PL-SGI-008
Plan de Respuesta a Incidentes

Responsables

Elaboró:	Especialista de Ciberinteligencia
Revisó:	Control de Documentos
Aprobó:	Normativa y cumplimiento

Control de versiones

Versión	Fecha	Descripción del cambio
1	22/06/2020	Emisión inicial
2	27/09/2021	Actualización del plan de acuerdo con las mejores prácticas de acuerdo con el FIRST.
3	27/09/2022	Actualización de Formato

Clave del formato de procedimiento: F-SGI-002 v3
Comentarios o dudas: sgi@silent4business.com

Contenido

1. Objetivo del plan

El objetivo de este documento es definir los procedimientos de respuesta a incidentes a seguir por Silent for Business cuando se presente un Incidente en Seguridad.
Este documento es una guía paso a paso de las medidas que deberá considerar el personal de Silent for Business como parte del ciclo de vida de los incidentes de seguridad, desde la identificación inicial hasta la restauración de las operaciones. Estos procedimientos buscan asegurar que todos incidentes de seguridad sean detectados, analizados, contenidos y erradicados; que las medidas necesarias sean tomadas para prevenir ocurrencias futuras, y que, donde sea necesario o apropiado, se de conocimiento a entidades externas y autoridades competentes, personal, o entidades afectadas.

2. Alcance

Este documento aplica principalmente a las áreas Operativas, de Ciberinteligencia, Clientes y terceras partes.
Considerando las siguientes actividades:

- Detección.
- Análisis.
- Contención.
- Erradicación.
- Recuperación.
- Actividades Post-Incidente.

3. Definiciones

Activo de información.
Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios, que, en consecuencia, debe ser protegido.

Controles de Seguridad.
Son los mecanismos implementados por la organización para mantener en los niveles establecidos por la misma, la disponibilidad, confidencialidad e integridad de la información.

Debilidad de Seguridad de la información.
Es la vulnerabilidad de que un activo pueda ser expuesto ante una amenaza, misma que podría conllevar a un incidente de seguridad de la información, en caso de no tomar las acciones pertinentes.

Evento.
Un cambio de estado significativo en un elemento de configuración, servicio o tecnología. No necesariamente implica una afectación.
Los eventos generalmente se reconocen a través de notificaciones creadas por las herramientas de monitoreo.

Evento de seguridad.
Suceso identificado en un sistema, servicio o red, que indica una posible brecha a la política de seguridad de la información, una posible explotación de una vulnerabilidad de seguridad o debilidad de seguridad, o una situación que pueda ser relevante en términos de seguridad.

Incidente.
Una ocurrencia que, real o potencialmente, pone en peligro la confidencialidad, integridad o disponibilidad de un sistema de información; o la información que el sistema procesa, almacena o transmite; o que constituye una violación o amenaza inminente de violación de las políticas, normas o procedimientos de seguridad de la organización.

Incidente de seguridad.

Incidente relacionado con la seguridad de las Tecnologías de la Información y las Comunicaciones que se produce en el Ciberespacio. Este término engloba aspectos como los ataques a sistemas TIC, el fraude electrónico, el robo de identidad, el abuso del Ciberespacio, etc.

Plan de respuesta a incidentes.

Conjunto predeterminado y ordenado de instrucciones o procedimientos para detectar, responder y limitar las consecuencias de un incidente de seguridad.

4. Responsabilidades

Rol	Responsabilidades y/o funciones
Gerente de Ciberinteligencia	• Vigilar el correcto desempeño del plan de respuesta a incidentes de acuerdo con lo planeado. • Asegurar el cumplimiento del plan de auditoría al proceso.
Cumplimiento y Mejora Contina	• Realizar las auditorías programadas para evaluar su cumplimiento e identificar oportunidades de mejora. • Mantener actualizada la documentación.
Centro de operaciones de seguridad S4B (SOC S4B)	• Recibir notificaciones de reportes de incidentes, eventos o debilidades de seguridad de la información. • Evaluar si los reportes cumplen con las características de un Incidente en Seguridad. • Registrar, clasificar y priorizar los incidentes de seguridad de la información. • Convocar a sesiones con el personal involucrado para el análisis del incidente y definición de acciones a seguir.

	• Recopilar información necesaria que sirva como evidencia para el análisis de los incidentes. • Mantener registro del seguimiento y atención de los incidentes. • Asegurar el cierre de los tickets de incidentes de seguridad
Equipo CERT	• Analizar los incidentes de Seguridad, así como de las medidas de mitigación y erradicación. • Contribuir en la recopilación de información que sirva como evidencia para el análisis de los Incidentes de Seguridad. • Documentar estado del incidente en las fases correspondientes. • Definición de acciones para detección, análisis, contención y erradicación de Incidentes de Seguridad. • Mantener informada a Dirección General sobre el desempeño del Plan.
Personal interno, terceros o clientes	• Notificar al SOC S4B de Eventos y Debilidades en Seguridad.
Área Jurídica	• Facultar la información necesaria para realizar una entrega de servicios adecuada en relación con las leyes del Estado Mexicano y acuerdos Internacionales.
Alta Dirección	• Facultar al equipo CERT para desempeñar sus funciones de acuerdo con el plan. • Facilitar los recursos necesarios para la gestión adecuada de los incidentes de seguridad.

