GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Gestión de incidentes y mejoras en la seguridad de la información
Tiene como objetivo el asegurar que se aplique un enfoque coherente y efectivo para la gestión de los incidentes de seguridad de la información, incluyendo la comunicación de los eventos y debilidades de seguridad.

Responsabilidades y procedimientos
Se deberían establecer responsabilidades y procedimientos de gestión para asegurarse de tener una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.

Las siguientes directrices para las responsabilidades y procedimientos de gestión relacionado con la gestión de incidentes de seguridad de la información deberían considerarse:

a) deberían establecerse responsabilidades de gestión para asegurarse de que los siguientes procedimientos sean desarrollados y comunicados adecuadamente dentro de la organización:

    1) procedimientos para la planificación y preparación de respuesta a incidentes;

    2) procedimientos para el seguimiento, detección, análisis e informe de eventos e incidentes de seguridad de la información;

    3) procedimientos para el registro en bitácora de las actividades de gestión de incidentes;

    4) procedimientos para el manejo de evidencia forense;

    5) procedimientos para la evaluación y la decisión sobre los eventos de seguridad de la información, así como la evaluación de las debilidades de seguridad de la información;

    6) procedimientos de respuesta incluyendo aquellos para el escalamiento, la recuperación controlada de un incidente y la comunicación a personas internas o externas u organizaciones;

b) los procedimientos establecidos deberían asegurar que:

    1) el personal competente maneje los asuntos relacionados con los incidentes de seguridad de la información dentro de la organización;

    2) se implemente un punto de contacto para la detección e informe de los incidentes de seguridad;

    3) se mantengan los contactos apropiados con las autoridades, los grupos de interés externos o foros que se encargan de los asuntos relacionados con los incidentes de seguridad de la información;

c) los procedimientos de presentación de informes deberían incluir:

1) la preparación de formularios de informes de eventos de seguridad de la información para apoyar la acción de informar y para ayudar a la persona que informa a recordar todas las acciones necesarias en el caso de un evento de seguridad de la información;

2) el procedimiento a ser llevado a cabo en el caso de un evento de seguridad de la información, por ejemplo, señalando inmediatamente todos los detalles, tales como tipo de incumplimiento o violación, fallas que ocurren, mensajes en la pantalla e inmediatamente reportar al punto de contacto y solamente mediante acciones coordinadas;

3) la referencia a un proceso disciplinario formal establecido para tratar con los empleados que cometen violaciones de la seguridad;

4) procesos de retroalimentación adecuados para asegurarse de que las personas que informan los eventos de seguridad de la información sean notificadas de los resultados después de que el asunto haya sido tratado y cerrado.

Los objetivos para la gestión de incidentes de seguridad de la información deberían acordarse con la dirección, y debería asegurarse de que aquellos responsables de esta gestión entiendan las prioridades de la organización para manejar incidentes de seguridad de la información.

Reporte de eventos de seguridad de la información
Los eventos de seguridad de la información deberían ser reportados a través de canales de gestión adecuados tan pronto como sea posible.

Todos los empleados y contratistas deberían ser advertidos de su responsabilidad de reportar cualquier evento de seguridad de la información lo más rápidamente posible. Deberían también conocer el procedimiento para reportar los eventos de seguridad de la información y el punto de contacto al que los eventos deberían reportarse.

Las situaciones a ser consideradas para el reporte de eventos de seguridad de la información incluyen:

a) el control inefectivo de la seguridad;

b) la violación de las expectativas de la integridad, confidencialidad y disponibilidad de la información;

c) los errores humanos;

d) los incumplimientos de las políticas o directrices;

e) las violaciones de los acuerdos de seguridad física;

f) los cambios no controlados del sistema;

g) el mal funcionamiento del software o hardware;

h) las violaciones de acceso.

