GUÍA PARA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

1. ANEXO NO. 1 – CATEGORÍA DE INCIDENTE DE SEGURIDAD INFORMÁTICA

Acceso lógico no autorizado.
Ingreso de personas no autorizadas a su información.

Bloqueo de cuenta debido a intentos de contraseña incorrecta.
Acceso lógico no autorizado.
Sistema o aplicación que no cumple las políticas de contraseñas.
Cuenta no autorizada o sin debida novedad.
Privilegios de administración no autorizados.
Denegación de privilegios.
Modificación no autorizada de privilegios.

Seguridad de Redes.
Evidenciar acceso no autorizado a la red de la entidad, el uso indebido, la modificación o la denegación de una red informática y sus recursos accesibles.

Eventos irregulares en la infraestructura de red.
Eventos irregulares en dispositivos de seguridad perimetral.
Conexión no autorizada de terceros.
Pruebas de penetración no autorizadas.
Cambios no autorizados en los dispositivos de seguridad perimetral.
Uso no autorizado de utilitarios (rootkit).
Ataques contra servidores de nombre de dominios (DNS).
Ataques contra sistema cortafuegos (firewall).
Ataques externos a los activos.
Ataques internos a los activos.
Ataques contra sitios web.
Ataques contra componentes de red (routers/switches/accesspoint).
Ataques contra sistemas de producción o contingencia.
Ataques contra la infraestructura IT.

Manejo de la información.
Detección del acceso no autorizado a información que usted maneja, reportar cambios o pérdida de la información física o digital.

Uso no autorizado de mensajería electrónica (carta cadena, spam)
Divulgación no autorizada de información clasificada o reservada.
Pérdida de archivos almacenados.
Divulgación no autorizada de datos.
Pérdida de datos de clientes o datos personales.
Inadecuada clasificación, etiquetado y manejo de la información.

Incumplimiento normativo o de políticas.
Función que permite a las organizaciones detectar y gestionar el riesgo de cumplimiento de las obligaciones regulatorias internas y externas a través de políticas o procedimientos adecuados

Incumplimiento de la normatividad colombiana relacionada con la seguridad de la información.
Incumplimiento de las políticas específicas de seguridad de la información de la ANT.

Indisponibilidad de servicios o sistemas.
Reportar malfuncionamiento de las herramientas tecnológicas que utiliza para el desarrollo de sus actividades.

Mal funcionamiento o problemas de equipos.
Error de configuración de aplicaciones.
Funcionamiento inadecuado de software.
Indisponibilidad de servicios de red o aplicaciones.
Fallas eléctricas
Problemas de hardware
Problemas de temperatura

Código malicioso.
Software dañino o software malintencionado que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.

Malware (adware, spyware, activex, vbscript, backdoor, trapdoor).
Virus (gusanos, troyanos, hoax).
CallBack
Botnet
Ransoware

Otros

Reporte de controles ineficientes.
Desastres naturales.
Violación de controles de seguridad.
Fraude o actividad criminal.

Acceso físico no autorizado
Reportar evidencias de acceso no autorizado al datacenter de la ANT.

Acceso físico no autorizado.
Pérdida o robo de infraestructura de red (routers, switches).
Pérdida o robo de otros activos tecnológicos (printers, token, RAM).
Fallas en centros de datos o cuartos de comunicaciones.
Consolas de administración sin protección.
Acceso físico no autorizado.

2. ANEXO NO. 2 – NIVELES DE CLASIFICACIÓN

En la siguiente tabla se definen los niveles de clasificación de incidentes de seguridad de la información definidos en la Agencia Nacional de Tierras (ANT). La descripción de la afectación del mismo en cuanto a la confidencialidad, disponibilidad e integridad de la información en sus diferentes estados:

NIVEL	RANGO	DESCRIPCIÓN	AFECTACIÓN PORCENTUAL DE LA OPERACIÓN
4	**Críticos**	El incidente provoca efectos críticos para la confidencialidad, integridad y disponibilidad de los activos de información críticos de la Agencia Nacional de Tierras (ANT).	76% a 100%
3	**Grave**	El incidente provoca efectos graves para la confidencialidad, integridad y disponibilidad de los activos de información críticos de la Agencia Nacional de Tierras (ANT).	51% a 75%
2	**Moderado**	El incidente provoca efectos moderados para la confidencialidad, integridad y disponibilidad de los activos de información críticos de la Agencia Nacional de Tierras (ANT).	26% a 50%
1	**Bajo**	El incidente provoca efectos bajos para la confidencialidad, integridad y disponibilidad de los activos de información críticos de la Agencia Nacional de Tierras (ANT).	0% A 25%

Tabla 1. Clasificación del nivel de la gestión de incidentes

Crítico: Este nivel se da para aquellos incidentes que son detectados y/o notificados, porque en ellos, es posible establecer una amenaza capaz proporcionar acceso a datos y sistemas no autorizados, a un nivel de administración. Los aspectos de confidencialidad y/o integridad y/o disponibilidad de los activos de información de la Agencia Nacional de Tierras (ANT), afectando la continuidad del negocio en un porcentaje mayor al 75%. ***Prioridad de atención:*** Inmediata.

