la seguridad de la información.

Esta forma de proceder ayuda al órgano rector a tomar decisiones relativas a los objetivos estratégicos de la organización y a proporcionar información sobre la seguridad de la información que pueda afectar a esos objetivos. También garantiza que la estrategia de seguridad de la información se ajuste a los objetivos generales de la entidad.

Los directivos y demás personas que trabajan en las organizaciones deben comprender:

- los requisitos de gobernanza que afectan a su labor; y
- cómo cumplir con los requisitos de gobernanza que exigen tomar medidas.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1054	2012-09-07	17	11.1002/1000/11594
2.0	ITU-T X.1054	2021-04-30	17	11.1002/1000/14248

Palabras clave

Gestión de la información de la seguridad, gobernanza de la seguridad de la información, seguridad de la información, SGSI.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de la existencia de propiedad intelectual, protegida por patente o derecho de autor, que puede ser necesaria para implementar esta Recomendación. Sin embargo, debe señalarse a los implementadores que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar las correspondientes bases de datos del UIT T disponibles en el sitio web del UIT T en http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Página

Introducción

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial. La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas. La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT. En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

La ISO (Organización Internacional de Normalización) y la CEI (Comisión Electrotécnica Internacional) constituyen el sistema especializado para la normalización en el plano mundial. Los organismos nacionales que son miembros de la ISO y de la CEI participan en la elaboración de Recomendaciones | Normas Internacionales a través de comités técnicos establecidos por la respectiva organización para tratar determinados campos de actividad técnica. Los comités técnicos de la ISO y de la CEI colaboran en campos de interés mutuo. También participan en los trabajos otras organizaciones internacionales, gubernamentales y no gubernamentales, en coordinación con la ISO y la CEI. En el campo de la seguridad de la información, la ciberseguridad y la protección de la privacidad, la ISO y la CEI han creado un comité técnico mixto, el JTC 1 de ISO/CEI.

Esta Recomendación | Norma Internacional se ha elaborado con arreglo a las disposiciones que figuran en las Directivas ISO/CEI, Parte 2.

La principal tarea del comité técnico mixto consiste en la elaboración de esta Recomendación | Norma Internacional. Los proyectos de Recomendaciones | Normas Internacionales adoptados por el comité técnico mixto se someten a la votación de los organismos nacionales. Para que se publiquen como Norma Internacional se requiere la aprobación, por lo menos, del 75% de los organismos nacionales que votan.

Conviene recordar que existe la posibilidad de que algunos elementos de esta Recomendación | Norma Internacional estén sujetos a derechos de patentes. La UIT, la ISO o la CEI no se hacen responsables en ningún caso de indicar algunos o todos los derechos de patente.

La Recomendación UIT-T X.1504 | ISO/CEI 27014 fue elaborada por el Comité Técnico Mixto (JTC) 1 de ISO/CEI, *Tecnología de la información*, Subcomité (SC) 27, *Seguridad de la información, ciberseguridad y protección de la privacidad*, en colaboración con la CE 17 del UIT-T.

NORMA INTERNACIONAL
RECOMENDACIÓN UIT-T

Seguridad de la información, ciberseguridad y protección de la privacidad – Gobernanza de la seguridad de la información

1 Alcance

En esta Recomendación | Norma Internacional se presentan los conceptos, objetivos y procesos para la gobernanza de la seguridad de la información, con el fin de que las organizaciones pueden evaluar, dirigir, supervisar y comunicar los procesos relacionados con la seguridad de la información dentro de la organización.

Este documento está dirigido a:

- el órgano rector y la cúpula directiva;
- los responsables de evaluar, orientar y supervisar el sistema de gestión de seguridad de la información (SGSI) basado en la ISO/CEI 27001;
- los responsables de la gestión de la seguridad de la información que tiene lugar fuera del ámbito de un SGSI basado en la norma ISO/CEI 27001, pero dentro del ámbito de la gobernanza.

Esta Recomendación | Norma Internacional es aplicable a organizaciones de todo tipo y tamaño.

Toda referencia a un SGSI en el presente documento se refiere a un SGSI basado en la norma ISO/CEI 27001.

Esta Recomendación | Norma Internacional se concentra en los tres tipos de organizaciones SGSI descritas en el Anexo B. No obstante, también puede ser utilizada por otros tipos de organizaciones.

2 Referencias normativas

Las siguientes Recomendaciones y Normas Internacionales contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación | Norma Internacional. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y Normas son objeto de revisiones, por lo que se preconiza que los participantes en acuerdos basados en la presente Recomendación | Norma Internacional investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y las Normas citadas a continuación. Los miembros de la CEI y de la ISO mantienen registros de las Normas Internacionales actualmente vigentes. La Oficina de Normalización de las Telecomunicaciones de la UIT mantiene una lista de las Recomendaciones UIT-T actualmente vigentes.

– ISO/CEI 27000: en vigor, *Information technology – Security techniques – Information security management systems – Overview and vocabulary*.

– ISO/CEI 27001: en vigor, *Information technology – Security techniques – Information security management systems – Requirements*.

3 Definiciones

En la presente Recomendación | Norma Internacional se utilizan los términos y definiciones que figuran en las normas ISO/IEC 27000 y las siguientes.

La ISO, la CEI y la UIT mantienen bases de datos terminológicas para la normalización en las siguientes direcciones:

- Electropedia de la CEI: http://www.electropedia.org/.
- Plataforma de navegación en línea de la ISO: http://www.iso.org/obp.
- Términos y definiciones de la UIT: http://www.itu.int/go/terminology-database.