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Reporte de debilidades de seguridad de la información
Los empleados y contratistas que utilizan los sistemas y servicios de información de la organización deberían estar obligados a notar y reportar cualquier debilidad observada o sospechosa de la seguridad de la información en los sistemas o servicios

Todos los empleados y contratistas deberían reportar esos asuntos al punto de contacto tan pronto como sea posible para prevenir incidentes de seguridad de la información. El mecanismo de reporte debería ser tan fácil, accesible y disponible como sea posible.

Evaluación y decisión sobre los eventos de seguridad de información
Los eventos de seguridad de la información deberían ser evaluados y se deberían decidir si serán clasificados como incidentes de seguridad de la información.

El punto de contacto debería evaluar cada evento de seguridad de la información utilizando la escala acordada de clasificación de eventos e incidentes de seguridad de la información y decidir si el evento debería ser clasificado como un incidente de seguridad de la información. La clasificación y la priorización de incidentes pueden ayudar a identificar el impacto y la extensión de un incidente.

En los casos en que la organización tenga un equipo de respuesta a incidentes de seguridad de la información (ERISI), la evaluación y la decisión pueden ser enviadas al ERISI para su confirmación o reevaluación.

Los resultados de la evaluación y la decisión deberían registrarse en detalle con el fin de futura referencia y verificación.

Respuesta a incidentes de seguridad de la información
Se debería responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados

Se debería responder a los incidentes de seguridad de la información por medio de un punto de contacto designado y otras personas pertinentes de la organización o partes externas.

La respuesta debería incluir lo siguiente:

a) la recopilación de evidencia tan pronto como sea posible después de la ocurrencia;

b) la realización de análisis forenses de seguridad de la información, según corresponda;

c) escalamiento, según corresponda;

d) asegurarse de que todas las actividades de respuesta involucradas sean registradas en una bitácora adecuadamente para su posterior análisis;

e) comunicar la existencia del incidente de seguridad de la información o cualquier detalle pertinente sobre éste a otro personal interno o externo u organizaciones que necesiten conocerlo.

f) tratar las debilidades de seguridad de la información encontradas que causen o contribuyan al incidente;

g) una vez que el incidente ha sido tratado con éxito, cerrarlo y registrarlo formalmente.

Debería realizarse un análisis post-incidente, si corresponde, para identificar el origen de éste.

Aprendiendo de los incidentes de seguridad de la información
El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de la información debería ser utilizado para reducir la posibilidad o el impacto de incidentes en el futuro.

Deberían existir mecanismos para permitir que los tipos, volúmenes y costos de los incidentes de seguridad de la información sean cuantificados y se les dé seguimiento. La información obtenida de evaluación de los incidentes de seguridad de la información debería utilizarse para identificar los incidentes recurrentes o de alto impacto.

Recolección de evidencia
La organización debería definir y aplicar procedimientos para la identificación, recopilación, adquisición y preservación de la información que puede servir como evidencia.

Deberían desarrollarse y seguirse procedimientos internos al tratar con evidencia para los propósitos de acción disciplinaria y legal.

En general, estos procedimientos de evidencia deberían proporcionar procesos de identificación, recolección, adquisición y conservación de evidencia de acuerdo con los diferentes tipos de medios, dispositivos y estado de los dispositivos, por ejemplo, encendido o apagado. Los procedimientos deberían tener en cuenta:

a) la cadena de custodia;

b) la seguridad de la evidencia;

c) la seguridad del personal;

d) las funciones y responsabilidades del personal involucrado;

e) la competencia del personal;

f) la documentación;

g) la reunión informativa.

Cuando esté disponible, debería buscarse la certificación u otros medios pertinentes de la calificación del personal y las herramientas, con el fin de fortalecer el valor de la evidencia preservada.

1) La evidencia forense puede trascender los límites organizacionales o jurisdiccionales. En tales casos, debería asegurarse de que la organización tenga derecho a recopilar la información requerida como evidencia forense. Deberían considerarse también los requisitos de las distintas jurisdicciones para maximizar las posibilidades de admisión en todas las jurisdicciones pertinentes.