Unión Internacional de Telecomunicaciones

UIT-T X.1054

(09/2012)

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

Tecnología de la información – Técnicas de seguridad – 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	
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	X.1140–X.1149
Protocolos de seguridad	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	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
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/eurística	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

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

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

Tecnología de la información – Técnicas de seguridad – 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 se ha convertido en un asunto esencial para las organizaciones. Hay cada vez más exigencias normativas, y a ello se suma el hecho de que medidas deficientes de seguridad de la información en una organización pueden repercutir directamente en su reputación.

Por consiguiente, el órgano rector, en el marco de sus responsabilidades de gobernanza, debe supervisar cada vez más la seguridad de la información para garantizar la consecución de los objetivos de la organización.

Además, la gobernanza de la seguridad de la información establece un fuerte vínculo entre el órgano rector de una organización, la dirección ejecutiva y los responsables de implementar y operar un sistema de gestión de la seguridad de la información.

Constituye el mandato esencial para llevar a cabo iniciativas de seguridad de la información en toda la realización.

Además, una gobernanza eficaz de la seguridad de la información garantiza que el órgano rector reciba información pertinente, enmarcada en un contexto comercial, sobre actividades relacionadas con la seguridad de la información. De este modo se pueden tomar decisiones pertinentes y oportunas sobre cuestiones de seguridad de la información en pro de los objetivos estratégicos de la organización.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio
1.0	ITU-T X.1054	2012-09-07	17

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 propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Página

1 Alcance 1
2 Referencias normativas 1
3 Definiciones 1
4 Conceptos 1
4.1 Consideraciones generales 1
4.2 Objetivos 2
4.3 Resultados deseados 2
4.4 Relación 2
5 Principios y procesos 3
5.1 Aspectos generales 3
5.2 Principios 3
5.3 Procesos 4
Anexo A – Ejemplo de estado de seguridad de la información 7
Anexo B – Ejemplo de estado de seguridad de la información detallado 8
Bibliografía 9

NORMA INTERNACIONAL
RECOMENDACIÓN UIT-T

Tecnología de la información – Técnicas de seguridad – Gobernanza de la seguridad de la información

1 Alcance

En esta Recomendación | Norma Internacional se presentan conceptos y orientaciones sobre los principios y procesos de gobernanza de la seguridad de la información de acuerdo con los cuales las organizaciones pueden evaluar, dirigir y controlar la gestión de la seguridad de la información.

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

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/IEC 27000:2009, *Information Technology – Security techniques – Information security management systems – Overview and vocabulary*.

3 Definiciones

A los efectos de esta Recomendación | Norma Internacional serán de aplicación los términos y definiciones de ISO/CEI 27000, así como los que se presentan a continuación:

3.1 dirección ejecutiva: Persona o grupo de personas en quienes el órgano rector ha delegado la responsabilidad de poner en práctica estrategias y políticas para la consecución de los objetivos de la organización.

NOTA 1 – La dirección ejecutiva forma parte del equipo directivo principal. Para aclarar los cometidos, esta norma distingue entre dos grupos de gestión de alto nivel: el órgano rector y los directores ejecutivos.

NOTA 2 – La dirección ejecutiva puede incluir directores ejecutivos, directores financieros, directores de operaciones, directores de información, directores de seguridad de la información y semejantes.

3.2 órgano rector: Persona o grupo de personas que son en último término responsables del funcionamiento de la organización.

NOTA – El órgano rector forma parte del equipo directivo principal. Para aclarar las responsabilidades, esta norma distingue entre dos grupos de gestión de alto nivel: el órgano rector y la dirección ejecutiva.

3.3 gobernanza de la seguridad de la información: Sistema mediante el cual se dirigen y supervisan las actividades relacionadas con la seguridad de la información de una organización.

3.4 interesado: Persona u organización que puede afectar, verse afectado o considerarse afectado por las actividades de la organización.

NOTA – Un ente decisorio puede ser un interesado.

4 Conceptos

4.1 Consideraciones generales

La gobernanza de la seguridad de la información debe armonizar los objetivos y estrategias de la seguridad de la información con los objetivos y estrategias empresariales y exige el cumplimiento de la legislación, los reglamentos y los contratos. Dicha gobernanza se ha de evaluar, analizar y poner en práctica de acuerdo con un enfoque de gestión de riesgos, respaldado por un sistema de control interno.

