Guía para gestionar incidentes de seguridad de la información

Proceso de Tecnologías de la Información

Julio de 2020

Tabla de contenido

1. Objetivo

Gestionar de manera oportuna, ordena y efectiva los incidentes y eventos de seguridad de la información que puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información en el Departamento Administrativo de la Función Pública, realizando acciones correctivas y preventivas que reduzcan los impactos de los eventos de seguridad.

Construir una base de conocimientos que facilite la gestión de incidentes y eventos de seguridad.

Identificar oportunidades de mejora que reduzcan la probabilidad o impacto de eventos, incidentes y riesgos de seguridad de la información

2. Alcance

Inicia con la identificación, registro y clasificación del incidente o evento de seguridad de la información; continua con la contención de efectos negativos y remediación de daños. Sigue con la erradicación de las fuentes identificadas del evento o incidente y el análisis e investigación de sus causas; finaliza con el cierre del incidente y la activación del procedimiento de administración del plan de mejoramiento

3. Base Legal

Ley 527 de 1999, Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales

Ley 599 del 2000, Código penal colombiano.

Ley 1266 de 2008, Disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países

Ley 1273 de 2009, Modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”

Ley 1581 de 2012, Disposiciones generales para la protección de datos personales

Ley 1712 de 2014, Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional

Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

4. Equipo de respuesta a incidentes de la seguridad de la información (ERISI)

El responsable de seguridad de la información del Departamento Administrativo de la Función Pública, debe activar un equipo de respuesta a incidentes de seguridad de la información, cuando se presenten incidentes o eventos de seguridad que puedan afectar la integridad, confidencialidad y disponibilidad de los activos de información institucionales.

El equipo de respuesta a incidentes de seguridad de la información con el apoyo de la Oficina de las Tecnologías de Información y las Comunicaciones, genera los planes de contención, erradicación y recuperación de los activos, servicios y sistemas de información, cuando se presentan eventos o afectaciones sobre los mismo, para prevenir la materialización de desastres y apoyar la continuidad de los servicios en el Departamento Administrativo de la Función Pública.

El ERISI podrá estar conformado según la naturaleza del incidente por:

- Profesionales asignados a la gestión de la plataforma tecnológica (hardware, software base y comunicaciones/redes).
- Profesionales asignados a la gestión de las de Bases de Datos.
- Líderes funcionales de los Sistemas de Información y portales.
- Representantes de los procesos institucionales.
- Representantes del nivel directivo de la Entidad.

De ser necesario y de acuerdo con la naturaleza del incidente se pueden vincular a otros profesionales como abogados, profesionales de comunicación social o especialistas en otras disciplinas relacionadas con el incidente, el centro de respuesta a incidentes cibernéticos del gobierno, autoridades competentes como la Fiscalía o el centro cibernético de la Policía Nacional.

5. Detección y análisis del incidente o evento de seguridad

Los incidentes o eventos de seguridad de la información pueden ser identificados o detectados a través de todas o algunas de las siguientes fuentes de información:

- Alertas de las plataformas tecnológicas de la Entidad.
- Reportes de fallas de la infraestructura tecnológica.
- Reportes de fallas en los sistemas de información o portales.
- Reportes de los usuarios de servicios o activos de información.
- Registros de las herramientas administrativas.
- Consolas de antivirus.
- Comunicaciones anónimas.
- Mensajes o alertas redes sociales.
- Personal de la mesa de ayuda.
- Grupos de valor.
- Reportes de grupos especializados en seguridad informática.

Todo evento o incidente de seguridad debe ser registrado en la herramienta de mesa de servicio - ProactivaNet, donde se documentan los datos de la fuente de información mediante la cual se identificó el evento o incidente de seguridad. La finalidad de este registro es establecer la ocurrencia o no del incidente o evento de seguridad.

Cuando se asigne el posible evento o incidente de seguridad al responsable de seguridad de la información, se debe registrar la información adicional relacionada con la cronología del incidente, el activo de información afectado, estableciendo su nivel de criticidad de acuerdo con el inventario de activos de información institucional, así como otros datos que permitan evaluar plenamente la incidencia.

Los niveles de clasificación de los incidentes o eventos de seguridad son:

Nivel	Valor del activo	Tiempo de atención
Extremo	17	1 hora
Muy alto	15 a 16	6 horas
Alto	12 a 14	12 horas
Medio	9 a 11	2 días
Bajo / Despreciable	Menor A 9	1 semana

Tabla 1 – Clasificación de los incidentes y/o eventos de Seguridad

Para establecer la prioridad o tiempo de atención del incidente o evento de seguridad de la información, es necesario remitirse al inventario de activos de información y en la columna "*Valoración del activo"*, comprobar el valor del activo para determinar la prioridad de atención del evento o incidente de seguridad.

