TABLA DE CONTENIDO

1. OBJETIVO

Establecer los lineamientos para dar respuesta a los incidentes de seguridad de la información que se les pueda presentar a todas las personas (funcionarios, contratistas y proveedores) que tenga acceso a los recursos de información y tecnología de Parques Nacionales Naturales de Colombia.

2. ALCANCE

Inicia con la identificación y análisis del incidente y finaliza con la respuesta a los incidentes de seguridad de la información que se pueden presentar en todos los niveles de gestión de Parques Nacionales Naturales de Colombia.

3. DEFINICIONES

Evento: Es cualquier situación observable en el comportamiento de un equipo o servicio de tecnología. Los eventos pueden ser normales o anormales. Algunos ejemplos de eventos incluyen situaciones como: ingreso de un usuario a la red de computadores, el inicio de una copia de respaldo, la verificación de la dirección de destino de correo electrónico por parte del servidor de correo, un usuario enviando un correo electrónico, un firewall bloqueando o una conexión no autorizada. Los eventos pueden tener efectos negativos para los servicios o equipos de información o tecnología, como, por ejemplo: caída de servicios, saturación de canales de red, fallas en los sistemas de respaldo de información, energía o refrigeración, acceso no autorizado a sistemas o información confidencial, ejecución de código malicioso o destrucción de equipos

Incidente de seguridad: Un incidente de seguridad de la información es cualquier evento que puede dañar o representar una amenaza para toda o una parte de la infraestructura tecnológica y activos de información de PARQUES NACIONALES NATURALES DE COLOMBIA (sistemas de cómputo, sistemas de información, red de datos), como pueden ser: ausencia de servicios, indisponibilidad de los sistemas de información, incluyendo cambios no autorizados al hardware, firmware, software o datos

Incidente de seguridad computacional: Es una violación o potencial amenaza de violación[i] de las políticas de seguridad de la información, los procedimientos de seguridad de la información o la reglamentación que cobija el uso de los servicios o equipos de información de tecnología. Algunos ejemplos de incidente computacional incluyen:

- **Denegación de servicios**: Un atacante envía un paquete de datos que bloquea o congestiona el servidor de páginas web y suspende el sitio web. Un atacante coordina a miles de estaciones de trabajo externas a la red para que envíen miles de solicitudes ICMP a la red de la entidad para que se inhabiliten los servicios de red.
- **Código malicioso**: Un gusano informático usa archivos compartidos para contaminar cientos de estaciones dentro de la entidad. La entidad recibe un reporte del vendedor de sus antivirus en donde alerta de un virus que se

dispersa a gran velocidad mediante correo electrónico por Internet. El virus aprovecha una vulnerabilidad presente en los servidores de la entidad, basado en la experiencia de la entidad en otros incidentes se estima que el virus podría afectar a los equipos en un lapso de tres horas.

- **Acceso no autorizado**: Un atacante utiliza una herramienta de explotación de vulnerabilidades para tener acceso al archivo de password de usuarios. Un perpetrador obtiene acceso no autorizado a nivel de administrador a un servidor y a la información confidencial que contiene y luego intimida a la víctima amenazando la de divulgar a la prensa la información si no realiza el pago de un dinero.
- **Uso inapropiado**: Un usuario entrega copias de software de la entidad a personas no autorizadas. Una persona amenaza a otra vía correo electrónico.

Sistema de información: Cualquier equipo de cómputo o telecomunicaciones, sistema o subsistema interconectado o no conectado usado para la adquisición, almacenamiento, manipulación, gestión, movimiento, control, despliegue, conmutación, intercambio, transmisión o recepción de voz, datos, vídeo en formas análogas o digitales, así como el software, firmware o hardware que forme parte del sistema.

Clasificación y priorización de servicios expuestos: Identificación de servicios sensibles y aplicaciones expuestas para la prevención o remediación de ataques.

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

CSIRT (Equipo de respuestas ante incidentes de seguridad de la Información) Es un grupo de profesionales que buscan restituir las actividades con el impacto mínimo aceptable para la entidad, así mismo brindan apoyo al funcionario u área afectada en la respuesta rápida para contener un incidente de seguridad de la información de igual manera recibe los informes sobre incidentes de seguridad, analiza las situaciones y responde a las amenazas.

