NORMA TÉCNICA PERUANA

NTP-ISO/IEC 27035
2013

Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias - INDECOPI
Calle de La Prosa 104, San Borja (Lima 41) Apartado 145 Lima, Perú

TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Gestión de incidentes de seguridad de la información

INFORMATION TECHNOLOGY. Security techniques. Information security incident management

(EQV. ISO/IEC 27035:2011 Information technology -- Security techniques -- Information security incident management)

2013-06-26
1ª Edición

R.0045-2013/CNB-INDECOPI. Publicada el 2013-07-19 Precio basado en 123 páginas
I.C.S.: 35.040 ESTA NORMA ES RECOMENDABLE
Descriptores: Tecnología, información, técnica, seguridad, gestión, incidente

INDECOPI

Calle de La Prosa 104, San Borja
Lima- Perú
Tel.: +51 1 224-7777
Fax.: +51 1 224-1715
sacreclamo@indecopi.gob.pe
www.indecopi.gob.pe

ÍNDICE

		página
	ÍNDICE	ii
	PREFACIO	iii
	PRÓLOGO (ISO)	v
	INTRODUCCIÓN (ISO)	vi
1.	OBJETO Y CAMPO DE APLICACIÓN	1
2.	REFERENCIAS NORMATIVAS	1
3.	TÉRMINOS Y DEFINICIONES	2
4.	GENERALIDADES	3
5.	FASE DE PLANEAMIENTO Y PREPARACIÓN	12
6.	FASE DE DETECCIÓN Y REPORTE	39
7.	FASE DE EVALUACIÓN Y DECISIONES	46
8.	FASE DE RESPUESTAS	55
9.	FASES DE LECCIONES APRENDIDAS	72
	ANEXO A	78
	ANEXO B	81
	ANEXO C	86
	ANEXO D	107
	ANEXO E	120

PREFACIO

A. RESEÑA HISTÓRICA

A.1 La presente Norma Técnica Peruana ha sido elaborada por el Comité Técnico de Normalización de Codificación e intercambio electrónico de datos, mediante el Sistema 1 o de Adopción, durante los meses de abril a mayo de2012, utilizando como antecedente a la norma ISO/IEC 27035:2011 Information technology -- Security techniques -- Information security incident management.

A.2 El Comité Técnico de Normalización de Codificación e intercambio electrónico de datos presentó a la Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias –CNB-, con fecha 2013-05-21, el PNTP-ISO/IEC 27035:2013, para su revisión y aprobación, siendo sometido a la etapa de discusión pública el 2013-05-24. No habiéndose presentado observaciones fue oficializada como Norma Técnica Peruana **NTP-ISO/IEC 27035:2013 TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Gestión de incidentes de seguridad de la información,** 1ª Edición, el 19 de julio de 2013.

A.3 La presente Norma Técnica Peruana presenta cambios editoriales referidos principalmente a terminología empleada propia del idioma español y ha sido estructurada de acuerdo a las Guías Peruanas GP 001:1995 y GP 002:1995.

B. INSTITUCIONES QUE PARTICIPARON EN LA ELABORACIÓN DE LA NORMA TÉCNICA PERUANA

Secretaría	GS1 PERU
Presidente	Roberto Puyó
Secretaria	Mary Wong

ENTIDAD	**REPRESENTANTE**
B2IMPROVE S.A.C.	Belén Alvarado

CONSULTOR	Carlos Horna
DELOITTE & TOUCHE S.R.L.	Christian Garratt Diana Lagos
DISTRIBUIDORA MAYORISTA SYMBOL S.A.	Adela Bárcenas Walter Equizabel
INDECOPI	Judith Blanco Martha Arce
INTERNATIONAL ANALYTICAL SERVICE S.A.C.	Raúl Miranda
OFICINA DE NORMALIZACION PREVISIONAL	Roberto Puyó
SUPERINTENDENCIA DE ADMINISTRACION TRIBUTARIA – SUNAT	Daniel Llanos Janet Sánchez
GS1 PERU	Milagros Dávila
CONTRALORÍA GENERAL DE LA REPÚBLICA	Marco Bermúdez Joel Mercado

PRÓLOGO
(ISO)

ISO (la Organización Internacional para la Normalización) e IEC (la Comisión Electrotécnica Internacional) forman el sistema especializado para la normalización mundial. Los organismos nacionales que son miembros de ISO o de IEC participan en el desarrollo de normas internacionales a través de comités técnicos establecidos por la organización respectiva para ocuparse de campos particulares de actividad técnica. Los comités técnicos de ISO y de IEC colaboran en campos de interés mutuos. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en relación con ISO e IEC también participan en el trabajo. En el campo de la tecnología de la información, ISO e IEC han establecido un comité técnico conjunto, ISO / IEC JTC 1.
Las Normas Internacionales se redactan de acuerdo con las reglas proporcionadas por las Directivas ISO / IEC, Parte 2.

La tarea principal del comité técnico conjunto es preparar Normas Internacionales. La versión preliminar de las Normas Internacionales adoptadas por el comité técnico conjunto se circula a los organismos nacionales para votación. La publicación de una Norma Internacional requiere aprobación de al menos 75 % de los Organismos Nacionales que votan.

Se debe notar la posibilidad de que algunos de los elementos de esta Norma Técnica Peruana puedan estar sujetos a derechos de patentes. ISO e IEC no serán responsabilizados de identificar cualquiera o todos esos derechos de patentes.
ISO/IEC 27035 fue preparada por el comité técnico conjunto ISO/IEC JTC 1, *Tecnología de la Información*, Subcomité SC 27, *Técnicas de Seguridad de TI.*

Esta primera edición de ISO/IEC 27035 cancela y reemplaza ISO/IEC TR 18044:2004, la cual ha sido revisada técnicamente.

INTRODUCCIÓN
(ISO)

En general, las políticas o controles de seguridad de la información por sí mismos no garantizarán una protección total de la información, de los sistemas, servicios o redes de información. Luego de haberse implementado los controles, probablemente persisten vulnerabilidades residuales que pueden hacer que la seguridad de la información sea ineficaz y, de esta manera, sean posibles los incidentes de seguridad de la información. Esto puede tener potencialmente impactos tanto directos como indirectos en las operaciones de negocios de una organización. Además, es inevitable que ocurran nuevas instancias de amenazas previamente no identificadas. La preparación insuficiente de una organización para ocuparse de dichos incidentes hará que cualquier respuesta sea menos eficaz e incrementará el grado de impacto potencial adverso en las actividades. Por lo tanto, es esencial que cualquier organización que sea seria respecto de seguridad de la información tenga un enfoque estructurado y planificado respecto de:

– detectar, informar y evaluar incidentes de seguridad de la información;

– responder a los incidentes de seguridad de la información, incluyendo la activación de controles apropiados para la prevención, reducción y recuperación de impactos (por ejemplo, en soporte a las áreas de gestión de crisis);

– informar sobre vulnerabilidades de seguridad de la información que todavía no hayan sido explotadas para causar eventos de seguridad de la información y posiblemente incidentes de seguridad de la información, así como evaluarlas y tratarlas apropiadamente;

– aprender de los incidentes y vulnerabilidades de seguridad de la información, instituir controles preventivos, y hacer mejoras al enfoque general sobre la gestión de incidentes de seguridad de la información.

Esta Norma Internacional provee guía sobre la gestión de incidentes de seguridad de la información en los capítulos 4 a 9. Estos capítulos consisten de varios apartados, los que incluyen una descripción detallada de cada fase.

El término ‘gestión de incidentes de seguridad de la información se utiliza en esta Norma Internacional para abarcar la gestión no solamente de los incidentes de seguridad de la información sino también de las vulnerabilidades de seguridad de la información.

---oooOooo---

TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Gestión de incidentes de seguridad de la información

1. OBJETO Y CAMPO DE APLICACIÓN

Esta Norma Técnica Peruana provee un enfoque estructurado y planificado para:

a) detectar, informar y evaluar incidentes de seguridad de la información;

b) responder a los incidentes de seguridad de la información y manejarlos;

c) detectar, evaluar y manejar las vulnerabilidades de seguridad de la información; y

d) mejorar continuamente la gestión de incidentes y seguridad de la información como resultado de manejar los incidentes y las vulnerabilidades de seguridad de la información.

Esta Norma Técnica Peruana proporciona guía sobre la gestión de incidentes de seguridad de la información para organizaciones grandes y medianas. Las organizaciones más pequeñas pueden usar un conjunto básico de documentos, procesos y rutinas descritos en esta Norma Técnica Peruana, dependiendo de su tamaño y del tipo de negocio relacionado a la situación de riesgo de seguridad de la información. También proporciona guía para que las organizaciones externas provean servicios de gestión de incidentes de seguridad de la información.

2. REFERENCIAS NORMATIVAS

Los siguientes documentos son indispensables para la aplicación de esta Norma Técnica Peruana. Para referencias con fecha, solo aplica la edición citada. Para referencias sin fecha, aplica la última edición del documento en referencia (incluyendo cualquier modificación).

ISO/IEC 27000	Tecnología de la información – Técnicas de seguridad – Sistema de gestión de seguridad de la información – Generalidades y vocabulario

3. TÉRMINOS Y DEFINICIONES

Para propósitos de esta Norma Técnica Peruana, se aplican los términos y definiciones proporcionados en ISO/IEC 27000 así como los siguientes:

3.1
Criminalística de seguridad de la información
Aplicación de técnicas de investigación y análisis para captar, registrar y analizar incidentes de seguridad de la información

3.2
Equipo de respuesta a incidentes de seguridad de la información
ERISI
Equipo de miembros apropiadamente calificados y de confianza de la organización que maneja los incidentes de seguridad de la información durante su ciclo de vida.

NOTA: ElERISI, tal como se describe en esta Norma Técnica Peruana, es una función organizativa que cubre el proceso para los incidentes de seguridad de la información y se centra principalmente en incidentes relacionados a TI. Otras funciones comunes (con abreviaciones similares) dentro del manejo de incidentes pueden tener un alcance y propósito ligeramente diferentes. Las abreviaciones siguientes de uso común tienen un significado similar al de ERISI aunque no exactamente el mismo:

- EREC: Un Equipo de Respuesta de Emergencias de Computadoras se centra principalmente en incidentes sobre tecnología de información y comunicación (TIC). Puede haber otras definiciones nacionales específicas de EREC.

- ERISC: Un Equipo de Respuesta a Incidentes de Seguridad de Computadoras es una organización de servicios responsable de recibir, revisar y responder a los reportes y actividad de incidentes de seguridad de computadoras. Estos servicios se realizan normalmente para un público definido que puede ser una entidad matriz, como una corporación, organización gubernamental u organización educativa; una región o país; una red de investigación; o un cliente pagado.

3.3
Evento de seguridad de la información
Ocurrencia identificada de un sistema, servicio o red que indica una posible ruptura de la seguridad, de la política o una falla en los controles de la información, o una situación desconocida previamente que pueda ser relevante para la seguridad.
[ISO/IEC 27000:2009]

3.4
Incidentes de seguridad de la información
Un evento o una serie de eventos de seguridad de la información, no deseados o inesperados, que tienen una probabilidad importante de comprometer las operaciones de negocios y de amenazar la seguridad de la información.

[ISO/IEC 27000:2009]

4. GENERALIDADES

4.1 Conceptos básicos

Un evento de seguridad de la información es una ocurrencia identificada de un sistema, servicio o estado de la red que indica una posible ruptura de la política de seguridad de la información o una falla de los controles, o bien una situación desconocida previamente que pueda ser relevante para la seguridad. Un incidente de seguridad de la información es un evento único o una serie de eventos de seguridad de la información, no deseados o inesperados, que tienen una probabilidad importante de comprometer las operaciones de negocios y de amenazar la seguridad de la información.

La ocurrencia de un evento de seguridad de la información no significa necesariamente que un intento haya sido exitoso o que haya cualquier implicación sobre la confidencialidad, integridad y/o disponibilidad; es decir, no todos los eventos de seguridad de la información están clasificados como incidentes de seguridad de la información.

Una amenaza actúa de manera no deseada para explotar las vulnerabilidades (debilidades) de los sistemas, servicios o redes de información. Se trata de la ocurrencia de eventos de seguridad de la información y causa potencialmente incidentes no deseados en los activos de información expuestos por las vulnerabilidades. La figura 1 muestra esta relación de

objetos en una cadena de incidentes de seguridad de la información. Los objetos sombreados son preexistentes, afectados por los objetos no sombreados en la cadena que resulta en un incidente de seguridad de la información.

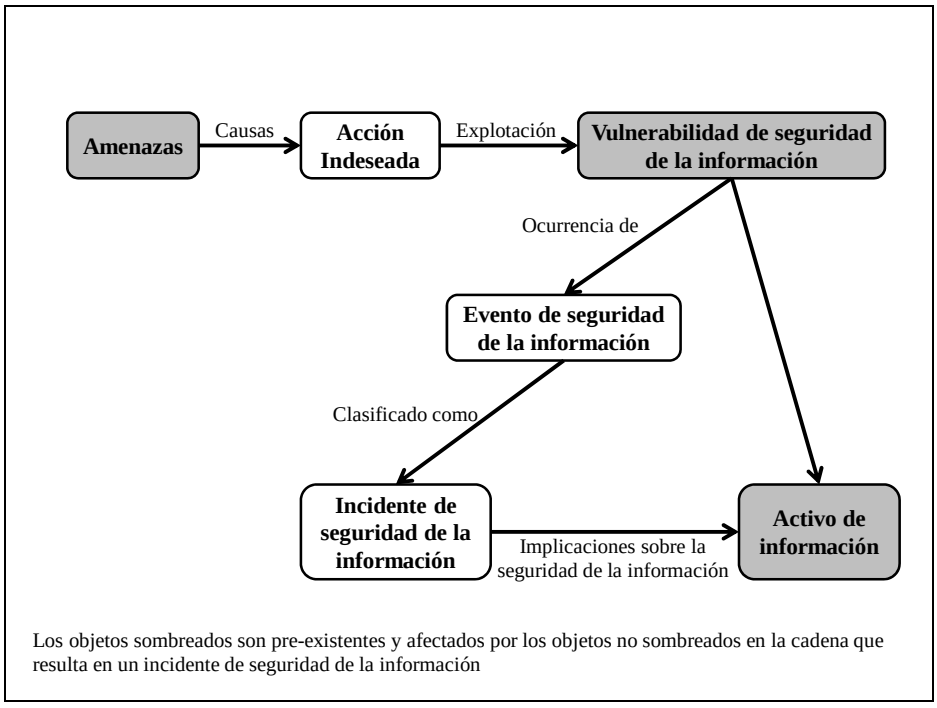

FIGURA 1 - La relación de objetos en una cadena de incidentes de seguridad de la información

4.2 Objetivos

Como parte clave de una estrategia de seguridad de la información general de la organización, la organización debería poner controles y procedimientos para habilitar un enfoque estructurado bien planificado respecto de la gestión de los incidentes de seguridad de la información. Desde una perspectiva de negocios, el objetivo principal es evitar o contener el impacto de los incidentes de seguridad de la información para reducir los costos directos e indirectos causados por los incidentes.

Los pasos principales para minimizar el impacto negativo directo de los incidentes de seguridad de la información son los siguientes:

- detener y contener,
- erradicar,
- analizar y reportar, y
- seguir

Los objetivos de un enfoque estructurado bien planificado son más refinados y deberían asegurar lo siguiente:

a) se detecta eventos de información de seguridad y se los trate eficientemente, en particular identificando si se les tiene que categorizar y clasificar como incidentes de seguridad de la información o no.

b) los incidentes de seguridad de la información identificados se evalúan y se responde a ellos de la manera más apropiada y eficiente.

c) los efectos adversos de los incidentes de seguridad de la información sobre la organización y sus operaciones de negocio se minimizan por medio de controles apropiados como parte de la respuesta al incidente, posiblemente en conjunción con elementos relevantes de un plan o planes de gestión de crisis.

e) las vulnerabilidades reportadas de seguridad de la información se evalúan y se las trata apropiadamente.

e) se aprende rápidamente de las lecciones de los incidentes de seguridad de la información, de las vulnerabilidades y de la gestión que se asocia a ellos. Esto es para incrementar las posibilidades de prevenir la ocurrencia de futuros incidentes de seguridad de la información, de mejorar la implementación y el uso de los controles de seguridad de la información, y de mejorar el esquema general de gestión de incidentes de seguridad de la información.

Para ayudar a lograr esto, las organizaciones deberían asegurar que los incidentes de seguridad de la información se documenten de manera consistente, utilizando normas apropiadas para la categorización y clasificación de incidentes, y compartiendo, de tal manera que se cree métricas a partir de datos agregados sobre un periodo. Esto provee información valiosa para ayudar en el proceso de toma de decisiones estratégicas cuando se invierte en controles de seguridad de la información.

Se reitera que otro objetivo asociado con esta Norma Técnica Peruana es proporcionar una guía a las organizaciones que buscan cumplir con los requisitos especificados en ISO/IEC 27001 (y así, apoyadas por medio de una guía proveniente de ISO/IEC 27002). Esto incluye formación de requisitos relacionados a la gestión de incidentes de seguridad de la información. En el Anexo A se muestra una tabla que tiene referencias cruzadas de los apartados relacionadas a la gestión de incidentes de seguridad de la información en ISO/IEC 27001 e ISO/IEC 27002, así como los apartados en esta Norma Técnica Peruana.

4.3 Beneficios de un enfoque estructurado

Una organización que utiliza un enfoque estructurado para la gestión de incidentes de seguridad de la información acumulará beneficios importantes, los cuales se pueden agrupar bajo los siguientes apartados:

a) Mejora general de seguridad de la información

Un proceso estructurado para la detección, información y evaluación de y toma de decisiones relativas a los eventos e incidentes de seguridad de la información permitirá una identificación y respuesta rápidas. Esto mejorará la seguridad en general ayudando a identificar e implementar rápidamente una solución consistente y así proveer un medio de prevenir incidentes similares futuros de seguridad de la información. Más aún, habrá beneficios facilitados por la métrica, el compartir y la agregación. La credibilidad de la organización mejorará por la demostración de su implementación de mejores prácticas respecto de la gestión de incidentes de seguridad de la información.

b) Reducción de impactos adversos al negocio

Un enfoque estructurado de la gestión de incidentes de seguridad de la información puede ayudar a reducir el nivel de impactos potenciales y adversos al negocio asociados con incidentes de seguridad de la información. Estos impactos pueden incluir pérdida financiera inmediata y pérdida de más largo plazo que surge de una reputación y credibilidad dañada (para ver una guía sobre el análisis de impactos al negocio, véase ISO/IEC 27005:2008).

c) Fortalecimiento del enfoque de prevención de incidentes de seguridad de la información

La utilización de un enfoque estructurado para la gestión de incidentes de seguridad de la información ayuda a crear un mejor enfoque sobre la prevención de incidentes dentro de una organización, incluyendo los métodos de identificación de amenazas y

vulnerabilidades. El análisis de datos relacionados en los incidentes permitiría la identificación de patrones y tendencias, facilitando así el concentrarse más exactamente en la prevención de incidentes y de este modo lograr la identificación de acciones apropiadas para prevenir la ocurrencia de incidentes.

d) Fortalecimiento de la priorización

Un enfoque estructurado a la gestión de incidentes de seguridad de la información proveerá una base sólida para la priorización cuando se conduce investigaciones de incidentes de seguridad de la información incluyendo el uso de escalas eficaces de categorización y clasificación. Si no hay procedimientos claros, hay un riesgo de que las actividades de investigación pudieran conducirse de manera reactiva, respondiendo a los incidentes a medida que ocurren y pasando por alto qué actividades se necesitan. Esto podría impedir que las actividades de investigación se dirijan a áreas donde puede ser una alta prioridad, donde realmente se les necesitan y son la prioridad real.

e) Fortalecimiento de la evidencia

Los procedimientos claros de investigación de incidentes pueden ayudar a asegurar que la recolección y la manipulación de datos sean seguras desde el punto de vista de la producción de evidencias y sean legalmente admisibles. Estos son consideraciones importantes si se fuera a seguir un proceso judicial o una acción disciplinaria. Sin embargo, se debería reconocer que existe una posibilidad de que las acciones necesarias para recuperarse de un incidente de seguridad de la información pudieran poner en peligro la integridad de cualquier evidencia recolectada de dicha manera.

f) Contribución a las justificaciones presupuestarias y de recursos

Un enfoque bien definido y bien estructurado respecto de la gestión de incidentes de seguridad de la información ayudará a justificar y a simplificar la asignación de presupuestos y recursos dentro de unidades organizativas involucradas. Además, el beneficio se acumulará para el esquema mismo de gestión de incidentes de seguridad de la información con:

- el uso de personal calificado para identificar y filtrar las alarmas de anormalidad o anomalía,
- la provisión de una mejor dirección de las actividades del personal calificado, y
- la utilización de personal calificado solamente para aquellos procesos en los que se necesite sus habilidades y solamente en la etapa de proceso en la que se necesite su contribución.

Otro enfoque útil para controlar y optimizar el presupuesto y los recursos es añadir el rastreo de tiempo a la gestión de incidentes de seguridad de la información para facilitar las evaluaciones cuantitativas del manejo que la organización realiza de los incidentes de seguridad de la información. Por ejemplo, debería ser posible proveer información sobre cuánto tiempo toma resolver los incidentes de seguridad de la información de distintas prioridades y sobre diferentes plataformas. Si hay cuellos de botella en el proceso de gestión de incidencias de seguridad de la información, estos también deberían ser identificables.

g) Mejoramiento de las actualizaciones respecto de la evaluación y de los resultados de la gestión de riesgos de seguridad de la información.

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

- la mejor recolección de datos para ayudar en la identificación y determinación de las características de los distintos tipos de amenazas y vulnerabilidades asociadas, y
- la provisión de datos sobre frecuencias de ocurrencias de los tipos de amenazas identificadas.

La recolección de datos sobre los impactos adversos a las operaciones de negocios debido a los incidentes de seguridad de la información será útil en el análisis de impactos al negocio. Los datos recolectados para identificar la frecuencia de ocurrencias de los diversos tipos de amenaza ayudarán en gran medida a la calidad de la evaluación de la amenaza. De manera similar, los datos recolectados sobre vulnerabilidades ayudarán en gran medida a la calidad de las futuras evaluaciones de vulnerabilidad. (Para ver una guía sobre la evaluación y la gestión de riesgos de seguridad de la información, consultar ISO/IEC 27005:2008).

h) Proporción de una mejor consciencia de seguridad de la información y de material de programas de capacitación.

Un enfoque estructurado de la gestión de incidencias de seguridad de la información proveerá información focalizada a los programas sobre consciencia de seguridad de la información. Esta información focalizada proporcionará ejemplos reales que demuestren que los incidentes de seguridad de la información le ocurren a organizaciones reales. También será posible demostrar los beneficios asociados con la rápida disponibilidad de información sobre soluciones. Por otro lado, dicha conciencia ayuda a reducir un error o el pánico/la confusión de un individuo en caso se produjera un incidente de seguridad de la información.

i) Proporción de insumos a la política de seguridad de la información y a las revisiones de documentación relacionadas

Los datos que proporciona un esquema de gestión de incidentes de seguridad de la información podrían proveer insumos valiosos a las revisiones de la eficacia y subsecuente mejora de las políticas de seguridad de la información (y a otros documentos relacionados de seguridad de la información). Eso se aplica a las políticas y otros documentos aplicables tanto para toda la organización como para los sistemas, servicios y redes en particular.

4.4 Adaptabilidad

La guía que esta Norma Técnica Peruana proporciona es extensa y si se adopta plenamente podría requerir de importantes recursos para operar y gestionarse. Por lo tanto, es importante que una organización que aplique esta guía tenga un sentido de la perspectiva y asegure que los recursos aplicados a la gestión de incidentes de seguridad de la información y la complejidad de los mecanismos implementados se mantengan en proporción a lo siguiente:

a) tamaño, estructura y naturaleza del negocio de una organización,

b) alcance de cualquier sistema de gestión de seguridad de la información dentro del que se manejan los incidentes,

c) potencial de pérdida a través del surgimiento de incidentes no previstos, y

d) las metas del negocio.

Una organización que utiliza esta Norma Técnica Peruana debería por lo tanto adoptar esta guía en proporción debida a la escala y características de su negocio.

4.5 Fases

Para lograr los objetivos delineados en el apartado 4.2, la gestión de incidentes de seguridad de la información consiste en las siguientes 5 fases distintivas:

- planeamiento y preparación,

- detección e información,
- evaluación y decisión,
- respuesta, y
- lecciones aprendidas.

La primera fase incluye obtener todo lo que se requiere para realizar una gestión exitosa de incidentes de seguridad de la información. Las otras cuatro fases involucran el uso operativo de la gestión de incidentes de seguridad de la información.

La figura 2 muestra una vista general de estas fases:

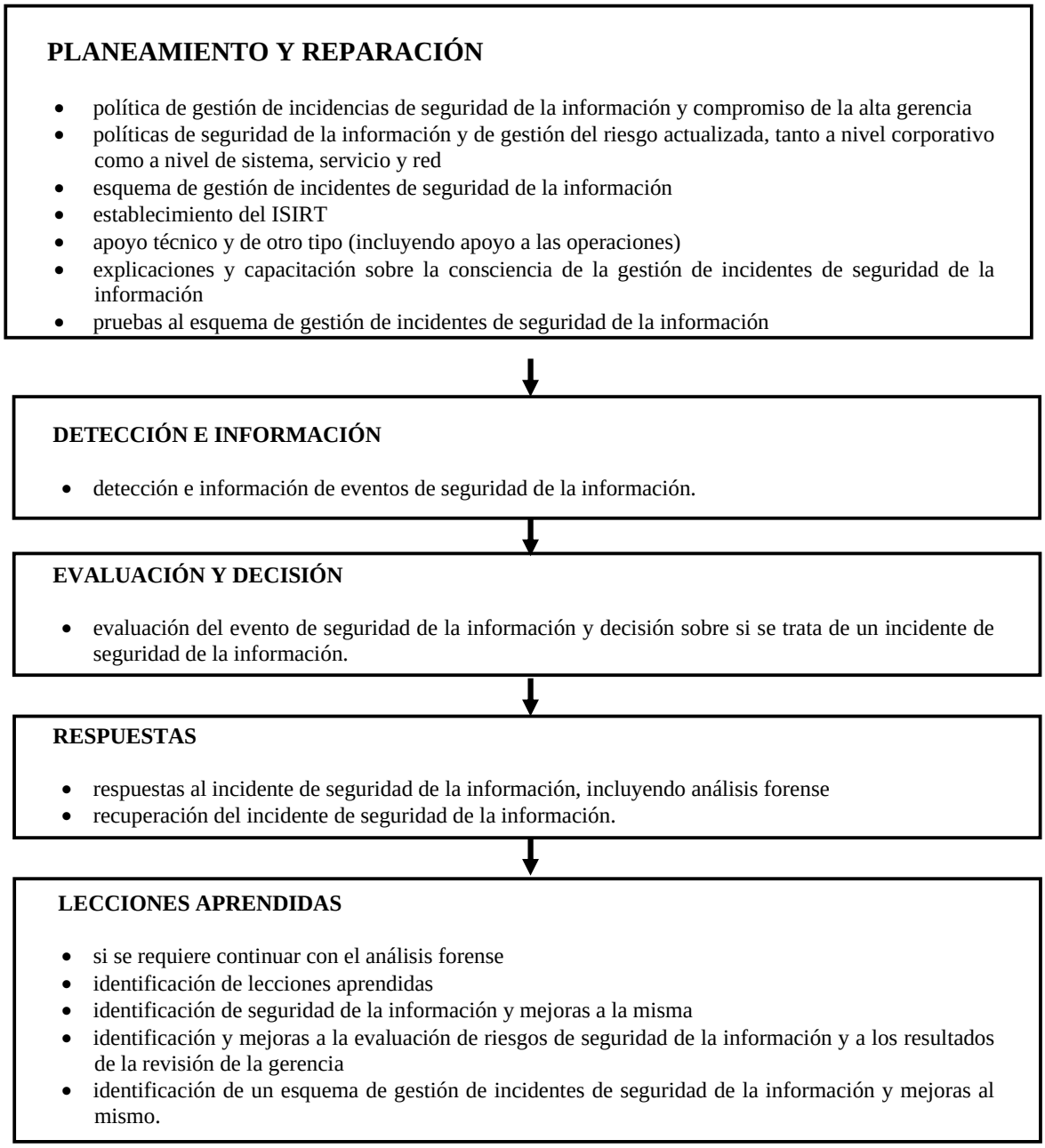

FIGURA 2 – Fases de gestión de incidentes de seguridad de la información

4.6 Ejemplos de incidentes de seguridad de la información

Los incidentes de seguridad de la información pueden ser deliberados o accidentales (por ejemplo, causados por error o por actos de la naturaleza), y pueden ser causados por medios técnicos o físicos. Sus consecuencias pueden incluir la revelación, modificación, destrucción o no disponibilidad de la información de manera no autorizada, o el daño o robo de activos de la organización. Si se determina que los eventos de seguridad de la información no reportados son incidentes, se hace difícil investigar los incidentes y tomar el control para prevenir la recurrencia.

