CONTENIDO

Elaborado por:	Revisado y Aprobado por:	Aprobación Metodológica por:
Nombre: Oscar Fabián Ramírez Torres Cargo: Coordinador Grupo de Trabajo de Informática Forense y Seguridad Digital.	Nombre: Jaroslav Marlen López Chávez Cargo: Jefe Oficina de Tecnología e Informática (E).	Nombre: Giselle Johanna Castelblanco Muñoz Cargo: Representante de la Dirección para el Sistema de Gestión de Calidad Fecha: 2024-02-09

1 OBJETIVO

Establecer los lineamientos y definición de las etapas para la gestión de eventos e incidentes de seguridad de la información de la Superintendencia de Industria y Comercio, con el fin de proteger, prevenir, detectar, evaluar, analizar, tratar, reportar y responder ante de los incidentes de seguridad de la información. De esta manera, generar la recuperación, solución y documentación de los mismos, generando lecciones aprendidas y también, iniciando el proceso legal relacionado con los incidentes de seguridad de la información de la SIC de considerarse necesario.

2 DESTINATARIOS

Este procedimiento va dirigido a los servidores públicos, contratistas y terceros directos o indirectos de la Superintendencia de Industria y Comercio, que participen con la gestión de incidentes de seguridad de la información.

3 GLOSARIO

AGENTE DEL PRIMER PUNTO DE CONTACTO: Profesional de la mesa de servicios, encargado de recibir, registrar escalar los posibles incidentes de seguridad de la información reportados por los usuarios.

BCP (plan de continuidad del negocio): Es un plan logístico para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

CIO (Chief Information Officer): Es el líder de la gestión estratégica de tecnologías de información, encargado de planificar, organizar, coordinar, gestionar y controlar la estrategia de uso y apropiación de TI y el Modelo de Seguridad y Privacidad de la Información, y todo lo que conlleva esta tarea.

COMITÉ DE RESPUESTA: El equipo de respuesta es el responsable de definir e implementar las acciones necesarias para reducir el impacto de un incidente de seguridad en los Titulares de la información.

CONFIDENCIALIDAD: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

DATO PERSONAL: El dato personal se refiere a cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos personales pueden ser públicos, semiprivados o privados.

DISPONIBILIDAD: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

DRP (plan de recuperación ante desastres): es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos.

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: Presencia identificada de un estado del sistema, servicio o de red de datos, que indica un posible incumplimiento de la política de seguridad de la información, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.

GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

GRUPOS DE INTERÉS ESPECIAL: Grupos u otros foros y asociaciones profesionales especializadas en seguridad de la información.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: Un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

INCIDENTES DE SEGURIDAD QUE AFECTEN LOS DATOS PERSONALES: Ocurrencia de uno o varios eventos que atentan contra la confidencialidad, la integridad y la disponibilidad de la información personal administrada por la Entidad.

INTEGRIDAD**:** Propiedad de salvaguardar la exactitud y estado completo de los activos.

INVESTIGACIÓN FORENSE DE SEGURIDAD DE LA INFORMACIÓN: Aplicación de técnicas de investigación y análisis para recolectar registrar y analizar información de incidentes de seguridad de la información.

MSPI: Modelo de Seguridad y Privacidad de la Información.

OFICIAL DE PROTECCIÓN DE DATOS PERSONALES: Colaborador encargado de estructurar, diseñar y administrar el programa que permita a la organización cumplir las normas sobre protección de datos personales, así como establecer los controles de ese programa, su evaluación y revisión permanente.

OFICIAL DE SEGURIDAD DE LA INFORMACIÓN: Es el profesional responsable de alinear las iniciativas de seguridad con los objetivos misionales, garantizando que los bienes y las tecnologías de la información están adecuadamente protegidos.

PLAYBOOK: Los playbook complementan al Plan de Respuesta a Incidentes, ya que definen las líneas de acción específicas para cada tipología de incidente.

PROFESIONAL DEL LABORATORIO DE INFORMÁTICA FORENSE: Es el profesional responsable de aplicar técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal o no legal.

RESPONSABLE DE LA ATENCIÓN DE INCIDENTES DE SEGURIDAD: Es el profesional responsable de llevar a cabo la implementación, notificación y registro de la solución al incidente que se haya identificado.

RESPONSABLE DEL TRATAMIENTO: El responsable del tratamiento determina los fines y los medios relacionados con el tratamiento de los datos personales.

SALVAGUARDA: Prácticas, procedimientos o mecanismos que pueden proteger contra una amenaza y reducir la probabilidad de explotación de una vulnerabilidad.

