Agencia Nacional de Tierras	PROCEDIMIENTO	PROCEDIMIENTO GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	CÓDIGO	GINFO-P-011
	ACTIVIDAD	ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES	VERSIÓN	1
	PROCESO	GESTION DE LA INFORMACIÓN	FECHA	3-nov.-20

OBJETIVO	Establecer las directrices necesarias para la detección, registro y clasificación de los incidentes y/o eventos de seguridad; junto con su análisis, investigación, contención y erradicación del mismo, estableciendo un plan de recuperación de aquellos eventos de interrupción que afecten la confidencialidad, integridad, disponibilidad de la información, así como la posible afectación de las actividades de la Agencia Nacional de Tierras (ANT).
ALCANCE	Aplica a todas las fallas de control e incidentes de seguridad de la información, que sucedan durante actividades desarrolladas por funcionarios, contratistas, terceros y visitantes en general de la Agencia Nacional de Tierras (ANT). La gestión de fallas de control e incidentes va desde la detección en la entidad hasta la divulgación de las lecciones aprendidas con el fin de generar conciencia sobre los mismos al interior de la Agencia Nacional de Tierras (ANT) y el aseguramiento de la aplicación de la mejor práctica, para evitar su ocurrencia en el futuro.
RESPONSABLE	Subdirección de Sistemas de Información de Tierras Equipo de Infraestructura y Soporte Tecnológico

1. DEFINICIONES (Términos y Siglas)

Incidente de Seguridad de la Información: es el resultado de un evento o una serie de eventos de seguridad de la información no deseada o inesperada, que tienen la probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (confidencialidad, integridad y disponibilidad).

Activos de información: son los recursos que utiliza un Sistema de Gestión de Seguridad de la Información para que las organizaciones funcionen y consigan los objetivos que se han propuesto por la alta dirección.

Causas: La razón por la cual se sucede el evento y cuya identificación depende del nivel de experiencia sobre el entorno y los elementos involucrados.

Contención: Son aquellas acciones tendientes a evitar la propagación de la amenaza que ocasiono el incidente de seguridad de la información detectado.

Control: Cualquier acción o elemento del sistema de gestión cuyo propósito es el de prevenir la ocurrencia de un incidente o disminuir la severidad de las consecuencias.

Erradicación: Una vez el incidente de seguridad de la información es contenido, este debe erradicarse, es decir, eliminar cualquier tipo de rastro que pudiera existir con ocasión de comportamiento inusual sobre los activos de información y/o infraestructura de TI.

Evento de Seguridad de la Información: Es 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, la falla de las salvaguardas o una situación desconocida previamente que puede ser pertinente para la seguridad. En resumen, el evento se clasifica como “Evento de seguridad” cuando la confidencialidad, integridad o disponibilidad de la información no se ha comprometido aún o su probabilidad de afectar negativamente la información del negocio es baja.

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

Antivirus: son programas cuyo objetivo es detectar y eliminar virus informáticos

Amenaza informática: es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas.

Riesgo: es un incidente o situación, que ocurre en un sitio concreto en un intervalo de tiempo determinado, con consecuencia negativas o positivas que pueden afectar el cumplimiento de los objetivos.

Firewall (llamado también «cortafuego»): es un sistema que permite proteger a una computadora o una red de computadoras de las intrusiones que provienen de una tercera red (expresamente de Internet)

Equipo de respuestas ante incidentes de seguridad de la Información CSIRT: es un centro de respuesta a incidentes de seguridad en tecnologías de la información. Se trata de un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información

COLCERT: es el organismo coordinador a nivel nacional en aspectos de ciberseguridad y ciberdefensa En colombia.

Aranda: SOFTWARE DELIVERY (ASD), es la solución que facilita la distribución centralizada y programada de software y archivos en cualquiera de las estaciones de trabajo de una organización, en forma desatendida y sin interferir en la productividad de los usuarios.

Monitoreo: Verificación, supervisión, observación crítica o determinación continúa del estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado.

Oficial de Seguridad de la Información: Persona responsable de planificar, desarrollar, controlar, velar y gestionar el cumplimiento de las políticas, procedimientos y acciones de la Seguridad de la Información con el fin de obtener la mejora continua y propender por la protección de la confidencialidad, integridad y disponibilidad de la información.