El órgano rector es en último término responsable de las decisiones de la organización y de su funcionamiento. En cuanto a la seguridad de la información, el principal deber del órgano rector es asegurarse de que el enfoque adoptado por la organización a este respecto es eficaz, efectivo y aceptable, tomando debidamente en consideración las expectativas de los interesados. Cada interesado puede tener distintos valores y necesidades.

4.2 Objetivos

Los objetivos de la gobernanza de la seguridad de la información son los siguientes:

- armonizar la estrategia de seguridad de la información con la estrategia/los objetivos empresariales (armonización estratégica);
- aportar valor al órgano rector y los interesados (aportación de valor);
- asegurar que se cubren adecuadamente los riesgos de información (responsabilidad).

4.3 Resultados deseados

A continuación se indican los resultados que se desea obtener con la aplicación efectiva de la gobernanza de la seguridad de la información:

- que el órgano rector conozca la situación de la seguridad de la información;
- agilidad en la toma de decisiones acerca de los riesgos de información;
- inversión eficaz y efectiva en la seguridad de la información;
- cumplimiento de los requisitos externos (jurídicos y reglamentarios).

4.4 Relación

Dentro de una organización coexisten diversos modelos de gobernanza, como la gobernanza de la tecnología de la información y la gobernanza orgánica. Cada uno de estos modelos forma parte integrante de la gobernanza de una organización, lo que pone de manifiesto cuán importante es armonizarla con los objetivos empresariales. Suele ser conveniente que el órgano rector elabore una visión global e integrada de su modelo de gobernanza, del que debe formar parte la gobernanza de la seguridad de la información. En ocasiones los ámbitos de los modelos de gobernanza se solapan. Por ejemplo, en la Figura 1 se muestra la relación entre la gobernanza de la seguridad de la información y la gobernanza de la tecnología de la información.

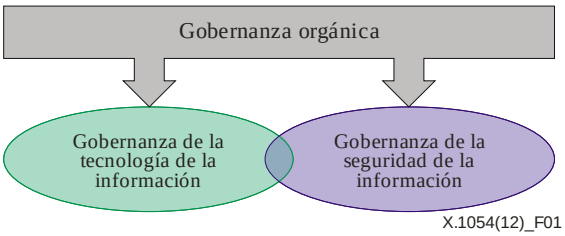

Figura 1 – Relación entre la gobernanza de la seguridad de la información y la gobernanza de la tecnología de la información

Si bien el ámbito global de aplicación de la gobernanza de TI son los recursos necesarios para adquirir, procesar, almacenar y divulgar la información, el de la gobernanza de la seguridad de la información es la confidencialidad, la integridad y la disponibilidad de la información. Ambos esquemas se han de regir por los siguientes procesos de gobernanza: evaluar, dirigir, supervisar (EDM, *evaluate, direct, monitor*). Sin embargo, la gobernanza de la seguridad de la información requiere el proceso interno adicional "comunicar".

En la cláusula 5 se presentan las tareas que ha de efectuar el órgano rector para establecer una gobernanza de la seguridad de la información. Las tareas de gobernanza también atañen a los requisitos de dirección especificados en ISO/CEI 27001 y en otras normas de la familia ISMS, como se indica en la Bibliografía.

5 Principios y procesos

5.1 Aspectos generales

En esta cláusula se describen los principios y procesos que, en conjunto, forman la gobernanza de la seguridad de la información. Los principios de gobernanza de la seguridad de la información son normas aceptadas para regir o dirigir, que sirven de guía para la implantación de la gobernanza. Un proceso de gobernanza para la seguridad de la información describe una serie de tareas que permiten aplicar esa gobernanza y sus relaciones. También muestra la relación entre la gobernanza y la gestión de la seguridad de la información. Estos dos componentes se exponen más detalladamente en las siguientes subcláusulas.

5.2 Principios

Ajustarse a las necesidades de los interesados y aportar valor a cada uno de ellos es fundamental para el éxito de la seguridad de la información a largo plazo. En esta subcláusula se establecen seis principios activos destinados a lograr el objetivo de la gobernanza de armonizar la seguridad de la información con los objetivos de la empresa y aportar valor a los interesados.

Los principios sirven de base para realizar las actividades de gobernanza de la seguridad de la información. El enunciado de cada principio se refiere a los que debe hacerse, pero no define cómo, cuándo o quién ha de poner en práctica tales principios, pues son variables dependientes de cada organización. El órgano rector ha de exigir que se apliquen tales principios y nombrar a una persona con la responsabilidad y autoridad suficientes para ello.

Principio 1: Dar seguridad a 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 organización 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.

