NORMA
CHILENA

NCh ISO/IEC 27035/1

Primera edición
2018.12.26

Tecnología de la información — Técnicas de seguridad — Gestión de incidentes de seguridad de la información — Parte 1: Principios de gestión de incidentes

Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management

ICS 35.030

INSTITUTO NACIONAL DE NORMALIZACION

Número de referencia
NCh-ISO/IEC 27035/1:2018
29 páginas

DOCUMENTO PROTEGIDO POR COPYRIGHT

Instituto Nacional de Normalización - INN

Av. Libertador Bernardo O'Higgins 1449, Santiago Downtown Torre 7, piso 18 • Santiago de Chile

Tel. + 56 2 2445 88 00

Correo Electrónico contacto@inn.cl

Sitio Web www.inn.cl

Publicado en Chile

Contenido

Página

Figuras

Tablas

Preámbulo

El Instituto Nacional de Normalización, INN, es el organismo que tiene a su cargo el estudio y preparación de las normas técnicas a nivel nacional. Es miembro de la INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO) y de la COMISION PANAMERICANA DE NORMAS TECNICAS (COPANT), representando a Chile ante esos organismos.

Esta norma se estudió a través del Comité Técnico CL013 *Tecnologías de la Información*, para entregar herramientas básicas orientadas a la gestión de incidentes de la seguridad de la información, con el objeto de detectar, informar, analizar y responder a incidentes, y aplicar las lecciones aprendidas.

Esta norma es una adopción idéntica de la versión en inglés de la Norma ISO/IEC 27035-1:2016 *Information technology - Security techniques - Information security incident management - Part 1: Principles of incident management*, y ha sido elaborada por el Instituto Nacional de Normalización.

Para los propósitos de esta norma, se han realizado los cambios editoriales que se indican y justifican en Anexo E.

La Nota Explicativa incluida en un recuadro en Anexo D Bibliografía, es un cambio editorial que se incluye con el propósito de informar la equivalencia de las Normas Internacionales citadas en esta norma con las Normas Chilenas.

Los Anexos A, B, C, D y E no forman parte de la norma, se insertan sólo a título informativo.

Esta norma ha sido aprobada por el Consejo del Instituto Nacional de Normalización, en sesión efectuada el 26 de diciembre de 2018.

Si bien se ha tomado todo el cuidado razonable en la preparación y revisión de los documentos normativos producto de la presente comercialización, INN no garantiza que el contenido del documento es actualizado o exacto o que el documento será adecuado para los fines esperados por el Cliente.

En la medida permitida por la legislación aplicable, el INN no es responsable de ningún daño directo, indirecto, punitivo, incidental, especial, consecuencial o cualquier daño que surja o esté conectado con el uso o el uso indebido de este documento.

Introducción

Las políticas de seguridad de la información o los controles por si solos no garantizan la protección total de la información, sistemas de información, servicios o redes. Luego de la implementación de controles, permanecerán vulnerabilidades residuales, las que pueden reducir la eficacia de la seguridad de la información y facilitar la ocurrencia de incidentes de seguridad. Esto puede tener impactos negativos tanto directos como indirectos en las operaciones de negocio de una organización. Además, es inevitable que ocurran instancias nuevas de amenazas que no hayan sido identificadas previamente. Una preparación insuficiente para lidiar con estos incidentes, por parte de una organización hará menos efectiva cualquier respuesta y aumentará el impacto negativo sobre la empresa. Por este motivo, es esencial para cualquier organización que desea un programa sólido de seguridad de la información, que posea un enfoque estructurado y enfocado a:

— detectar, informar y analizar los incidentes de seguridad de la información;

— responder a estos incidentes, incluyendo a la activación adecuada de controles para la prevención, reducción y recuperación de los impactos del incidente;

— informar las vulnerabilidades de seguridad de la información, para que se puedan analizar y tratar adecuadamente;

— aprender de los incidentes y vulnerabilidades, instituir controles preventivos y realizar mejoras al enfoque general de la gestión de la seguridad de la información.

Con el propósito de lograr este enfoque planificado, ISO/IEC 27035 provee orientaciones sobre los aspectos de gestión de la seguridad de la información en las siguientes partes.

— ISO/IEC 27035-1, Principios de la gestión de incidentes (esta norma), presenta los conceptos básicos y las fases de la gestión de la seguridad de la información, así como mejorar la gestión de incidentes. Esta parte combina estos conceptos con los principios en un enfoque estructurado para detectar, informar, analizar y responder a los incidentes, además de aplicar las lecciones aprendidas.

— ISO/IEC 27035-2, Directrices para planificar y preparar una respuesta ante un incidente, describe como se debe planificar y preparar una respuesta ante un incidente. Esta parte abarca las fases de "Planificar y Preparar" junto con las "Lecciones Aprendidas" del modelo presentado en ISO/IEC 27035-1.

ISO/IEC 27035 está destinada a complementar otros estándares y documentos que proporcionan orientación para la investigación y preparación para investigar incidentes de seguridad de la información. ISO/IEC 27035 no es una guía exhaustiva, sino más bien una referencia para ciertos principios fundamentales que permiten la selección de las herramientas, técnicas y métodos adecuados para este propósito.

Mientras que ISO/IEC 27035 abarca la gestión de los incidentes de seguridad de la información, también cubre algunos aspectos de vulnerabilidades de seguridad de la información. La orientación para la divulgación de vulnerabilidades y su administración por los proveedores se encuentran en ISO/IEC 29147 y ISO/IEC 30111, respectivamente.

ISO/IEC 27035 pretende también informar a los entes decisorios que necesitan determinar la fiabilidad de la evidencia digital presentados a ellos. Es aplicable a organizaciones que necesiten proteger, analizar y presentar posibles pruebas digitales. Es relevante para los organismos políticos que crean y evalúan procedimientos relacionados a las evidencias digitales, como parte de un gran cuerpo de evidencias.

Más información sobre estándares investigativos se encuentra disponible en el Anexo A.

Tecnología de la información — Técnicas de seguridad — Gestión de incidentes de seguridad de la información — Parte 1: Principios de gestión de incidentes

1 Alcance y campo de aplicación

Esta parte de ISO/IEC 27035 es la base de esta norma multiparte. Presenta conceptos y fases básicos para la gestión de incidentes de la seguridad de la información, combinando estos conceptos con principios en un enfoque estructurado para la detección, informe, análisis y respuesta a los incidentes, además de aplicar las lecciones aprendidas.

Los principios entregados en esta parte de ISO/IEC 27035, son genéricos con la intención de poder ser aplicables a todas las organizaciones, sin importar su tipo, tamaño o naturaleza. Las organizaciones pueden ajustar las orientaciones entregadas en esta parte de ISO/IEC 27035, de acuerdo a su tipo, tamaño o naturaleza de su negocio en relación a una situación de riesgo de seguridad de la información. Esta parte de ISO/IEC 27035 es también aplicable a organizaciones externas que entreguen servicios de gestión de la seguridad de la información.

2 Referencias Normativas

Los siguientes documentos, en todo o en parte, están referenciados normativamente en este documento y son indispensables para su aplicación. Para las referencias con fecha, sólo se aplica la edición citada. Para las referencias sin fecha, se aplica la última edición citada. Para las referencias sin fecha, se aplica la última edición del documento referenciado (incluidas las enmiendas).

ISO/IEC 27000, *Information technology - Security techniques - Information security management systems - Overview and vocabulary.*

ISO/IEC 27035-2, *Information technology - Security techniques - Information security incident management - Part 2: Guidelines to plan and prepare for incident response.*

NOTA EXPLICATIVA NACIONAL

La equivalencia de las Normas Internacionales señaladas anteriormente con Norma Chilena, y su grado de correspondencia es el siguiente:

Norma Internacional	Norma nacional	Grado de correspondencia
ISO/IEC 27000:2018	NCh-ISO IEC 27000:2018	Idéntica
ISO/IEC 27035	No existe	-

3 Términos y definiciones

Para los propósitos de esta norma, se aplican los términos y definiciones dados en ISO/IEC 27000 y los siguientes:

ISO y la Comisión Electrónica Internacional, IEC, mantienen bases de datos terminológicas para su uso en la normalización en las siguientes direcciones:

— Plataforma de navegación ISO: disponible en http://www.iso.org/obp

— IEC Electropedia: disponible en http://www.electropedia.org/

3.1
investigación de seguridad de la información
aplicación de pruebas, análisis e interpretaciones para ayudar a comprender un incidente de seguridad de la *información* (3.4)

[Fuente: ISO/IEC 27042, 3.1, modificada - La frase "un incidente" fue reemplazada por "incidente de seguridad de la información".]

3.2
equipo de respuesta a incidente
IRT[1]
equipo de miembros calificados y confiables de la organización que maneja los incidentes durante su ciclo de vida

Nota 1 a la entrada: CERT[2] (Equipo de respuesta a emergencias) y CSIRT[3] (Equipos de respuesta a incidentes de seguridad de la información) son términos usados comúnmente para los IRT.

3.3
evento de seguridad de la información
suceso que indica una posible brecha en la seguridad de la información o falla en el control de ésta

3.4
incidente de seguridad de la información
uno o varios eventos identificados con relación a *seguridad de la información* (3.3) que puedan dañar los activos de una organización o comprometer sus operaciones

3.5
gestión de incidentes de seguridad de la información
actividad de un enfoque eficaz y coherente para el manejo de incidentes de seguridad de la información

3.6
manejo de incidentes
acción de detectar, informar, analizar, reaccionar, enfrentar y aprender de los *incidentes de seguridad de la información* (3.4)

1 En inglés: *Incident response team, IRT.*

2 En inglés: *Computer Emergency Response Team, CERT.*

3 En inglés: *Computer Security Incident Response Team, CSIRT.*

3.7
respuesta a incidentes
acciones para mitigar o resolver un incidente de seguridad de la información (3.4), incluyendo aquellas acciones tomadas para proteger y restaurar las condiciones normales de operación de un sistema de información, así como la información almacenada en él

3.8 punto de contacto
PoC[4]
función o rol definido en una organización que sirve como coordinador o punto focal de información relacionadas con las actividades de gestión del incidente

4 Resumen

4.1 Conceptos básicos y principios

Un evento de seguridad de la información es un suceso que indica una posible brecha en la seguridad de la información o falla en el control de ésta. Un incidente de seguridad de la información corresponde a uno o varios eventos identificados que cumplen una serie de criterios establecidos y que puedan dañar los activos de una organización o comprometer sus operaciones.