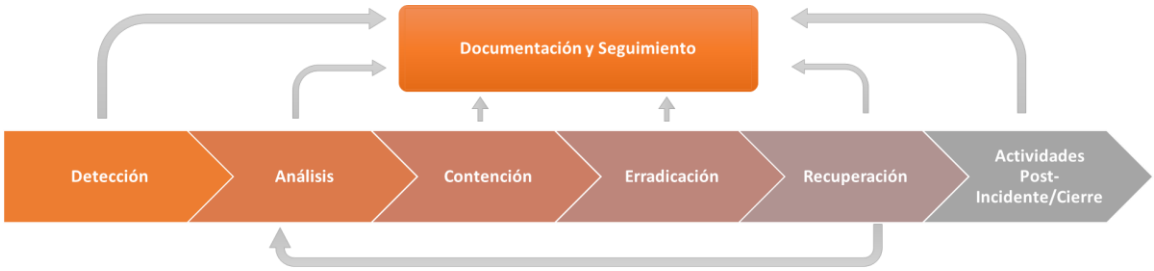

Diagrama 1

5. Descripción de Fases del Plan de Respuesta a Incidentes

1. Preparación y prevención

Al ser la llave de una respuesta a incidentes efectiva, esta fase define todos los requerimientos para una efectiva ejecución de las siguientes fases.
Se considera el plan de capacitación (interno/externo), así como en la participación en foros y conferencias, con la finalidad de mantener actualizado al equipo CERT en las normas vigentes y en el desempeño de sus funciones.

Medio de contacto con el S4B CERT

Los medios de contacto del S4B CERT son los siguientes:

Teléfono	7823 3000
Correo Electrónico	S4b.cert@silent4business.com
Redes Sociales	@silent4business (Facebook, Twitter, Linkedin)
Página de internet	Pendiente
Blog	https://silent4business.com/cyberblog/

Se podrán reportar incidentes de manera interna y externa a Silent4Business y estos deberán ser atendidos por el S4B CERT para su clasificación y atención de acuerdo al *Plan-Proceso de respuesta a incidentes P*.

2. Clasificación de incidentes

La siguiente tabla muestra la clasificación de incidentes, de acuerdo con el origen del mismo. Dicha clasificación deberá ser considerada en el reporte del incidente. Los incidentes identificados podrán entrar en uno o varios tipos y sub-tipos:

ID	Nombre	Descripción	Sub-categoría	Responsable
1	Código malicioso	Software cuyo objetivo es infiltrarse o dañar un ordenador, servidor u otro dispositivo de red, sin el conocimiento de su responsable o usuario y con finalidades muy diversas.	-Virus -Gusano -Troyano -Spyware -Adware -Ransomware -Remote Access Tool	Ciberinteligencia
2	Disponibilidad	Incidentes cuya característica es la interrupción total o parcial de un servicio o sistema, y que puede causar afectación en la productividad o la imagen de las entidades afectadas. Dichas interrupciones no deben ser derivadas de fallas técnicas, errores humanos.	-Denegación del Servicio o Denegación Distribuida del servicio DoS/DDoS -Sabotaje	Operaciones

3	Fuga de información	Incidentes en los cuales la confidencialidad de la información de la organización se ve comprometida; es decir, es accedida por personas no autorizadas.	-Mapeo o identificación de activos y vulnerabilidades (escaneo) -Sniffing -Ingeniería social -Phishing	Ciberinteligencia
4	Intrusiones	Ataques dirigidos a la explotación de una vulnerabilidad, en código o configuración, de alguna tecnología; con el fin de obtener acceso no autorizado a los sistemas de la organización.	-Cuenta de usuario comprometida -Defacement -Cross-Site Scripting (XSS) -Cross-Site Request Forgery -Inyección de SQL -Spear Phishing -Pharming -Ataque de fuerza bruta -Inyección remota de ficheros -Explotación de vulnerabilidad en hardware o software -Acceso no autorizado a la red	Operaciones / Ciberinteligencia
5	Compromiso de la información	Incidentes asociados con la afectación a la integridad (acceso, modificación, borrado) de la información de la organización.	-Acceso no autorizado -Modificación o borrado no autorizados -Publicación no autorizada -Exfiltración	Operaciones
6	Fraude	Incidentes asociados a acciones derivadas de una suplantación de identidad, en todas sus variantes	-Suplantación/Spoofing -Uso no autorizado de recursos -Uso ilegítimo de credenciales -Violación a la propiedad intelectual	Operaciones / Cumplimiento y mejora continua

7	Contenido ilegal	Incidentes derivados del uso indebido de recursos y medios para consulta, almacenamiento o distribución de contenido ilícito o indebido.	-Spam -Acoso, extorsión, mensajes ofensivos. -Pederastía, racismo, apología del delito, delitos, etc.	Operaciones / Cumplimiento y mejora continua
8	Política de seguridad	Incidentes asociados a la violación de las políticas y lineamientos que rigen la organización.	-Abuso de privilegios -Acceso no autorizado a recursos o servicios -Vulnerabilidades en los sistemas -Otros	Operaciones / Cumplimiento y mejora continua
9	Otros	Incidentes no considerados en las categorías anteriores, pero que implican una afectación a la confidencialidad, integridad o disponibilidad de la información o sistemas de la organización afectada.		Operaciones / Ciberinteligencia