SGSI (Sistema de Gestión de la Seguridad de la Información): Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información.

SOC: Centro de operaciones de seguridad, responsable de supervisar, administrar y garantizar la seguridad de la información a través de distintas herramientas y procedimientos técnicos.

SOLICITUD DEL SERVICIO**:** Petición realizada por un usuario sobre información o asesoramiento, solicitud de un cambio estándar, o solicitud de acceso a un servicio de TI.

TI (Tecnología de la Información): Se refiere a los elementos de hardware, software, servicios, procesos y en general cualquier otro elemento usado en la generación, procesamiento, almacenamiento y transmisión de la información.

TITULAR DE LA INFORMACIÓN: El titular de la información es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos. Ejemplo: Un usuario que celebró el contrato de prestación de servicio de comunicaciones.

VULNERABILIDAD: Corresponde a una debilidad o fragilidad de un sistema (físico, técnico, organizacional, cultural, etc.) que puede ser explotada por una amenaza, causando daños o perjuicios.

4 REFERENCIAS NORMATIVAS

Jerarquía de la norma	Numero/ Fecha	Título	Artículo	Aplicación Específica
Ley	1581 de 2012	Ley de Protección de Datos Personales, Reglamentada parcialmente por el Decreto Nacional 1377 de 2013.	Aplicación total	Aplicación total
NTC-ISO-IEC	27035:2011	Tecnología de la información. Técnicas de seguridad. Gestión de incidentes de seguridad de la información.	Aplicación total	Aplicación total
Guía	2021	Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información de MINTIC.	Aplicación parcial	Aplicación parcial

5 GENERALIDADES

De acuerdo con el Modelo de Seguridad y Privacidad de la Información - MSPI del Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, las entidades deben establecer un procedimiento para la gestión de los incidentes de seguridad de la información.

Para la gestión de incidentes de seguridad, se debe llevar a cabo una revisión y/o control efectivo y ordenado, asegurando una respuesta a tiempo de un evento de seguridad de la información y lograr mitigar el riesgo de que se transforme en un incidente de seguridad, donde se pueda ver afectada la disponibilidad, confidencialidad e integridad de la información de la entidad. Por otra parte, tener las lecciones aprendidas basadas en las experiencias previas y brindar una solución de acuerdo con el incidente que se presente.

6 REPRESENTACIÓN ESQUEMÁTICA DEL PROCEDIMIENTO

No	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
1	PREVENIR INCIDENTES SEGURIDAD DE LA INFORMACIÓN	Comunicaciones, actualizaciones y alertas emitidas por grupos de interés especial y proveedores. Comunicados pensados en materia de protección de datos Personales.	Establecer acciones para prevenir los incidentes de seguridad de la información, a través de las siguientes actividades: - Establecer contacto con grupos de interés especial. - Analizar los comunicados emitidos por los grupos de interés especial. - Gestionar e implementar las actualizaciones y recomendaciones de los proveedores de TI. - Implementar las medidas preventivas necesarias. - Diseñar comunicados sobre la prevención y gestión adecuada de protección de datos personales	Oficial de Seguridad de la Información o a quien él delegue. Grupo de Informática Forense y Seguridad Digital Grupo de Trabajo de Servicios Tecnológicos Centro de Servicios Integrados de TI – CSIT Oficial Protección de Datos Personales	Documentación generada de las actividades realizadas (Actas, Informes, Correos Electrónicos) con el resultado de la aplicación de las medidas preventivas