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.

Contener: Son aquellas actividades que se llevan a cabo para solucionar o mitigar algún tipo de incidente de seguridad, estas acciones evitan la materialización o propagación de eventos de seguridad anómalos en un sistema de información o una arquitectura de TI

4. NORMAS LEGALES

Ley 1273 de (5 enero 2009): Por medio de la cual se modifica el Código Penal. Título VII Bis "De la protección de la información y de los datos". Artículos 269A a 269J.
Ley 1581 de (17 octubre 2012): Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1712 de 2014 (06 marzo 2014): Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones
Decreto 1377 de (27 junio 2013): Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Decreto 886 de (13 de mayo 2014): Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
Decreto 2573 de 2014 (12 dic 2014): Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 1078 de (26 mayo 2015): Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Capítulo 1, Título 9, Libro 2, Parte 2 subrogado por el Decreto 1008 de 2018.
Decreto 1081 de (26 mayo 2015): Por medio del cual se expide el Decreto Único Reglamentario del Sector Presidencia de la República. Parte 1, Titulo 1.
Decreto 1008 de (14 junio 2018): Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones. Política de Gobierno Digital
CONPES 3701 de (14 julio 2018): Lineamientos de Política para Ciberseguridad y Ciberdefensa.
CONPES 3854 de (11 abril 2016): Política Nacional de Seguridad Digital.

5. NORMAS TÉCNICAS

NTC-ISO /IEC 20000-1:2011: Norma Técnica Colombiana NTC-ISO/IEC 27001 colombiana. Tecnología de la Información. Gestión de Servicio. Parte 1: Requisitos del Sistema de Gestión del Servicio
NTC-ISO /IEC 27001:2013: Norma Técnica Colombiana NTC-ISO-IEC 27001.Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información
Modelo de Seguridad de la Información: Documento adoptado por PARQUES NACIONALES NATURALES DE COLOMBIA.

6. LINEAMIENTOS GENERALES Y/O POLITICAS DE OPERACIÓN

Es responsabilidad del Comité Institucional Gestión y Desempeño de Parques Nacionales Naturales de Colombia, garantizar la aplicación del procedimiento incidentes de seguridad de la información, actualizarlo y evaluar las acciones de mejora que se identifiquen en el tratamiento de los incidentes de seguridad que sean detectados.

Los posibles incidentes de seguridad y/o eventos se reportarán a la Mesa de Servicio GLPI a través de los siguientes canales:

- A través del módulo de auto servicio de la herramienta GLPI https://glpi.parquesnacionales.gov.co/front/central.php en donde se puede reportar el caso.
- Enviando un mensaje de correo electrónico con la solicitud a la dirección redes.seguridad@parquesnacionales. gov.co
- Llamando a la Mesa de Servicio a las extensiones 3115, 3118

Una vez recepcionado el requerimiento el colaborador que identifique el posible incidente y/o evento de seguridad debe reunir la información que llevó a determinar que es un posible incidente, las cuales pueden estar respaldadas con las siguientes evidencias:(capturas de pantalla, correos electrónicos, fotografías, videos entre otros).
Posteriormente, el analista de la mesa de servicio GLPI debe realizar la primera categorización en la herramienta GLPI, para iniciar con la atención del mismo, si cumple con algunos de los siguientes criterios puede ser considerado como un incidente de seguridad, de lo contrario se tratará como un evento o como un incidente de tecnología así:

- Hubo daño o pérdida de información física o digital.
- Hubo fuga y/o robo de información física o digital.
- Hubo robo de credencias o información mediante Phishing.
- Se presentó modificación no autorizada de la información.
- Se presentó suplantación de identidad.
- Se presentó un acceso no autorizado.
- Se presentó pérdida o alteración de registros de base de datos.
- Se presentó una pérdida de un activo de información.
- Hubo presencia de código malicioso “malware, Ransomware”.
- Se presentó una denegación del servicio.
- Se presentó algún ciberataque.
- Uso indebido de imagen institucional.
- Se presentó la suspensión de algún servicio de tecnología.

