PARQUES NACIONALES NATURALES DE COLOMBIA

DIRECCIÓN GENERAL
GRUPO DE CONTROL INTERNO

INFORME FINAL DE AUDITORIA INTERNA
PROCESO DE GESTIÓN DE TECNOLOGÍAS Y SEGURIDAD DE LA INFORMACIÓN
GRUPO DE TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES GTIC

Bogotá, 10 de agosto de 2023

1. INFORMACIÓN GENERAL

PROCESO O ACTIVIDAD:	Proceso de Gestión de Tecnologías y Seguridad de la Información
AUDITOR LÍDER:	Gladys Espitia Peña
EQUIPO AUDITOR:	Raimon Sales Contreras - Carlos Fredy Rey Camacho
AUDITADO:	Proceso Gestión de Gestión de Tecnologías y Seguridad de la Información.
OBJETIVO:	Evaluar la implementación del Sistema de Control Interno, en las diferentes etapas mediante la verificación sistemática, objetiva e independiente de las actividades asociadas al Proceso de Gestión de Tecnologías y Seguridad de la Información, enfocados en la gestión, avance, cumplimiento y la aplicación de los diferentes Planes Institucionales, el Modelo de Seguridad y Privacidad de la Información en el marco de lo establecido en la Normatividad vigente.
ALCANCE:	La Auditoría se realizó en el Grupo de Tecnologías de la Información y las Comunicaciones - Nivel Central -Direcciones Territoriales, se enfocará a las actividades realizadas para las vigencias 2022 y hasta mayo de 2023, del Proceso de Gestión de Tecnologías y Seguridad de la Información.
CRITERIOS-MARCO LEGAL:	Caracterización del proceso. Procedimientos, Guías, Instructivos, Normatividad Vigente, MIPG, Riesgos y Sistema de Control Interno.
TIPO DE AUDITORIA:	Interna de Gestión

REUNIÓN DE APERTURA						**EJECUCIÓN DE LA AUDITORÍA**				**REUNIÓN DE CIERRE**					
Día	22	**Mes**	06	**Año**	2023	**Desde**	22/06/2023 DD / MM /AA	**Hasta**	24/07/2023 DD / MM /AA	**Día**	21	**Mes**	07	**Año**	2023

2. DETERMINACIÓN DE LA MUESTRA DE AUDITORÍA

El Grupo de Control Interno seleccionó los documentos de mayor impacto para la revisión en la auditoria, en torno a la seguridad y privacidad de la información, los planes de acción, la ejecución de proyectos, la implementación de buenas prácticas y el cumplimiento de la normatividad vigente, bajo la gestión, responsabilidad y acatamiento del Proceso de Gestión de Tecnologías y Seguridad de la Información. En consecuencia, los documentos utilizados como soporte para la ejecución de la auditoría fueron:

GTSI_CA_01. V7. Caracterización Proceso de Tecnología y Gestión de Seguridad de la Información.
GTSI_IN_01 V5 Mantenimiento correctivo y preventivo.
GTSI_PR_01 V5 Procedimiento Radiocomunicaciones y Telecomunicaciones.
GTSI_PR_06 V4 Operación del Servicio Tecnologías de la información y las comunicaciones – TIC.
GTSI_PR_03 V2 Gestión de Cambios TI.
Modelo Integrado de Planeación y Gestión - Política de Seguridad Digital.
Documentos Modelo Integrado de Planeación y Gestión - SGI - PNNC.
Plan Anual de Adquisiciones 2022.
Reporte Mensual Plan de Mejoramiento por Procesos – Gestión abril 2023.
NTC ISO 9001 2015.
ISO/IEC 27001 de 2013.
Modelo de Seguridad y Privacidad de la Información - MSPI - MINTIC.

Ley 1712 de 2014 - Transparencia y Acceso a la Información.
Ley 1581 de 2012 - ley de protección de datos personales.
Ley 23 de 1982.
Decreto 612 DE 2018.
Decreto 103 de 2015.
Decreto 1078 de 2015.
Decreto 1082 de 2015 sector administrativo de Planeación Nacional.
Resolución 500 de 2021.
Directiva presidencial No 001 de 1999.
Política de Control Interno - MIPG.
Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. v5.
Modelo Integrado de Planeación y Gestión - Política de Seguridad Digital.

3. METODOLOGÍA

Descripción de las herramientas y técnicas de auditorías empleadas, bajo orden cronológico del ejercicio auditor. De acuerdo con el Plan Anual de Auditoria, el Grupo de Control Interno llevó a cabo la ejecución de la actividad conforme a lo registrado en los formatos del Plan de Auditorias y la Lista de Verificación, dando así cumplimiento a las fechas acordadas y cubriendo en su totalidad los temas que fueron registrados en el formato EI_FO_03 – Lista de verificación, a través de las siguientes metodologías:

- Entrevistas.
- Prueba de técnicas.
- Aplicación de la matriz de auditoría.
- Recopilación y análisis de evidencias.

El Grupo de Control Interno dio inicio al proceso de auditoría a partir del 23 de junio de 2023 con la presentación de apertura al responsable del Proceso de Gestión de Tecnologías y Seguridad de la Información. En la jornada de apertura se dio a conocer el objetivo, alcance y los criterios que serían tenidos en cuenta durante el proceso de auditoría.