3.1 **entidad**: Organización (3.2) y otros órganos o partes.

NOTA – Una entidad puede ser un grupo de empresas, una sola empresa, una empresa sin fines de lucro, o de otro tipo. La entidad tiene autoridad sobre la organización. La entidad puede ser idéntica a la organización, por ejemplo, en empresas más pequeñas.

3.2 **organización**: La parte de una entidad (3.1) que hace funcionar y gestiona el SGSI.

3.3 **órgano rector**: Persona o grupo de personas que son en último término responsables del funcionamiento y la conformidad de la entidad.

NOTA – FUENTE: ISO/CEI 27000:2018, 3.24, modificada – "organización" se ha reemplazado por "entidad".

3.4 **cúpula directiva**: Persona o grupo de personas que dirige y controla una organización (3.2) al más alto nivel

NOTA 1 – FUENTE ISO/CEI 9001.

NOTA 2 – La cúpula directiva tiene la facultad de delegar autoridad y proporcionar recursos dentro de la organización.

NOTA 3 – Si el alcance del sistema de gestión abarca sólo una parte de una entidad, entonces la cúpula directiva se refiere a quienes dirigen y controlan esa parte de la entidad. En esta situación, los altos directivos son responsables ante el órgano rector de la entidad.

NOTA 4 – Dependiendo del tamaño y los recursos de la organización, la cúpula directiva puede ser equivalente al órgano rector.

NOTA 5 – La cúpula directiva rinde cuentas al órgano rector. [FUENTE: ISO/CEI 27000:2018, 3.75].

NOTA 6 – La ISO/CEI 37001 también contiene las definiciones de órgano rector y cúpula directiva.

4 Abreviaturas

A los efectos de la presente Recomendación | Norma Internacional, se aplican las abreviaturas siguientes:

SGSI Sistema de gestión de la seguridad de la información

TI Tecnología de la información

5 Utilización y estructura de la presente Recomendación | Norma Internacional

Esta Recomendación | Norma Internacional describe cómo funciona la gobernanza de la seguridad de la información en el contexto de un SGSI basado en la norma ISO/CEI 27001, y cómo estas actividades están relacionadas con otras actividades de gobernanza fuera del ámbito del SGSI. Se describen cuatro procesos principales en los que se puede estructurar un SGSI dentro de una organización, a saber, "evaluar", "dirigir", "supervisar" y "comunicar", y se proponen métodos para integrar la gobernanza de la seguridad de la información en las actividades de gobernanza de la organización, para cada uno de estos procesos. Por último, en el Anexo A se describen las relaciones entre la gobernanza de la organización, la gobernanza de la tecnología de la información y la gobernanza de la seguridad de la información.

El SGSI comprende, por definición, la totalidad de la organización (véase ISO/CEI 27000). Puede comprender toda la entidad, o parte de ella. Esto se ilustra en la Figura B.1.

6 Normas de gobernanza y gestión

6.1 Generalidades

La gobernanza de la seguridad de la información es el medio por el cual el órgano rector de una organización orienta y controla las actividades que afectan a la seguridad de su información. Esta orientación y control se concentra en las circunstancias en las que la inadecuada seguridad de la información podría afectar negativamente a la capacidad de la organización para lograr sus objetivos generales. Por lo general, para alcanzar sus objetivos de gobernanza el órgano rector:

- proporcionar orientaciones mediante el establecimiento de estrategias y políticas;
- supervisa el rendimiento de la organización; y
- evalúa las propuestas y planes elaborados por los gerentes.

La gestión de la seguridad de la información guarda relación con garantizar el logro de los objetivos de la organización descritos en las estrategias y políticas establecidas por el órgano rector. A tal efecto, la interacción con el órgano rector puede consistir en:

- someter propuestas y planes a la consideración del órgano rector; y
- suministrar información al órgano rector sobre el rendimiento de la organización.

Para lograr una gobernanza eficaz de la seguridad de la información es necesario que tanto los miembros del órgano rector como los gerentes cumplan coherentemente sus respectivas funciones.

6.2 Actividades de gobernanza en el contexto del SGSI

La norma ISO/CEI 27001 especifica los requisitos para establecer, implementar, mantener y mejorar continuamente el sistema de gestión de la seguridad de la información en el contexto de la organización. Incluye asimismo los requisitos para la evaluación y tratamiento de los riesgos de seguridad de la información adaptada a las necesidades de la organización.

La norma ISO/CEI 27001 no utiliza el término "gobernanza" pero especifica una serie de requisitos que son actividades de gobernanza. En la siguiente lista se dan ejemplos de esas actividades. Como se ha señalado anteriormente, las referencias a la organización y a la cúpula directiva están relacionadas con el alcance del SGSI según la norma ISO/CEI 27001.