Una vez clasificado el incidente de seguridad este deberá ser categorizado en su impacto de acuerdo con la “Tabla 1 Impacto vs Valoración”, y en su urgencia de acuerdo con la “Tabla 2 urgencia” en la herramienta de gestión GLPI.

Tabla 1. Impacto vs Valoración

IMPACTO	DESCRIPCIÓN	VALORACION DEL IMPACTO
Catastrófico	Si el incidente que se está reportando puede generar consecuencias graves o efectos sobre la entidad a nivel de: • Pérdidas Económicas superiores a 2000 SMLV. • Afectación de la imagen a Nivel Nacional e Internacional. • Sanciones de Contraloría, Procuraduría y Fiscalía.	ALTO

	• Daños totales de la infraestructura de la Entidad. • Afecta a sistemas críticos. • Afecta directamente el cumplimiento de los objetivos misionales de la Entidad. • El incidente afecta activos de información considerados de impacto muy alto y alto	
Mayor	Si el incidente que se está reportando puede generar consecuencias o efectos sobre la entidad: • Pérdidas Económicas entre 1501 a 2000 SMLV. • Afectación de la imagen a Nivel Nacional. • Sanciones de Contraloría, Procuraduría y Fiscalía. • Daños parciales de la infraestructura de la Entidad. • Afecta Sistemas con funciones críticas. • El incidente afecta activos de información considerados de impacto muy alto y alto	
Moderado	Si el incidente que se está reportando puede generar consecuencias moderadas o efectos sobre la entidad: • Pérdidas Económicas entre 1001 a 1500 SMLV. • Afectación de la imagen del proceso o área a Nivel de Entidad. • Sanciones a nivel de Oficina Jurídica o Control Interno. • Daños parciales de la infraestructura de la Entidad. • Afecta sistemas que apoyan más de una dependencia o proceso en la Entidad. • Llamados de atención a nivel Organizacional. • El incidente afecta activos de información considerados de impacto medio	MEDIO
Menor	Si el incidente que se está reportando puede generar consecuencias menores o efectos sobre la entidad: • Pérdidas Económicas entre 501 a 1000 SMLV. • Afectación Imagen grupo o área a nivel del proceso. • Sanciones a nivel procesos. • Daños pequeños de la infraestructura de la Entidad. • Afecta sistemas que apoyan a una sola dependencia o proceso en de la Entidad • Llamados de atención a nivel proceso. • El incidente afecta activos de información considerados de impacto bajo.	BAJO

	Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto	
Insignificante	Si el incidente que se está reportando puede generar consecuencias menores o efectos sobre la entidad. • Pérdidas Económicas menores a 500 SMLV. • Afectación Imagen grupo a nivel área o proceso. • Sanciones a nivel grupo. • Daños pequeños de la infraestructura de la Entidad. • Afecta sistemas no críticos, como estaciones de trabajo de usuarios con funciones no críticas. • Llamados de atención a nivel grupo. • El incidente afecta activos de información considerados de impacto bajo. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto	

En la anterior tabla, se muestra el impacto vs valoración del incidente, identificando así las consecuencias que puede ocasionar en la entidad la materialización de un incidente de seguridad.

Para el caso de atención de incidentes de seguridad se han establecido unos tiempos máximos de atención de estos, con el fin de dar trámite adecuadamente a lo requerido de acuerdo con su impacto y valoración del mismo. Los tiempos expresados en la en la "Tabla No. 2 Urgencia", son un acercamiento al tiempo máximo en que el incidente debe ser atendido, y no al tiempo en el cual el incidente debe ser solucionado. Esto se debe a que la solución de los incidentes puede variar dependiendo del caso.

Tabla 2 Urgencia

Valoración del Impacto	Tiempo Máximo de Atención
Alto	El incidente de seguridad debe atenderse en un periodo máximo de 2 horas
Medio	El incidente de seguridad debe atenderse en un periodo máximo de 4 horas
Bajo	El incidente de seguridad puede atenderse en un periodo mayor a 4 horas

Los equipos de respuesta que atiendan el incidente de seguridad, estarán conformados como mínimo por el propietario y/o custodio del activo de información afectado por el incidente, y los colaboradores de la oficina TIC, el Oficial de Seguridad de la Información, Líder oficina TIC o el proveedor de servicios tecnológicos que tengan a cargo activos o servicios que se vean afectados por el mismo.
Dependiendo del análisis realizado producto del resultado del incidente se conformarán los equipos que podrán solicitar información o la participación de otros colaboradores de otros procesos requeridos para la atención del incidente de seguridad.

