POLÍTICA DE GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

UNIDAD
DE RESTITUCIÓN
DE TIERRAS

Bogotá, junio de 2021

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐ **Fecha de aprobación**: 18/08/2021

TABLA DE CONTENIDO

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐ **Fecha de aprobación**: 18/08/2021

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 los posibles incidentes de seguridad de la información que puedan presentarse al interior de la Unidad Administrativa Especial de Gestión de Restitución de Tierras Despojadas (UAEGRTD).

1. OBJETIVO

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

2. ALCANCE

Este documento contiene los componentes generales de la gestión de incidentes de seguridad, 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

4. Ver definición de los términos en el Sistema de Información STRATEGOS.

5. MARCO NORMATIVO APLICABLE

Ver Normograma en Strategos.

6. 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:

6.1. 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 Servicios de TI

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, deben notificarlo a mesa de servicios 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 servicios 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, proveedor o tercero que evidencie la materialización de un incidente de seguridad dentro de los escenarios mencionados en el cuadro anterior, deben 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.

4.2. 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.

4.3 SISTEMA INTEGRADO DE PLANEACIÓN Y GESTIÓN (SIPG)

El líder del SIPG es el/la Director (a) General de la UAEGRTD, como responsable del direccionamiento estratégico y del seguimiento a la implementación y mejora del SIPG y propende por la consecución de los recursos para su adecuado funcionamiento. El/la Jefe de la Oficina Asesora de Planeación es el representante de la dirección para el SIPG. Se encargará de Informar al Comité Institucional de Gestión y Desempeño sobre el desempeño del SIPG y de cualquier necesidad de mejora en cuanto a los Incidentes de Seguridad de la Información que sean escalados.

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

La UAEGRTD, realizará este proceso de seis pasos para la GISI, los cuales permiten gestionar un incidente desde el momento anterior a su ocurrencia, hasta la forma en cómo se debe aprender y obtener la experiencia para eventos futuros:

Ilustración 1 - Gestión de Incidentes de Seguridad de la Información

5.1. 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 importancias y responsabilidades en la seguridad de la información con todos los colaboradores de la UAEGRTD.

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.

5.1.1. CRITERIOS DE CLASIFICACIÓN DE UN INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: La Gestión de los incidentes de Seguridad de la Información se clasificarán por prioridad y por impacto:

La clasificación de la prioridad se realizará de acuerdo con lo establecido en Strategos en el módulo de gestión de incidentes de seguridad de la información.

Inferior (sistemas no críticos como estaciones de trabajo de usuarios,confusiones no criticas)

Bajo (sistemas que apoyan a una solo dependencia o proceso)

Medio (sistemas que apoyan más de una dependencia o proceso)

Alto (sistemas pertenecientes al proceso de OTI y/o estaciones de trabajo de usuarios con funciones criticas)

Superior(sistemas críticos)

Ilustración 2 - Prioridad en Strategos para incidentes de seguridad

Para clasificar impacto se realizará de la manera como está establecido en Strategos en el módulo de gestión de incidentes de seguridad de la información.

Inferior (impacto leve en uno de los componente de cualquier sistema de información o estación de trabajo)

Bajo (impacto moderado en uno de los componente de cualquier sistema de información o estación de trabajo)

Medio (impacto alto en uno de los componente de cualquier sistema de información o estación de trabajo)

Alto (impacto moderado en uno o más componentes de más de un sistema de información)

Superior (impacto alto en uno o más componentes de más de un sistema de información)

Ilustración 3 - Impacto en Strategos para incidentes de seguridad

5.2. 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 identificación reporte de los incidentes a los niveles adecuados se debe tener en cuenta la siguiente información:

Escenarios de Incidentes	Impacto del Incidente	Personas Notificadas	Tipo de Incidente
Ataques	Inferior hasta Superior	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 Institucional de Desarrollo Administrativo. Adicionalmente enviar el reporte a ColCERT.	- Ataque dirigido - Modificación de sitios web (Defacement)
Código malicioso	Inferior o Bajo	Atendido por la Mesa de Servicio, 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 Superior	Deben ser atendidos por el Dominio de Seguridad de la Información, en coordinación con los dominios de TI afectados. Se deben registrar en un informe y reportar al Comité Institucional de Desarrollo Administrativo. Adicionalmente enviar el reporte a ColCERT.	- Infección extendida
Denegación del servicio	Inferior o Bajo	Estos casos deben ser atendidos el administrador responsable del servicio, y con una debida notificación al dueño del activo de información o servicio 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