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

Principio 2: Adoptar un enfoque basado en los riesgos

La gobernanza de la seguridad de la información se ha de basar en decisiones tomadas en función de los riesgos. Para determinar qué nivel de seguridad es suficiente es necesario evaluar los riesgos de la organización, incluida la pérdida de ventaja competitiva, los riesgos de cumplimiento y responsabilidad civil, las interrupciones operativas, la reputación y la pérdida financiera.

La gestión de riesgos apropiada para la organización ha de ser coherente con el método de gestión de riesgos general e integrarse en él. El órgano rector ha de aprobar el nivel de riesgos que la organización puede aceptar y deberá atribuir los recursos adecuados para aplicar los métodos de gestión de riesgos correspondientes.

Principio 3: Determinar la orientación de las decisiones de inversión

La gobernanza de la seguridad de la información debe establecer una estrategia de inversión en seguridad basada en los resultados empresariales obtenidos, de manera que se armonicen los requisitos empresariales y de seguridad, colmando así las necesidades de los interesados.

Para optimizar las inversiones de seguridad en pro de los objetivos orgánicos, el órgano rector ha de asegurarse de que la seguridad de la información se integre en los procesos orgánicos existentes de gastos operativos y de capital, de cumplimiento legal y reglamentario, y de detección de riesgos.

Principio 4: Garantizar el cumplimiento de requisitos internos y externos

La gobernanza de la seguridad de la información ha de garantizar que las políticas y prácticas de seguridad de la información se ajustan a los reglamentos y leyes de obligado cumplimiento correspondientes.

Para hacer frente a los problemas de conformidad y cumplimiento, el órgano rector ha de asegurarse de que las actividades de seguridad de la información se ajustan adecuadamente a los requisitos internos y externos encargando que se realicen auditorías de seguridad independientes.

Principio 5: Fomentar un entorno propicio a la seguridad

La gobernanza de la seguridad de la información se ha de basar en el comportamiento humano, incluidas las necesidades presentes y futuras de todos los interesados, pues la seguridad de la información es básicamente un problema humano. De no coordinarse adecuadamente, los objetivos, funciones, responsabilidades y recursos pueden entrar en conflicto unos con otros y hacer que no se cumplan los objetivos empresariales. Por consiguiente, la armonización y la concertación entre los distintos interesados son muy importantes.

Para crear una cultura de la seguridad de la información, el órgano rector exigirá que se coordinen las actividades de los interesados de manera coherente para la seguridad de la información, para lo que comprenderán, entre otras cosas, programas de educación, formación y concienciación en materia de seguridad.

Principio 6: Examen del rendimiento en relación con los resultados empresariales

La gobernanza de la seguridad de la información deberá garantizar que el enfoque 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 ajustarse a los requisitos empresariales actuales y futuros.

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.

5.3 Procesos

5.3.1 Aspectos generales

El órgano rector y la dirección ejecutiva utilizan los procesos "evaluar", "dirigir", "supervisar" y "comunicar" para regir la seguridad de la información. Además, el proceso "asegurar" ofrece una opinión independiente y objetiva de la gobernanza de la seguridad de la información y del nivel alcanzado. En la Figura 2 se muestra la relación entre estos procesos.

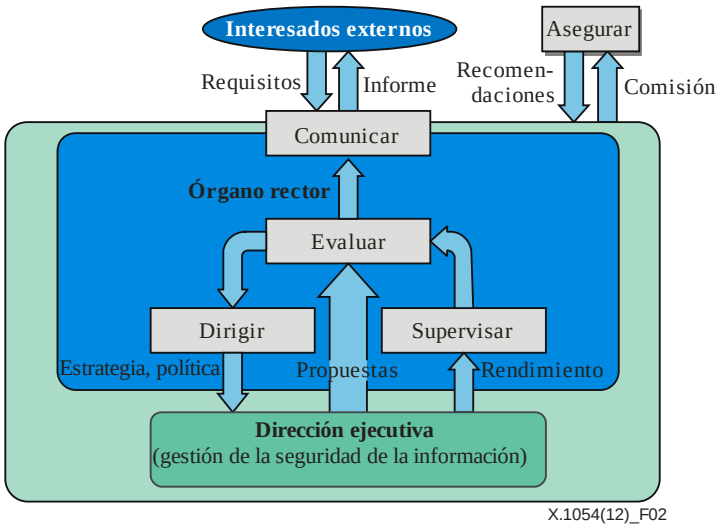

Figura 2 – Procesos de gobernanza de la seguridad de la información

5.3.2 Evaluar

"Evaluar" es 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 el logro de los objetivos estratégicos en el futuro.