No	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
2	DETECTAR, REPORTAR, VALIDAR ANALIZAR Y EVALUAR LOS EVENTOS DE SEGURIDAD DE LA INFORMACIÓN	Evento de seguridad de la información.	Se deben detectar, reportar, analizar y evaluar los eventos para determinar si este corresponde a un incidente de seguridad de la información, que puede afectar la seguridad de la información de la Entidad, a través de las siguientes actividades: - Detectar eventos de seguridad de la información. - Reportar eventos de seguridad de la información. - Validar el evento de seguridad de la información. - Analizar el evento de seguridad de la información (llevar acabo un levantamiento de información con relación a Datos Personales). - Evaluar el impacto del incidente.	Todos los servidores públicos, contratistas y terceros de la SIC. Centro de Servicios Integrados de TI - CSIT Grupo de Informática Forense y Seguridad Digital Grupo de Trabajo de Servicios Tecnológicos Oficial de Seguridad de la Información o quien él delegue. Oficial de Protección de Datos Personales	Reporte del incidente a interesados (correo electrónico, mensajes, video conferencia). Documentación en la herramienta de gestión de casos TI, análisis del evento y determinación de incidente. Formato Informe de Gestión de Incidente (Estándar-Masivo) GS01-F29.
3	SOLUCIONAR EL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN	Documentación inicial del incidente. Reporte a interesados.	Definir las acciones para contener el incidente e implementar la solución definitiva, a través de las siguientes actividades: - Definir la contención y/o solución del incidente de seguridad de la información. - Implementar la solución al incidente de seguridad de la información. - Notificar la solución del incidente. - Validar y verificar los impactos asociados con Datos Personales relacionados en el Incidente de seguridad de la información. - Establecer contacto con las autoridades.	Oficial de Seguridad de la Información o quien él delegue. Responsable de la atención de incidentes de seguridad de la información. Oficial de Protección de Datos Personales	Resultado del análisis del incidente. Evidencias de la solución del incidente Formato Informe de Gestión de Incidente (Estándar-Masivo) GS01-F29.

No	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
4	DOCUMENTAR EL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN	Resultado del análisis del incidente reportado. Evidencias de la solución del incidente.	El responsable de la atención del incidente de seguridad de la información es el encargado de hacer y documentar el incidente en la herramienta de gestión TI, a través de las siguientes actividades: - Documentar las actividades y acciones relacionadas con el incidente de seguridad de la información con las evidencias necesarias. - Diligenciar el seguimiento SLD Incidentes de seguridad de la información, como apoyo al SGSI.	Responsable de la atención de incidentes de seguridad. Grupo de Informática Forense y Seguridad Digital Centro de Servicios Integrados de TI - CSIT Oficial de Protección de Datos Personales	Registro y documentación del incidente en la herramienta de gestión de registro de casos TI Formato Informe de Gestión de Incidente (Estándar-Masivo) GS01-F29. Registro en Seguimiento Segunda Línea de Defensa- Incidentes de Seguridad de la Información.
5	RECUPERAR Y ANALIZAR LECCIONES APRENDIDAS	Resultado del análisis de la documentación. .	Realizar las labores de recuperación y registro de lecciones aprendidas: - Recuperar los sistemas de información y/o procesos afectados. - Definir y analizar las lecciones aprendidas.	Oficial de Seguridad de la Información o quien él delegue. Centro de Servicios Integrados de TI - CSIT Grupo de Informática Forense y Seguridad Digital Oficial de Protección de Datos Personales	Registro en documento maestro de casos y/o Reporte de Eventos e Incidentes de SI. Lecciones aprendidas documentadas y adición a playbook de ser necesario. Formato Informe de Gestión de Incidente (Estándar-Masivo) GS01-F29. Evidencias forenses si aplica un proceso legal.

No	ETAPAS	ENTRADAS	DESCRIPCIÓN DE LA ETAPA	RESPONSABLE	SALIDAS
6	INICIAR PROCESO LEGAL	Evidencias forenses recolectadas.	Cuando se requiera puede iniciarse un proceso legal, a través de la siguiente actividad: - Iniciar el proceso legal.	Oficial de Seguridad de la Información o quien él delegue. CIO. Oficial de Protección de Datos Personales	Memorando de solicitud de un proceso legal.

7 DESCRIPCION DE ETAPAS Y ACTIVIDADES

7.1 ETAPA 1: PREVENIR INCIDENTES SEGURIDAD DE LA INFORMACIÓN

En esta etapa, se establecen las acciones para prevenir los incidentes de seguridad de la información.

7.1.1 Establecer contacto con grupos de interés especial

El Oficial de Seguridad de la Información y los profesionales de apoyo a la gestión operativa del SGSI, mantienen contactos apropiados con grupos de interés especial, foros y asociaciones profesionales especializadas en seguridad, con el fin de prevenir los incidentes de seguridad de la información y con el propósito de:

- Mejorar el conocimiento acerca de las mejores prácticas y permanecer al día con la información de seguridad pertinente.
- Recibir advertencias tempranas de, vulnerabilidades y parches de seguridad para prevenir ataques o brechas de seguridad.
- Obtener acceso a asesoría especializada en seguridad de la información.
- Compartir e intercambiar información acerca de nuevas tecnologías, productos, amenazas o vulnerabilidades.
- Brindar puntos de enlace adecuados cuando se trata de incidentes de seguridad de la información.

A continuación, se presenta un listado base de organizaciones alas cuales el Oficial de Seguridad de la Información o a quien él delegue, debe inscribirse a sus boletines, comunicados, alertas y participar de las reuniones que ellas organicen, según aplique.