- ISO/CEI 27001:2013, 4.1 requiere que la organización determine lo que pretende lograr, es decir, sus metas y objetivos de seguridad de la información. Éstos deben estar relacionados con las metas y objetivos generales de la entidad y contribuir a su logro. Guarda relación con los objetivos de gobernanza 1, 3 y 4 estipulados en la cláusula 7.2 de la presente Recomendación | Norma Internacional.
- ISO/CEI 27001:2013, 4.2 requiere que la organización identifique las partes interesadas que son pertinentes para su SGSI, y los requisitos de esas partes interesadas que resultan pertinentes para la seguridad de la información. Guarda relación con el objetivo de gobernanza 4 estipulado en el párrafo 7.2 de la presente Recomendación | Norma Internacional.
- ISO/CEI 27001:2013, 4.3 requiere que la organización defina los límites y la aplicabilidad del SGSI para establecer su alcance, habida cuenta de las cuestiones externas e internas, los requisitos y las interfaces y dependencias. También se especifica que la organización incorporará los requisitos y expectativas de las partes interesadas en su SGSI, además de las cuestiones externas e internas (como leyes, reglamentos y contratos). Guarda relación con el objetivo de gobernanza 1 estipulado en el párrafo 7.2 de la presente Recomendación | Norma Internacional.
- ISO/CEI 27001:2013, 5 especifica que la organización que definirá su política y objetivos e integrará la seguridad de la información en sus procesos (pudiendo incluir los procesos de gobernanza). Se exige a la organización que ponga a disposición los recursos adecuados y comunique la importancia que reviste la gestión de la seguridad de la información. Lo que es más importante, también establece que la organización dirigirá y ayudará a las personas para que contribuyan a la eficacia del SGSI, y que dará soporte a otras funciones de gestión pertinentes en sus esferas de responsabilidad. ISO/CEI 27001:2013, 5 contiene instrucciones para establecer la política y asignar funciones para la gestión de la seguridad de la información y la presentación de informes. Guarda relación con los objetivos de gestión 1 y 3 enunciados en el párrafo 7.2 de la presente Recomendación | Norma Internacional.
- La cláusula ISO/CEI 27001:2013, 6 estudia el diseño de un planteamiento de gestión de riesgos para la organización, en la que se identificarán los riesgos y oportunidades que debe abordar la organización para asegurar que su SGSI sea eficaz. Introduce el concepto de propietarios de los riesgos y sitúa sus responsabilidades en el contexto de las actividades de la organización para gestionar el riesgo y aprobar las actividades de tratamiento del riesgo. También requiere que la organización establezca objetivos de seguridad de la información. Guarda relación con el objetivo de gobernanza 2 enunciado en el párrafo 7.2 de la presente Recomendación | Norma Internacional.
- ISO/CEI 27001:2013, 7 especifica que las personas serán competentes en el cumplimiento de sus obligaciones en materia de seguridad de la información, y establecer el requisito para las comunicaciones de la organización. Guarda relación con el objetivo de gobernanza 5 enunciado en el párrafo 7.2 de la presente Recomendación | Norma Internacional.
- ISO/CEI 27001:2013, 8 especifica la responsabilidad de la organización de planificar, aplicar y controlar su SGSI, incluidos los acuerdos de contratación externa. Esto se relaciona con los objetivos de gobernanza 4 y 6 recogidos en el párrafo 7.2 de la presente Recomendación | Norma Internacional.
- ISO/CEI 27001:2013, 9 requiere la supervisión y notificación de todos los aspectos pertinentes del SGSI, las auditorías internas y el examen y las decisiones de la cúpula directiva y los órganos rectores sobre la eficacia operacional del SGSI, incluidos los cambios necesarios. Guarda relación con el objetivo 6 de la gobernanza enunciado en el párrafo 7.2 de la presente Recomendación | Norma Internacional.
- ISO/CEI 27001:2013, 10 especifica la identificación y el tratamiento de las faltas de conformidad, el requisito de identificación de oportunidades de mejora continua y la actuación ante esas oportunidades. Guarda relación con el objetivo de gobernabilidad 4 establecido en el párrafo 7.2 de la presente Recomendación | Norma Internacional.

6.3 Otras normas relacionadas

La norma ISO/CEI 38500 describe los principios rectores para los miembros de los órganos rectores de las organizaciones sobre la utilización eficaz, eficiente y aceptable de la tecnología de la información en sus organizaciones. También proporciona orientación a quienes asesoran, informan o ayudan a los órganos rectores en la gobernanza de la tecnología de la información.

6.4 Aspectos de la gobernanza dentro de la organización

Estos aspectos se corresponden exactamente con los procesos de gobernanza de la organización descritos en la cláusula 7. Los dos últimos elementos de la lista son equivalentes a sus aspectos de gobernanza en el contexto de la seguridad de la información:

- armonizar los objetivos de seguridad de la información con los objetivos empresariales;
- gestionar el riesgo de seguridad de la información de conformidad con esos objetivos de seguridad de la información;
- evitar conflictos de intereses en la gestión de la seguridad de la información;
- evitar que la tecnología de la información de la organización se utilice para perjudicar a otras organizaciones.

7 Gobernanza de la entidad y gobernanza de la seguridad de la información

7.1 Generalidades

La organización cuenta con muchas esferas de gobernanza, como la seguridad de la información, la tecnología de la información, la salud y la seguridad, la calidad y las finanzas. Cada aspecto de la gobernanza es un componente de los objetivos generales de la gobernanza de la organización y, por consiguiente, debe estar en consonancia con la disciplina organizativa. Los alcances de los modelos de gobernanza a veces se solapan. En las subcláusulas 7.2 y 7.3 se describen los objetivos y procesos de la gobernanza, que pueden aplicarse a cualquier esfera de gobierno.

El SGSI se centra en la gestión de los riesgos relacionados con la información. No aborda directamente temas como la rentabilidad, la adquisición, la utilización y la realización de activos, o la eficiencia de otros procesos, aunque debe apoyar cualquier objetivo organizativo sobre estos temas.

