INTECO

K

Tecnologías de la información y comunicación

INTE/ISO/IEC 27035-1:2022

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

Correspondencia: Esta norma nacional es idéntica (IDT) a la norma ISO/IEC 27035-1:2016, “Information technology – Security techniques — Information security incident management — Part 1: Principles of incident management”.

Miembros de

ISO

Fecha: 2022-06-17
Primera Edición
Secretaría: INTECO
Editada e impresa por ©INTECO

ICS 35.040

AVISOS IMPORTANTES SOBRE ESTE DOCUMENTO

Aviso y descargo de responsabilidad concerniente al uso de documentos INTECO

Las normas, los documentos normativos y otros instrumentos documentales de la Dirección de Normalización de INTECO, entre ellos el presente, son elaborados a través de un proceso de desarrollo de normas que se llevan a cabo bajo los principios de transparencia, apertura, imparcialidad, consenso, efectividad, relevancia, coherencia y dimensión del desarrollo, que emanan del Organismo Mundial de Comercio (OMC).

Ese proceso reúne a expertos voluntarios en distintas materias, integrados en comités que llevan el nombre del objeto de cada norma y representan distintas visiones. Forman parte los consumidores, empresarios, el Estado, y otros interesados en la norma, que exponen diferentes puntos de vista e intereses para lograr el consenso de la norma; mientras que la Dirección de Normalización de INTECO coordina el proceso y establece reglas para promover la equidad en el consenso para aprobar cada norma. La Dirección de Normalización de INTECO no forma parte de ningún comité, no vota, ni evalúa o verifica el contenido de ninguna norma, solo facilita el proceso de desarrollo de esta.

Por ello, INTECO no se hace responsable por el contenido de cada norma aprobada en un órgano de estudio, ya que esa responsabilidad recae en los miembros que participaron y la aprobaron pues son los expertos en la materia objeto de la norma.

INTECO no aceptará responsabilidad alguna por la aplicación de una norma, en especial no la acepta sobre daño personal, o sobre las cosas o derechos, u otros de cualquier naturaleza, ya sean especiales, directos o indirectos como consecuencia de la utilización del presente documento. Tampoco por la calidad resultante del producto o servicio al cual aplica.

La Dirección de Normalización de INTECO tampoco garantiza la precisión o que la información aquí publicada esté completa. Al expedir y poner este documento a la disposición del público, la Dirección de Normalización de INTECO no se responsabiliza por la prestación de servicios profesionales o de alguna otra índole a nombre de cualquier otra persona o entidad. Si el interesado no es experto o duda del contenido de la norma, deberá buscar la ayuda de un profesional competente y capacitado para determinar el ejercicio razonable en cualquier circunstancia.

La Dirección de Normalización de INTECO, desde el proceso de desarrollo de normas, no tiene poder, ni responsabilidad, para vigilar o hacer cumplir los contenidos de este documento. Este proceso de desarrollo de normas no certifica, prueba o inspecciona productos, diseños o instalaciones en cumplimiento de ninguna norma. Cualquier certificación u otra declaración de cumplimiento con los requerimientos de este documento es únicamente responsabilidad del Ente Certificador o la persona o entidad que hace la declaración.

Las observaciones a este documento han de dirigirse a:
Instituto de Normas Técnicas de Costa Rica
San Pedro de Montes de Oca
San José, Costa Rica
Tel: +506 2283 4522

info@inteco.org
www.inteco.org

© INTECO 2022

CONTENIDO PÁGINA

PRÓLOGO

El Instituto de Normas Técnicas de Costa Rica, INTECO, es el Ente Nacional de Normalización, según la Ley N° 8279 del año 2002. Organización de carácter privado, sin ánimo de lucro, cuya Misión es “desarrollar la normalización del país con el soporte de los servicios de evaluación de la conformidad y productos relacionados a nivel nacional e internacional, con un equipo humano competente, con credibilidad e independencia”. Colabora con el sector gubernamental y apoya al sector privado del país, para lograr ventajas competitivas en los mercados interno y externo.

La representación de todos los sectores involucrados en el proceso de Normalización Técnica está garantizada por los Comités Técnicos y el periodo de Consulta Pública, este último caracterizado por la participación del público en general.

Esta norma ha sido desarrollada en cumplimiento de los requisitos de nivel 1 y nivel 2 del Standards Council of Canada (SCC).

Esta norma INTE/ISO/IEC 27035-1:2022 fue aprobada por INTECO en la fecha del 2022-06-17.

Esta norma está sujeta a ser actualizada permanentemente con el objeto de que responda en todo momento a las necesidades y exigencias actuales.

A continuación, se mencionan las organizaciones que colaboraron en el estudio de esta norma a través de su participación en el Comité Técnico CTN 27 SC 01, Seguridad de la información.

Participante	Organización
Luis Benavides Arce	Compañía Nacional de Fuerza y Luz S.A (CNFL)
Mariela Cecilia Varela José Luna	Banco Promérica
Armando Camacho	Freudenberg Medical
Roberto Lemaitre	Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT)
Andrés Alvarado Alvaro Castro	Caja Costarricense de Seguro Social (CCSS)
Karen Córdoba Álvaro Castro	Instituto Costarricense de Electricidad (ICE)
Ricardo Morales Javier Mena	Banco Central de Costa Rica (BCCR)
Marco Vinicio Gamez	Consejo Nacional de Supervisión del Sistema Financiero (Conassif)
Ricardo Villalón	Universidad de Costa Rica (UCR)
Kevin Moraga	Tecnológico de Costa Rica (TEC)
Claudio Valverde	Universidad CENFOTEC
Gilberth González	Colegio de Profesionales en Informática y Computación (CPIC)
Mauricio Solano	Consultor

0 INTRODUCCIÓN

Las políticas o los controles de seguridad de la información no garantizan por sí solos la protección total de la información, los sistemas de información, los servicios o las redes. Después de aplicar los controles, es probable que queden vulnerabilidades residuales que pueden reducir la eficacia de la seguridad de la información y facilitar la aparición de incidentes de seguridad de la información. Esto puede tener impactos adversos directos e indirectos en las operaciones de negocio de una organización. Además, es inevitable que se produzcan nuevos casos de amenazas no identificadas anteriormente. Una preparación insuficiente por parte de una organización para hacer frente a tales incidentes hará que cualquier respuesta sea menos efectiva, y aumentará el grado de impacto potencial adverso en el negocio. Por lo tanto, es esencial para cualquier organización que desee un programa sólido de seguridad de la información tener un enfoque estructurado y planificado para

- detectar, informar y evaluar los incidentes de seguridad de la información;
- responder a los incidentes de seguridad de la información, incluyendo la activación de los controles apropiados para prevenir, reducir y recuperar los impactos;
- reportar las vulnerabilidades de la seguridad de la información, para que puedan ser evaluadas y tratadas adecuadamente;
- aprender de los incidentes de seguridad de la información y de las vulnerabilidades, instituir controles preventivos y mejorar el enfoque general de la gestión de incidentes de seguridad de la información.

Con el fin de lograr este enfoque planificado, la norma INTE/ISO/IEC 27035 proporciona orientación sobre los aspectos de la gestión de incidentes de seguridad de la información en las siguientes partes correspondientes.

- INTE/ISO/IEC 27035-1, Principios de la gestión de incidentes (este documento), presenta los conceptos básicos y las fases de la gestión de incidentes de seguridad de la información, y cómo mejorar la gestión de incidentes. Esta parte combina estos conceptos con los principios en un enfoque estructurado para detectar, informar, evaluar y responder a los incidentes, y aplicar las lecciones aprendidas.
- INTE/ISO/IEC 27035-2, Directrices para Planificación y preparación la respuesta a incidentes, describe cómo Planificación y preparación la respuesta a incidentes. Esta parte cubre las fases de "Planificación y preparación" y "Lecciones aprendidas" del modelo presentado en INTE/ISO/IEC 27035 1.

La norma INTE/ISO/IEC 27035 pretende complementar otras normas y documentos que dan orientación sobre la investigación de incidentes de seguridad de la información y la preparación para investigarlos. La norma INTE/ISO/IEC 27035 no es una guía exhaustiva, sino una referencia para ciertos principios fundamentales que pretenden asegurar que las herramientas, técnicas y métodos puedan seleccionarse de forma adecuada y que se demuestre que son aptos para el propósito en caso de que sea necesario.

Aunque la norma INTE/ISO/IEC 27035 abarca la gestión de los incidentes de seguridad de la información, también cubre algunos aspectos de las vulnerabilidades de la seguridad de la información. En la norma INTE/ISO/IEC 29147 y en la ISO/IEC 30111 se ofrece orientación sobre la divulgación de vulnerabilidades y el manejo de vulnerabilidades por parte de los proveedores, respectivamente.

La norma INTE/ISO/IEC 27035 también pretende informar a los responsables de la toma de decisiones que necesitan determinar la fiabilidad de las evidencias digitales que se les presentan.

Es aplicable a las organizaciones que necesitan proteger, analizar y presentar posibles evidencias digitales. Es pertinente para los organismos encargados de elaborar políticas que crean y evalúan procedimientos relacionados con las evidencias digitales, a menudo como parte de un conjunto más amplio de pruebas.

En el Anexo A se ofrece más información sobre las normas de investigación.