Un evento de seguridad de la información no significa necesariamente que un ataque ha sido exitoso o que se hayan visto afectadas la confidencialidad, integridad o disponibilidad, por nombrar algunos ejemplos. Es decir, no todos los eventos de seguridad de la información son clasificados como incidentes de seguridad.

Los incidentes de seguridad de la información pueden ser deliberados (por ejemplo, causados por un software malicioso o una falta disciplinaria intencional) o accidentales (por ejemplo, un error humano involuntario o por actos inevitables de la naturaleza) y pueden ser causados por medios técnicos (por ejemplo, virus computacional) o no técnicos (pérdida o robo de un computador). Las consecuencias pueden incluir la divulgación no autorizada, modificación, destrucción, la inaccesibilidad de información, o daño o robo de activos de la organización que contengan información.

El Anexo B, proporciona descripciones de los ejemplos de incidentes de seguridad de la información seleccionados, así como sus causas para fines informativos. Es importante destacar que estos ejemplos no son exhaustivos.

Una amenaza aprovecha las vulnerabilidades (debilidades) en los sistemas, servicios o redes de información, causando eventos de seguridad de la información y con ello potenciales incidentes a los activos de información expuestos por estas vulnerabilidades. Figura 1 muestra la relación entre objetos en un incidente de seguridad de la información.

4 En inglés: *Point of contact, PoC.*

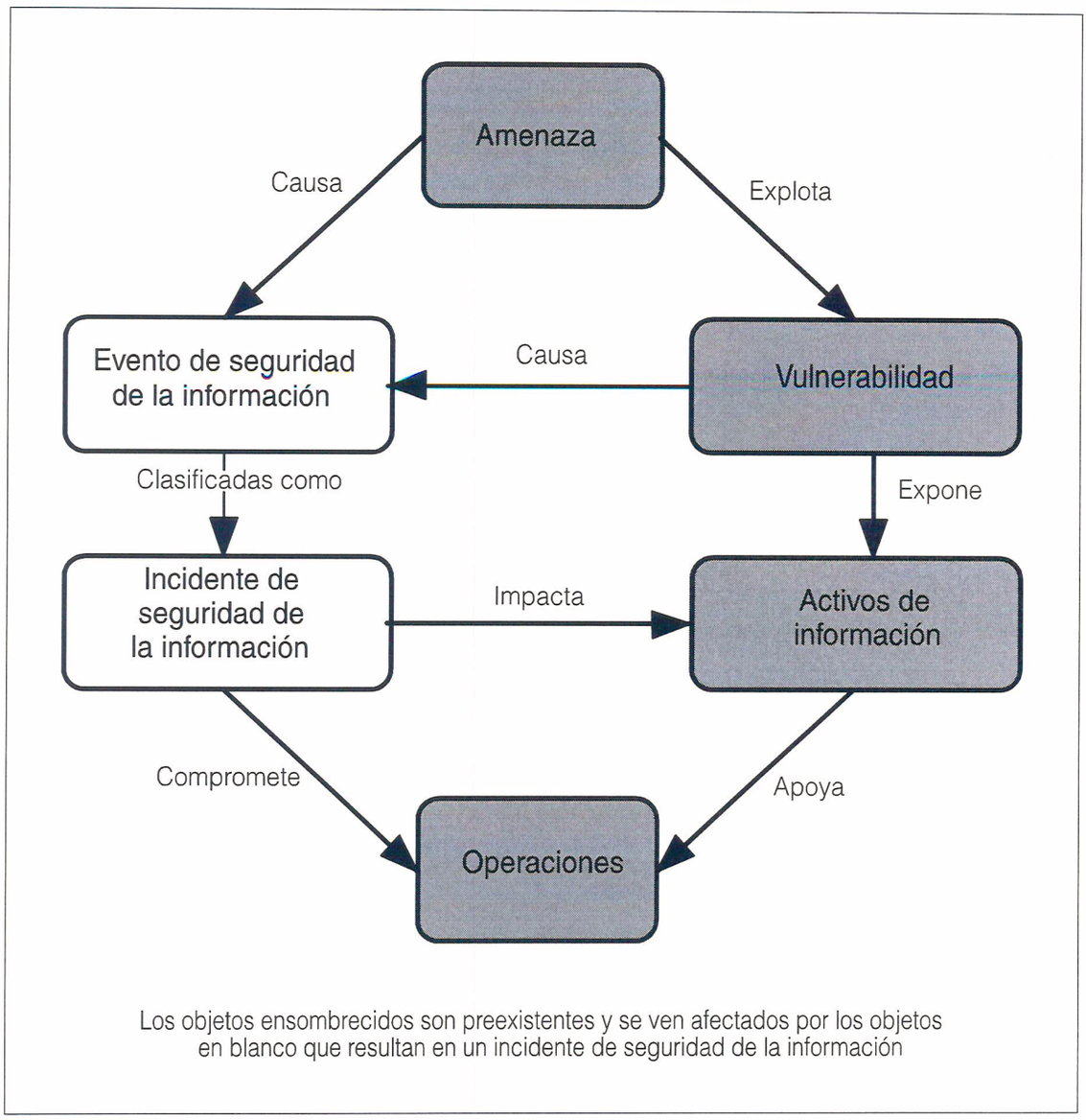

Figura 1 – Relación de los objetos en un incidente de seguridad de la información

Es importante considerar la coordinación e intercambio de información con los IRTs externos. Muchos incidentes cruzan las barreras organizacionales y no pueden ser resueltos fácilmente por un solo IRT. El intercambio de información y las relaciones de coordinación o sociedades con IRTs externos puede mejorar la capacidad de respuesta o resolución de estos incidentes. Para mayor detalle sobre el intercambio de información, ver ISO/IEC 27010.

4.2 Objetivos de la gestión de incidentes

Como parte fundamental de las estrategias de seguridad de la información de una organización, esta debería establecer controles y procedimientos para permitir un enfoque estructurado y planificado para la gestión de incidentes de seguridad de la información. Desde el punto de vista de una organización, el objetivo principal es evitar o contener el impacto de un incidente de seguridad de la información, para minimizar un daño directo o indirecto a sus operaciones. Debido a que el daño a los activos de información pueden tener un impacto negativo en las operaciones, las perspectivas del negocio u operacionales deberían dar énfasis a la definición de objetivos mas específicos para la gestión de la seguridad de la información.

Algunos objetivos específicos de una metodología estructurada y planificada para la gestión de incidentes debería incluir lo que sigue:

a) los eventos de seguridad de la información son detectados y tratados eficientemente, en particular cuando estos deberían ser clasificados como incidentes de seguridad de la información;

b) los incidentes de seguridad de la información identificados, son analizados y tratados de la forma más eficiente y apropiada;

c) los efectos adversos de los incidentes de seguridad de la información en las organizaciones y sus operaciones son minimizados por medio controles adecuados, como parte de la respuesta a este incidente;

d) establecer un enlace con los elementos más importantes de la gestión de crisis y la gestión de la continuidad del negocio, por medio de un proceso escalonado;

e) analizar las vulnerabilidades de la seguridad de la información y hacer un tratamiento apropiado para prevenir o reducir los incidentes. Este análisis puede ser realizado por el IRT u otro equipo al interior de la organización, dependiendo de la distribución de las tareas;

f) las lecciones se aprenden rápidamente debido a los incidentes de seguridad de la información, así como las vulnerabilidades y su gestión. Este mecanismo de retroalimentación está diseñado para aumentar las oportunidades de prevención de un futuro incidente de seguridad de la información, mejorando la implementación y uso de los controles de seguridad de la información, y también mejorar el plan de gestión de incidentes de seguridad de la información.

Para ayudar a lograr estos objetivos, las organizaciones deberían asegurar que los incidentes de seguridad de la información se documenten de forma detallada, utilizando los estándares apropiados para la categorización del incidente, su clasificación además de compartirlos, así estas mediciones pueden ser derivadas de los datos acumulados durante un período de tiempo. Esto proporciona información valiosa para ayudar en el proceso estratégico de toma de decisiones, cuando se invierte en controles de seguridad de la información. El sistema de gestión de incidentes de seguridad de la información debería ser capaz de compartir esta información con colaboradores externos pertinentes e IRTs.

Otro objetivo asociado con esta parte de ISO/IEC 27035, es proporcionar las orientaciones para las organizaciones que buscan obtener los requerimientos para el Sistema de Gestión de la Seguridad de la información (SGSI[5]), especificados en ISO/IEC 27001, la cual se basa en la orientación

5 En Inglés: *Information Security Management System, ISMS.*

de ISO/IEC 27002. ISO/IEC 27001, incluye requerimientos relacionados a la gestión de incidentes de seguridad de la información. El Anexo C proporciona una tabla con referencias cruzadas de las cláusulas de la gestión de incidentes de seguridad de la información de ISO/IEC 27001 y las cláusulas en esta parte de la norma ISO/IEC 27035.Las relaciones con SGSI se explican en Figura 2. Esta parte de ISO/IEC 27035 también puede apoyar los requerimientos de los sistemas de gestión de seguridad de la información aparte de los SGSI.