Propietario del activo: Persona o cargo que administra, autoriza el uso, regula o gestiona el activo de información. El propietario del activo aprueba el nivel de protección requerido frente a confidencialidad, integridad y disponibilidad.

Vulnerabilidad: Debilidad identificada sobre un activo y que puede ser aprovechado por una amenazas para causar una afectación sobre la confidencialidad, integridad y/o disponibilidad de la información.

2. GENERALIDADES

3. RIESGOS Y CONTROLES ASOCIADOS AL PROCEDIMIENTO

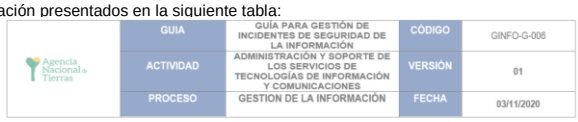
A partir del análisis de los riesgos que pueden afectar el cumplimiento de los objetivos de los procesos, la Oficina de Planeación orienta a las dependencias en la identificación de las tareas críticas de sus procedimientos en las que se puede materializar un riesgo y el establecimiento de las correspondientes tareas de control preventivo, detectivo o correctivo.

Para facilitar la identificación de las tareas críticas y las correspondientes tareas de control, el procedimiento presenta el siguiente método de señalización:

Tareas Críticas	Son las tareas donde se puede materializar un riesgo que impacte negativamente el logro del objetivo del procedimiento. En la matriz de desarrollo del procedimiento y en el diagrama de flujo se identifican tareas críticas con **texto en color rojo** y con el símbolo ®

Tareas de Control	Son las tareas que permiten prevenir o corregir el impacto de los riesgos en el logro del objetivo del procedimiento. En la matriz de desarrollo del procedimiento y en el diagrama de flujo se identifican tareas de control con **texto en color azul** y con el símbolo ©