Los integrantes del ERISI deben realizar el análisis del incidente o evento de seguridad, y a partir de los resultados identificar un plan de acción en el cual quedarán plasmadas las actividades que se ejecutarán. Las acciones de respuesta al incidente que puede incluir: recolección de las evidencias, contención y erradicación del incidente, así como la recuperación del activo de información en caso de que se haya afectado la continuidad del negocio.

6. Recolección, aseguramiento y análisis de evidencias digitales.

Las actividades de recolección y aseguramiento de las evidencias digitales comprenden: hallazgo, recaudo, aseguramiento, transporte, custodia y análisis de las evidencias digitales, que con ocasión de un incidente o evento de seguridad de la información se logren identificar y recopilar.

Las evidencias que podrían encontrarse y recaudarse con ocasión del incidente de seguridad de la información pueden incluir:

- Registro de actividades de servidores tecnológicos.
- Registro de actividades de aplicaciones.
- Registro de actividades en los sistemas operacionales.
- Registro de actividades en herramientas de seguridad.
- Computadores de escritorio.
- Computadores portátiles.
- Teléfonos inteligentes.
- Tabletas.
- Buzones de correo electrónico.
- Archivos almacenados en sistemas informáticos.
- Registro de cámaras de seguridad.
- Testimonios.
- En general cualquier evidencia que pueda dar indicios sobre la ocurrencia del evento de seguridad.

La recolección de la evidencia debe documentarse en el lugar en donde se encuentren *–lugar de la escena–*, mediante los diferentes medios de fijación (descriptivo, fotográficos, video o gráficos).

El aseguramiento de la evidencia digital se hace mediante técnicas propias de la informática forense, es decir, se identifica inicialmente la información contenida en los medios de almacenamiento recaudados, mediante técnicas criptográficas denominadas *HASHING* o *CHECKSUMS*; así mismo, se extraen copias idénticas

de los datos a través de la extracción de imágenes forenses físicas o lógicas y, de ser posible, se extrae una estampa de tiempo –*Time Stamping.*

Las evidencias recolectadas se analizan en detalle con la finalidad de encontrar información pertinente para la investigación, logrando así determinar y comprobar la ocurrencia de los hechos frente al incidente de seguridad denunciado y en los casos en que sea factible, identificar posibles responsables o causa raíz del incidente.

Para la realización de las actividades de recolección y análisis de evidencias digitales se pueden usar según su disponibilidad, elementos como:

- Portátiles para análisis forense.
- Laboratorios especializados de análisis forense.
- *Software* de adquisición de imágenes forenses.
- *Software* de recolección de evidencias digitales.
- *Software* de análisis forense.

Si no se cuenta con las habilidades, conocimientos o herramientas para realizar adecuadamente las actividades de recolección de evidencias digitales, la labor se debe solicitar a una entidad competente: Fiscalía, centro cibernético policial, centro de respuesta a incidentes informáticos de Gobierno.

7. Contención, erradicación y recuperación

Una vez se ha establecido el impacto del incidente de seguridad de la información, es necesario que se ejecuten las actividades de contención, erradicación y recuperación, tal y como se describe a continuación:

Contención: son las acciones que buscan evitar la propagación del incidente de seguridad de la información, para prevenir daños sobre los otros activos de información de la Entidad.

El grupo de acciones de contención debe enfocarse en la detección del incidente y a la estrategia para contenerlo. A continuación, se exponen algunos ejemplos de estrategias de contención:

Incidente de Seguridad	Ejemplo de estrategia de contención
Accesos no Autorizados	Bloqueos de cuenta Apagado de la máquina Bloqueo de puertos
Códigos Maliciosos	Desconexión de la red del equipo afectado Bloqueo de puertos de comunicaciones Actualización de herramientas de detección y bloqueo de software malicioso
Reconocimiento no autorizado de puertos o servicios	Activación o actualización de reglas de filtrado de comunicaciones Bloqueo de Puertos de comunicación
Daño físico a equipos	Retiro del atacante del área Bloqueo de cuentas de acceso

Tabla 2 - Estrategia de Contención de Incidentes de Seguridad

Erradicación y Recuperación: Cuando se haya contenido el incidente de seguridad de la información, se debe continuar con la erradicación de este, es decir, eliminar cualquier tipo de agente, elemento que sea el causante del comportamiento inusual en los activos de información. Paralelamente se pueden iniciar las tareas de restauración inmediata al normal funcionamiento de los servicios o activos de información afectados, para que retornen de manera oportuna y eficaz no solo las funcionalidades normales, sino a estados que permitan realizar seguidamente las actividades de endurecimiento –Hardening–, para proceder luego a cerrar las vulnerabilidades que permitieron la ocurrencia del incidente o evento de seguridad.