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

1 OBJETO Y CAMPO DE APLICACIÓN

Esta parte de la norma INTE/ISO/IEC 27035 es la base de esta norma internacional de varias partes. Presenta los conceptos básicos y las fases de la gestión de incidentes de seguridad de la información y combina estos conceptos con los principios en un enfoque estructurado para detectar, reportar, evaluar y responder a los incidentes, y aplicar las lecciones aprendidas.

Los principios que se ofrecen en esta parte de la norma INTE/ISO/IEC 27035 son genéricos y pretenden ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza. Las organizaciones pueden ajustar las orientaciones dadas en esta parte de la norma INTE/ISO/IEC 27035 según su tipo, tamaño y naturaleza del negocio en relación con la situación de riesgo de la seguridad de la información. Esta parte de la norma INTE/ISO/IEC 27035 también es aplicable a las organizaciones externas que prestan servicios de gestión de incidentes de seguridad de la información.

2 NORMAS DE REFERENCIA

Las siguientes normas contienen disposiciones que, al ser citadas en este texto, constituyen requisitos de esta norma. Las ediciones indicadas estaban en vigencia en el momento de esta publicación. Como toda norma está sujeta a revisión, se recomienda a aquellos que realicen acuerdos con base a ellas, que analicen la conveniencia de usar las ediciones recientes de las normas citadas seguidamente.

INTE/ISO/IEC 27010,	Tecnología de la información. Técnicas de seguridad. Gestión de la seguridad de la información para comunicaciones intersectoriales e interorganizacionales.
INTE/ISO/IEC 27035-2,	Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información. Parte 1: Principios de la gestión de incidentes.

3 TÉRMINOS Y DEFINICIONES

A los efectos de este documento, se aplican los términos y definiciones que figuran en la norma INTE/ISO/IEC 27000 y los siguientes.

La ISO y la IEC mantienen bases de datos terminológicas para su uso en la normalización en las siguientes direcciones

- IEC Electropedia: disponible en http://www.electropedia.org/
- Plataforma de navegación en línea de la ISO: disponible en http://www.iso.org/obp

3.1 investigación sobre la seguridad de la información:

aplicación de exámenes, análisis e interpretación para ayudar a la comprensión de un incidente de seguridad de la información (ver 3.4)

[FUENTE: INTE/ISO/IEC 27042, 3.10, modificado - La frase "un incidente" fue sustituida por "un incidente de seguridad de la información"].

3.2 equipo de respuesta a incidentes, IRT[1]:

equipo de miembros de la organización debidamente capacitados y de confianza que maneja los incidentes durante su ciclo de vida

Nota: CERT[2] (Equipo de Respuesta a Emergencias Informáticas) y CSIRT[3] (Equipo de Respuesta a Incidentes de Seguridad Informática) son términos comúnmente utilizados para IRT.

3.3 evento de seguridad de la información:

suceso que indica una posible violación de la seguridad de la información o un fallo de los controles

3.4 incidente de seguridad de la información:

uno o varios *eventos de seguridad de la información* (ver 3.3) relacionados e identificados que pueden dañar los activos de una organización o comprometer sus operaciones

3.5 gestión de incidentes de seguridad de la información:

ejercicio de un enfoque consistente y efectivo para el manejo de *incidentes de seguridad de la información* (ver 3.4)

3.6 manejo de incidentes:

acciones de detección, reporte, evaluación, respuesta, tratamiento y aprendizaje de los *incidentes de seguridad de la información* (ver 3.4)

3.7 respuesta a incidentes:

acciones tomadas para mitigar o resolver un *incidente de seguridad de la información* (ver 3.4), incluyendo aquellas tomadas para proteger y restaurar las condiciones operativas normales de un sistema de información y la información almacenada en él

3.8 punto de contacto, PoC[4]:

función o rol organizativo definido que sirve de coordinador o punto focal de la información relativa a las actividades de gestión de incidentes

[1] Por sus siglas en inglés, Incident Response Team
[2] Por sus siglas en inglés, Computer Emergency Response Team
[3] Por sus siglas en inglés, Computer Security Incident Response Team
[4] Por sus siglas en inglés, Point of Contact

4 VISIÓN GENERAL

4.1 Conceptos y principios básicos

Un evento de seguridad de la información es un suceso que indica una posible violación de la seguridad de la información o un fallo de los controles. Un incidente de seguridad de la información es uno o varios eventos de seguridad de la información relacionados e identificados que cumplen con los criterios establecidos y que pueden dañar los activos de una organización o comprometer sus operaciones.

La ocurrencia de un evento de seguridad de la información no significa necesariamente que un ataque haya tenido éxito o que haya implicaciones sobre la confidencialidad, la integridad o la disponibilidad, es decir, no todos los eventos de seguridad de la información se clasifican como incidentes de seguridad de la información.

Los incidentes de seguridad de la información pueden ser deliberados (por ejemplo, causados por programas maliciosos o por una violación intencionada de la disciplina) o accidentales (por ejemplo, causados por un error humano involuntario o por actos inevitables de la naturaleza) y pueden ser causados por medios técnicos (por ejemplo, virus informáticos) o no técnicos (por ejemplo, pérdida o robo de computadores). Las consecuencias pueden incluir la divulgación no autorizada, la modificación, la destrucción o la falta de disponibilidad de la información, o el daño o el robo de los activos de la organización que contienen información.

En el Anexo B se describen algunos ejemplos de incidentes de seguridad de la información y sus causas con fines meramente informativos. Es importante señalar que estos ejemplos no son en absoluto exhaustivos.

Una amenaza explota las vulnerabilidades (debilidades) de los sistemas, servicios o redes de información, provocando la aparición de eventos de seguridad de la información y, por tanto, causando potencialmente incidentes en los activos de información expuestos por las vulnerabilidades. La figura 1 muestra la relación de objetos en un incidente de seguridad de la información.

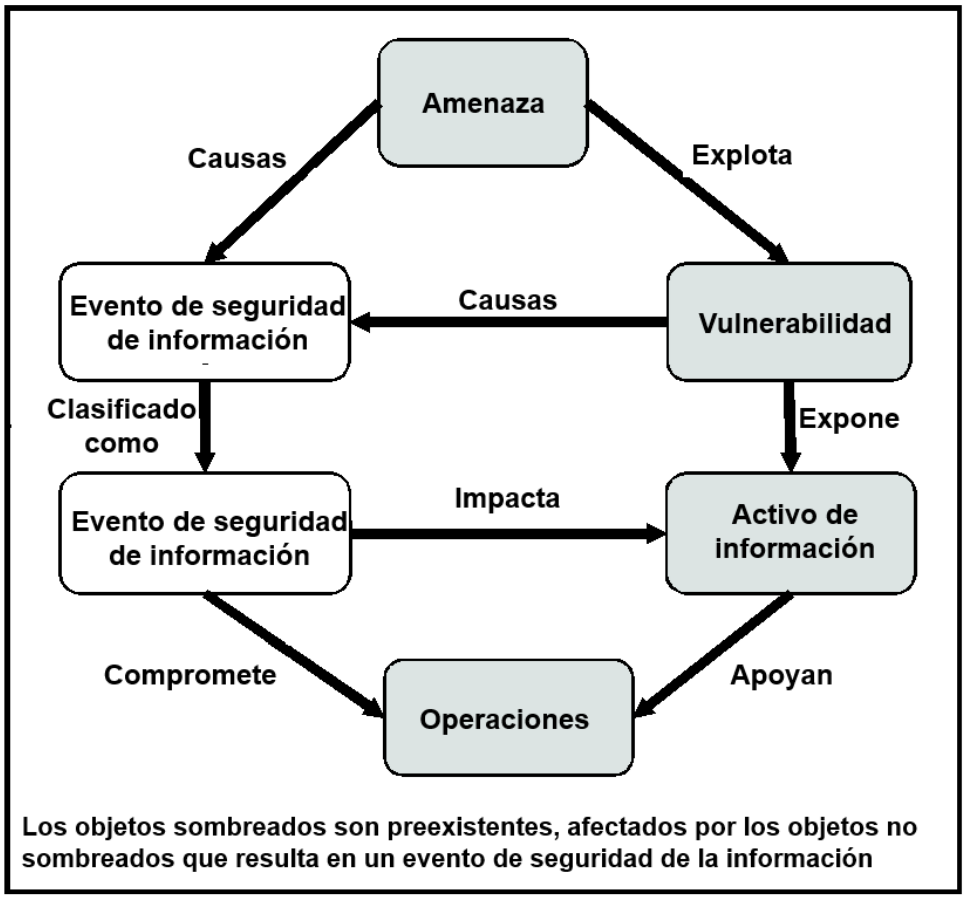

Figura 1 – Relación de objetos en un incidente de seguridad de la información

El compartir información y la coordinación con los IRT externos son consideraciones importantes. Muchos incidentes cruzan los límites de la organización y no pueden ser resueltos fácilmente por un solo IRT. Las relaciones o asociaciones para compartir información y la coordinación con los IRT externos pueden mejorar en gran medida la capacidad de responder y resolver los incidentes. Para más detalles sobre compartir información, ver la norma INTE/ISO/IEC 27010.

4.2 Objetivos de la gestión de incidentes

Como una parte clave de la estrategia global de seguridad de la información de una organización, ésta debería establecer controles y procedimientos que permitan un enfoque estructurado y bien planificado para la gestión de los incidentes de seguridad de la información. Desde la perspectiva de una organización, el objetivo principal es evitar o contener el impacto de los incidentes de seguridad de la información para minimizar el daño directo e indirecto a sus operaciones causado por los incidentes. Dado que los daños a los activos de información pueden tener un impacto negativo en las operaciones, las perspectivas de negocio y operativas deberían tener una gran influencia en la determinación de objetivos más específicos para la gestión de la seguridad de la información.