- CSIRT, https://cc-csirt.policia.gov.co/.
- COLCERT, http://www.colcert.gov.co/?q=tags/alertas-de-seguridad
- INCIBE, https://www.incibe.es/.
- CCOC, Comando Conjunto Cibernético.

- Centro Cibernético Policial, https://caivirtual.policia.gov.co
- Ministerio de Tecnologías de la Información y las Comunicaciones.

7.1.2 Analizar los comunicados emitidos por los grupos de interés especial

Cuando los grupos de interés especial emitan comunicados y alertas, es deber del Oficial de Seguridad de la Información o a quien él delegue, analizar su aplicabilidad en la Entidad, y en caso de ser necesario debe tomar las acciones pertinentes dependiendo de la situación. Para el caso de alertas de correos maliciosos y vulnerabilidades que pongan en riesgo la plataforma tecnológica de la SIC, estos deben ser remitidos, vía correo electrónico al Centro de Servicios Integrados de TI - CSIT.

7.1.3 Gestionar e implementar las actualizaciones y recomendaciones de los proveedores de TI.

La Oficina de Tecnología e Informática debe gestionar e implementar las actualizaciones y recomendaciones brindadas por los proveedores de TI y/o el Centro de Servicios Integrados de TI – CSIT, con el fin de tomar las medidas preventivas para las plataformas tecnológicas de la entidad.

7.1.4 Implementar las medidas preventivas necesarias

Una vez el Centro de Servicios Integrados de TI - CSIT o el profesional asignado reciba el reporte, debe tomar las medidas preventivas necesarias para que no se vea afectada la plataforma tecnológica de la SIC y sus usuarios. El resultado de la implementación de las medidas preventivas debe ser notificado a los interesados a través del correo electrónico.

Para la prevención de incidentes de seguridad de la información se deben gestionar las mejores prácticas para el aseguramiento de las redes, sistemas, y aplicaciones, por ejemplo:

- Gestión de vulnerabilidades
- Aseguramiento de las plataformas
- Seguridad en las redes
- Prevención del código con el desarrollo seguro.
- Sensibilización y entrenamiento de los usuarios
- Monitoreo del hardware y software de la SIC
- Equipo de respuesta de incidentes de seguridad de la información (Equipo de respuesta de incidentes de la información.)
- Recursos para el análisis de incidentes de seguridad de la información
- Recursos de mitigación y remediación, entre otras.

7.1.5 Diseñar comunicados sobre la prevención y gestión adecuada de protección de datos personales.

Con el apoyo del oficial de datos personales se debe gestionar y validar las comunicaciones pertinentes, para la sensibilización y prevención del adecuado manejo de los datos personales gestionados al interior de la entidad, enfocados hacia la prevención de incidentes de seguridad de la información.

7.2 ETAPA 2: DETECTAR, REPORTAR, VALIDAR, ANALIZAR Y EVALUAR LOS EVENTOS DE SEGURIDAD DE LA INFORMACIÓN.

En esta etapa, se deben detectar, reportar, analizar y evaluar los eventos para determinar si corresponden a incidentes de seguridad de la información que pueden afectar la seguridad de la información de la Entidad.

7.2.1 Detectar eventos de seguridad de la información.

Identificación y gestión de eventos que señalen que posiblemente un incidente ha ocurrido, generalmente algunos de estos elementos son:

- Alertas en sistemas de seguridad
- Indisponibilidad de servidores
- Reportes de usuarios
- Alertas de software antivirus

La identificación y gestión de elementos que alertan sobre un incidente, proveen información que puede alertar sobre la futura ocurrencia del mismo y preparar procedimientos para minimizar su impacto. Algunos de estos elementos pueden ser:

- Logs de servidores
- Logs de aplicaciones
- Logs de herramientas de seguridad
- Cualquier otra herramienta que permita la identificación de un incidente de Seguridad.

De acuerdo con lo anterior, se debe hacer seguimiento y registro de las fuentes generadoras de eventos que permitan la identificación de un incidente de seguridad de la información por parte de Centro de Servicios Integrados de TI – CSIT.

7.2.2 Reportar eventos de seguridad de la información.

Todos los servidores públicos y contratistas de la SIC deben reportar presuntos incidentes de seguridad de la información. Los canales de comunicación definidos para este reporte son los siguientes:

- Portal web: https://aranda.sic.gov.co/usdkv8/,
- Correo electrónico: mesadeservicios@sic.gov.co,
- Llamada telefónica: Extensión 10502, que serán gestionados por el proveedor de la mesa de servicios de la SIC.

