PROCEDIMIENTO DE INCIDENTES DE SEGURIDAD

1. Objetivo:

Definir las actividades para detección, reporte, gestión de incidentes de seguridad de la información y datos personales con su registro de conocimientos aprendidos.

2. Alcance:

Este procedimiento se aplica cuando se detecten durante la labor diaria un incidente de seguridad de la información que pueda o está afectando la confidencialidad, integridad, disponibilidad de la información.

3. Responsables:

El comité ISIRT y en especial el oficial de datos personales deberán seguir las actividades especificadas en este procedimiento en el manejo de los incidentes de seguridad de la información.

4. Desarrollo del procedimiento:

4.1 Las actividades a realizar en la gestión de incidentes son coordinadas por el Oficial de la seguridad de la información o datos personales:

- Supervisar los sistemas en busca de infracciones de seguridad.
- Servir como punto central de comunicación, tanto para recibir los informes de incidentes de seguridad, como para difundir información esencial sobre los incidentes a las entidades correspondientes.
- Documentar y catalogar los incidentes de seguridad.

- Aumentar el nivel de conciencia con respecto a la seguridad dentro de la compañía para ayudar a evitar que se den incidentes en la organización.

- Posibilitar la auditoría de sistemas y redes mediante procesos como la evaluación de vulnerabilidades y pruebas de penetración.

- Obtener más información sobre las nuevas vulnerabilidades y estrategias de ataque empleadas por los atacantes.

- Investigar acerca de nuevas revisiones de software.

- Analizar y desarrollar nuevas tecnologías para minimizar los riesgos y vulnerabilidades de seguridad.

- Perfeccionar y actualizar continuamente los sistemas y procedimientos actuales.

4.2. Las siguientes son las descripciones de cada una de las actividades a realizar en la gestión de un incidente de seguridad de la información.

a. Evaluación inicial

- Tomar medidas para determinar si está tratando con un incidente verdadero o un falso positivo.

- Clasificar inicialmente el incidente.

- Registrar las acciones minuciosamente.

Se deben evitar los falsos positivos siempre que sea posible; no obstante, siempre es preferible actuar sobre un falso positivo que no hacerlo sobre un verdadero incidente.

b. Comunicación del incidente

El Oficial de seguridad de la Información o datos personales, junto con las personas que se consideren necesarias, debe identificar rápidamente con quién se debe contactar. Así se garantiza que se puede mantener un control y una coordinación de incidentes adecuada, al tiempo que se minimizan los daños.

Para evitar que los atacantes estén avisados, sólo se debe informar a aquellos implicados en la respuesta a incidentes hasta que el incidente esté totalmente controlado.

c. Contención de daños y minimización de riesgos

El Oficial de seguridad de la Información o datos personales en coordinación con el área de tecnología debe actuar rápidamente para reducir los efectos reales y potenciales de un ataque, por medio de una respuesta inicial.

La siguiente es la prioridad en la ejecución de las actividades:

- Proteger la vida humana y la seguridad de las personas.
- Proteger la información restringida y confidencial.
- Proteger otra información, como datos de transacciones, sobre propiedad intelectual o del ámbito directivo.
- Proteger el hardware y software contra el ataque.
- Minimizar la interrupción de los sistemas de información (incluidos los procesos).

d. Acciones de respuesta a los incidentes

Evitar que los atacantes sepan que conocen sus actividades. Puede resultar difícil, porque algunas respuestas esenciales pueden alertar a los atacantes.

Comparar el costo de dejar sin conexión los sistemas en peligro y los sistemas relacionados con el riesgo de continuar funcionando.

Evaluar la toma de acciones legales, en caso de daños severos.

Determinar los puntos de acceso usados por el atacante e implementar las medidas adecuadas para evitar futuros accesos.

Evaluar acciones de cambio de unidades de almacenamiento y claves de acceso a los sistemas de información y dispositivos de comunicación

e. Identificación de la gravedad del ataque

Para identificar la gravedad del incidente:

- Determinar la naturaleza del ataque (puede ser diferente a lo que sugiere la evaluación inicial).
- Determinar el punto de origen del ataque
- Determinar la intención del ataque.
- Identificar los sistemas puestos en peligro.
- Identificar los archivos a los que se ha tenido acceso y determinar su grado de confidencialidad.

Se deben tener en cuenta las siguientes acciones:

- Consultar con las personas necesarias.

- Examinar los grupos clave (administradores de dominio, administradores, etc.) en busca de entradas no autorizadas.

- Buscar software de evaluación o de detección de vulnerabilidades de seguridad. A menudo, se pueden encontrar utilidades de violación en los sistemas en peligro durante la recopilación de pruebas.

- Buscar procesos o aplicaciones no autorizados en ejecución o configurados para ejecutarse usando las carpetas de inicio o las entradas del Registro.

- Buscar espacios en blanco, o la ausencia de estos, en los registros del sistema.

- Revisar los registros del sistema de detección de intrusiones en busca de signos de intrusión, qué sistemas pueden estar afectados, los métodos de ataque, el tiempo y la duración del ataque, así como el grado de los posibles daños.

- Examinar otros archivos de registro en busca de conexiones inusuales, auditorías de seguridad correctas no habituales, inicio de sesión fallidos, intentos de inicio de sesión en cuentas predeterminadas, actividad fuera del horario laboral, cambios de permisos en los archivos, directorios y recursos compartidos, y permisos de usuario elevados o cambiados.

- Comparar los sistemas con comprobaciones de integridad del sistema y los archivos realizadas con anterioridad. Esto le permite identificar las adiciones, supresiones, modificaciones del permiso y control realizadas en el sistema de archivos y el Registro. Puede ahorrar mucho tiempo al responder a los incidentes si identifica exactamente qué ha sufrido peligro y qué áreas hay que recuperar.