Durante la ejecución de la auditoría, a través de entrevistas se realizó el levantamiento de información, se solicitaron evidencias y se realizaron pruebas técnicas. De manera paralela, el equipo auditor creó carpetas en la nube que fueron compartidas con Proceso de Gestión de Tecnologías y Seguridad de la Información, para que subieran allí las evidencias relacionadas con los temas tratados en cada jornada. Las evidencias aportadas eran validadas por el equipo auditor y se mantenía una comunicación constante con Proceso de Gestión de Tecnologías y Seguridad de la Información para que se corrigieran o se aportaran las evidencias que no daban cumplimiento a lo inicialmente solicitado. El equipo auditor organizó y compartió las carpetas en la nube, para que se dispusieran allí las evidencias que se solicitaban y que posteriormente se analizaban:

https://drive.google.com/drive/folders/1_CJ9FZcBCgIskDXcRRSCifmftKi3V9Y5?usp=drive_link

La reunión de cierre se llevó a cabo en el 21 de julio de 2023, donde se dio a conocer al grupo las fortalezas, recomendaciones y No conformidades evidenciadas en el proceso de auditoría.

4. ASPECTOS EVIDENCIADOS DURANTE EL EJERCICIO DE LA AUDITORÍA

Durante el proceso de la auditoría Proceso de Gestión de Tecnologías y Seguridad de la Información mostró interés en el desarrollo, respondiendo oportunamente a las preguntas con el apoyo del personal idóneo, aportando las evidencias solicitadas y aceptando las debilidades que eran evidentes.

Apoyados en la lista de verificación, el equipo auditor desarrolló las jornadas de auditoría en torno a los criterios planteados, lo que al final del ejercicio dio como resultado el análisis y conclusión de los temas relevantes relacionados con la seguridad y privacidad de la información y la gestión estratégica del proceso:

Caracterización del proceso

La correcta caracterización de un proceso permite identificar y fortalecer las acciones que apoyan los objetivos estratégicos de la Entidad, lo que a su vez fortalece la gobernabilidad del proceso y lo potencia en si nivel jerárquico. Así mismo la identificación y caracterización de usuarios y grupos de interés; en particular para el proceso de TI, promueve la innovación, fortalecimiento, acceso y usabilidad de tecnologías implementadas que requiere la Entidad para impulsar el avance de sus procesos y facilitar el alcance de la misión y los objetivos, evolucionando de esa manera hacia la transformación digital.

El proceso no cuenta con una caracterización documentada que permita evidenciar la gestión del proceso enfocado en atender las necesidades de sus usuarios tanto internos como externos, por lo que es necesario ejecutar acciones que permitan contar con un documento de caracterización que esté alineado con las estrategias y objetivos institucionales.

Planes estratégicos

El Grupo TIC identifica cuatro (4) planes que conforman su Plan de Acción, (Plan estratégico tecnologías de la información y las comunicaciones - PETIC, Plan de tratamiento de riesgos de seguridad y privacidad de la información, Plan de seguridad y privacidad de la información y Plan de mantenimiento y servicios tecnológicos), sin embargo, estos planes deben ser fortalecidos en concordancia con el Plan Estratégico.

El documento PETIC debe concebirse como el resultado de un adecuado ejercicio de planeación estratégica de TI y debe hacer parte integral de la estrategia Institucional en el marco de la Arquitectura Empresarial.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, debe estar constituido mediante acciones que permitan reducir la afectación a la entidad en caso de una materialización. Esta tarea debe ser participativa, con mesas de trabajo conjunto en donde se planteen estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de riesgos. Al final del ejercicio, el plan de tratamiento debe cubrir los riesgos de información de todos las grupos y direcciones territoriales que conforman la Entidad.

El Plan de Seguridad y Privacidad de la Información, debe evidenciar un inventario de actividades que conlleve a la ejecución de acciones para actualizar y publicar los activos de información, actualizar los riesgos asociados, gestionar los incidentes de seguridad y gestionar obligaciones con relación a datos personales, entre otros.

Seguridad y privacidad de la información

El manual de políticas de seguridad y privacidad de la información ofrece a los usuarios un documento detallado de cuidados y buenas prácticas, frente al uso de Tecnologías de Información y particularmente con los activos de información.

El Plan de seguridad y Privacidad de la Información cobra sentido con la existencia de un inventario de activos de información que los identifique plenamente al interior de toda la Entidad. Esta tarea debe estar incluida dentro del Plan estratégico; particularmente en el Plan de Seguridad y Privacidad de la Información, y debe ser apoyado y construido de manera activa por todos los Grupos y Direcciones Territoriales. El propósito principal de esta acción es la de mantener un inventario de la información, identificar los diferentes responsables de la información y clasificar la información de acuerdo a su nivel de confidencialidad, integridad y disponibilidad. Al realizar un levantamiento de activos de información liderado por el Grupo de TIC, se tendrá pleno conocimiento de quienes son los usuarios, derechos de acceso y responsabilidades asignadas sobre cada activo de información, de esa manera se mitigará el riesgo de corrupción identificado. En el mismo ejercicio de clasificación de seguridad y privacidad de la información, se deben fijar los lineamientos para su valoración, a fin de involucrar a aquellos terceros que soportan sistemas de información o aplicaciones tecnológicas para que responda en todo o en parte por el riesgo que pueda conllevar la inadecuada ejecución de una actividad.

