Contenido

OBJETIVO

Definir los lineamientos para el tratamiento de los incidentes de seguridad que se presenten sobre los activos de información de la Agencia Nacional de Infraestructura, que atenten contra sus características de confidencialidad, integridad y disponibilidad, así como bridar las herramientas para una atención eficaz y oportuna de estos.

OBJETIVOS ESPECÍFICOS

- Detectar y tratar en forma eficiente incidentes de seguridad de la información.
- Minimizar los efectos adversos que por incidentes de seguridad de la información se pudiesen generar.
- Implementar correctivos sobre vulnerabilidades de seguridad de la información reportadas con el propósito de evitar su reaparición.
- Gestionar el conocimiento basado en las lecciones aprendidas de los incidentes de seguridad de la información y/o vulnerabilidades y evitar que ocurran futuras situaciones de impacto para la Entidad.

ALCANCE

Este documento está dirigido a todos los colaboradores, partes interesadas de la Agencia Nacional de Infraestructura y equipo técnico que gestiona los incidentes de seguridad, que en apoyo al sistema gestión de incidentes de seguridad de la información y de acuerdo con la naturaleza de su función y/o vinculación con la entidad, aplicarán las diferentes actividades aquí mencionadas, tales como: reporte, gestión, recolección de evidencias (cuando aplique) y comunicación, hasta las acciones de solución al incidente de seguridad.

GLOSARIO

- **Análisis forense de seguridad de la información (Information Security Forensics):** Aplicación de técnicas de investigación y análisis para recolectar, registrar y analizar información de incidentes de seguridad de la información.
- **Código malicioso**: Es un tipo de código informático o script web dañino diseñado para crear vulnerabilidades en el sistema que permiten la generación de puertas traseras, brechas de seguridad, robo de información y datos, así como otros perjuicios potenciales en archivos y sistemas informáticos.

- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Contenido malicioso**: Hace referencia a la difusión de contenido que ataca en forma maliciosa a personas o a la Agencia, por ejemplo, bromas pesadas o acoso.
- **Contención**: Estrategia tendiente a evitar la propagación de la amenaza que ocasionó el incidente de seguridad de la información detectado.
- **Denegación de Servicio (DDS)**: Es cuando durante el uso de recursos de red y de sistemas de información tales como CPU, memoria, espacio en disco o ancho de banda de red, se interrumpe la operación normal de los sistemas de información, impidiendo el uso total o parcial de estos.
- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad o persona autorizada.
- **Erradicación**: Una vez el incidente de seguridad de la información es contenido, este debe erradicarse, es decir, se elimina cualquier tipo de rastro que pueda existir con ocasión de comportamiento inusual sobre los activos de información y/o infraestructura de TI.
- **Evento de seguridad de la información**: También llamado incidente, corresponde a la presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falta de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.
- **Gusano**: de red es un tipo de programa malicioso que se auto disemina y auto replica automáticamente, a través de las redes, aprovechando las vulnerabilidades de los sistemas de información en las redes.
- **Ingeniería social**: Consiste en la recolección de información de una persona utilizando medios no técnicos, por ejemplo, mentiras, trampas, sobornos o amenazas.
- **Impacto catastrófico:** Bajo el contexto de seguridad de la información, cuando un incidente afecte o implique pérdidas económicas de gran magnitud, afectación de imagen a nivel nacional e internacional, sanciones de entes de control y daños totales a la infraestructura de la entidad.
- **Impacto crítico**: Bajo el contexto de seguridad de la información, cuando se afecta la operación misional de la entidad o hay indisponibilidad de servicios sobre procesos administrativos que tienen términos de cumplimiento.
- **LOG (registro):** es un archivo de texto en el que constan cronológicamente los acontecimientos que han ido afectando a un sistema informático (programa, aplicación, servidor, etc.), así como el conjunto de cambios que estos han generado.
- **Mesa de servicios**: Sistema manual o automatizado donde los colaboradores o entes externos registran las solicitudes e incidencias sobre los servicios que presta el G.I.T de Tecnologías de la Información y las Telecomunicaciones.

- **Phishing de redes:** consiste en hacer uso de la tecnología fraudulenta de redes de computador para convencer a los usuarios para que divulguen información importante, tal como detalles de cuentas bancarias de usuarios y contraseñas, mediante uso de correos electrónicos engañosos.
- **Puertas traseras**: Hace referencia al uso de componentes o de programas peligrosos dejados en los procesos de diseño de sistemas de software y de hardware.
- **Recolección y análisis de evidencia**: Actividad referente a la toma, preservación, documentación y análisis de datos o información que pueda usarse como prueba o evidencia.
- **Virus informático**: Es un conjunto de instrucciones o códigos informáticos que se insertan en los programas de computador. Tiene la capacidad de auto-replicación y usualmente porta una carga que puede afectar las operaciones del computador y destruir los datos.
- **Vulnerabilidad de seguridad de la información**: Debilidad de un activo o de un grupo de activos que podría permitir que una amenaza se materialice y genere un impacto no deseado a la Entidad.