Los eventos y/o debilidades que se pueden reportar para su respectiva investigación, análisis y gestión deben ser los que atenten contra la confidencialidad, disponibilidad, integridad y privacidad de la información, entre los cuales se pueden mencionar:

- Accesos no autorizados a los sistemas de información.
- Uso indebido de los recursos informáticos de la Entidad.
- Divulgación de información a quien no tiene derecho a conocerla.
- Uso de la información con el fin de obtener beneficio propio o de terceros.
- Hacer pública la información sin la debida autorización.
- Realización de copias no autorizadas de software.
- Descargar software a través de internet sin la debida autorización.
- Intentar modificar, reubicar o sustraer equipos de cómputo, software, información o periféricos sin la debida autorización.
- Transgredir o burlar los mecanismos de autenticación u otros sistemas de seguridad.
- Enviar cualquier comunicación electrónica fraudulenta.
- Violación de cualquier ley o regulación nacional respecto al uso de sistemas de información.
- Robo de información sensible.
- Robo y pérdida de equipos de cómputo con información sensible.
- Denegación de servicio sobre equipos de la red de datos, afectando la operación diaria de la Entidad.
- Denegación de servicio por el ingreso y propagación de virus que explotan vulnerabilidades.
- Amenazas a través de diferentes medios de comunicación (por ejemplo, correo electrónico) que generen un impacto directo sobre la seguridad de la información.
- Cambios o modificaciones en registros de bases de datos sin previa autorización.
- Generación o distribución de código malicioso.
- Fallas en los sistemas de información y pérdidas de servicio.

- Otros eventos y/o vulnerabilidades relacionadas con la seguridad de la información.

Para la clasificación de eventos y/o incidentes de seguridad de la información, se debe tomar como referencia la Matriz de Categorización, la cual también se encuentra integrada en la herramienta de gestión y registro de casos de la SIC.

7.2.3 Validar el evento de seguridad de la información.

Luego de ser recibido un reporte del evento de seguridad de la información, el Centro de Servicios Integrados de TI - CSIT deberá validar si el evento de seguridad reportado está relacionado con una afectación a nivel de confidencialidad, integridad, disponibilidad y privacidad de la información de la SIC, de acuerdo con el listado de eventos y/o debilidades relacionado en el numeral 7.2.2 de este documento. Si esta validación es positiva, se debe comunicar el incidente de seguridad de la información, vía correo electrónico o por medio de un flujo programado dentro del aplicativo de gestión de incidencias al Oficial de Seguridad de la Información, o quien él delegue.

En el caso de que el evento reportado no se trate de un incidente o evento de seguridad de la información, por ejemplo, si se trata de un evento o actividad de soporte técnico, el Centro de Servicios Integrados de TI - CSIT de la SIC procederá a tratar el evento siguiendo los procedimientos establecidos para tal fin.

7.2.4 Analizar el evento de seguridad de la información (llevar acabo un levantamiento de información con relación a Datos Personales).

Para el análisis de incidentes de seguridad de la información, se debe tener en cuenta algunos componentes:

- Conocer las características normales de la red y los sistemas
- Los administradores de TI deben tener conocimiento total de los comportamientos de la infraestructura de la Entidad.
- Se debe centralizar toda la información que permita el análisis de posible incidente de seguridad (Logs de servidores, redes y aplicaciones).
- Se debe verificar la correlación de eventos, ya que esto permitirá validar patrones de comportamiento anormal.
- Para el correcto análisis de un incidente de seguridad de la información se debe tener una única fuente de tiempo, es decir sincronización de relojes, esto facilita la correlación de eventos y análisis de la información.
- Se debe mantener y usar una base de conocimiento con la información relacionada con nuevas vulnerabilidades, información de los servicios habilitados y experiencias con incidentes anteriores.

- Se debe crear documentación para el diagnóstico e información para los administradores nuevos en la entidad o con menos experiencia.
- Analizar y llevar a cabo el levantamiento de información con relación a Datos Personales de ser necesario.

7.2.5 Evaluar el impacto del incidente.

El Oficial de Seguridad de la Información, o quien él delegue, determina el tipo de incidente de seguridad de la información que ha sido reportado.