El anexo B provee descripciones de ejemplos seleccionados de incidentes de seguridad de la información y de sus causas solamente para propósitos informativos. Es importante notar que estos ejemplos no son en absoluto exhaustivos.

5. FASE DE PLANEAMIENTO Y PREPARACIÓN

5.1 Revisión de actividades claves

La gestión eficaz de incidentes de seguridad de la información requiere un planeamiento y preparación apropiados. Para poder hacer operativo un esquema de gestión, vulnerabilidades, incidentes y eventos de seguridad de la información de manera eficiente y eficaz, una organización debería completar un número de actividades preparatorias luego del planeamiento necesario. La organización debería asegurar que las actividades del plan y de la fase de preparación incluyan lo siguiente:

a) Actividad para formular y producir una política de gestión de eventos / incidentes / vulnerabilidades de seguridad, y obtener el compromiso de la alta gerencia respecto de esa política. Esto debería ser precedido por una revisión de seguridad de la información sobre las vulnerabilidades de la organización, de confirmación de la necesidad de un esquema de gestión de incidentes de seguridad de la información, y de identificación de los beneficios a la organización en su conjunto y a sus departamentos. (Véase el apartado 5.2) Asegurar el compromiso permanente de la gerencia es vital para la aceptación de un enfoque estructurado para la gestión de incidentes de seguridad de la información. El personal necesita reconocer un incidente, saber qué hacer y comprender los beneficios del enfoque para la organización. La gerencia necesita mostrar su apoyo del esquema de gestión para

asegurar que la organización se comprometa a brindar recursos y a mantener una capacidad de respuesta a los incidentes.

b) Actividad para actualizar la información de seguridad y las políticas de gestión del riesgo a un nivel corporativo y a nivel de sistemas, servicio y redes específicos. Esto debería incluir referencia a la gestión de eventos, incidentes y vulnerabilidades de seguridad de la información. Se tiene que revisar regularmente las políticas en el contexto de los resultados provenientes del esquema de gestión de incidentes de seguridad de la información. (Véase el apartado 5.3)

c) Actividad para definir y documentar un esquema detallado de gestión de incidentes de seguridad de la información. En general, la documentación del esquema debería abarcar los formularios, procedimientos, elementos organizativos y herramientas de apoyo para la detección y para la información de evaluación y toma de decisiones relacionadas a proporcionar respuestas a y lecciones aprendidas de los incidentes de seguridad de la información. Los temas que se deben incluir son los siguientes:

1) Se debe utilizar una escala de clasificación de eventos / incidentes de seguridad de la información para graduar los eventos / incidentes. En cualquier caso, la decisión debería basarse en los impactos adversos reales o proyectados sobre las operaciones de negocios de la organización.

NOTA: El Anexo C muestra un enfoque como ejemplo de categorización y clasificación de eventos e incidentes de seguridad de la información.

2) Los formularios de eventos / incidentes / vulnerabilidades de seguridad de la información son:

i) llenados por la persona que proporciona información sobre el evento de seguridad (es decir, no un miembro del equipo de gestión de incidentes de seguridad de la información), con la información registrada en una base de datos de eventos / incidentes / vulnerabilidades de seguridad de la información,

ii) usados por el personal de gestión de incidentes de seguridad de la información para construir sobre la información del evento de seguridad de la información reportado y habilitar un registro continuo de evaluaciones de incidentes, etc. a lo largo del tiempo hasta que el incidente se resuelva plenamente. En cada etapa se registra la actualización en la base de datos de eventos / incidentes / vulnerabilidades de seguridad de la información. Luego se usa el registro de la base de datos de eventos / incidentes / vulnerabilidades

de seguridad de la información ya llenados en las actividades de resolución post-incidente, y

iii) llenados por la persona que reporta una vulnerabilidad de seguridad de la información (que todavía no ha sido explotada para causar un evento de seguridad de la información y posiblemente un incidente de seguridad de la información) con la información registrada en la base de datos de eventos / incidentes / vulnerabilidades de seguridad de la información.

Se recomienda que estos formularios sean electrónicos (por ejemplo, alguna página web segura), se enlacen directamente a la base de datos electrónica de eventos/incidentes/vulnerabilidades de seguridad de la información. En el mundo de hoy en día, la operación de un esquema basado en papel consumiría mucho tiempo. Sin embargo, un esquema basado en papel podría ser necesario para un caso en el que no se puede utilizar un esquema electrónico.

NOTA: El Anexo D muestra formularios como ejemplo.

3) Los procedimientos y acciones documentados relacionados al uso de los formularios, es decir asociados con la detección de eventos, incidentes y vulnerabilidades de seguridad de la información, con enlaces a los procedimientos normales para el uso de planes de gestión de crisis y respaldo de sistemas, servicios y/o redes.

4) Procedimientos operativos para ERISI, con procesos documentados y responsabilidades asociadas, y la asignación de roles a personas designadas para que conduzcan diversas actividades (se puede asignar a un individuo más de un rol, dependiendo del tamaño, estructura y naturaleza del negocio de una organización) incluyendo por ejemplo:

i) cierre de un sistema, servicio y/o red afectado, en ciertas circunstancias acordado por arreglo previo con la gestión relevante de TI y/o el negocio,

ii) dejar un sistema, servicio y/o red afectado conectado y funcionando,

iii) monitorear el flujo de datos de, a y dentro de un sistema, servicio y/o red afectado,

iv) activar procedimientos y acciones normales de respaldo y gestión de crisis en línea con la política de seguridad del sistema, servicio y/o red,

v) monitorear y mantener la preservación segura de evidencia electrónica en caso se requiera para un proceso legal o una acción disciplinaria interna, y

vi) comunicar detalles del incidente de seguridad de la información a personas u organizaciones internas y externas.

En algunas organizaciones, el esquema se puede conocer como plan de respuesta a incidentes de seguridad de la información (véase el apartado 5.4.)

d) Actividad para establecer el ERISI, con un programa de capacitación apropiado diseñado, desarrollado y proporcionado a su personal. De acuerdo con el tamaño, estructura y naturaleza del negocio, una organización puede tener un ERISI de un equipo dedicado, un equipo virtual, o una mezcla de las dos opciones. Un equipo dedicado puede tener miembros virtuales identificados en unidades/funciones específicas que deberían cooperar de cerca con el ERISI durante la resolución de un incidente de seguridad de la información (TIC, legal, relaciones públicas, compañías tercerizadas, etc.). Un equipo virtual puede tener un alto gerente que lidere el equipo apoyado por grupos de individuos especializados en temas particulares, por ejemplo en el manejo de ataques de código malicioso, a quienes se llamará dependiendo del tipo de incidente concernido. (véase el apartado 5.5)

e) Actividad para establecer y preservar relaciones y conexiones apropiadas con organizaciones internas y externas que están directamente involucradas en la gestión de eventos, incidentes y vulnerabilidades de seguridad de la información.

f) Actividad para establecer, implementar y operar mecanismos de apoyo técnico y de otro tipo (incluyendo la organizacional) para apoyar el esquema de gestión de incidentes de seguridad de la información y, de esta manera, el trabajo del ERISI, y para impedir ocurrencias de incidentes de seguridad de la información o reducir la posibilidad de ocurrencias de incidentes de seguridad de la información. (véase el apartado 5.6) Dichos mecanismos podrían incluir lo siguiente:

1) Mecanismo de auditoría interna de seguridad de la información para evaluar el nivel de seguridad y rastrear los sistemas vulnerables,

2) Gestión de vulnerabilidades (incluyendo actualizaciones de seguridad y parchado de seguridad de los sistemas vulnerables),

3) Vigilancias de la tecnología para detectar nuevos tipos de amenazas y ataques,

4) Sistema de detección de intrusiones (para más detalles, véase ISO/IEC 18043),

5) Dispositivos, medios de protección y herramientas de monitoreo de seguridad de la red (para más detalles, véase ISO/IEC 27033),

6) Software contra código malicioso,

7) Registros del historial de auditorías y software de monitoreo del historial,

8) Responsabilidades y procedimientos operativos documentados para el equipo de apoyo a las operaciones.

g) Actividad para diseñar y desarrollar la conciencia y el programa de capacitación sobre gestión de eventos, incidentes y vulnerabilidades de seguridad de la información. Todo el personal de la organización debería hacerse consciente a través de explicaciones y/u otros mecanismos de la existencia del esquema de gestión de eventos, incidentes y vulnerabilidades de seguridad de la información, sus beneficios y cómo reportar eventos, incidentes y vulnerabilidades de información. En paralelo, se debería proporcionar capacitación apropiada al personal responsable de manejar el esquema de gestión de eventos, incidentes y vulnerabilidades de seguridad de la información, los formuladores de decisiones involucrados en determinar si los eventos de seguridad de la información son incidentes, y aquellos individuos involucrados en la investigación de incidentes. Se debería repetir posteriormente las explicaciones sobre la consciencia y sesiones de capacitación para acomodarse a los cambios en el personal. (Véase el apartado 5.7)

h) Actividad para comprobar el uso del esquema de gestión de incidentes de seguridad de la información así como sus procesos y procedimientos. Se debería organizar periódicamente pruebas no sólo para comprobar el esquema de una situación real sino también para verificar cómo se comporta el ERISI bajo la presión de un incidente complejo grave. Se debería dar atención particular a la creación de pruebas que se centren en los escenarios de vulnerabilidades, amenazas y riesgos a medida que evolucionan. (véase el apartado 8). El esquema debería incluir normas que apoyen el compartir información, tanto dentro como fuera de la organización (si la organización lo requiere). Uno de los beneficios de compartir es la agregación de datos en métrica útil para ayudar a las decisiones estratégicas para el negocio. La membresía de una comunidad que comparte información y en la cual se confía también proporciona advertencia temprana sobre los ataques y se debería alentar en cualquier esquema de gestión de incidente de seguridad de la información y política que se le asocie.

Una vez que se completa esta fase, las organizaciones deberían estar plenamente preparadas para manejar apropiadamente los incidentes de seguridad de la información. Los apartados siguientes describen cada una de las actividades listadas anteriormente incluyendo los contenidos de cada documento requerido.

5.2 Política de gestión de incidentes de seguridad de la información

5.2.1 Introducción

Una organización debería documentar su política para manejar los eventos, incidentes y vulnerabilidades de seguridad de la información como un documento independiente, como parte de su política general del sistema de gestión de seguridad de la información (véase el apartado 4.2.1 b o ISO/IEC 27001:2005), o como parte de su Política de Seguridad de la Información (véase el apartado 5.1.1 de ISO/IEC 27002:2005). El tamaño, estructura y naturaleza del negocio de una organización y la extensión de su programa de gestión de incidentes de seguridad de la información son factores decisivos para determinar cuál de estas opciones adoptar. Cada organización debería dirigir su política de gestión de incidentes de seguridad de la información a cada persona que tenga acceso legítimo a sus sistemas de información y ubicaciones relacionadas.

Antes de que se formule la política, la organización debería conducir una revisión de seguridad de la información que destaque sus vulnerabilidades, que confirme la necesidad de una gestión de incidentes de seguridad de la información y que identifique los beneficios para la organización en su conjunto y para sus departamentos.

5.2.2 Partes involucradas

Una organización debería asegurar que su política de gestión de incidentes de seguridad de la información sea aprobada por un alto funcionario ejecutivo de la organización con el compromiso documentado confirmado de toda la alta gerencia. Debería hacerse disponible a todos los empleados y contratistas y también debería tratarse en las explicaciones y capacitación sobre la consciencia de la seguridad de la información. (véase el apartado 5.7)

5.2.3 Contenido

Una organización debería asegurar que su contenido en la política de gestión de incidentes de seguridad de la información trate de los siguientes temas:

a) La importancia de la gestión de incidentes de seguridad de la información para la organización y el compromiso de la alta gerencia con ella y con el esquema relacionado a la misma.

b) Una revisión de la detección, información y recolección de información relevante sobre eventos de seguridad de la información y sobre cómo debería utilizarse esta información para determinar los incidentes de seguridad de la información.

Esta revisión debería incluir un resumen de posibles tipos de eventos de seguridad de la información, cómo informar sobre ellos, qué informar, dónde y a quién y cómo manejar íntegramente los nuevos tipos de eventos de seguridad de la información, también debería incluir un resumen de los informes y manejo de vulnerabilidades de seguridad de la información.

c) Una revisión de la evaluación de incidentes de seguridad de la información, incluyendo un resumen de quién es responsable, qué se tiene que hacer, de la notificación y el escalamiento.

d) Un resumen de las actividades que siguen a la confirmación de que un evento de seguridad de la información es un incidente de seguridad de la información.

e) Una referencia respecto de la necesidad de asegurar que todas las actividades de gestión de incidentes de seguridad de la información se registran apropiadamente para su análisis posterior y que se conduce un monitoreo continuo para asegurar la preservación segura de evidencia electrónica, en caso se requiera proceso legal o una acción disciplinaria interna.

f) Actividades posteriores de resolución de incidentes de seguridad de la información, incluyendo el aprendizaje de y el mejoramiento del proceso, luego de los incidentes de seguridad de la información.

g) Una revisión de los informes y manejos de las vulnerabilidades de seguridad de la información.

h) Detalles de dónde se mantiene la documentación del esquema, incluyendo los procedimientos.

i) Una revisión del ERISI, abarcando los temas siguientes.

1) La estructura organizativa del ERISI y la identidad del gerente del ERISI, así como de otros miembros clave del personal, incluyendo quién es responsable de:

i) explicar a la alta gerencia los incidentes,

ii) resolver consultas, incentivar el seguimiento, etc., y

iii) el enlace con la organización externa (cuando sea necesario).

2) El estatuto sobre gestión de seguridad de la información que especifica lo que debe hacer el ERISI y la autoridad bajo la cual lo hace. Como mínimo, el estatuto debería incluir una declaración de misión, una definición del alcance del ERISI y detalles del auspiciador a nivel del directorio del ERISI y su autoridad.

3) La declaración de misión del ERISI que se centra en actividades principales del equipo. Para considerarse un ERISI, el equipo debería apoyar la evaluación de, responder a, y manejar los incidentes de seguridad de la información hasta una conclusión exitosa. Las metas y propósitos del equipo son especialmente importantes y requieren definiciones claras y no ambiguas.

4) Una definición del alcance de las actividades del ERISI. Normalmente, el alcance del ERISI de una organización cubre todos sistemas, servicios y redes de información de la organización. En otros casos, la organización puede, por cualquier razón, requerir que el alcance sea menor que esto, en cuyo caso debería documentarse claramente lo que se incluye y lo que se excluye del alcance.

5) Identificación de un alto funcionario ejecutivo, miembro del directorio o alto gerente que tenga la autoridad de tomar una decisión sobre el ERISI y también de establecer los niveles de autoridad del ERISI. Saber esto ayuda a todo el personal de la organización a comprender los antecedentes y la constitución del ERISI y es información vital para construir confianza en el ERISI. Se debería notar que antes de que se promulgue este detalle debería verificarse desde una perspectiva legal. En

algunas circunstancias, la divulgación de la autoridad de algún equipo puede exponerlo a demandas de responsabilidad.

6) Enlaces a organizaciones que proveen apoyo específico externo, como equipos forenses. (Véase el apartado 5.5.4)

j) Una revisión de los mecanismos técnicos y sobre otros soportes.

k) Una revisión de la consciencia de la gestión de incidentes de seguridad de la información y del programa de capacitación.

l) Un resumen de los aspectos legales y regulatorios que tienen que tratarse. (Véase más detalles en el anexo E)

5.3 Integración en otras políticas de la gestión de incidentes de seguridad de la información

5.3.1 Introducción

Una organización debería incluir contenido sobre la gestión de incidentes de seguridad en la información en sus políticas sobre seguridad de la información y gestión del riesgo a nivel corporativo, así como sobre los niveles de sistemas, servicios y redes específicos y relacionar este contenido a la política de gestión de incidentes. La integración debería tener los siguientes objetivos:

a) Describir por qué es importante tener una gestión de incidentes de seguridad, particularmente un esquema para reportar y manejar incidentes de seguridad de la información.

b) Indicar el compromiso de la alta gerencia respecto de la necesidad de una preparación y respuesta apropiadas a los incidentes de seguridad de la información, es decir, al esquema de gestión de incidentes de seguridad de la información.

c) Asegurar consistencia a lo largo de las diversas políticas.

d) Asegurar respuestas planeadas, sistemáticas y calmadas ante los incidentes de seguridad de la información, minimizando así los impactos adversos de los incidentes.

Véase ISO/IEC 27005:2008 para guiarse sobre la evaluación y la gestión de riesgos de seguridad de la información.

5.3.2 Contenido

Cada organización debería actualizar y mantener sus políticas corporativas de gestión del riesgo y de seguridad de la información, y sus políticas de seguridad de la información de sistemas, servicios o redes específicos. Éstas políticas tienen que referirse a una política corporativa de gestión de incidentes de seguridad de la información y al esquema que se le asocia explícitamente.

a) Las secciones relevantes deberían referirse al compromiso de la alta gerencia.

b) Las secciones relevantes deberían delinear la política.

c) Las secciones relevantes deberían delinear los procesos del esquema y la infraestructura relacionada.

d) Las secciones relevantes deberían delinear los requisitos para detectar, reportar, evaluar y administrar eventos, incidentes y vulnerabilidades de seguridad de la información.

e) Las secciones relevantes deberían indicar claramente quiénes son las personas responsables de autorizar y / o llevar a cabo ciertas acciones cruciales dentro del personal (por ejemplo, sacar de la línea un sistema de información o incluso cerrarlo).

Las políticas deberían incluir el requisito de establecer mecanismos de revisión apropiados. Estos mecanismos tienen que asegurar que la información de la detección, monitoreo y resolución de incidentes de seguridad de la información y del tratamiento de las vulnerabilidades de seguridad de la información reportadas se utilice como insumo para asegurar la eficacia continua de las políticas corporativas de seguridad de la información y gestión del riesgo y de las políticas de seguridad de la información de sistemas, servicios o redes específicos.

5.4 Esquema de gestión de incidentes de seguridad de la información

5.4.1 Introducción

El objetivo de un esquema de gestión de incidentes de seguridad de la información es proporcionar documentación detallada que describa las actividades y procedimientos para tratar los eventos e incidentes de seguridad de la información y la comunicación de dichos eventos, incidentes y vulnerabilidades. El esquema de gestión de incidentes de seguridad de la información entra en efecto siempre que se detecte un evento de seguridad de la información o se reporte una vulnerabilidad de seguridad de la información. Cada organización debería utilizar el esquema como una guía para:

a) responder a eventos de seguridad de la información,

b) determinar si los eventos de seguridad de la información se convierten en incidentes de seguridad de la información,

c) administrar los incidentes de seguridad de la información hasta una conclusión,

d) responder a las vulnerabilidades de seguridad de la información,

e) identificar las lecciones aprendidas y cualquier mejora al esquema y / o a la seguridad en general que se requiera, y

f) realizar las mejoras identificadas.

5.4.2 Partes involucradas

Una organización debe asegurar que el esquema de gestión de incidentes de seguridad de la información sea compartido con todo el personal y contratistas asociados, proveedores de servicios de TIC, proveedores de telecomunicaciones y compañías tercerizadas, cubriendo así las siguientes responsabilidades:

a) detectar y reportar eventos de seguridad de la información (esto es responsabilidad de cualquier miembro del personal permanente o contratado en una organización y sus compañías),

b) evaluar y responder a eventos e incidentes de seguridad de la información, involucrándose en las actividades de aprendizaje luego de que el incidente se resuelva y mejorando la seguridad de la información así como el esquema mismo de gestión de incidentes de seguridad de la información (esto es responsabilidad de los miembros del punto de contacto (PdC), el ERISI, la gerencia, el personal de relaciones públicas y los representantes legales), y

c) reportar las vulnerabilidades de seguridad de la información (esto es responsabilidad de cualquier miembro del personal permanente o contratado en una organización y sus compañías), y ocuparse de ellas.

El esquema debería tomar en cuenta cualquier usuario tercero y los incidentes y vulnerabilidades asociados de seguridad de la información reportados desde organizaciones tercerizadas y la información sobre incidentes y vulnerabilidades de seguridad de la información gubernamental y comercial así como las de organizaciones proveedoras.

5.4.3 Contenido

Cada organización debería asegurar que el contenido de la documentación del esquema de gestión de incidentes de seguridad de la información incluya lo siguiente:

a) Una revisión de la política de la gestión de incidentes de seguridad de la información.

b) Una revisión de todo el esquema de gestión de incidentes de seguridad de la información.

c) Las actividades, procedimientos e información detallados asociados con lo siguiente:

1) Planeamiento y preparación

i) Un enfoque estandarizado respecto de la categorización y clasificación de eventos / incidentes de seguridad de la información para permitir proveer resultaos consistentes. En cualquier caso, la decisión debe basarse en los impactos reales o proyectados sobre las operaciones de negocios de la organización y la guía que se les asocia.

NOTA: El Anexo C muestra como ejemplo un enfoque de la categorización y clasificación de eventos e incidentes de seguridad de la información.

ii) Una estructura de base de datos de eventos / incidentes / vulnerabilidad de seguridad de la información estándar, que probablemente provee la capacidad de comparar resultados, mejora la información de alertas y permite una visión más exacta de las amenazas a los sistemas de información y sus vulnerabilidades.

iii) Una guía para determinar si se requiere llevar el asunto a un nivel superior durante cada proceso relevante y a quién y los procedimientos asociados. En base a la guía proporcionada en la documentación del esquema de gestión de incidentes de seguridad de la información, cualquiera que evalúe un evento, incidente o vulnerabilidad de seguridad de la información debería conocer en qué circunstancias es necesario llevar los asuntos a un nivel superior y a quién se los debería llevar. Además, existen circunstancias imprevistas de cuándo esto puede ser necesario. Por ejemplo, un incidente menor de seguridad de la información podría evolucionar hacia una situación importante o de crisis si no se maneja apropiadamente o un incidente menor de seguridad de la información al que no se hace seguimiento en una semana podría convertirse en un incidente de seguridad de la información mayor. La guía debería definir tipos de eventos e incidentes de seguridad de la información, tipos de escalamiento y quién debe instituir el escalamiento.

iv) Procedimientos a seguirse para asegurar que todas las actividades de gestión de incidentes de seguridad de la información se registran adecuadamente en el formulario apropiado y que personal designado conduce un análisis del registro.

v) Procedimientos y mecanismos para asegurar que el régimen de control de cambios se mantiene cubriendo el rastreo de eventos, incidentes y vulnerabilidades de seguridad de la información así como las actualizaciones de los reportes de eventos / incidentes / vulnerabilidades de seguridad de la información y las actualizaciones del esquema mismo.

vi) Procedimientos para el análisis forense de seguridad de la información.

vii) Procedimientos y guía sobre cómo utilizar Sistemas de Detección de Intrusiones (SDI), asegurando que se ha resuelto los aspectos legales y regulatorios. La guía debe incluir una discusión de las ventajas y desventajas de realizar actividades de vigilancia de atacantes. En ISO/IEC 18043:2006 se proporciona mayor información sobre el SDI.

viii) Guía y procedimientos asociados con los mecanismos técnicos y organizativos que se establecen, implementan y operan para prevenir ocurrencias de incidentes de seguridad de la información y para reducir la posibilidad de ocurrencias de incidentes de seguridad de la información así como para ocuparse de los incidentes de seguridad de la información que ocurrieron.

ix) Material para el programa de capacitación y concientización sobre la gestión de eventos, incidentes y vulnerabilidades de seguridad de la información.

x) Procedimientos y especificaciones para hacer pruebas al esquema de gestión de incidentes de seguridad de la información.

xi) El esquema del organigrama para la gestión de incidentes de seguridad de la información.

xii) Los términos de referencia y responsabilidades del ERISI en su conjunto y de miembros individuales.

xiii) Información de contacto importante.

2) Detección y reporte

i) Detectar y reportar la ocurrencia de eventos de seguridad de la información (por medios humanos o automáticos).

ii) Recolectar la información sobre eventos de seguridad de la información.

iii) Detectar y reportar vulnerabilidades de seguridad de la información.

iv) Registrar por completo toda la información recolectada en la base de datos de gestión de incidentes de seguridad de la información.

3) Evaluación y decisión

i) El PdC que dirige evaluaciones de eventos de seguridad de la información (incluyendo el escalamientos según se requiera), utilizando la escala de clasificación de incidentes / eventos de seguridad de la información acordada (incluyendo la determinación de los impactos de eventos basados en los activos / servicios afectados) y decidiendo si los eventos deben clasificarse como incidentes de seguridad de la información.

ii) El ERISI que evalúa los eventos de seguridad de la información debería confirmar si un evento es un incidente de seguridad de la información o no y luego se debería conducir otra evaluación utilizando la escala de clasificación de eventos / incidentes de seguridad de la información para confirmar los detalles del tipo de evento (potencial de incidente) y recurso afectado (categorización). Esto debería estar seguido por las decisiones realizadas sobre cómo debe tratarse el incidente de seguridad de la información confirmado, quién debe tratarlo, con qué prioridad, así como los niveles de escalamiento.

iii) Evaluación de vulnerabilidades de seguridad de la información (que todavía no han sido explotadas para causar eventos de seguridad de la información e incidentes potenciales de seguridad de la información), con las decisiones tomadas en base a las que necesitan ser tratadas, por quién, cómo y en qué prioridad.

iv) Registro completo de todos los resultados de evaluación y decisiones relacionadas en la base de datos de incidentes de seguridad de la información.

4) Respuestas

i) Revisión por parte del ERISI para determinar si el incidente de seguridad de la información está bajo control y

- Si el incidente está bajo control, promover la respuesta requerida, ya sea inmediatamente (en tiempo real o en tiempo casi real) o en un momento posterior,

- Si el incidente no está bajo control o si va a tener un impacto severo sobre los servicios medulares de las

organizaciones, promover actividades de crisis a través del escalamiento a una función de manejo de crisis.

ii) Definición de un mapa de todas las funciones y organizaciones internas y externas que deberían estar involucradas durante la gestión de un incidente.

iii) Conducción de análisis forenses de seguridad de la información, según se requiera.

iv) Escalamiento, según se requiera.

v) Aseguramiento de que todas las actividades involucradas se registren adecuadamente para un análisis posterior.

vi) Aseguramiento de que se recoge evidencia electrónica y se la almacena de manera comprobadamente segura.

vii) Aseguramiento de que el régimen de control de cambios se mantenga y de este modo se mantenga actualizada la base de datos de eventos / incidentes / vulnerabilidades de seguridad de la información.

viii) Comunicación de que existe un incidente de seguridad de la información o cualquier detalle relevante del mismo a otras personas u organizaciones internas y externas.

ix) Tratamiento de las vulnerabilidades de seguridad de la información.

x) Una vez que el incidente se ha tratado exitosamente, cerrarlo formalmente y registrar esto en la base de datos de gestión de incidentes de seguridad de la información.

Cada organización debería asegurar que la documentación del esquema de gestión de incidentes de seguridad de la información permita respuestas a los incidentes de seguridad de la información, tanto de manera inmediata como a un plazo más largo. Todos los incidentes de seguridad de la información deberían pasar por una evaluación temprana de los impactos potenciales adversos a las operaciones del negocio tanto en el corto como en el largo plazo (por ejemplo, podría ocurrir un desastre importante algún tiempo después de un incidente inicial de seguridad de la información). Además, esto debería permitir algunas respuestas necesarias a incidentes de seguridad de la información que son completamente

imprevistos, en donde se requieren controles ad hoc. Incluso para esta situación, las organizaciones deberían incluir lineamientos generales en la documentación del esquema sobre los pasos que pueden ser necesarios.