Marco legal

El Decreto 415 de 2016, establece los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones a través del posicionamiento de los líderes de áreas TI. El numeral 7 del artículo 2.2.35.3 establece que para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones las entidades deben: liderar los procesos de adquisición de bienes y servicios de tecnología, mediante la definición de criterios de optimización y métodos que direccionen la toma de decisiones de inversión en tecnologías de la información, buscando el beneficio económico y de los servicios de la entidad.

El Plan Estratégico de TI está reglamentado en el Decreto 612 de 2018, por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado, en el cual, en el artículo 1, se requiere la Integración de los planes institucionales y estratégicos al Plan de Acción. Para ello, las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar - todos los planes institucionales y estratégicos entre los que se encuentran el Plan Estratégico de Tecnologías de la Información y las Comunicaciones – PETI. Adicional a lo anterior, existen otros instrumentos dentro del marco legal y buenas prácticas que ayudan a fortalecer las oficinas de TI y facilitan su gobernanza:

- Ley 1712 - Artículo 13. Registros de Activos de Información. Todo sujeto obligado deberá crear y mantener actualizado el Registro de Activos de Información haciendo un listado de:
  Todas las categorías de información publicada por el sujeto obligado;
  Todo registro publicado;
  Todo registro disponible para ser solicitado por el público.

- El Ministerio Público podrá establecer estándares en relación a los Registros Activos de Información. Todo sujeto obligado deberá asegurarse de que sus Registros de Activos de Información cumplan con los estándares establecidos por el Ministerio Público y con aquellos dictados por el Archivo General de la Nación, en relación a la constitución de las Tablas de Retención Documental (TRD) y los inventarios documentales.

- Ley 1581 - ARTÍCULO 1. Objeto. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

- Ley 23 de 1982- ARTÍCULO 1.- Los autores de obras literarias, científicas y artísticas gozarán de protección para sus obras en la forma prescrita por la presente Ley y, en cuanto fuere compatible con ella, por el derecho común. También protege esta Ley a los intérpretes o ejecutantes, a los productores de programas y a los organismos de radiodifusión, en sus derechos conexos a los del autor.

- Directiva Presidencial No 001 de 1999 - Numeral 5. Los organismos y entidades no deberán utilizar o adquirir obras literarias, artísticas, científicas, programas de computador, fonogramas y señales de televisión captadas violatorias o que se presuma violen el derecho de autor o los derechos conexos. Numeral 8. Todas las entidades deberán establecer procedimientos para asegurar, determinar y mantener dentro de sus respectivas entidades bienes que cumplan con los derechos de autor.

- Decreto 612 - "2.2.22.3.14. Integración de los planes institucionales y estratégicos al Plan de Acción. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año.

- Decreto 103 - Capítulo 1. Artículo 38 parágrafo 2. El sujeto obligado, debe actualizar el Registro de Activos de Información de acuerdo con los procedimientos y lineamientos definidos en su Programa de Gestión Documental - PGD.

- Decreto 1082 - ARTÍCULO 2.2.1.1.1.4.1. Plan Anual de Adquisiciones. Las Entidades Estatales deben elaborar un Plan Anual de Adquisiciones, el cual debe contener la lista de bienes, obras y servicios que pretenden adquirir durante el año.

- Resolución 500 de 2021: Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

- MIPG - 3.2.1.3 Política de Seguridad Digital. Con la política se fortalecen las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socio-económicas en el entorno digital, así como en la creación e implementación de instrumentos de resiliencia, recuperación y respuesta nacional en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad eco-nómica y social en el país.

- ISO/IEC 27001:2013 Numeral 5. La alta dirección debe establecer una política de seguridad de la información.

- ISO/IEC 27001 A.12.3.1 establece la creación y prueba regular de copias de seguridad que involucren a la información, software e imágenes de sistemas, todo en concordancia con una política de respaldo.

4.1 ASPECTOS POSITIVOS: FORTALEZAS

- Se resalta la disposición de los responsables en el equipo de trabajo del Grupo de Tecnologías de la Información y las Comunicaciones en el marco del Proceso de Gestión de Tecnologías y Seguridad de la Información.

- Oportuna entrega de la información solicitada en las pruebas de recorrido realizadas con cada responsable en el equipo de trabajo.

- Puntualidad en el desarrollo y ejecución del plan de auditorías por cada responsable agendado en las pruebas de recorrido.

- El Grupo de Tecnologías de la Información y las Comunicaciones, ocupa un espacio en el organigrama institucional acorde con lo establecido en el decreto 415 de 2016, lo que le facilita al líder de TI, llevar a cabo el cumplimiento de los lineamientos para el fortalecimiento institucional y la ejecución de los planes, programas y proyectos de tecnologías y sistemas de información.

4.2 LIMITACIONES

No se presentaron limitaciones en el alcance y desarrollo de la auditoría interna que impidieran dar cumplimiento al plan de auditoria establecido por el Grupo de Control Interno.