4.1. ROLES Y RESPONSABILIDADES

A continuación, se describen los roles que participan en el tratamiento de incidentes de seguridad de la Información:

4.1.1. Encargado de seguridad de la información

Es responsabilidad del encargado de la Seguridad de la Información (rol ubicado en el GIT de Tecnologías de la Información y las Telecomunicaciones), garantizar la aplicación del instructivo, realizar el seguimiento correspondiente a la atención de los incidentes de seguridad y evaluar las acciones de mejora que se identifiquen como tratamiento de estos, aplicar dichas acciones y/o sugerirlas al área encargada de la infraestructura tecnológica de la entidad, o quien haga sus veces.

Responsabilidades:

- Analizar y clasificar los reportes de situaciones especiales de seguridad de la información (incidentes).
- Validar las causas del incidente, para elegir las acciones correctivas.
- Asignar prioridad de atención del incidente de seguridad de la información de acuerdo con su severidad e impacto.
- Dar respuesta de manera eficiente y adecuada a los incidentes.

- Revisar y/o complementar detalles del incidente.
- Asignar el incidente a quienes puedan ejecutar la solución de este.
- Encargar la gestión de seguimiento al incidente como apoyo al tratamiento de incidentes de seguridad de la información.
- Contactar a la autoridad para recolección de evidencia a través del análisis forense.
- Revisar y monitorear la atención y solución de los incidentes de seguridad de la información.
- Sensibilizar a la Entidad con respecto al tratamiento de incidentes de seguridad de la información.
- Establecer planes para el mejoramiento continuo.
- Identificar, implementar y verificar las acciones de contención (si aplica).
- Mantener la base de conocimiento de lecciones aprendidas de incidentes de seguridad de la información.
- Presentar informes de gestión de incidentes de seguridad de la información.

4.1.2. Colaboradores ANI

Responsabilidades:

- Reportar situaciones especiales de seguridad de la información.
- Apoyar en la documentación del incidente de seguridad de la información.
- Realizar pruebas de verificación de recuperación del activo de información.
- Acatar lo dispuesto en la GTEC-PT-001 Política de Seguridad y Privacidad de la Información.

Si un colaborador o tercero externo de la ANI sospecha o identifica la materialización de un incidente de seguridad deberá notificarlo al principal punto de contacto (correo electrónico), con la mayor información posible de la situación.

4.2. REPORTE DEL INCIDENTE

El reporte corresponde a la acción de informar un evento o suceso que pueda ser catalogado como incidente de seguridad de la información. Los incidentes de seguridad de la información pueden ser reportados por un colaborador o tercero de la ANI que haya evidenciado una situación o hecho que está afectando o puede afectar la seguridad de la información, para tal fin se dispone de los siguientes puntos de contacto:

Punto de contacto:

- soporte@ani.gov.co – Buzón de mesa de servicios de la ANI.

Para el reporte del incidente se debe enviar un correo electrónico al punto de contacto antes indicado, detallando en el asunto: "Incidente de Seguridad", proporcionando la mayor cantidad de información posible de la que se relaciona a continuación:

1. Fecha y hora del reporte del incidente
2. Lugar del incidente
3. Nombre de quien reporta el incidente
4. Cargo o relación con la ANI de quien reporta el incidente: (funcionario, contratista, tercero externo).
5. Detalles del incidente:
   a. Fecha y hora en la que sucedió el incidente
   b. Fecha y hora en la que se descubrió el incidente
   c. ¿Qué sucedió?
   d. ¿Cómo sucedió?
   e. ¿Qué recursos de información o de hardware fueron afectados?
   f. ¿La respuesta a este incidente ya ha finalizado?: (SI/NO), En caso afirmativo, especifique cuánto tiempo duró el incidente (Días / Horas / Minutos): Una hora Aprox.

4.3. GESTIÓN Y MANEJO DEL INCIDENTE

La gestión del incidente comprende las actividades que se realizan desde que se recibe el reporte hasta que se realizan las actividades de tratamiento de este, tales como: análisis, detección, evaluación y clasificación, las cuales se describen a continuación:

4.3.1. Requisitos para realizar el análisis del incidente

Para el análisis del incidente detectado, es preciso que las personas encargadas a nivel de administración de la infraestructura tecnológica, que hacen parte del equipo técnico de T.I., cumplan con:

- Tener conocimientos de las características normales a nivel de red y de los sistemas.
- Tener conocimiento sobre los comportamientos de la Infraestructura que están administrando.
- Toda información que permita realizar análisis al incidente debe estar centralizada (Logs de servidores, redes, aplicaciones).