5) Lecciones Aprendidas

i) Conducir análisis forenses de seguridad de la información adicionales, según se requiera.

ii) Identificar las lecciones aprendidas a partir de los incidentes y vulnerabilidades de seguridad de la información.

iii) Revisar, identificar y hacer mejoras a la implementación del control de seguridad de la información (controles nuevos y / o actualizados), así como a la política de gestión de incidentes de seguridad de la información como resultado de las lecciones aprendidas.

iv) Revisar, identificar y, si es posible, hacer mejoras a la evaluación existente de riesgos de seguridad de la información y a los resultados de la revisión de la gestión de la organización, como un producto de las lecciones aprendidas.

v) Revisar cuán eficaces han sido los procesos, procedimientos, formatos de reporte y / u organigramas para responder a la evaluación y recuperación de cada incidente de seguridad de la información y para ocuparse de las vulnerabilidades de seguridad de la información, y, sobre la base de las lecciones aprendidas, identificar y hacer mejoras al esquema de gestión de incidentes de seguridad de la información y a su documentación.

vi) Actualizar la base de datos de eventos / incidentes / vulnerabilidades de seguridad de la información

vii) Comunicar y compartir los resultados de la revisión dentro de una comunidad de confianza (si así lo desea la organización)

5.4.4 Procedimientos

Antes de poder comenzar la operación del esquema de gestión de incidentes de seguridad de la información, es importante que una organización haya documentado y verificado que

se dispone de procedimientos. Dichos procedimientos deben indicar aquellos grupos o individuos responsables de su uso y manejo según sea apropiado a partir del PdC y / o ERISI. Dichos procedimientos deberían asegurar que se reúna y almacene de manera segura la evidencia electrónica y de que se monitoree continuamente su preservación segura, en caso se requiera para un proceso legal o una acción disciplinaria interna. Más aún, debería haber procedimientos documentados que cubran no solamente las actividades del PdC y del ERISI, sino de aquellos involucrados en el análisis forense de seguridad de la información y en las actividades de crisis - si esto no estuviera cubierto en algún otro lugar, por ejemplo, en un plan de continuidad del negocio o en un plan de gestión de crisis. Los procedimientos documentados deberían estar enteramente en línea con la política documentada de gestión de incidentes de seguridad de la información y otra documentación del esquema de gestión de incidentes de seguridad de la información.

Es importante comprender que no todos los procedimientos tienen que estar disponibles públicamente, por ejemplo, no es necesario que todo el personal de la organización comprenda la operación interna de un ERISI para interactuar con él. El ERISI debería asegurar que la guía disponible públicamente, incluyendo la información resultante del análisis de gestión de incidentes de seguridad de la información esté en un formato disponible inmediatamente, por ejemplo, en la intranet de la organización. También es importante mantener algunos detalles del esquema de gestión de incidentes de seguridad de la información bien resguardados para evitar que un miembro interno perturbe el proceso de investigación. Por ejemplo, si un empleado de banco que está malversando fondos es consciente de algunos detalles del esquema, él o ella puede ser capaz de esconder mejor sus actividades a los investigadores o de impedir de una u otra manera la detección, investigación y recuperación de un incidente de seguridad de la información.

El contenido de los procedimientos operativos depende de una serie de criterios especialmente relacionados con la naturaleza de los eventos, incidentes y vulnerabilidades conocidos y potenciales de seguridad de la información y los tipos de activos de sistemas de información que podrían estar involucrados, así como su entorno. De este modo, se puede relacionar un procedimiento operativo a un tipo particular de incidente o producto (firewalls, bases de datos, sistemas operativos, aplicaciones) o a un producto específico. Cada procedimiento operativo debería identificar claramente los pasos a seguir y quién debe llevarlos a cabo. Debería reflejar experiencia de fuentes externas (por ejemplo, ERISIS gubernamentales o comerciales o similares, y proveedores) e internas.

Debería haber procedimientos operativos para ocuparse de los tipos de eventos e incidentes de seguridad de la información que ya se conocen, así como las vulnerabilidades. Debería haber procedimientos operativos a seguirse cuando un evento, incidente o vulnerabilidad

de seguridad de la información que se ha identificado no es de ningún tipo conocido. En este caso, se debería resolver lo siguiente:

a) el proceso de reporte para manejar dichas excepciones,

b) guía sobre la oportunidad de recibir aprobación de la gerencia para evitar cualquier demora en la respuesta, y

c) delegación pre-autorizada de toma de decisiones sin el proceso normal de aprobación.

5.4.5 Confianza

El ERISI desempeña un papel crucial para la seguridad de la información general de una organización. El ERISI requiere la colaboración de todo el personal de la organización para detectar, resolver e investigar los incidentes de seguridad de la información. Es fundamental que el ERISI tenga la confianza de todos tanto internamente como externamente. La adopción de la anonimidad con respecto a reportar vulnerabilidades, eventos e incidentes de seguridad de la información puede ser útil para construir la confianza.

Una organización debería asegurar que su esquema de gestión de incidentes de seguridad de la información se ocupe de situaciones donde es importante asegurar la anonimidad de la persona o la parte que reporta los incidentes o vulnerabilidades potenciales de seguridad de la información en ciertas circunstancias específicas. Cada organización debería tener disposiciones que ilustren claramente la expectativa de anonimidad, o carencia de la misma, para las personas o partes que reportan un incidente o vulnerabilidad potencial de seguridad de la información. El ERISI puede requerir obtener información adicional no transmitida inicialmente por la persona o parte que reporta el incidente. Además, la persona que detecta primero el incidente o vulnerabilidad mismos puede derivar información importante acerca del incidente o vulnerabilidad de seguridad de la información.

Otro enfoque que ERISI puede adoptar es conquistar la confianza de los usuarios a través de la transparencia y de procesos más maduros. El ERISI debería trabajar para educar a los usuarios, explicar cómo funciona el ERISI, cómo protege la confidencialidad de la información recolectada y cómo maneja los reportes de eventos, incidentes y vulnerabilidades por parte de los usuarios.

El ERISI debería ser capaz de satisfacer eficientemente las necesidades funcionales, financieras, legales y políticas de la organización y ser capaz de ejercer la discreción operativa cuando maneja incidentes y vulnerabilidades de seguridad de la información. La función del ERISI también debería estar auditada independientemente para confirmar que todos los requisitos de negocio se cumplan eficazmente.

Además, una buena manera de lograr otro aspecto de la independencia es separar la cadena de reportes de incidentes y vulnerabilidades de la gestión de la línea operativa y hacer que un alto gerente sea directamente responsable de manejar las respuestas a incidentes y vulnerabilidades. También se debe segregar las finanzas de la capacidad para evitar influencia indebida.

5.4.6 Confidencialidad

Un esquema de gestión de incidentes de seguridad de la información puede contener información sensible y las personas involucradas en resolver los incidentes y vulnerabilidades pueden tener que manejar información sensible. Una organización debería asegurar que se establezca los procesos necesarios para anonimizar la información sensible y exigir que el personal que tiene acceso a información sensible firme contratos de confidencialidad. Si se registra los eventos / incidentes / vulnerabilidades de seguridad de la información por medio de un sistema generalizado de gestión de problemas, quizás se tenga que omitir detalles sensibles. Adicionalmente, una organización debería asegurar que el esquema de gestión de incidentes de seguridad de la información haga provisiones para controlar la comunicación de incidentes y vulnerabilidades a terceros externos, incluyendo los medios de comunicación masiva, los socios del negocio, los clientes, las organizaciones de aplicación de la ley y el público en general.

5.5 Establecimiento del ERISI

5.5.1 Introducción

El objetivo de establecer el ERISI es proveer a la organización de una capacidad apropiada para evaluar, responder a y aprender de los incidentes de seguridad de la información y proveer la coordinación, gestión, retroalimentación y comunicación necesarias. Un ERISI contribuye a la reducción del daño físico y monetario, así como a la reducción del daño a la reputación de la organización que a veces se asocia con los incidentes de seguridad de la información.

5.5.2 Miembros y estructura

El tamaño, la estructura y la composición de un ERISI deberían ser apropiados para el tamaño, la estructura y la naturaleza del negocio de la organización. Aunque el ERISI puede constituir un equipo o departamento aislado, los miembros pueden compartir otros deberes que alientan a que los miembros de muchas áreas dentro de la organización proporcionen insumos. Una organización debería evaluar si requiere un equipo dedicado, un equipo virtual o una combinación de ambos. El número de incidentes y las actividades realizadas por el ERISI deberían guiar a la organización en esta elección.

El ERISI atraviesa distintas etapas de madurez y a menudo se adoptan ajustes al modelo organizativo en base al escenario específico que la organización enfrenta. Siempre que se justifique, se recomienda tener un quipo permanente liderado por un alto gerente. Los equipos virtuales de ERISI pueden estar liderados por un alto gerente. El alto gerente debería ser apoyado por individuos que se especializan en temas particulares, por ejemplo, en manejar ataques de código malicioso, a los que se llama dependiendo del tipo del incidente de seguridad de la información en cuestión. Dependiendo del tamaño, estructura y naturaleza del negocio de una organización, un miembro también puede desempeñar más de un papel dentro del ERISI. El ERISI puede comprender individuos de diferentes partes de la organización (por ejemplo, operaciones de negocios, TIC, auditoría, recursos humanos y marketing). Esto también se aplica a los ERISI permanentes, incluso en el caso de personal dedicado, el ERISI siempre requiere apoyo de otros departamentos.

Los miembros del equipo deberían estar accesibles para el contacto de tal manera que los nombres y los detalles de contacto de cada miembro y de sus miembros de respaldo estén disponibles dentro de la organización. Se debe indicar claramente los detalles necesarios en la documentación del esquema de gestión de incidentes de seguridad de la información, incluyendo cualquier documento de procedimiento y los formularios de reporte, pero no en las declaraciones de política.

El gerente del ERISI debería normalmente tener una línea de reporte separada de la alta gerencia, separada de las operaciones normales del negocio. Él / ella deberían tener autoridad delegada para tomar decisiones inmediatas sobre cómo tratar un incidente y debería asegurar que todos los miembros del ERISI tengan los niveles de conocimiento y habilidades requeridos y que éstos continúen manteniéndose. El gerente del ERISI debería asignar la investigación de cada incidente al miembro más apropiado de su equipo y cada incidente debería estar asignado a un gerente con nombre propio.

5.5.3 Relación con otras partes de la organización

El ERISI debería tener la responsabilidad de asegurar que se resuelvan los incidentes y en este contexto el gerente del ERISI y los miembros de su equipo deberían tener un grado de autoridad como para tomar las acciones necesarias que se consideren apropiadas para responder a los incidentes de seguridad de la información. Sin embargo, se debería acordar con la alta gerencia las acciones que pueden tener efectos adversos en toda la organización, ya sea financieramente o en términos de reputación. Por esta razón, es esencial que la política y el esquema de gestión de incidentes de seguridad de la información detalle a qué autoridad apropiada reporta el gerente del ERISI los incidentes serios de seguridad de la información.

Se debe acordar con la alta gerencia y documentar los procedimientos y responsabilidades para tratar con los medios de comunicación masiva. Estos procedimientos deben especificar quién se ocupa en la organización de las consultas de los medios y cómo esa parte de la organización interactúa con el ERISI.

5.5.4 Relaciones con partes interesadas externas

Las organizaciones deberían establecer relaciones entre ERISI y las partes interesadas externas apropiadas. Las partes interesadas externas pueden incluir los siguientes:

a) personal de apoyo externo contratado,

b) ERISI de organizaciones externas,

c) proveedores de servicios administrados, incluyendo proveedores de servicios de telecomunicaciones, ISP y proveedores,

d) organizaciones de aplicación de la ley,

e) autoridades de emergencia,

f) organizaciones del gobierno apropiadas,

g) personal legal,

h) funcionarios de relaciones públicas y / o miembros de los medios de comunicación,

i) socios de negocios,

j) clientes, y

k) público en general.

5.6 Apoyo técnico y de otro tipo (incluyendo apoyo operativo)

Para asegurar que se pueda lograr dar respuestas rápidas y eficaces a los incidentes de seguridad de la información, una organización debe adquirir, preparar y probar todos los medios necesarios de apoyo técnico y de otro tipo. Esto incluye lo siguiente:

a) acceso a los detalles de los activos de la organización con un registro e información actualizados sobre sus vínculos con las funciones del negocio,

b) acceso a los procedimientos y documentos relacionados al manejo de crisis,

c) procesos de comunicación documentados y promulgados,

d) el uso de una base de datos de eventos / incidentes / vulnerabilidades de seguridad de la información y los medios técnicos para poblar y actualizar rápidamente la base de datos, analizar su información y facilitar respuestas (en algunas instancias una organización puede requerir registros manuales), manteniendo segura la base de datos de manera comprobable,

e) facilidades para la recolección y análisis de evidencia forense sobre seguridad de la información, y

f) arreglos adecuados para la gestión de crisis en la base de datos de eventos / incidentes / vulnerabilidades de seguridad de la información (para consultar una guía sobre gestión de la continuidad del negocio, véase ISO / IEC 27031).

Una organización debe asegurar que los medios técnicos utilizados para poblar y actualizar rápidamente la base de datos, analizar su información y facilitar respuestas a los incidentes de seguridad de la información apoyen lo siguiente:

g) adquisición rápida de reporte de eventos / incidentes / vulnerabilidades de seguridad de la información,

h) notificación al personal previamente seleccionado por medios apropiados (por ejemplo, correo electrónico, fax o teléfono) requiriendo de este modo el

mantenimiento de una base de datos de contacto confiable e inmediatamente accesible (incluyendo el papel y otros medios de respaldo), y la facilidad de transmitir información a individuos de una manera segura cuando sea apropiado,

i) tomar precauciones que correspondan a los riesgos evaluados para asegurar que la comunicación electrónica, ya sea por Internet o no, no pueda observarse sin autorización y siga estando disponible mientras que el sistema, servicio y / o red esté bajo ataque (esto puede requerir mecanismos de comunicación alternativos pre-planificados),

j) asegurar la recolección de todos los datos sobre el sistema, servicio y / o red de información, y todos los datos procesados,

k) usar control de integridad criptográfica para ayudar a determinar si se ha cambiado algunas partes del sistema, servicio y / o red y cuáles, si corresponde, son los riesgos evaluados,

l) facilitar el archivamiento y aseguramiento de información recolectada (por ejemplo, aplicando firmas digitales a los registros y otra evidencia antes del almacenamiento fuera de línea en medios sólo de lectura como CD o DVD ROM),

m) habilitar la preparación de impresiones (por ejemplo, de registros), incluyendo los que muestran el progreso de un incidente y el proceso de resolución y cadena de custodia,

n) recuperación del sistema, servicio y / o red de información a la operación normal, con los siguientes procedimientos que están en línea con el manejo relevante de la crisis:

1) pruebas de respaldo,

2) control de código malicioso,

3) medios originales con software de sistema y de aplicación,

4) medios ejecutables, y

5) parches de sistemas y aplicaciones limpios, confiables y actualizados.

Cada vez es más común que las organizaciones creen una imagen de línea de base estándar de los medios de instalación y utilicen esa imagen como la

base limpia para crear sistemas. Utilizar una imagen así en vez de los medios originales a veces es preferible porque la imagen ya se ha parchado, fortalecido, probado, etc.

Un sistema, servicio o red de información atacados pueden no funcionar correctamente. Así, en la medida en que sea posible, ningún medio técnico (software y hardware) necesario para responder a un incidente de seguridad de la información debería basarse en sus operaciones en los sistemas, servicios y / o redes 'regulares' de la organización, de manera proporcional a los riesgos evaluados. Se debe seleccionar cuidadosamente todos los medios técnicos, implementados y comprobados regularmente de manera correcta (incluyendo pruebas a los respaldos realizados). Si es posible, los medios técnicos deben ser plenamente independientes.

NOTA: Los medios técnicos descritos en este apartado no incluyen medios técnicos utilizados para detectar incidentes e intrusiones de seguridad de la información directamente y para notificar automáticamente a las personas apropiadas. Dichos medios técnicos se describen en ISO / IEC 18043.

A la vez que el PdC de la organización tiene un papel permanente mucho más amplio en la organización para proporcionar apoyo a todos los aspectos de TI y manipulación de la información relacionada, tiene un papel clave que desempeñar en la gestión de incidentes de seguridad de la información. Cuando se reporta por primera vez los eventos de seguridad de la información, el PdC se ocupa de ellos en la fase de detección y reporte. El PdC debe revisar la información reunida y hacer la evaluación inicial respecto de si los eventos deberían clasificarse como incidentes o no. Si el evento no se clasifica como un incidente, el PdC debe tratarlo de acuerdo con esto. Si un evento se clasifica como un incidente el PdC mismo puede ocuparse de él, aunque se espera que en la mayoría de los casos la responsabilidad de tratar el incidente tenga que ser entregada al ERISI. No se espera que el personal del PdC sea experto en seguridad.

5.7 Concientización y capacitación

La gestión de incidentes de seguridad de la información es un proceso que involucra no sólo medios técnicos sino también personas. De este modo, debe estar apoyada por individuos apropiadamente conscientes de la seguridad de la información y capacitados en la misma dentro de la organización.

La consciencia y participación de todo el personal de la organización es crucial para el éxito de un enfoque estructurado de gestión de incidentes de seguridad de la información.

Mientras que se debe exigir a los usuarios que participen, probablemente no participarán tan eficazmente en esta operación si no son conscientes de cómo ellos y su departamento pueden beneficiarse de participar en un enfoque estructurado de la gestión de incidentes de seguridad de la información. Además, la eficiencia operativa y la calidad de un enfoque estructurado de la gestión de incidentes de seguridad de la información se basan en una serie de factores, incluyendo la obligación de notificar incidentes, la calidad de la notificación, la facilidad de la utilización, la velocidad y la capacitación. Algunos de estos factores se relacionan a asegurarse de que los usuarios sean conscientes del valor de la gestión de incidentes de seguridad de la información y estén motivados a reportar incidentes.

La organización debería asegurar que el papel de la gestión de incidentes de seguridad de la información se promueva activamente como parte del programa corporativo de concientización y capacitación sobre seguridad de la información. El programa de concientización y el material relacionado al mismo deben estar disponibles a todo el personal, incluyendo los nuevos empleados, los usuarios de terceros y los contratistas, según sea relevante. Debería haber un programa de capacitación específico para el PdC, para los miembros del ERISI, para el personal de seguridad de la información y los administradores específicos, según sea necesario. Cada grupo de personas directamente involucradas con la gestión de incidentes puede requerir diferentes niveles de capacitación, dependiendo del tipo, frecuencia y carácter crítico de la interacción con el esquema de gestión de incidentes de seguridad de la información.

Las explicaciones sobre concientización de la organización deben abarcar lo siguiente:

a) beneficios a ser derivados del enfoque estructurado de la de gestión de incidentes de seguridad de la información, tanto para la organización como para su personal,

b) cómo funciona el esquema de gestión de incidentes de seguridad de la información, incluyendo su alcance y el flujo de trabajo de gestión de eventos, incidentes y vulnerabilidades de seguridad,

c) cómo reportar sobre eventos, incidentes y vulnerabilidades de información

d) información retenida del incidente y resultados de la base de datos de eventos / incidentes / vulnerabilidades de seguridad de la información,

e) controles sobre la confidencialidad de las fuentes según sea relevante,

f) acuerdos sobre el nivel de servicios del esquema,

g) notificación de resultados-en qué circunstancias se avisa a las fuentes,

h) cualquier restricción impuesta por acuerdos de confidencialidad,

i) la autoridad de la organización de gestión de incidentes de seguridad de la información y su línea de reporte, y

j) quién recibe informes del esquema de gestión de incidentes de seguridad de la información y cómo se distribuyen los informes.

En algunos casos, puede ser deseable que la organización incluya específicamente detalles sobre la consciencia de la gestión de incidentes de seguridad de la información en otros programas de capacitación (por ejemplo, programas de orientación al personal o programas de concientización general sobre seguridad corporativa). Este enfoque de la concientización puede proveer un contexto valioso relevante a grupos particulares de personas y mejora la eficacia y la eficiencia del programa de capacitación.

Antes de que el esquema de gestión de incidentes de seguridad de la información se convierta en operativo, la organización debería asegurar que todo el personal relevante esté familiarizado con los procedimientos involucrados con la detección y reporte de eventos de seguridad de la información y que haya personal seleccionado con mucho conocimiento respecto de las actividades subsiguientes. Esto debería ser seguido de explicaciones de concientización y cursos de capacitación regulares. La capacitación debería de ser apoyada por ejercicios específicos y pruebas el PdC y los miembros del ERISI, así como para el personal de seguridad de la información y para administradores específicos.

Además, los programas de concientización y capacitación deben complementarse por el establecimiento y operaciones de apoyo de línea dedicada del personal de gestión de incidentes de seguridad de la información, para minimizar las demoras en el reporte y manipulación de eventos, incidentes y vulnerabilidades de seguridad de la información.

5.8 Pruebas del esquema

La organización debe programar verificaciones y pruebas regulares de los procesos y procedimientos de gestión de incidentes de seguridad de la información para destacar las fallas y problemas potenciales que pueden surgir durante el manejo de eventos, incidentes

y vulnerabilidades de seguridad de la información. Se debería organizar pruebas periódicas para verificar procesos / procedimientos y para verificar cómo responde el ERISI a incidentes complejos y severos a través de la simulación de ataques, fallas o faltas realistas. Se debe prestar atención particular a la creación de escenarios simulados, los que deben basarse en nuevas amenazas reales a la seguridad de la información. Las pruebas deben involucrar no solamente al ERISI, sino también a todas las organizaciones internas y externas que participan en la gestión de incidentes de seguridad de la información. Las organizaciones deberían asegurar que cualquier cambio realizado como resultado de revisiones posteriores a las pruebas esté sujeto a una verificación exhaustiva, incluyendo más pruebas antes de aplicar el esquema cambiado.

6. FASE DE DETECCIÓN Y REPORTE

6.1 Revisión de las actividades clave

La primera fase del uso operacional de un esquema de gestión de incidentes de seguridad de la información incluye la detección de, recolección de información asociada con, y reporte sobre ocurrencias de eventos de seguridad de la información y existencia de vulnerabilidades de seguridad de la información por medios humanos o automáticos. La gestión de incidentes de seguridad de la información en la operación comprende tres fases principales: detección y reporte, evaluación y decisión (véase el apartado 7) y respuestas (véase el apartado 8). Estas fases están seguidas por la fase de lecciones aprendidas (véase el apartado 9) donde se identifica y realiza las mejoras. Estas fases y sus actividades asociadas se introdujeron en el apartado 4.5.

Los siguientes apartados tratan predominantemente sobre la manipulación de eventos e incidentes de seguridad de la información. La organización debe asegurar que el personal apropiado se ocupe de las vulnerabilidades reportadas de seguridad de la información de manera similar a la que se manipulan las faltas de seguridad no pertenecientes a la información, posiblemente con evaluación y resolución utilizando al personal técnico (que puede o ser miembro del ERISI). La información sobre vulnerabilidades y sus resoluciones debe ingresarse en la base de datos de eventos / incidentes / vulnerabilidades de seguridad de la información manejada por el ERISI. El Anexo D muestra una plantilla como ejemplo del formulario de reporte de vulnerabilidades de seguridad de la información.

La figura 3 muestra todas las fases operativas y actividades relacionadas:

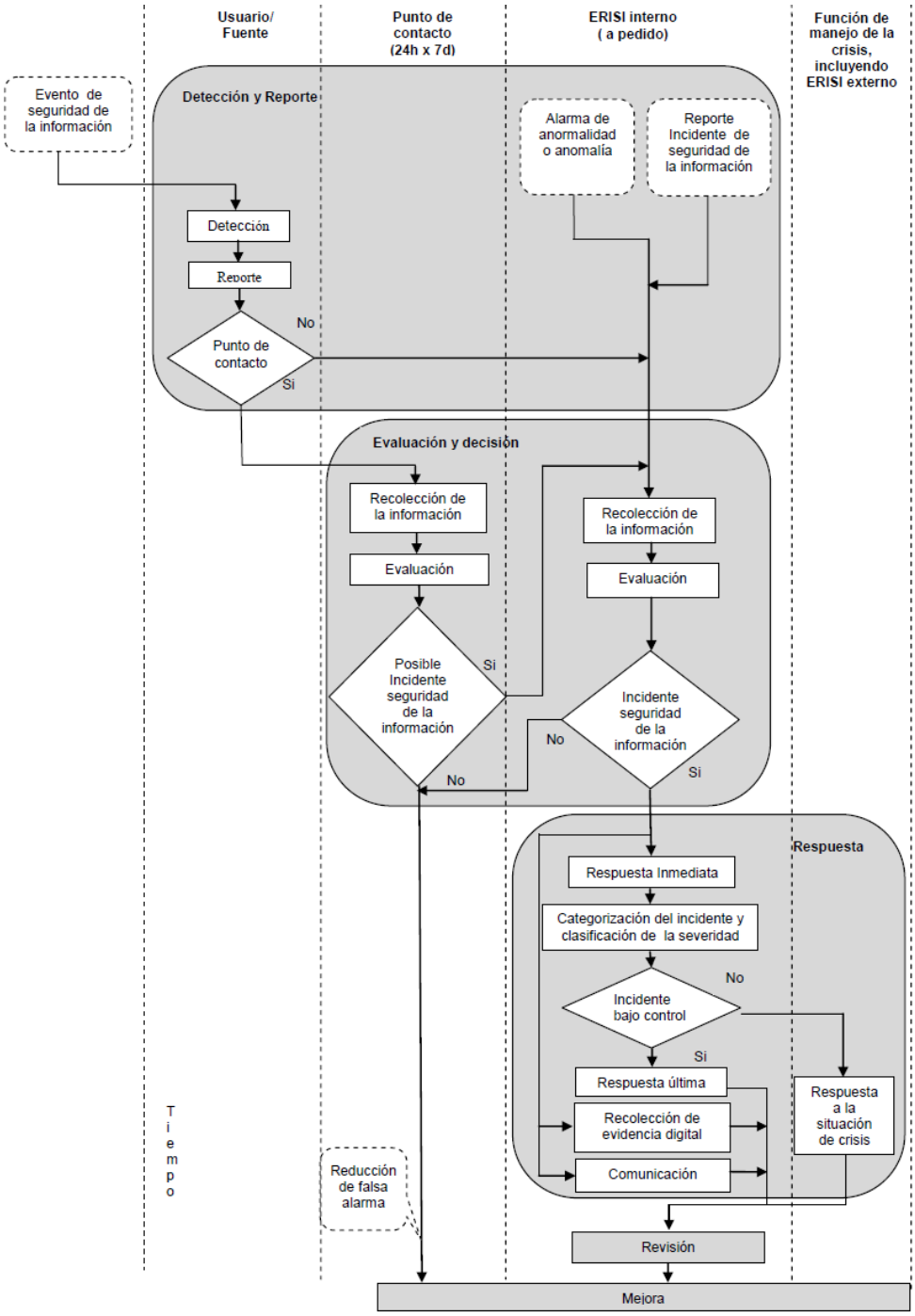

FIGURA 3 – Diagrama de flujo de eventos e incidentes de seguridad de la información

NOTA: La falsa alarma es una indicación de un evento no deseado, pero se descubre que no es real ni tiene consecuencias.

La primera fase del uso operativo de un esquema de gestión de incidentes de seguridad de la información incluye la detección de, recolección de información asociada con y reporte sobre ocurrencias de eventos de seguridad de la información por medios humanos o automáticos. La organización debe asegurar que esta fase incluye la detección de vulnerabilidades de seguridad de la información que todavía no se han explotado causando eventos de seguridad de la información y posiblemente incidentes de seguridad de la información, y el reporte sobre los mismos.