En caso que un incidente de seguridad tenga una valoración **ALTO**, el Oficial de Seguridad de la Información deberá informar al Líder del Sistema de Gestión de Seguridad de la Información (Jefe Oficina TIC), la ocurrencia de dicho Procedimiento Incidentes en Seguridad de la Información GTSI_PR_02 Versión 1 vigente desde 08/11/2021 evento, quien deberá informar a la Alta Dirección, para determinar si se instala una mesa de crisis, en donde se analizará los recursos financieros, humanos y tecnológicos correspondientes a la atención del incidente, al igual evaluar las alternativas para la contención, erradicación y solución del mismo.
Los incidentes de seguridad con valoración **ALTO,** deben ser documentados en la herramienta de gestión de seguridad de la información (segurinfo.pnnc.local) y adicionalmente el Oficial de Seguridad de la información debe generar un reporte independiente en el formato establecido por el CSIRT de Gobierno, donde se evidencie las actividades realizadas de contención y solución.

En caso de que se requiera dar a conocer el incidente a entes externos, este debe ser comunicado a las siguientes instancias:

- ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia), reportar al correo electrónico: contacto@colcert.gov.co o al Teléfono: (+571) 2959897.
- CSIRT Gobierno reportar al correo csirtgob@mintic.gov.co
- Centro cibernético Policial reportar en la siguiente ruta: https://caivirtual.policia.gov.co/

7. FORMATOS, REGISTROS O REPORTES

- Lista de chequeo de herramientas para atención de incidentes de seguridad
- Formato de documentación de incidentes
- Registro de lecciones aprendidas, respuesta a incidentes de seguridad de la información

8. PROCEDIMIENTO PASO A PASO

No.	ACTIVIDAD	RESPONSABLE	DOCUMENTOS DE REFERENCIA	PUNTOS DE CONTROL
1	Registrar el posible incidente de seguridad.	Todos los niveles de gestión (funcionarios, contratistas y proveedores)	Instructivo vigentes solicitudes de servicio de Tecnologías de la Información – TI Código GTSI_IN_04	Correo electrónico Herramienta mesa de ayuda GLPI
2	Categorizar el posible incidente de seguridad. ¿Es un incidente de seguridad? **NO:** Continua con la actividad 3. **SÍ**: Continua con la actividad 4.	Analistas de mesa de Servicio-GTIC	Procedimiento operación del servicio tecnologías de seguridad de la información y comunicaciones - GAINF_PR_15	Herramienta mesa de ayuda GLPI
3	Continuar con el soporte técnico	Analistas de mesa de Servicio-GTIC	Procedimiento operación del servicio tecnologías de seguridad de la información y comunicaciones - GAINF_PR_15	Herramienta mesa de ayuda GLPI
4	Realizar el escalamiento del incidente de seguridad al Profesional de la Oficina TIC para su análisis y clasificación.	Analistas de mesa de Servicio-GTIC	Procedimiento operación del servicio tecnologías de seguridad de la información y comunicaciones - GAINF_PR_15	Herramienta mesa de ayuda GLPI
5	Gestionar el incidente de seguridad, en caso de que el incidente tenga una valoración en su impacto como ALTO se debe aplicar las políticas de operación.	Oficial de Seguridad de la Información-GTIC	Herramienta de gestión de servicios	Herramienta mesa de ayuda GLPI
6	Seleccionar y conformar el equipo de atención del incidente política de operación.	Oficial de Seguridad de la Información-GTIC	N/A	Correo electrónico, tener en cuenta que en el caso de que la