- Es importante efectuar correlación de eventos, ya que por medio de este proceso se pueden descubrir patrones de comportamiento anormal y se puede identificar de manera más fácil la causa del incidente.
- Para un correcto análisis de un incidente debe existir una única fuente de tiempo (sincronización de relojes) ya que esto facilita la correlación de eventos y el análisis de información.
- Se debe mantener y usar una base de conocimiento con la información relacionada sobre nuevas vulnerabilidades, información de los servicios habilitados, y experiencias con incidentes anteriores, la cual se ubica en el repositorio de información del GIT de Tecnologías de la información y las Telecomunicaciones.
- Crear matrices de diagnóstico e información para los administradores menos experimentados.

4.3.2. Detección del Incidente

Dentro de un ejercicio preventivo, en la tarea de identificar y alertar sobre la ocurrencia de posibles incidentes que puedan llegar a presentarse, existen algunos elementos que proporcionan información valiosa y que deben permanentemente ser utilizados y consultados.

- Logs de servidores
- Logs de aplicaciones
- Logs de herramientas de seguridad
- Cualquier otra herramienta que permita la identificación de un incidente de seguridad
- En la entidad debe existir un listado de fuentes generadoras de eventos que permitan la identificación de un incidente de seguridad de la información.

Para la detección de los incidentes se debe revisar la presencia de alguno de los siguientes indicadores que indican que posiblemente un incidente de seguridad de la información ha ocurrido:

- Alertas en sistemas de seguridad
- Caídas de servidores
- Reportes de usuarios
- Software antivirus dando informes
- Otros funcionamientos fuera de lo normal del sistema

4.3.3. Evaluación del Incidente

En esta tarea se debe identificar la severidad del incidente teniendo en cuenta los niveles de impacto sobre los activos de información de la entidad. El siguiente es el criterio definido:

- **Alto Impacto**: El incidente de seguridad afecta activos de información considerados de impacto catastrófico y mayor que influyen directamente en los objetivos misionales de la entidad. Se incluyen en esta categoría aquellos incidentes que afecten la reputación y el buen nombre o involucren aspectos legales. Estos incidentes deben tener respuesta inmediata.

- **Medio Impacto:** El incidente de seguridad afecta activos de información considerados de impacto moderado, es decir, influyen directamente en los objetivos de un proceso determinado.
- **Bajo Impacto:** El incidente de seguridad afecta activos de información considerados de impacto menor e insignificante, que no influyen en ningún objetivo. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto.

4.3.4. Clasificación del Incidente

La clasificación de los incidentes de seguridad se debe realizar teniendo en cuenta la siguiente tabla con base en los tiempos estimados para solución:

NIVEL	NOMBRE	TIEMPO DE SOLUCIÓN
1	BAJO	1 SEMANA
2	MEDIO	2 DIAS
3	ALTO	12 HORAS
4	CRITICO	1 HORA

La ponderación para la clasificación de estos niveles es la siguiente[1]:

- **Bajo**: Este nivel de criticidad se da para aquellos incidentes que son detectados y/o denunciados como posibles amenazas para los activos de información, es decir, que pueden impactar sus características de integridad y/o confidencialidad y/o disponibilidad, sin embargo, los controles de seguridad resultan efectivos anulando cualquier impacto para la Agencia Nacional de Infraestructura.
- **Medio**: Este nivel de criticidad se da para aquellos incidentes que son detectados y/o denunciados como posibles amenazas, que pueden afectar los activos de información de la Agencia, impactando de modo limitado sus características de integridad y/o confidencialidad y/o disponibilidad frente a un activo no crítico para la ANI.
- **Alto**: Este nivel de criticidad se da para aquellos incidentes que son detectados y/o denunciados, porque en ellos, es posible establecer una amenaza sobre los activos de información capaz de impactar de manera considerable las características de integridad y/o confidencialidad y/o disponibilidad de un activo no crítico o crítico para la ANI.
- **Crítico**: Este nivel de criticidad se da para aquellos incidentes que son detectados y/o denunciados, porque en ellos, es posible establecer una amenaza sobre los activos de información capaz de impactar de manera considerable las características de integridad y/o confidencialidad y/o disponibilidad de un activo crítico de la ANI.

4.3.5. Criticidad del Impacto

Para determinar la criticidad de impacto del incidente se debe apoyar en la siguiente tabla:

[1] https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf

CRITICIDAD	VALOR	DEFINICIÓN
Inferior	0,10	Sistemas no críticos, como estaciones de trabajo de usuario con funciones no críticas.
Bajo	0,25	Sistemas que apoyan a una sola dependencia o proceso de la Agencia.
Medio	0,50	Sistemas que apoyan más de una dependencia o proceso de la Agencia.
Alto	0,75	Sistemas pertenecientes al área de tecnología y estaciones de trabajo de usuarios con funciones críticas.
Superior	1,00	Sistemas críticos.