Si el Oficial de Seguridad de la Información o quien él delegue, determina que no se trata de un incidente de seguridad de la información, procede a informar a quien lo notifico directamente, las razones para no procesarlo como un incidente de seguridad de la información. Desde la primera línea de comunicación se informará al usuario acerca de qué son los incidentes de seguridad de la información y cómo reportarlos. Las comunicaciones de concientización y educación dirigidas a los usuarios al respecto de incidentes de seguridad de la información pueden realizarse utilizando los siguientes medios:

- De forma verbal con los colaboradores o áreas involucradas.
- Mediante correo electrónico.
- Capacitaciones.

Si el Oficial de Seguridad de la Información, o quien él delegue, determina que efectivamente se trata de un incidente de seguridad de la información, éste se debe valorar en función del tipo de impacto que puede causar para la SIC, considerando la afectación a alguno de los tres pilares de seguridad de la información Confidencialidad y/o Privacidad, Integridad y Disponibilidad.

Los valores posibles se describen en la siguiente tabla:

Niveles de impacto del incidente	Confidencialidad o privacidad	Integridad	Disponibilidad
Alta	La Información es sensible para la operación de la entidad.	La información ha sido modificada en gran parte o en su totalidad de forma accidental o intencionada.	El daño estimado para la entidad en términos de tiempo (horas hombre involucradas) es de más de una semana laboral.
Media	La Información es medianamente sensible para la operación de la entidad.	La información ha sufrido algunas modificaciones accidentales o intencionadas.	El daño estimado para la entidad en términos de tiempo (horas hombre involucradas) está entre un día y una semana laboral.

Niveles de impacto del incidente	Confidencialidad o privacidad	Integridad	Disponibilidad
Baja	La Información no es sensible para la operación de la entidad.	La información está libre de modificaciones no autorizadas.	El daño estimado para la entidad en términos de tiempo (horas hombre involucradas) está entre horas y un día laboral.
Desconocida	No existe un criterio para determinar la sensibilidad de la información.	No se puede determinar si la información ha sido modificada.	No se puede determinar el daño para la entidad en términos de tiempo.

7.3 ETAPA 3: SOLUCIONAR EL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

En esta etapa se definen las acciones para contener el incidente e implementar la solución definitiva.

7.3.1 Definir la contención y/o solución del incidente de seguridad de la información.

Es importante aclarar que previo a una solución definitiva del incidente y cuando aplique, se debe implementar una respuesta inmediata con el fin de evitar mayores afectaciones a los activos de información de la SIC.

El Oficial de Seguridad de la Información, o quien él delegue, es el encargado de definir la solución al incidente reportado. En caso de ser necesario, se puede convocar a otros servidores públicos o contratistas de la SIC para aportar en la solución del incidente. En el caso de que no se encuentre una solución que dé respuesta al incidente se puede contactar grupos de apoyo como autoridades, grupos de interés externos que manejen asuntos relacionados a incidentes de seguridad de información para dar solución al mismo.

Para la definición de la solución definitiva del incidente se puede consultar el playbook, en la sección que corresponda según la naturaleza del incidente, existencia de incidencias similares que hayan ocurrido en el pasado y que aporten en la solución del incidente actual.

7.3.2 Implementar la solución al incidente de seguridad de la información.

El administrador o custodio del activo afectado, junto con el o los) responsable(s) de la atención del incidente de seguridad de la información debe llevar a cabo la implementación de la solución al incidente que se haya definido previamente. Las soluciones de incidentes que impliquen cambios sobre los activos de información que la OTI tiene a cargo, se deben llevar a cabo siguiendo el procedimiento (DE04-

P04 - Procedimiento Control De Cambios), el tipo de cambio será definido por el Oficial de seguridad de la información, junto con el líder o responsable del área al cual pertenece el sistema/dispositivo y/o proceso que requiere cambio.

Si después de aplicar controles para mitigar el incidente, aún no se ha controlado, se retorna a la actividad anterior para redefinir la solución al incidente.

7.3.3 Notificar la solución del incidente.

El responsable de la atención del incidente de seguridad debe informar vía correo electrónico a los interesados, incluyendo al usuario que reportó el incidente, la conclusión y forma en que se resolvió y mitigó el incidente.

7.3.4 Validar y verificar los impactos asociados con Datos Personales relacionados en el Incidente de seguridad de la información.

Analizar los incidentes de seguridad de la información, con el fin de determinar si se presenta un impacto sobre los derechos de los titulares de la información, a través de una evaluación preliminar que contenga lo siguiente:

- Una evaluación de los impactos asociados con el incidente de seguridad de la información.
- Identificar los daños para las personas, organizaciones y público en general.
  - Dependiendo de la criticidad del incidente, reportar a la Superintendencia de Industria y Comercio (SIC) RNBD.
  - Dependiendo de la criticidad, comunicar a los titulares.
  - Establecer con el comité de respuesta y verificar las actividades pendientes enfocadas en la protección de datos personales para la prevención de futuros incidentes de seguridad de la información.