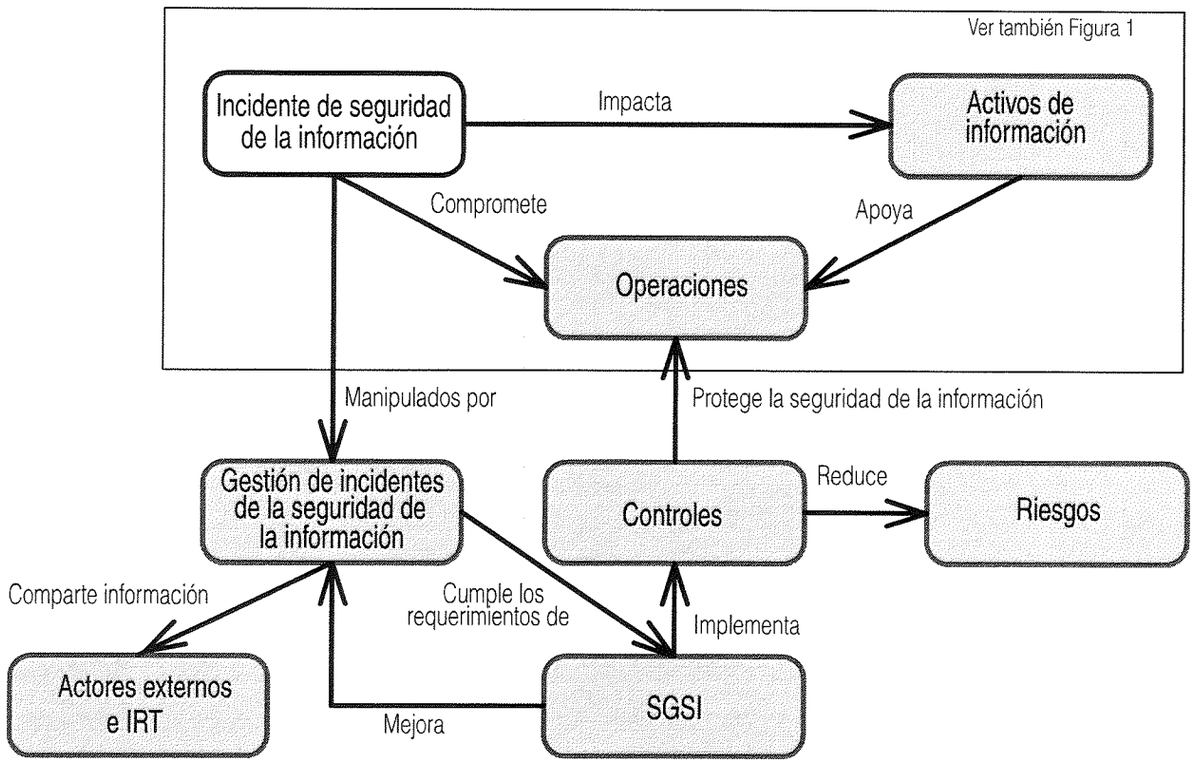

Figura 2 – Gestión de incidentes de la seguridad de la información en relación con el SGSI y controles aplicados

4.3 Beneficios de un enfoque estructurado

Utilizar un enfoque estructurado para la gestión de incidentes de seguridad de la información, puede generar beneficios importantes, los cuales pueden ser agrupados bajo los siguientes temas.

a) Mejora de la seguridad de la información en general

Un proceso estructurado para la detección, informe y análisis de eventos e incidentes de seguridad de la información y la toma de decisiones relacionadas, permitirán una rápida identificación y respuesta. Esto mejorará la seguridad en general, ayudando a identificar e implementar rápidamente una solución coherente y con esto proporcionar una forma de prevenir incidentes similares de seguridad de la información a futuro. Además, existirán beneficios ganados por las mediciones, el intercambio y la acumulación. La credibilidad de la organización mejorará mediante la demostración de la implementación de las mejores prácticas, en relación a la gestión de incidentes de seguridad de la información.

b) Reducir los impactos adversos en el negocio

Un enfoque estructurado de la gestión de incidentes de seguridad de la información permite reducir el nivel de impacto adverso en el negocio, asociado a incidentes de seguridad de la información. Estos impactos pueden incluir una pérdida financiera inmediata o a largo plazo, que surge por el daño a la reputación y su credibilidad. Para orientaciones sobre el análisis del impacto en el negocio, ver ISO/IEC 27005. Para orientaciones sobre la disponibilidad de tecnologías de la información y comunicación para la continuidad del negocio, ver ISO/IEC 27031.

c) Fortalecer el foco sobre la prevención de incidentes de seguridad de la información

Utilizar un enfoque estructurado para la gestión de incidentes de la seguridad de la información, ayuda al fortalecimiento del enfoque preventivo al interior de la organización, incluyendo el desarrollo de métodos para identificar nuevas amenazas y vulnerabilidades. El análisis de datos relacionados a un incidente permite la identificación de patrones y tendencias, facilitando en enfoque más preciso en la prevención de incidentes, así como la identificación de acciones preventivas a seguir para evitar eventos futuros.

d) Mejorar la priorización

Un enfoque estructurado para la gestión de incidentes de seguridad de la información, proporcionará una base sólida para priorizar cuando se investigan de incidentes de seguridad de la información, incluyendo el uso de categorizaciones efectivas y escalas de clasificación. Si no existen procedimientos claros, existe el riesgo que la investigación se vuelva demasiado reactiva, respondiendo a los incidentes una vez que estos ocurren, pasando por alto actividades que se deberían manejar con mayor prioridad.

e) Apoyar la investigación y recopilación de evidencia

Cuando sea necesario, procedimientos claros de investigación de incidentes permitirá asegurar que la recopilación de datos y su manipulación sean consecuentes y admisibles legalmente. Estas son consideraciones muy importantes en el caso de continuar una prosecución legal o se tomen acciones disciplinarias. Para más información sobre evidencia digital y las investigaciones, ver estándares investigativos contenidos en Anexo A.

f) Contribuir al presupuesto y justificación de recursos

Utilizar un enfoque bien definido y estructurado para la gestión de incidentes de seguridad de la información, ayudará a justificar y simplificar la asignación de presupuestos y recursos a las unidades organizacionales involucradas. Además, estas ventajas cubrirán el plan de gestión de incidentes de seguridad de la información, permitiendo planificar una mejor asignación de personal y recursos.

Un ejemplo de una forma de controlar y optimizar el presupuesto y los recursos es incorporar un seguimiento temporal a las tareas de gestión de incidentes de seguridad, para facilitar el análisis cuantitativo del manejo de los incidentes de seguridad de la información por parte de la organización. Esto debería proporcionar información de cuánto tiempo se tarda en resolver un incidente de seguridad de la información de diferentes prioridades y en diferentes plataformas. Si existe un obstáculo en el proceso de gestión de incidentes en la seguridad de la información, esto se debería identificar.

g) Mejorar actualizaciones para el análisis de riesgos de seguridad de la información y la gestión de resultados

Utilizar un enfoque estructurado para la gestión de incidentes de seguridad de la información, facilitará:

— mejorar la recopilación de datos para facilitar la identificación y resolución de las características de las diferentes amenazas y vulnerabilidades asociadas;

— proveer de datos sobre frecuencia de ocurrencia de los tipos identificados de amenazas.

Los datos recopilados sobre los impactos negativos en las operaciones del negocio debido a incidentes de seguridad de la información, serán útiles en el análisis del impacto en el negocio. Los datos recopilados para identificar la frecuencia de varios tipos de amenazas, mejorará la calidad del análisis de amenazas. De forma similar, los datos recopilados sobre las vulnerabilidades mejorarán la calidad de los análisis de los mismos. Para orientaciones sobre la gestión y análisis de los riesgos de seguridad de la información, ver ISO/IEC 27005.

h) Proporcionar un mejor conocimiento de seguridad de la información y el material para un programa de entrenamiento

Utilizar un enfoque estructurado para la gestión de incidentes de seguridad de la información, permitirá a la organización incorporar experiencias y conocimiento sobre el manejo de incidentes, los cuales serán un material valioso para el programa de conocimiento de seguridad de la información. Un programa de conocimiento que incluya las lecciones aprendidas desde la experiencia real ayudará a reducir los errores o confusiones durante un futuro incidente de seguridad de la información.

i) Proporcionar entradas a las políticas de seguridad de la información y revisiones de los documentos relacionados

Los datos proporcionados por el plan de gestión de incidentes de seguridad de la información, podrían ser un aporte valioso para las revisiones de efectividad y un mejoramiento subsecuente de las políticas de gestión de incidentes de seguridad (y cualquier otro documento relacionado con la seguridad de la información). Esto aplica a las políticas específicas y otros documentos aplicables tanto para la organización completa como para un sistema, servicio o red en particular.

4.4 Adaptabilidad

Las directrices entregadas por ISO/IEC 27035 (todas sus partes) es extensa, si se adopta en forma completa, y podría requerir una importante cantidad de recursos para su operación y gestión. Entonces, es importante que una organización que aplique estas orientaciones debería retener un sentido de perspectiva y asegurar que los recursos aplicados a la gestión de incidentes de seguridad de la información y la complejidad de los mecanismos implementados son proporcionales a lo siguiente:

a) tamaño, estructura y naturaleza del negocio de una organización, incluyendo sus activos críticos principales, procesos y los datos que deberían estar protegidos;

b) alcance y campo de aplicación de los sistemas de gestión de la seguridad de la información para el manejo de incidentes;

c) riesgos potenciales debido a incidentes;

d) objetivos de la empresa.

Una organización que haga uso de esta parte de ISO/IEC 27035 debería por lo tanto adoptar estas orientaciones de forma que sean relevantes para las proporciones y características del negocio.