4.3 DESCRIPCIÓN DE LAS OBSERVACIONES / NO CONFORMIDADES

CRITERIO – MARCO LEGAL	DESCRIPCION DE LA SITUACION:
Procedimiento Radiocomunicaciones y Telecomunicaciones: GTSI_PR_01, V5, Vigente desde el 19-11-2022.	El Grupo de Tecnologías de la Información y Comunicaciones no demostró el cumplimiento de las actividades establecidas en el procedimiento, lo que se evidencia no solo en la falta de seguimientos, sino además en la falta de actualización de la documentación. No se evidenció el cumplimiento del Objetivo del procedimiento relacionado con: "…Establecer los lineamientos para implementar y optimizar la utilización de la red de radiocomunicaciones y telecomunicaciones con el propósito de tener una comunicación constante y efectiva en todos los niveles de gestión, garantizando una atención oportuna y eficaz de cualquier eventualidad o requerimiento presentado…". Se observó que en la actividad No 4 relacionada con: "…Verificar las solicitudes de la información suministrada frente a la información disponible en formatos anteriores y semanales del formato "GTSI_FO_09 Reporte-radial-semanal.xlsx" (diligenciados por las AP) con el inventario de equipos del formato "GAINF_FO_21-Inventario-radial.xlsx" diligenciado mensualmente por las DT

	¿La información presenta inconsistencias? SI: Solicitar aclaraciones a la DT y/o AP mediante el canal remitido inicialmente. NO: Continuar con el paso 5...". No se aportaron evidencias que permitieran establecer el cumplimiento y aplicación de la actividad que concentra toda la documentación que hace parte del procedimiento en toda su extensión.

OBSERVACION / NO CONFORMIDAD:

NO CONFORMIDAD No.1:
En el proceso de verificación realizado por el Equipo Auditor del Grupo de Control Interno en el marco del procedimiento Radiocomunicaciones y Telecomunicaciones, no se evidenció la aplicación e implementación que demuestre su desarrollo y ejecución en las actividades establecidas y sus responsables en el Nivel Central, Territorial y Local para las vigencias 2022 – 2023.

CRITERIO – MARCO LEGAL	DESCRIPCION DE LA SITUACION:
Procedimiento Gestión de Cambios GTSI_PR_03, V2, Vigente desde el 19-11-2022.	El Grupo de Tecnologías de la Información y Comunicaciones no demostró el cumplimiento de las actividades establecidas en el procedimiento, lo que se evidencia no solo en la falta de seguimientos, Procedimiento Gestión de Cambios GTSI_PR_03, V2, Vigente desde el 19-11-2022. Se verificó el objetivo del procedimiento relacionado con: "… Establecer las actividades y controles para implementar la gestión de cambios TI que se realicen sobre la infraestructura de Parques Nacionales Naturales de Colombia, de manera que se reduzca la probabilidad de materialización de algún riesgo que atente contra la estabilidad, disponibilidad y continuidad de los servicios que se prestan de la entidad…". No se evidenció cumplimiento de la actividad No 1: "…Identificar y/o recibir la necesidad del cambio…", con la cual inicia el desarrollo y ejecución del procedimiento y con él, la aplicación y documentación creada en el Sistema de Gestión de Calidad.

OBSERVACION / NO CONFORMIDAD:

NO CONFORMIDAD No.2:
En la evaluación realizada por el Equipo Auditor del Grupo de Control Interno en el marco del procedimiento Gestión de Cambios TI, no se observó la aplicación e implementación que demuestre el desarrollo y ejecución de todas las actividades definidas con cada responsable en el Nivel Central para las vigencias 2022 – 2023. sino además en la falta de actualización de la documentación.

CRITERIO – MARCO LEGAL	DESCRIPCION DE LA SITUACION:

Procedimiento Incidentes en Seguridad de la Información GTSI_PR_02, V3, Vigente desde el 21-11-2022.	Se realizó la verificación del objetivo relacionado con: "…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…". En lo correspondiente a las evidencias evaluadas en el desarrollo de la ejecución de la auditoria, no se encontró alguna que demuestre el cumplimiento de las actividades (5, 6, 7, 8, 9, 10, 11, 12, 13, 14 y 15), que involucran como responsable al oficial de seguridad. Es necesario precisar que no se encontraron evidencias de los puntos de control establecidos como formatos y actas.
OBSERVACION / NO CONFORMIDAD: **NO CONFORMIDAD No.3:** En la evaluación realizada por el Equipo Auditor del Grupo de Control Interno en el marco del procedimiento Incidentes en Seguridad de la Información, no se observó la aplicación e implementación que demuestre el desarrollo y ejecución de todas las actividades definidas en el procedimiento, que involucra como responsable un Oficial de Seguridad de la Información-GTIC, además que esta figura (Oficial de Seguridad de la Información), no existe en el personal de planta o como contratista para que desempeñe tales actividades dentro de la Entidad.	

CRITERIO – MARCO LEGAL	**DESCRIPCION DE LA SITUACION:**
Procedimiento Estrategia y Proyectos – Tecnologías de la Información - TI GTSI_PR_04, V1, Vigente desde el 01-08-2022.	Se realizó la verificación del objetivo relacionado con: *"…Gestionar los requerimientos, implementación del proyecto y los recursos tecnológicos bajo el esquema de Gobierno Digital y con la oferta de servicios T.I, alineándose con la estrategia misional de PNNC a través de la aplicación y actualización del Plan Estratégico de Tecnologías de la Información y las Comunicaciones…".* En la evaluación realizada por el Equipo Auditor del Grupo de Control Interno en el marco del Plan de Acción Anual vigencia 2002, se evidencia que el proceso hace el seguimiento a la implementación de proyectos nuevos en concordancia con los controles establecidos en el procedimiento, lo cual se refleja en la documentación de evidencias aportadas.
OBSERVACION / NO CONFORMIDAD: No se presentaron No Conformidades u Observaciones.	