7.3.5 Establecer contacto con las autoridades.

En la siguiente tabla se presentan las entidades competentes en caso de presentarse un incidente de seguridad de la información que requiera ser notificado, estas entidades, sólo podrán ser contactadas por el Oficial de Seguridad de la Información, o quien él delegue:

Descripción	Organización	Contacto
Denuncias de Habeas Data y Gestión de Incidentes de Seguridad en Protección de datos personales.	Superintendencia de Industria y Comercio.	http://www.sic.gov.co/ https://www.sic.gov.co/registro-nacional-de-bases-de-datos Registro Nacional de Bases de Datos | Superintendencia de Industria y Comercio Coordinación Del Grupo De Trabajo De Investigaciones Administrativas. 5870000 ext. 70027
Cuando se tenga evidencia de un incidente informático y se requiera recibir asesoría para posterior judicialización de acuerdo con la Ley 1273 de 2009. Ejemplos: - Acceso abusivo a sistemas informáticos. - Ingeniería social. - Uso de software malicioso. - Suplantación de sitios web. - Transferencia no consentida de activos. - Hurto por medios informáticos. - Phishing	Centro Cibernético Policial (CCP).	https://caivirtual.policia.gov.co/ Correo electrónico: caivirtual@correo.policia.gov.co E-mail: lineadirecta@policia.gov.co
Incidentes con afectación a componentes de la infraestructura tecnológica (sitios web, aplicaciones, servicios en línea, sistemas de información, entre otros).	COLCERT – Grupo de Respuesta a Emergencias Cibernéticas en Colombia.	www.colcert.gov.co/ Línea de atención: (+ 57 1) 295 98 97 E-mail: contacto@colcert.gov.co
Incidentes con afectación a infraestructuras Criticas Cibernéticas.	Comando Conjunto Cibernético de Colombia – CCOC.	(57 1) 3150111 ext. 3085 – 3087 2660247 Email: servicio@ccoc.mil.co ccoc@ccoc.mil.co

Descripción	Organización	Contacto
Requerimientos de apoyo en los siguientes temas: - Atención efectiva de eventos e incidentes, con el fin de restablecer la operación y mitigar el impacto causado. - Asistencia y atención con el fin de ayudar a tomar medidas para proteger y asegurar las plataformas tecnológicas, prever futuros ataques, dificultades o eventos que afecten la confidencialidad e integridad de la información. - Establecimiento de estándares y buenas prácticas para mejorar la seguridad de la información, generando recomendaciones, comentarios y sensibilizaciones con base en las lecciones aprendidas. - Análisis de Malware.	CSIRT-CCIT – Centro de Coordinación Seguridad Informática Colombia.	https://cc-csirt.policia.gov.co Análisis de malware: https://cc-csirt.policia.gov.co/Sandbox
Incidentes relacionados con los siguientes temas: - Robo. - Acceso no autorizado. - Emergencia por incendio. - Emergencia con sustancias peligrosas (ejemplo: Gases tóxicos). - Antisecuestro y antiextorsión. - Siniestros ambientales.	Línea de emergencia única.	123

7.4 ETAPA 4: DOCUMENTAR EL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

En esta etapa se documenta las acciones y actividades una vez solucionado el incidente de seguridad de la información.

7.4.1 Documentar las actividades y acciones relacionadas con el incidente de seguridad de la información con las evidencias necesarias.

El responsable de la atención del incidente de seguridad de la información es el encargado de hacer y documentar el incidente en la herramienta de gestión TI con las evidencias necesarias.

7.4.2 Diligenciar el seguimiento SLD Incidentes de seguridad de la información, como apoyo al SGSI.

El responsable del Grupo de Trabajo de Informática Forense y Seguridad Digital debe diligenciar el documento y realizar seguimiento de cada incidente de seguridad de la información como apoyo al SGSI de la SIC.