Entre los objetivos más específicos de un enfoque estructurado y bien planificado de la gestión de incidentes deberían incluir los siguientes:

a) detectar y tratar de manera eficiente los eventos de seguridad de la información, en particular decidiendo cuándo deberían clasificarse como incidentes de seguridad de la información;
b) evaluar y responder de la manera más adecuada y eficiente los incidentes de seguridad de la información identificados;
c) minimizar mediante controles apropiados, los efectos adversos de los incidentes de seguridad de la información en la organización y sus operaciones, como parte de la respuesta a los incidentes
d) establecer un vínculo con los elementos pertinentes de la gestión de crisis y la gestión de la continuidad del negocio mediante un proceso de escalamiento
e) evaluar y tratar adecuadamente las vulnerabilidades de la seguridad de la información para prevenir o reducir los incidentes. Esta evaluación puede ser realizada por el IRT o por otros equipos dentro de la organización, dependiendo de la distribución de funciones;
f) aprender las lecciones rápidamente a partir de los incidentes de seguridad de la información, de las vulnerabilidades y de su gestión. Este mecanismo de retroalimentación pretende aumentar las posibilidades de evitar que se produzcan futuros incidentes de seguridad de la información, mejorar la implementación y el uso de los controles de seguridad de la información y mejorar el plan general de gestión de incidentes de seguridad de la información.

Para ayudar a lograr estos objetivos, las organizaciones deberían asegurarse de que los incidentes de seguridad de la información se documenten de manera coherente, utilizando normas adecuadas para la categorización, clasificación y compartición de incidentes, de manera que se puedan derivar métricas de los datos agregados durante un período de tiempo. Esto proporciona información valiosa para ayudar al proceso de toma de decisiones estratégicas a la hora de invertir en controles de seguridad de la información. El sistema de gestión de incidentes de seguridad de la información debería ser capaz de compartir la información con las partes externas pertinentes y los IRT.

Otro objetivo asociado a esta parte de la norma INTE/ISO/IEC 27035 es proporcionar orientación a las organizaciones que pretenden cumplir los requisitos del Sistema de Gestión de la Seguridad de la Información (SGSI) especificados en la norma INTE/ISO/IEC 27001, que se apoyan en la orientación de la norma ISO/IEC 27002. La norma INTE/ISO/IEC 27001 incluye requisitos relacionados con la gestión de incidentes de seguridad de la información. En el Anexo C se incluye una tabla que hace referencia a los apartados de gestión de incidentes de seguridad de la información de la norma INTE/ISO/IEC 27001 y a los capítulos de esta parte de la norma INTE/ISO/IEC 27035. Esta parte de la norma INTE/ISO/IEC 27035 también puede respaldar los requisitos de los sistemas de gestión de la seguridad de la información distintos del SGSI.

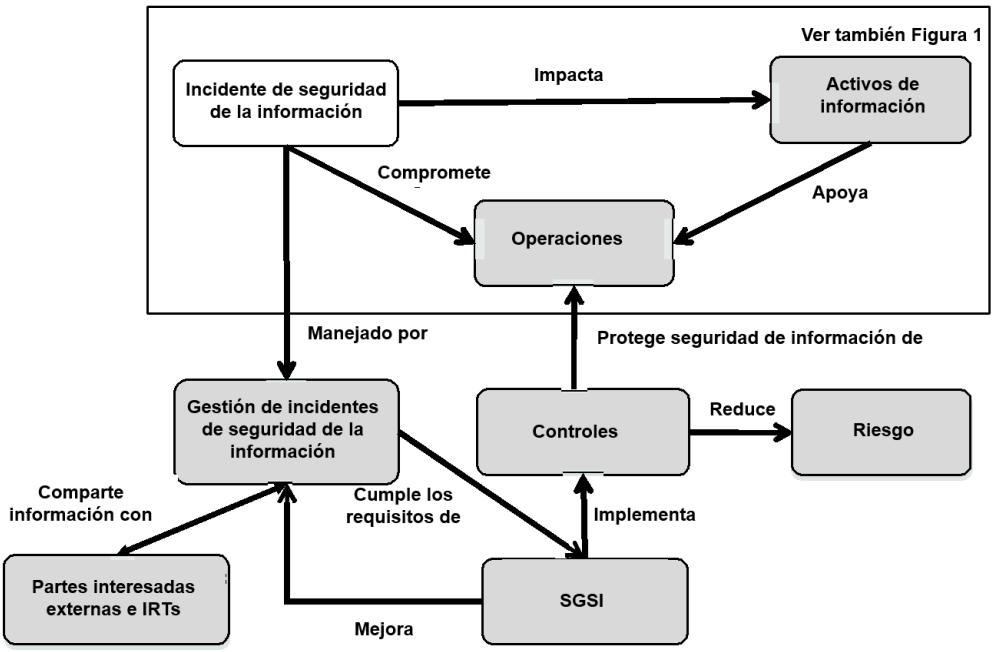

Figura 2 - Gestión de incidentes de seguridad de la información en relación con el SGSI y los controles aplicados

4.3 Ventajas de un enfoque estructurado

El uso de un enfoque estructurado para la gestión de incidentes de seguridad de la información puede producir importantes beneficios, que pueden agruparse en los siguientes temas.

a) Mejorar la seguridad general de la información

Un proceso estructurado de detección, reporte, evaluación y toma de decisiones en relación con los eventos e incidentes de seguridad de la información permitirá una rápida identificación y respuesta. Esto mejorará la seguridad general al ayudar a identificar e implementar rápidamente una solución consistente, y proporcionar así un medio para prevenir futuros incidentes de seguridad de la información similares. Además, se obtendrán beneficios mediante la medición, la compartición y la agregación. La credibilidad de la organización mejorará gracias a la demostración de su implementación de las mejores prácticas con respecto a la gestión de incidentes de seguridad de la información.

b) Reducción de los impactos adversos en el negocio

Un enfoque estructurado de la gestión de incidentes de seguridad de la información puede ayudar a reducir el nivel de los posibles impactos adversos para el negocio asociados con los incidentes de seguridad de la información. Estos impactos pueden incluir pérdidas financieras inmediatas y pérdidas a largo plazo derivadas del daño a la reputación y la credibilidad. Para obtener orientación sobre el análisis del impacto en el negocio, ver la norma ISO/IEC 27005. Para obtener orientación sobre la preparación de las tecnologías de la información y la comunicación para la continuidad del negocio, ver la norma ISO/IEC 27031.

c) Reforzar el enfoque en la prevención de incidentes de seguridad de la información

El uso de un enfoque estructurado para la gestión de incidentes de seguridad de la información ayuda a crear un mejor enfoque en la prevención de incidentes dentro de una organización, incluyendo el desarrollo de métodos para identificar nuevas amenazas y vulnerabilidades. El análisis de los datos relacionados con los incidentes permite la identificación de patrones y tendencias, facilitando así un enfoque más preciso en la prevención de incidentes y la identificación de acciones apropiadas para evitar que se produzcan más.

d) Mejorar la priorización

Un enfoque estructurado de la gestión de incidentes de seguridad de la información proporcionará una base sólida para el establecimiento de prioridades a la hora de realizar investigaciones sobre incidentes de seguridad de la información, incluido el uso de escalas efectivas de categorización y clasificación. Si no existen procedimientos claros, existe el riesgo de que las actividades de investigación se lleven a cabo de un modo excesivamente reactivo, respondiendo a los incidentes a medida que se producen y pasando por alto qué actividades deberían tratarse con mayor prioridad.

e) Apoyar la recopilación de evidencia y la investigación

Cuando sea necesario, unos procedimientos claros de investigación de incidentes ayudarán a asegurar que la recopilación y el manejo de los datos sean evidentemente sólidos y legalmente admisibles. Se trata de consideraciones importantes si se puede emprender un proceso judicial o una acción disciplinaria. Para más información sobre la evidencia digital y la investigación, ver las normas de investigación del Anexo A.

g) Contribuir a la justificación del presupuesto y los recursos

Un enfoque bien definido y estructurado de la gestión de incidentes de seguridad de la información ayudará a justificar y simplificar la asignación de presupuestos y recursos para las unidades organizativas involucradas. Además, el propio plan de gestión de incidentes de seguridad de la información se beneficiará de la posibilidad de planificar mejor la asignación de personal y recursos.

Un ejemplo de una forma de controlar y optimizar el presupuesto y los recursos es añadir el seguimiento del tiempo a las tareas de gestión de incidentes de seguridad de la información para facilitar la evaluación cuantitativa del manejo de incidentes de seguridad de la información por parte de la organización. Debería ser posible proporcionar información sobre el tiempo que se tarda en resolver incidentes de seguridad de la información de diferentes prioridades y en diferentes plataformas. Si existen cuellos de botella en el proceso de gestión de incidentes de seguridad de la información, éstos también deberían ser identificables.

h) Mejorar la actualización de los resultados de la evaluación y gestión de los riesgos para la seguridad de la información

El uso de un enfoque estructurado para la gestión de incidentes de seguridad de la información facilitará:

- una mejor recopilación de datos para ayudar en la identificación y determinación de las características de los distintos tipos de amenazas y vulnerabilidades asociadas, y
- el suministro de datos sobre la frecuencia de aparición de los tipos de amenazas identificados.