A continuación, se exponen algunas estrategias de recuperación:

Incidente de Seguridad	Ejemplo de estrategia de Erradicación o Recuperación
Denegación de Servicios	Restitución del servicio caído Restauración de *copias de respaldo*
Códigos Maliciosos	Corrección de efectos causados Restauración de copias de respaldo Actualización de antivirus
Vandalismo	Nuevas reglas de filtrado Bloqueo de puertos
Alteración no autorizada	Restauración de *copias de respaldo* Reconfiguración del activos a condición inicial
Intrusión	Restauración de equipos y servicios Recuperación de los datos Limpieza y eliminación de cuentas de usuario no autorizadas

Tabla 3 – Posible estrategia de Erradicación o Recuperación de Incidentes de Seguridad

8. Comunicación

A través del Comité Institucional de Gestión y Desempeño se deben definir las acciones necesarias y pertinentes para las comunicaciones externas e internas, que se deban emitir con motivo del incidente de seguridad de la información. Así mismo, el comité determinará la necesidad de coordinar todas aquellas denuncias que deban ser instauradas ante los entes de control y vigilancia, aportando para ello las evidencias recaudadas, así como aquellos informes desarrollados con ocasión de la atención del incidente de seguridad.

9. Base de datos de conocimiento

En la Gestión de Incidentes de Seguridad de la Información, uno de los aspectos más importantes es la mejora continua, ello implica retroalimentar los temas de seguridad a las partes interesadas, lo que implica mantener siempre un registro de lecciones aprendidas. El registro de lecciones aprendidas, debe estar debidamente documentado en planes de mejoramiento de acuerdo con los procedimientos institucionales. El registro de lecciones aprendidas se debe documentar acciones ejecutadas para la gestión de incidentes de seguridad, los recursos asignados, los resultados, las dificultades y la información que permite actuar frente a situaciones similares en caso de volver a presentar el incidente.

10. Desarrollo

Nº	ACTIVIDAD	RESPONSABLE	DOCUMENTO
1	Detectar el incidente o evento potencial de seguridad utilizando las alertas o medios de comunicación disponibles en la Entidad. Por ejemplo: alertas de las plataformas de TIC, caídas del sistema, reportes de usuario, registros de las herramientas administrativas, consolas de antivirus, comunicaciones anónimas, redes sociales, mesa de ayuda, grupos de valor, entre otros.	Servidores Públicos, pasantes, contratistas, administradores de infraestructura y grupos de valor	Correo electrónico Llamada telefónica Redes sociales Mensajería instantánea

Nº	ACTIVIDAD	RESPONSABLE	DOCUMENTO
2	Registrar el incidente o evento de seguridad de la información en la herramienta ProactivaNet, registrando datos como: instante de tiempo del incidente, activo de información involucrado, identificación de las fuentes de información usadas.	Servidores Públicos, pasantes, contratistas, administradores de infraestructura y grupos de valor	Registro herramienta ProactivaNet
3	Clasificar el incidente de seguridad conforme la Tabla 1 – Clasificación de los incidentes y/o eventos de Seguridad, y los tiempos de respuesta esperados para la atención de incidente. Si se confirma que el evento es un Incidente de seguridad, se debe informar al responsable de Seguridad de la Información, quien evaluará la necesidad de activar un equipo de respuesta a incidente de seguridad (ERISI) y realizará el análisis del incidente. *Ir al paso 4.* © Si no se clasifica como un incidente o evento de seguridad de la información, el caso se debe cerrar o atender con el procedimiento definido en la herramienta de mesa de servicio ProactivaNet. *Ir al paso 11*.	Responsable de Seguridad de la Información	Registro herramienta ProactivaNet
4	Preparar un plan de trabajo que permita definir las actividades que se deben ejecutar para responder al Incidente de Seguridad. Determinar los lugares a intervenir frente a la recolección de las evidencias digitales, las acciones de contención, erradicación y recuperación, de los servicios o activos de información afectados.	ERISI Responsable de Seguridad de la Información	Plan de respuesta al incidente
5	Recolectar las evidencias digitales en las áreas o activos afectadas por el incidente de seguridad. En caso de que se defina que las evidencias se usaran para procesos legales, se deben aplicar los lineamientos propios de cadena de custodia e informática forense, para preservar el valor probatorio de las pruebas que se recolecten. ©	ERISI Responsable Seguridad de la Información Representante de Organismo Judicial	Informes de Recolección de Evidencias Evidencias