7.2 Objetivos

7.2.1 Objetivo 1: Establecer una seguridad de la información amplia e integrada en toda la organización

La gobernanza de la seguridad de la información ha de garantizar la globalidad e integración de las actividades de seguridad de la información. La seguridad de la información ha de abarcar toda la entidad y la toma de decisiones al respecto deberá tomar en consideración los aspectos empresariales, de seguridad de la información y de TI convenientes. Las actividades relativas a la seguridad física y lógica deben estar estrechamente coordinadas. Sin embargo, no se requiere un conjunto único de medidas de seguridad ni un único SGSI en toda la entidad.

Para dar seguridad a toda la entidad, la responsabilidad y rendición de cuentas sobre la seguridad de la información debe cubrir todas las actividades de la entidad. Con frecuencia esta responsabilidad va más allá de las "fronteras" percibidas de la entidad, por ejemplo, cuando la información se almacena y transfiere en el exterior.

7.2.2 Objetivo 2: Adoptar un planteamiento basado en los riesgos

La gobernanza de la seguridad de la información debe basarse en las obligaciones de cumplimiento y también en las decisiones de la entidad tomadas en función de los riesgos. La determinación del grado de seguridad aceptable debe basarse en el riesgo que la entidad está dispuesta a asumir, como la pérdida de ventaja competitiva, los riesgos relativos al cumplimiento y responsabilidad, las perturbaciones operativas, la reputación y las pérdidas económicas.

La gestión de riesgos para la seguridad de la información debe ser coherente en toda la entidad y tener en cuenta los efectos negativos sobre las finanzas, el funcionamiento y la reputación resultantes de las filtraciones y la falta de conformidad. Además, la gestión de riesgos para la seguridad de la información debe integrarse en el planteamiento general de gestión del riesgo de la entidad, en lugar de realizarse de manera aislada, y no debe causar confusión, por ejemplo, estableciendo claramente la relación con la metodología de la entidad o consignando los riesgos de la información estratégica en el registro de riesgos para la entidad.

En el marco del proceso de gobernanza de la seguridad, deben asignarse los recursos adecuados para poner en práctica la gestión de los riesgos de la información.

7.2.3 Objetivo 3: Determinar la orientación de las decisiones de inversión

Los efectos del riesgo para la seguridad de la información deben evaluarse adecuadamente antes de emprender nuevas actividades, como inversiones, compras, fusiones, adopción de nueva tecnología, acuerdos de subcontratación y contratos con proveedores externos.

A fin de optimizar las inversiones en seguridad de la información en pro de sus objetivos, el órgano rector debe asegurarse de que la seguridad de la información se integre en los procesos internos existentes, incluida la gestión de proyectos, las adquisiciones, los gastos financieros, el cumplimiento de las leyes y reglamentos y la gestión estratégica de los riesgos.

La cúpula directiva del SGSI debe establecer una estrategia de seguridad de la información basada en los objetivos de la entidad y velar por la armonización entre los requisitos de la entidad y los requisitos de seguridad de la información de la organización, satisfaciendo así las necesidades actuales y cambiantes de las partes interesadas.

7.2.4 Objetivo 4: Garantizar el cumplimiento de requisitos internos y externos

La gobernanza de la seguridad de la información debe garantizar que las políticas y prácticas de seguridad de la información están en consonancia con los requisitos de las partes interesadas. Quedan comprendidos la legislación y los reglamentos, así como los requisitos contractuales y los compromisos internos.

Para hacer frente a las cuestiones de conformidad y cumplimiento, la cúpula directiva puede encargar obtener auditorías de seguridad independientes con el fin de asegurarse de que las actividades de seguridad de la información cumplen satisfactoriamente los requisitos internos y externos.

7.2.5 Objetivo 5: Fomentar un entorno propicio a la seguridad

La gobernanza de la seguridad de la información debe basarse en la cultura interna, comprendidas las necesidades cambiantes de todos los interesados, ya que el comportamiento humano es uno de los factores fundamentales para lograr el nivel adecuado de seguridad de la información. Si no se coordinan adecuadamente, los objetivos, las funciones, las responsabilidades y los recursos pueden entrar en conflicto entre sí, dando lugar al incumplimiento de los objetivos. Es, por consiguiente, muy importante la armonización y la orientación concertada entre las diversas partes interesadas.

A fin de crear una cultura de seguridad de la información, el órgano rector debe exigir, promover y apoyar la coordinación de las actividades de las partes interesadas con el fin de lograr una orientación coherente en materia de seguridad de la información. De esta manera se contribuye al suministro de programas de educación, formación y sensibilización en materia de seguridad. Las responsabilidades en materia de seguridad de la información deberían integrarse en las funciones del personal y otras partes, y deberían contribuir al éxito del SGSI por el hecho de asumir dichas responsabilidades.

7.2.6 Objetivo 6: Asegurarse de que los resultados en materia de seguridad satisfacen los requisitos presentes y futuros de la entidad

La gobernanza de la seguridad de la información debe garantizar que el planteamiento adoptado para proteger la información es el adecuado para la organización y ofrece los niveles acordados de seguridad de la información. La seguridad se ha de mantener en los niveles necesarios para cumplir los requisitos empresariales actuales y futuros.

A fin de evaluar el rendimiento de la seguridad de la información desde la perspectiva de la gobernanza, el órgano rector debe evaluar el rendimiento de la seguridad de la información en relación con su impacto empresarial y no limitarse a efectuar controles de eficacia y efectividad.

Dentro de cada SGSI, debe requerirse a la cúpula directiva del SGSI para que aplique un programa de cuantificación del rendimiento para supervisar, auditar e identificar las esferas susceptibles de mejora. El órgano rector debe vincular el rendimiento de la seguridad de la información con el de la organización y de la entidad.