Los datos recopilados sobre los impactos negativos de los incidentes de seguridad de la información en las operaciones de la empresa serán útiles para el análisis del impacto en el negocio. Los datos recopilados para identificar la frecuencia de varios tipos de amenazas mejorarán la calidad de una evaluación de amenazas.

Del mismo modo, los datos recolectados recopliados sobre las vulnerabilidades mejorarán la calidad de las futuras evaluaciones de estas. Para obtener orientación sobre la evaluación y gestión de los riesgos para la seguridad de la información, ver la norma ISO/IEC 27005.

i) Proporcionar material mejorado del programa de formación y concienciación sobre la seguridad de la información

Un enfoque estructurado de la gestión de incidentes de seguridad de la información permitirá a una organización recopilar la experiencia y el conocimiento de cómo la organización maneja los incidentes, lo que será un material valioso para un programa de concienciación de seguridad de la información. Un programa de concienciación que incluya las lecciones aprendidas de la experiencia real ayudará a reducir los errores o la confusión en futuros incidentes de seguridad de la información.

j) Aportar insumos a las revisiones de la política de seguridad de la información y de la documentación relacionada

Los datos proporcionados por un plan de gestión de incidentes de seguridad de la información podrían brindar un insumo valioso a las revisiones de la eficacia y posterior mejora de las políticas de seguridad de la gestión de incidentes (y otros documentos de seguridad de la información relacionados). Esto aplica a las políticas de temas específicos y a otros documentos aplicables tanto a toda la organización como a sistemas individuales, servicios y redes.

4.4 Adaptabilidad

La orientación proporcionada por la norma INTE/ISO/IEC 27035 (en todas sus partes) es extensa y, si se adopta en su totalidad, podría requerir importantes recursos para su funcionamiento y gestión. Por lo tanto, es importante que una organización que aplique esta orientación debería mantener un sentido de la perspectiva y asegurar que los recursos aplicados a la gestión de incidentes de seguridad de la información y la complejidad de los mecanismos implementados sean proporcionales a lo siguiente:

a) el tamaño, la estructura y la naturaleza del negocio de una organización, incluidos los activos, procesos y datos críticos clave que deberían protegerse
b) el alcance de cualquier sistema de gestión de la seguridad de la información para el manejo de incidentes
c) el riesgo potencial debido a los incidentes
d) los objetivos del negocio.

Por lo tanto, una organización que utilice esta parte de la norma INTE/ISO/IEC 27035 debería adoptar su orientación de tal manera que sea pertinente a la escala y características de su negocio.

5 FASES

5.1 Visión general

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

- Planificación y preparación (ver 5.2);
- Detección y reporte (ver 5.3);
- Evaluación y decisión (ver 5.4);
- Respuestas (ver 5.5);
- Lecciones aprendidas (ver 5.6).

En la figura 3 se muestra una vista de alto nivel de estas fases.

Algunas actividades pueden tener lugar en varias fases o a lo largo del proceso de manejo de incidentes. Entre estas actividades se encuentran las siguientes

- la documentación de la evidencia del evento y del incidente y de la información clave, las acciones de respuesta tomadas y las acciones de seguimiento realizadas como parte del proceso de manejo de incidentes;
- coordinación y comunicación entre las partes involucradas
- notificación a la administración y a otras partes interesadas de incidentes significativos;
- compartición de información entre las partes interesadas y los colaboradores internos y externos, tales como los proveedores y otros IRT.

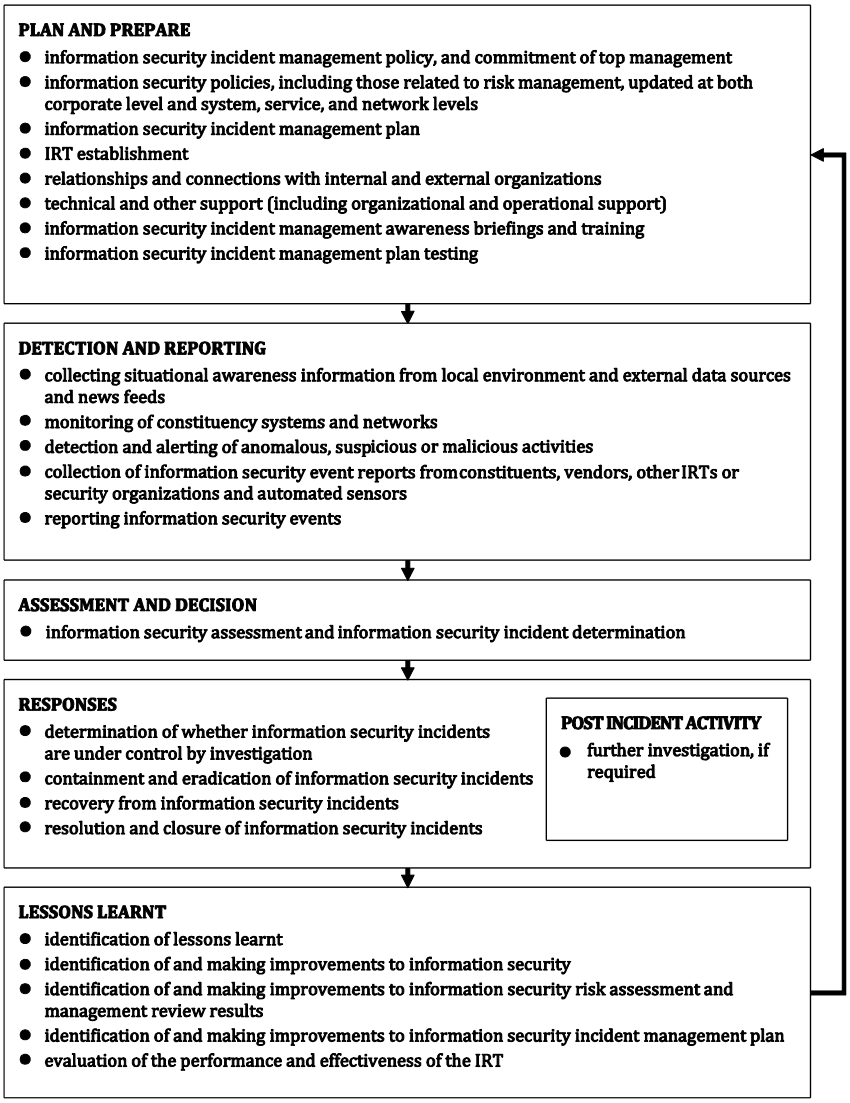

Figura 3 - Fases de la gestión de incidentes de seguridad de la información

Como se ha señalado en la introducción, la norma INTE/ISO/IEC 27035 consta de dos partes.

- La INTE/ISO/IEC 27035 1 cubre las cinco fases.
- La INTE/ISO/IEC 27035 2 cubre
- Planificación y preparación, y
- Lecciones aprendidas