Escenarios de Incidentes	Impacto del Incidente	Personas Notificadas	Tipo de Incidente
	Medio hasta Superior	Estos casos deben ser atendidos por los administradores de servicios con el Dominio de Seguridad de la Información, con una debida notificación al dueño 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 o servicio y Seguridad de la Información. Se deben reportar al Comité Institucional de Desarrollo Administrativo. Adicionalmente enviar el reporte a ColCERT.	- Exitosa
Acceso no autorizado	Inferior hasta Superior	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	Inferior hasta Crítico	Estos casos deben ser atendidos por el área Administrativa, previa notificación del propietario del activo, de infraestructura, o cualquier colaborador de la entidad. Se debe registrar el incidente y si es Alto hasta Crítico reportar al Comité Institucional de Desarrollo Administrativo.	- Robo o pérdida de equipos
Perdida o alteración de Datos	Inferior hasta Superior	Estos casos deben ser atendidos por el Oficial de Seguridad de la información. Si es alto o crítico, Se debe registrar el incidente y se debe reportar al Comité Institucional de Gestión y Desempeño. Adicionalmente enviar el reporte a ColCERT.	- Pérdida o alteración de datos

Escenarios de Incidentes	Impacto del Incidente	Personas Notificadas	Tipo de Incidente
Escaneo, pruebas y reconocimientos	Inferior hasta Superior	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	Inferior hasta Medio	Estos casos deben ser atendidos por el área Administrativa.	- Daños o cambios físicos no autorizados. -Alarmas de sistemas de monitoreo de zonas de bajo riesgo.
	Alto hasta Superior	Estos casos deben ser atendidos por el área Administrativa y se debe informar a Seguridad de la Información, la cual llevará un registro de estos incidentes e informará al Comité Institucional 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 Superior	Estos casos deben ser atendidos por el Oficial de Seguridad de la información, en caso de ser necesario se debe solicitar apoyo de Control Interno para que determinar si se debe realizar una investigación. Se debe informar al Comité Institucional 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

5.3. CONTENCIÓN

La contención como su nombre lo indica, es 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:

5.3.1. IMPACTO DE INCIDENTE INFERIOR O 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 eliminar 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 los mismos, y que puede ser utilizado posteriormente como base de consulta para la resolución de incidentes futuros, reforzar y/o generar las políticas de seguridad.

5.3.2. IMPACTO DE INCIDENTE MEDIA:

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 (60 min.), 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.

5.3.3. IMPACTO DE INCIDENTE ALTO O SUPERIOR:

Son trabajos que deben ser realizados de manera conjunta entre los Dominios de Seguridad de la Información, Sistemas de Información, Información e Infraestructura de TI, notificando al propietario del activo de información o servicio. 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.

5.4. 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 realizado, 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.

5.5 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.

5.6 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 aplicación STRATEGOS en el módulo de incidentes de seguridad de la información:
    - 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, ante la ocurrencia de un incidente de seguridad de criticidad medio a critico informar al Jefe de la Oficina de Tecnologías de la Información, acerca de la gestión realizada sobre los incidentes 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 el registro de los mismos que conlleve a un mejoramiento en los temas de seguridad y protección de la información, así como de sus activos.

6. CONTROL DE CAMBIOS

Primera versión: Inicial
Segunda Versión

- ✓ Ajustes en el objetivo
- ✓ Ajustes en la terminología como mesa de ayuda por mesa de servicios, servicios tecnológicos por dominio de infraestructura de TI, etc.
- ✓ Descripción del comité de gestión y desempeño.
- ✓ Rol de la alta dirección en la gestión de incidentes.
- ✓ mención a la GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO Y OPORTUNIDADES de la UAEGRTD
- ✓ Cambios en la presentación de reportes trimestrales por informar inmediatamente al Jefe de la OTI sobre la ocurrencia de un incidente medio hasta superior.

- ✓ Ajustes a los criterios para definir los impactos de un incidente de acuerdo con la herramienta de Strategos.

7. PARTICIPANTES EN LA ELABORACIÓN

Francisco Daza – Oficial de Seguridad– Oficina de tecnologías de la información