Para la fase de detección y reporte, una organización debe asegurar que las siguientes sean actividades clave:

a) Actividad para 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 por uno de los miembros del personal / clientes de la organización o automáticamente, asistidos por los siguientes:

1) alertas de los sistemas de monitoreo de seguridad como IDS / IDP, programa antivirus, “honeypots” [tarros de miel] (término genérico para un sistema de señuelo utilizado para engañar, distraer, desviar y alentar al atacante a pasar tiempo en información que parece muy valiosa pero que en realidad está fabricada y que no sería de interés a un usuario legítimo[ISO/IEC 18043:2006]) /“tarpits” [pozos de brea] (sistemas que se exponen y diseñan intencionalmente para demorar los ataques), sistemas de monitoreo de registros, sistemas de gestión de seguridad de la información, motores de correlación y otros,

2) alertas de sistemas de monitoreo de la red tales como firewalls, análisis de flujos de red, filtrado de web y otros,

3) análisis de información del registro desde dispositivos, servicios, sistemas anfitriones y otros diversos sistemas,

4) escalamiento de eventos anómalos detectados por TIC,

5) escalamiento de eventos anómalos detectados por escritorios de ayuda,

6) reportes de usuarios, y

7) notificaciones externas provenientes de terceros como otros ERISI, servicios de seguridad de la información, proveedores de servicios de Internet, proveedores de servicios de telecomunicación, compañías tercerizadas o ERISI nacionales.

b) Actividad para recolectar información sobre un evento o vulnerabilidad de seguridad de la información.

c) Actividad para asegurar que todos los involucrados en el PdC registren apropiadamente todas las actividades, resultados y decisiones relacionadas para análisis posterior.

d) Actividad para asegurar que se reúne evidencia electrónica y se la almacena de manera segura, y que su preservación segura se monitorea frecuentemente, en caso esto se requiera para un proceso legal o una acción disciplinaria interna.

NOTA: Una Norma Internacional futura (ISO/IEC 27037) proveerá información más detallada sobre la identificación, recolección, adquisición y preservación de evidencia digital.

e) Actividad para asegurar que el régimen de control de cambios se mantiene cubriendo el rastreo de eventos y vulnerabilidades de seguridad de la información y las actualizaciones de los reportes sobre eventos y vulnerabilidades y que, de esta manera, la base de datos de eventos / incidentes / vulnerabilidades de seguridad de la información se mantiene al día.

f) Actividad para llevar a un nivel superior, según se requiera durante la fase, para una revisión y / o decisiones posteriores.

g) Actividad para registrar un Sistema de Rastreo de Incidentes.

Toda la información recolectada perteneciente a un evento o vulnerabilidad de seguridad de la información debe almacenarse en la base de datos de eventos / incidentes / vulnerabilidades de seguridad de la información que maneja el ERISI. La información reportada durante cada actividad debe ser tan completa como sea posible en el momento para asegurar que haya una buena base disponible para las evaluaciones y las decisiones que se deben tomar, y por supuesto de las acciones tomadas.

6.2 Detección del evento

Los eventos de seguridad de la información pueden ser detectados directamente por una persona o grupo de personas que noten algo que cause preocupación, ya sea relacionado

con aspectos, físicos o de procedimiento. La detección puede ser, por ejemplo, por alarmas de los detectores de fuego / humo o de intrusos (ladrones), y las alertas se notifican en lugares designados de antemano para la acción humana. Los eventos de seguridad de la información técnica pueden detectarse por medios automáticos, por ejemplo, alertas de las instalaciones de análisis del rastro de auditorías, firewalls, sistemas de detección de intrusiones, y herramientas contra código (incluyendo virus), en cada caso estimulados por parámetros pre-establecidos.

Las posibles fuentes de detección de eventos de seguridad de la información incluyen las siguientes:

a) usuarios,

b) gerentes de línea y gerentes de seguridad,

c) clientes,

d) departamento de TI, incluyendo Centro de Operaciones de la Red y Centro de Operaciones de Seguridad (hasta el segundo nivel de apoyo),

e) escritorio de ayuda de TI (hasta el nivel uno de apoyo),

f) proveedores de servicios administrados (incluyendo proveedores de servicios de Internet, proveedores de servicios de telecomunicaciones y otros proveedores),

g) ERISIs,

h) otras unidades y personal que puede detectar anomalías durante su trabajo cotidiano,

i) medios de comunicación masiva (periódicos, televisión, etc.), y

j) páginas web (páginas web públicas de información de seguridad, páginas web de investigadores de seguridad, archivos de desfiguración de páginas web, etc.).

6.3 Reporte de eventos

Cualquiera que fuera la fuente de la detección de un evento de seguridad de la información, la persona notificada por medios automáticos, o que nota directamente algo inusual, es responsable de iniciar el proceso de detección y reporte. Esta persona podría ser cualquier miembro del personal de una organización, ya sea personal permanente o contratado.

La persona debe seguir los procedimientos y utilizar el formulario de reporte de eventos de seguridad de la información especificado por el esquema de gestión de incidentes de seguridad de la información para hacer que el evento de seguridad de la información sea conocido por el PdC y la gerencia. De manera correspondiente, es esencial que todo el personal esté muy consciente de y tenga acceso a los lineamientos para reportar los distintos tipos de posibles eventos de seguridad de la información. Esto incluye el formato del formulario de reporte de eventos de seguridad de la información y detalles del personal que debe ser notificado en cada ocasión (todo el personal debería al menos ser consciente del formato del formulario de reporte de incidentes de seguridad de la información para ayudar a su comprensión del esquema). Debe notarse que no se consideran seguros los teléfonos fijos, inalámbricos y celulares sin una salvaguarda contra las intercepciones. Cuando se trata con información altamente confidencial o secreta, se debe tomar salvaguardas adicionales.

La información siguiente puede utilizarse como base para un formulario del sistema de rastreo de incidentes:

- Tiempo / fecha para la detección,
- Observaciones, e
- Información de contacto (opcional)

El formulario lleno y entregado (ya sea en papel o en un correo electrónico o un formulario de página web) debe ser utilizado por el personal del ERISI sólo cuando registran incidentes de seguridad de la información en el Sistema de Rastreo de Incidentes. Es más importante obtener conocimientos / informes de un evento de seguridad de la información del que se sospecha / el que se experimenta / el que se detecta que el tener toda la información completa.

Siempre que sea posible, una aplicación automatizada debe ser el soporte del rastreo de eventos (posiblemente incidentes) de seguridad de la información. El uso de un sistema de información es esencial para forzar al personal a seguir procedimientos y listas de verificación establecidos. También es algo extremadamente útil para ayudar a rastrear "quién hizo qué y cuándo", detalles que podrían olvidarse por error durante un evento de seguridad de la información (posiblemente incidente de seguridad de la información).

Cómo se maneja un evento de seguridad de la información depende de qué es y de las implicaciones y repercusiones que puedan derivarse del mismo. Para mucha gente, ésta será una decisión que está más allá de su competencia. De esta manera, la persona que reporta un evento de seguridad de la información debería llenar el formulario de reporte de eventos de seguridad de la información con tanto detalle y tanta información como le resulte inmediatamente disponible en el momento, enlazándose con su gerente local si es necesario. Ese formulario debe ser comunicado de manera segura al PdC designado, con una copia al responsable del ERISI. El PdC debe de preferencia proveer un servicio de 24 horas al día por 7 días de la semana. El Anexo D muestra una plantilla como ejemplo de formulario de reporte de eventos de seguridad de la información.
El ERISI debe nombrar a un miembro del equipo o a un delegado por turno para que sea responsable de todos los informes en trámites vía correo electrónico, teléfono, fax, formularios y conversación directa. Esta responsabilidad puede rotar entre los miembros del equipo semanalmente. El miembro del equipo nombrado realiza la evaluación y toma acciones apropiadas para informar a las partes responsables e involucradas así como para resolver el incidente de seguridad de la información.

Se enfatiza que no sólo es importante la exactitud sino también la oportunidad en el contenido que se llena en el formulario de reporte de eventos de seguridad de la información. No es una buena práctica demorar la entrega de un formulario de reporte para mejorar la exactitud de su contenido. Si la persona que reporta no está segura de los datos en cualquier campo del formulario de reporte, debe entregarlo con una anotación apropiada y las revisiones deben comunicarse posteriormente. También debe reconocerse que algunos mecanismos de reporte (por ejemplo, correo electrónico) son en sí mismos blancos visibles para el ataque.

Cuando existen problemas, o se considera que existen, con los mecanismos de reporte electrónico (por ejemplo, correo electrónico) se debe usar medios de comunicación alternativos. Esto incluye cuando se piensa que es posible que el sistema esté bajo ataque y que hay personas no autorizadas que podrían leer los formularios de reporte electrónico. Los medios alternativos podrían incluir: en persona, por teléfono o por mensajes de texto. Dichos medios alternativos deben usarse particularmente cuando es evidente al inicio de una investigación que un evento de seguridad de la información parece probablemente

clasificable como un incidente de seguridad de la información, particularmente uno que puede ser importante.

Aunque en muchos casos, un evento de seguridad de la información tiene que reportarse en adelante para que el PdC actúe, puede haber ocasiones donde un evento de seguridad de la información se maneje localmente, posiblemente con ayuda de la gerencia local. Es aconsejable que la gerencia local esté capacitada para hacer la misma evaluación que el ERISI y tomar contramedidas similares / iguales así como utilizar el mismo sistema de rastreo de incidentes, para utilizar con éxito los recursos localmente. Esto evitará que el ERISI haga doble trabajo.

Se puede determinar rápidamente que un evento de seguridad de la información es una falsa alarma, o puede resolverse hacia una conclusión satisfactoria. En dicho caso se debe llenar y enviar un formulario de reporte a la gerencia local, al PdC y al ERISI para propósitos de registro en la base de datos de eventos / incidentes / vulnerabilidades de seguridad de la información. En dicha circunstancia, la persona que reporta el cierre de un evento de seguridad de la información puede ser capaz de llenar parte de la información requerida para el formulario de reporte de incidentes de seguridad de la información. Si éste es el caso, entonces el formulario de reporte de incidentes de seguridad de la información también debe llenarse y enviarse. El uso de herramientas automáticas puede asistir con el llenado de algunos campos, por ejemplo, sellos de tiempos. También puede ayudar con compartir y transferir información necesaria.

7. FASE DE EVALUACIÓN Y DECISIONES

7.1 Revisión de las actividades clave

La segunda fase del uso operativo de un esquema de gestión de incidentes de seguridad de la información incluye la evaluación de información asociada con ocurrencias de eventos de seguridad de la información y la decisión sobre si se trata de un incidente de seguridad de la información. Para la fase de evaluación y toma de decisiones, una organización debe asegurar que las actividades clave son las siguientes:

a) Actividad para el PdC, quien conduce la evaluación para determinar si el evento es un incidente de seguridad de la información posible o que ha concluido o una falsa alarma, y si no es una falsa alarma, si se requiere escalamiento. Las

evaluaciones deben incluir el uso de la escala acordada de clasificación de eventos / incidentes de seguridad de la información (incluyendo la determinación de los impactos de eventos basados en los impactos de eventos respecto de los activos / servicios afectados) y debe decidir si los eventos deberían clasificarse como incidentes de seguridad de la información (véase Anexo C para obtener lineamientos como ejemplo). Mientras determinan los impactos de los eventos de seguridad de la información (y, de este modo, los posibles incidentes) en términos de los efectos de las rupturas de confidencialidad, integridad y disponibilidad, las organizaciones deben asegurar que se identifique lo siguiente:

1) dominio del impacto (físico o lógico),

2) activos, infraestructuras, información, procesos, servicios y aplicaciones afectadas o que vayan a ser afectadas, y

3) posibles efectos en los servicios medulares de la organización.

b) Actividad que realiza el ERISI para conducir la evaluación que confirme los resultados de la evaluación del PdC respecto a si el evento es un incidente de seguridad de la información o no, si se aplica. Según sea necesario, se debe conducir otra evaluación utilizando la escala acordada de clasificación de eventos / incidentes de seguridad de la información, con detalles del tipo de eventos (posiblemente incidentes) y del recurso afectado (categorización) (véase el Anexo C para lineamientos como ejemplo). Esto debe ser seguido de decisiones sobre cómo debe tratarse el incidente confirmado de seguridad de la información, quién debe tratarlo y con qué prioridad. Debe involucrar el proceso predeterminado de priorización para permitir un enfoque claro sobre asignar cada incidente de seguridad de la información a personas convenientes y determinar la urgencia del manejo y las respuestas a los incidentes de seguridad de la información, incluyendo si se requiere una respuesta inmediata, análisis forense de seguridad de la información y actividades de comunicación, en la siguiente fase (Respuestas – véase el apartado 8).

c) Actividad para llevar el asunto a un nivel superior, sobre la base de necesidades a lo largo de las fases para evaluaciones y / o decisiones adicionales.

d) Actividad para asegurar que todos los involucrados, particularmente en el ERISI, registren apropiadamente todas las actividades para su análisis posterior.

e) Actividad para asegurar que se reúne y almacena de manera segura la evidencia electrónica y que su presencia segura se monitorea continuamente, en caso se requiera para un proceso legal o acción disciplinaria interna.

f) Actividad para asegurar que el régimen de control de cambios se mantiene cubriendo el rastreo de los incidentes de seguridad de la información y las actualizaciones de reportes de incidentes y, de este modo, que se mantenga al día la base de datos de eventos / incidentes / vulnerabilidades de seguridad de la información.

Toda la información recolectada que pertenece a un evento, incidente o vulnerabilidad de seguridad de la información debe almacenarse en la base de datos de eventos / incidentes / vulnerabilidades de seguridad de la información administrada por ERISI. La información reportada durante cada actividad debe ser tan completa como sea posible en el momento para asegurar que haya una buena base disponible para las evaluaciones y decisiones que se realicen y, por supuesto, las acciones que se tomen.

Una vez que se ha detectado y reportado un evento de seguridad de la información, las actividades posteriores son las siguientes.

g) Actividad para distribuir la responsabilidad respecto de las actividades de gestión de incidentes de seguridad de la información a través de una jerarquía apropiada de personal, con evaluación, toma de decisiones y acciones que incluyen tanto al personal de seguridad como al personal no dedicado a la seguridad.

h) Actividad para proveer procedimientos formales para que cada persona notificada los siga, incluyendo la revisión y modificación del reporte realizado, evaluación del daño, y notificación del personal relevante. Las acciones individuales dependen del tipo y de la severidad del incidente.

i) Actividad para usar lineamientos para una documentación exhaustiva del evento de seguridad de la información.

j) Actividad para usar lineamientos para una documentación exhaustiva de las acciones subsiguientes respecto de si un incidente de seguridad de la información se clasifica como un incidente de seguridad de la información.

k) Actividad para actualizar la base de datos de eventos / incidentes / vulnerabilidades de seguridad de la información.

La organización debe asegurar que esta fase incluya la evaluación de la información reunida sobre las vulnerabilidades reportadas de seguridad de la información que todavía no han sido explotadas para causar eventos de seguridad de la información y posiblemente incidentes de seguridad de la información. Debe tratarse las decisiones que se tomó, quién las tomó y con qué prioridad.

7.2 Evaluación y decisión inicial de PdC

La persona de recepción en el PdC debe acusar recibo del formulario llenado de reporte de eventos de seguridad de la información, ingresarlo en la base de datos de eventos / incidentes / vulnerabilidades de seguridad de la información y revisarlo. Dicha persona debe buscar cualquier aclaración de la persona que reporta el evento de seguridad de la información y recolectar cualquier información adicional requerida y que se sabe está disponible, ya sea de la persona que reporta o de cualquier otro lugar. Entonces, el PdC debe conducir una evaluación para determinar si el evento de seguridad de la información debe clasificarse como un incidente de seguridad de la información o si es, de hecho, una falsa alarma (incluyendo el uso de la escala acordada de clasificación de incidentes de la organización). Si se determina que el evento de seguridad de la información es una falsa alarma, el formulario de reportes de eventos de seguridad de la información debe llenarse y comunicarse al ERISI para añadirlo a la base de datos de eventos / incidentes / vulnerabilidades y revisar y copiar a la persona que reporta y a su gerente local.

La información y otra evidencia recolectada en esta etapa pueden tener que utilizarse en el futuro para procedimientos disciplinarios o judiciales. La persona o personas que se ocupan de las tareas de recolección y evaluación deben estar capacitadas respecto de los requisitos para la recolección y preservación de evidencia.

Además de registrar la(s) fecha(s) y la(s) hora(s) de las acciones, es necesario documentar plenamente lo siguiente:

a) lo que se vio e hizo (incluyendo las herramientas utilizadas) y por qué,

b) la ubicación de la evidencia potencial,

c) cómo está archivada la evidencia (si es aplicable),

d) cómo se realizó la verificación de la evidencia (si es aplicable), y

e) los detalles de la custodia de almacenamiento / seguro del material y el acceso posterior al mismo.

Si se determina que el evento de seguridad de la información es probablemente un incidente de seguridad de la información y si la persona del PdC tiene el nivel apropiado de competencia, se puede conducir más evaluaciones. Esto puede requerir acciones de

solución, por ejemplo, identificar controles adicionales de emergencia y referir el tema a la persona apropiada para que tome acción. Puede ser evidente que se determine que un evento de seguridad de la información sea un incidente de seguridad de la información significativo (utilizando la escala de severidad predeterminada en la organización), en cuyo caso el gerente del ERISI debe ser informado directamente. Puede ser evidente que una situación de crisis deba declararse y, por ejemplo, el gerente de gestión de crisis sea notificado para una posible activación de un plan de gestión de crisis y que se informe al gerente del ERISI y a la alta gerencia. Sin embargo, la situación más probable es que el incidente de seguridad de la información requiera ser referido directamente al ERISI para una evaluación y acción adicionales.

Cualquiera que se determina como el siguiente paso, el PdC debe llenar tanto como sea posible el formulario de reporte de incidentes de seguridad de la información. El formulario de reporte de incidentes de seguridad de la información debe contener una narración de los hechos y tanto como sea posible debe confirmar y describir lo siguiente:

a) qué es el incidente de seguridad de la información,

b) cómo, qué o quién lo causó,

c) a qué afecta o podría afectar,

d) el impacto o el impacto potencial del incidente de seguridad de la información en el negocio de la organización,

e) una indicación respecto de si el incidente de seguridad de la información se considera significativo o no (utilizando la escala predeterminada de clasificación de la organización), y

f) cómo se ha tratado hasta el momento.

Cuando se considera los efectos adversos potenciales o reales de un incidente de seguridad de la información sobre el negocio de una organización, los siguientes son algunos ejemplos:

a) divulgación no autorizada de la información,

b) modificación no autorizada de la información,

c) repudio de la información,

d) no disponibilidad de la información y / o del servicio,

e) destrucción de la información y / o del servicio, y

f) desempeño reducido del servicio.

El primer paso es considerar cuál consecuencia es relevante dentro de una serie de consecuencias. Para aquellas que se considera relevante, se debe utilizar el lineamiento de la categoría relacionada para establecer los impactos potenciales o reales de modo que se los ingrese en el reporte de incidentes de seguridad de la información. En el Anexo C se encuentran los lineamientos como ejemplo. Algunos ejemplos de categorías son los siguientes:

a) pérdida financiera / interrupción de las operaciones de negocios,

b) intereses comerciales y económicos,

c) información personal,

d) obligaciones legales y regulatorias,

e) operaciones de la gerencia y del negocio,

f) pérdida de fondos de comercio,

g) daño o pérdida de vida, y

h) trastornos sociales.

Si se ha resuelto un incidente de seguridad de la información, el informe debe incluir detalles de los controles que se ha tomado y sobre cualquier lección aprendida (por ejemplo, los controles a adoptarse para evitar que vuelva a ocurrir o que haya ocurrencias similares). Una vez que se llena tanto como sea posible, el formulario de reporte debe entonces referirse al ERISI para que se ingrese a la base de datos de eventos / incidentes / vulnerabilidades de seguridad de la información y se lo revise.

Si una investigación va a ser posiblemente más larga que un periodo definido en la política de gestión de incidentes de seguridad de la información, se debe producir un informe interino dentro de un periodo especificado por la política.

Se enfatiza que el PdC que evalúa un incidente de seguridad de la información debe ser consciente del mismo, basándose en la guía proporcionada en la documentación del esquema de gestión de incidentes de seguridad de la información. Incluye lo siguiente como ejemplo:

a) cuándo es necesario escalar los asuntos y a quién, y

b) los procedimientos de control de cambios deben ser seguidos en todas las actividades conducidas por el PdC.

De manera similar a lo mencionado en los apartados 6.2 y 6.3 anteriores respecto de la detección y reporte de eventos, se debe utilizar medios de comunicación alternativos a los formularios de reportes actualizados cuando existan problemas, o cuando se consideren que existen, con los mecanismos de reporte electrónico (por ejemplo, correo electrónico).

7.3 Evaluación y confirmación de incidentes por el ERISI

La evaluación y la confirmación de la decisión respecto a si un evento de seguridad de la información debe clasificarse como un incidente de seguridad de la información debe ser responsabilidad del ERISI. La persona de recepción en el ERISI debe hacer lo siguiente:

a) Acusar recibo del formulario de reportes de incidentes de seguridad de la información, llenado tanto como sea posible por el PdC.

b) Ingresar el formulario en la base de datos de eventos / incidentes / vulnerabilidades de seguridad de la información si el PdC no lo hizo y actualizar la base de datos si es necesario.

c) Buscar aclaraciones por parte del PdC, si es necesario.

d) Revisar el contenido del formulario de reportes.

e) Recolectar cualquier información adicional requerida y que se conozca está disponible, ya sea del PdC, de la persona que llenó el formulario de reportes de eventos de seguridad de la información o de otro lugar.

Si sigue habiendo un cierto grado de incertidumbre respecto de la autenticidad del incidente de seguridad de la información o de la exhaustividad de la información reportada, el miembro del ERISI debe conducir una evaluación para determinar si el incidente de seguridad de la información es real o es, de hecho, una falsa alarma a través del uso de la escala acordada de clasificación de incidentes de la organización. Si se determina que el incidente de seguridad de la información es una falsa alarma, se debe llenar el reporte de eventos de seguridad de la información, se debe añadir el reporte a la base de datos de eventos/incidentes/vulnerabilidad de seguridad de la información y comunicarse al gerente del ERISI. Se debe enviar copias del informe al PdC y a la persona que reporta y a su gerente local.

Un informe de incidentes de seguridad debe correlacionarse con cualquier otro evento/incidente reportado al ERISI. Esta importante actividad debe verificar si el incidente está conectado a cualquier otro evento/incidente o si es simplemente el efecto de otro incidente, por ejemplo en los Ataques de Denegación de Servicio (DoS) y Denegación Distribuida del Servicio (DDoS). La correlación de incidentes también es importante para priorizar los esfuerzos del ERISI.

Si se determina que el incidente de seguridad de la información es real, el miembro del ERISI y sus colegas, según se requiera, deben conducir una evaluación adicional. El objetivo es confirmar lo siguiente tan pronto como sea posible:

a) Qué es el incidente de seguridad de la información, cómo se causó y qué y quién lo causó, qué afecta o podría afectar, el impacto o impacto(s) potencial(es) del incidente de seguridad de la información sobre el negocio de la organización, una indicación de si el incidente de seguridad de la información se considera significativo o no utilizando la escala predeterminada de gravedad que tiene la organización. Si el incidente causa un impacto negativo grave en el negocio, se ha de iniciar actividades de crisis. (Véase el apartado 8.2.4)

b) Se debe tomar en cuenta los siguientes aspectos para ataque técnico humano deliberado a un sistema, servicio y/o red de información:

1) cuán profundamente ha sido infiltrado el sistema/servicio y/o red y que nivel de control tiene el atacante,

2) qué datos han sido obtenidos por el atacante, posiblemente copiados, alterados o destruidos,

3) qué software ha sido copiado, alterado o destruido por el atacante.

c) Los efectos directos e indirectos (por ejemplo, si el acceso físico queda abierto debido a un incendio, si un sistema de información es vulnerable debido a algún mal funcionamiento del software o de las comunicaciones o debido a error humano), y

d) Cómo se ha tratado el incidente de seguridad de la información hasta el momento y quién lo ha tratado.

Cuando se revisa os efectos adversos potenciales o reales de un incidente de seguridad de la información sobre el negocio de una organización de cierta información y/ o servicios mostrados en el apartado 7.2, es necesario confirmar cuál de una serie de consecuencias es relevante. El apartado 7.2 y el Anexo C muestran algunas categorías como ejemplo.

Se debe utilizar un proceso de priorización para asignar un incidente de seguridad de la información a la persona o grupos de personas más convenientes en el ERISI de modo que den respuesta adecuada al incidente de seguridad de la información. En particular, cuando se trabaja sobre varios incidentes de seguridad de la información a la vez, se debe fijar prioridades para ordenar las respuestas que se debe dar a los incidentes de seguridad de la información.

Se debe fijar prioridades de acuerdo con los impactos adversos al negocio que se ha determinado que están asociados con el incidente de seguridad de la información y el esfuerzo que se estima necesario para responder al incidente de seguridad de la información. Para los incidentes con la misma prioridad, el esfuerzo requerido es una métrica que determine el orden en el que se tiene que responder para ellos. Por ejemplo, un incidente que se resuelva fácilmente puede tratarse antes de un incidente que requiere un mayor esfuerzo.

Para aquellos que se consideran relevantes, se debe utilizar el lineamiento de la categoría relacionada para establecer los impactos potenciales o reales de modo que se los ingrese en el reporte de incidentes de seguridad de la información. En los Anexos C y D se proporcionan lineamientos como ejemplo.

8. FASE DE RESPUESTAS

8.1 Revisión de las actividades claves

La tercera fase del uso operativo de un esquema de gestión de incidentes de seguridad de la información incluye dar respuestas a los incidentes de seguridad de la información de acuerdo con las acciones acordadas en la fase de evaluación y toma de decisiones. Dependiendo de las decisiones, las respuestas deben darse inmediatamente, en tiempo real o en tiempo casi real y algunas podrían involucrar análisis forense de seguridad de la información.

Para la fase de respuesta, una organización debe asegurar que las actividades claves sean las siguientes:

a) Actividad de revisión para que el ERISI determine si el incidente de seguridad de la información está bajo control, así como las actividades siguientes:

1) Actividad para desencadenar la respuesta requerida si está bajo control. Ésta podría ser una respuesta inmediata que podría incluir la activación del proceso de recuperación y/o la emisión de comunicaciones al personal involucrado relevante o un tipo de respuesta más lento (por ejemplo, facilitando la plena recuperación de un desastre) a la vez que se asegura que toda la información esté lista luego del incidente.

2) Actividad para desencadenar las actividades de crisis a través del escalamiento a la función de manejo de crisis, si no está bajo control o si va a tener un impacto grave en los servicios medulares de la organización (véase el apartado 8.2.4). Entonces, la función de manejo de crisis es responsable del incidente, con pleno apoyo del ERISI (incluyendo la activación de un plan de gestión de crisis) involucrando al personal relacionado, por ejemplo al gerente de gestión de crisis de la organización y su equipo (para obtener guía sobre la gestión de continuidad del negocio véase ISO/IEC 27031 y ISO/PAS 22399:2007).

b) Actividad para asignar recursos internos e identificar recursos externos de manera que se responda a un incidente.

c) Actividad para conducir análisis forenses de seguridad de la información según se requiera y relativa al puntaje de la escala de clasificación de incidentes de

seguridad de la información y el cambio de ese puntaje de la escala según sea necesario.

d) Actividad para llevar el asunto a un nivel superior según se requiera a lo largo de la fase, para evaluaciones y/o decisiones adicionales.

e) Actividad para asegurar que todos los involucrados, particularmente en el ERISI, registren apropiadamente todas las actividades para su análisis posterior.

f) Actividad para asegurar que se regule y almacene de manera probadamente segura la evidencia electrónica y que su preservación segura se monitoree continuamente, en caso se requiera para un proceso legal o acción disciplinaria interna.

g) Actividad para asegurar que el régimen de control de cambios se mantenga cubriendo el rastreo de incidentes de seguridad de la información y las actualizaciones de los reportes de incidentes y, de este modo, que se mantenga al día la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información.

h) Actividad para comunicar la existencia del incidente de seguridad de la información o cualquier detalle relevante del mismo a otras personas u organizaciones internas o externas, en particular los encargados de activos/informaciones/servicios (que se determine durante el análisis de impacto) y las organizaciones internas/externas que deben participar en la gestión y resolución del incidente.

Toda la información recolectada perteneciente a un evento, incidente o vulnerabilidad de seguridad de la información debe almacenarse en la base de datos de eventos / incidentes / vulnerabilidades de seguridad de la información manejada por el ERISI, incluyendo su utilización para propósitos de análisis adicionales. La información reportada durante cada actividad debe ser tan completa como sea posible en el momento para asegurar que hay una buena base disponible para las evaluaciones y decisiones a realizarse y, por supuesto, acciones a tomarse.