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

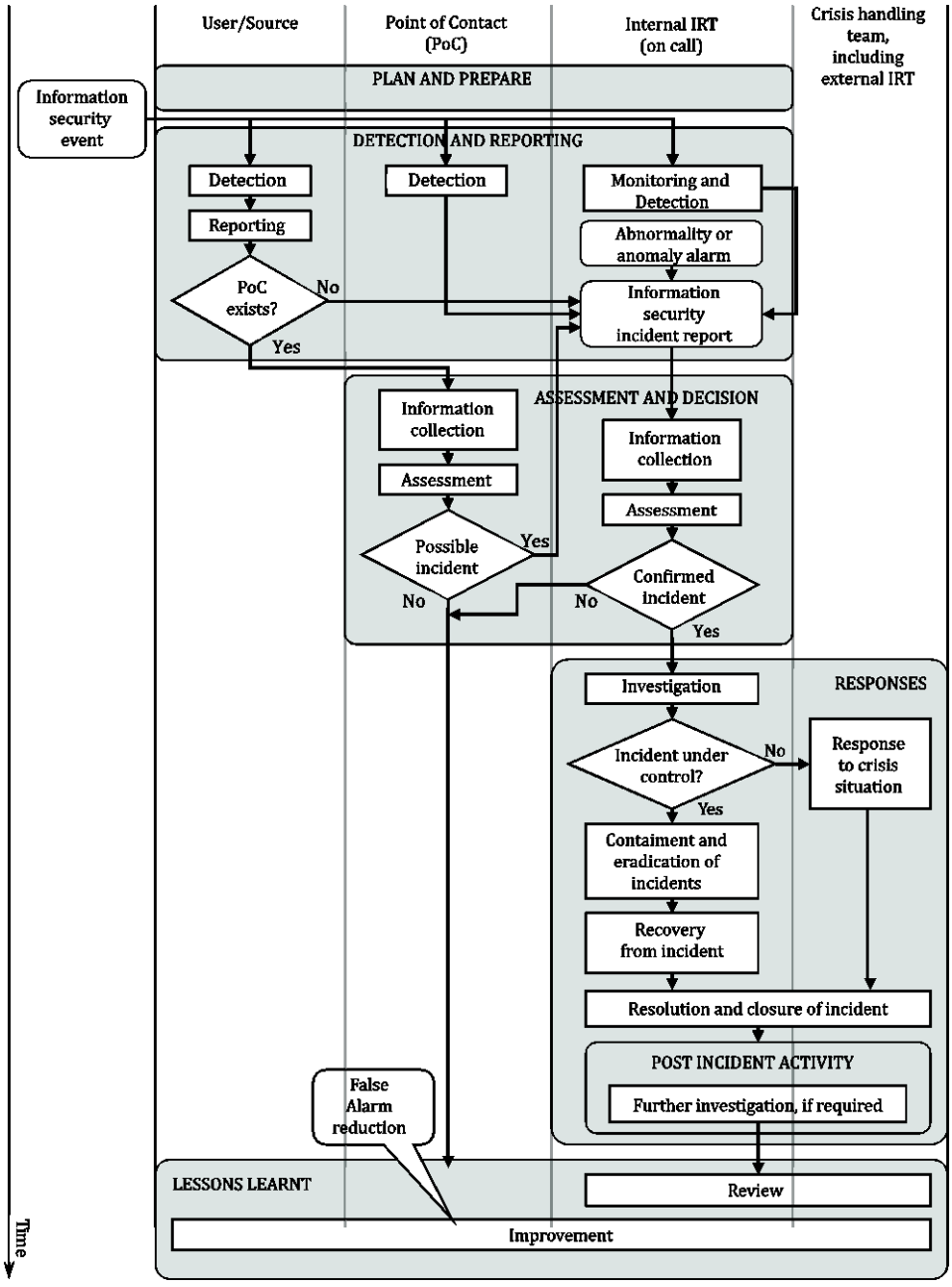

Figura 4 - Diagrama de flujo de eventos e incidentes de seguridad de la información

5.2 Planificación y preparación

Una gestión efectiva de los incidentes de seguridad de la información requiere una planificación y una preparación adecuadas. Para poner en marcha un plan de gestión de incidentes de seguridad de la información eficiente y efectivo, una organización debería completar una serie de actividades preparatorias, a saber:

a) formular y elaborar una política de gestión de incidentes de seguridad de la información y obtener el compromiso de la alta dirección con dicha política;
b) actualizar las políticas de seguridad de la información, incluidas las relacionadas con la gestión de riesgos, a nivel corporativo y a niveles específicos de sistemas, servicios y redes
c) definir y documentar un plan detallado de gestión de incidentes de seguridad de la información, que incluya temas que abarquen las comunicaciones y la divulgación de información
d) establecer el IRT, con un programa de formación adecuado diseñado, desarrollado e impartido a su personal
e) establecer y conservar las relaciones y conexiones apropiadas con organizaciones internas y externas que estén directamente involucradas con la gestión de eventos de seguridad de la información, incidentes y vulnerabilidades
f) establecer, implementar y operar mecanismos técnicos, organizativos y operativos para apoyar 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, incluyendo una base de datos de seguridad de la información. Estos mecanismos y sistemas están destinados a prevenir la ocurrencia de los incidentes de seguridad de la información o a reducir la probabilidad de que éstos se produzcan;
g) diseñar y desarrollar un programa de toma de conciencia y formación para la gestión de eventos de seguridad de la información, incidentes y vulnerabilidades
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 totalmente preparadas para gestionar adecuadamente los incidentes de seguridad de la información. La norma INTE/ISO/IEC 27035-2 describe cada una de las actividades enumeradas anteriormente, incluyendo el contenido de los documentos de política y planificación.

5.3 Detección y reporte

La segunda fase de la gestión de incidentes de seguridad de la información implica la detección, la recolección de información asociada y el reporte de la ocurrencia de eventos de seguridad de la información y de la existencia de vulnerabilidades de seguridad de la información por medios manuales o automáticos. En esta fase, los eventos y las vulnerabilidades pueden no estar todavía clasificados como incidentes de seguridad de la información.

El reporte de los eventos de seguridad de acuerdo con las políticas de notificación de la organización permite un análisis posterior si es necesario.

Para la fase de Detección y Reporte, una organización debería llevar a cabo las siguientes actividades clave:

a) dar seguimiento y registrar en bitácora la actividad del sistema y de la red de la casa matriz de la organización o subsidiarias, según corresponda;
b) detectar y reportar la ocurrencia de un evento de seguridad de la información o la existencia de una vulnerabilidad de seguridad de la información, ya sea manualmente por el personal o automáticamente;

c) recolectar información sobre un evento de seguridad de la información o una vulnerabilidad;
d) recolectar información sobre la situación a partir de fuentes de datos internas y externas, incluidos registros de actividad y tráfico de red y del sistema local, noticias sobre las actividades políticas, sociales o económicas en curso que podrían afectar la actividad del incidente, fuentes externas sobre tendencias de los 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 en bitácora adecuadamente para su posterior análisis;
f) asegurar que las evidencias digitales se reúnen y almacenan de forma segura, y que se le da seguimiento continuamente a su preservación segura, en caso de que las evidencias sean necesarias para un proceso judicial o una acción disciplinaria interna. Para obtener información más detallada sobre la identificación, la recolección, la adquisición y la preservación de las evidencias digitales, ver las normas de investigación del Anexo A;
g) asegurar que se sigue un régimen de control de cambios para permitir el seguimiento de los eventos de seguridad de la información y de las vulnerabilidades y la actualización de los reportes, así como para mantener actualizada la base de datos de seguridad de la información
h) escalar, según sea necesario a lo largo de la fase, para posterior revisión o decisiones.

Toda la información recopilada relativa a un evento de seguridad de la información o a una vulnerabilidad debería almacenarse en la base de datos de seguridad de la información gestionada por el IRT. La información comunicada durante cada actividad debería ser lo más completa posible en ese momento. Esto apoyará las evaluaciones, las decisiones y las acciones a tomar.

5.4 Evaluación y decisión

La tercera fase de la gestión de los incidentes de seguridad de la información implica 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 se ha detectado y reportado un evento de seguridad de la información, deberían realizarse las siguientes actividades

a) distribuir la responsabilidad de las actividades de gestión de los incidentes de seguridad de la información a través de una jerarquía adecuada de personal, con evaluación, toma de decisiones y acciones que impliquen tanto al personal de seguridad como al que no lo es;
b) proporcionar procedimientos formales para que cada persona notificada los siga, incluyendo la revisión y modificación de los reportes, la evaluación de los daños y la notificación al personal pertinente. Las acciones individuales dependerán del tipo y la severidad del incidente
c) utilizar directrices para la documentación exhaustiva de un evento de seguridad de la información y las acciones subsiguientes 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 debería realizar las siguientes actividades clave:

- recolectar información que puede incluir pruebas, mediciones y otra recolección de datos sobre la detección de un evento de seguridad de la información. El tipo y la cantidad de información recolectada dependerá del evento de seguridad de la información que haya ocurrido;
- realizar una evaluación por parte del gestor de 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 reportado que se descubre que no es real o que no tiene ninguna consecuencia. Si lo desea, el IRT puede llevar a cabo una revisión de calidad para asegurarse de que el gestor de incidentes ha declarado correctamente un incidente;
- asegurarse de que todas las partes implicadas, especialmente el IRT, registran adecuadamente todas las actividades, resultados y decisiones relacionadas para su posterior análisis
- asegurar que se mantiene el régimen de control de cambios para cubrir el seguimiento de los incidentes de seguridad de la información y las actualizaciones de los reportes de incidentes, y para mantener actualizada la base de datos de seguridad de la información.

Toda la información recolectada relativa a un evento de seguridad de la información, un incidente o una vulnerabilidad debería almacenarse en la base de datos de seguridad de la información gestionada por el IRT. La información reportada durante cada actividad debería ser lo más completa posible en ese momento. Esto apoyará las evaluaciones, las decisiones y las 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 con las acciones determinadas en la fase de Evaluación y Decisión. Dependiendo de las decisiones, las respuestas podrían realizarse inmediatamente, en tiempo real o casi en tiempo real, y algunas respuestas podrían implicar la investigación de la seguridad de la información.

Una vez que se ha confirmado un incidente de seguridad de la información y se han determinado las respuestas, deberían llevarse a cabo las siguientes actividades:

a) distribuir la responsabilidad de las actividades de gestión de los incidentes de seguridad de la información a través de una jerarquía adecuada de personal con capacidad de decisión y de actuación, que involucre tanto al personal de seguridad como al que no lo es, según sea necesario;
b) proporcionar procedimientos formales para que los siga cada persona involucrada, incluyendo la revisión y modificación de los reportes, la reevaluación de los daños y la notificación al personal pertinente. Las acciones individuales dependerán del tipo y la severidad del incidente
c) utilizar directrices para documentar exhaustivamente un incidente de seguridad de la información y las acciones posteriores.

Para la fase de Respuesta, una organización debería realizar las siguientes actividades clave:

- investigar los incidentes según sea necesario y en relación con la calificación de la escala de clasificación de incidentes de seguridad de la información. La escala debería modificarse según sea necesario. La investigación puede incluir diferentes tipos de análisis para proporcionar una comprensión más profunda de los incidentes.
- revisar por parte del IRT para determinar si el incidente de seguridad de la información está bajo control y, en caso afirmativo, realizar la respuesta requerida. Si el incidente no está bajo control o va a tener un impacto severo en las operaciones de la organización, realizar las actividades de respuesta a la crisis mediante el escalamiento a la función de gestión 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 posteriores evaluaciones o decisiones.
- asegurarse de que todas las partes involucradas, en particular el IRT, registren adecuadamente todas las actividades para su posterior análisis.