CRITERIO – MARCO LEGAL	**DESCRIPCION DE LA SITUACION:**

Procedimiento Gestión de Usuarios GTSI_PR_05, V2, Vigente desde el 05-04-2023.	Se realizó la verificación del objetivo del procedimiento relacionado con: "…Definir los lineamientos necesarios para la gestión de usuarios de directorio activo y correo electrónico incluyendo la creación, inactivación, novedades, acceso a los sistemas de información (aplicaciones, correos, etc.) de los funcionarios y contratistas de Parques Nacionales Naturales de Colombia…". En las evidencias presentas por Proceso de Gestión de Tecnologías y Seguridad de la Información, no se observó el cumplimiento de la actividad No 14 relacionada con: *"…Diligenciar formato de devolución de bienes y servicios tecnológicos por desvinculación de la Entidad…"* y la actividad No 15, en lo que compete a : *"…Cargar el formato al GLPI, informando el usuario al que se redirecciona la información y continuar con el paso 11…";* para las solicitudes de inactivación de los usuarios Rolando Duque López y Luz Yadira Castro Obando en cuanto a la carga del formato Devolución Bienes Servicios Tecnológicos GTSI_FO_04 en el punto de control Mesa de Ayuda, generando un incumplimiento en él procedimiento.
OBSERVACION / NO CONFORMIDAD: **NO CONFORMIDAD No.4:** En el proceso de verificación realizado por el Equipo Auditor del Grupo de Control Interno en el marco del procedimiento Operación de Servicios de Tecnologías, no se observó la aplicación e implementación de los formatos Asignación de Bienes y Servicios Tecnológicos GTSI_FO_03 y Devolución Bienes y Servicios Tecnológicos GTSI_FO_04 para la desactivación de los usuarios Luz Yadira Castro Obando y Rolando Duque López por la novedad de retiro de la entidad en el Nivel Central para la vigencia 2022.	

CRITERIO – MARCO LEGAL	DESCRIPCION DE LA SITUACION:
Plan de Acción Anual – PAA 2022	En las evidencias presentadas por Proceso de Gestión de Tecnologías y Seguridad de la Información, se observó que los resultados de las metas alcanzadas, según el proceso alcanzan el 100%, sin embargo, en la revisión de los soportes se observó que el seguimiento de los proyectos incluidos en el PETIC, por ejemplo, no había un seguimiento riguroso en cuanto a la medición de avances significativos que alcanzaran esa cuantificación.
OBSERVACION / NO CONFORMIDAD: **NO CONFORMIDAD No.5:** En la evaluación realizada por el Equipo Auditor del Grupo de Control Interno en el marco del Plan de Acción Anual vigencia 2002, el indicador establecido para la actualización de los 4 planes incorporados el Modelo Integrado de Planeación y Gestión MIPG, el porcentaje alcanzado fue del 100% y se evidenció que no se actualizó el Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETIC publicado en el portal WEB de la entidad.	

CRITERIO – MARCO LEGAL	DESCRIPCION DE LA SITUACION:

GTSI_CA_01. V7. Caracterización Proceso de Tecnología y Gestión De Seguridad de la Información.	En la verificación realizada por el Grupo de Control Interno, se logró establecer, que no cuenta con la caracterización documentada y actualizada que permita evidenciar la gestión del proceso enfocado en atender las necesidades de sus usuarios internos como externos.
OBSERVACION / NO CONFORMIDAD: NO CONFORMIDAD No.6: En el proceso de verificación realizado por el Equipo Auditor del Grupo de Control Interno en el marco de la Caracterización del Proceso de Gestión de Tecnologías y Seguridad de la Información, no se observó la Identificación de los Usuarios Internos y Externos caracterizados en el Nivel Central, Direcciones Territoriales y Áreas Protegidas para las vigencias 2022 – 2023.	

CRITERIO – MARCO LEGAL	DESCRIPCION DE LA SITUACION:
GTSI_CA_01. V7. Caracterización Proceso de Tecnología y Gestión De Seguridad de la Información.	El grupo auditado no muestra evidencias de actividades que se hubieran ejecutado con el fin identificar grupos de interés o público objetivo. La ejecución de acciones que permitan identificar estos usuarios, son de vital importancia para emprender el camino hacia la implementación del Marco de Referencia de Arquitectura Empresarial - MRAE, lo que a su vez se convierte en el habilitador de Arquitectura de la Política de Gobierno Digital.
OBSERVACION / NO CONFORMIDAD: NO CONFORMIDAD No. 7: En la verificación realizada por el Equipo Auditor del Grupo de Control Interno en el marco de la aplicación y ejecución del Proceso de Gestión de Tecnologías y Seguridad de la Información, no existe una caracterización documentada que permita evidenciar la gestión del proceso enfocado en atender las necesidades de sus usuarios tanto internos como externos.	

CRITERIO – MARCO LEGAL	**DESCRIPCION DE LA SITUACION:**
Modelo de Seguridad y Privacidad de la Información – MSPI Resolución 500 de 2021	El proceso de Gestión de Tecnologías y Seguridad de la Información, no lleva un control de inventario tecnológico unificado, que recoja la información de toda la infraestructura tecnológica de la Entidad, con relación a sus características de hardware y tipo de licencias en uso.
OBSERVACION / NO CONFORMIDAD: **NO CONFORMIDAD No.8:** En la verificación realizada por el Equipo Auditor del Grupo de Control Interno, en el marco de la aplicación y ejecución del Proceso de Gestión de Tecnologías y Seguridad de la Información, no se evidencia la existencia de un instrumento que permita llevar un control del inventario tecnológico que cumpla con:"… Gestionar los recursos tecnológicos que	

permiten optimizar, agilizar y soportar la operación de los procesos de la entidad, para mejorar la trazabilidad, disponibilidad y escalabilidad de la plataforma tecnológica de Parques Nacionales Naturales de Colombia a través de los controles de infraestructura y seguridad definidos…".