Una vez que se ha determinado un incidente de seguridad de la información y se ha acordado las respuestas, las actividades posteriores son las siguientes:

a) Actividad para distribuir la responsabilidad respecto de las actividades de manejo de gestión de incidentes a través de una jerarquía apropiada de personal. La

toma de decisiones y acciones involucran tanto al personal de seguridad como al personal que no se dedica a la seguridad, según sea necesario.

b) Actividad para proveer procedimientos formales para que cada persona involucrada los siga, incluyendo la revisión y modificación a los reportes hechos, la reevaluación del daño y la notificación al personal relevante. Las acciones individuales dependen del tipo y gravedad del incidente.

c) Actividad para usar lineamientos para una documentación exhaustiva de un incidente de seguridad de la información, de las acciones subsiguientes y para actualizar la base de datos de eventos / incidentes / vulnerabilidades de seguridad de la información.

d) Actividad para utilizar lineamientos para una documentación exhaustiva de las acciones subsiguientes.

e) Actividad para actualizar la base de datos de eventos / incidentes / vulnerabilidades de seguridad de la información.

Una vez que se ha tratado exitosamente un incidente de seguridad de la información se debe cerrar formalmente y esto debe registrarse en la base de datos de gestión de incidentes de seguridad de la información. La organización debe asegurar que esta fase también incluya dar respuestas a las vulnerabilidades de seguridad de la información reportadas de acuerdo con las acciones acordadas en las fases de evaluación y toma de decisiones. Una vez que se ha tratado cualquier vulnerabilidad se debe registrar los detalles en la base de datos de gestión de incidentes de seguridad de la información.

El apartado 8.2 proporciona guía sobre respuestas a los incidentes de seguridad de la información.

8.2 Respuestas

8.2.1 Respuestas inmediatas

8.2.1.1 Revisión

En la mayoría de los casos, las actividades siguientes para el miembro de lERISI son identificar las acciones inmediatas de respuesta para ocuparse del incidente de seguridad de la información, registrar detalles del formulario de incidentes de seguridad de la información dentro de la base de datos de eventos / incidentes / vulnerabilidades de seguridad de la información, y notificar las acciones referidas a las personas o grupos apropiados. Esto puede resultar en controles de emergencia (por ejemplo, corte / cierre de un sistema, servicio y / o red de información afectado, con el acuerdo previo de la gerencia relevante de TI y / o del negocio), y / o identificación de controles adicionales permanentes así como notificación a la persona o grupo apropiado para que actúe. Si no se ha hecho ya, se debe determinar la importancia del incidente de seguridad de la información, utilizando la escala predeterminada de clasificación de la organización y si es suficientemente significativa se debe notificar directamente a la alta gerencia correspondiente. Si es evidente que debe aclararse una situación de crisis, por ejemplo se debe notificar al gerente de gestión de crisis para la posible activación de un plan de gestión de crisis, también se debe informar al gerente del ERISI y a la alta gerencia.

Los objetivos generales cuando se responde a los incidentes de seguridad de la información son los siguientes:

a) confinar los impactos adversos potenciales (de incidentes de seguridad de la información), y

b) mejorar la seguridad de la información.

El fin principal del esquema de gestión de incidentes de seguridad de la información y las actividades asociadas al mismo debería ser la minimización de impactos adversos al negocio, mientras que la identificación del atacante debe considerarse como un fin secundario.

8.2.1.2 Ejemplos de acciones

Un ejemplo de acción de respuesta inmediata relevante en caso de un ataque deliberado a un sistema, servicio y / o red de información es dejarlo conectado a Internet o a otra red. Esto permitirá que las aplicaciones críticas del negocio funcionen correctamente y recolectará tanta información como sea posible sobre el atacante siempre y cuando el atacante no sepa que está siendo vigilado.

Es vital seguir los procesos planificados y registrar la acción. Hay que tener cuidado de los troyanos, los "rootkits" y los módulos de núcleo que pueden causar graves daños al sistema. Se puede proteger evidencia con criptografía, candados y registros de acceso.

a) Cuando se toma una decisión de esta naturaleza, se debe considerar que el atacante puede darse cuenta de que lo están observado y puede realizar acciones que pueden causar más daño al sistema, servicio y / o red de información afectado y datos relacionados, y que el atacante puede destruir la información que podría ser útil para rastrearlo.

b) Es esencial que sea técnicamente posible cortar y / o cerrar de manera rápida el sistema, servicio y / o red de información atacado una vez que se ha tomado una decisión. Esto sirve para contener el incidente.

Una consideración adicional es que la prevención de re-ocurrencias es normalmente de alta prioridad y podría muy bien concluirse que el atacante ha expuesto una vulnerabilidad que debería rectificarse y las ventajas de rastrearlo no justifican el esfuerzo de hacerlo. Es especialmente relevante cuando el atacante no es malicioso y ha causado poco o ningún daño.

Respecto de los incidentes de seguridad de la información causados por una cosa diferente a un ataque deliberado, se debe identificar la fuente. Puede ser necesario cerrar el sistema, servicio y / o red de información o aislar la parte relevante y cerrarla (con acuerdo previo de la gerencia relevante de TI y / o del negocio) mientras se implementan los controles. Esto puede tomar más tiempo si la vulnerabilidad es fundamental al diseño del sistema, servicio y / o red de información, o si es una vulnerabilidad crucial.

Otra actividad de respuesta puede ser activar técnicas de vigilancia (por ejemplo, honeypots – véase ISO/IEC 18043). Esto debe hacerse en base a procedimientos documentados para el esquema de gestión de incidentes de seguridad de la información.
Un miembro del ERISI debe verificar la información que puede haber sido corrompida por el incidente de seguridad de la información contra registros de respaldo para ver las modificaciones, eliminaciones o inserciones de información. Puede ser necesario verificar la integridad de los registros ya que un atacante deliberado puede haber manipulado estos registros para cubrir su rastro.

8.2.1.3 Actualización de información de incidentes

Sin importar qué paso siguiente se determine, el miembro del ERISI debe actualizar el reporte de incidentes de seguridad de la información tanto como sea posible, añadirlo a la base de datos de eventos / incidentes / vulnerabilidades de seguridad de la información y notificar al gerente del ERISI y otros según sea necesario. La actualización puede cubrir información adicional sobre lo siguiente:

a) qué es el incidente de seguridad de la información,

b) cómo se causó y qué o quién lo causó,

c) a qué afecta o podría afectar,

d) el impacto o el impacto potencial del incidente de seguridad de la información sobre el negocio de la organización,

e) cambios a la indicación de si se considera el incidente de seguridad de la información como importante o no (utilizando la escala predeterminada de gravedad que tiene la organización), y

f) cómo se ha tratado hasta este momento.

Si se ha resuelto un incidente de seguridad de la información, el reporte debe incluir detalles de los controles que se han tomado y de cualquier otra lección aprendida (por ejemplo, mayores controles a adoptarse para evitar la re-ocurrencia u ocurrencias similares). El reporte actualizado debe añadirse a la base de datos de eventos / incidentes / vulnerabilidades de seguridad de la información y notificarse al gerente del ERISI y a otros según se requiera.

Se enfatiza que el ERISI es responsable de asegurar la retención segura de toda la información que corresponde a un incidente de seguridad de la información para su análisis posterior y para su utilización potencial como evidencia legal. Por ejemplo, para un incidente de seguridad de la información orientado a la TI, se debe tomar las acciones siguientes.

Luego del descubrimiento inicial del incidente, se debe recolectar todos los datos volátiles antes de que se cierre el sistema, servicio y / o red de TI afectado, para una investigación forense completa sobre la seguridad de la información. Se debe recolectar información incluyendo los contenidos de la memoria, cache y registros y el detalle de cualquier actividad corriente así como los siguientes:

a) Debe realizarse una duplicación forense completa de la seguridad de la información del sistema afectado o un respaldo de bajo nivel de los registros y archivos importantes dependiendo de la naturaleza del incidente de seguridad de la información.

b) Debe recolectarse y revisarse registros de sistemas, servicios y redes vecinas, por ejemplo de ruteadores y firewalls.

c) Se debe almacenar toda la información recolectada de manera segura en medios de solo lectura.

d) Debe haber dos o más personas presentes cuando se realiza la duplicación forense de seguridad de la información para establecer y certificar que todas las actividades se han llevado a cabo de acuerdo con la legislación y los lineamentos relevantes.

e) Se debe documentar y almacenar junto con los medios originales las especificaciones y descripciones de las herramientas y comandos para realizar la duplicación forense de seguridad de la información.

Un miembro del ERISI también es responsable de facilitar el retorno de la instalación afectada (ya sea de TI u otro) a un estado operativo seguro que no sea susceptible de ser comprometido por el mismo ataque, si es posible en esta etapa.

8.2.1.4 Actividades adicionales

Si un miembro del ERISI determina que un incidente de seguridad de la información es real, entonces otras actividades importantes deberían ser las siguientes:

a) actividad para instituir el análisis forense de seguridad de la información, y

b) actividad para informar a aquellos que son responsables de las comunicaciones internas y externas sobre los hechos y propuestas de lo que se debe comunicar, de qué manera y a quién.

Una vez que se ha llenado un reporte de incidentes de seguridad de la información tanto como sea posible, debe ingresarse en la base de datos de eventos / incidentes / vulnerabilidades de seguridad de la información y comunicárselo al gerente del ERISI.

Es probable que una investigación sea más larga que un periodo acordado de antemano dentro de la organización. En ese caso se debe producir un reporte interino.

El miembro del ERISI que evalúa un incidente de seguridad de la información debe ser consciente, en base a la guía proporcionada en la documentación del esquema de gestión de incidentes de seguridad de la información, entre otros, de lo siguiente:

a) cuándo es necesario escalar los asuntos y a quién, y

b) los procedimientos de control de cambios deben seguirse en todas las actividades conducidas por el ERISI.

Cuando existen o se considera que existen problemas con las instalaciones de las comunicaciones electrónicas (por ejemplo, correo electrónico o web), incluso cuando se pensó que era posible que el sistema estuviera bajo ataque, se debe reportar a las personas relevantes por teléfono o mensaje de texto.

Si se concluye que un incidente de seguridad de la información es importante o que se ha determinado una situación de crisis, entonces el gerente del ERISI, en enlace con el gerente de seguridad de la información de la organización y el miembro del directorio / alto gerente relevante, debe enlazarse con todas las partes relacionadas, tanto internas como externas a la organización.

Para asegurar que los enlaces se organizan de manera rápida y eficaz, es necesario establecer un método seguro de comunicación de antemano que no se base por completo en el sistema, servicio y / o red que puede ser afectado por el incidente de seguridad de la información. Estos arreglos pueden incluir el nombramiento de asesores o representantes de respaldo en caso de ausencia.

8.2.2 Evaluación del control sobre los incidentes de seguridad de la información

Luego de que un miembro del ERISI ha desencadenado las respuestas inmediatas y las actividades relevantes del análisis forense de seguridad de la información y de las comunicaciones, se necesita determinar rápidamente si el incidente de seguridad de la información está bajo control. Si es necesario, el miembro del ERISI puede consultar con sus colegas, el gerente del ERISI y / u otras personas o grupos.

Si se ha confirmado que el incidente de seguridad de la información está bajo control, el miembro del ERISI debe instituir cualquier respuesta posterior requerida, así como el análisis forense de seguridad de la información y las comunicaciones para terminar con el incidente de seguridad de la información y restaurar el sistema de información aceptado a sus operaciones normales.

Si se confirma que el incidente de seguridad de la información no está bajo control, entonces el miembro del ERISI debe instituir actividades de crisis.

Si el incidente de seguridad de la información está relacionado con pérdidas de seguridad, la métrica para evaluar si un incidente de seguridad de la información está bajo control podría ser el tiempo que transcurre antes de recuperar una situación normal luego de la ocurrencia de un incidente de seguridad de la información. La organización debería determinar para cada activo en base a los resultados de la evaluación de riesgo de seguridad de la información su ventana de interrupción aceptable, que es la base del objetivo de tiempo de recuperación antes de retomar el servicio o el acceso a la información. Tan pronto la respuesta exceda la ventana de interrupción aceptable del activo meta, el incidente de seguridad de la información puede ya no estar bajo control y debería tomarse la decisión de llevar el incidente de seguridad de la información a un nivel superior.

Los incidentes de seguridad de la información relacionados a las pérdidas de confidencialidad, integridad, etc. requieren otro tipo de criterio para determinar que la

situación está bajo control y las métricas relacionadas posibles de acuerdo con los planes de manejo de crisis de la organización.

8.2.3 Respuestas posteriores

Una vez que se haya determinado que el incidente de seguridad de la información está bajo control y no está sujeto a actividades de crisis, el miembro del ERISI debe identificar si se requiere respuestas para tratar el incidente de seguridad de la información y cuáles respuestas se requiere. Esto podría incluir restaurar el (los) tema(s), servicio(s) y / o red(es) de información afectado(s) a su operación normal. Dicho miembro debe entonces registrar los detalles en el formulario de reportes de incidentes de seguridad de la información y en la base de datos de eventos / incidentes / vulnerabilidades de seguridad de la información y notificar a los que son responsables de culminar las acciones relacionadas. Una vez que esas acciones se han culminado con éxito, se debe registrar los detalles en el formulario de reporte de incidentes de seguridad de la información y en la base de datos de eventos / incidentes / vulnerabilidades de seguridad de la información y luego el incidente de seguridad de la información se debe cerrar y se debe notificar al personal apropiado.

Algunas respuestas están dirigidas a prevenir que vuelva a ocurrir un incidente de seguridad de la información o una ocurrencia similar. Por ejemplo si se determina que la causa de un incidente de seguridad de la información es una falla del hardware o software de la TI y si hay un parche disponible, se debe contactar inmediatamente al proveedor. Si una vulnerabilidad conocida de la TI estuvo involucrada en un incidente de seguridad de la información, debe parcharse con la actualización relevante de seguridad de la información. Cualquier problema relacionado a la configuración de la TI que el incidente de seguridad de la información pone de relieve debe tratarse de ahí en adelante. Otras medidas para reducir la posibilidad de que vuelva a ocurrir un incidente de seguridad de la información de la TI u otra ocurrencia similar puede incluir el cambio de las claves de acceso al sistema y la inhabilitación de servicios no utilizados.

Otra área de actividad de respuesta puede involucrar el monitoreo del sistema, servicios y / o red de TI. Luego de la evaluación de un incidente de seguridad de la información, puede ser apropiado tener controles de monitoreo adicionales para ayudar a detectar eventos inusuales y sospechosos que serían sintomáticos en otros incidentes de seguridad de la información. Dicho monitoreo puede también revelar una mayor profundidad del incidente de seguridad de la información e identificar otros sistema de TI que fueron afectados.

Pueden ser necesarios para la activación de respuestas específicas documentadas en el plan de gestión de crisis relevante. Esto puede aplicarse tanto a incidentes de seguridad de la información relacionados con TI o no. Dichas respuestas deberían incluir las de todos los aspectos del negocio, no solamente directamente relacionados con TI, sino también mantenimiento y posterior restauración de funciones clave del negocio incluyendo, según sea relevante telecomunicaciones de voz y facilidades a los niveles del personal y físicas.
La última área de actividad es la restauración del (de los) sistema(s), servicio (s) y / o la(s) red(es) de información afectado(s) a la operación normal. La restauración de un (o varios) sistema(s), servicio(s) y / o red(es) afectado(s) a un estado operativo seguro puede lograrse a través de la aplicación de parches para las vulnerabilidades conocidas o inhabilitando un elemento que fue el sujeto de la afectación. Si todo el incidente de seguridad de la información es desconocido debido a la destrucción de los registros durante el incidente, entonces puede ser necesario reconstruir un sistema, servicio y / o red completo. Puede ser necesario también para la activación de partes del plan de gestión de crisis relevante.

Si un incidente de seguridad de la información no está relacionado a la TI, por ejemplo causado por un incendio, inundación o bomba, entonces las actividades de recuperación que se debe seguir son aquellas documentadas en el plan de gestión de crisis relevante.

8.2.4 Respuestas a las situaciones de crisis

Tal como se mencionó en el apartado 8.2.2 puede ser que el ERISI determine que un incidente de seguridad de la información no está bajo control y tenga que escalarse a una situación de crisis, utilizando un plan diseñado de antemano.

Las mejores opciones para tratar todos los tipos de incidentes de seguridad de la información que puedan afectar la disponibilidad y en cierta medida la integridad de un sistema de información deben haber sido identificados en el plan de gestión de crisis de la organización. Estas opciones deben relacionarse directamente a las prioridades del negocio de la organización y a las escalas de tiempo relacionadas para la recuperación y, de este modo, los periodos máximos aceptables para que la TI, los equipos de voz, las personas y las ubicaciones estén fuera de funcionamiento. La estrategia debe haber identificado lo siguiente:

a) las medidas preventivas, de capacidad de recuperación y de gestión de crisis requeridas,

b) la estructura organizativa requerida así como las responsabilidades para responder a la crisis,

c) la estructura y contenido descriptivo requeridos para el plan o los planes de gestión de crisis.

El (los) plan(es) de gestión de crisis y los controles establecidos para apoyar la activación de ese (esos) plan(es), una vez que se prueban satisfactoriamente, forman la base para tratar con la mayoría de incidentes escalados una vez que se definan como tales.

Dependiendo del tipo de incidente y si no está bajo control, el escalamiento puede llevar a actividades serias para tratar el incidente y activar el plan de gestión de crisis si existe. Dichas actividades pueden incluir, pero no taxativamente, la activación de:

a) procedimientos de instalaciones contra incendios y evacuación,

b) procedimientos de instalaciones contra inundaciones y evacuación,

c) procedimientos para el manejo de bombas y evacuación relacionada,

d) investigadores especialistas en fraudes de sistemas de información, y

e) investigadores especialistas en ataques técnicos.

8.2.5 Análisis forense de seguridad de la información

El ERISI debe conducir análisis forenses de seguridad de seguridad de la información donde se identifique de acuerdo a una evaluación previa y según se requiera para propósitos de evidencia de facto en el contexto de un incidente significativo de seguridad de la información. Debe involucrar el uso de técnicas y herramientas de investigación basadas en TI, apoyadas por procedimientos documentados para revisar el (los) incidente (s) de seguridad de la información designados en más detalles que hasta ese momento en el proceso de gestión de incidentes de seguridad de la información. Debe conducirse de manera estructurada y, según sea relevante, identificar lo que puede utilizarse como evidencia, ya sea procedimientos disciplinarios o acciones legales.

Las facilidades que se necesitan para el análisis forense de seguridad de la información probablemente se clasifican en técnicas (por ejemplo, herramientas de auditorías, facilidades para recuperar evidencia), procedimentales, de personal e instalaciones seguras de oficina. Dicha actividad de análisis forense de seguridad de la información debería documentarse plenamente, incluyendo fotografías relevantes, informes de análisis del registro de auditoría y registros de recuperación de datos. Se debe documentar la experiencia y profesionalismo de la persona o personas que realizan el análisis forense de seguridad de la información junto los registros de las pruebas de su experiencia y profesionalismo. También debe documentarse cualquier otra información que demuestre la objetividad y la naturaleza lógica del análisis. Todos los registros de los incidentes mismos de seguridad de la información, las actividades de análisis forense de seguridad de la información, etc. y los medios asociados deben almacenarse en un entorno físicamente seguro y controlado por procedimientos para impedir el acceso, alteración o indisposición del material por parte de personas no autorizadas. Las herramientas basadas en TI para el análisis forense de seguridad de la información deben cumplir con normas de tal modo que su exactitud no se pueda impugnar legalmente y se deben mantener actualizadas en línea con los cambios de la tecnología. El entorno físico del ERISI debe proveer condiciones demostrables que aseguren que la evidencia se está manejando de tal manera que la acción no pueda ser impugnada. Se debe disponer de suficiente personal, si es necesario acceder al mismo a pedido para ser capaces de responder en cualquier momento.

Con el tiempo pueden surgir nuevas necesidades para revisar la evidencia de una serie de incidentes de seguridad de la información, incluyendo el fraude, el hurto y el vandalismo. De este modo, para ayudar al ERISI debe haber una serie de medios basados en TI y de procedimientos de apoyo disponibles para descubrir información oculta en un sistema, servicio o red de información, incluyendo información que en una inspección inicial parece haber sido eliminada, encriptada o dañada. Estos medios deben tratar todos los aspectos asociados con tipos de incidentes de seguridad de la información conocidos y deben documentarse en los procedimientos del ERISI.

En el entorno de hoy en día, a menudo se necesita hacer un análisis forense de seguridad de la información para abarcar entornos complejos en red, donde la investigación requiere abarcar un entorno operativo completo, incluyendo una multitud de servidos (por ejemplo, archivo, impresiones, comunicaciones y correo electrónico) así como facilidades de acceso remoto. Existen muchas herramientas disponibles, incluyendo herramientas de búsqueda de texto, software que conduce a imágenes y suites forenses de seguridad de la información. El foco principal de los procedimientos de análisis forenses de seguridad de la información es asegurar que la evidencia se mantenga intacta y verificada para estar seguros de que resistirá cualquier impugnación legal.

Se enfatiza que el análisis forense se mantenga debe realizarse en una copia exacta de los datos originales para evitar que el trabajo de análisis perjudique la integridad original de los medios. El proceso general del análisis forense de seguridad de la información de abarcar, según sea relevante, las siguientes actividades:

a) Actividad para asegurar que el sistema, servicio y / o red objetivo esté protegido durante el análisis forense de seguridad de la información contra su indisposición, alteración o afectado de otro modo, incluyendo la introducción de código malicioso (incluso virus) y que no haya ningún efecto o algún efecto mínimo en las operaciones normales.

b) Actividad para priorizar la adquisición y recolección de evidencia, por ejemplo procediendo a partir de la más volátil a la menos volátil (esto depende en gran medida de la naturaleza del incidente de seguridad de la información).

c) Actividad para identificar todos los archivos relevantes sobre el sistema, servicio y / o red correspondiente, incluyendo archivos normales, claves de acceso o archivos protegidos de otro modo, así como archivos encriptados.

d) Actividad para recuperar tanto como sea posible los archivos eliminados descubiertos y otros datos.

e) Actividad para descubrir direcciones IP, nombres de anfitriones, rutas de redes e información de páginas web.

f) Actividad para extraer los contenidos de archivos ocultos, temporales y de intercambio (swap) utilizados tanto por la aplicación como por el sistema operativo.

g) Actividad para acceder a los contenidos de archivos protegidos o encriptados (salvo que la ley lo prohíba).

h) Actividad para analizar todos los datos relevantes posibles que se encuentran en áreas de almacenamiento de disco y que son normalmente inaccesibles.

i) Actividad para analizar las horas de acceso, modificación y creación de archivos.

j) Actividad para analizar registros de sistemas / servicios / redes y aplicaciones.

k) Actividad para determinar la actividad de usuarios y / o aplicaciones en un sistema / servicio / red.

l) Actividad para analizar correos electrónicos para obtener información y contenido de la fuente.

m) Actividad para realizar verificaciones de integridad de los archivos para detectar archivos con caballos troyanos y archivos que no estaban originalmente en el sistema.

n) Actividad para analizar, si fuera aplicable, evidencia física, por ejemplo huellas digitales, daño a la propiedad, vigilancia por video, registros de sistemas de alarmas, registros de acceso a tarjetas de pase y entrevistas a testigos.

o) Actividad para asegurar que la evidencia potencial extraída se maneja y almacena de tal manera que no pueda dañarse ni hacerse inutilizable y que el material sensible no pueda ser visto por aquellos que no están autorizados. Se enfatiza que la reunión de evidencia debería estar siempre de acuerdo con las reglas del tribunal o la audiencia en la que se pueda presentar la evidencia.

p) Actividad para concluir sobre las razones para el incidente de seguridad de la información, las acciones requeridas y en qué tiempo. La evidencia debe comprender listas de archivos relevantes incluidos en un anexo al informe principal.

q) Actividad para proporcionar apoyo experto a cualquier acción disciplinaria o legal, según se requiera.

El (los) método (s) a seguirse deben documentarse en los procedimientos del ERISI.

El ERISI debe poseer suficientes combinaciones de habilidades para proveer amplia cobertura de conocimiento técnico (incluyendo conocimiento de las herramientas y técnicas que probablemente utilicen atacantes deliberados), experiencia en el análisis y en la investigación (incluyendo respecto de la preservación de evidencia utilizable), conocimiento de las implicaciones relevantes de la legislación y los reglamentos y conocimiento actualizado de las tendencias de incidentes.

Se debe reconocer lo siguiente:

a) algunas organizaciones pueden no tener estos recursos disponibles y pueden requerir tercerizar el trabajo de análisis forense de seguridad de la información a especialistas,

b) la recolección de material forense de seguridad de la información puede ser sólo un recurso (por ejemplo, si se justifican el esfuerzo y el gasto) cuando ha ocurrido una pérdida seria y / o probablemente se vaya a realizar una acción penal, y

c) la no utilización de recursos por parte de los especialistas para capturar material forense de seguridad de la información puede hacer que los hallazgos sean inadmisibles si se requiere acción del tribunal.

8.2.6 Comunicaciones

En muchos casos, cuando el ERISI ha confirmado que un incidente de seguridad de la información es real, es necesario que algunas personas sean informadas tanto internamente (fuera de las líneas de comunicación normales entre el ERISI y la gerencia) y externamente, incluyendo a la prensa. Puede ser necesario que esto ocurra en una serie de etapas, por ejemplo cuando se confirma que un incidente de seguridad de la información es real, cuando se confirma que está bajo control, cuando se designa para actividades de crisis, cuando se cierra y cuando se ha culminado la revisión luego del incidente y se ha llegado a conclusiones.
Cuando se necesita la comunicación, se debe prestar atención a asegurar quién debe saber qué y cuándo. Las partes interesadas afectadas deben de terminarse y preferiblemente dividirse en grupos como:

a) partes interesadas internas directas (gestión de crisis, personal de gerencia, etc.),

b) partes interesadas directas (propietarios, clientes, socios, proveedores, etc.), y

c) otros contactos externos como la prensa y/u otras medios.

Cada grupo puede requerir información especial que debe ir a través de los canales apropiados de la organización. Una de las tareas más importantes para la comunicación luego de que se produce un incidente de seguridad de la información es asegurar que las partes interesadas directas externas e internas tengan la información antes de que llegue a través de otros contactos externos como la prensa.

Para ayudar en esta actividad cuando surge la necesidad, es sensato practicar para preparar cierta información de antemano de tal modo que se ajuste rápidamente la circunstancias de

un incidente de seguridad de la información en particular y se emitan a cada grupo relevante y, en particular, a la prensa y/u otros medios. Si cualquier información correspondiente a los incidentes de seguridad de la información va a divulgarse a la prensa debe hacerse de acuerdo con la política de divulgación de información de la organización. La información a divulgarse debe ser revisada por las partes relevantes, lo cual puede incluir la alta gerencia, los coordinadores de relaciones públicas y el personal de seguridad de la información.

NOTA: Las comunicaciones de incidentes de seguridad de la información pueden variar dependiendo del incidente y de su impacto en combinación con las relaciones de la organización y su tipo de negocio. El tipo de negocio debe también establecer reglas específicas respecto de cómo debe revisarse la comunicación, por ejemplo si la organización cotiza en bolsa.

8.2.7 Escalamiento

En circunstancias extremas, los asuntos pueden tener que escalar para poderse ocupar de incidentes que están fuera de control y que tienen un peligro potencial de producir un impacto inaceptable para el negocio. Estos incidentes tienen que escalarse para activar el plan de continuidad del negocio, si existe, reportando a cada alto gerente, a otro grupo dentro de la organización o a personas o grupos fuera de la organización. Esto puede ser para poder tomar una decisión sobre acciones recomendadas para tratar un incidente de seguridad de la información o para una evaluación adicional que permita determinar qué acciones se requiere tomar. Esto puede ser el paso siguiente a las actividades de evaluación escrita anteriormente en los apartados 7.2 y 7.3 o durante esas actividades si se hace evidente tempranamente algún problema importante. Debe disponerse de guía en la documentación del esquema de gestión de incidentes de seguridad de la información para aquellos que probablemente tengan que escalar los asuntos en algún momento, por ejemplo los miembros del PdC y del ERISI.