7.3 Procesos

7.3.1 Generalidades

El órgano rector de la entidad lleva a cabo los procesos "evaluar", "dirigir", "supervisar" y "comunicar". En la Figura 1 se indica la relación entre estos procesos.

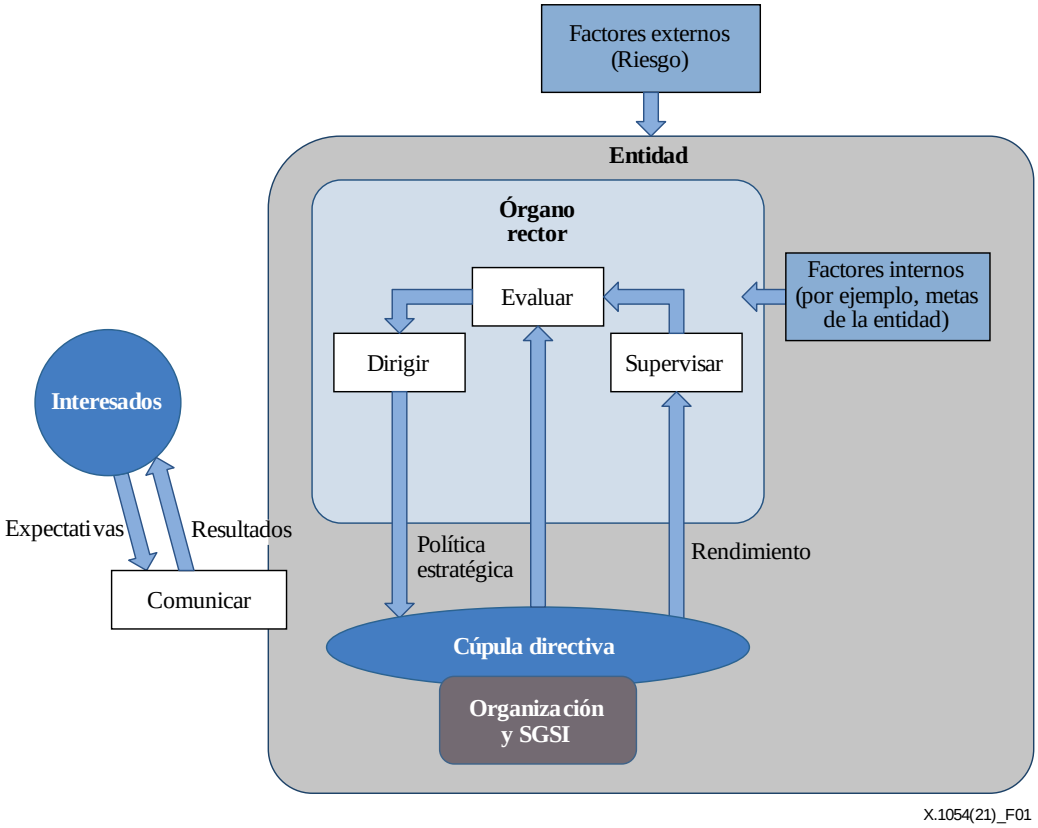

Figura 1 – Modelo de gobernanza para una entidad con un SGSI

NOTA 1 – La definición de "organización", [3.2], significa que la cúpula directiva siempre participa plenamente en el funcionamiento de la organización.

NOTA 2 – Una entidad puede contener más de un SGSI y puede haber partes de una entidad, a las que se aplica la gobernanza, que no sean parte del SGSI. Véanse la cláusula 8 y el Anexo B.

7.3.2 Evaluar

Por "Evaluar" se entiende el proceso de gobernanza que considera la consecución real y prevista de los objetivos de seguridad a partir de los procesos en vigor y de los cambios planificados, y determina qué ajustes se han de efectuar para optimizar la consecución de los objetivos estratégicos en el futuro.

Para realizar el proceso "evaluar":

- el órgano rector de la entidad debe:
  - garantizar que las iniciativas tienen en cuenta los riesgos y oportunidades correspondientes;
  - responder a las mediciones e informes de seguridad de la información y del SGSI especificando y dando prioridad a los objetivos requeridos en el contexto de cada SGSI (lo cual incluye la toma en consideración de los requisitos exteriores al alcance del SGSI); y
- la cúpula directiva de cada SGSI debe:
  - garantizar que la seguridad de la información da soporte y contribuye a los objetivos de la entidad;
  - someter a la consideración del órgano rector nuevos proyectos de seguridad de la información de gran importancia para la organización.

7.3.3 Dirigir

Por "Dirigir" se entiende el proceso de gobernanza mediante el cual el órgano rector determina los objetivos y estrategias de la entidad. Dirigir puede conllevar cambios en los niveles de provisión, atribución de recursos, prioridad de las actividades, así como en la aprobación de políticas, aceptación de riesgos materiales y planes de dirección de riesgos.

Para realizar el proceso "dirigir":

- el órgano rector debe:
  - establecer la orientación y los objetivos estratégicos globales de la entidad;
  - definir el nivel de riesgo que la organización está dispuesta a correr;

- aprobar la estrategia de seguridad de la información; y

– la cúpula directiva de cada SGSI debe:

- atribuir las inversiones y recursos necesarios;
- armonizar los objetivos de seguridad de la información con los objetivos de la entidad;
- asignar funciones y responsabilidad en materia de seguridad de la información;
- establecer una política de seguridad de la información.