CRITERIO – MARCO LEGAL	DESCRIPCION DE LA SITUACION:
Modelo de Seguridad y Privacidad de la Información – MSPI Resolución 500 de 2021	El Proceso no cuenta con un instrumento que permita llevar a cabo acciones para el tratamiento de riesgos de seguridad de la información o para llevar a cabo acciones de recuperación ante una eventual materialización de riesgo.

OBSERVACION / NO CONFORMIDAD:

NO CONFORMIDAD No.9:
En la verificación realizada por el Equipo Auditor del Grupo de Control Interno en el marco de la aplicación y ejecución del Proceso de Gestión de Tecnologías y Seguridad de la Información, no se evidencia la implementación de un plan de tratamiento de riesgos de seguridad y privacidad de la información, que contemple acciones para reducir la afectación a la entidad en caso de una materialización. Esta tarea debe ser participativa, con mesas de trabajo conjunto en donde se planteen estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de riesgos. Al final del ejercicio, el plan de tratamiento debe cubrir los riesgos de información de todos las grupos y direcciones territoriales que conforman la Entidad.

CRITERIO – MARCO LEGAL	DESCRIPCION DE LA SITUACION:
Plan Estratégico Tecnologías de la Información – PETI.	Realizada la verificación por parte del equipo auditor se evidencia que el Proceso no adelanta acciones que permitan mantener actualizado el documento PETI, mediante la medición de niveles de cumplimiento o la inclusión de nuevos proyectos.

OBSERVACION / NO CONFORMIDAD:

NO CONFORMIDAD No.10:
En la verificación realizada por el Equipo Auditor del Grupo de Control Interno en el marco de la aplicación y ejecución del Proceso de Gestión de Tecnologías y Seguridad de la Información, no se evidencia que el documento PETI fuera el resultado de un adecuado ejercicio de planeación estratégica de TI que hiciera parte integral de la estrategia Institucional en el marco de la Arquitectura Empresarial. Este documento debe ser actualizado constantemente en función del cumplimiento de los objetivos allí planteados y de los ejercicios que den como resultado la inclusión de un nuevo proyecto.

CRITERIO – MARCO LEGAL	DESCRIPCION DE LA SITUACION:

Decreto 415 de 2016.	Se evidencia que algunas Direcciones Territoriales y Procesos adelantan acciones para la adquisición de bienes y servicios tecnológicos, desconociendo la responsabilidad que tiene el Proceso de Gestión de Tecnologías y Seguridad de la Información. Teniendo en cuenta las evidencias aportadas en la respuesta al informe preliminar, **se descarta la No Conformidad**.
OBSERVACION / NO CONFORMIDAD: **NO CONFORMIDAD No.11:** Se descarta la No Conformidad**.** .	

CRITERIO – MARCO LEGAL	**DESCRIPCION DE LA SITUACION:**
GTSI_IN_08 – Instructivo de copias de seguridad para los sistemas de información de la entidad en el esquema Onpremise y nube. ISO/IEC 27001	El Proceso auditado contrata servicios que incluye una mesa de ayuda para resolver problemas técnicos de sistemas de información contratados, sin embargo, no se evidencia una política que traslade la responsabilidad de la seguridad de la información de los servicios soportados por terceros. Teniendo en cuenta las evidencias aportadas en la respuesta al informe preliminar, **se descarta la No Conformidad**.
OBSERVACION / NO CONFORMIDAD: **NO CONFORMIDAD No. 12:** Se descarta la No Conformidad**.** .	

CRITERIO – MARCO LEGAL	**DESCRIPCION DE LA SITUACION:**
GTSI_IN_08 – Instructivo de copias de seguridad para los sistemas de información de la entidad en el esquema onpremise y nube ISO/IEC 27001	No se evidencia la existencia de una política de seguridad que cubra la gestión de copias de respaldo al interior de la entidad.
OBSERVACION / NO CONFORMIDAD: **NO CONFORMIDAD No.13:** En la verificación realizada por el Equipo Auditor del Grupo de Control Interno, en el marco de la aplicación y ejecución del Proceso de Gestión de Tecnologías y Seguridad de la Información, se evidencia que no existe una política de copias de respaldo.	

CRITERIO – MARCO LEGAL	**DESCRIPCION DE LA SITUACION:**

GTSI_PR_06 V4 - Procedimiento operación del servicio tecnologías de la información y las comunicaciones – TIC	Se realizó la verificación del objetivo relacionado con: *"Definir y coordinar las actividades para gestionar las solicitudes de servicios tecnológicos, estableciendo los lineamientos para asegurar que los servicios de tecnologías de la información - TI se ofrezcan efectiva y eficientemente"*. En la evaluación realizada por el Equipo Auditor del Grupo de Control Interno en el marco del Plan de Acción Anual vigencia 2002, se evidencia que el proceso atiende los requerimientos relacionados con servicios tecnologías de información, a través del Sistema de información de mesa de mesa de ayuda GLPI, donde reposa la traza de los casos abiertos por los usuarios, tal como se describe en el procedimiento GTSI_PR_06 V4.
OBSERVACION / NO CONFORMIDAD: No se presentaron No Conformidades u Observaciones.	

