POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

UNIDAD
DE RESTITUCIÓN
DE TIERRAS

Bogotá D.C., julio de 2018

TABLA DE CONTENIDO

INTRODUCCIÓN

La presente política de Gestión de Incidentes de Seguridad es elaborada tomando como referencia la Norma Técnica Colombiana NTC-ISO-27001. Esta política establece los lineamientos para poner en marcha un Sistema de Gestión de Incidentes de Seguridad de la información, a través de un modelo propuesto, el cual está concebido para el manejo de los posibles incidentes de seguridad de la información que puedan presentarse al interior de la Unidad de Restitución de Tierras (URT).

1. OBJETIVO

Dar a conocer los lineamientos generales definidos por Seguridad de la Información y aprobados por el Comité de Gestión y Desempeño, para el manejo de los posibles incidentes de seguridad de la información que puedan presentarse al interior de la entidad.

2. ALCANCE

Este documento contiene los componentes generales de la gestión de incidentes de seguridad y sus principales acciones, las cuales son aplicables indistintamente de la plataforma operacional, o el tipo de información o activo de información sobre el cual se presente o exista un indicio de incidente de seguridad.

3. DEFINICIONES

Ver definiciones en el listado de términos del sistema de información - STRATEGOS.

4. MARCO NORMATIVO APLICABLE

Ver la normatividad aplicable en el normograma del sistema de información - STRATEGOS.

5. ROLES PERFILES Y RESPONSABILIDADES

A continuación, se describen los perfiles y responsabilidades de quienes pueden intervenir ante un incidente de seguridad dentro de la entidad:

5.1. USUARIOS

Los usuarios son la primera línea con la que se pueden identificar eventos adversos sobre la información o algún activo de información, y es de su responsabilidad y deber reportar cualquier situación anormal que pueda llegar a convertirse en un incidente de seguridad de la información. Dependiendo de la criticidad del incidente (Bajo, Medio, Alto, Critico), estos deben tener un proceso de notificación diferente reportando directamente a:

- Mesa de Ayuda

Escenarios de Incidentes	Criticidad del Incidente
Código malicioso	Bajo
Denegación del servicio	Bajo
Daños físicos	Bajo hasta Crítico

Un colaborador, tercero o contratista que sospeche sobre la materialización de un incidente de seguridad dentro de los escenarios mencionados en el cuadro anterior, debe notificarlo a la mesa de ayuda quien será el primer punto de contacto. El incidente debe ser notificado a través de la herramienta de apertura de requerimientos GLPI, diligenciado la mayor cantidad posible de información relacionada con el incidente.

La mesa de ayuda identificará el tipo de incidente, el escenario y la criticidad. Analizará si el incidente reportado corresponde a un incidente de seguridad de la información o está relacionado con requerimientos propios de la infraestructura de TI. En caso de ser catalogado como un incidente de seguridad se notificará al Oficial de Seguridad de la Información para realizar el seguimiento del Incidente hasta su cierre definitivo.

- Oficial de Seguridad

Escenarios de Incidentes	Criticidad del Incidente
Ataques	Bajo hasta Crítico
Código malicioso	Medio hasta Crítico
Denegación del servicio	Medio hasta Crítico
Acceso no autorizado	Bajo hasta Crítico
Robo o pérdida de equipos	Bajo hasta Crítico
Uso indebido de la información y recursos tecnológicos.	Bajo hasta Crítico

Un colaborador, cliente, tercero o contratista que evidencie la materialización de un incidente de seguridad dentro de los escenarios mencionados en el cuadro anterior, debe notificarlo directamente al Oficial de Seguridad de la Información debido a su criticidad. Así mismo, existe el correo seguridaddigital@restituciondetierras.gov.co, el cual es un canal en el que se podrá reportar cualquier evento relacionado dentro de las anteriores categorías y que pueda ser generado debido a un incidente de seguridad de la información. Estos eventos serán tratados con la debida reserva y confidencialidad notificando solamente al personal involucrado en la gestión para solventar el incidente.