Para realizar el proceso "evaluar", el órgano rector debe:

- garantizar que las iniciativas empresariales tienen en cuenta los problemas de seguridad de la información;
- responder a los resultados del rendimiento de la seguridad de la información, establecer prioridades y tomar las medidas necesarias.

Para realizar el proceso "evaluar", la dirección ejecutiva debe:

- garantizar que la seguridad de la información respalda y sostiene los objetivos empresariales;
- someter a la consideración del órgano rector nuevos proyectos de seguridad de la información de gran importancia para la organización.

5.3.3 Dirigir

"Dirigir" es el proceso de gobernanza mediante el cual el órgano rector determina qué objetivos de seguridad de la información se han de lograr y qué estrategia se va a utilizar para ello. 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:

- determinar el nivel de riesgo que la organización está dispuesta a correr;
- aprobar la estrategia y la política de seguridad de la información;
- atribuir las inversiones y recursos necesarios.

Para realizar el proceso "dirigir", la dirección ejecutiva debe:

- elaborar y poner en práctica una estrategia y una política de seguridad de la información;
- armonizar los objetivos de seguridad de la información con los objetivos empresariales;
- fomentar una cultura positiva de la seguridad de la información.

5.3.4 Supervisar

"Supervisar" es el proceso de gobernanza que permite al órgano rector evaluar el logro de los objetivos estratégicos.

Para realizar el proceso "supervisor", el órgano rector debe:

- evaluar la eficacia de las actividades de gestión de la seguridad de la información;
- garantizar la conformidad con los requisitos internos y externos;
- considerar los cambios en el entorno empresarial, jurídico y reglamentario y sus posibles consecuencias en materia de riesgos para la información.

Para realizar el proceso "supervisor", la dirección ejecutiva debe:

- seleccionar los parámetros de medición del rendimiento adecuados desde la perspectiva empresarial;
- comunicar los resultados del rendimiento de la seguridad de la información al órgano rector, incluido el rendimiento de las actividades determinadas previamente por el órgano rector y sus repercusiones sobre la organización;
- alertar al órgano rector de las novedades que puedan afectar a los riesgos en material de información y a la seguridad de la información.

5.3.5 Comunicar

"Comunicar" es 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 medios para "comunicar" es el estado de seguridad de la información, donde se explican las actividades de seguridad de la información, y los problemas correspondientes, a los interesados. En los Anexos A y B se muestran ejemplos de ello.

Para realizar el proceso "comunicar", el órgano rector debe:

- informar a los interesados externos de que las prácticas de la organización en cuanto a seguridad de la información se ajustan a la naturaleza del negocio;
- notificar a la dirección ejecutiva los resultados de todo examen externo realizado donde se hayan identificado problemas de seguridad de la información, y solicitar la aplicación de medidas correctivas;
- aceptar información sobre obligaciones reglamentarias, expectativas de los interesados y necesidades de la empresa, con respecto a la seguridad de la información.

Para realizar el proceso "comunicar", la dirección ejecutiva debe:

- aconsejar al órgano rector acerca de cualquier tema que merezca su atención y, posiblemente, decisión;
- encargar a los interesados internos la adopción de medidas concretas de acuerdo con las directivas y decisiones adoptadas por el órgano rector.

5.3.6 Asegurar

"Asegurar" es el proceso de gobernanza mediante el cual el órgano rector encarga que se realicen auditorías, exámenes o certificaciones independientes y objetivos, que identificarán y validarán los objetivos y las medidas adoptadas para llevar a cabo las actividades de gobernanza y llevar a cabo las operaciones a fin de alcanzar el nivel deseado de seguridad de la información.

Para realizar el proceso "asegurar", el órgano rector debe:

- solicitar opiniones independientes y objetivas sobre cómo se está responsabilizando de alcanzar el nivel deseado de seguridad de la información.

Para realizar el proceso "asegurar", la dirección ejecutiva debe:

- respaldar las auditorías, exámenes o certificaciones encargados por el órgano rector.

Anexo A

Ejemplo de estado de seguridad de la información

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

Una organización puede preparar un estado de seguridad de la información y comunicarlo a sus clientes e interesados como herramienta de comunicación para la seguridad de la información.

La organización debe seleccionar el formato y el contenido del estado de seguridad de la información. En este Anexo A se presenta un ejemplo que utiliza las conclusiones positivas de una auditoría de seguridad de la información.