4. DESARROLLO DEL PROCEDIMIENTO

No	Tarea	Descripción	Tiempo de Ejecución	Responsable
1	Categorizar y clasificar el incidente de seguridad	Los responsables deberán categorizar el incidente de seguridad de la información, acorde con el **anexo 1 GINFO-G-006-Guía de Gestión de Incidentes de Seguridad de la Información** y posteriormente realizar su clasificación según el nivel, rango y porcentaje de afectación presentados en la siguiente tabla:  Agencia Nacional de Tierras GUIA: GUÍA PARA GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN — CÓDIGO: GINFO-G-006 ACTIVIDAD: ADMINISTRACIÓN Y SOPORTE DE LOS SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES — VERSIÓN: 01 PROCESO: GESTION DE LA INFORMACIÓN — FECHA: 03/11/2020 **NIVEL / RANGO / DESCRIPCIÓN / AFECTACIÓN PORCENTUAL DE LA OPERACIÓN** 4 — Críticos — El incidente provoca efectos crítico 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 grave 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* Posteriormente, se deberá diligenciar la **GINFO-F-028-Registro de Incidentes de Seguridad de la Información.**		Equipo de Infraestuctura y Soporte Tecnologico Oficial de Seguridad o quien haga sus veces
2	Dectectar investigar y analizar incidente	Los responsables deberán detectar, investigar y analizar lo ocurrido y en caso necesario realizar una visita al lugar de los hechos y: 1. Revisar las posibles causas, efectos y daños. 2. Revisión y análisis de logs, archivos, plataforma y otros elementos involucrados. 3. Determinar si fue generado por un trabajador de la ANT o un externo. 4. Realizar un plan de acción para determinar las actividades de contención, erradicación y recuperación frente a los servicios y/o plataformas afectadas por el incidente de seguridad de la información. Para este Plan se deben considerar las actividades mencionadas en el "Anexo - Procedimiento de Gestión de Incidentes de seguridad de la Información".		Equipo de Infraestuctura y Soporte Tecnologico Oficial de Seguridad o quien haga sus veces
3	Contener el incidente	Los responsables deberán realizar la contención del incidente de manera inmedita evitando cualquier tipo de propagación que pueda seguir afectado los activos de información de la Agencia Nacional de Tierras (ANT). En caso que los responsables puedan remediar el incidente de seguridad, proceden con la actividad "Notificar incidente", de lo contrario, pasa a la actividad "Escalar atención del incidente".		Equipo de Infraestuctura y Soporte Tecnologico Oficial de Seguridad o quien haga sus veces
4	Notificar incidente	Los responsables determinarán los entes de control a los cuales se notificará, comunicará y denunciará el incidente (en el caso que se necesario) según sea el caso y de acuerdo con el procedimiento de **GTHU-P-018 CONTROL INTERNO DISCIPLINARIO – PROCESO VERBAL**.		Equipo de Infraestuctura y Soporte Tecnologico Oficial de Seguridad o quien haga sus veces
5	Escalar atención del incidente	En caso de que la remediación no pueda ser ejecutada por los respondables, deberán ser escalado a un tercero experto salvaguardando la confidencialidad, integridad y disponibilidad de la información a la que tuvieran acceso con el fin de recibir apoyo para la solución del incidente de seguridad, por lo tanto, deberán ejecutar como mínimo las siguientes actividades: 1) Contactar al Equipo de Respuesta a Incidentes del Gobierno Nacional (ColCERT, CSIRT Policía nacional y MINTIC) y reportar el incidente de seguridad de la información. 2) Entregar los detalles de investigación, análisis y acciones ejecutadas al Equipo de Respuesta a Incidentes del Gobierno Nacional.	8 Horas	Equipo de Infraestuctura y Soporte Tecnologico Oficial de Seguridad o quien haga sus veces
6	Erradicar incidente	Después de que el incidente haya sido contenido se realiza la erradicación y eliminación de los rastros generados por el mismo, por lo cual se solicita la autorización al responsable del activo afectado y se ejecutan las siguientes acciones: 1) Eliminar las causas del incidente 2) Mejorar los esquemas de seguridad y protección actuales 4) Reinstalar o restaurar los sistemas afectados. 3) Revisar los lineamientos y política de seguridad de la información para determinar si requiere algún ajuste. Todos estos detalles deben quedar documentados en el formato **GINFO-F-028-Registro de Incidentes de Seguridad de la Información.**		Equipo de Infraestuctura y Soporte Tecnologico Oficial de Seguridad o quien haga sus veces

7	Recuperar sistemas	Los reponsables proceden con la remediación de los servicios y/o sistemas afectados fortaleciendo los controles y evitando futuros incidentes similares, para lo cual deberán ejecutar las siguientes acciones en caso necesario: 1) Recuperar o implementar nuevas configuraciones de seguridad 2) Recuperar o restaurar backups de bases de datos, servidores e información general. 3) Implementar auditorias y/o fortalecer las existentes 4) Programar alertas y notificaciones de seguridad 5) Reestablecer los servicios afectados. 6) Hacer pruebas de Vulnerabilidad para revisar el estado final		Equipo de Infraestuctura y Soporte Tecnologico Oficial de Seguridad o quien haga sus veces
8	Cerrar incidente	Los responsables deben registrar en el **GINFO-F-028-Registro de Incidentes de Seguridad de la Información** los hechos, análisis, impacto y solución de las actividades realizadas para solucionar el incidente de seguridad de la información y documentarlo en la mesa de servicios de TI.		Equipo de Infraestuctura y Soporte Tecnologico Oficial de Seguridad o quien haga sus veces
9	Revisar post incidente de seguridad	Los responsables deben realizar una mesa de trabajo, en la cual se discutan las lecciones aprendidas para fortalecer e implementar nuevos controles de seguridad de la información y proceder de una manera más efectivas en la presentación de eventos similares.		Equipo de Infraestuctura y Soporte Tecnologico Oficial de Seguridad o quien haga sus veces