No.	ACTIVIDAD	RESPONSABLE	DOCUMENTOS DE REFERENCIA	PUNTOS DE CONTROL
				notificación se realice de manera verbal la comunicación debe formalizarse a través de correo electrónico o de manera escrita.
7	Analizar el incidente de seguridad con el fin de identificar la causa raíz que dieron origen al incidente de seguridad	Oficial de Seguridad de la Información-GTIC Equipo de atención del incidente Persona que reporta el incidente.	N/A	Formato de documentación del incidente Lista de chequeo de herramientas para atención de incidentes de seguridad.
8	. ¿Se requiere definir plan de mejoramiento? **No**: Continua con la actividad 9 **Si**: Documentar plan de mejoramiento de acuerdo a el Procedimiento de acciones correctivas y de mejora EI_PR_01.	Oficial de Seguridad de la Información-GTIC Equipo de atención del incidente Persona que reporta el incidente.	N/A	Formato de documentación del incidente Lista de chequeo de herramientas para atención de incidentes de seguridad.
9	Atender el incidente de seguridad mediante las tareas que permitan contener y minimizar su impacto	Oficial de Seguridad de la Información-GTIC Equipo de atención del incidente		Formato de documentación
10	. ¿Se logró contener el incidente de seguridad? **Si**: Continua con la actividad 11.	Oficial de Seguridad de la Información-GTIC Equipo de atención del incidente	N/A	Formato de documentación

No.	ACTIVIDAD	RESPONSABLE	DOCUMENTOS DE REFERENCIA	PUNTOS DE CONTROL
	No: Evaluar las acciones tomadas para contener el incidente Volver a la actividad 8			
11	Solucionar el incidente de seguridad mediante todas aquellas tareas necesarias que permitan erradicar la causa raíz detectada.	Oficial de Seguridad de la Información-GTIC Equipo de atención del incidente	N/A	Formato de documentación
12	¿Se logró erradicar la causa? **Si**: Continua con la actividad 13 **No**: Devolver a la actividad 8.	Oficial de Seguridad de la Información-GTIC Equipo de atención del incidente	N/A	Formato de documentación
13	Documentar, recopilar, organizar y guardar las evidencias producto de la investigación del incidente de seguridad.	Oficial de Seguridad de la Información-GTIC Equipo de atención del incidente	N/A	Formato de documentación y cargar la evidencias en la herramienta de GLPI.
14	Implementar las lecciones aprendidas del incidente de seguridad que serán incluidas en la base de datos de conocimiento.	Oficial de Seguridad de la Información-GTIC Equipo de atención del incidente	N/A	Formato de lecciones aprendidas.
15	Informar o notificar a los afectados sobre incidentes que afecten la confidencialidad o integridad de su información, así como de las medidas adoptadas para la remediación del incidente.	Oficial de Seguridad de la Información-GTIC	N/A	Acta de reunión cierre de incidente

9. ANEXOS

Anexo 1. Flujograma procedimiento incidentes en seguridad de la información

10. CONTROL DE CAMBIOS

FECHA DE VIGENCIA VERSIÓN ANTERIOR	VERSIÓN ANTERIOR	MOTIVO DE LA MODIFICACIÓN
08/11/2021	1	Se realiza actualización en el capítulo de lineamientos generales y políticas de operación de teniendo en cuenta las observaciones recibidas por el Grupo de Control Interno y responsables del proceso de acuerdo a la resolución 310 de la creación del Grupo de Sistemas de la Información y las Comunicaciones.
23/09/2022	2	Se relaciona flujograma en la hoja de anexos de acuerdo a las observaciones recibidas en la Auditoria final de verificación de documentos del SGI realizada por el GCI.

CRÉDITOS		
Elaboró	Nombre	Fernando Bolívar Sandra Milena Gómez
	Cargo	Profesional Contratistas Grupo de Tecnologías de la Información y las Comunicaciones.
	Fecha	25/10/2022
Revisó	Nombre	Carlos Arturo Sáenz Barón
	Cargo	Coordinador de Tecnologías de la Información y las Comunicaciones
	Fecha:	25/10/2022
Aprobó	Nombre	Carlos Arturo Sáenz Barón
	Cargo	Coordinador de Tecnologías de la Información y de las Comunicaciones
	Fecha:	10/11/2022

PARQUES NACIONALES NATURALES DE COLOMBIA	**ANEXOS 1** **FLUJOGRAMA PROCEDIMIENTO INCIDENTES EN SEGURIDAD DE LA INFORMACIÓN**	Código: GTSI_PR_02 Versión: 03 Vigente desde: 21/11/2022