5.2. OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

Es el responsable de coordinar los esfuerzos necesarios para dar atención a un incidente dentro de la entidad, de igual manera, tiene la responsabilidad de informar a los respectivos niveles administrativos de los incidentes y su grado de severidad dentro de la entidad, así como coordinar los esfuerzos con entidades externas (proveedores, ColCERT, Comando Cibernético, fuerzas policiales, entre otros) en caso de ser necesario.

5.3. COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO

Este grupo multidisciplinario compuesto por:

El (la) Director(a) General, o su delegado (a).
El (la) Subdirector(a) General.
El (la) Secretario (a) General.
El (la) jefe de la Oficina Asesora de Planeación.
El (la) jefe de la Oficina Asesora de Comunicaciones.
El (la) jefe de la Oficina de Tecnologías de la Información.
El (la) Director (a) Social.
El (la) Director (a) Jurídico de Restitución.
El (la) Director (a) Catastral y de Análisis Territorial.
El (la) Director (a) de Asuntos Étnicos.

Se encarga de aprobar las políticas de seguridad de la información, así como, de la orientación en el direccionamiento que debe seguir la institución en la materia. También aprueba el presupuesto requerido según planeación presentada por la Oficina de Tecnologías de la Información con la debida oportunidad, a través del Plan Anual de Adquisiciones.

6. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN (GISI)

La URT, realizará este proceso de seis (6) pasos para la GISI, los cuales permiten gestionar un incidente desde el momento anterior a su ocurrencia, hasta la forma en cómo se deben establecer acciones de mejora que consoliden los aprendizajes para eventos futuros:

Ilustración 1. Gestión de Incidentes de Seguridad de la Información

6.1. PREPARACIÓN

La preparación es la fase con la que se dispone a anticiparse a la ocurrencia de los incidentes, como primer objetivo, y como segundo objetivo definir los lineamientos básicos con los cuales afrontar los incidentes que se presenten dentro de la entidad.

Para cumplir con el primer objetivo la entidad cuenta con un conjunto de medidas de protección base, derivadas de los controles aplicables a cada uno de los dominios de seguridad según la Norma ISO 27001:2013, con las cuales se repelen los ataques que puedan llegar a presentarse; adicional a ello se han aplicado las mejores prácticas para el manejo de los recursos tecnológicos y la información. Así como, permanentes campañas y estrategias de sensibilización sobre la importancia y responsabilidades en la seguridad de la información con todos los colaboradores de la URT.

De la misma manera se ha establecido como línea base de defensa la formulación de la atención de incidentes a través de este documento, con lo cual se busca mejorar la arquitectura de seguridad de la entidad.

6.1.1. CRITERIOS DE CLASIFICACIÓN DE UN INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

La Gestión de Seguridad de la Información mediante la relación del impacto del incidente asociado con la importancia del recurso, preserva la metodología para la medición de Riesgo Operativo contemplada en el manual de Riesgos de la Entidad.

Es así como los criterios para clasificar los incidentes estarán determinados por:

- **Impacto del incidente:** Cuales son las implicaciones tanto técnicas y operacionales al momento de presentarse un incidente de seguridad, y que tan crítico es el recurso o activo de información al que puede afectar el incidente presentado, para la operación del negocio. Para este nivel de indicador se han definido las siguientes escalas:

Impacto del Incidente			
MENOR (1)	***MODERADO (2)***	***MAYOR (3)***	***CATASTROFICO(4)***
Aquellos recursos o activos de información que al ser afectados, no poseen ningún grado de afectación en la operación de las funciones básicas de la entidad o los colaboradores de la misma.	Aquellos recursos o activos de información que al ser afectados, interfieren en las operaciones básicas de la entidad y de los colaboradores, pero que no detienen la operación de los mismos.	Aquellos recursos o activos de información que al ser afectados interfieren en las operaciones de soporte de la entidad o los colaboradores, como la Operación del correo electrónico. Servicios de Internet Servicios de telefonía IP. Sistema de control de acceso físico. Es importante tener presente que en esta categoría solo debe presentarse uno de los eventos anteriormente mencionados	Aquellos recursos o activos de información que al ser afectados interfieren en las operaciones misionales y de soporte de la entidad o de los colaboradores, que afectan de manera parcial o total la prestación de los servicios de la entidad.