- Buscar datos confidenciales, que se puedan haber cambiado de ubicación o escondido para modificarlos o recuperarlos en el futuro. Comprobar si en los sistemas hay información no empresarial, copias ilegales de software y mensajes de correo electrónico u otros registros que puedan ayudar en una investigación. Determinar si se ha podido infringir la privacidad u otras leyes al buscar en un sistema durante la investigación para contactar el área jurídica.

- Comparar el rendimiento de los sistemas sospechosos con sus niveles de rendimiento de línea de base.

f. Protección de las pruebas

Se deben realizar dos copias de seguridad de los sistemas en medios no regrabables, antes de realizar cualquier acción que pueda afectar a la integridad de los datos y almacenarlas en lugares seguros. Una copia se usará para fines legales de ser necesario y la otra para recuperación de datos. Se actuará de acuerdo al procedimiento de respaldo, asegurando que la documentación del incidente quede registrada en el formato "Reporte, registro y seguimiento de incidentes".

g. Notificación a organismos externos o titulares de la información

Evaluar con las Áreas involucradas si se debe comunicar a entidades externas como: autoridades competentes locales y nacionales, Superintendencia de industria y comercio SIC, unidad de delitos informáticos de la Fiscalía General de la nación, organismos externos de seguridad y expertos en seguridad de la información incluyendo a los titulares de la información para que ellos mismos puedan adoptar las medidas necesarias para protegerse de las consecuencias de un incidente de seguridad

En ciertas circunstancias es posible que se tenga que notificar la situación a los ciudadanos y al público general, especialmente si pueden verse directamente afectados por el incidente.

En caso de tenerse la necesidad de comunicación del incidente a los medios de comunicación, solo se realizará mediante la persona autorizada para hacerlo.

h. Recuperación de los sistemas

Determinar si se puede restaurar el sistema existente dejando intacto todo lo posible, o si es necesario volver a crear completamente el sistema.

Para restaurar los datos se debe contar con las copias de seguridad limpias, realizadas antes de que ocurriera el incidente.

i. Recopilación y organización de pruebas del incidente

El Oficial de seguridad de la Información o de datos personales debe documentar minuciosamente todos los procesos al tratar con un incidente. Se debe incluir una descripción del incidente y detalles de cada acción tomada (quién llevó a cabo la acción, cuándo lo hizo y por qué motivos). Se debe avisar a todas las personas implicadas con acceso durante el proceso de respuesta.

Organizar la documentación cronológicamente, comprobar que está completa, firmarla y revisarla con el nivel directivo y los abogados, si es del caso.

j. Valoración de los daños y costos del incidente

Al determinar los daños que sufre la organización, se debe considerar tanto los costos directos como los indirectos. El daño y los costos del incidente constituirán una prueba

importante y necesaria si se decide emprender acciones legales. Dentro de los elementos a considerar están:

- Costos debidos a la pérdida de la ventaja competitiva por la divulgación de información confidencial o de propietario.
- Costos legales.
- Costos laborales por el análisis de las infracciones, la reinstalación del software y la recuperación de datos.
- Costos relacionados con el tiempo de inactividad del sistema (por ejemplo, productividad de los empleados, sustitución del hardware, del software y de otras propiedades).
- Costos relacionados con la reparación y posible actualización de las medidas de seguridad físicas dañadas o ineficaces (cierres, paredes, cajas, etc.).
- Otros daños derivados, como la pérdida de la reputación o de la confianza del cliente.

k. Revisión de la respuesta y actualización de las directivas

El Oficial de seguridad de la Información o de datos personales en coordinación con el área de tecnología revisará qué pasos se siguieron correctamente y qué errores se cometieron. En casi todos los casos se descubrirá que se deben modificar algunos procedimientos para controlar mejor futuros incidentes.

l. Prevenir futuros incidentes de seguridad

A través de la metodología de mejora continua, se realizan planes de acción para evitar que futuros incidentes de seguridad se materialicen. La socialización de las causas de los

incidentes es una de las mejores actividades para crear barreras de protección. Además, se realizarán las siguientes tareas recomendadas:

- Revisar las condiciones del Tratamiento.
- Realizar auditorías internas, externas o mixtas.
- Robustecer las políticas, procesos y procedimientos.
- Ajustar las evaluaciones de impacto en datos personales.
- Establecer esquemas de trabajo a corto, mediano y largo plazo, así como los roles y responsabilidades.
- Generar apoyo y compromiso de la Alta Gerencia para desplegar los cambios que se requieran al interior de las organizaciones.

Algunos ejemplos para de las medidas a implementar con posterioridad a la ocurrencia de un incidente son:

- Reforzar los programas de capacitación y educación del personal.
- Identificar y mejorar los controles internos que no tuvieron el efecto esperado en la contención de la brecha de seguridad.
- Identificar y eliminar malware o desactivar cuentas de usuarios vulnerables.
- Realizar un contraste con las medidas adoptadas para solucionar el incidente de seguridad en cuestión, y garantizar un análisis pormenorizado de las soluciones que pudieron haberse adoptado.
- Actualizar el antivirus de la organización.
- Analizar con el antivirus todo el sistema operativo, incluidas aquellas secciones que no se vieron afectadas.

- Garantizar que la estrategia adoptada encuentre un balance entre la continuidad del negocio y el riesgo intrínseco en los activos que se hayan visto afectados por el incidente de seguridad.
- Elaborar un informe final tendiente a recopilar la información, plazos de actuación y medidas adoptadas, de cara a una revisión por terceras personas.