NOTA – La asunción de riesgos es la cantidad y el tipo de riesgos que una organización está dispuesta a aceptar. [8]

7.3.4 Supervisar

Por "supervisar" se entiende el proceso de gobernanza que permite al órgano rector evaluar el logro de los objetivos estratégicos.

Para realizar el proceso "supervisar":

– el órgano rector debe:

- recibir informes sobre la eficacia y el funcionamiento de cada SGSI;
- evaluarlos en el contexto de las prioridades de la entidad;
- comunicar las prioridades a la cúpula directiva de cada SGSI; y

– a tal efecto, la cúpula directiva de cada SGSI debe:

- evaluar la eficacia de las actividades de gestión de la seguridad de la información;
- velar por la conformidad con los requisitos internos y externos;
- tener en cuenta los cambios en la entidad, el entorno jurídico y reglamentario y cualquier posible incidencia en el riesgo de la información;
- seleccionar los parámetros de rendimiento adecuados y exigir la presentación oportuna de informes desde una perspectiva organizativa;
- proporcionar al órgano rector información sobre los resultados del rendimiento en materia de seguridad de la información;
- alertar al órgano rector de las novedades que afecten a los riesgos de la información y la seguridad de la información.

Para evaluar el rendimiento de la seguridad de la información desde la perspectiva de la gobernanza, el órgano rector debe evaluar el rendimiento de la seguridad de la información en relación con su impacto empresarial y no limitarse a efectuar controles de eficacia y efectividad. Estos controles pueden hacerse mediante exámenes obligatorios en función de un programa de medición del rendimiento destinado a supervisar, auditar y mejorar, vinculando así el rendimiento de la seguridad de la información al rendimiento empresarial.

7.3.5 Comunicar

Por "Comunicar" se entiende el proceso de gobernanza bidireccional mediante el cual el órgano rector y los interesados intercambian información sobre la seguridad de la información de acuerdo con sus necesidades específicas.

Uno de los métodos que puede emplearse para "comunicar" consiste en realizar una declaración del estado de la seguridad de la información en el que se explique a los interesados las actividades y problemas de seguridad de la información.

Uno de los motivos de la comunicación es permitir que las entidades rindan cuentas a los interesados, por ejemplo, a los accionistas. Esto resulta cada vez más importante, por lo que las organizaciones informan ahora sobre la implementación y mantenimiento de su gestión de la seguridad de la información, así como sobre su eficacia en la gestión de los riesgos. Análogamente, en el caso de que se haya producido un incidente de seguridad de la información, las entidades deben explicar las repercusiones, las causas y los cambios previstos en los controles para afrontar el riesgo de incidentes reiterados a sus partes interesadas y, si procede, hacer declaraciones públicas por separado.

La comunicación puede llevarse a cabo por diversos métodos y su contenido puede ser variado. Además, está destinada a distintas audiencias. Al preparar la comunicación debe tomarse en consideración su destinatario y el mensaje que se pretende transmitir. Estos dos factores sentarán las bases para determinar luego el contenido de las comunicaciones, así como los canales utilizados para hacer llegar las comunicaciones a la audiencia prevista. En el Anexo C se muestra un ejemplo.

Para realizar el proceso "comunicar":

– el órgano rector debe:
  - informar a los interesados externos de que las prácticas de la organización en materia de seguridad de la información están en consonancia con la naturaleza de sus actividades y prioridades;
  - identificar y priorizar las obligaciones reglamentarias, las expectativas de las partes interesadas y los requisitos de la entidad en materia de seguridad de la información;
  - asesorar a la cúpula directiva de cada SGSI sobre cualquier asunto que requiera su atención y decisión;
  - dar instrucciones a los interesados pertinentes sobre los objetivos detallados que deben adoptarse para las prioridades de seguridad de la información;
  - promover una cultura positiva de seguridad de la información;
  - impartir formación y mantener comunicación con el personal y otras personas en el ámbito del SGSI sobre sus responsabilidades.

8 Requisitos del órgano rector relativos al SGSI

8.1 Organización y SGSI

El órgano rector debe requerir el diseño de uno o varios SGSI para apoyar los objetivos de la entidad. Los objetivos de cada SGSI pueden ser los mismos que los de la entidad matriz, u otros dependiendo del tamaño, la escala y la estructura de toda la entidad, pero deben estar alineados. En el Anexo A se ilustran las posibles relaciones entre la gobernanza de la seguridad de la información y la gobernanza de la tecnología de la información.

El órgano rector también debe requerir que el diseño de cada SGSI sea compatible con las políticas y procesos generales de la entidad, incluida la gestión del riesgo. Convendría que un SGSI integrara el mismo proceso de evaluación de riesgos que el del órgano rector, a fin de permitir la comunicación clara de la información sobre los riesgos. Si el órgano rector utiliza un proceso de evaluación del riesgo que no se ajusta a los requisitos de la norma ISO/CEI 27001, para que la organización puede alcanzar la conformidad su SGSI debe utilizar un enfoque de evaluación del riesgo diferente del utilizado por la entidad y acordar un método para comunicar al órgano rector la información relacionada con el riesgo en términos que sean compatibles con el planteamiento del órgano rector. Alternativamente, el órgano rector puede optar por modificar el actual proceso de evaluación de riesgos de la entidad para adaptarlo a los requisitos de la norma ISO/CEI 27001.

El órgano rector puede ordenar el uso de un SGSI para gestionar los riesgos estratégicos relacionados con la pérdida de propiedad intelectual y de la reputación y las pérdidas económicas debidas al perjuicio sobre la confidencialidad, la integridad o la disponibilidad de la información.