6.1.2. CRITICIDAD DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La criticidad para la valoración de los incidentes de seguridad de la información está definida según la matriz de probabilidad e impacto, basado en la guía para la Administración del Riesgo y Oportunidades tal como se ilustra a continuación:

Probabilidad de Ocurrencia	**Impacto del Incidente**			
	MENOR (2)	*MODERADO (3)*	*MAYOR (4)*	*CATASTRÓFICO (5)*
Casi seguro (todos los meses)	Media	Medio	Alto o Critico	Alto o Critico
Probable (cada 6 meses)	Bajo	Medio	Alto o Critico	Alto o Critico
Posible (cada año)	Bajo	Bajo	Medio	Alto o Critico
Raro (cada 3 años o más)	Bajo	Bajo	Medio	Medio

6.1.3. TIEMPO DE ATENCIÓN DE UN INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

La atención del incidente se define en una escala de tiempo (Horas y días) y está estrechamente relacionada de acuerdo al nivel de criticidad de los incidentes de seguridad. La escala está definida como el tiempo máximo que puede tardarse en atender, o poner en marcha la gestión de atención de incidentes de seguridad de la información, más no necesariamente en dar su respuesta.

Calificación del Incidente	**Escala de Tiempo para atención al incidente**
Alto o Critico	2 Horas
Medio	1 Día
Bajo	1 Semana

6.2. DETECCIÓN

La detección de un incidente involucra que se deba identificar el incidente, validar si de acuerdo con los lineamientos definidos se considera un incidente de seguridad de la información, clasificar el incidente y reportarlo ante las personas y/o autoridades que correspondan.

Los incidentes pueden ser detectados desde las siguientes fuentes:

- Sistemas de detección automáticas de intrusiones (IDS/IPS), sistemas de antivirus.
- Sistemas de logs de sistemas de información, firewalls, Proxy, y auditorias.
- Reportes de los usuarios de la entidad

Es importante mencionar que todos los incidentes de seguridad deben ser canalizados hacia seguridad de la información, bien sea recibidos por medio del procedimiento definido en el proceso de gestión de requerimientos y de gestión de incidentes de seguridad de la información, o por reporte directo de algún colaborador de la entidad.

Para la tipificación del reporte de los incidentes a los niveles adecuados se debe tener en cuenta la siguiente información:

Escenarios de Incidentes	**Criticidad del Incidente**	**Personas Notificadas**	**Tipo de Incidente**
Ataques	Bajo hasta Crítico	Deben ser atendidos por el Oficial de Seguridad de la Información, en coordinación con el área de Servicios de TI. Se deben registrar en un informe y reportar al Comité de Gestión y Desempeño. Adicionalmente enviar el reporte a ColCERT.	- Ataque dirigido - Modificación de sitios web (Defacement)
Código malicioso	Bajo	Atendido por la mesa de ayuda y documentado por los mismos. Los reportes de atención de código malicioso deben ser informados a la gerencia de seguridad de la información.	- Infección Única
	Medio hasta Crítico	Deben ser atendidos por la gerencia de seguridad de la información, en coordinación con el área de Servicios de TI.	- Infección extendida