- asegurar que las evidencias digitales se recolecten y almacenen de forma segura, y que se da seguimiento continuamente a su preservación segura, en caso de que las evidencias sean necesarias para un proceso judicial o una acción disciplinaria interna. Para obtener información más detallada sobre la identificación, la recolección, la adquisición y la preservación de las evidencias digitales, ver las normas de investigación del Anexo A.
- asegurar que se mantiene el régimen de control de cambios para cubrir el seguimiento de los incidentes de seguridad de la información y las actualizaciones de los reportes de incidentes, y para mantener actualizada la base de datos de seguridad de la información
- comunicar la existencia del incidente de seguridad de la información y compartir cualquier detalle pertinente (por ejemplo, información sobre amenazas, ataques y vulnerabilidades) con otras personas u organizaciones internas y externas, de acuerdo con los planes de comunicación de la organización y del IRT y con las políticas de divulgación de información. Puede ser particularmente importante notificar a los propietarios de los activos (determinados durante el análisis de impacto) y a las organizaciones internas y externas (por ejemplo, otros equipos de respuesta a incidentes, agencias policiales, proveedores de servicios de Internet y organizaciones que comparten información) que podrían ayudar con la gestión y resolución del incidente. Compartir información también podría beneficiar a otras organizaciones, ya que las mismas amenazas y ataques suelen afectar a varias organizaciones. Para más detalles sobre compartir información, ver la norma INTE/ISO/IEC 27010.
- Tras la recuperación de un incidente, debería iniciarse una actividad posterior al Incidente, dependiendo de la naturaleza y la severidad del incidente. Esta actividad incluye:
- la investigación de la información relativa al incidente
- la investigación de otras fuentes relevantes, como el personal involucrado, y
- reporte resumido de los resultados de la investigación.
- Una vez resuelto el incidente, debe cerrarse de acuerdo con los requisitos del IRT o de la organización matriz y se debe notificar a todas las partes interesadas.

Toda la información recolectada relativa a un evento de seguridad de la información, incidente o vulnerabilidad debería almacenarse en la base de datos de seguridad de la información gestionada por el IRT. La información reportada durante cada actividad debería ser lo más completa posible en ese momento. Esto apoyará las evaluaciones, decisiones y acciones a tomar, incluyendo potenciales análisis posteriores.

5.6 Lecciones aprendidas

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

Para la fase de Lecciones Aprendidas, una organización debería realizar las siguientes actividades clave:

a) identificar las lecciones aprendidas de los incidentes de seguridad de la información y las vulnerabilidades;
b) revisar, identificar y mejorar la implementación de los controles de seguridad de la información (controles nuevos o actualizados), así como la política de gestión de incidentes de seguridad de la información. Las lecciones pueden provenir de uno o varios incidentes de seguridad de la información o de vulnerabilidades de seguridad reportadas. Las mejoras se ven favorecidas por las métricas introducidas en la estrategia de la organización sobre dónde invertir en controles de seguridad de la información;
c) revisar, identificar y mejorar la evaluación de riesgos de seguridad de la información y las revisiones de gestión existentes en la organización;

d) revisar cuán efectivos fueron los procesos, los procedimientos, los formatos de reporte y la estructura organizativa para responder, evaluar y recuperarse de los incidentes de seguridad de la información y hacer frente a las vulnerabilidades de la seguridad de la información. Sobre la base de las lecciones aprendidas, identificar e introducir mejoras en el 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 de confianza (si la organización lo desea)
f) determinar si la información sobre el incidente, los vectores de ataque asociados y las vulnerabilidades pueden compartirse con organizaciones asociadas para ayudar a prevenir que se produzcan los mismos incidentes en sus entornos. Para más detalles, ver la norma INTE/ISO/IEC 27010 sobre compartir información;
g) realizar una evaluación exhaustiva del rendimiento y la eficacia del IRT de forma periódica.

Se hace hincapié en que las actividades de gestión de incidentes de seguridad de la información son iterativas y, por lo tanto, una organización debería realizar mejoras periódicas en una serie de elementos de seguridad de la información a lo largo del tiempo. Estas mejoras deberían proponerse sobre la base de las revisiones de los datos sobre los incidentes de seguridad de la información, las respuestas y las vulnerabilidades de seguridad de la información reportadas.

La norma INTE/ISO/IEC 27035-2 describe en detalle cada una de las actividades mencionadas anteriormente.

6 CORRESPONDENCIA

Esta norma nacional es idéntica (IDT) a la norma ISO/IEC 27035-1:2016, “Information technology – Security techniques — Information security incident management — Part 1: Principles of incident management”.

ANEXO A (INFORMATIVO)

RELACIÓN CON LAS NORMAS DE INVESTIGACIÓN

Esta parte de la norma INTE/ISO/IEC 27035 describe parte de un proceso de investigación completo que incluye, pero no se limita a, la aplicación de las siguientes normas:

- ISO/IEC 27037, Directrices para la identificación, recolección, adquisición y preservación de evidencias digitales

Describe los medios por los que los involucrados en las primeras fases de una investigación, incluida la respuesta inicial, pueden asegurar la captura de suficientes evidencias digitales potenciales para permitir que la investigación avance adecuadamente.

- ISO/IEC 27038, Especificación para la redacción digital

Algunos documentos pueden contener información que no debería ser revelada a algunos grupos. Los documentos modificados pueden entregarse a estos grupos después de un tratamiento adecuado del documento original. El proceso de eliminación de la información que no debe divulgarse se denomina "redacción".

La redacción digital de documentos es un área relativamente nueva de la práctica de gestión de documentos, que plantea problemas únicos y riesgos potenciales. Cuando se redactan los documentos digitales, la información eliminada no debería ser recuperable. Por lo tanto, hay que tener cuidado para que la información redactada se elimine permanentemente del documento digital (por ejemplo, no debería ocultarse simplemente en partes del documento que no se puedan mostrar).

La norma ISO/IEC 27038 especifica métodos para la redacción digital de documentos digitales. También especifica los requisitos del software que puede utilizarse para la redacción.

- ISO/IEC 27040, Seguridad del almacenamiento

La norma ISO/IEC 27040 proporciona una orientación técnica detallada sobre cómo las organizaciones pueden definir un nivel adecuado de mitigación de riesgos mediante el empleo de un enfoque bien probado y coherente para la planificación, el diseño, la documentación y la implementación de la seguridad del almacenamiento de datos. La seguridad del almacenamiento aplica a la protección (seguridad) de la información donde se almacena y a la seguridad de la información que se transfiere a través de los enlaces de comunicación asociados al almacenamiento. La seguridad del almacenamiento incluye la seguridad de los dispositivos y medios de almacenamiento, la seguridad de las actividades de gestión relacionadas con los dispositivos y los medios de almacenamiento, la seguridad de las aplicaciones y los servicios, y la seguridad relevante para los usuarios finales durante la vida útil de los dispositivos y los medios de almacenamiento y después de que finaliza su utilización.

Los mecanismos de seguridad como el cifrado y la higienización pueden afectar a la capacidad de investigación al introducir mecanismos de ofuscación. Deberían tenerse en cuenta antes y durante la realización de una investigación. También puede ser importante para asegurar que el almacenamiento del material de evidencia durante y después de una investigación esté adecuadamente preparado y protegido.

- ISO/IEC 27041, Orientación para asegurar la idoneidad y adecuación de los métodos de investigación de incidentes.

Es importante que se pueda demostrar que los métodos y procesos utilizados durante una investigación son adecuados. Este documento proporciona orientación sobre cómo asegurar que los métodos y procesos cumplen los requisitos de la investigación y se han probado adecuadamente.

- INTE/ISO/IEC 27042, Directrices para el análisis y la interpretación de evidencias digitales

Describe cómo pueden diseñarse e implementarse los métodos y procesos que se utilizarán durante una investigación para permitir la correcta evaluación de las posibles evidencias digitales, la interpretación de estas y la comunicación efectiva de los hallazgos.

- ISO/IEC 27043, Principios y procesos de investigación de incidentes

Define los principios y procesos comunes clave que subyacen a la investigación de incidentes y proporciona un modelo marco para todas las etapas de las investigaciones.

- ISO/IEC 27050, Descubrimiento electrónico

La norma ISO/IEC 27050 aborda las actividades de descubrimiento electrónico, que incluyen, entre otras, la identificación, la preservación, la recolección, el procesamiento, la revisión, el análisis y la producción de información almacenada electrónicamente (ESI, por sus siglas en inglés). Además, proporciona orientación sobre las medidas, que abarcan desde la creación inicial de la ESI hasta su disposición final, que una organización puede emprender para mitigar el riesgo y los gastos en caso de que el descubrimiento electrónico se convierta en un problema. Es relevante tanto para el personal no técnico como para el técnico que participa en algunas o todas las actividades de descubrimiento electrónico. Es importante señalar que esta orientación no pretende contradecir o sustituir las leyes y reglamentos jurisdiccionales locales.

El descubrimiento electrónico a menudo sirve como motor para las investigaciones, así como para las actividades de adquisición y manejo de evidencia. Además, la sensibilidad y la criticidad de los datos a veces requieren protecciones como la seguridad del almacenamiento para evitar las violaciones de datos.