Un SGSI puede suministrar al órgano rector información de gestión relativa a:

- los riesgos para la entidad;
- la eficacia del SGSI.

El órgano rector debe:

- aprobar la creación de cada SGSI;
- definir el alcance de cada SGSI y el alcance para la certificación (pueden diferir);
- proporcionar orientación a cada SGSI, incluidos los objetivos, requisitos, funciones y recursos;
- tomar decisiones sobre los niveles aceptables de riesgo residual, o la gestión de riesgo apropiados;
- proporcionar a cada SGSI canales de comunicación y la autoridad para utilizar dichos canales a fin de comunicar la información apropiada a los interesados y a todas las personas en el ámbito del citado SGSI.

8.2 Casos (véase el Anexo B)

8.2.1 Tipo A: La organización SGSI constituye toda la entidad

Cuando el único sistema de gestión existente es conforme con la norma ISO/CEI 27001, puede utilizarse para suministrar información sobre los riesgos y, de ese modo, permitir que la organización se ocupe del riesgo de la información. Sin embargo, siguen existiendo diferentes procesos para dar soporte a la gobernanza de TI, financiera y operativa, así como otras actividades.

En el caso de que la organización del SGSI se aplique a toda la entidad:

- los procesos de gobernanza descritos en 7.3 no se modifican;
- la alta dirección tiene responsabilidades de gobernanza además de la gobernanza de la seguridad de la información, por ejemplo, la gobernanza corporativa.

Es probable que la armonización de los objetivos de seguridad de la información de la organización con los objetivos generales de la entidad sea sencilla, ya que la alta dirección es responsable de establecer ambos. En caso de que la responsabilidad de la gobernanza y de la gestión de la seguridad de la información esté a cargo de una sola función, se debe proporcionar el asesoramiento adecuado para garantizar que la responsabilidad de establecer la política, y su ejecución, estén adecuadamente separadas entre sí.

8.2.2 Tipo B: La organización SGSI forma parte de una entidad más grande

Algunas organizaciones SGSI forman parte de una entidad más grande. Dado que las actividades de gobernanza suelen aplicarse a toda una entidad jurídica, corporación, organización benéfica, organismo público u otra entidad, la gobernanza de esa entidad se extiende en este caso más allá del ámbito del SGSI. La organización puede disponer de múltiples SGSI dentro. Por consiguiente, el órgano rector puede administrar múltiples SGSI. La mayor parte del presente documento se ha redactado para permitir este planteamiento.

Los cuatro procesos de gobernanza descritos en el párrafo 7.3 siguen siendo pertinentes. Sin embargo, según la relación entre las organizaciones SGSI y la entidad matriz, puede darse una de las siguientes situaciones:

- Cada organización de SGSI funciona de manera autónoma dentro de la entidad matriz y, por consiguiente, tiene sus propios objetivos comerciales. En este caso, los objetivos de seguridad de la información de la organización SGSI deben estar armonizados con sus propios objetivos comerciales.
- Cada organización SGSI es responsable de lograr uno o varios de los objetivos comerciales de su entidad matriz. En este caso, los objetivos de seguridad de la información de la organización SGSI deben estar armonizados con los objetivos comerciales de su entidad matriz.

Cada organización SGSI tiene asignada la responsabilidad de gestionar un aspecto del riesgo de seguridad de la información en nombre de la entidad matriz, en cuyo caso los objetivos de seguridad de la información de la organización SGSI debe especificarlos la entidad matriz, que garantiza la armonización con los objetivos comerciales de la entidad matriz.

Por otra parte, también hay una relación entre la cúpula directiva de cada organización SGSI y el órgano rector de la entidad matriz. El equipo o equipos de la cúpula directiva y el órgano rector pueden ser los mismos, pueden tener algunas personas en común o pueden no tener ninguna en común. La Figura B.1 debe utilizarse para determinar qué personas deben asignarse a las funciones de miembro del órgano rector y de parte interesada.

8.2.3 Tipo C: La organización SGSI consta de partes de diversas entidades

En esta situación, la organización SGSI está regida y controlada por la cúpula directiva, como es habitual, pero abarca varias entidades. Este es el caso en el que una entidad más grande administra un grupo de entidades cuyo contexto y requisitos de seguridad de la información son comunes para un subconjunto de sus actividades, por ejemplo, cuando se reúnen, procesan, almacenan y utilizan datos personales para prestar servicios. También es posible que varios órganos rectores compartan un SGSI; por ejemplo, una organización puede prestar un SGSI como servicio para muchos clientes.

En el caso de que la organización SGSI conste de partes de diversas entidades:

- Los procesos de gobernanza descritos en el párrafo 7.3 no se modifican.
- Los objetivos de seguridad de la información de la organización SGSI deben estar armonizados con los objetivos comerciales mutuos que unen a las entidades miembros.

Anexo A

Relación de gobernanza

(Este anexo no forma parte integrante de la presente Recomendación | Norma Internacional.)

La Figura A.1 ilustra la relación entre la gobernanza de la seguridad de la información y la gobernanza de la tecnología de la información.