Escenarios de Incidentes	Criticidad del Incidente	Personas Notificadas	Tipo de Incidente
		Se deben registrar en un informe y reportar al Comité de Gestión y Desempeño. Adicionalmente enviar el reporte a ColCERT.	
Denegación del servicio	Bajo	Estos casos deben ser atendidos por los administradores de servicios, y con una debida notificación al propietario del activo de información implicado. De igual manera la notificación debe ser extensiva a Seguridad de la Información. Al terminar el proceso se debe entregar un informe por parte del administrador a las partes interesadas, propietario y a Seguridad de la Información, para registrar la situación presentada.	- No exitosa
	Medio hasta Crítico	Estos casos deben ser atendidos por los administradores de servicios con el dominio de seguridad de la información, con una debida notificación al propietario del activo de información implicado. Al terminar el proceso el administrador del servicio debe generar un informe para las partes interesadas, el propietario del activo de información y Seguridad de la Información. Se deben reportar al Comité de Gestión y Desempeño. Adicionalmente enviar el reporte a ColCERT.	- Exitosa
Acceso no autorizado	Bajo hasta Crítico	Estos casos deben ser atendidos por el Oficial de Seguridad de la información con una debida notificación al propietario del activo de información implicado.	- Acceso no autorizado
Robo o pérdida de equipos	Bajo hasta Crítico	Estos casos deben ser atendidos por el Grupo de Gestión de Seguimiento y Operación Administrativa, previa notificación del propietario del activo de infraestructura o cualquier colaborador de la entidad. Se debe registrar el incidente y reportar al Comité de Gestión y Desempeño. Si es Alto hasta Crítico enviar el reporte a ColCERT.	- Robo o pérdida de equipos
Perdida o alteración de Datos	Bajo hasta Crítico	Estos casos deben ser atendidos por el Oficial de Seguridad de la información. Se debe registrar el incidente. Si es alto o critico se debe reportar al de Gestión y Desempeño. Adicionalmente enviar el reporte a ColCERT.	- Pérdida o alteración de datos
Escaneo, pruebas y reconocimientos	Bajo hasta Crítico	Estos casos deben ser atendidos por el Oficial de Seguridad de la información, este debe llevar un registro de estos incidentes y según la criticidad, escalarlo.	- Pruebas no Autorizadas
Daños físicos	Bajo hasta Medio	Estos casos deben ser atendidos por el Grupo de Gestión de Seguimiento y Operación Administrativa y se debe informar a Seguridad de la Información, el cual llevará un registro de estos incidentes.	- Daños o cambios físicos no autorizados. -Alarmas de sistemas de monitoreo de zonas de bajo riesgo.
	Alto hasta Crítico	Estos casos deben ser atendidos por el Grupo de Gestión de Seguimiento y Operación Administrativa y se debe informar a Seguridad de la Información, el cual llevará un registro de estos incidentes e informará al Comité de Gestión y Desempeño	- Daños o cambios físicos no autorizados. - Alarmas de sistemas de monitoreo en zonas de alto riesgo por la criticidad de la información manejada.
Uso indebido de la información y recursos tecnológicos	Alto hasta Crítico	Estos casos deben ser atendidos por el Oficial de Seguridad de la información, en caso de ser necesario se debe solicitar apoyo a la Oficina de Control Interno para que determine si se debe realizar una investigación. Se debe informar al Comité de Gestión y Desempeño; este tipo de situaciones deben registrarse.	- Abuso de privilegios o de políticas de seguridad de la información - Infracciones de derechos de autor o piratería - Uso indebido de la marca

6.3. CONTENCIÓN

La contención como su nombre lo indica, se refiere a detener el impacto o efecto que un incidente pueda llegar a tener dentro de la infraestructura y arquitectura de la entidad.

Para las clasificaciones definidas se presentan las siguientes acciones:

6.3.1. CRITICIDAD DE INCIDENTE BAJA

Se puede proceder como se considere de acuerdo con las fallas que se presenten; quien atienda el incidente es autónomo para realizar acciones como: reiniciar un componente tecnológico o destruir un documento; sin embargo, esas acciones se podrán complementar con otras que puedan realizar.

Así mismo, debe quedar un registro de estos incidentes, como medida de control y seguimiento de estos, el cual puede ser utilizado posteriormente como base de consulta para la resolución de incidentes futuros, reforzar y/o generar las políticas de seguridad.

6.3.2. CRITICIDAD DE INCIDENTE ALTA

Son trabajos que deben ser realizados por el administrador de la máquina, informados a sus respectivos propietarios y de conocimiento del área de seguridad de la información; sin ser las únicas acciones el administrador puede:

- Reiniciar un servicio de información.
- Realizar cambios en las configuraciones.
- Desconectar por un periodo corto de tiempo, no mayor de 10 minutos un ambiente de red.
- Destruir la información con previa autorización del propietario.
- Reconstruir y recuperar la información en un ambiente de pruebas.
- Remover privilegios de los usuarios.