5 Fases

5.1 Resumen

Para alcanzar los objetivos descritos en 4.2, gestión de incidentes de seguridad de la información consta de las cinco fases siguientes:

— Planificación y preparación (ver 5.2);

— Detección e Informes (ver 5.3);

— Análisis y decisión (ver 5.4);

— Respuestas (ver 5.5);

— Lecciones aprendidas (ver 5.6).

Una imagen de alto nivel de estas fases se muestra en la Figura 3.

Algunas actividades pueden ocurrir en múltiples fases o durante el proceso de manejo del incidente. Tales actividades incluyen lo siguiente:

— documentación de evidencia de eventos e información clave de incidentes, acciones de respuesta tomadas y acciones de seguimiento realizadas como parte del proceso de manejo de incidentes;

— coordinación y comunicación entre las partes involucradas;

— notificación de incidentes significativos a la gerencia y otras partes interesadas;

— intercambio de información entre las partes interesadas y colaboradores internos y externos, tales como proveedores y otros IRTs.

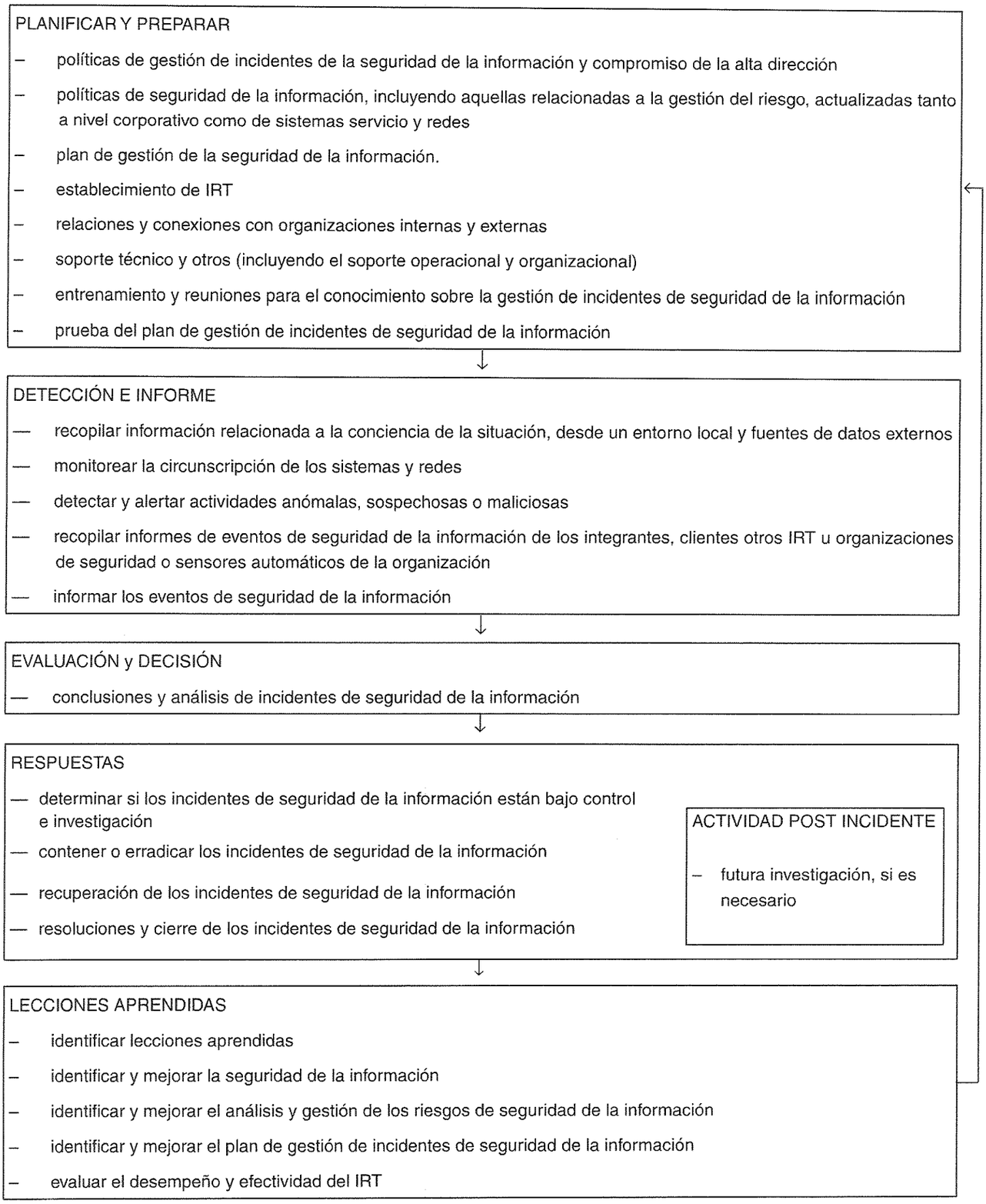

Figura 3 – Fases de la gestión de incidentes de seguridad de la información

Como se indicó en la Introducción, ISO/IEC 27035 está dividida en dos partes.

— ISO/IEC 27035-1 abarca completamente las cinco fases.

— ISO/IEC 27035-2 abarca:

  — Planificar y preparar, y

  — Lecciones aprendidas

Figura 4 muestra el flujo de eventos e incidentes de seguridad de la información a través de las fases de la gestión de incidentes de seguridad de la información y actividades relacionadas.

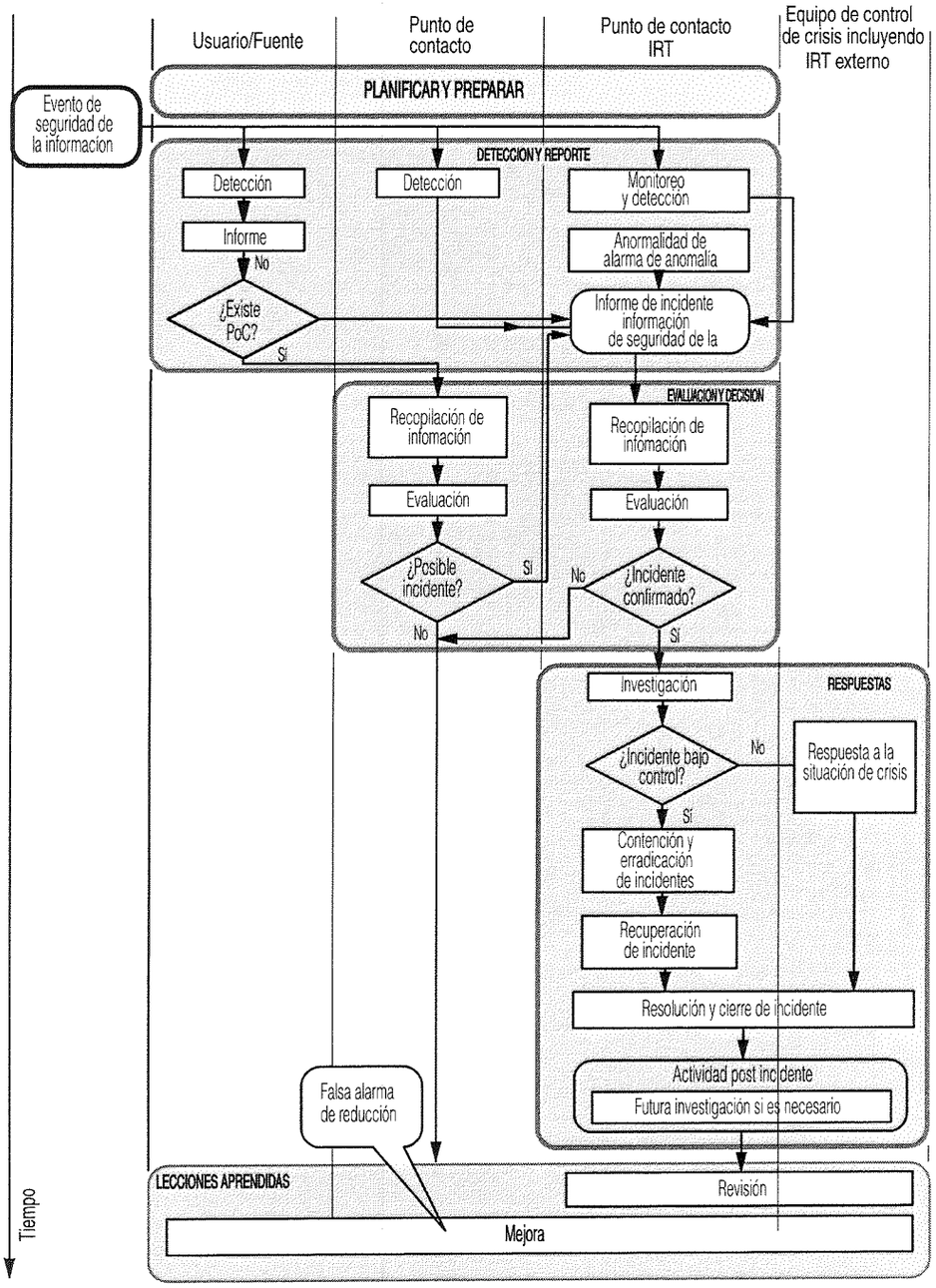

Figura 4 – Evento de seguridad de la información y diagrama de flujo de incidentes

5.2 Planificar y preparar

La eficaz gestión de incidentes de seguridad de la información requiere una planificación y preparación adecuadas. Para que un plan de gestión de incidentes de seguridad de la información eficiente y efectivo se ponga en funcionamiento, una organización debe completar una serie de actividades preparatorias, a saber:

a) formular y producir una política de gestión de incidentes de seguridad de la información y obtener el compromiso de la alta dirección con esa política;

b) actualizar las políticas de seguridad de la información, incluyendo las relacionadas con la gestión de riesgos, a nivel corporativo y a nivel de sistema, servicio y redes;

c) definir y documentar un plan detallado de gestión de incidentes de seguridad de la información, incluyendo los temas que cubran las comunicaciones y la divulgación de información;

d) establecer el IRT, con un programa de capacitación apropiado diseñado, desarrollado y proporcionado a su personal;

e) establecer y preservar las relaciones y conexiones adecuadas con organizaciones internas y externas que están directamente involucradas en la gestión de eventos, incidentes y vulnerabilidades de seguridad de la información;

f) establecer, implementar y operar mecanismos técnicos, organizativos y operativos para respaldar el plan de gestión de incidentes de seguridad de la información y el trabajo del IRT .Desarrollar y desplegar los sistemas de información necesarios para apoyar al IRT, incluida una base de datos de seguridad de la información. Estos mecanismos y sistemas están destinados a prevenir incidentes de seguridad de la información o reducir la probabilidad de incidentes de seguridad de la información;

g) diseñar y desarrollar un programa de conocimiento y capacitación para la gestión de eventos, incidentes y vulnerabilidades de seguridad de la información;

h) probar el uso del plan de gestión de incidentes de seguridad de la información, sus procesos y procedimientos.