CRITERIO – MARCO LEGAL	DESCRIPCION DE LA SITUACION:
Modelo Integrado de Planeación y Gestión - MIPG Política de seguridad digital	Durante las jornadas de auditoría no se evidenciaron prácticas concretas en el marco y la gestión de Tecnologías de Información – TI, desarrolladas por el Proceso que apoyaran una estrategia de uso y apropiación que aplique para toda la Entidad, cubriendo temas de impacto relacionados con la seguridad de la información.
OBSERVACION / NO CONFORMIDAD: **NO CONFORMIDAD No.14:** En la verificación realizada por el Equipo Auditor del Grupo de Control Interno en el marco de la aplicación y ejecución del Proceso de Gestión de Tecnologías y Seguridad de la Información, no se evidencia una estrategia de uso y apropiación que permita socializar los instructivos, formatos, procedimientos, políticas etc., del proceso.	

CRITERIO – MARCO LEGAL	DESCRIPCION DE LA SITUACION:
Modelo Integrado de Planeación y Gestión - MIPG Política de seguridad digital	Las Entidades en cabeza de los responsables de administrar las tecnologías de la información, deben garantizar el acceso a un documento de fácil interpretación por cualquier persona (funcionarios, contratistas, ciudadanos), donde se establecen principios orientadores a la seguridad, disponibilidad, integridad, confidencialidad, privacidad, continuidad, autenticidad y no repudio de la información, sin embargo, el Proceso de Gestión de Tecnologías y Seguridad de la Información no muestra evidencias de un manual de políticas de seguridad y privacidad de la información o un documento similar que dé cumplimiento a esta necesidad.

OBSERVACION / NO CONFORMIDAD: **NO CONFORMIDAD No.15:** En la verificación realizada por el Equipo Auditor del Grupo de Control Interno en el marco de la aplicación y ejecución del Proceso de Gestión de Tecnologías y Seguridad de la Información, no se evidencia la existencia de un manual de políticas de seguridad y privacidad de la información.

CRITERIO – MARCO LEGAL	**DESCRIPCION DE LA SITUACION:**
Modelo de Seguridad y Privacidad de la Información – MSPI Decreto 1078 de 2015.	El Proceso no tiene implementado un sistema que adopte medidas efectivas y verificables relacionadas con las buenas prácticas de seguridad de la información, enfocadas a salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información de la Entidad. De acuerdo a las evidencias aportadas en la respuesta al informe preliminar, **se descarta la No Conformidad**
OBSERVACION / NO CONFORMIDAD: **NO CONFORMIDAD No.16:** Se descarta la No Conformidad.	

CRITERIO – MARCO LEGAL	**DESCRIPCION DE LA SITUACION:**
Modelo Integrado de Planeación y Gestión - MIPG Política de seguridad digital	Durante las jornadas de auditoría no se evidenciaron prácticas concretas en el marco y la gestión de Tecnologías de Información – TI, desarrolladas por el Proceso que apoyaran una estrategia de uso y apropiación que aplique para toda la Entidad, cubriendo temas de impacto relacionados con la seguridad de la información.
OBSERVACION / NO CONFORMIDAD: **NO CONFORMIDAD No.17:** En la verificación realizada por el Equipo Auditor del Grupo de Control Interno en el marco de la aplicación y ejecución del Proceso de Gestión de Tecnologías y Seguridad de la Información, no se evidencia una estrategia de uso y apropiación que permita socializar los instructivos, formatos, procedimientos, políticas etc., del proceso.	

CRITERIO – MARCO LEGAL	**DESCRIPCION DE LA SITUACION:**

Modelo Integrado de Planeación y Gestión - MIPG Política de seguridad digital	Las Entidades en cabeza de los responsables de administrar las tecnologías de la información, deben garantizar el acceso a un documento de fácil interpretación por cualquier persona (funcionarios, contratistas, ciudadanos), donde se establezcan principios orientadores a la seguridad, disponibilidad, integridad, confidencialidad, privacidad, continuidad, autenticidad y no repudio de la información, sin embargo, el Proceso de Gestión de Tecnologías y Seguridad de la Información no muestra evidencias de un manual de políticas de seguridad y privacidad de la información o un documento similar que dé cumplimiento a esta necesidad.
OBSERVACION / NO CONFORMIDAD: **NO CONFORMIDAD No.18:** En la verificación realizada por el Equipo Auditor del Grupo de Control Interno en el marco de la aplicación y ejecución del Proceso de Gestión de Tecnologías y Seguridad de la Información, no se evidencia la existencia de un manual de políticas de seguridad y privacidad de la información.	

CRITERIO – MARCO LEGAL	DESCRIPCION DE LA SITUACION:
Modelo de Seguridad y Privacidad de la Información – MSPI Decreto 1078 de 2015.	El Proceso no tiene implementado un sistema que adopte medidas efectivas y verificables relacionadas con las buenas prácticas de seguridad de la información, enfocadas a salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información de la Entidad.
OBSERVACION / NO CONFORMIDAD: **NO CONFORMIDAD No.19:** En la verificación realizada por el Equipo Auditor del Grupo de Control Interno en el marco de la aplicación y ejecución del Proceso de Gestión de Tecnologías y Seguridad de la Información, no se evidencia la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, o un sistema que adopte medidas apropiadas, efectivas y verificables de seguridad que permitan demostrar el correcto cumplimiento de buenas prácticas. Esto con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información, atendiendo lo establecido en el decreto 1078 de 2015.	