Tabla 1

3. Priorización de Incidentes

La priorización de los incidentes se hará en función de los activos afectados en cada organización y/o de acuerdo con el proyecto gestionado por el CSIRT. La priorización del incidente se dará en relación con la urgencia y el impacto del incidente. La urgencia será definida por las siguientes categorías, de acuerdo con que tan apremiante es el incidente de seguridad:

Categoría	Descripción
Alto (H)	El daño causado por el incidente incrementa rápidamente Varios usuarios VIP afectados
Medio (M)	El daño causado por el incidente incrementa considerablemente en el tiempo Un solo usuario VIP es afectado
Bajo (L)	El daño causado por el incidente incrementa mínimamente en el tiempo

Tabla 2. Descripción de Categorías de Urgencia de Incidentes

El impacto se valora sobre los efectos que tiene el incidente en la organización y se categorizará de acuerdo con la siguiente tabla:

Categoría	Descripción
Alto (H)	Un número considerable de usuarios están siendo afectados y/o no pueden continuar con sus labores El daño a la reputación de la organización es alto
Medio (M)	Un número moderado de usuarios están siendo afectados y/o no están habilitados para continuar con su trabajo

	El daño a la reputación de la organización es moderado
Bajo (L)	Un número mínimo de usuarios están siendo afectados y/o están habilitados para hacer su trabajo, pero requiere atención extra El daño a la reputación de la organización es mínimo

Tabla 3. Descripción de Categorías de Impacto de Incidentes

Por lo que el impacto se mide de acuerdo con la Matriz de Prioridad de Incidentes mostrada en la Tabla 4, en donde se encuentra el código de prioridad del incidente, en relación con el impacto y la urgencia. El código de Prioridad se muestra en la Tabla 5.

Matriz de Prioridad de Incidentes		**Impacto**		
		H	**M**	**L**
Urgencia	**H**	1	2	3
	M	2	3	4
	L	3	4	5

Tabla 4. Matriz de Prioridad de Incidentes

Código de Prioridad	Descripción
1	Critico
2	Alto
3	Medio
4	Bajo
5	Muy Bajo

Tabla 5. Código de Prioridad de Incidentes

4. Matriz de Escalación

La escalación de un incidente podrá hacerse mediante correo electrónico o mediante los canales que se acuerden mediante el contrato con el cliente.

No	Rol	Correo Electrónico
1	Centro de operaciones de seguridad S4B (SOC S4B)	soc@silent4business.com
2	Equipo CERT	cert@silent4business.com
3	Gerente de Ciberinteligencia	oscar.castro@silent4business.com

3	Cumplimiento y Mejora Continua	sgi@silent4business.com

5. Plan de Comunicación Interna

- El Equipo CERT deberá asegurar que existe una comunicación abierta y ágil para garantizar que las partes relevantes sean informadas de los hechos, de sus responsabilidades, y las dudas y especulación sean disipados.
- Es importante documentar la información del Análisis Post-Incidente en el registro de los Incidentes de Seguridad; así como crear, en los casos que sean necesarios, un reporte que sea compartido con la Alta Gerencia.
- Para alcanzar los objetivos de comunicación, se podrán utilizar herramientas como correo electrónico, llamadas telefónicas, aplicaciones de mensajería instantánea, etc.

6. Plan de Comunicación Externa

- El Equipo CERT debe establecer un canal de comunicación de acuerdo con las necesidades y acuerdos pactados con los Clientes y entidades externas.
- El plan de comunicación externa debe ser comunicado internamente al Equipo CERT y a las partes interesadas para que en función de lo establecido se ejecuten las actividades con la finalidad de dar respuesta oportuna a los incidentes, tomar decisiones efectivas y mantener la información actualizada y relevante sobre los acontecimientos generados.

Cabe mencionar que se sugiere el uso de las llaves PGP, para el intercambio de información entre Equipos de Respuesta a Incidentes y/o otras entidades relacionadas.

Intercambio de información con otros CSIRTs

- La clasificación de información se hará de acuerdo con el Manual de Políticas del SGI sección 8.2 Clasificación de Información.
- Derivado de la colaboración con equipos de CSIRT y organismos internacionales (como FIRST) se podrá intercambiar información siempre y cuando esté alineado con el Manual de Políticas de SGI sección 13.2 Política de Intercambio de Información con partes externas.
- El intercambio de información con otros CSIRT se hará de acuerdo con la clasificación de la información intercambiada y el acuerdo de confidencialidad que se tenga con cada cliente.
- Se realizará el intercambio de información siempre y cuando sea justificada y el S4B CERT tenga un beneficio (técnico, comercial, entre otros) de ese intercambio.
- En caso de intercambiar información de cliente, se deberá restringir la divulgación del nombre del cliente y partes involucradas, para evitar su mal uso, a menos que el cliente autorice la divulgación de su nombre y/o marca.
- En caso de colaboración con otros CSIRTs se deberá tener un acuerdo de confidencialidad con los otros equipos para evitar la divulgación de información.
- Para CSIRTs en los que además se tenga una relación competitiva comercial se deberá consultar con la alta gerencia qué tipo de información se puede compartir en cada caso.
- El compartimiento de información se hará de acuerdo con el Manual de Políticas de SGI sección 13.2

Política de Intercambio de Información con partes externas.