Una vez completada esta fase, las organizaciones deberían estar completamente preparadas para gestionar adecuadamente los incidentes de seguridad de la información. ISO / IEC 27035-2 describe cada una de las actividades enumeradas anteriormente, incluidos los contenidos de la política y el documento de planificación.

5.3 Detección e informe

La segunda fase de la gestión de incidentes de seguridad involucra la detección, recopilación de la información asociada e informes sobre los sucesos de eventos de seguridad de la información y la existencia de vulnerabilidades de seguridad de la información por medios manuales o automáticos. En esta fase, es posible que los eventos y las vulnerabilidades aún no se clasifiquen como incidentes de seguridad de la información.

El informe de eventos de seguridad en línea con las políticas de informes de la organización permite, de ser necesario, un análisis posterior.

Para la fase de Detección e Informe, una organización debe realizar las siguientes actividades claves:

a) monitorear y registrar el sistema y la actividad de la red de la circunscripción u organización principal, según corresponda;

b) detectar e informar la ocurrencia de un evento de seguridad de la información o la existencia de una vulnerabilidad de seguridad de la información, ya sea de forma manual o automática;

c) recolectar información en un evento de seguridad de la información o vulnerabilidad;

d) recopilar información sobre la conciencia de la situación a partir de fuentes de datos internas y externas, incluidos el tráfico del sistema local y de la red y los registros de actividades, fuentes de noticias sobre actividades políticas, sociales o económicas en curso que podrían afectar la actividad de incidentes, fuentes externas sobre tendencias de incidentes, nuevos vectores de ataque, indicadores de ataque actuales y nuevas estrategias y tecnologías de mitigación;

e) asegurar que todas las actividades, resultados y decisiones relacionadas se registren correctamente para su posterior análisis;

f) asegurar que la evidencia digital sea recopilada y almacenada de forma segura, y que su preservación segura sea continuamente supervisada, en caso de ser requerida para un proceso judicial o una acción disciplinaria interna. Para obtener información más detallada sobre la identificación, recopilación, adquisición y conservación de evidencia digital, consultar las normas de investigación del Anexo A;

g) asegurar de seguir un régimen de control de cambios para habilitar el seguimiento de vulnerabilidades y eventos de seguridad de la información y actualizaciones de informes, y para mantener la base de datos de seguridad de la información actualizada;

h) escalar, según sea necesario a lo largo de la fase, para revisiones o decisiones futuras.

Toda la información recopilada relacionada a un evento o vulnerabilidad de seguridad de la información se debe almacenar en la base de datos de seguridad de la información administrada por el IRT. La información reportada durante cada actividad debería ser lo más completa posible al momento. Esto apoyará evaluaciones, decisiones y acciones a tomar.

5.4 Evaluación y decisión

La tercera fase de la gestión de incidentes de seguridad de la información trata la evaluación de la información asociada con la ocurrencia de eventos de seguridad de la información y la decisión de clasificar los eventos como incidentes de seguridad de la información.

Una vez que detectado e informado un evento de seguridad de la información, se deben realizar las actividades posteriores:

a) distribuir la responsabilidad de las actividades de gestión de incidentes de seguridad de la información a través de una jerarquía adecuada de personal con evaluación, toma de decisiones y acciones que involucren tanto al personal de seguridad como a otros;

b) proporcionar procedimientos formales para que cada persona notificada los siga, incluyendo la revisión y modificación de informes, la evaluación de daños y la notificación al personal relevante. Las acciones individuales dependerán del tipo y severidad del incidente;

c) usar directrices para la documentación completa de un evento de seguridad de la información y las acciones posteriores para un incidente de seguridad de la información, si el evento de seguridad de la información se clasifica como un incidente de seguridad de la información.

Para la fase de Evaluación y Decisión, una organización debe realizar las siguientes actividades claves:

— recopilar información que pueda incluir pruebas, mediciones y otras recopilaciones de datos sobre la detección de un evento de seguridad de la información. El tipo y la cantidad de información recopilada dependerán del evento de seguridad de la información que haya ocurrido;

— realizar una evaluación por parte del experto en incidentes para determinar si el evento es un incidente de seguridad de la información posible o confirmado o una falsa alarma. Una falsa alarma (es decir, un falso positivo) es una indicación de un evento informado que no es real o tiene alguna consecuencia. Si es necesario, el IRT puede realizar una revisión de calidad para garantizar que el experto en incidentes declaró correctamente un incidente;

— asegurar que todas las partes involucradas, particularmente el IRT, registren adecuadamente todas las actividades, resultados y decisiones relacionadas para su posterior análisis;

— asegurar que el régimen de control de cambios se mantenga para cubrir el seguimiento de incidentes de seguridad de la información y las actualizaciones de informes de incidentes, y para mantener la base de datos de seguridad de la información actualizada.

Toda información recopilada relacionada con un evento, incidente o vulnerabilidad de seguridad de la información, se debe almacenar en la base de datos de seguridad de la información administrada por el IRT. La información que se reporta durante cada actividad debería ser lo más completa posible. Esto apoyará evaluaciones, decisiones y acciones a tomar.

5.5 Respuestas

La cuarta fase de la gestión de incidentes de seguridad de la información implica responder a los incidentes de seguridad de la información, de acuerdo a las acciones determinadas en la fase de evaluación y decisión. Dependiendo de las decisiones, las respuestas podrían dar de manera inmediata, en tiempo real o casi en tiempo real, y algunas respuestas podrían involucrar una investigación de seguridad de la información.

Una vez que se haya confirmado un incidente de seguridad de la información y se hayan determinado las respuestas, se deben realizar las siguientes actividades:

a) distribuir la responsabilidad de las actividades de gestión de incidentes de seguridad de la información a través de una adecuada jerarquía de personal que tome decisiones y acciones, que involucren tanto al personal de seguridad como a otros según sea necesario;

b) proporcionar procedimientos formales para que cada persona involucrada siga, incluyendo la revisión y modificación de los informes, la reevaluación de los daños y la notificación al personal relevante. Las acciones individuales dependerán del tipo y severidad del incidente;

c) usar las directrices para la completa documentación de un incidente de seguridad de la información y las acciones posteriores.

Para la fase de Respuestas, una organización debería realizar las siguientes actividades claves:

— investigar incidentes según sea necesario y en relación con la clasificación de escala de clasificación de incidentes de seguridad de la información. La escala se debe cambiar según necesidad. La investigación puede incluir diferentes tipos de análisis para proporcionar una comprensión más profunda de los incidentes.

— revisión del IRT, para determinar si el incidente de seguridad de la información está bajo control y, de ser así, ejecutar la respuesta requerida. Si el incidente no está bajo control o va a tener un severo impacto en las operaciones de la organización, realizar actividades de respuesta a la crisis y a la función de manejo de crisis.

— asignar recursos internos e identificar recursos externos para responder a un incidente.

— escalar según sea necesario a lo largo de la fase para evaluaciones o decisiones adicionales.

— asegurar que todas las partes involucradas, especialmente el IRT, registren correctamente todas las actividades para su posterior análisis.

— asegurar que la evidencia digital se recopile y almacene de forma segura, y que su preservación segura sea supervisada continuamente, en caso de que se requiera evidencia para un proceso judicial o una acción disciplinaria interna. Para obtener información más detallada sobre la identificación, recopilación, adquisición y conservación de evidencia digital, consultar las normas de investigación en Anexo A.

— asegurar que el régimen de control de cambios se mantenga para cubrir el seguimiento de incidentes de seguridad de la información y las actualizaciones de informes de incidentes, y para mantener la base de datos de seguridad de la información actualizada.

— comunicar la existencia del incidente de seguridad de la información y compartir cualquier información relevante (por ejemplo, información sobre amenazas, ataques y vulnerabilidades) con otras personas u organizaciones internas y externas, de acuerdo con los planes de comunicación organizacionales e IRT y las políticas de divulgación de información. Puede ser particularmente importante notificar a los propietarios de activos (determinados durante el análisis de impacto) y a las organizaciones internas y externas (por ejemplo, otros equipos de respuesta a incidentes, agencias de aplicación de la ley, proveedores de servicios de Internet y organizaciones de intercambio de información) que podrían ayudar con la administración y resolución del incidente. Compartir información también podría beneficiar a otras organizaciones ya que las mismas amenazas y ataques a menudo afectan a múltiples organizaciones. Para mayor detalle sobre el intercambio de información, ver ISO/IEC 27010.

— después de la recuperación de un incidente, se debe iniciar una actividad posterior al incidente según la naturaleza y la gravedad de este. Esta actividad incluye:

  — investigación de la información relativa al incidente,

  — investigación de otras causas relevantes tales como personal implicado, e

  — informe resumido de los resultados de la investigación.

— una vez que se haya resuelto el incidente, se debe cerrar de acuerdo con los requisitos del IRT o de la organización matriz y se debe notificar a las partes interesadas.