8.2.8 Registro de actividades y control de cambios

Se enfatiza que todos los que están involucrados en el reporte y gestión de un incidente de seguridad de la información deberían registrar apropiadamente todas las actividades para su análisis posterior. Eso debería estar incluido dentro del formulario de reporte de incidentes de seguridad de la información y en la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información, mantenerse continuamente al día a través del ciclo de un incidente de seguridad de la información desde el primer reporte hasta la culminación de la revisión luego del incidente.

Esta información debe retenerse de manera probadamente segura y con un régimen de respaldo adecuado. Además, todos los cambios que se hacen en el contexto de rastrear un incidente de seguridad de la información y de actualizar el formulario de reportes de incidentes de seguridad de la información así como la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información deben estar bajo un esquema formalmente aceptado de control de cambios.

9. FASES DE LECCIONES APRENDIDAS

9.1 Revisión de actividades claves

La cuarta fase de uso operativo de un esquema de gestión de incidentes de seguridad de la información es el punto siguiente cuando se ha resuelto/cerrado los incidentes de seguridad de la información e involucra el aprendizaje de lecciones a partir de cómo se ha manejado y tratado los incidentes (y vulnerabilidades). Para la fase de lecciones aprendidas, una organización debe asegurar que las actividades claves sean las siguientes:

a) Actividad para conducir análisis forense de seguridad de la información posterior, según se requiera.

b) Actividad para identificar las lecciones aprendidas a partir de incidentes y vulnerabilidades de seguridad de la información.

c) Actividad para revisar, identificar y hacer mejoras a la implementación de controles de seguridad de la información (controles nuevos y / o actualizados) así como la política de gestión de incidentes de seguridad de la información, como resultado de las lecciones aprendidas, ya sea de un incidente de seguridad de la información o de muchos (o evidentemente de vulnerabilidades reportadas de seguridad). La métrica que alimenta a la estrategia de la organización ayuda a decidir cómo invertir en controles de seguridad de la información.

d) Actividad para revisar, identificar y hacer mejoras a los resultados de la revisión de la evaluación y gestión de riesgos de seguridad de la información existentes, como un resultado de las lecciones aprendidas.

e) Actividad para determinar cuán eficaces fueron los procesos, procedimientos, formato de reportes y / o estructura organizativa para responder, evaluar y recuperarse de cada incidente de seguridad de la información y para tratar las vulnerabilidades de seguridad de la información. Igualmente, sobre la base de las

lecciones aprendidas, identificar y hacer mejoras al esquema de gestión de incidentes de seguridad de la información y su documentación.

f) Actividad para actualizar la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información.

g) Actividad para comunicar y compartir los resultados de revisiones dentro de una comunidad de confianza (si la organización así lo desea).

Se enfatiza que las actividades de gestión de incidente de seguridad de la información son imperativas y, de este modo, una organización debe hacer mejoras regulares a una serie de elementos de seguridad de la información a lo largo del tiempo. Estas mejoras deben ser propuestas sobre la base de revisiones de los datos sobre incidentes de seguridad de la información y de las respuestas a los mismos y de vulnerabilidades reportadas de seguridad de la información, así como de las tendencias a lo largo del tiempo.

9.2 Análisis forense adicional sobre la seguridad de la información

Puede ocurrir que una vez que un incidente se haya resuelto todavía sea necesario un análisis forense de seguridad de la información para identificar evidencias. El ERISI debe conducir este análisis utilizando las mismas herramientas y procedimientos sufridos en el apartados 8.2.5.

9.3 Identificación de las lecciones aprendidas

Una vez que se ha cerrado un incidente de seguridad de la información, es importante que la organización identifique y aprenda rápidamente las lecciones obtenidas por el manejo de un incidente de seguridad de la información y se asegure de que se actúa a partir de las conclusiones, más aun, puede haber lecciones que aprender a partir de la evaluación y resolución de vulnerabilidades de seguridad de la información reportadas. Las lecciones pueden estar en términos de lo siguientes:

a) Requisitos nuevos o cambiados para los controles de seguridad de la información. Estos pueden ser controles técnicos o no técnicos (incluyendo físicos). Dependiendo de las lecciones aprendidas, estos pueden incluir la necesidad de una rápida actualización del material y entrega del mismo para las explicaciones de

concientización de seguridad (para usuarios y otro personal), y una rápida revisión, así como emisión de lineamientos y / o normas de seguridad.

b) Información nueva o cambiada sobre amenazas y vulnerabilidades y, por lo tanto, cambios a la evaluación de riesgos de seguridad de la información existente en la organización y a los resultados de la revisión de la gerencia.

c) Cambios al esquema de gestión de incidentes de seguridad de la información y sus procesos, procedimientos, formatos de reporte y / o estructura organizativa, así como la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información.

Una organización debe proyectarse más allá de un incidente o vulnerabilidad única de seguridad de la información y verificar si hay tendencias/patrones que puedan ayudar por sí mismas a identificar la necesidad de controles o de cambios de enfoque. También es sensato practicar, luego de un incidente de seguridad de la información orientado a la TI, la conducción de pruebas de seguridad de la información, particularmente una evaluación de vulnerabilidades. Así, una organización debe analizar los datos en la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información de manera regular para hacer lo siguiente:

a) identificar tendencias/patrones,

b) identificar áreas de preocupación, y

c) analizar dónde puede tomarse acción preventiva para reducir la probabilidad de futuros incidentes.

Se debe canalizar la información relevante adquirida a través del curso de un incidente de seguridad de la información dentro del análisis de tendencias/patrones (similarmente a la manera en que se maneja las vulnerabilidades de seguridad de la información reportadas). Contribuye significativamente la identificación temprana de incidentes de seguridad de la información y provee una advertencia de qué otros incidentes de seguridad de la información pueden surgir en base a la experiencia previa y al conocimiento documentado.

También se debe utilizar el incidente de seguridad de la información y la información sobre la vulnerabilidad relacionada que se recibe del gobierno, ERISI comerciales y proveedores.

Las pruebas de evaluación / seguridad de vulnerabilidades de un sistema, servicio y / o red de información que siguen a un incidente de seguridad de la información no deben consignarse solamente al sistema, servicio y / o red de información afectados por el incidente de seguridad de la información. Debe expandirse para incluir cualquier sistema, servicios y / o red de información relacionados. Una evaluación completa de la vulnerabilidad se utiliza para destacar la existencia de las vulnerabilidades explotadas durante el incidente de seguridad de la información sobre otros sistemas y / o servicios o redes de información y para asegurar que no se introduzcan nuevas vulnerabilidades.

Es importante enfatizar que las evaluaciones de vulnerabilidad deben conducirse regularmente y que la reevaluación de vulnerabilidades luego de que haya ocurrido un incidente de seguridad de la información debería ser parte de este proceso de evaluación continua y no un reemplazo.

Debe producirse análisis resumidos de incidentes y vulnerabilidades de seguridad de la información para presentarlos en cada reunión del foro de seguridad de la información de la gerencia de la organización y/u otro foro definido en la política general de seguridad de la información de la organización.

9.4 Identificar y hacer mejoras a la implementación del control de seguridad de la información

Durante la revisión, luego de que uno o más incidentes de seguridad de la información hayan sido resueltos, se puede identificar controles, la necesidad de tener nuevos controles o de cambiarlos. Las recomendaciones y necesidades de control relacionadas pueden ser no factibles de implementar inmediatamente ya sea financiera u operativamente, en cuyo caso deben aparecer en los objetivos de más largo plazo de la organización. Por ejemplo la migración a un firewall robusto más seguro puede ser no factible financieramente en el corto plazo, pero debe incluirse en las metas de seguridad de la información de largo plazo de la organización.

Según las recomendaciones acordadas, la organización debe implementar los controles actualizados y / o nuevos. Estos pueden ser técnicos (incluyendo físicos) y pueden incluir la necesidad de actualizaciones y entregas rápidas del material para las explicaciones de concientización sobre la seguridad (para los usuarios y otro personal) así como la revisión y emisión rápida de lineamientos y / o normas de seguridad. Además, los sistemas, servicios y / o redes de información de una organización pueden estar sujetos a evaluaciones de vulnerabilidad regulares para ayudar en la identificación de

vulnerabilidades y proporcionar un proceso de fortalecimiento continuo de los sistemas/servicios/redes.

Además, mientras que los procedimientos y documentación relacionados a las revisiones de seguridad de la información pueden realizarse inmediatamente después de tratar un incidente de seguridad de la información o de una vulnerabilidad, es más probable que esto se requiera como una respuesta posterior. Luego de tratar un incidente de seguridad de la información o una vulnerabilidad, si es relevante, una organización debe actualizar las políticas y procedimientos de seguridad de la información que ha recogido para revisar y cualquier asunto problemático identificado durante el curso del proceso de gestión del incidente. Debe ser un objetivo de largo plazo del ERISI, junto con el gerente de seguridad de la información de la organización el asegurar que estas actualizaciones a las políticas y procedimientos de seguridad de la información se propaguen a toda la organización.

9.5 Identificar y hacer mejoras a la evaluación del riesgo de seguridad de la información y a los resultados de revisión de las gerencias

Dependiendo de la seriedad y del impacto de un incidente de seguridad de la información (o de las severidad y potencial impacto relacionado a una vulnerabilidad de seguridad de la información reportada), puede ser necesario hacer un estudio de las evaluaciones de riesgos de seguridad de la información y de los resultados de revisión de las gerencias para tomar en cuenta nuevas amenazas y vulnerabilidades. Como seguimiento a la culminación de una revisión actualizada de la evaluación del riesgo de seguridad de la información y de la gerencia, puede ser necesario introducir controles nuevos o cambiados (véase el apartado 9.4).

9.6 Identificar y hacer mejoras al esquema de gestión de incidentes de seguridad de la información

Luego de la resolución de un incidente, el gerente del ERISI, o alguien designado, debe revisar todo lo que ha ocurrido para evaluar y anticipar así la eficacia de la respuesta íntegra a un incidente de seguridad de la información. Un análisis así tiene por objetivo determinar qué partes del esquema de gestión de incidentes de seguridad de la información funcionaron exitosamente e identificar si se requiere alguna mejora.

Un aspecto importante del análisis posterior a la respuesta es alimentar información y conocimiento al esquema de gestión de incidentes de seguridad de la información. Si es de

suficiente gravedad, una organización debe asegurar que se programe una reunión de todas las partes relevantes poco tiempo después del tratamiento de un incidente mientras que el tratamiento esta todavía fresco en las mentes de las personas. Los factores a considerar en una reunión como esta incluyen lo siguiente:

a) ¿Los procedimientos descritos en el esquema de gestión de seguridad de la información funcionan como se supone que deben funcionar?

b) ¿Hay algún procedimiento o método que habría ayudado a la detección del incidente?

c) ¿Se identificó algún procedimiento que podría haber sido de ayuda en el proceso de respuesta?

d) ¿Hubo algún procedimiento que podría haber ayudado para recuperar los sistemas de información del incidente identificado?

e) ¿La comunicación del incidente a todas las partes relevantes fue eficaz a lo largo de la detección, reporte y respuesta?

Deberían documentarse los resultados de la reunión. La organización debería asegurar que las áreas identificadas para mejorar el esquema de gestión de incidentes de seguridad de la información sean realizadas y se justifique los cambios incorporados en una actualización de la documentación del esquema. Los cambios a los procedimientos y formularios del reporte de gestión de incidentes de seguridad de la información deberían estar sujetos a una verificación y pruebas exhaustivas antes de aplicarse.

9.7 Otras mejoras

Se puede haber ido identificado otras mejoras durante la fase de lecciones aprendidas, por ejemplo cambios en las políticas, normas y procedimientos de seguridad de la información y cambios a las configuraciones de hardware y software de TI. La organización debe asegurar que éstas se accionen.

ANEXO A
(INFORMATIVO)

TABLA DE REFERENCIAS CRUZADAS DE ISO/IEC 27001 VS ISO/IEC 27035

ISO/IEC 27001:2005 Apartados	ISO/IEC 27035 Apartados
4.2.2 Implementar y operar el SGSI La organización debe hacer lo siguiente: h) Implementar procedimientos y otros controles capaces de permitir la pronta detección de eventos de seguridad y respuesta a los incidentes de seguridad.	4 (Revisión) para la revisión de la implementación de la gestión de incidentes de seguridad de la información. 5 (Planear y preparar) – el contenido podría ayudar a implementar la gestión de incidentes de seguridad de la información. 6 (Detección y reporte), 7(Evaluación y decisión), 8 (Respuestas) y 9 (Lecciones aprendidas) – el contenido podría ayudar a operar la gestión de incidentes de seguridad de la información.
4.2.3 Monitorear y revisar el SGSI La organización deberá hacer lo siguiente: a) Ejecutar procedimientos de monitoreo de revisión y otros controles: 2) identificar prontamente rupturas e incidentes intentados y exitosos contra la seguridad; 4) ayudar a detectar eventos de seguridad y con ello prevenir incidentes de seguridad por medio del uso de indicadores. b) Realizar revisiones regulares de la eficacia del SGSI (incluyendo el cumplimiento con las políticas y objetivos del SGSI y la revisión de los controles de seguridad) tomando en cuenta los resultados de las auditorías de seguridad, los incidentes, las mediciones de eficacia, las sugerencias y la retroalimentación de todas las partes interesadas.	9 (Lecciones aprendidas) – el contenido podría ayudar a monitorear y revisar la gestión de incidentes de seguridad de la información.
4.3.3 Control de registros Se debe mantener los registros de desempeño del proceso tal como se describe en 4.2 y de todas las ocurrencias significativas de incidentes de seguridad relacionadas al SGSI	5.1 (Revisión de actividades clave), 6 (Detección y reporte) y Anexo D (Ejemplo de Informes y Formularios sobre Eventos, Incidentes y Vulnerabilidades de Seguridad de la Información) – el contenido podría ayudar a definir el alcance de los servicios.
13 Gestión de incidentes de seguridad de la información	4 (Revisión) para la revisión de la implementación de la gestión de incidentes de seguridad de la información. 5 (Planear y preparar) – el contenido podría ayudar a implementar la gestión de incidentes de seguridad de la información.

ISO/IEC 27001:2005 Apartados	ISO/IEC 27035 Apartados
A.13.1 Reporte de eventos y vulnerabilidades de seguridad de la información Objetivo: Asegurar que se comunique sobre eventos y vulnerabilidades de seguridad de la información asociados con los sistemas de información de manera que se permita tomar una acción correctiva oportuna. Deben existir procedimientos formales de reporte y escalamiento de los eventos. Se debe hacer consciente a todos los empleados, contratistas y usuarios de terceros de los procedimientos para reportar los distintos tipos de eventos y vulnerabilidades que pueden tener un impacto en la seguridad de los activos de la organización. Se les debe felicitar por que informen cualquier evento y vulnerabilidad de seguridad de la información tan rápido como sea posible al PdC designado.	5 (Planear y preparar) (en particular, véase 5.4 Esquema de Gestión de Incidentes de Seguridad de la Información, 5.5 Establecimiento del ERISI, 5.6 Apoyo Técnico y de otro tipo, 5.7 Concientización y Capacitación, y 5.8 Pruebas del Esquema), 6 (Detección y Reporte), Anexos C (Ejemplo de Enfoques Respecto de la Categorización y Clasificación de Eventos e Incidentes de Seguridad de la Información) y Anexo D (Ejemplo de Reportes y Formularios sobre Eventos, Incidentes y Vulnerabilidades de Seguridad de la Información) – el contenido podría ayudar a reportar eventos y vulnerabilidades de seguridad de la información.
A.13.1. 1 Reporte de eventos de seguridad de la información Control: Se debe reportar los eventos de seguridad de la información a través de canales de gestión apropiados tan rápido como sea posible.	Anexo D.2.1 (Ejemplos de rubros del registro de eventos de seguridad de la información) y Anexo D.4.1 (Ejemplos de formulario de reporte de eventos de seguridad de la información) para el ejemplo del formulario de reporte.
A.13.1.2 Reporte de vulnerabilidades de seguridad Control: Se debe solicitar a todos los empleados, contratistas y usuarios de cajeros de sistemas y servicios de información que anoten y reporten cualquier vulnerabilidad observada o sospechada de la seguridad en los sistemas o servicios.	Anexo D.2.3 (Ejemplos de rubros del registro de vulnerabilidad de seguridad de la información) y Anexo D.4.3 (Ejemplos de formulario de reporte de vulnerabilidad de seguridad de la información) para el ejemplo del formulario del reporte.
A.13.2 Gestión de incidentes de seguridad de la información y mejoras Objetivo: Para asegurar que se aplica un enfoque consistente y eficaz a la gestión de incidentes de seguridad de la información. Deben existir responsabilidades y procedimientos para manejar los eventos y vulnerabilidades de seguridad de la información de manera eficaz una vez que se han reportado. Se debe aplicar un proceso de mejora continua a la respuesta a, monitoreo de, evaluación de y gestión general de incidentes de seguridad de la información.	7 (Evaluación y Decisión), 8 (Respuesta), y 9 (Lecciones aprendidas) y Anexo B (Ejemplo de Incidentes de Seguridad de la Información y sus Causas), Anexo C (Ejemplo de Enfoques a la Categorización y Clasificación de Eventos de Incidentes de Seguridad de la Información) y Anexo E (Aspectos Legales y Regulatorios).
Donde se requiera evidencia, se la debe reunir para asegurar el cumplimiento de los requisitos legales. **A.13.2.1 Responsabilidades y procedimientos** Control: Se debe establecer responsabilidades y procedimientos gerenciales para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	7 (Evaluación y decisión), 8 (Respuestas), Anexo D.2.2 (Ejemplo Rubros del Registros de Incidentes de Seguridad de la Información) y Anexo D.4.2 (Ejemplo de Formulario para el Reporte de Incidentes de Seguridad de la Información) – el contenido podría ayudar a definir las responsabilidades y procedimientos.

ISO / IEC 27001:2005 Apartados	ISO/IEC 27035 Apartados
A.13.2.2 Aprendizaje a partir de incidentes de seguridad de la información Control: deben existir mecanismos para permitir que se anticipe y monitoree los tipos, volúmenes y costos de los incidentes de seguridad de la información. **A.13.2.3 Recolección de evidencia** Control: una acción de seguimiento contra una persona u organización luego de un incidente de seguridad de la información involucre una acción legal (ya sea civil o penal), se debe reunir, retener y presentar evidencia conforme a las reglas para someter evidencia en la(s) jurisdicción(es) relevante(s).	9 (Lecciones aprendidas) y Anexo B (Ejemplo de Incidentes de Seguridad de la Información y sus Causas) y Anexo C (Ejemplo de Enfoques a la Categorización y Clasificación de Eventos e Incidentes de Seguridad de la Información) – el contenido podría ayudar a aprender de los incidentes de seguridad de la información. 7 (Evaluación de decisión), 8 (Respuestas) (en particular véase el apartado 8.2.5 Análisis Forense de Seguridad de la Información) y Anexo E (Aspectos Legales y Reglamentarios) – el contenido podría ayudar a definir los procedimientos para recolectar evidencia.

ANEXO B
(INFORMATIVO)

EJEMPLOS DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y SUS CAUSAS

B.1 Ataques

B.1.1 Denegación de Servicios

La Denegación de Servicio (DoS) y la Denegación Distribuida de Servicio (DDoS) son categorías amplias de incidentes con un hilo común. Estos incidentes hacen que un sistema, servicio o red no pueda continuar operando según la capacidad que debería tener, sobre todo con una denegación completa del acceso a los usuarios legítimos. Existen dos tipos principales de incidentes DoS/DDoS causados por medios técnicos: eliminación de recursos e inanición de recursos.

Algunos ejemplos típicos de incidentes deliberados de DoS/DDoS técnicos incluyen:

- saturar las direcciones de transmisión de las redes con paquetes de Protocolo Internet de Mensajes de Control –IPCM- para llenar el ancho de banda de la red con tráfico de respuestas,

- el envío de los datos en un formato inesperado a un sistema, servicio o red en un intento de hacerlo caer o interrumpir su operación normal,

- la apertura de sesiones autorizadas múltiples con un sistema, servicio o red particular en un intento de agotar sus recursos (por ejemplo para hacerlo más lento, cerrarlo o hacerlo caer).

Dichos ataques a menudo se realizan a través de Botnets, una colección de robots de software (código malicioso) que corren de manera autónoma y automática. Los Botnets pueden relacionarse a cientos o millones de computadoras afectadas.

Algunos incidentes de DoS técnicos pueden ser causados accidentalmente, por ejemplo causados por una mala configuración del operador o a través de la incompatibilidad de software de las aplicaciones, pero la mayoría del tiempo son deliberados. Algunos incidentes de DoS técnicos se lanzan intencionalmente para hacer caer un sistema o servicio, o para bajarse una red, mientras que otros netamente son los subproductos de otra actividad maliciosa. Por ejemplo, algunas del as técnicas más comunes de escaneo e identificación subrepticios pueden hacer que los sistemas o servicios más antiguos o mal configurados se caigan cuando se realiza el escaneo. Debe notarse que muchos incidentes deliberados de DoS técnicos a menudo se ejecutan anónimamente (es decir la fuente del ataque es 'simulada'), ya que normalmente no se basan en que el atacante reciba ninguna información de regreso de la red o del sistema que está atacando.

Los incidentes del DoS causados por medios no técnicos, resultan en pérdida de información, servicio y / o instalaciones y podrían ser causados, por ejemplo, por:

- rupturas de los arreglos de la seguridad física que resultan en hurto o daño y destrucción voluntaria de equipo,
- daño accidental al hardware (y / o su ubicación) por incendio o daño por agua/inundación,
- condiciones ambientales extremas, como altas temperaturas de operación (por ejemplo, debido a una falta del aire acondicionado),
- mal funcionamiento o sobrecarga del sistema,
- cambios incontrolados al sistema,
- mal funcionamiento del software o el hardware.

B.1.2 Acceso no autorizado

En general esta categoría de incidentes consiste de intentos no autorizados reales de acceder o utilizar mal un sistema, servicio o red. Algunos ejemplos de incidentes de acceso no autorizado estimulado técnicamente incluyen:

- intentos de encontrar archivos de claves,

- ataques la compensación del flujo de datos para intentar obtener acceso privilegiado (por ejemplo al administrador del sistema) a un blanco,

- explotación de vulnerabilidades del protocolo para secuestrar o dirigir a otro lugar las conexiones legitimas de la red,

- intentos de elevar los privilegios a los recursos o la 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 resultan en una divulgación o modificación directa o indirecta de la información, en rupturas de la rendición de cuentas o en el mal uso de los sistemas de información, podrían ser causados, por ejemplo, por:

- rupturas de los arreglos de seguridad física resultantes en un acceso no autorizado a la información,

- sistemas operativos deficientemente y / o mal configurados debido a cambios incontrolados del sistema o de mal funcionamiento de software o hardware.

B.1.3 Código malicioso

El código malicioso identifica un programa o parte de un programa insertado en otro programa con la intención de modificar su comportamiento original, normalmente para realizar actividades maliciosas como hurto de información e identidad, destrucción de información y recursos, negación de servicios, spam, etc. Los ataques de código malicioso pueden dividirse en cinco categorías: virus, gusanos, caballos troyanos, códigos móviles y combinados. Mientras que hace algunos años se creó virus para atacar cualquier sistema infectado vulnerable, hoy en día se usan los códigos maliciosos para realizar ataques con blancos. Esto se realiza a veces modificando un código malicioso existente, creando una variante que las tecnologías de detección de códigos maliciosos a menudo no reconocen.

B.1.4 Uso inapropiado

Este tipo de incidentes ocurre cuando un usuario viola las políticas de seguridad del sistema de información de una organización. Dichos incidentes no son ataques en el

sentido estricto de la palabra sino que a menudo se reportan como incidentes y deberían ser manejados por un ERISI. El uso inapropiado podría ser:

- bajar e instalar herramientas de jaqueo,
- utilizar correo electrónico corporativo para el spam o la promoción de negocios personales,
- utilizar recursos corporativos para establecer una página web no autorizada,
- utilizar actividades entre pares para adquirir o distribuir archivos pirateados (música, videos, software).

B.2 Reunión de información

En términos generales, la categoría de incidentes sobre reunión de información incluye aquellas actividades asociadas con la identificación de blancos potenciales y la inclusión de los servicios que corren sobre estos blancos. Este tipo de incidente implica el reconocimiento y su finalidad es de identificar:

- la existencia de un blanco, y comprender la topología de la red que lo rodea, así como con quién se comunica el blanco rutinariamente, y
- las vulnerabilidades potenciales o su entorno de red inmediato que podrían explotarse.

Los ejemplos típicos de ataques de reunión de información por medios técnicos incluyen:

- eliminación de Registros de los Sistema de Nombres de Dominio (DNS) para el dominio de Internet (transferencia de zona de DNS) del blanco,
- búsqueda por medio de pings de direcciones de red para encontrar sistemas que estén funcionando,
- sondear el sistema para identificar (por ejemplo huellas dactilares) el sistema operativo del anfitrión,

- escanear los puertos de red disponibles en un sistema para identificar los servicios relacionados (por ejemplo correo electrónico, FTP, web, etc.) y la versión del software de esos servicios,

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

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

Los incidentes de reunión de información causados por medios no técnicos resultan en:

- divulgación o modificación directa o indirecta de la información,

- hurto de propiedad intelectual almacenada electrónicamente,

- rupturas de la rendición de cuentas, por ejemplo en el registro de cuentas,

- mala utilización de sistemas de información (por ejemplo contraria a las leyes o a las políticas de la organización), esto podría ser causados por:

- rupturas de los arreglos de seguridad física resultantes en un acceso no autorizado en la información y hurto del equipo de almacenamiento de datos que contienen datos importantes, por ejemplo claves de encriptado,

- sistemas operativos deficientemente y / o mal configurados debido a cambios no controlados del sistema o al mal funcionamiento del software o hardware, lo que resulta en que el personal interno o externo adquiera acceso a información para la cual no tiene autoridad.

ANEXO C
(INFORMATIVO)

EJEMPLO DE ENFOQUE A LA CATEGORIZACIÓN Y CLASIFICACIÓN DE EVENTOS E INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

C.1 Introducción

Este anexo proporciona ejemplos de enfoques a la categorización y clasificación de incidentes de seguridad de la información. Estos enfoques permiten al personal y a las organizaciones documentar de manera consistente los incidentes de seguridad de la información de tal modo que se logre los beneficios siguientes:

- promover el intercambio y el compartir información sobre incidentes de seguridad de la información,
- hacer que sea más fácil el reporte automatizado de incidentes de seguridad de la información y las respuestas del mismo,
- mejorar la eficiencia y eficacia del manejo y gestión de incidentes de seguridad de la información,
- facilitar la recolección y análisis de datos sobre incidentes de seguridad de la información, e
- identificar los niveles de gravedad de los incidentes de seguridad de la información utilizando criterios consistentes.

Estos ejemplos de enfoques de categorización y clasificación también pueden aplicarse a los eventos de seguridad de la información, pero no cubre las vulnerabilidades de seguridad de la información.

C.2 Categorización de incidentes de seguridad de la información

Los incidentes de seguridad de la información pueden ser causados por acciones deliberadas o accidentales de los seres humanos o pueden ser causados por medios técnicos o físicos. El siguiente enfoque categoriza los incidentes de seguridad de la información considerando las amenazas como factores de categorización (Respecto de las amenazas, consultar ISO/IEC 27005:2008, Anexo C ejemplo de amenazas típicas). La tabla C.1 muestra una lista de categorías de incidentes de seguridad de la información.

TABLA C.1 – Categorías de incidentes de seguridad de la información de acuerdo con las amenazas

Categoría	Descripción	Ejemplos
Incidente de desastre natural	La pérdida de seguridad de la información es causada por desastres naturales más allá del control humano.	Terremoto, volcán, inundación, viento violento, rayo, tsunami, colapso, etc.
Incidente de agitación social	La pérdida de seguridad de la información es causada por la inestabilidad de la sociedad.	Protesta pacífica, ataque terrorista, guerra, etc.
Incidente por daño físico	La pérdida de seguridad de la información es causada por acciones físicas deliberadas accidentales.	Incendio, agua, electroestática, medioambiente abominable (como contaminación, polvo, corrosión, congelamiento), destrucción del equipo, destrucción de los medios, hurto del equipo, hurto de los medios, pérdida del equipo, pérdida de los medios, manipulación mal intencionada del equipo, manipulación mal intencionada de los medios.
Incidente por falla de la infraestructura	La pérdida de seguridad de la información es causada por las fallas de los sistemas y servicios básicos que soportan la administración de los sistemas de información.	Falla de suministro de energía, falla de la red, falla del aire acondicionado, falla del suministro de agua, etc.