6.3.3. CRITICIDAD DE INCIDENTE MUY ALTO O CRÍTICO

Son trabajos que deben ser realizados de manera conjunta entre las áreas de Seguridad de la Información, Sistemas de Información y Servicios Tecnológicos, con el apoyo de los Administradores de Plataformas, y con notificación al propietario del activo de información; sin ser las únicas acciones se puede:

- Reiniciar de manera completa un sistema de información.
- Desconectar por largos periodos de tiempo un recurso tecnológico para determinar la falla.
- Remover privilegios de los usuarios.
- Reconstruir en el ambiente de producción.
- Instalar herramientas y software que se requiera.
- Solicitar contacto con entes externos en caso de investigaciones judiciales.
- Indagar, y tomar evidencias a través de procesos forenses para una posible investigación.

6.4. ERRADICACIÓN

Busca remover la causa del incidente. Es importante para esta fase que se determinen las siguientes acciones:

- Causas del incidente, eliminándolas completamente.
- Buscar mejoras en los esquemas de protección actuales.
- Una vez erradicado, realizar pruebas de vulnerabilidad para revisar el estado final.
- En caso de ser necesario restaurar el sistema o reinstalar por completo.
- Revisar los lineamientos y políticas para determinar si deben ser modificados, así como los controles e indicadores de riesgo.

6.5. RECUPERACIÓN

En esta etapa, es necesario que se garanticen las siguientes operaciones:

- Recuperación de los datos y configuraciones.
- Realizar procesos de actualización.
- Mejoramiento de los niveles de auditoría.
- Restablecimiento de los servicios afectados.

6.6. SEGUIMIENTO

Comprobar que todo realmente vuelve a la normalidad, y además se mantenga de la misma manera hasta una nueva eventualidad. Se deben realizar las siguientes tareas.

- Documentar el incidente: Es importante registrar el incidente, para eso se debe usar la herramienta STRATEGOS:
  - Tipo de incidente.
  - Recurso Afectado.
  - Criticidad del incidente.
  - Acciones de tratamiento.
  - Estado del incidente: Abierto (Sin dar una respuesta definitiva al incidente, con lo cual se vuelva a su estado normal de operación), Cerrado (Incidente tratado y manejado adecuadamente)

- Reporte de incidente: Es muy importante tener un reporte de los incidentes de seguridad, el cual debe entregarse de manera trimestral al Jefe de la Oficina de Tecnologías de la Información, en donde se identifique la cantidad de incidentes trimestrales y la forma cómo se han tratado.
- Lecciones aprendidas: Es importante aprender de los incidentes, de tal manera que a la siguiente presencia del mismo tipo de incidente se responda de una manera eficaz, para ello se busca que el registro de estos conlleve a un mejoramiento en los temas de seguridad y protección de la información, así como de sus activos. De igual manera, se debe presentar trimestralmente ante el Comité de Riesgos y Seguridad de la Información, un informe acerca de los incidentes tratados y las acciones emprendidas, de tal forma que se determine las acciones necesarias cuando un incidente se presente más de una vez.

7. CONTROL DE CAMBIOS

Primera Versión

	NOMBRE:	CARGO / ROL	FECHA	FIRMA:
ELABORADO POR:	Francisco Andrés Daza Cardona	Contratista OTI / Oficial de Seguridad de la información	18/07/2018	**Original Firmado**
	Martin J. Puerto Ch.	Contratista Oficina Asesora de Planeación	18/07/2018	**Original Firmado**
REVISADO POR:	Alba Rocío Ortiz Alfaro	Jefe Oficina Asesora de Planeación / Representante de la Dirección para el SIG	19/07/2018	**Original Firmado**
APROBADO POR:	Luis Alberto Clavijo Cuineme	Jefe Oficina de Tecnologías de la Información	18/07/2018	**Original Firmado**

Revisado en sesión del Comité de Gestión y Desempeño el día 12/07/2018, de acuerdo a la resolución 0372 de 2018.