Toda la información recopilada relacionada a un evento de seguridad de la información, un incidente o una vulnerabilidad se debe almacenar en la base de datos de seguridad de la información administrada por el IRT. La información reportada durante cada actividad debería ser lo más completa posible. Esto apoyará las evaluaciones, decisiones y acciones que se tomarán, incluyendo un posible análisis futuro.

5.6 Lecciones aprendidas

La quinta fase de la gestión de incidentes de seguridad de la información se produce cuando se han resuelto los incidentes de seguridad de la información. Esta fase implica aprender lecciones de cómo se han manejado los incidentes (y las vulnerabilidades).

Para la fase de lecciones aprendidas, una organización debe realizar las siguientes actividades claves:

a) identificar las lecciones aprendidas de incidentes y vulnerabilidades de seguridad de la información;

b) revisar, identificar y realizar mejoras en la implementación del control de seguridad de la información (controles nuevos o actualizados), así como de la política de administración de incidentes de seguridad de la información. Las lecciones pueden provenir de uno o varios incidentes de seguridad de la información o vulnerabilidades de seguridad informadas. Las mejoras son asistidas por métricas integradas en la estrategia de la organización sobre dónde invertir en controles de seguridad de la información;

c) revisar, identificar y hacer mejoras en la evaluación de la seguridad de la información existente de la organización y las revisiones de gestión;

d) revisar cuán efectivos fueron los procesos, procedimientos, formatos de informes y estructura organizacional para responder, evaluar y recuperarse de incidentes de seguridad de la información y tratar las vulnerabilidades de seguridad de la información. Sobre la base de las lecciones aprendidas, identificar y hacer mejoras al plan de gestión de incidentes de seguridad de la información y su documentación;

e) comunicar y compartir los resultados de la revisión dentro de una comunidad confiable (si la organización así lo desea);

f) determinar si la información del incidente, los vectores de ataque asociados y las vulnerabilidades se pueden compartir con las organizaciones asociadas para ayudar a prevenir los mismos incidentes en sus entornos. Para más detalles, ver ISO/IEC 27010 sobre intercambio de información;

g) realizar una evaluación integral del desempeño y la eficacia de IRT de forma periódica.

Se enfatiza que las actividades de gestión de incidentes de seguridad de la información son reiterativas y, por lo tanto, una organización debe realizar periódicamente mejoras en varios elementos de seguridad de la información a lo largo del tiempo. Estas mejoras se deben proponer sobre la base de revisión de los datos sobre incidentes de seguridad de la información, respuestas y vulnerabilidades de seguridad de la información informadas.

ISO/IEC 27035-2 describe en detalle cada una de las actividades anteriores.

Anexo A
(informativo)

Relación de los estándares investigativos

Esta parte de ISO/IEC 27035, describe parte de un proceso investigativo el cual incluye, pero se no limita, la aplicación de los siguientes estándares:

— ISO/IEC 27037, *Directrices para la identificación, recopilación, adquisición y preservación de evidencia digital*

Esta norma describe los medios por los cuales aquellos involucrados en las primeras etapas de una investigación, incluyendo la respuesta inicial, pueden asegurar la captura de la suficiente evidencia digital que permita a la investigación proceder de manera adecuada.

— ISO/IEC 27038, *Especificaciones para la redacción digital*

Algunos documentos pueden contener información que podría no ser divulgada a otras partes. Los documentos modificados pueden ser entregados a estas partes luego de un proceso adecuado del documento original. El proceso de eliminar información que no debe ser divulgada se denomina "redacción".

La redacción digital de documentos es un área relativamente nueva en la práctica de la gestión de documentos, surgiendo asuntos propios y potenciales riesgos. Una vez que los documentos son redactados, la información eliminada no debería ser recuperable. Por este motivo es necesario ser cauteloso al redactar la información (por ejemplo, no debe estar simplemente escondida dentro de porciones no desplegables dentro del documento).

ISO/IEC 27038, especifica los métodos para la redacción digital de documentos electrónicos. También especifica los requerimientos de software que se pueden usar para la redacción.

— ISO/IEC 27040, *Seguridad de almacenamiento*

ISO/IEC 27040, proporciona una orientación técnica detallada de cómo las organizaciones pueden definir un nivel apropiado de mitigación de riesgos al utilizar un enfoque probado y coherente a la planificación, diseño, documentación e implementación de la seguridad de almacenamiento de los datos. La seguridad de almacenamiento aplica a la protección (seguridad) de la información del lugar donde se almacena la información y a la seguridad de la información que se transmite a través de los enlaces de comunicación asociados con el almacenamiento. La seguridad de almacenamiento incluye la seguridad de los dispositivos y medios, la seguridad de las actividades de gestión relacionados a los dispositivos y medios, la seguridad de aplicaciones y servicios, y la seguridad relativa al usuario final durante el período útil de los dispositivos y medios hasta después de su uso.

Los mecanismos de seguridad como la encriptación y la sanitización pueden afectar la capacidad investigativa al introducir mecanismos de ofuscación. Estos se deberían considerar prioritarios durante el transcurso de una investigación. Estos también pueden ser importante para asegurar que el almacenamiento del material de evidencia durante y después de una investigación, está debidamente preparado y asegurado.

— ISO/IEC 27041, D*irectrices para garantizar la idoneidad y adecuación del método de investigación de incidentes*

Es importante que los métodos y procesos desarrollados durante una investigación demuestren ser apropiados. Esta norma proporciona las directrices del cómo ofrecer garantía que los métodos y procesos cumplan los requerimientos de la investigación y hayan sido debidamente probados.

— ISO/IEC 27042, *Directrices para el análisis e interpretación de la evidencia digital.*

Describe el cómo los métodos y procesos usados durante una investigación, se pueden diseñar e implementar para permitir la correcta evaluación de la posible evidencia digital, su interpretación y el informe de los hallazgos.

— ISO/IEC 27043, *Principios y procesos para la investigación de incidentes*

Esta norma, define los principios y procesos comunes claves durante una investigación de incidentes y proporciona un marco para todas las etapas de investigación.

— ISO/IEC 27050, *Extracción electrónica*

ISO/IEC 27050, trata sobre las actividades en la extracción electrónica, pero no limitada a la identificación, preservación, recopilación, procesamiento, revisión, análisis y producción de Información Electrónicamente Almacenada (ESI[6]). Además, proporciona orientaciones sobre las medidas a tomar, abarcando desde la creación inicial del ESI hasta su disposición final, en el cual una organización puede asumir para mitigar el riesgo y el gasto de la extracción electrónica se debería convertir en un tema a tomar en cuenta. Esto es relevante tanto para el personal técnico como no técnico involucrado en alguna o todas las actividades de extracción electrónica. Es importante destacar que estas orientaciones no intentan contradecir o superponerse a la legislación local y sus regulaciones.

La extracción electrónica a menudo sirve como un conductor para las investigaciones, así como para la adquisición de evidencia y el manejo de actividades. Además, la sensibilidad y criticidad de los datos a menudo necesitan de protección como la seguridad de almacenamiento para proteger contra transgresiones a la seguridad.

— ISO/IEC 30121, *Gobernanza del marco de referencia de riesgo forense digital*

ISO/IEC 30121, proporciona un marco de trabajo para los organismos rectores de las organizaciones (incluyendo propietarios, miembros de la mesa directiva, directores, socios, executivos seniors o similares) sobre la mejor forma de preparar una organización para las investigaciones digitales antes de que ocurran. ISO/IEC 30121, se aplica al desarrollo de procesos estratégicos (y decisiones) relacionados a la retención, disponibilidad, acceso y rentabilidad de la divulgación de evidencia digital. ISO/IEC 30121 es aplicable a organizaciones de todos tipos y tamaños. ISO/IEC 30121 trata sobre la prudente preparación estratégica para la investigación digital de una organización. La preparación forense asegura que una organización ha realizado una preparación adecuada y estratégica para aceptar los potenciales eventos probatorios. Las acciones pueden ocurrir como resultado de una transgresión inevitable de la seguridad, fraude o reivindicación de la reputación. En cada situación TI se debería desplegar de forma estratégica para maximizar la efectividad de la disponibilidad probatoria, accesibilidad y rentabilidad.

6 En inglés: *Electronically stored information, ESI..*

Figura A.1 muestra las actividades típicas alrededor de un incidente y su investigación. Los números que se muestran en el diagrama (por ejemplo 27037) indican la norma en la lista inferior y las barras ensombrecidas muestran cual es más aplicable o posee alguna influencia sobre el proceso investigativo (por ejemplo, establecer las políticas o crear restricciones). Se recomienda, sin embargo, que todos las normas se consulten de antemano y durante la preparación y planificación de las fases. Las clases de procesos mostrados se definen con más detalle en ISO/IEC 27043, y las actividades identificadas concuerdan con aquellas mostradas en mayor detalle en ISO/IEC 27035-2, ISO/IEC 27037, ISO/IEC 27042 y ISO/IEC 27041.