- ISO/IEC 30121, Marco de gobernanza del riesgo forense digital

La norma ISO/IEC 30121 proporciona un marco para los órganos de gobernanza de las organizaciones (incluidos los propietarios, los miembros del consejo de administración, los directores, los socios, los altos ejecutivos o similares) sobre la mejor manera de preparar una organización para las investigaciones digitales antes de que se produzcan. La norma ISO/IEC 30121 aplica al desarrollo de procesos (y decisiones) estratégicos relacionados con la retención, la disponibilidad, el acceso y la efectividad en costos de la divulgación de evidencias digitales. La norma ISO/IEC 30121 es aplicable a todo tipo y tamaño de organizaciones. La ISO/IEC 30121 trata de la preparación estratégica prudente para la investigación digital de una organización. La preparación forense asegura que una organización ha realizado la preparación estratégica adecuada y relevante para aceptar posibles eventos de naturaleza evidencial. Las acciones pueden producirse como resultado de inevitables violaciones de la seguridad, fraudes reclamos de reputación. En cada situación, la tecnología de la información (TI) debería desplegarse estratégicamente para maximizar la eficacia de la disponibilidad, la accesibilidad y la eficiencia de costos de las evidencias.

La figura A.1 muestra las actividades típicas en torno a un incidente y su investigación. Los números que aparecen en este diagrama (por ejemplo, 27037) indican las normas internacionales enumeradas anteriormente y las barras sombreadas muestran dónde es más probable que cada una sea directamente aplicable o tenga alguna influencia en el proceso de investigación (por ejemplo, estableciendo políticas o creando restricciones). No obstante, se recomienda consultar todas las normas internacionales antes y durante las fases de planificación y preparación.

Las clases de procesos que se muestran se definen en su totalidad en la norma ISO/IEC 27043 y las actividades identificadas coinciden con las que se tratan con más detalle en las normas INTE/ISO/IEC 27035-2, ISO/IEC 27037, INTE/ISO/IEC 27042 e ISO/IEC 27041.

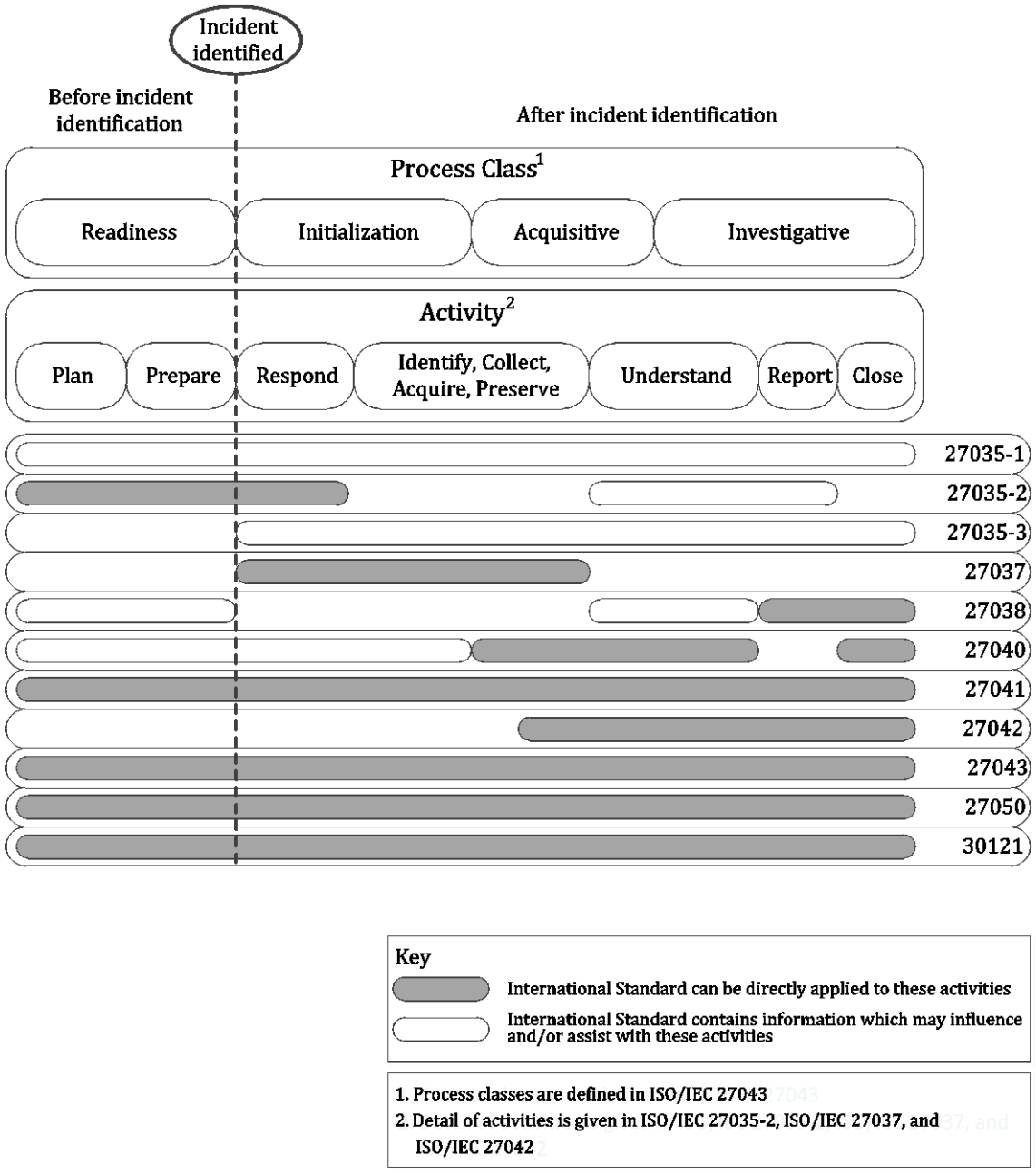

Figura A.1 - Aplicabilidad de las normas a las clases de procesos y actividades de investigación

ANEXO B (INFORMATIVO)

EJEMPLOS DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y SUS CAUSAS

B.1 Ataques

B.1.1 Denegación de Servicio

La denegación de servicio (DoS, por sus siglas en inglés) y la denegación de servicio distribuida (DDoS, por sus siglas en inglés) son una amplia categoría de incidentes con un hilo conductor común. Dichos incidentes provocan que un sistema, servicio o red no pueda seguir operando en su capacidad prevista, la mayoría de las veces con una negación total del acceso a los usuarios legítimos. Hay dos tipos principales de incidentes DoS/DDoS causados por medios técnicos: eliminación de recursos y escases de recursos.

Ejemplos típicos de incidentes DoS/DDoS técnicos deliberados son los siguientes:

- hacer ping a direcciones de difusión de la red para llenar el ancho de banda de la red con tráfico de respuesta;
- enviar datos en un formato inesperado a un sistema, servicio o red para intentar colapsarlo o interrumpir su funcionamiento normal
- abrir múltiples sesiones autorizadas con un sistema, servicio o red en particular para intentar agotar sus recursos (es decir, ralentizarlo, bloquearlo o colapsarlo).

Este tipo de ataques suele realizarse a través de bots, un sistema informático que ejecuta un software malicioso controlado a través de una red de bots (botnet). Una botnet es una red central de mando y control de bots gestionada por humanos. El tamaño de las redes de bots puede oscilar entre cientos y millones de computadores afectados.

Algunos incidentes técnicos de DoS pueden ser causados accidentalmente, por ejemplo, por una mala configuración del operador o por la incompatibilidad del software de aplicación, pero la mayoría de las veces son deliberados. Algunos incidentes técnicos de DoS se lanzan intencionadamente con el fin de colapsar un sistema o servicio, o derribar una red, mientras que otros son simplemente los subproductos de otra actividad maliciosa. Por ejemplo, algunas de las técnicas más comunes de escaneo e identificación sigilosa pueden hacer que los sistemas o servicios más antiguos o mal configurados se caigan cuando se escanean. Debe tenerse en cuenta que muchos incidentes DoS técnicos deliberados se ejecutan a menudo de forma anónima (es decir, el origen del ataque es "falso"), ya que normalmente no dependen de que el atacante reciba ninguna información de vuelta de la red o el sistema atacado.

Los incidentes de DoS causados por medios no técnicos, que provocan la pérdida de información, servicios y/o instalaciones, pueden ser causados, por ejemplo, por:

- infracciones de las disposiciones de seguridad física que den lugar a robos o a daños intencionados y a la destrucción de los equipos
- daños accidentales a los equipos (y/o a su ubicación) a causa de un incendio o de daños por agua o inundaciones
- condiciones ambientales extremas, por ejemplo, altas temperaturas de funcionamiento (por ejemplo, debido a un fallo del aire acondicionado)
- mal funcionamiento o sobrecarga del sistema,
- cambios incontrolados del sistema, y
- fallos en el software o el hardware.

B.1.2 Acceso no autorizado

En general, esta categoría de incidentes consiste en intentos reales no autorizados de acceso o uso indebido de un sistema, servicio o red. Algunos ejemplos de incidentes de acceso técnico no autorizado son:

- intentos de recuperar archivos de contraseñas,
- ataques de desbordamiento del búfer para intentar obtener acceso privilegiado (por ejemplo, de administrador del sistema) a un objetivo,
- explotación de vulnerabilidades de protocolo para secuestrar o desviar conexiones de red legítimas, e
- intentos de elevar los privilegios a recursos o información más allá de lo que un usuario o administrador ya posee legítimamente.
- Los incidentes de acceso no autorizado causados por medios no técnicos, que dan lugar a la divulgación o modificación directa o indirecta de la información, a la violación de la responsabilidad o al uso indebido de los sistemas de información, podrían ser causados, por ejemplo, por:
- violaciones de los dispositivos de seguridad física que den lugar a un acceso no autorizado a la información, y
- sistemas operativos deficientes y/o mal configurados debido a cambios incontrolados en el sistema, o a un mal funcionamiento del software o del hardware.