Nº	ACTIVIDAD	RESPONSABLE	DOCUMENTO
6	Realizar la contención del incidente con apoyo de la Oficina de las TIC, evitando cualquier tipo de propagación que pueda seguir afectando los activos de información de la Entidad. ©	ERISI Responsable de Seguridad de la Información Oficina de TIC	Informe de Contención del incidente de seguridad de la Información documentado en ProactivaNet
7	Si el incidente no puede ser controlado con los recursos internos de la Entidad, se debe evaluar la necesidad de pedir apoyo de terceras partes como fabricantes o equipos de respuesta a incidentes de Csirt Gobierno o ColCERT	ERISI Responsable de Seguridad de la Información Oficina de TIC	Informe de Contención del incidente de seguridad de la Información documentado ProactivaNet
8	Eliminar la causa raíz del incidente de seguridad. Elaborar un plan de recuperación, con la finalidad de poder cerrar las vulnerabilidades detectadas.	Grupo ERISI Oficial o encargado de Seguridad de la Información Oficina de TIC	Informe de Erradicación y Remediación en ProactivaNet
9	Evaluar la necesidad de notificar y denunciar a los entes de control según sea el caso, de acuerdo con las disposiciones establecidas frente a la ocurrencia de los incidentes de seguridad y su impacto dentro de la Entidad. En caso de incidentes de seguridad de la información que afecten bases de datos o información de carácter personal, se debe realizar el reporte ante la Superintendencia de Industria y comercio – Delegatura de protección de datos personales. En el caso de incidentes contemplados en la ley de delitos informáticos ley 1273 de 2009 (http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1676699), se realiza el reporte a la fiscalía general de la nación. En el caso de incidentes asociados al incumplimiento de las políticas de seguridad de	Subdirección	Informe de Contención del incidente de seguridad de la Información en ProactivaNet Correos electrónicos

Nº	ACTIVIDAD	RESPONSABLE	DOCUMENTO
	la información institucionales, la normatividad interna de la Entidad o el Código Único Disciplinario (http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1667339) el reporte se realiza de acuerdo con el procedimiento de control disciplinario del proceso de Gestión del Talento Humano.		
10	Realizar el registro detallado de toda la gestión del incidente de seguridad, para poder documentar acciones correctivas para posteriores eventos o incidentes.	ERISI Responsable de Seguridad de la Información	Plan de mejoramiento en el Sistema de gestión Institucional Registro en ProactivaNet de: Plan de respuesta al incidente. Informe de recolección de Evidencias. Informe de Contención del incidente. Informe de Erradicación y remediación Formato de reporte de Incidente de seguridad de la información.
11	Cerrar el incidente de Seguridad de la Información, actualizando en ProactivaNet el estado del incidente.	ERISI Servidores Públicos, contratistas, Administradores de infraestructura.	Registro en herramienta ProactivaNet

11. Definiciones

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la entidad.

Cadena de Custodia: es un procedimiento documentado y controlado que se le aplica a toda evidencia física o elemento material probatorio desde su recolección hasta su disposición final, en donde se puede observar su descripción e identificación, una línea de tiempo, y las personas que han participado en su custodia.

Evento de Seguridad: ocurrencia identificada de un estado en un sistema de información, servicio o red de telecomunicaciones, que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.

ERISI: Equipo de Respuesta a Incidentes de Seguridad de la Información.

Estampa de Tiempo: certificar mediante una secuencia de caracteres, que un conjunto de datos ha existido y no ha sido modificado en un espacio de tiempo determinado. La secuencia de caracteres está relacionada con la fecha y el momento en que ocurre dicho evento y específicamente cuando fue creado en un sistema de cómputo**.**

***Hardening*:** (ingles: endurecimiento) es el proceso de asegurar un sistema informático mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios innecesarios en el sistema, así como cerrando puertas de acceso que tampoco estén en uso.

Incidente de Seguridad: evento único o serie de eventos de seguridad de la información inesperados o no deseados, que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Informática Forense: es la aplicación de técnicas científicas y analíticas especializadas a infraestructura de TIC, que permiten identificar, preservar, analizar, custodiar y presentar datos – *Evidencia Digital* – de tal manera que sean válidos dentro de un proceso legal y/o administrativo preservando su valor probatorio.

Integridad: propiedad de la información relativa a su exactitud y completitud.

Imagen Forense: copia binaria de la información que se encuentra en un medio de almacenamiento, la cual es trasladada a otro, sin que se cambien ninguna de sus

características y/o atributos.

Lugar de la Escena: lugar de ocurrencia de un incidente y/o evento de seguridad. Entiéndase en la investigación como cualquier lugar mueble o inmueble donde se presuma la comisión de un hecho en contra de la norma y el sitio en donde se sospeche la presencia de elementos materia de prueba y evidencia física relacionados con la misma.

Técnicas *HASHING* o *CHECKSUMS*: son funciones matemáticas y algorítmicas que tiene como propósito principal detectar cambios en una secuencia de datos para proteger la integridad de estos, verificando que no haya discrepancias entre los valores obtenidos al hacer una comprobación inicial y otra final tras el tratamiento realizado.

Vulnerabilidad: debilidad de un activo o control que pueda ser explotado por una o más amenazas.

12. Historial de cambios

Fecha	Versión	Descripción
2020-07-07	1	Creación del documento