Grave: Este nivel se da para aquellos incidentes que son detectados y/o notificados, porque en ellos, es posible establecer una amenaza capaz de impactar de manera considerable los aspectos de confidencialidad y/o integridad y/o disponibilidad de los activos de información de la Agencia Nacional de Tierras (ANT), afectando la continuidad del negocio en un porcentaje mayor al 50%. ***Prioridad de atención:*** Inmediata.

Moderado: Este nivel de criticidad se da para aquellos incidentes que sean reportados como posibles amenazas, que pueden afectar los activos de información de la entidad, impactando de modo limitado sus características de confidencialidad y/o integridad y/o disponibilidad frente a un activo crítico para la Agencia Nacional de Tierras (ANT). Adicionalmente su porcentaje de afectación a la continuidad del negocio está en un rango entre el 25% y 50%. ***Prioridad de atención:*** Entre 4 y 8 horas.

Bajo: Este nivel de criticidad se da para aquellos incidentes o eventos que sean reportados como posibles amenazas para los activos de información, es decir, que pueden impactar sus características de confidencialidad y/o integridad y/o disponibilidad, sin embargo, los controles de seguridad resultan efectivos anulando cualquier impacto para la Agencia Nacional de Tierras (ANT). Así mismo su porcentaje de afectación a la continuidad del negocio no supera el 25%. Si la evaluación da en este rango, se determina como evento de seguridad de la información. ***Prioridad de atención:*** Entre 8 y 24 horas.

3. ANEXO No. 3 – PLANES DE RESPUESTA A INCIDENTES

A continuación, se describen los planes generales de respuesta a incidentes por cada una de las categorías de incidentes. Sin embargo, dado que todos los incidentes no suceden bajo el mismo contexto o con las mismas características, el responsable de atender el incidente deberá utilizar estos planes como base y profundizar o complementar las actividades descritas para dar respuesta a la situación específica.

3.1. Seguridad física

Durante el Incidente:

a) Alertar al proveedor de seguridad física y guardas de seguridad.
b) Notificar oportunamente al personal de la Entidad sobre el desplazamiento fuera del sitio donde se encuentra el personal no autorizado.
c) Notificar el incidente de forma oportuna a los entes de control y de apoyo. Policía y Cuadrante.
d) Intentar identificar el sospechoso tomando registro a partir de la observación, fotos, videos o cualquier otro medio que permita reconocerlo posteriormente.
e) Seguir las directrices del proveedor de vigilancia y de la Policía.

Posterior al Incidente:

f) Identificar y evaluar la afectación física y daños causados por la intrusión.
g) Determinar el alcance del incidente. Por ejemplo, si existen equipos tecnológicos físicos involucrados, conexión de medios físicos en equipos o puntos de red, o elementos físicos que atenten contra las personas de la Entidad o su información.

3.2. Control de acceso

Durante el Incidente:

a) Realizar una verificación de conexiones activas a los equipos donde se detectó el incidente.
b) Efectuar actividades de recolección de evidencia de acuerdo con los procedimientos del Tercero experto.
c) Desconectar el cable de red en caso de que se detecten transferencias de archivos, extracción o borrado de información.
d) Realizar copia de logs del activo de información o aplicación objeto del incidente.
e) Realizar la verificación de logs con el fin de identificar la naturaleza de la intrusión.
f) Realizar cambios de contraseñas desde otros equipos (Por ejemplo, si se usó una cuenta del directorio activo para cometer la intrusión).
g) Determinar el alcance del incidente en cuanto a los equipos afectados, la información comprometida, modificada o eliminada.
h) Aislar completamente los equipos afectados.

Después del incidente:

i) Verificar la afectación final causada por el incidente.
j) Erradicar. Es decir, reinstalar el sistema operativo o firmware de los equipos comprometidos y restaurar backup de configuraciones e información. Si es necesario, ajustar políticas de control de acceso lógico.

3.3. Código Malicioso

Durante el Incidente:

Aislar el equipo de la red. Esto incluye desconexión del cable de red y de red inalámbrica.

a) Efectuar actividades de recolección de evidencia de acuerdo con los procedimientos del Tercero experto.
b) Apagar el (los) equipo(s) de forma manual, oprimiendo el botón de apagado.

Después del Incidente:

c) Verificar la afectación final causada por el incidente en cuanto a información comprometida, modificada o eliminada.
d) Erradicar. Es decir, reinstalar el sistema operativo o firmware de los equipos comprometidos y restaurar backup de configuraciones e información.
e) Con las copias de disco tomadas por parte del Tercero experto, analizar posteriormente el comportamiento del malware y determinar el origen de intrusión y su forma de replicación.