Niveles de Criticidad de Impacto[2]

4.3.6. Tiempos máximos de atención de incidentes

Los tiempos expresados en la siguiente tabla son un acercamiento al tiempo aproximado en que el incidente debe ser atendido, entendiéndose que, **no es el tiempo en que debe ser solucionado**; esto se debe a que la solución del incidente puede variar dependiendo su el caso y su complejidad. Se debe tener en cuenta tanto la prioridad como los tiempos en dar atención.

NIVEL DE PRIORIDAD	VALOR
Inferior	3 horas
Bajo	1 hora
Medio	30 minutos
Alto	15 minutos
Superior	5 minutos

Tiempos máximos de atención de incidente[3]

4.3.7. Tratamiento del incidente

Una vez identificado como un incidente de seguridad de la información, las actividades para desarrollar el tratamiento estarán acorde con las descritas en el procedimiento "GTEC-P-002 Gestión de incidentes y Requerimientos de T.I", en donde una vez escalado a segundo nivel como incidente de seguridad, el responsable que reciba el caso deberá analizar, evaluar, definir la criticidad de incidente de acuerdo con lo establecido en los capítulos anteriores del presente documento y gestionar el incidente hasta finalizar las actividades de tratamiento. Las actividades de gestión y atención del incidente podrán incluir la recuperación de los sistemas de información y servicios afectados, o restauración si fuese pertinente y requerido.

[2] https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf
[3] Ibid.

En caso de requerir apoyo de externos, el encargado de la seguridad de la información debe realizar las gestiones pertinentes de contacto y compromiso para asegurar la presencia del externo según las modalidades y acuerdos de niveles de servicio establecidos contractualmente o en los convenios establecidos.

En cualquier caso, el incidente deberá ser documentado en el repositorio de información establecido para tal fin, con las acciones adelantadas para su resolución.

Se considera importante que el responsable de seguridad de la información, en conjunto con el equipo pertinente de acuerdo con la naturaleza del caso, validen si las acciones de contención fueron eficaces y tuvieron los resultados esperados; caso contrario, se deberán identificar acciones adicionales para contener el incidente y mediante el escalamiento adecuado.

4.4. RECOLECCIÓN DE EVIDENCIA DEL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

Para aquellos incidentes de seguridad de la información en los cuales se pueda o se deba recolectar evidencia con propósito legal (implicación de acciones disciplinarias y/o legales (civiles o penales), se deberá realizar el levantamiento a través de actividades estructuradas de análisis forense de seguridad de la información, y con el uso de medios técnicos (ejemplo, herramientas de auditoría, instalaciones para recuperación de evidencia), en oficinas seguras, mediante herramientas de investigación basadas en TI, apoyadas en procesos documentados, y realizadas por personal con la competencia profesional.

Para asegurar una adecuada recolección de evidencia, el encargado de la seguridad de la información deberá contactar a las autoridades pertinentes y especializadas para los propósitos de recolección de información y aseguramiento de cadena de custodia, quienes definirán las acciones a seguir para la recolección de la información y la correspondiente cadena de custodia.

4.5. COMUNICACIÓN DE LA SOLUCIÓN DEL INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

Posterior a la verificación del adecuado tratamiento, solución y cierre del incidente de seguridad de la información, se deberá comunicar a las partes interesadas (directivos, colaboradores, etc.), acerca del restablecimiento de los activos de información.

4.6. SANCIONES POR EL INCUMPLIMIENTO A LAS POLÍTICAS

Teniendo en cuenta que el presente instructivo tiene directa relación con la “GTEC-PT-001 Política de Seguridad y Privacidad de la Información” definida por la entidad, el no cumplimiento acarreará las acciones disciplinarias establecidas por la ANI o las sanciones específicas establecidas en la Ley 1952 de 2019 y demás normas que reglamentan los procesos disciplinarios para los funcionarios públicos, contratistas y terceros. El incumplimiento será evaluado de acuerdo con el impacto

generado y al criterio de las instancias de control, pudiendo éste, ser aplicado con medidas correctivas administrativas, disciplinarias o legales.

En los casos que aplique, la entidad iniciará las acciones disciplinarias y/o legales dependiendo la situación aplicable a los colaboradores que infrinjan la normatividad o desatiendan las responsabilidades aquí especificadas.

5. CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
001	30/07/2020	Creación del documento

6. APROBACIÓN

	NOMBRE	CARGO	APROBACIÓN
Elaboró	Guillermo Cadena Ronderos	Contratista	Documento aprobado mediante Radicado No. 20206070094913
Revisó	Erika Díaz Abella	Contratista	
Aprobó	Andrés Francisco Boada	Coordinador G.I.T. Tecnologías de la Información y las Telecomunicaciones	
Vo. Bo. SGC	Daniela Mendoza	Contratista	