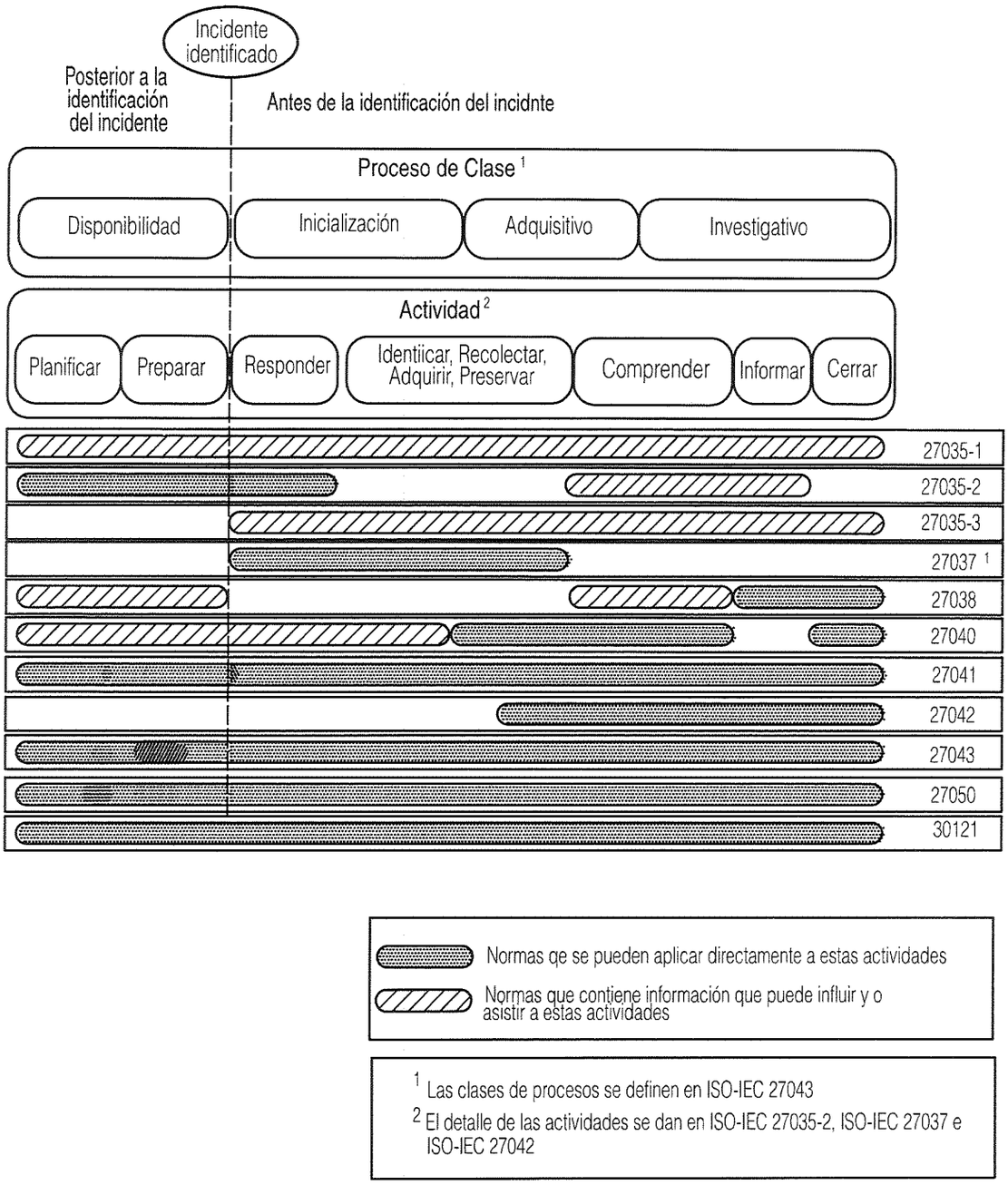

Figura A.1 – Aplicabilidad de los estándares para la clases y actividades de los procesos de investigación.

Anexo B
(informativo)

Ejemplos de incidentes de seguridad de la información y sus causas

B.1 Ataques

B.1.1 Denegación del servicio

La Denegación del Servicio (DoS[7]) y la Denegación del Servicio Distribuido (DDoS[8]) conforman una amplia categoría de incidentes con una amenaza en común. Tales incidentes causan una falla del sistema, servicio o red, evitando que opere a su capacidad normal, por lo general impide el acceso usuarios legítimos. Existen dos tipos de incidentes de DoS y DDoS, causados por medios técnicos: la eliminación de recursos o el agotamiento de recursos.

Ejemplos típicos de un incidente deliberado de DoS y DDoS incluyen los siguientes:

— Ping a las direcciones de red de transmisión con el objetivo de llenar el ancho de banda del tráfico de respuesta.

— Enviar datos en un formato inesperado para un sistema, servicio o red con el objetivo de colapsar o interrumpir su operación normal.

— Abrir múltiples sesiones autorizadas de un sistema, servicio o red en particular, con el objetivo de agotar sus recursos (por ejemplo, ralentizar, bloquear o colapsar).

Tales ataques a menudo los realizan bots, un sistema computacional que ejecuta malware que es controlado por un botnet. Un botnet es un comando bot central que comanda y controla a la red administrada por humanos. El tamaño de botnet abarcan de los cientos a millones de computadores afectados.

Algunos incidentes técnicos DoS pueden ser accidentales, por ejemplo, causados por una mala configuración de un operador o por la incompatibilidad de una aplicación de software, aunque la mayoría de las veces son deliberados. Algunos incidentes técnicos de DoS son lanzados intencionalmente con el objetivo de colapsar un sistema o servicio o derribar una red, mientras otros ocurren producto de una actividad maliciosa. Por ejemplo, algunos escaneos comunes y sigilosos y técnicas de identificación pueden causar el colapso de sistemas o servicios antiguos o mal configurados. Se debe hacer presente que los incidentes deliberados de DoS se ejecutan a menudo de forma anónima (por ejemplo la fuente del ataque es "falsa"), ya que estos no pretenden que el atacante reciba alguna información de regreso de la red o sistema atacado.

7 En inglés: *Denial of service, DoS.*

8 En inglés: *Distributed denial of service, DDoS.*

Los incidentes DoS causados por medios no técnicos, tienen como resultado la pérdida de información, servicio o instalaciones, que pueden ser causados por:

— vulneraciones físicas a las instalaciones de seguridad, resultando en un robo o daño y destrucción de equipos,

— daño accidental de hardware (y/o instalación) por incendios o inundaciones,

— condiciones medioambientales extremas, por ejemplo, altas temperaturas de operación (por ejemplo, debidas a fallas del aire acondicionado),

— desperfectos o sobrecarga de los sistemas,

— cambios descontrolados del sistema, y

— esperfectos de software o hardware.

B.1.2 Accesos no autorizados

En general, esta categoría de incidentes consiste en un intento no autorizado por acceder o hacer mal uso del sistema, servicio o red. Algunos ejemplos de incidentes por accesos técnicos no autorizados incluyen:

— intentos por obtener archivos de contraseñas,

— ataques por desbordamiento de la memoria intermedia o buffer, para obtener accesos privilegiados (por ejemplo, accesos de administrador) de un objetivo,

— explotación de vulnerabilidades del protocolo para secuestrar o redireccionar las conexiones de red legítimas,

— intentos por elevar los privilegios a recursos o información más allá de los límites que ya posee un usuario o administrador.

Los incidentes por accesos no autorizados causados por método no técnicos, que provocan la divulgación directa o indirecta, modificación de información, carencias en la rendición de cuentas o mal uso de los sistemas de información, pueden ser causados por:

— transgresiones a la seguridad física, lo que provoca un acceso no autorizado a la información, y

— sistemas operativos mal o pobremente configurados debido a cambios de sistema descontrolados o desperfectos de software o hardware.

B.1.3 Malware

Se identifican como malware a un programa o parte de un programa insertado en otro programa con la intención de modificar su comportamiento original, por lo general para realizar actividades maliciosas como el robo de información o identidad, destrucción de información o recursos, DoS, spam, otros. Los ataques por malwares podrían ser divididos en cinco categorías: virus, gusanos, caballos de troya, código móvil y combinado. Mientras los virus son creados para atacar las vulnerabilidades de un sistema, otros malwares se usan para realizar ataques más específicos. Esto, en ocasiones se realiza al modificar un malware existente y crear una variante que a menudo no es reconocida por las tecnologías de detección de malwares.

B.1.4 Abuso

Este tipo de incidentes suceden cuando un usuario viola las políticas de seguridad de un sistema informático de una organización. Tales incidentes no constituyen un ataque en estricto sentido de la palabra, pero a menudo son informados como incidentes y se deben manejar por un IRT. Se podría considerar un uso inapropiado lo siguiente:

— descarga o instalación de herramientas de hackeo.

— uso del correo corporativo para spam o promoción de un negocio personal.

— usar recursos de la empresa para establecer un sitio web no autorizado.

— usar el servicio peer-to-peer para adquirir o distribuir archivos pirateados (música, videos, programas).

B.2 Reunión de información

En términos generales, la categoría de reunir información de los incidentes incluye a aquellas actividades asociadas con identificar potenciales objetivos y comprender la ejecución de los servicios sobre esos objetivos. Este tipo de incidentes involucran el reconocimiento, con el fin de identificar:

— existencia de un objetivo y comprender la topología alrededor de la red y con quien el objetivo se comunica constantemente, y

— vulnerabilidades potenciales en el objetivo o su entorno de red circundante que podría ser explotada.

Ejemplos típicos de ataques de reunión de información por medios técnicos incluyen los siguientes:

— bajar los registros del Sistema de Nombres de Dominio (DNS[9]) para el dominio de internet del objetivo (zona de transferencia de DNS);

— ping a las direcciones de red para encontrar sistemas que se encuentren “activos”;

— sondear el sistema para identificar (por ejemplo una huella digital) el host de un sistema operativo;

— escanear los puertos disponibles de una red para identificar los servicios de red (por ejemplo, los protocolos de transferencia de archivos (FTP[10]), Web, otros) y las versiones de software de esos servicios;

— escanear uno o más servicios vulnerables conocidos en un rango de direcciones de la red (escaneo horizontal).

9 En Inglés: *Domain Name System, DNS.*

10 En Inglés: *File Transfer Protocol, FTP.*

En algunos casos, la reunión de información técnica se extiende a un acceso no autorizado si, por ejemplo, como parte de una búsqueda de vulnerabilidades, el atacante intenta también ganar accesos no autorizados. Esto ocurre comúnmente con herramientas automáticas que no buscan solo vulnerabilidades, sino que también intentan automáticamente explotar los sistemas, servicios y/o redes vulnerables que se encuentren.