4. Manejo de la información

a) Determinar la cantidad y tipo de información comprometida, modificada o eliminada.
b) Alertar a los involucrados sobre el incidente.
c) Seguir los pasos descritos en los demás planes de respuesta del presente documento con el fin de determinar las acciones técnicas que se deben aplicar dependiendo del tipo de ataque bajo el cual se afectó la información.

5. Indisponibilidad de servicios o sistemas

Durante el incidente:

a) A través de un diagnóstico, determinar el alcance del incidente. Es decir, los equipos afectados por el ataque.
b) Identificar los orígenes a través de los cuales se está cometiendo el incidente. Esto incluye revisión de información de logs en switchs, firewall u otros dispositivos de red, así como las conexiones abiertas en el equipo afectado.
c) Notificar al proveedor de servicios de red (interno o externo) con el fin de generar los respectivos bloqueos de direcciones IP y tipo de paquetes.
d) Validar si es posible aumentar las conexiones concurrentes del equipo afectado mientras se realizar la contención.
e) Reducir los tiempos de respuesta de las conexiones iniciadas con el equipo perimetral o en su defecto, con el equipo afectado.

Después del incidente:

f) Detectar los orígenes generadores de conexiones y denegación de servicio.
g) Reportar lo sucedido con los entes de control ColCERT, CSIRT, Policía, entre otros.
h) En caso de que sea requerido, restaurar los servicios a la normalidad. A través de backups de configuración o información.

5.1. Ingeniería Social

Durante el Incidente:

a) Dependiendo del tipo de ataque de ingeniería social, se aplican los planes de respuesta de “Código Malicioso”, “Manejo de la Información”, “Acceso lógico no autorizado” o” Acceso físico no autorizado”.
b) Adicionalmente, en caso de que se presenten ataques de dichas categorías o Phishing, Malware en USB, entre otros, se debe notificar oportunamente a TODA la entidad, con el fin de que no se propague a más funcionarios o contratistas dicho ataque.
c) Determinar y diagnosticar el origen del incidente. Identificar Direcciones IP, cuentas de correo electrónico, páginas web, entre otros, que sean origen del incidente o medios por los cuales se está replicando el ataque.
d) Bloquear dichos orígenes en los dispositivos de la Agencia.

Después del Incidente:

e) Reportar el incidente a los entes de control ColCERT, CSIRT, Policía, MINTIC entre otros.
f) Sensibilizar a los usuarios a través de campañas publicitarias sobre el ataque sucedido y mejores prácticas para prevenir los ataques de ingeniería social.

5.5. Incumplimiento de normatividad o de políticas

Para esta categoría se debe:

a) Diagnosticar el nivel de impacto que tiene el incidente.
b) Notificar el incidente al Oficial de Seguridad, al Equipo de Infraestructura y Soporte Tecnológico y Jefe Inmediato, con el fin de que se definan las acciones internas y/o legales a tomar, dependiendo de la criticidad del incidente.
c) Notificar al usuario la violación de la política específica de seguridad de la Información y las implicaciones legales del caso. En caso de que sea un origen externo, se debe manejar a través de los Entes de control como ColCERT, CSIRT, Policía, MINTIC entre otros.

6. CONTROL DE CAMBIOS

HISTORIAL DE CAMBIOS		
Fecha	**Versión**	**Descripción**
03-11-2020	01	Primera versión del documento.

Elaboró: Alexandra Ruiz Bedoya	**Revisó**: Duberly Eduardo Murillo Barona	**Aprobó**: Felipe A. Espinosa Camacho
	Cargo: Subdirector de Sistemas de Información de Tierras	
Cargo: Contratista - Secretaría Genera	**Firma**: ORIGINAL FIRMADO	
	Revisó: Carlos Alberto Salinas Sastre	
Firma: ORIGINAL FIRMADO	**Cargo**: Secretario General	
	Firma: ORIGINAL FIRMADO	
Elaboró: Cesar Da Ferzón Mosquera Valencia	**Revisó**: Daniel Alejandro Camargo Rodríguez	**Cargo**: Director de Gestión de Ordenamiento Social de la Propiedad
Cargo: Contratista Subdirección de Sistemas de Información de Tierras	**Cargo**: Contratista Dirección de Gestión de Ordenamiento Social de la Propiedad	
Firma: ORIGINAL FIRMADO	**Firma**: ORIGINAL FIRMADO	
Elaboró: Andrés Fernando Cabrera Ochoa	**Revisó**: Fabián Augusto Patarroyo Morales	
Cargo: Contratista Subdirección de Sistemas de Información de Tierras	**Cargo**: Contratista - Secretaría Genera	**Firma**: ORIGINAL FIRMADO
Firma: ORIGINAL FIRMADO	**Firma**: ORIGINAL FIRMADO	