B.1.3 Software malicioso

El software malicioso es un programa o parte de un programa que se inserta en otro programa con la intención de modificar su comportamiento original, normalmente para realizar actividades maliciosas como el robo de información e identificación, la destrucción de información y recursos, la denegación de servicio, el *spam*, entre otros. Los ataques de software malicioso pueden dividirse en cinco categorías: virus, gusanos, caballos de Troya, código móvil y mezclado. Mientras que los virus se crean para dirigirse a cualquier sistema vulnerable infectado, también se utilizan otros programas maliciosos para realizar ataques dirigidos. A veces se realiza modificando el software malicioso existente y creando una variante que a menudo no es reconocida por las tecnologías de detección de software malicioso.

B.1.4 Abuso

Este tipo de incidente se produce cuando un usuario viola las políticas de seguridad de los sistemas de información de una organización. Este tipo de incidentes no son ataques en el sentido estricto de la palabra, pero a menudo se notifican como incidentes y deberían ser gestionados por un IRT. El uso inapropiado puede ser:

- descargar e instalar herramientas de *hacking*,
- el uso del correo electrónico corporativo para el *spam* o la promoción de negocios personales,
- utilizar recursos corporativos para crear un sitio web no autorizado, y
- el uso de actividades "*peer to peer*" para adquirir o distribuir archivos piratas (música, vídeo, software).

B.2 Recolección de información

En términos generales, la categoría de incidentes de recolección de información incluye las actividades asociadas con la identificación de objetivos potenciales y la comprensión de los servicios que se ejecutan en esos objetivos. Este tipo de incidente implica el reconocimiento, con el objetivo de identificar:

- la existencia de un objetivo, y comprender la topología de la red que lo rodea, y con quién se comunica habitualmente el objetivo, y
- las posibles vulnerabilidades del objetivo o de su entorno de red inmediato que podrían explotarse.

Algunos ejemplos típicos de ataques de recolección de información por medios técnicos son los siguientes:

- volcar los registros del Sistema de Nombres de Dominio (DNS, por sus siglas en inglés) del dominio de Internet del objetivo (transferencia de zona DNS);
- hacer ping a las direcciones de red para encontrar sistemas que estén "vivos";
- sondear el sistema para identificar (por ejemplo, la huella digital) el sistema operativo del host;
- escanear los puertos de red disponibles en un sistema para identificar servicios de red (por ejemplo, correo electrónico, Protocolo de Transferencia de Archivos (FTP, por sus siglas en inglés), web, entre otros.) y las versiones de software de esos servicios;
- escanear uno o más servicios vulnerables conocidos en un rango de direcciones de red (escaneo horizontal).

En algunos casos, la recolección de información técnica se extiende al acceso no autorizado si, por ejemplo, como parte de la búsqueda de vulnerabilidades, el atacante también intenta obtener acceso no autorizado. Esto suele ocurrir con herramientas automatizadas que no sólo buscan vulnerabilidades, sino que también intentan explotar automáticamente los sistemas, servicios y/o redes vulnerables que se encuentran.

Incidentes de recolección de información causados por medios no técnicos, que resultan en:

- divulgación o modificación directa o indirecta de información,
- robo de propiedad intelectual almacenada electrónicamente,
- violaciones de la rendición de cuenta, por ejemplo, en el registro de cuentas, y
- uso indebido de los sistemas de información (por ejemplo, en contra de la ley o de la política de la organización).

Los incidentes de recolección de información pueden ser causados, por ejemplo, por:

- infracciones de los dispositivos de seguridad física que den lugar a un acceso no autorizado a la información, y el robo de equipos de almacenamiento de datos que contengan datos importantes, por ejemplo, claves de cifrado
- sistemas operativos mal configurados o no configurados debido a cambios no controlados en el sistema, o a un mal funcionamiento del software o del hardware, lo que da lugar a que personal interno o externo acceda a información para la que no tiene autoridad, y
- la ingeniería social, que es un acto de manipulación de las personas para que realicen acciones o divulguen información confidencial, por ejemplo, el *phishing*.

ANEXO C (INFORMATIVO)

TABLA DE REFERENCIAS CRUZADAS DE LA NORMA INTE/ISO/IEC 27001 A LA NORMA INTE/ISO/IEC 27035

INTE/ISO/IEC 27001	INTE/ISO/IEC 27035
A.16 Gestión de incidentes de seguridad de la información	INTE/ISO/IEC 27035-1: 4 Visión general (para la visión general de la gestión de incidentes de seguridad de la información)
A.16.1 Gestión de los incidentes de seguridad de la información y mejoras Objetivo: Asegurar un enfoque coherente y efectivo para la gestión de los incidentes de seguridad de la información, incluida la comunicación sobre los eventos de seguridad y debilidades.	INTE/ISO/IEC 27035-1: 5 Fases (para las fases de la gestión de incidentes de seguridad de la información) Anexo B (informativo) Ejemplos de incidentes de seguridad de la información y sus causas INTE/ISO/IEC 27035-2: Anexo A (informativo) Aspectos legales y reglamentarios Anexo B (informativo) Ejemplos de reportes y formularios de eventos, incidentes y vulnerabilidades de seguridad de la información Anexo C (informativo) Ejemplos de enfoques para la categorización y clasificación de eventos e incidentes de seguridad de la información
A.16.1.1 Responsabilidades y procedimientos Control: Se deben establecer responsabilidades y procedimientos de gestión para asegurar razonablemente una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.	INTE/ISO/IEC 27035-1: 5.2 Planificación y preparación 5.4 Evaluación y decisión a), b) INTE/ISO/IEC 27035-2: 4 Política de gestión de incidentes de seguridad de la información 5 Actualización de las políticas de seguridad de la información

INTE/ISO/IEC 27001	INTE/ISO/IEC 27035
	6 Creación de un plan de gestión de incidentes de seguridad de la información 7 Establecimiento de un equipo de respuesta a incidentes (IRT) 8 Establecimiento de relaciones con otras organizaciones 9 Definición del apoyo técnico y de otro tipo 10 Creación de concienciación y formación acerca de incidentes de seguridad de la información
A.16.1.2 Reporte de eventos de seguridad de la información Control: Los eventos de seguridad de la información deben ser reportados a través de los canales de gestión apropiados tan pronto como sea posible.	INTE/ISO/IEC 27035-1: 5.3 Detección y reporte
A.16.1.3 Reportar sobre las debilidades de la seguridad de la información Control: Los empleados y contratistas que utilicen los sistemas y servicios de información de la organización deben anotar y reportar cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	INTE/ISO/IEC 27035-1: 5.3 Detección y reporte
A.16.1.4 Evaluación y decisión sobre eventos de seguridad de la información Control: Los eventos de seguridad de la información deberán ser evaluados y se decidirá si deben ser clasificados como incidentes de seguridad de la información.	INTE/ISO/IEC 27035-1: 5.4 Evaluación y decisión
A.16.1.5 Respuesta a los incidentes de seguridad de la información	INTE/ISO/IEC 27035-1: 5.5 Respuestas

INTE/ISO/IEC 27001	INTE/ISO/IEC 27035
Control: Se debe responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados.	
A.16.1.6 Aprender de los incidentes de seguridad de la información Control: Los conocimientos adquiridos al analizar y resolver los incidentes de seguridad de la información deben utilizarse para reducir la probabilidad o el impacto de futuros incidentes.	INTE/ISO/IEC 27035-1: 5.6 Lecciones aprendidas ISO/CEI 27035-2: 12 Lecciones aprendidas
A.16.1.7 Recolección de evidencia Control: La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	INTE/ISO/IEC 27035-1: 5.3 Detección y reporte d), g) 5.4 Evaluación y decisión d), g) 5.5 Respuestas d), i), l)

BIBLIOGRAFÍA

[1] ISO/IEC 20000 (all parts), Information technology — Service management

[2] ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements

[3] ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security controls

[4] ISO/IEC 27003, Information technology — Security techniques — Information security management system implementation guidance

[5] ISO/IEC 27004, Information technology — Security techniques — Information security management — Measurement

[6] ISO/IEC 27005, Information technology — Security techniques — Information security risk management

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

[8] ISO/IEC 27031, Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity

[9] ISO/IEC 27033 1, Information technology — Security techniques — Network security — Part 1: Overview and concepts

[10] ISO/IEC 27033 2, Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security

[11] ISO/IEC TS 27033 3, Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues

[12] ISO/IEC 27037, Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence

[13] ISO/IEC 27039, Information technology — Security techniques — Selection, deployment and operations of intrusion detection systems (IDPS)

[14] ISO/IEC 27041, Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method

[15] ISO/IEC 27042, Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence

[16] ISO/IEC 27043, Information technology — Security techniques — Incident investigation principles and processes

[17] ISO/IEC 29147, Information technology — Security techniques — Vulnerability disclosure

[18] ISO/IEC 30111, Information technology — Security techniques — Vulnerability handling processes