Los incidentes de recolección de datos causados por medio no técnicos, dan como resultado:

— la divulgación directa o indirecta o la modificación de la información,

— robo de propiedad intelectual almacenada electrónicamente,

— transgresiones a las responsabilidades, por ejemplo, el ingreso de una cuenta, y

— mal uso de sistemas de información (por ejemplo, uso contrario a las políticas de una organización o las leyes).

Los incidentes por recolección de información se pueden causar, por ejemplo, por:

— transgresiones físicas de las medidas de seguridad, como resultado de accesos no autorizados a información, y robo de equipos de almacenamiento que contengas datos importantes, por ejemplo, llaves de encriptación,

— sistemas operativos deficientemente configurados o sin configuración debido a cambios no controlados del sistema o desperfectos de software o hardware, teniendo como resultado que personal interno o externo obtenga accesos a información para la cual no posee los permisos, e

— ingeniería social, la cual es el acto de manipular a las personas para que realicen acciones o divulguen información confidencial, por ejemplo, 'phishing'.

Anexo C
(informativo)

Tabla de referencia cruzada de ISO/IEC 27001 con ISO/IEC 27035

ISO/IEC 27001:2013	ISO/IEC 27035
A.16 Gestión de incidentes de seguridad de la información	**ISO/IEC 27035-1:** **4 Resumen** (para información general sobre gestión de incidentes de seguridad de la información)
A.16.1 Gestión de incidentes de seguridad de la información y mejoras Objetivo: Asegurar un enfoque efectivo y consistente en la gestión de los incidentes de seguridad de la información, incluyendo los eventos de seguridad comunicacional y sus debilidades.	**ISO/IEC 27035-1:** **5 Fases** (para las fases sobre la gestión de incidentes de seguridad de la información) **Anexo B (informativo) Ejemplos de incidentes de seguridad de la información y sus causas** **ISO/IEC 27035-2:** **Anexo A (informativo) Aspectos legales y regulatorios** **Anexo B (informativo) Ejemplo de evento de seguridad de la información, incidente e informes y formularios de vulnerabilidad** **Anexo C (informativo) Ejemplo de enfoques para la categorización y clasificación de eventos e incidente de seguridad de la información**
A.16.1.1 Responsabilidades y procedimientos Control: La gestión de responsabilidades y procedimientos debe asegurar la respuesta rápida, efectiva y ordenada para los incidentes de seguridad de la información.	**ISO/IEC 27035-1:** **5.2 Planificación y preparación** **5.4 Evaluación y decisión a), b)** **ISO/IEC 27035-2:** **4 Gestión de incidentes de seguridad de la información** **5 Actualización de las política de seguridad de la información** **6 Creación de un plan de gestión de incidentes de seguridad de la información** **7 Establecer un equipo de respuesta a incidentes (IRT)** **8 Establecer relaciones con otras organizaciones** **9 Definir el apoyo técnico u otro necesario** **10 Creación de un conocimiento de incidentes de seguridad informática y entrenamiento relacionado**
A.16.1.2 Informe de eventos de seguridad de la información Control Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados lo antes posible.	**ISO/IEC 27035-1:** **5.3 Detección e Informes**

ISO/IEC 27001:2013	ISO/IEC 27035
A.16.1.3 Informe de las debilidades de seguridad de la información Control: Los empleados y empleadores que utilizan el sistema de información de la organización y sus servicios, deben ser capaces de informar y distinguir cualquier vulnerabilidad en la seguridad de la información en los sistemas o servicios.	**ISO/IEC 27035-1:** **5.3 Detección e Informes**
A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de la información Control: Los eventos de seguridad de la información deben ser evaluados y se debe decidir si clasifican como incidente de seguridad de la información.	**ISO/IEC 27035-1:** **5.4 Evaluación y decisión**
A.16.1.5 Respuestas ante incidentes de seguridad de la información: Control: Los incidentes de seguridad de la información se deben responder de acuerdo con los procedimientos documentados.	**ISO/IEC 27035-1:** **5.5 Respuestas**
A.16.1.6 Aprendizaje de los incidentes de seguridad de la información Control: El conocimiento obtenido del análisis y resolución de los incidentes de seguridad de la información, se deben utilizar para reducir la probabilidad e impacto de los futuros incidentes.	**ISO/IEC 27035-1:** **5.6 Lecciones aprendidas** **ISO/IEC 27035-2:** **12 Lecciones aprendidas**
A.16.1.7 Recolección de evidencia Control La organización debe definir y aplicar los procedimientos para la identificación, recolección, adquisición y preservación de la información, la cual puede servir como evidencia.	**ISO/IEC 27035-1:** **5.3 Detección e Informes** d), g) **5.4 Análisis y decisión** d), g) **5.5 Respuestas** d), i), l)

Anexo D
(informativo)

Bibliografía

ISO/IEC 20000 (all parts), *Information technology -Service management.*

ISO/IEC 27001, *Information technology - Security techniques - Information security management systems - Requirements.*

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

ISO/IEC 27003, *Information technology - Security techniques - Information security management systems - Guidance.*

ISO/IEC 27004, *Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation.*

ISO/IEC 27005, *Information technology - Security techniques - Information security risk management.*

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

ISO/IEC 27031, *Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity.*

ISO/IEC 27033-1, *Information technology - Security techniques - Network security - Part 1: Overview and concepts.*

ISO/IEC 27033-2, *Information technology - Security techniques - Network security - Part 2: Guidelines for the design and implementation of network security.*

ISO/IEC 27033-3, *Information technology - Security techniques -Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues.*

ISO/IEC 27037, *Information technology - Security techniques - Guidelines for identification, collection, acquisition, and preservation of digital evidence.*

ISO/IEC 27039, *Information technology - Security techniques - Selection, deployment and operations of intrusion detection and prevention systems (IDPS).*

ISO/IEC 27041, *Information technology - Security techniques - Guidance on assuring suitability and adequacy of incident investigative method.*

ISO/IEC 27042, *Information technology - Security techniques -- Guidelines for the analysis and interpretation of digital evidence.*

ISO/IEC 27043, *Information technology - Security techniques - Incident investigation principles and processes.*

ISO/IEC 29147, *Information technology - Security techniques - Vulnerability disclosure.*

ISO/IEC 30111, *Information technology - Security techniques - Vulnerability handling processes.*

NOTA EXPLICATIVA NACIONAL

La equivalencia de las Normas Internacionales señaladas anteriormente con Norma Chilena, y su grado de correspondencia es el siguiente:

Norma Internacional	Norma nacional	Grado de correspondencia
ISO/IEC 20000-1	NCh-ISO 20000/1:2013	La Norma Chilena NCh-ISO 20000/1:2013 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 20000/1:2011.
ISO/IEC 20000-2	NCh-ISO 20000/2:2013	La Norma Chilena NCh-ISO20000/2:2013 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 20000/2:2012.
ISO/IEC 20000-3	NCh-ISO 20000/3:2014	La Norma Chilena NCh-ISO20000/3:2014 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 20000-3:2012.
ISO/IEC TR 20000-4	No existe	-
ISO/IEC TR 20000-5	NCh-ISO 20000/5:2014	La Norma Chilena NCh-ISO20000/5:2014 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC TR 20000-5:2013.
ISO/IEC 20000-6	No existe	-
ISO/IEC TR 20000-9	No existe	-
ISO/IEC 20000-10	NCh-ISO 20000/10:2014	La Norma Chilena NCh-ISO20000/10:2014 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC TR 20000-10:2013.
ISO/IEC TR 20000-11	No existe	-
ISO/IEC TR 20000-12	No existe	-
ISO/IEC 27001	NCh-ISO 27001:2013	La Norma Chilena NCh-ISO27001:2013 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27001:2013.
ISO/IEC 27002	NCh-ISO 27002:2013	La Norma Chilena NCh-ISO27002:2013 es una adopción idéntica de la versión en español de la Norma Internacional NCh-ISO 27002:2009.
ISO/IEC 27003	NCh-ISO 27003:2014	La Norma Chilena NCh-ISO27003:2014 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27003:2010.
ISO/IEC 27004	No existe	-
ISO/IEC 27005	NCh-ISO 27005:2014	La Norma Chilena NCh-ISO27005:2014 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27005:2011.

(continúa)

(conclusión)

ISO/IEC 27010	No existe	-
ISO/IEC 27031	NCh-ISO 27031:2015	La Norma Chilena NCh-ISO 27031:2015 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27031:2011.
ISO/IEC 27033-1	No existe	-
ISO/IEC 27033-2	No existe	-
ISO/IEC 27033-3	No existe	-
ISO/IEC 27037	NCh-ISO 27037:2015	La Norma Chilena NCh-ISO 27037:2015 es una adopción idéntica de la versión en español de la Norma Internacional ISO/IEC 27037:2012.
ISO/IEC 27039	No existe	-
ISO/IEC 27041	No existe	-
ISO/IEC 27042	No existe	-
ISO/IEC 27043	No existe	-
ISO/IEC 29147	No existe	-
ISO/IEC 30111	No existe	

Anexo E
(informativo)

Justificación de los cambios editoriales

Tabla E.1 – Cambios editoriales

Cláusula/subcláusula	Cambios editoriales	Justificación
En toda la norma	Se reemplaza "esta Norma Internacional" por "esta norma"	La norma es de alcance nacional.
1	Se reemplaza "Alcance" por "Alcance y campo de aplicación".	De acuerdo con estructura de NCh2.
2 y Anexo D	Se agrega Nota Explicativa Nacional.	Para detallar la equivalencia y el grado de correspondencia de las Normas Internacionales con las Normas Chilenas.
Anexo D	Se reemplaza "Bibliografía" por "Anexo D (informativo) Bibliografía".	De acuerdo con estructura de NCh2.