TABLA C.1 (continuación)

Categoría	Descripción	Ejemplos
El incidente por perturbación de radiación	La pérdida de seguridad de la información es causada por la perturbación debida a la radiación.	Radiación electromagnética, pulso electromagnético, congestión electrónica, fluctuación de voltaje, radiación térmica, etc.
Incidente por falla técnica	La pérdida de seguridad de la información es causada por las fallas en los sistemas de información o en las instalaciones no técnicas relacionadas, así como por problemas no intencionales causados por personas, que resultan en la no disponibilidad o la destrucción de los sistemas de información.	Falla de hardware, mal funcionamiento del software, sobrecarga (que satura la capacidad de los sistemas de información), ruptura del mantenimiento, etc.
Incidente por malware	La pérdida de seguridad de la información es causada por programas maliciosos creados y difundidos deliberadamente. Un programa malicioso se inserta en los sistemas de información para dañar la confidencialidad, integridad o disponibilidad de los datos, aplicaciones o sistemas operativos, y / o afectar la operación normal de los sistemas de información.	Virus de computadora, gusano de red, caballo troyano, botnet, ataques combinados, código malicioso incrustado en página web, sitio que alberga códigos maliciosos, etc. Un virus de computadora es un conjunto de instrucciones o código para la computadora insertados en programas de cómputo. A diferencia de los programas normales, tiene una capacidad auto-replicante y conlleva normalmente un contenido que puede perturbar las operaciones de las computadoras o destruir datos. En contraste con un virus de computadora, un gusano de red es un tipo de programa malicioso que se expande y se replica automáticamente a través de las redes, explotando las vulnerabilidades de los sistemas de información en las redes. Un caballo troyano es un tipo de programa malicioso disfrazado como una función benigna en los sistemas de información y capaz de permitir que el autor controle los sistemas de información incluyendo el robo o intercepción de la información desde los sistemas. Un botnet es un grupo de computadoras afectadas (‘zombis’) en redes que el autor del botnet, al cual se le conoce como controlador o pastor de botnet, controla centralmente. Los botnets se forman infectando una masa de computadores en las redes con programas del bot. Los botnets pueden utilizarse para ataques oportunistas a las redes, para hurto de información, y para la difusión de caballos troyanos, gusanos de redes

		y otros programas maliciosos. Los ataques combinados pueden tener características combinadas de virus de computadoras, gusanos de redes, caballos troyanos o botnets y así sucesivamente. Los ataques combinados también pueden resultar a partir de la combinación de operaciones de una serie de distintos programas maliciosos. Por ejemplo, un virus de computadora o un gusano de red se introduce en un sistema de cómputo y luego instala un caballo troyano en el sistema. Un código malicioso incrustado en una página web desfigura la página web incluyendo código malicioso que instala malware en un sistema de cómputo que accede a la misma. Un sitio que alberga código malicioso hace de señuelo para que una página web albergue código malicioso que luego los usuarios objetivos descargan.

TABLA C.1 (continuación)

Categoría	Descripción	Ejemplos
Incidente por ataque técnico	La pérdida de seguridad de la información es causada por sistemas informáticos que atacan a través de redes u otros medios técnicos, ya sea explotando las vulnerabilidades de los sistemas de información en las configuraciones, protocolos o programas o, a la fuerza, lo cual resulta en una condición anormal de los sistemas de información, o en daño potencial a las operaciones actuales del sistema.	Escaneo de redes, explotación de vulnerabilidades, explotación de la puerta trasera, intentos de login, interferencia, DoS, etc. El escaneo de redes nos hace utilizar software de escaneo de redes para adquirir información sobre configuraciones de red, puertos, servicios y vulnerabilidades existentes. La explotación de vulnerabilidades explota y hace que usemos defectos de los sistemas de información en las configuraciones, protocolos o programas. La explotación de puerta falsa nos hace usar las puertas falsas o programas dañinos que se dejan en los procesos de diseño de software y hardware. Los intentos de login tratan de adivinar, romper o tomar por la fuerza las claves de acceso. La interferencia obstruye las redes de computadoras, las redes de transmisión de radio y televisión cableadas o no cableadas, o las señales satelitales de radio y televisión a través de medios técnicos. La DoS se causa por un uso excesivo de los recursos del sistema de información y de la red tales como el CPU, la memoria, el espacio de disco o el ancho de banda de la red, y afectar así la operación normal de los sistemas de información, por ejemplo, SYS-a, inundación por pings, bombardeo de correos electrónicos.
Incidente por ruptura de reglas	La pérdida de seguridad de la información es causada por la ruptura deliberada o accidental de reglas	Uso no autorizado de recursos, infracción de derechos de autor, etc. El uso no autorizado de recursos da acceso a los recursos para propósitos no autorizados, incluyendo emprendimientos que buscan lucro, por ejemplo el uso de correo electrónico para participar en cadenas de cartas ilegales para lucrar o en esquemas de pirámides. La infracción de derechos de autor se realiza vendiendo o instalando copias de un software comercial no licenciado u otros materiales protegidos, por ejemplo, warez.
Compromiso por afectación de funciones	La pérdida de seguridad de la información es causada por afectar de manera deliberada o accidental las funciones de sistemas de	Abuso de derechos, falsificación de derechos, negación de acciones, malas operaciones, ruptura de la disponibilidad del personal, etc. El abuso de derechos usa derechos más allá de los

	información en términos de la seguridad.	términos de referencia. La falsificación de derechos crea falsos derechos para engañar. La negación de acciones es cuando alguien niega lo que ha hecho. Las malas operaciones llevan a cabo operaciones incorrectamente o no intencionalmente. La ruptura de la disponibilidad del personal se causa por la falta o ausencia de recursos humanos.

TABLA C.1 (continuación)

Categoría	Descripción	Ejemplos
Incidente por afectación de la información	La pérdida de seguridad de la información es causada por afectar deliberadamente o accidentalmente la seguridad de la información tal como la confidencialidad, la integridad, la disponibilidad, etc.	Intercepción, espionaje, escucha, divulgación, mascarada, ingeniería social, phishing de redes, hurto de datos, pérdida de datos, manipulación malintencionada de los datos, errores en los datos, análisis en los flujos de datos, detección de posición, etc. La intercepción capta datos antes de que puedan llegar a los receptores legítimos. El espionaje es recolectar secretamente y reportar información sobre las actividades de otra organización. La escucha es estar oyendo la conversación externa de un tercero sin que lo sepa. La divulgación es revelar públicamente información delicada. La mascarada es cuando una entidad pretende ser otra. La ingeniería social es reunir información de una persona de manera no técnica, por ejemplo, con mentiras, engaños, sobornos o amenazas. El phishing de redes es utilizar tecnología fraudulenta de redes de computadoras para conducir a los usuarios a divulgar información importante, tal como obtener los detalles de cuentas bancarias de los usuarios y sus claves con correos engañosos. El hurto de datos es robar datos. La manipulación malintencionada de los datos es tocar o hacer cambios a los datos sin autorización. Los errores en los datos son equivocaciones que se cometen cuando se ingresa o procesa los datos. La detección de posición es detectar la posición de información o sistemas sensibles.
Incidente por contenido dañino	La pérdida de seguridad de la información es causada por propagar contenido no deseable a través de redes de información, lo cual pone en peligro la seguridad nacional, la	Contenido ilegal, contenido de pánico, contenido malicioso, contenido abusivo, etc. El contenido ilegal es contenido publicado que viola las constituciones, las leyes y reglamentos nacionales o internacionales, por ejemplo, pornografía infantil,

	estabilidad social y / o la seguridad y beneficios del público.	glorificación de la violencia, falsificación, fraude. El contenido de pánico es la discusión o comentario sensacionalizado maliciosamente sobre asuntos delicados en el Internet, lo cual resulta en eventos tales como la turbulencia social o el pánico. El contenido malicioso es la difusión de contenido que ataca maliciosamente a la sociedad o a las personas, por ejemplo, acoso o engaño. El contenido abusivo es la transmisión de contenido cuya recepción no ha sido aprobada por los receptores, por ejemplo, el spam.
Otros incidentes	No categorizados en ninguna de las categorías de incidentes anteriores.	

C.3 Clasificación de incidentes de seguridad de la información

A continuación se presentan dos ejemplos de enfoques para clasificar incidentes de seguridad de la información.

Se enfatiza que estos son ejemplos. Existen otros, tales como FIRST / Mitre Common Vulnerability Scoring System (CVSS – Sistema Común de Puntaje de Vulnerabilidad) y el Structured Warning Information Format (SWIF – Formato Estructurado de Información de Advertencias) del gobierno británico.

C.3.1 Ejemplo del enfoque 1

C.3.1.1 Factores de clasificación

C.3.1.1.1 Introducción

Este enfoque clasifica incidentes de seguridad de la información considerando los tres factores siguientes:

- importancia del sistema de información,

- pérdida de negocio,
- impacto social.

C.3.1.1.2 Importancia de los Sistemas de Información

La importancia de los sistemas de información afectados por los incidentes de seguridad de la información se determina considerando la importancia de las operaciones de negocios de la organización apoyadas por los sistemas de información. La importancia puede expresarse en relación con la seguridad nacional, el orden social, el desarrollo económico y el interés público y la dependencia que las empresas tienen respecto de los sistemas de información. Este enfoque clasifica la importancia de los sistemas de información en tres niveles amplios: sistema de información especialmente importante, sistema de información importante y sistema de información ordinario.

C.3.1.1.3 Pérdida de negocio

La pérdida de negocio de la organización causada por incidentes de seguridad de la información se determina considerando la gravedad del impacto a la interrupción del negocio debido al daño del hardware / software, de las funciones y datos de los sistemas de información. La gravedad del impacto puede depender del costo de recuperar el negocio hasta su operación normal y de otros efectos negativos de los incidentes de seguridad de la información incluyendo la pérdida de ganancia y / u oportunidad. Este enfoque clasifica la pérdida de negocio en cuatro niveles amplios: pérdida de negocio especialmente grave, pérdida de negocio grave, pérdida de negocio considerable y pérdida de negocio menor, tal como se describe a continuación.

a) Pérdida de negocio especialmente grave significaría una gran parálisis del negocio al extremo de perder la capacidad de negocio y / o daño muy serio a la confidencialidad, integridad y disponibilidad de los datos claves del negocio. Significaría un enorme costo recuperar el negocio hasta su operación normal y eliminar los efectos negativos. Una organización no podría soportar este nivel de pérdida del negocio.

b) Pérdida grave del negocio significaría interrupción de las operaciones del negocio por un largo tiempo o parálisis del negocio local al extremo de influenciar gravemente la capacidad del negocio, y / o daño serio a la confidencialidad, integridad y disponibilidad de datos clave del negocio. Significaría un alto costo

recuperar el negocio hasta su operación normal y eliminar los efectos negativos. Una organización podría soportar este nivel de pérdida del negocio.

c) Pérdida considerable del negocio significaría interrupción de las operaciones del negocio al extremo de influenciar considerablemente la capacidad del negocio, y / o daño considerable a la confidencialidad, integridad y disponibilidad de datos clave del negocio. Significaría un costo considerable recuperar el negocio hasta su operación normal y eliminar los efectos negativos. Una organización podría soportar enteramente este nivel de pérdida del negocio.

d) Pérdida menor del negocio significaría interrupción de las operaciones del negocio por un periodo corto de modo que se influencie en parte la capacidad del negocio, y / o se impacte levemente la confidencialidad, integridad y disponibilidad de datos clave del negocio. Significaría un costo menor recuperar el negocio hasta su operación normal y eliminar los efectos negativos. Una organización podría soportar enteramente este nivel de pérdida del negocio.

C.3.1.1.4 Impacto social

El impacto en la sociedad causado por incidentes de seguridad de la información se determina considerando la escala y grado del impacto sobre la seguridad nacional, el orden social, el desarrollo económico y el interés público. Este enfoque clasifica el impacto social en cuatro niveles: impacto social especialmente importante, impacto social importante, impacto social considerable e impacto social menor, tal como se describe a continuación.

I. Impacto social especialmente importante significaría efectos adversos que cubren la mayor parte de áreas de una o más provincias / estados, amenazando en gran medida la seguridad nacional, causando turbulencia social, trayendo consecuencias extremadamente adversas sobre el desarrollo económico y / o dañando seriamente el interés público.

II. Impacto social importante significaría efectos adversos que cubren la mayor parte de áreas de una o más ciudades, amenazando en gran medida la seguridad nacional, causando pánico social, trayendo consecuencias extremadamente adversas sobre el desarrollo económico y / o dañando seriamente el interés público.

III. Impacto social considerable significaría efectos adversos que cubren áreas parciales de una o más ciudades, con una amenaza limitada a la seguridad nacional,

algo de perturbación del orden social, trayendo algunas consecuencias adversas sobre el desarrollo económico y / o influenciando el interés público.

IV. Impacto social menor significaría efectos adversos en un área parcial de una ciudad, y pocas posibilidades de amenazar la seguridad nacional, el orden social, el desarrollo económico y el interés público, pero dañando los intereses de individuos, corporaciones y otras organizaciones.

C.3.1.2 Clases

C.3.1.2.1 Introducción

En base a determinados factores de clasificación, los incidentes de seguridad de la información deberían clasificarse por gravedad utilizando una escala. Dicha escala puede ser simple, como de 'mayor' a 'menor' o más detallada como:

- Emergencia: impacto grave;
- Crítico: impacto medio;
- Advertencia: impacto bajo;
- Información: ningún impacto, pero se podría utilizar el análisis para mejorar las políticas, procedimientos o controles de seguridad de la información.

De acuerdo con los factores de clasificación antes mencionados, este enfoque clasifica los incidentes de seguridad de la información en cuatro clases:

- Muy grave (Clase IV)
- Grave (Clase III)
- Menos graves (Clase II)
- Pequeño (Clase I)

Se enfatiza que la numeración en las clases de gravedad es un ejemplo. En algunos enfoques, la clase más grave está representada con el número más alto. En otros enfoques, la clase más grave está representada con el número más bajo.

C.3.1.2.2 Muy grave (Clase IV)

Los incidentes muy graves son aquellos que:

a) actúan sobre sistemas de información especialmente importantes, y

b) resultan en pérdida del negocio especialmente grave, o

c) llevan a impacto social especialmente importante.

C.3.1.2.3 Grave (Clase III)

Los incidentes graves son aquellos que:

a) actúan sobre sistemas de información especialmente importantes o sistemas de información importantes, y

b) resultan en pérdida del negocio grave, o

c) llevan a impacto social importante.

C.3.1.2.4 Menos grave (Clase II)

Los incidentes menos graves son aquellos que:

a) actúan sobre sistemas de información importantes o sistemas de información ordinarios, y

b) resultan en pérdida del negocio considerable, o

c) llevan a impacto social importante.

C.3.1.2.5 Pequeño (Clase I)

Los incidentes pequeños son aquellos que:

a) actúan sobre sistemas de información importantes u ordinarios, y

b) resultan en pérdida del negocio menor o en ninguna pérdida de negocio, y

c) llevan a impacto social leve o a ningún impacto social,

d) no se requiere ninguna acción y no hay consecuencias.

C.3.1.3 Categoría de incidentes y clase de gravedad

A menudo se relaciona la categoría de incidentes de seguridad de la información y la clase de gravedad. Una categoría de incidentes de seguridad de la información pueden tener distintas clases de gravedad dependiendo no solamente del negocio sino también de la naturaleza del incidente de seguridad de la información, como:

- intencional,
- con objetivo,
- oportunidad,
- volumen.

La tabla C.2 proporciona algunos ejemplos de categorías de incidentes de seguridad de la información que pueden tener distintas clases de gravedad dependiendo de su naturaleza.

TABLA C.2 – Ejemplos de categorías de incidentes y clase de gravedad

Clase de gravedad / Categoría del incidente	**Pequeño**	**Menos grave**	**Grave**	**Muy grave**
Ataques técnicos	Intentos fallidos	Ordinario y único (afecta a los usuarios)	Múltiples (afecta a los usuarios) importante y único (afecta a las aplicaciones y a la raíz)	Masivo (afecta a las aplicaciones y a la raíz)
Ataques técnicos		Molestia (superficial)	Perturbación (impacto en el flujo de la producción)	No disponibilidad (paro en los servicios)
Malware	Conocido y único (detectado y bloqueado por protección de antivirus)	Desconocido y único	Infecciones múltiples Infecciones de servidores	Infecciones masivas

C.3.2 Ejemplo del segundo enfoque

C.3.2.1 Introducción

Este enfoque presenta lineamientos descriptivos como ejemplos para evaluar las consecuencias adversas de los incidentes de seguridad de la información. Cada lineamiento utiliza una escala de 1 (bajo) a 10 (alto) para clasificar los incidentes de seguridad de la información. (En la práctica, se puede utilizar otras escalas, como de 1 a 5, y cada organización debe adoptar la escala que más convenga a su entorno).

Antes de leer los lineamientos a continuación, se debe explicar lo siguiente:

- En algunos lineamientos establecidos a continuación como ejemplo, se anota algunas de las entradas como “no entradas”. Esto es porque los lineamientos se formulan de tal manera que las consecuencias adversas en cada uno de los niveles ascendentes expresados en la escala de 1 a 10 son similares en general en los seis tipos que se muestran en el apartado C.3.2.2 hasta el apartado C.3.2.7. Sin embargo, en algunos de los niveles (en la escala de 1 a 10) para algunos de los tipos, se considera que no hay suficiente diferenciación en las entradas de consecuencias más

bajas inmediatas para hacer una entrada y esto se anota como “No entrada”. De manera similar, en el extremo más alto de algunos tipos se considera que no hay una consecuencia mayor que la entrada más alta mostrada, de este modo, las entradas más altas se anotan como “No entrada”. (Por lo tanto, sería lógicamente incorrecto sacar las líneas de “No entrada” y compactar la escala).

De esta manera, utilizando lo siguiente como un conjunto de ejemplos de lineamientos, cuando se consideran las consecuencias adversas de un incidente de seguridad de la información sobre el negocio de una organización, desde:

- revelación no autorizada de la información,
- modificación no autorizada de la información,
- repudio de la información,
- no disponibilidad de la información y / o servicio,
- destrucción de la información y / o servicio.

El primer paso es considerar cuál de los siguientes tipos es relevante. Para aquellos que se consideren relevantes, debería utilizarse el lineamiento tipo para establecer el impacto adverso real sobre las operaciones (o el valor) del negocio para su ingreso en el formulario de reportes de incidentes de seguridad de la información.

C.3.2.2 Pérdida financiera / Interrupción de operaciones de negocio

Las consecuencias de la revelación y modificación no autorizada, del repudio, así como de la no disponibilidad y destrucción de dicha información, pueden bien implicar una pérdida financiera, por ejemplo a partir de la reducción del precio de las acciones, por fraude o bien una infracción de contrato debido a no tomar acción o tomar acción tardíamente. Igualmente, las consecuencias –particularmente de no disponibilidad o destrucción de cualquier información- podrían ser perturbaciones a las operaciones de negocio. Rectificar y / o recuperarse de dichos incidentes requerirá invertir tiempo y esfuerzo. Esto en algunos casos será significativo y hay que considerarlo. Para usar un común denominador, el tiempo hasta la recuperación debería calcularse por unidades de tiempo del personal y convertirse a un costo financiero. Este costo se debería calcular por referencia al costo

normal de una persona al mes en el grado / nivel apropiado dentro de la organización. Se puede utilizar la siguiente pauta:

1. Resultado en pérdidas / costos financieros de x_1 o menos
2. Resultado en pérdidas / costos financieros de entre $x_1 + 1$ y x_2
3. Resultado en pérdidas / costos financieros de entre $x_2 + 1$ y x_3
4. Resultado en pérdidas / costos financieros de entre $x_3 + 1$ y x_4
5. Resultado en pérdidas / costos financieros de entre $x_4 + 1$ y x_5
6. Resultado en pérdidas / costos financieros de entre $x_5 + 1$ y x_6
7. Resultado en pérdidas / costos financieros de entre $x_6 + 1$ y x_7
8. Resultado en pérdidas / costos financieros de entre $x_7 + 1$ y x_8
9. Resultado en pérdidas / costos financieros de más de x_8
10. La organización sale del negocio

Donde x_i (i = 1,2,…, 8) representa las pérdidas / costos financieros en ocho grados / niveles, los que son determinados por la organización en su contexto.

C.3.2.3 Intereses comerciales y económicos

Se tiene que proteger la información comercial y económica y ésta se valora considerando su valor para los competidores o por el efecto que su afectación podría tener en los intereses comerciales. Se debe utilizar la siguiente pauta.

1. Ser de interés a un competidor pero sin valor comercial
2. Ser de interés a un competidor a un valor que es y_1 o menos (facturación)
3. Ser de valor a un competidor a un valor que está entre $y_1 + 1$ e y_2 (facturación), o causar pérdida financiera, o pérdida de potencial de ganancia, o facilitar ganancia inapropiada o ventaja para individuos u organizaciones, o constituir

una infracción de emprendimientos apropiados para mantener la confianza de la información proporcionada por terceros

4. Ser de valor a un competidor a un valor que está entre $y_2 + 1$ e y_3 (facturación)

5. Ser de valor a un competidor a un valor que está entre $y_3 + 1$ e y_4 (facturación)

6. Ser de valor a un competidor a un valor que es más de $y_4 + 1$ (facturación)

7. *No entrada*[1]

8. *No entrada*

9. Podría minar sustancialmente los intereses comerciales, o minar sustancialmente la viabilidad financiera de la organización

10. *No entrada*

Donde y_i (i = 1,2,…, 4) representa los valores para un competidor en términos de facturaciones en cuatro grados / niveles, los que son determinados por la organización en su contexto.

C.3.2.4 Información Personal

Allí donde se guarde y procese información sobre individuos, es moral y éticamente correcto, y ocasionalmente la ley lo exige, que se proteja la información contra revelación no autorizada, la que podría resultar en el mejor de los casos en una situación embarazosa y en el peor de los casos en acciones legales adversas, por ejemplo de acuerdo con la legislación de protección de datos. Igualmente, se requiere que la información sobre las personas sea siempre correcta, ya que la modificación no autorizada que resulta en información incorrecta podría tener efectos similares a los de la revelación no autorizada. También es importante que no se ponga a disposición ni destruya la información sobre las personas, ya que esto podría resultar en decisiones incorrectas, o que no se tome ninguna opción en el tiempo requerido, o efectos similares para revelación o modificación no autorizada. Se podría utilizar los siguientes lineamientos.

[1]La frase ‘no entrada’ significa que no hay entrada correspondiente para este nivel de impacto.

1. Ocurre una angustia menor (preocupación) para un individuo (ira, frustración, molestia) pero ninguna infracción de un requisito legal o reglamentario

2. Ocurre una angustia (preocupación) para un individuo (ira, frustración, molestia) pero ninguna infracción de un requisito legal o reglamentario

3. Ocurre una infracción en un requisito legal, reglamentario o ético o intención publicitada sobre la protección de la información que lleva a una situación embarazosa menor para un individuo.

4. Ocurre una infracción en un requisito legal, reglamentario o ético o intención publicitada sobre la protección de la información que lleva a una situación embarazosa importante para un individuo o a una situación embarazosa menor para un grupo de individuos.

5. Ocurre una infracción en un requisito legal, reglamentario o ético o intención publicitada sobre la protección de la información que lleva a una situación embarazosa grave para un individuo.

6. Ocurre una infracción en un requisito legal, reglamentario o ético o intención publicitada sobre la protección de la información que lleva a una situación embarazosa grave para un grupo de individuos.

7. *No entrada*

8. *No entrada*

9. *No entrada*

10. *No entrada*

C.3.2.5 Obligaciones legales y reglamentarias

Los datos guardados y procesados por una organización pueden estar sujetos a, o guardados y procesados para permitir que una organización cumpla con obligaciones legales y regulatorias. El no cumplimiento de dichas obligaciones, ya sea de manera intencional o no intencional, puede resultar en acciones legales o administrativas contra individuos dentro de la organización concernida. Estas acciones pueden resultar en multas y / o sentencias de prisión. Se debe utilizar los siguientes lineamientos.

1. *No entrada*

2. *No entrada*

3. Notificación de cumplimiento, proceso civil o delito penal resultante en daños financieros / penalidad de z_1 o menos

4. Notificación de cumplimiento, proceso civil o delito penal resultante en daños financieros / penalidad de entre $z_1 + 1$ y z_2

5. Notificación de cumplimiento, proceso civil o delito penal resultante en daños financieros / penalidad de entre $z_2 + 1$ y z_3 o una pena en prisión de hasta dos años.

6. Notificación de cumplimiento, proceso civil o delito penal resultante en daños financieros / penalidad de entre $z_3 + 1$ y z_4 o una pena en prisión de más de dos años y de hasta diez años.

7. Notificación de cumplimiento, proceso civil o delito penal resultante en daños financieros / penalidad una pena en prisión de más de diez años.

8. *No entrada*

9. *No entrada*

10. *No entrada*

C.3.2.6 Gestión y operaciones del negocio

La información puede ser de tal naturaleza que su afectación perjudicaría el desempeño eficaz de una organización. Por ejemplo, la información relativa a un cambio en una política puede provocar una reacción pública si se revela en la medida en que no sería posible implementar la política. La modificación, repudio o no disponibilidad de información referente a aspectos financieros, o al software de cómputo, también podría tener ramificaciones serias para la operación de una organización. Además, el repudio de los compromisos podría tener consecuencias adversas en el negocio. Se debe utilizar los siguientes lineamientos:

1. Operación ineficiente de una parte de la organización

2. *No entrada*

3. Minado de la gestión apropiada de la organización y su operación

4. *No entrada*

5. Impedimento del desarrollo efectivo o de la operación de las políticas de la organización

6. Desventaja para la organización en sus negociaciones comerciales o de política con otros.

7. Impedimento serio al desarrollo u operación de políticas organizativas importantes o cierre, o sino disrupción sustancial de operaciones importantes

8. *No entrada*

9. *No entrada*

10. *No entrada*

C.3.2.7 Pérdida de renombre comercial

La divulgación o modificación, repudio o incluso la no disponibilidad no autorizada de la información podría llevar a la pérdida de renombre comercial de una organización, con un daño resultante a su reputación, pérdida de credibilidad y otras consecuencias adversas. Se debe utilizar los siguientes lineamientos.

1. *No entrada*

2. Causa de situación embarazosa local dentro de la organización

3. Afectación adversa de las relaciones con los accionistas, clientes, proveedores, empleados, usuarios de terceros, organismos regulatorios, el gobierno, otras organizaciones o el público, lo que resulta en una publicidad local / regional adversa.

4. *No entrada*

5. Afectación adversa de las relaciones con los accionistas, clientes, proveedores, empleados, usuarios de terceros, organismos regulatorios, el gobierno, otras organizaciones o el público, lo que resulta en una publicidad adversa nacional

6. *No entrada*

7. Afectación importante de las relaciones con los accionistas, clientes, proveedores, empleados, usuarios de terceros, organismos regulatorios, el gobierno, otras organizaciones o el público, lo que resulta en una publicidad adversa generalizada

8. *No entrada*

9. *No entrada*

10. *No entrada*

ANEXO D
(INFORMATIVO)

EJEMPLO DE INFORMES Y FORMULARIOS DE EVENTOS, INCIDENTES Y VULNERABILIDAD DE SEGURIDAD DE LA INFORMACIÓN

D.1 Introducción

Este anexo contiene ejemplos de asuntos que deben registrarse para los eventos, incidentes y vulnerabilidades de seguridad de la información y ejemplos de formularios para el reporte sobre eventos, incidentes y vulnerabilidades de seguridad de la información con notas relacionadas. Se enfatiza que estos son ejemplos. Existen otros, como el Formato de Intercambio de Información sobre Objetos de Incidentes (IODEF), que es un formulario estándar.

D.2 Ejemplos de rubros en los registros

D.2.1 Ejemplos de rubro de los registros para eventos de seguridad de la información

Esto incluye información básica del evento de seguridad de la información como, por ejemplo, cuándo, qué, cómo y por qué ocurrió el evento, así como la información de contacto de la persona que reporta.