Cuadro A – Estado de seguridad de la información

La administración se satisface en comunicar que durante el periodo comprendido entre **mmm** y **nnn**, el funcionamiento de los controles y procedimientos de seguridad de la información, realizados de conformidad con los criterios **xyz** (por ejemplo, serie 27000, COBIT) sobre los procedimientos y sistemas operativos de la organización, suplementados por controles de gestión de alto nivel, fue suficiente para garantizar razonablemente que se han logrado los objetivos de control de la seguridad de la información definidos con respecto a la confidencialidad, la integridad y la disponibilidad. La administración ha transmitido a **ABC**, auditores de seguridad de la información externos, una carta de representación a tal efecto. La Junta de Directores encargó a ABC el examen de la afirmación de control de la seguridad de la información de la administración. Este examen se realizó de conformidad con las normas establecidas y comprendió una evaluación de la eficacia estructural y operativa de los controles y procedimientos de seguridad de la información por muestreo. **ABC** comunicó a la administración su opinión, según la cual los resultados de las pruebas indican que, con excepciones concretas, de acuerdo con los criterios de gestión identificados, **xyz** (por ejemplo, serie 27000, CobiT), los controles son materialmente eficaces. La carta de plena afirmación de la administración y el Informe de auditoría externa con las excepciones identificadas en relación con los controles de seguridad de la información se discutió con la Comisión de Auditoría y se distribuyó entre todos los miembros de la Junta. Los interesados pueden solicitar copias.

NOTA – "nnn", "mmm", "xyz", "ABC" son genéricos. En los estados reales deberán incluirse las fechas y los nombres específicos.

Anexo B

Ejemplo de estado de seguridad de la información detallado

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

En este Anexo B se presenta un ejemplo de estado de seguridad de la información donde se detallan los contenidos. Este modelo es particularmente útil para las organizaciones que esperan mejorar su reputación haciendo hincapié en su seguridad, por ejemplo, empresas de TIC. La transparencia en cuanto a riesgos de seguridad y comunicación de información también sirve para aumentar la confianza. Gracias a estas actividades los interesados pueden estar al tanto de la situación.

Cuadro B – Estado de seguridad de la información detallado

Introducción

- **Alcance** (estrategia, políticas, normas), **perímetro** (unidades geográficas/orgánicas), **periodo abarcado** (mes/trimestre/semestre/año)

Estado general

- **Satisfactorio/casi satisfactorio/no satisfactorio**

Actualizaciones (según proceda y sea pertinente)

- Progreso de la estrategia de seguridad de la información

  Elementos completados/en curso/planificados
- Modificación del sistema de gestión de seguridad de la información

  Revisión de la política ISMS, estructura orgánica para la aplicación de ISMS (incluida la asignación de responsabilidades)
- Progreso hacia la certificación

  (Re)certificación ISMS, auditorías de seguridad de la información certificadas
- Presupuesto/dotación de personal/formación

  Situación financiera, adecuación de la plantilla, cualificación en seguridad de la información
- Otras actividades de seguridad de la información

  Participación en la dirección de continuidad empresarial, campañas de concienciación, asistencia de auditoría interna/externa

Problemas significativos (de haberlos)

- Resultado de los exámenes de seguridad de la información

  Recomendaciones, respuestas de gestión, planes de acción, plazos
- Progreso en relación con los informes de auditoría interna/externa más importantes

  Recomendaciones, respuestas de gestión, planes de acción, plazos
- Incidentes de seguridad de la información

  Consecuencias previstas, planes de acción, plazos
- (In)cumplimiento de la legislación y los reglamentos correspondientes

  Consecuencias previstas, planes de acción, plazos

Decisión(es) necesarias (en su caso)

- Recursos adicionales

  Destinados a que la seguridad de la información sustente las iniciativas empresariales

Bibliografía

[1] Recomendación UIT-T X.1051 (2008) | ISO/CEI 27011:2008, *Tecnología de la información – Técnicas de seguridad – Directrices basadas en la norma ISO/CEI 27002 para la gestión de la seguridad de la información para organizaciones de telecomunicaciones*.

[2] ISO/IEC 27001:2005, *Information technology – Security techniques – Requirements of information security management systems*.

[3] ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management*.

[4] ISO/IEC 27005:2011, *Information technology – Security techniques – Information security risk management.*

[5] ISO/IEC 38500:2008, *Corporate Governance of Information technology*.

[6] ITGI, *Information Security Governance framework: 2009*.

[7] ISF, *Standard of Good Practice for Information Security: 2011*.

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
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	Construcción, instalación y protección de los cables y otros 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	Terminales y métodos de evaluación subjetivos y objetivos
Serie Q	Conmutación y señalización
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 y redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2013