Divulgación de Información del S4B CERT

Dentro de las actividades del S4B se encuentra la generación de boletines de seguridad los cuales deberán ser divulgados de acuerdo con su nivel de confidencialidad. En caso de boletines, alertas, notificaciones entre otros, se deberá utilizar el Traffic Light Protocol, el cual deberá estar debidamente identificado.
Toda la información publicada en internet, como redes sociales, página y/o blog del CERT, no deberá ser información confidencial y deberá ser TLP:WHITE.
Toda la información divulgada a clientes que esté dirigida a un sector o comunidad deberá ser TLP:GREEN
La información etiquetada como TLP:AMBER Y TLP:RED no será expuesta de manera pública, y solo se hará a través de canales autorizados por el cliente.

Traffic Light Protocol

Los destinatarios de la información tienen permitida la redistribución de información recibida de acuerdo al alcance de la enumeración “RED”, “AMBER”, “GREEN”, “WHITE”, los cuales deberán estar debidamente identificadas en el documento con los colores mostrados en la Tabla N, en letra capital y con tamaño mayor a 12 pts.

	R	G	B
TLP:RED	255	0	51
TLP:AMBER	255	192	0
TLP:GREEN	51	255	0
TLP:WHITE	255	255	255
background	0	0	0

Tabla 6. Colores RGB para TLP

Definiciones TLP

TLP:RED
No se permite su divulgación, está permitida solo a ciertos participantes.
Los receptores de la información no deben compartir la información a terceros. La divulgación de esta información puede impactar en reputación, operación y políticas de privacidad de Silent4Business y sus clientes.
La información es limitada a el destinatario.

TLP:AMBER
Divulgación limitada, restringido a individuos de organizaciones. No se permite su divulgación, está restringida solo a ciertos participantes.
Los receptores de la información no deben compartir la información a otras organizaciones.
La información es limitada a el destinatario y su organización.

TLP:GREEN
Información restringida a la comunidad, divulgación limitada. Los receptores de la información pueden compartir la información con cierta comunidad.
La información es limitada a la comunidad del destinatario.

TLP:WHITE
Divulgación de información no limitada.
Los receptores de la información pueden compartir la información a terceros. La divulgación de esta información no debe impactar en reputación, operación y políticas de privacidad de Silent4Business y sus clientes.

7. Registro de Incidentes

El sistema que se ha utilizar para el registro, almacenamiento y clasificación de incidentes de seguridad de la información es Remedy haciendo uso del módulo de incidentes de seguridad.
Esta herramienta garantiza la asignación de una clave de seguimiento para cada incidente (dependiendo de cada cliente)
Para el registro del incidente de seguridad se deberá de incluir la información siguiente:

- Persona que reporta el incidente de seguridad.
- Fecha y hora cuando se produjo el incidente.
- Que sucedió – Una sinopsis breve y concisa sobre el incidente.
- Categoría del incidente.
- Que personas estuvieron involucradas.
- Acciones inmediatas realizadas.
- Análisis y comentarios
- Estado del incidente.
- Activo.
- Prioridad
- Grupo resolutor
- Fuente reportada.
- Etapa del proceso
- Clasificación del incidente

Los estados de la herramienta de ticketing que se considerarán para cada etapa de la atención al incidente son:

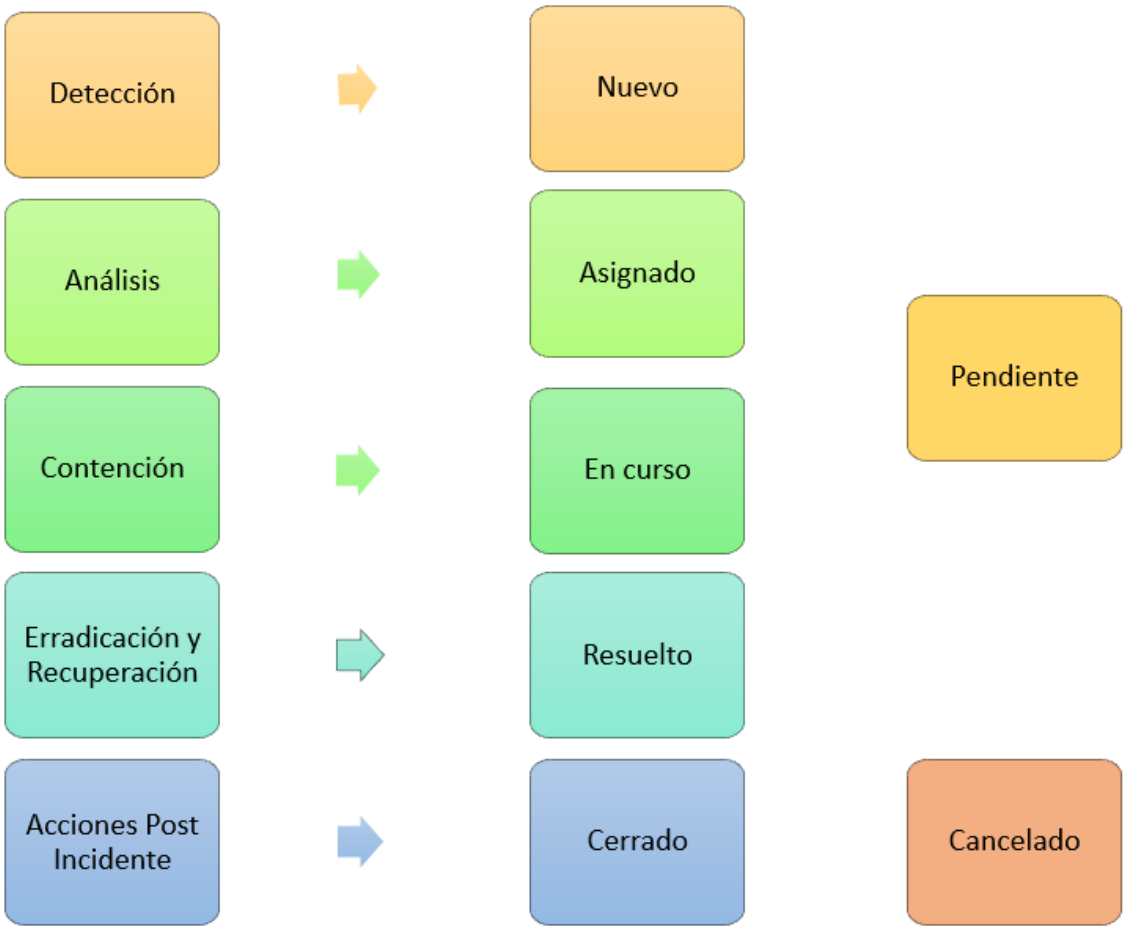

Ilustración 1. Tracking de Incidentes

Prevención

La organización deberá contar con mecanismos que contribuyan en la prevención de incidentes, por medio del control de amenazas. Dichos mecanismos podrán ser, más no están limitados a:

- Software anti-virus y anti-spam.
- Escaneos periódicos de vulnerabilidades.
- Pruebas de penetración.
- Capacitación y concientización del personal.

Detección

En la fase de detección, el Equipo CERT, o algún individuo interno o externo, identifica un Evento de Seguridad resultado de una explotación, o como resultado de un error no intencional.

Inmediatamente después de la observación o sospecha de un incidente de seguridad, el personal deberá reportar dicha sospecha al área de operaciones, por medio de los siguientes medios:

- Enviando un correo electrónico a soc@silent4business.com
- Desde el interior de las instalaciones, marcando la extensión “111”

- Desde el exterior de las instalaciones, marcando el número "+52 55 7823 3000 ext 111"

Dicho reporte no implica que el evento será tratado como un incidente, ya que el mismo será evaluado para determinar los pasos a seguir.
Un evento de Seguridad puede ser identificado de diversas formas, incluyendo las siguientes:

- Afectación a la disponibilidad, total o parcial, de los sistemas de la organización como (Página web, Remedy, intranet, Listado de sistemas y herramientas institucionales, como correo electrónico, Management Pro).
- Incumplimiento de las políticas y lineamientos de Seguridad de la información descritos en el presente documento y documentos de soporte.
- Accesos no autorizados a las instalaciones y/o áreas restringidas (Centro de cómputo, cuarto eléctrico, bodega, cuarto de telecomunicaciones) de la organización. Aquellas personas que no cuenten con una identificación de la organización y no se encuentren acompañadas por algún colaborador, deberán ser consideradas dentro de este punto.
- Modificación (afectación a la integridad) no autorizada a los sistemas de la organización.
- Daño físico o lógico a equipos e instalaciones de la organización.
- Sospecha de ejecución de código malicioso (malware) en cualquier equipo (propio o no), de la organización o externo (de algún proveedor, visitante, cliente, etc.).
- Ejecución de cualquier acto que amenace la integridad, confidencialidad o disponibilidad de cualquier recurso, físico o lógico, de la organización o de alguno de sus colaboradores, clientes, proveedores, o aliados estratégicos.

Para evaluar si un Evento de Seguridad debe ser reportado, el personal debe considerar si hay alguna de las siguientes señales:

- Información fue empleada por personal o terceros no autorizados;
- Algún dispositivo con información de la organización ha sido dañado o se ha perdido;
- Algún dispositivo con información de la organización fue sujeto de actividad no autorizada (p.ej. malware, hackeo);
- Datos personales, internos o externos, han sido expuestos públicamente

Adicionalmente, se deben considerar las siguientes circunstancias para reportar un Evento de Seguridad:

- Controles de seguridad no efectivos.
- Amenaza o afectación a la integridad, confidencialidad o disponibilidad de la información;
- Errores humanos
- Incumplimiento a las políticas o estándares;
- Violación a los controles de seguridad físicos;
- Funcionamiento inadecuado o errante del software y sistemas.