Información básica
- Fechas del evento
- Número del evento
- Números de los eventos y/o incidentes relacionados (si se aplica)

Reporte de detalles de personas
- Nombre
- Información de contacto como dirección, organización, departamento, teléfono y correo electrónico

Descripción del evento

Qué ocurrió
Cómo ocurrió
Por qué ocurrió
Puntos de listas iniciales sobre componentes/activos afectados
Impactos adversos al negocio
Cualquier vulnerabilidad identificada

Detalles de eventos
Fecha y hora en que ocurrió el evento
Fecha y hora en que se descubrió el evento
Fecha y hora en que se reportó el evento

D.2.2 Ejemplos de rubros del registro de incidentes de seguridad de la información

Esto incluye información básica del incidente de seguridad de la información como cuándo, qué, cómo y por qué ocurrió el incidente, así como la categoría e impacto del incidente, y el resultado de la respuesta al incidente.

Información básica
Fecha del incidente
Número del incidente
Números y/o incidentes relacionados (si se aplica)

Persona que reporta
Nombre
Información de contacto como dirección, organización, departamento, teléfono y correo electrónico

Miembro del punto de contacto (PdC)
Nombre
Información de contacto como dirección, organización, departamento, teléfono y correo electrónico

Detalles del miembro del ERISI
Nombre
Información de contacto como dirección, organización, departamento, teléfono y correo electrónico

Descripción del incidente
Qué ocurrió
Cómo ocurrió

Por qué ocurrió
Puntos de vista iniciales sobre los componentes/activos afectados
Impactos adversos al negocio
Cualquier vulnerabilidad identificada

Detalles de los incidentes
Fecha y hora en qué ocurrió el incidente
Fecha y hora en que se descubrió el incidente
Fecha y hora en que se reportó el incidente

Categoría del incidente
Componentes/activos afectados
Impacto adverso al negocio/ efecto del incidente
Costo total de recuperación del incidente
Resolución del incidente
Persona(s)/perpetrador(es) involucrado(s) (si el incidente es causado por personas)
Descripción del perpetrador
Motivación real o percibida
Acciones tomadas para resolver un incidente
Acciones planeadas para resolver un incidente
Acciones pendientes
Conclusión

Individuos/entidades internos notificados

Individuos/entidades externos notificados

D.2.3 Ejemplos de rubros del registro de vulnerabilidad de seguridad de la información

Esto incluye información básica de la vulnerabilidad de seguridad de la información como cuándo, qué y cómo se identificó la vulnerabilidad, así como el impacto potencial y el tratamiento de la misma.

Información básica
Fecha de la vulnerabilidad identificada
Número de la vulnerabilidad

Detalles de la persona que reporta
Nombre
Información de contacto como dirección, organización, departamento, teléfono y correo electrónico

Descripción de la vulnerabilidad
Tratamiento de la vulnerabilidad

D.3 Cómo utilizar formularios

D.3.1 Formato de fecha y hora

Las fechas deben ingresarse en el formato Año – Mes – Día (y si se requiere Hora – Minuto – Segundo). Si es relevante se debe utilizar el UTC para una comparación inmediata cuando pueden estar ocurriendo muchos eventos en diferentes husos horarios (y por lo menos mencionar la desfase que se aplica al tiempo respecto del UTC).

D.3.2 Notas para el llenado

El propósito de los formularios de reporte de eventos e incidentes de seguridad de la información es proveer información sobre un evento de seguridad de la información, y luego, si se determina que es un incidente de seguridad de la información, sobre el incidente, a las personas apropiadas.

Si se sospecha que está ocurriendo o puede haber ocurrido un evento de seguridad de la información-particularmente uno que pueda causar perdida o daños sustanciales a la propiedad o reputación de la organización, se debe llenar y presentar un formulario de reporte del evento de seguridad de la información *inmediatamente* (véase primera parte de este anexo) de acuerdo con los procedimientos descritos en el esquema de gestión de incidentes de seguridad de la información de la organización.

La información que usted provea se utilizará para iniciar la evaluación apropiada, la cual determinará si el evento debe clasificarse como un incidente de seguridad de la información o no, y si se necesita cualquier medida de solución para prevenir o limitar cualquier pérdida o daño. Dada la naturaleza potencialmente crítica respecto del tiempo en este proceso, *no es esencial llenar todos los campos en el formulario de reporte en este momento.*

Si usted es un miembro del PdC que está revisando formularios ya llenados completamente o parcialmente, entonces será necesario que usted tome una decisión respecto de si el

evento debe clasificarse como un incidente de seguridad de la información. Si se clasifica un evento de esa manera, usted debe llenar el formulario de incidentes de seguridad de la información con tanta información como pueda y pasar al ERISI tanto el formulario sobre eventos como el formulario sobre incidentes de seguridad de la información. Si el evento de seguridad de la información se clasifica como un incidente o no, se debe actualizar la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información.

Si usted es un miembro del ERISI que está revisando formularios de eventos e incidentes de seguridad de la información entregados por un miembro del PdC, entonces el formulario de incidentes debe actualizarse a medida que la investigación progrese y se haga actualizaciones relacionadas a la base de datos de eventos/incidentes/vulnerabilidades de seguridad de la información.

El propósito del formulario de reporte de vulnerabilidad de seguridad de la información es proveer información sobre una vulnerabilidad percibida y actuar como repositorio de información en torno al tratamiento solución de la vulnerabilidad reportada.

Sírvanse observar los siguientes puntos cuando se llenan los formularios:

- Se recomienda que el formulario se llene y presente electrónicamente[2] (cuando existen problemas o se considera que existen con los mecanismos de reporte electrónico (por ejemplo correo electrónico), incluyendo cuando se piensa que es posible que el sistema esté bajo ataque y los formularios electrónicos de reporte pudieran ser leídos por personas no autorizadas, entonces se debe utilizar medios alternativos de reporte. Los medios alternativos de reporte podrían incluir en persona, por teléfono o mensaje de texto).

- Proveer solamente información que usted sepa que es fáctica. No especule para llenar los campos. Donde sea necesario proveer información que usted no pueda confirmar, por favor mencione claramente que la información no está confirmada y qué lo lleva a considerar que podría ser verdadera.

- Usted debe proveer sus detalles de contacto completos. Puede ser necesario contactarlo – sea urgentemente o posteriormente para obtener mayor información respecto de su reporte.

[2] Y por ejemplo en un formulario de página web segura con enlaces a la base de datos electrónica de eventos / incidentes / vulnerabilidades de seguridad de la información. En el mundo de hoy en día, operar un esquema basado en papel tomaría mucho tiempo. Sin embargo, el esquema basado en papel es también necesario para prepararse para el caso en el que no se pueda utilizar el esquema electrónico.

Si usted descubre luego que cualquier información que usted ha proporcionado es inexacta, está incompleta o conduce a error, usted debe corregirla y volver a presentar su formulario.

D.4 Ejemplos de formularios

D.4.1 Ejemplo de formulario para el reporte de evento de seguridad de la información

Reporte de Evento de Seguridad de la Información

1. Fecha del evento	**Página 1 de 1**
2. Número del evento[3]	3. (Si se aplica) Números de identidad de eventos y / o incidentes relacionados

4. DETALLES DE LA PERSONA QUE REPORTA

4.1 Nombre	4.2 Dirección
4.3 Organización	4.4 Departamento
4.5 Teléfono	4.6 Correo Electrónico

5. DESCRIPCIÓN DEL EVENTO DE SEGURIDAD DE LA INFORMACIÓN

5.1 Descripción del evento - Qué ocurrió - Cómo ocurrió - Por qué ocurrió - Puntos de vista iniciales sobre componentes / activos afectados - Impactos adversos al negocio - Cualquier vulnerabilidad identificada

6. DETALLES DEL EVENTO DE SEGURIDAD DE LA INFORMACIÓN

6.1 Fecha y hora en que ocurrió el evento		
6.2 Fecha y hora en que se descubrió el evento		
6.3 Fecha y hora en que se reportó el evento		
6.4 ¿Está cerrada la respuesta a este evento? ***(marcar según sea apropiado)***	SÌ	NO
6.5 Si la respuesta es Sí, especificar cuánto tiempo duró el evento en días / horas / minutos		

¡

[3] Los números de eventos deben ser asignados por el Gerente del ERISI de la organización

D.4.2 Ejemplo de formulario para el reporte de incidente de seguridad de la información

Reporte de Incidente de Seguridad de la Información

1. Fecha del incidente	**Página 1 de 6**
2. Número del incidente[4]	3. (Si se aplica) Números de identidad de eventos y / o incidentes relacionados
4. DETALLES DEL MIEMBRO DEL PUNTO DE CONTACTO	
4.1 Nombre	4.2 Dirección
4.3 Organización	4.4 Departamento
4.5 Teléfono	4.6 Correo Electrónico
5. DETALLES DEL MIEMBRO DEL ERISI	
5.1 Nombre	5.2 Dirección
5.3 Organización	5.4 Departamento
5.5 Teléfono	5.6 Correo Electrónico
6. DESCRIPCIÓN DEL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN	
6.1 Descripción adicional del incidente - Qué ocurrió - Cómo ocurrió - Por qué ocurrió - Puntos de vista iniciales sobre componentes / activos afectados - Impactos adversos al negocio - Cualquier vulnerabilidad identificada	
7. DETALLES DEL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN	
7.1 Fecha y hora en que ocurrió el evento	
7.2 Fecha y hora en que se descubrió el evento	
7.3 Fecha y hora en que se reportó el evento	
7.4 Detalles de identidad / contacto de la persona que reporta	
7.5 ¿Se ha terminado el incidente? *(marcar según sea apropiado)*	**SÌ** **NO**
7.6 Si la respuesta es Sí, especificar cuánto tiempo duró el incidente en días / horas / minutos	

[4] El Gerente del ERISI de la organización debe asignar un número al incidente y enlazarlo con los números del evento asociado

Reporte de Incidente de Seguridad de la Información

8. CATEGORÍA DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

(Marcar una, luego llenar la sección relacionada abajo)	**8.1 Real** ***(el incidente ha ocurrido)***		**8.2 Sospechado** ***(se piensa que el incidente ha ocurrido pero no se ha confirmado)***	
(Marcar sólo una)	**8.3 Desastre natural**		(Indicar tipos de amenaza involucrada)	
	Terremoto	**Volcán**	**Inundación**	**Viento violento**
	Rayo	**Tsunami**	**Colapso**	**Otro**
Especificar:				
(Marcar sólo una)	**8.4 Disturbio social**			*(indicar tipos de amenaza involucrados)*
	Protesta pacífica	**Asalto terrorista**	**Guerra**	Otro
Especificar:				
(Marcar sólo una)	**8.5 Daño físico**			*(indicar tipos de amenaza involucrados)*
	Incendio	**Agua**	**Electrostático**	
	Medioambiente abominable (tal como contaminación, polvo, corrosión, congelamiento)			
	Destrucción del equipo	**Destrucción de los medios**	**Hurto del equipo**	
	Hurto de los medios	**Pérdida del equipo**	**Pérdida de los medios**	
	Manipulación malintencionada del equipo	**Manipulación malintencionada de los medios**	**Otros**	
Especificar:				
(Marcar sólo una)	**8.6 Falla de la infraestructura**			*(indicar tipos de amenaza involucrados)*
	Falla del suministro de energía	**Falla de la red**	**Falla de aire acondicionado**	
	Falla del suministro de agua	**Otro**		
Especificar:				
(Marcar sólo una)	**8.7 Perturbación por radiación**			*(indicar tipos de amenaza involucrados)*
	Radiación electromagnética	**Pulso electromagnética**	**Congestión electromagnética**	
	Fluctuación de voltaje	**Radiación térmica**	**Otro**	
Especificar:	**8.8 Falla técnica**			*(indicar tipos de amenaza involucrados)*
(Marcar sólo una)	**Falla del hardware**	**Mal funcionamiento del software**		
	Sobrecarga (saturación de la capacidad de los sistemas de información)			
	Ruptura del mantenimiento	**Otro**		
Especificar:				

Reporte de incidente de seguridad de la información

8. CATEGORÍA DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

(Marcar sólo una)	**8.9 Malware**			*(indicar tipos de amenaza involucrados)*
	Gusano de red	**Caballo troyano**	**Botnet**	**Ataques combinados**
	Página web con código malicioso subyacente		**Sitio que alberga código malicioso**	**Otro**
Especificar:				
(Marcar sólo una)	**8.10 Ataque técnico**			*(indicar tipos de amenaza involucrados)*
	Escaneo de la red	**Explotación de vulnerabilidad**	**Explotación de puerta trasera**	
	Intentos de hacer login, interferencia	**Denegación de servicio (DoS)**	**Otro**	
Especificar:				
(Marcar sólo una)	**8.11 Infracción de regla**			*(indicar tipos de amenaza involucrados)*
	Uso no autorizado de recursos	**Infracción de derechos de autor**	**Otro**	
Especificar:				
(Marcar sólo una)	**8.12 Afectación de funciones**			*(indicar tipos de amenaza involucrados)*
	Abuso de derechos	**Falsificación de derechos, negación de acciones**	**Operaciones erróneas**	
	Ruptura de disponibilidad del personal	**Otro**		
Especificar:				
(Marcar sólo una)	**8.13 Afectación de la información**			***(indicar tipos de amenaza involucrados)***
	Intercepción	**Espionaje, escucha no autorizada**	**Divulgación**	
	Mascarada, ingeniería social	**Phishing en la red**	**Hurto de datos**	
	Pérdida de datos	**Adulteración malintencionada de datos**	**Error de datos**	**Análisis del flujo de datos**
	Detección de la posición	**Otro**		
Especificar:	**8.14 Contenidos dañinos**			*(indicar tipos de amenaza involucrados)*
(Marcar sólo una)	**Contenidos ilegales**	**Contenidos de pánico**	**Contenidos maliciosos**	
	Contenidos abusivos	**Otros**		
Especificar:				
	8.15 Otros			*(Si todavía no ha establecido si el incidente pertenece a la categoría anterior, marcar aquí)*
Especificar:				

Reporte de incidente de seguridad de la información

9. COMPONENTES / ACTIVOS AFECTADOS[5]

Componentes / activos afectados *(si los hubiera)*	*(Proporcionar descripciones de los componentes / activos afectados por o relacionados al incidente, incluyendo números de serie, de licencia y de versión donde sea relevante)*
9.1 Información / Datos	
9.2 Hardware	
9.3 Software	
9.4 Comunicaciones	
9.5 Documentación	
9.6 Procesos	
9.7 Otro	

10. IMPACTO / EFECTO ADVERSO DEL INCIDENTE EN EL NEGOCIO

Para cada uno de los siguientes, indicar si es relevante en el recuadro para marcar, luego en "valor" registrar el (los) nivel(es) de impacto adverso al negocio, cubriendo a todas las partes afectadas por el incidente, en una escala de 1 a 10 utilizando los lineamientos para las categorías de: Pérdida financiera / Interrupción de las operaciones del negocio, intereses comerciales y económicos, información personal, obligaciones legales y regulatorias, operaciones de la gerencia y del negocio, y pérdida de renombre comercial. (Véase Anexo C.3.2 para revisar ejemplos). Registrar las letras del código para los lineamientos aplicables en "Lineamiento", y si se conoce los costos reales ingresarlos en "Costo"

	VALOR	**LINEAMIENTO (S)**	**COSTO**
10.1 Ruptura de confidencialidad (es decir, divulgación no autorizada)			
10.2 Ruptura de integridad (es decir, modificación no autorizada)			
10.3 Ruptura de disponibilidad (es decir, no disponibilidad)			
10.4 Ruptura de no repudiación			
10.5 Destrucción			

11. COSTOS TOTALES DE RECUPERACIÓN DEL INCIDENTE

	VALOR	**LINEAMIENTOS**	**COSTO**
(Donde sea posible, los costos reales totales de recuperación del incidente deberían mostrarse en su conjunto en "valor" utilizando la escala de 1 a 10 y en "costo" en cifras reales).			

[5] Esto es para proporcionar más detalles sobre los componentes / activos afectados que estén disponibles a medida que procede la investigación y el análisis (en las etapas tempranas del análisis de eventos e incidentes sólo se recolectará normalmente información de "alto nivel").

Reporte de incidente de seguridad de la información

12. RESOLUCIÓN DEL INCIDENTE

12.1 Fecha de inicio de investigación del incidente	
12.2 Nombre (s) del (de los) investigador (s) del incidente	
12.3 Fecha final del incidente	
12.4 Fecha final del impacto	
12.5 Fecha de culminación de la investigación del incidente	
12.6 Referencia y ubicación del reporte de investigación	

13. (SI EL INCIDENTE FUE CAUSADO POR PERSONA(S) LA(S) PERSONA(S) / PERPETRADOR(ES) INVOLUCRADO(A)(AS)

(Marcar sólo una)

Persona	**Institución / Organización establecida legalmente**
Grupo organizado	**Accidente**
	No perpetrador ***Por ejemplo: elementos naturales, falla de equipos, error humano***

14. DESCRIPCIÓN DEL PERPETRADOR

15. MOTIVACIÓN REAL O PERCIBIDA

(Marcar sólo una)

Beneficio criminal / financiero	**Pasatiempo / hacking**
Política / terrorismo	**Venganza**
	Otro

Especificar:

16. ACCIONES TOMADAS PARA RESOLVER EL INCIDENTE

(Por ejemplo: 'ninguna acción', 'acción interna', 'investigación externa por…')

17. ACCIONES PLANEADAS PARA RESOLVER EL INCIDENTE

(Por ejemplo: véase ejemplos anteriores)

18. ACCIONES PENDIENTES

(por ejemplo: todavía se requiere investigación por parte de otro miembro del personal)

Informe de incidente de seguridad de la información

Página 6 de 6

19. CONCLUSIÓN

(Marcar para indicar que el incidente se considera Mayor o Menor e incluir una narración corta para justificar la conclusión)

Mayor **Menor**

(Indicar cualquier otra conclusión)

20. INDIVIDUOS / ENTIDADES INTERNOS NOTIFICADOS

(Este detalle debe ser proporcionado por completo por la persona relevante con responsabilidades en torno a la seguridad de la información, estableciendo las acciones requeridas. Según sea relevante, esto puede ser ajustado por el Gerente de Seguridad de la Información de la organización u otro funcionario responsable).

Gerente / Funcionario responsable de Seguridad de la Información

Gerente del ERISI

Gerente del Sitio (indicar cuál sitio)

Gerente de Sistemas de Información

Originador del Reporte

Gerente del Originador del Reporte / Gerencia usuaria de la Línea afectada

Otro
(por ejemplo: Escritorio de Ayuda, Recursos Humanos, Gerencia, Auditoría Interna)
Especificar:

21. INDIVIDUOS / ENTIDADES EXTERNOS(AS) NOTIFICADOS(AS)

(Este detalle debe ser completado por la persona relevante con responsabilidades en torno a la seguridad de la información, estableciendo las acciones requeridas. Según sea relevante, esto puede ser ajustado por el Gerente de Seguridad de la Información de la organización u otro funcionario responsable).

Policía

Otro
(por ejemplo: Organismo regulatorio, ERISI externo)

Especificar:

21. FIRMAS

ORIGINADOR	**REVISOR**	**REVISOR**
Firma digital	**Firma digital**	**Firma digital**
Nombre	**Nombre**	**Nombre**
Cargo	**Cargo**	**Cargo**
Fecha	**Fecha**	**Fecha**

D.4.3 Ejemplo de formulario para el reporte de vulnerabilidad de seguridad de la información

Reporte de Vulnerabilidad de Seguridad de la Información

1. Fecha de la vulnerabilidad identificada		**Página 1 de 1**
2. Número de vulnerabilidad[6]		
3. DETALLES DE LA PERSONA QUE REPORTA		
3.1 Nombre	**3.2 Dirección**	
3.3 Organización	**3.4 Departamento**	
3.5 Teléfono	**3.6 Correo electrónico**	
4. DESCRIPCIÓN DE VULNERABILIDAD DE SEGURIDAD DE LA INFORMACIÓN		
4.1 Fecha y hora de la vulnerabilidad reportada		
4.2 Descripción en términos narrativos de la vulnerabilidad de seguridad de la información percibida **- Cómo se notó la vulnerabilidad** **- Características de la vulnerabilidad – físicas, técnicas, etc.** **- Si son técnicas, qué TI / componente de red / activos están concernidos** **- Componentes / Activos que podrían ser afectados si se explotara la vulnerabilidad** **- Impactos potenciales adversos al negocio si la vulnerabilidad se explotara**		
5. RESOLUCIÓN DE VULNERABILIDAD DE SEGURIDAD DE LA INFORMACIÓN		
5.1 ¿Se ha confirmado la vulnerabilidad? *(marcar según sea apropiado)*	**SÍ**	NO
5.2 Fecha y hora de confirmación de la vulnerabilidad		
5.3 Nombre de la persona que autoriza	**5.4 Dirección**	
5.5 Organización		
5.6 Teléfono	**5.7 Correo electrónico**	
5.8 ¿Se ha resuelto la vulnerabilidad? (marcar según sea apropiado)	**SÍ**	NO
5.9 Explicación de cómo se ha resuelto la vulnerabilidad de seguridad de la información con fecha y nombre de la persona que autoriza la resolución		

[6] El Gerente del ERISI de la organización debe asignar un número a la vulnerabilidad.

ANEXO E
(INFORMATIVO)

ASPECTOS LEGALES Y REGLAMENTARIOS

Los siguientes aspectos legales y reglamentarios de la sección de incidentes de seguridad de la información se deben tratar en la policía de gestión de incidentes de seguridad de la información y esquema asociado:

*** Se proporciona protección adecuada de los datos y de la privacidad de la información personal.** En aquellos países donde exista legislación específica que cubra confidencialidad e integridad de datos, a menudo se restringe al control de datos personales. Como los incidentes de seguridad normalmente tienen que atribuirse a un individuo, la información de naturaleza personal, por lo tanto, puede tener que registrarse y manejarse de manera correspondiente. Un enfoque estructurado de la gestión de incidentes de seguridad de la información requiere, en consecuencia, tomar en cuenta la protección privada apropiada. Esto puede incluir:

- aquellos individuos con acceso a los datos personales deberían, en la medida que sea práctico, no conocer personalmente a la(s) persona(s) a la(s) que se investiga.

- aquellos individuos que tengan acceso a los datos personales deben firmar contrato de no divulgación antes de que se les permita acceso a los datos.

- la información debe utilizarse solo para el propósito expreso para el que se la ha obtenido, es decir para la investigación del incidente de seguridad de la información.

*** Se mantiene apropiadamente los registros.** Algunas leyes nacionales requieren que las compañías mantengan registros apropiados de sus actividades para su revisión en el proceso de auditoría anual de la organización. Existen similares requisitos respecto de las realizaciones gubernamentales. En algunos países, se requiere que las organizaciones informen o generen archivos para las fuerzas de la ley (por ejemplo respecto a cualquier caso que involucre un delito serio o penetración de un sistema comprometedor del gobierno).

*** Existen controles para asegurar el cumplimiento de las obligaciones contractuales comerciales.** Allí donde haya requisitos vinculantes sobre la provisión de un servicio de gestión de incidentes de seguridad de la información, por ejemplo cubriendo los tiempos de respuesta requeridos, una organización debe asegurar que se provea seguridad de la información apropiada de modo que se pueda cumplir con dichas obligaciones en todas las circunstancias. (En relación con esto, si una organización contrata a una parte externa para recibir apoyo, por ejemplo un ERISI externo, entonces debe asegurarse de que se incluya todos los requisitos incluyendo los tiempos de respuesta, en el contrato con la parte externa).

*** Se trata los asuntos legales relacionados con políticas y procedimientos.** Las políticas y procedimientos asociadas con el esquema de la gestión de incidentes de seguridad de la información debe verificarse respecto de asuntos potenciales legales y reglamentarios, por ejemplos si existen afirmaciones sobre una acción disciplinaria y/o legal tomada contra aquellos que causan incidentes de seguridad de la información. En algunos países no es fácil despedir a las personas de sus empleos.

*** Se verifica la validez legal de los descargos.** Todos los descargos respecto de acciones tomadas por el equipo de gestión de incidentes de información y cualquier personal de apoyo externo deben verificarse respecto de su validez legal.

*** Los contratos con el personal de apoyo externo cubren todos los aspectos requeridos.** Los contratos con cualquier personal de apoyo externo, por ejemplo de un ERISI externo, deben verificarse exhaustivamente respecto de descargos de responsabilidad, de no divulgación, de disponibilidad del servicio y de las implicaciones de los consejos equivocados.

*** Los contratos de no divulgación son exigibles.** Los miembros del equipo de gestión de incidentes de seguridad de la información pueden tener que firmar contratos de no divulgación tanto al inicio como al final de su empleo. En algunos países, el haber firmado un contrato de no divulgación puede no ser exigible por ley. Esto debe verificarse.

*** Se tratan los requisitos de las fuerzas de la ley**. Los asuntos asociados con la posibilidad de que agencias de las fuerzas de la ley puedan solicitar legalmente información de un esquema de gestión de incidentes de seguridad de la información tienen que ser claros. Puede ser el caso que se requiera claridad sobre el nivel mínimo exigido por la ley en el cual debe documentarse los incidentes y sobre el tiempo durante el cual se debe retener dicha documentación.

*** Los aspectos de responsabilidad son claros.** Se debe aclarar los asuntos de la responsabilidad potencial y de la existencia de controles relacionados a la misma. A continuación se muestra algunos ejemplos de eventos que podrían tener asuntos asociados de responsabilidad:

- Si un incidente pudiera afectar a otra organización (por ejemplo la divulgación de información compartida) y si no se notifica a tiempo y la otra organización sufre impacto adverso.
- Si se descubre una nueva vulnerabilidad en un producto y no se notifica al proveedor y ocurre un incidente relacionado importante más adelante con un impacto mayor sobre una o más organizaciones.

- No se hace un informe donde, en el país en particular, las organizaciones tienen obligación de informar y generar archivos para las agencias de las fuerzas de la ley respecto de cualquier caso que pueda involucrar un delito serio, o penetración de un sistema gubernamental comprometedor o parte de la infraestructura nacional crucial.

- Se divulga información que parece indicar que alguien o una organización puede estar involucrado en un ataque. Esto podría dañar la reputación y el negocio de la persona u organización involucrada.

- Se divulga información de que puede haber un problema con un artículo de software en particular y se encuentra que esto no es cierto.

*** Se trata los requisitos reglamentarios específicos.** Cuando sea necesario debido a requisitos reglamentarios específicos, se debe reportar los incidentes a un organismo designado, por ejemplo tal como se exige en la industria de la energía nuclear, de las compañías de telecomunicaciones y de los proveedores de servicios de Internet en muchos países.

*** Las acusaciones o procedimientos disciplinarios internos pueden ser exitosos**. Deben existir controles de seguridad de la información apropiados, incluyendo rastros de auditorías a prueba de adulteración malintencionada que se puedan probar, para ser capaces de acusar con éxito o presentar un procedimiento disciplinario interno contra ‘atacantes’ ya sea que los ataques sean técnicos o físicos. En apoyo de esto, será necesario reunir evidencia de tal manera que sea admisible en los tribunales nacionales de justicia u otro foro disciplinarios. Debe ser posible mostrar que:

- los registros están completos y no se los ha manipulado malintencionadamente de ningún modo.

- las copias de evidencia electrónica son probadamente idénticas a las originales.

- cualquier sistema de TI del cual se haya reunido evidencia estaba operando correctamente en el momento en que se registró la evidencia.

*** Se trata los aspectos legales asociados con las técnicas de monitoreo.** Las implicaciones de utilizar técnicas de monitoreo tienen que tratarse en el contexto de la legislación nacional relevante. La legalidad de diferentes técnicas variará de un país a otro. Por ejemplo, en algunos países, es necesario hacer que las personas sean conscientes de que se monitorea sus actividades, incluyendo las técnicas de vigilancia. Hacer que la gente sea consciente de que están ocurriendo. Los factores que hay que considerar incluyen quién /qué se está monitoreando, cómo se está(n) monitoreando, y cuándo ocurre el monitoreo. También debe notarse que el monitoreo/vigilancia en el contexto de los Sistemas de Detección de Intrusos se trata específicamente en ISO/IEC 18043.

*** Se define y comunica la política de uso aceptable.** Se debe de tener una práctica o uso aceptable dentro de la organización, y se debe documentar a todos los usuarios posibles.(Por ejemplo, los usuarios deben estar informados de la política de usos aceptables y se les debe pedir que proporcionen reconocimiento escrito de que comprenden y aceptan esa política cuando entran a trabajar en una organización o se les proporcionan acceso a los sistemas de información).