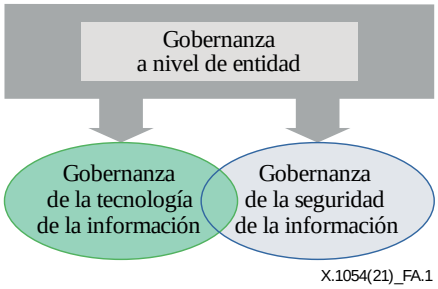

Figura A.1 – Relación entre la gobernanza de la seguridad de la información y la gobernanza de la tecnología de la información

Mientras que el ámbito general de la gobernanza de la tecnología de la información tiene por objeto los recursos necesarios para adquirir, procesar, almacenar y difundir información, el ámbito de la gobernanza de la seguridad de la información abarca, en cambio, la confidencialidad, la integridad y la disponibilidad de la información. Ambos métodos de gobernanza pueden manejarse mediante los siguientes procesos de gobernanza: evaluar, dirigir, supervisar y comunicar.

Anexo B

Tipos de organización SGSI

(Este anexo no forma parte integrante de la presente Recomendación | Norma Internacional.)

Existen tres tipos de relación entre la organización que administra el SGSI y la entidad que aplica el SGSI. Estas relaciones también afectan a los miembros de la cúpula directiva del SGSI y al órgano rector de la entidad. Estos tipos de relación se enumera en la siguiente lista y se ilustra en la Figura B.1.

Tipo A: La entidad y la organización del SGSI son la misma entidad.

- El órgano rector es el mismo que la cúpula directiva del SGSI.

Tipo B: La entidad contiene la organización del SGSI (y puede haber más de un SGSI operativo dentro de esa entidad).

- El órgano rector puede compartir algunos miembros con cada SGSI, pero los miembros no son idénticos.

Tipo C: Múltiples entidades comparten el SGSI:

- Si las entidades tienen un interés directo en el SGSI, el órgano rector de cada entidad puede ser miembro de la cúpula directiva del SGSI.
- Si el SGSI se presta como un servicio por un tercero, es improbable que haya miembros comunes entre la cúpula directiva del SGSI y los órganos rectores de las entidades que comparten el SGSI.

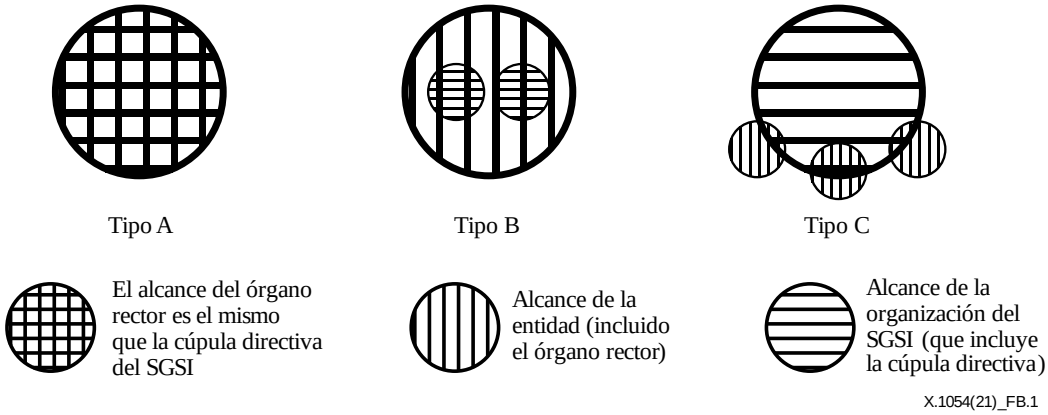

Figura B.1 – Posibles relaciones entre entidades y sus SGSI

Anexo C

Ejemplos de comunicación

(Este anexo no forma parte integrante de la presente Recomendación | Norma Internacional.)

Los mercados de valores constituyen un buen ejemplo de comunicación, ya que las empresas están obligadas a revelar los riesgos para la seguridad de la información conforme estipula la legislación o la normativa de la industria. Otro ejemplo es el informe medioambiental, social y de gobernanza (MSG), mediante el cual las organizaciones explican/comunican sus esfuerzos desde las perspectivas ambiental, social y económica a las partes interesadas. En algunos informes MSG se describe el planteamiento de la protección de los datos personales, las actividades de seguridad de la información y la gestión de crisis para la prevención de incidentes de seguridad.

Al diseñar las comunicaciones se deben considerar también los efectos no deseados de que los destinatarios entiendan mal o lleguen a conclusiones adicionales, y de que las comunicaciones lleguen a otros destinatarios no previstos.

Bibliografía

[1] Recomendación UIT-T X.1051(04/2016) | ISO/CEI 27011:2016, *Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations*.

[2] ISF, Standard of Good Practice for Information Security: 2018.

[3] ISO 37001:2016, *Anti-bribery management systems – Requirements with guidance for use*.

[4] ISO/IEC 9001:2015, *Quality management systems – Requirements*.

[5] ISO/IEC 27000:2018, *Information security, cybersecurity and privacy protection – Overview and vocabulary*.

[6] ISO/IEC 27002:2013, *Information security, cybersecurity and privacy protection – Code of practice for information security controls*.

[7] ISO/IEC 38500:2015, *Information technology – Governance of IT for the organization*.

[8] Iso Guide 73: 2009

[9] IT Governance Institute (ITGI), *Information Security Governance: Guidance for Information Security Managers: 2008*.

[10] ITGI, *Information Security Governance Guidance for Boards of Directors and Executive Management*, 2nd Edition: 2006.

[11] ITGI, COBIT *Control Practices: Guidance to Achieve Control Objective for Successful IT Governance*, 2nd Edition: 2007.

[12] Ohki E., Harada Y., Kawaguchi S., Shiozaki T., Kgaua T., *Information Security Governance framework, Proceedings of the first ACM workshop on Information security governance*, pp. 1-6, 2009.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2022