Incluso cuando el personal no esté seguro de que un Evento en Seguridad sea un Incidente de Seguridad, está obligado a reportarlo a fin de que el Equipo CERT tome las precauciones necesarias.
El Equipo CERT pedirá al individuo que reporta más información del Evento de Seguridad, que dependerá de la naturaleza de este. Dicha información deberá considerar:

- Nombre de la persona que reporta el Incidente de Seguridad, e información de contacto;
- Fecha y hora en que ocurrió el evento o en que fue identificado;

- Tipo y circunstancias en las que ocurrió el Evento de Seguridad;
- Tipo de datos, información, o equipos involucrados;
- Ubicación del Evento de Seguridad y datos o equipos afectados;
- Si el Evento de Seguridad pone en riesgo a cualquier persona o información adicional;

El Gerente de Ciberinteligencia deberá asegurarse de que el Equipo CERT sea informado de inmediato, tan pronto como la notificación es recibida. Las siguientes acciones serán ejecutadas:

1. El Equipo CERT deberá procurar y hacer lo posible para hacer un análisis inicial del Evento de Seguridad dentro de las primeras 4 horas hábiles después de la notificación o de acuerdo con los niveles de servicio establecidos por el cliente en el contrato, y decidir cómo se procederá con la fase de Análisis del Plan de Respuesta a Incidentes.
    a. La determinación debe ser rápidamente emitida, de forma que el personal pueda saber a urgencia y seriedad de la situación.

Para clientes externos, el tiempo de respuesta dependerá de los acuerdos de servicios establecidos al inicio del contrato con este último.

2. Una vez realizada la determinación de comenzar con la fase de análisis, si existe sospecha de algún daño a la reputación o responsabilidad legal para la organización, se deberá iniciar una evaluación legal de los daños reales o potenciales.

Detección automatizada

Una manera alternativa de detección es la detección automatizada. La misma podrá ser llevada a cabo por medio del uso de herramientas como: Consola de administración de antivirus, IDS, Correlacionadores, etc.
Es conveniente que se ejecuten revisiones, al menos 2 veces al año, para la definición de reglas de identificación automatizada, así como actualización de las existentes.

Análisis

La respuesta inicial a la detección de un Evento de Seguridad es la fase de análisis, en la que el SOC S4B determina si un Evento de Seguridad es un Incidente de Seguridad. Para ello, se toman en cuenta las siguientes consideraciones:

1. Recolectar información de diagnóstico para el análisis del Evento de Seguridad, utilizando herramientas propias del sistema operativo o aplicativo. Esto puede incluir, mas no está limitado a:
    a. Tomar capturas de pantalla, volcados de memoria, bitácoras de eventos y trazas de red
    b. Análisis de información proporcionada por el personal que reporta
    c. Análisis de antecedentes(precursores) e indicadores
    d. Correlacionar información
    e. Investigar información adicional (por ejemplo, motores de búsqueda en internet, bases de conocimiento)
2. Identificar si el evento de seguridad fue a causa de un error no intencional, o derivado de las acciones de un atacante. En caso de que se trate de este último escenario, se deberán iniciar acciones para identificar al atacante potencial:
    a. Validar la dirección IP del atacante
    b. Investigar al atacante en motores de búsqueda

c. Utilizando bases de datos de otros incidentes o indicadores de compromiso
d. Monitorear, en la medida de lo posible, los canales de comunicación del atacante

Validar si este incidente pudiera estar relacionado con un evento pasado (eventos correlacionados o combinados), por el cual se deberá identificar con la parte afectada mediante una entrevista. La evidencia recolectada de eventos pasados deberá estar documentada.
En caso de que el SOC S4B determine que un evento de Seguridad ha desencadenado un Incidente de Seguridad, se involucrará a los miembros del ERIS necesarios y se comenzará la documentación de la investigación y la adquisición de evidencias. Se deberá determinar la categoría del incidente, de acuerdo con lo descrito en la sección "**¡Error! No se encuentra el origen de la referencia.**".
En caso de que se determine que no ha ocurrido un incidente, se deben desencadenar las actividades definidas en la sección "Actividades Post Incidente".
El impacto potencial del Incidente de Seguridad a Silent for Business o un tercero, deberá ser evaluado desde un inicio, y el Equipo CERT deberá asignar un nivel inicial de severidad que podrá ser bajo, medio, alto o crítico. A fin de determinar el alcance, se deberá considerarlo siguiente:

1. Definir de forma inicial un nivel de severidad e impacto potencial; y confirmarlos a medida que avancen las investigaciones.
2. Identificar el o los activos afectados, sí como aquellos que podrían tener una afectación derivada del Incidente de Seguridad.
3. Estimar el efecto, actual y potencial, del Incidente de Seguridad

El Equipo CERT deberá estimar el alcance y si el Incidente de Seguridad sigue ocurriendo. La determinación de dicho alcance puede incluir la recolección de información forense de los sistemas sospechosos y la adquisición de evidencia que soporte la investigación. También se puede considerar si el incidente implica robo o destrucción de información.
Como se indicó anteriormente, el Incidente de Seguridad puede requerir la recolección de evidencia. En caso de ser así, dicha recolección se deberá ejecutar con debido cuidado y pudiendo aplicar procedimientos para lo siguiente:

1. Adquisición y manejo de evidencia (forense digital) puede incluir:
    a. Identificación de información (por ejemplo, localización, números de serie, modelos, nombre de host, dirección MAC, y dirección IP).
    b. Nombre, puesto, y datos de contacto como correo electrónico y número telefónico, de todos aquellos que hayan recolectado o manipulado la evidencia durante la investigación.
    c. Fecha y hora, incluyendo la zona horaria, de cada ocasión en que la evidencia sea manipulada.
    d. Lugares en los que la evidencia es almacenada, y condiciones del almacenamiento.
    e. Idealmente, y en medida de lo posible, se deberán crear dos respaldos del sistema afectado, utilizando medios vírgenes; de forma que uno se mantenga sellado y en resguardo como evidencia, y otro sea utilizado para la generación de otros respaldos o investigaciones.
2. A fin de asegurar que la evidencia no sea destruida o alterada, en la medida de lo posible se deberán implementar medidas de monitoreo y forense digital, y se deberán confiscar las computadoras y/o dispositivos electrónicos del personal sospechoso en la participación de un Incidente de Seguridad.
    a. Esta tarea puede realizarse de manera encubierta
    b. El Equipo CERT podrá considerar la restricción de acceso equipos y periféricos conectados, hasta el término de las labores de investigación.

3. En caso aplicable, y dependiendo de la severidad del Incidente de Seguridad, se podrá restringir el acceso y uso de:
    a. Áreas de trabajo
    b. Hardware
    c. Software
    d. Medios de almacenamiento
    e. Documentos
    f. Componentes secundarios
    g. Si un equipo se encuentra apagado, deberá ser mantenido así. Si el equipo se encuentra encendido, el Equipo CERT deberá determinar las acciones a seguir; y no deberá ser apagado sin previa determinación del Equipo CERT.
4. Es de suma importancia establecer la persona que estaba ocupando el equipo o equipos involucrados en el incidente de seguridad al momento de que ocurriera este, así como las personas que se encontraban en las inmediaciones físicas (oficinas, lugar de trabajo) o digitales (VPN, segmento de red). El ERIS deberá recolectar las bitácoras que considere relevantes para la investigación, así como registro de circuito cerrado.
5. Dependiendo de la severidad y categorización del Incidente de Seguridad, el Equipo CERT deberá notificar al personal para que tomen medidas.
6. Hasta que el Equipo CERT, previa aprobación de la alta gerencia de la Organización, den a conocer el incidente a personal ajeno al Equipo CERT, todas las actividades deben ser confidenciales.

Si se determina, durante la fase anterior, que ha ocurrido un Incidente de Seguridad que implica una brecha; y siguiendo las medidas regulatorias y legales, se deberá notificar la brecha al dueño de la información por el medio que se haya acordado con este; o vía correo electrónico para personal interno; dentro las primeras 24 horas de confirmado el incidente de seguridad y la brecha. De igual forma, se podrá iniciar las tareas definidas en la sección “Actividad post-incidente”.

Contención

Esta fase se pretende mitigar la causa raíz del Incidente de Seguridad, a fin de prevenir mayor daño o exposición. También se intenta limitar su impacto previo a la erradicación y la recuperación, por medio de la implementación de los controles que se consideren necesarios. En caso de que el Incidente de Seguridad haya sido originado de manera no intencional, la fase de erradicación podría no ser necesaria.
Una vez que se haya realizado el análisis de la información que ha sido recolectada para la investigación, el ERIS puede:

1. Asegurar el perímetro físico y de red
    a. Por ejemplo, apagando un sistema, desconectándolo o aislándolo de la red, o desactivando ciertas funcionalidades y servicios.
2. Conectarse por medio de una conexión de confianza y realizar la obtención de información volátil del sistema o sistemas afectados.
3. Determinar la integridad del sistema.
4. Si es necesario y en caso de existir, aplicar un respaldo al sistema afectado.
5. Cambiar la contraseña de acceso al sistema o sistemas afectados, notificando al personal necesario a fin de no causar conflicto.

6. Determinar si es seguro mantener las operaciones sobre los sistemas involucrados.
    a. En caso de que sea seguro mantener las operaciones sobre los activos afectados, el Equipo CERT deberá:
        i. Actualizar el registro del Incidente.
        ii. Dar paso a la fase de recuperación.
    b. En caso de que mantener la operación no sea seguro, se deberá detener el uso del activo o activos afectados, y dar paso a la fase de erradicación.
    c. El Equipo CERT podrá permitir la operación del sistema o sistemas afectados, bajo una estricta supervisión y monitoreo si:
        i. Dicha actividad contribuirá a la identificación de personas involucradas en el Incidente de Seguridad.
        ii. El sistema puede mantener su operación normal sin riesgo de daño o compromiso de información
        iii. Existe consenso del Equipo CERT para la operación del activo
7. Documentar el estado de esta fase en el Registro del Incidente

Durante las fases de análisis y contención, el Equipo CERT deberá mantener registro por medio de una cadena de custodia para asegurar que la evidencia adquirida durante el Incidente de Seguridad pueda servir ante la toma de una acción legal.