El proceso de registro debe incluir los siguientes datos:

- # Incidente herramienta de gestión TI: Número de incidente asignado en la herramienta de gestión TI.
- Categorización: Diligenciar la categoría asignada del incidente de acuerdo con la matriz de categorización.
- Descripción: Detalle del suceso considerado incidente de seguridad de la información.
- Proveedor: Datos de proveedor si el incidente tuviese relación con uno.
- Producto: Nombre del producto/servicio relacionado con el incidente.
- Tipo: Seleccionar de acuerdo con el incidente, cuál de los tres componentes se vio afectado (Confidencialidad, integridad, disponibilidad)
- Impacto: Seleccionar el tipo de impacto causado por el incidente (Financiero, Reputacional, Operacional, Legal)
- Nivel de impacto: Seleccionar el nivel de impacto de acuerdo con el análisis del incidente presentado (Alto, Medio, Bajo y Desconocido).
- Área: Área de la SIC afectada por el incidente
- Fecha y Hora de inicio del incidente: Fecha y hora en la que se sucede/descubre el incidente.
- Especialista TI que reporta: Nombre del usuario o del administrador que reporta al oficial de seguridad, Oficial de Datos Personales u OTI SIC, según sea necesario.
- Fecha y hora de comunicación del incidente a Seguridad de la Información: Al oficial de seguridad u OTI SIC. del incidente.
- Registra: Cliente que registra el incidente en la herramienta de gestión TI.
- Fecha y Hora del Registro: Fecha y hora del registro del incidente en la herramienta de gestión de TI.
- Solución: Descripción de la solución o acción correctiva aplicada para dar solución a la incidencia y lecciones aprendidas.
- Fecha y Hora fin del Incidente: Fecha en que se finaliza el incidente.

7.5 ETAPA 5: RECUPERAR Y ANALIZAR LECCIONES APRENDIDAS

En esta etapa se realizan las labores de recuperación de sistemas de información y registro del caso como lección aprendida.

7.5.1 Recuperar los sistemas de información y/o procesos afectados

El Oficial de Seguridad de la Información o quien él delegue, junto con el administrador o dueño del proceso afectado proceden a la recuperación y restauración de estos. Después del restablecimiento será necesario verificar que el sistema y/o proceso ha sido endurecido con el propósito de prevenir incidentes similares.

Este proceso puede o no incluir la utilización del BCP o el DRP en caso de que aplique, su uso depende de la determinación de criticidad y de la decisión tomada por el oficial de seguridad y responsables.

7.5.2 Definir y analizar las lecciones aprendidas

El Oficial de Seguridad de la Información o el designado para la solución del incidente, junto con el equipo o personal interesado deben identificar las lecciones aprendidas después de presentarse un incidente, lo cual es sumamente útil en la mejora de las medidas de seguridad y el proceso de gestión de incidentes, así como para robustecer el procedimiento.

Para mantener un adecuado registro de lecciones aprendidas la documentación de la lección aprendida debe permitir conocer:

- Exactamente lo que sucedió, en qué momento y cómo el personal gestionó el incidente.
- Si se tomaron las medidas o acciones que facilitaron la recuperación eficiente.
- Cuál sería la gestión de personal y que debería hacerse la próxima vez que ocurra un incidente similar.
- Las acciones correctivas que pueden prevenir incidentes similares en el futuro.
- Cuáles herramientas o recursos adicionales son necesarios para detectar, analizar y mitigar los incidentes en el futuro.
- En caso de ser necesario se deben realizar adiciones al playbook.

7.6 ETAPA 6: INICIAR PROCESO LEGAL

En esta etapa, cuando se requiera puede iniciarse un proceso legal.

7.6.1 Iniciar el proceso legal

En caso de que el análisis de la evidencia digital recopilada determine que se amerita el inicio de acciones legales (civiles o penales), el Oficial de Seguridad de la Información o quien él delegue, procederá a comunicar el hecho al CIO, vía correo electrónico y este hará la solicitud para iniciar los trámites respectivos a través de la Oficina Asesora Jurídica de la SIC.

8 DOCUMENTOS RELACIONADOS

SC05-POL01 Políticas Del Sistema De Gestión De Seguridad De La Información – SGSI.
DE04-P04 Procedimiento control de cambios.
GS01-F29 Formato Informe de Gestión de Incidente (Estándar-Masivo).

8.1 DOCUMENTOS EXTERNOS

Guía para la Gestión de Incidentes de Seguridad – En El Tratamiento de Datos Personales. https://www.sic.gov.co/registro-nacional-de-bases-de-datos

9 RESUMEN CAMBIOS RESPECTO A LA ANTERIOR VERSIÓN

1. Se ajustó la norma de referencia.
2. Se ajustó normas y documentos de referencia.
3. Inclusión del ítem “Validar los impactos asociados con Datos Personales relacionados en el Incidente de seguridad de la información”

_____
Fin documento