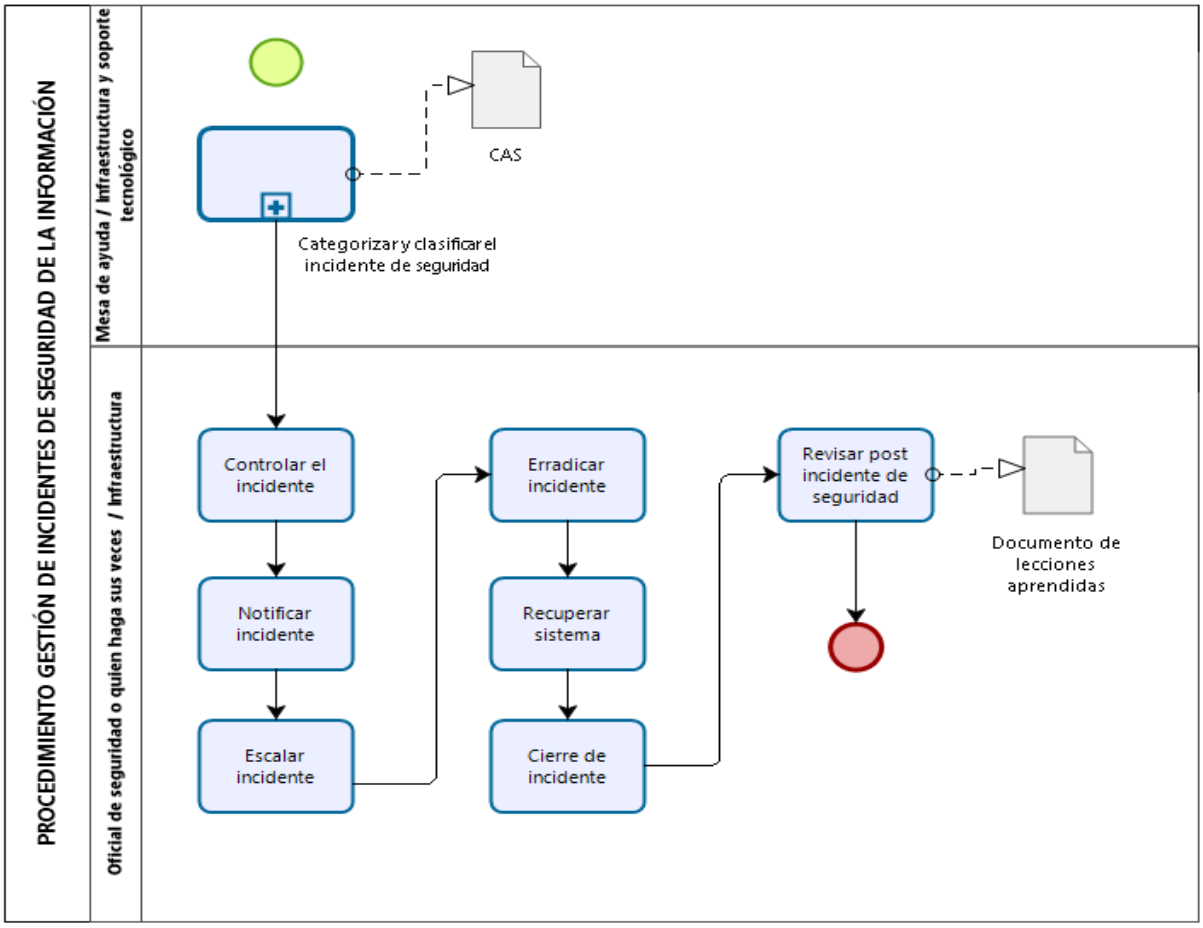
5. NORMATIVIDAD APLICABLE

La ANT incluye este control como requisito de la NTC-ISO-IEC 27001:2013 para su SGSI.
Decreto 2573 de 2014. Lineamientos Generales estrategia GEL. Aspectos relacionados con seguridad y privacidad de la información.
Decreto 1008 de 2018. Por el cual se establecen lineamientos generales de la política de Gobierno Digital.
Ley 1581 de 212. Por la cual se expide el Regimen General de Protección de Datos Personales.
Ley 23 de 1982 Sobre los Derechos de Autor.

6. DOCUMENTOS ASOCIADOS

SGSI-F-011- Registro de Incidentes de Seguridad de la Información.
SGSI-D-012-Directorio de Contacto de Autoridades y GE.

7. DIAGRAMA DE FLUJO



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