Erradicación y recuperación

La fase de erradicación es aquella en la que las vulnerabilidades que dieron origen al Incidente de Seguridad, y cualquier compromiso asociado, son eliminados el entorno. La erradicación efectiva de un ataque dirigido elimina el acceso del atacante al entorno tecnológico, coordinando acciones durante las fases de contención y erradicación.

Aunque las acciones son particulares para cada Incidente de Seguridad, el proceso de erradicación deberá considerar lo siguiente:

1. Determinar los síntomas y causas asociadas a la infraestructura afectada.
2. Eliminar los componentes que dieron origen al Incidente de Seguridad. Esto puede incluir la eliminación de malware, des habilitación de cuentas comprometidas, etc.
3. Robustecer los controles asociados a la infraestructura afectada. De ser necesario, se puede realizar un análisis de riesgos. El fortalecimiento de controles puede incluir:
    a. Robustecimiento de las defensas en el perímetro de red.
    b. Mejora en el alcance o reglas de monitoreo.
    c. Remediación de cualquier problema de seguridad en los sistemas afectados, como remoción de servicios o cuentas no utilizadas, o implementación de controles de robustecimiento.
    d. Ejecución de un análisis de vulnerabilidades, para validar que las vulnerabilidades que pueden ser explotadas han sido remediadas.
4. Si se identifican problemas o síntomas adicionales, se deberán tomar las medidas necesarias para reducir o eliminar el potencial de futuros compromisos.
5. Actualizar el Registro del Incidente, con la información de esta fase, incluyendo causas, síntomas, y métodos utilizados para resolver el problema.
6. Informar a la alta gerencia del progreso de esta fase.

Una vez que la Organización haya implementado los cambios para la erradicación, es importante verificar que las causas técnicas, así como entidades que dieron origen al incidente, son eliminados del entorno, y se han tomado las medidas disciplinarias pertinentes. Es importante que el Equipo CERT valide la efectividad de los controles y cambios implementados.

La fase de recuperación consta de las actividades ejecutadas por el Equipo CERT para restaurar los sistemas afectados o la operación después de los problemas que dieron origen al Incidente de Seguridad, así como la corrección de las consecuencias. Las acciones de recuperación dependen de cada escenario, y pueden requerir planes complejos para su efectividad.

A pesar de ello, las actividades generales que debe seguirse son:

1. Ejecución de las siguientes tareas, según corresponda:
    a. Instalación de parches
    b. Reinstalación de sistemas
    c. Restauración de sistemas desde respaldos
    d. Cambio de contraseñas de acceso
    e. Sustitución de archivos dañados por versiones limpias
2. Determinación de cambios sobre los sistemas afectados
    a. Si un sistema ha sido modificado derivado de un incidente, el mismo deberá ser restaurado a un estado funcional.
        i. Una vez restaurado, se debe validar el adecuado funcionamiento del mismo. Esto involucra a los dueños de los sistemas o de la información afectada.
        ii. Si la operación ha sido interrumpida, la misma deberá ser restaurada y validada, y el comportamiento del sistema monitoreado a fin de determinar su adecuado funcionamiento.
    b. Si el sistema no ha sido alterado, pero su operación fue interrumpida, la misma deberá ser restaurada y monitoreada, para validar su adecuado funcionamiento.
3. En caso de ser identificadas, se podrán implementar medidas adicionales de monitoreo y alertamiento, a fin de mejorar la detección automatizada de eventos similares.
4. Actualizar el registro del Incidente de Seguridad con aquellos detalles relevante de esta fase.

Actividades Post-Incidente

Adicionalmente a las tareas realizadas en las fases de análisis, y después de una adecuada validación de las actividades de contención y erradicación, el ERIS podrá ejecutar las siguientes actividades, según corresponda:

Documentación del Incidente (reportes)

Emisión de Actividades Recomendadas

Generación de boletines o avisos de seguridad en caso de que este sea de carácter prioritario para la seguridad del Sector y Nacional. En estos avisos deberán ser compartidos de acuerdo con el nivel de confidencialidad de cada cliente, y podrá solo compartirse información sobre modus operandis e indicadores de compromiso

Seguimiento y cierre

Retención y revisión de registros y documentación del Incidente de Seguridad

Es responsabilidad del Equipo CERT investigar el Incidente y realizar las actualizaciones pertinentes al Registro del Incidente de Seguridad. Durante esta etapa, el registro deberá ser revisado para asegurar:

1. La información vertida es relevante y comprobable

2. Los hallazgos están basados en evidencia concreta

- La finalidad de crear y mantener registros de Incidentes de seguridad es que las autoridades puedan ser informadas y puedan tomar acción legal en contra de aquellos individuos que causen algún Incidente. Debido a que las implicaciones de un Incidente de Seguridad no son discernibles desde el inicio, e incluso durante la ocurrencia de este, es importante que la información se encuentre documentada y los eventos y evidencia relevante sean almacenados.
- La información asociada podrá ser registrada de manera manual o electrónica; en este último escenario, es importante que se implementen medidas que garanticen la protección contra alteración o eliminación de los registros.
- Asimismo, es importante el mantenimiento y mejora continua al plan.

6. Documentos relacionados

- P-SGI-007 Proceso Ciberinteligencia