CRITERIO – MARCO LEGAL	DESCRIPCION DE LA SITUACION:
Plan Estratégico Tecnologías de la Información – PETI.	De acuerdo con la Circular 2 del mes de julio de 2011 expedida por el Ministerio de Tecnologías de la información y las Comunicaciones, las entidades públicas deberán adoptar todas las medidas necesarias para la adopción del protocolo IPv6, implementando estrategias que garanticen la disponibilidad de los servi-

	cios durante el proceso de transición a través de las diferentes fases establecidas, sin embargo el Proceso no presenta evidencias concretas que demuestren la implantación del protocolo IPv6 en sus tres fases. Teniendo en cuenta las evidencias aportadas en la respuesta al informe preliminar, **se cambia la connotación de No Conformidad a Observación.**

OBSERVACION / NO CONFORMIDAD:

OBSERVACIÓN No.1:
En la verificación realizada por el Equipo Auditor del Grupo de Control Interno en el marco de la aplicación y ejecución del Proceso de Gestión de Tecnologías y Seguridad de la Información, no se evidencian los resultados de las fases I y III del proceso de transición del protocolo IPv6, los servicios publicados en Internet no responden a través de este protocolo, no se aporta evidencia del prefijo IPv6 suministrado por LACNIC a la Entidad y los equipos de usuario final no están configurados con el protocolo IPv6.

5. RECOMENDACIONES

- Realizar seguimiento efectivo a la documentación que hace parte del proceso Gestión de Tecnologías y Seguridad de la Información con el fin de asegurar su aplicación e implementación. Se evidencian formatos que no se están diligenciados.

- El Grupo de Tecnologías de la Información y las Comunicaciones debe asegurar su participación en todos los procesos de adquisición de Tecnologías al interior de la entidad con el fin de dar cumplimiento al objetivo y funciones definidas.

- Se recomienda asegurar que la cuantificación porcentual de los indicadores establecidos en el Plan de Acción Anual, guarden coherencia con lo definido en la actualización de los planes incorporados en el Modelo Integrado de Planeación y Gestión MIPG para la vigencia 2023.

- Se recomienda al Grupo de Tecnologías de la Información y las Comunicaciones adelantar las gestiones necesarias que permitan al proceso construir un documento de caracterización de usuarios y grupos de interés.

- Se recomienda al proceso adelantar actividades que permitan actualizar los documentos del Sistema de Gestión Integrado, fundamentando su contenido en torno a las necesidades de los usuarios, con un contenido claro y que identifique plenamente al grupo o proceso responsable.

- Se recomienda actualizar la actividad 3 del procedimiento GTSI_PR_03 V2 gestión de cambios TI: puesto que en la verificación realizada por el Equipo Auditor del Grupo de Control Interno se evidenció que dicha actividad no se ejecuta.

- Como buena práctica, establecida en el estándar ISO/IEC 27001 A.12.3.1, se recomienda al Grupos de las Tecnologías de la Información y las Comunicaciones ejecutar acciones que permitan validar la efectividad de las copias de respaldo que involucren a la información, software e imágenes de sistemas, mediante pruebas de restauración.

- Se recomienda al Grupo de las Tecnologías de la Información y las Comunicaciones ajustar el instructivo GTSI_IN_08 - copias de seguridad para los sistemas de información de la entidad en el esquema On-premise y nube, con el fin de dar cumplimiento uniforme a los tres niveles de aplicación.

- Se recomienda al Grupo de las Tecnologías de la Información y las Comunicaciones alinear la clasificación de los activos de información, a la TRD actualmente aprobada por el AGN, por lo que la participación del Grupo de Gestión Documental en las mesas de trabajo que se adelanten, será de vital importancia.

- Se recomienda a la Entidad contar con el apoyo de un oficial de seguridad de la información, quien tendrá la responsabilidad de implementar lineamientos de seguridad y privacidad de la información en todos los procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

- Se recomienda al Grupo de las Tecnologías de la Información y las Comunicaciones alinear la clasificación de los activos de información, a la TRD actualmente aprobada por el AGN, por lo que la participación del Grupo de Gestión Documental en las mesas de trabajo que se adelanten, será de vital importancia.

- Se recomienda a la Entidad contar con el apoyo de un oficial de seguridad de la información, quien tendrá la responsabilidad de implementar lineamientos de seguridad y privacidad de la información en todos los procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

- Se recomienda al proceso revisar y ajustar los proyectos del Plan Estratégico de Tecnologías de Información -PETI, para que estos se enfoquen en la solución de necesidades trasmitidas por los mismos usuarios. Importante tener en cuenta que el documento PETI debe concebirse como el resultado de un adecuado ejercicio de planeación estratégica de TI y debe hacer parte integral de la estrategia Institucional en el marco de la Arquitectura Empresarial. Es importante que el Grupo de Tecnologías de la Información y comunicaciones, fortalezca este documento, alineándolo a la estrategia y la visión Institucional, mediante ejercicios de participación en mesas de trabajo que permitan plantear proyectos de innovación e inclusión de tecnologías.

- El Decreto 415 de 2016, establece los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones a través del posicionamiento de los líderes de áreas TI. El Grupo de las Tecnologías de la Información y las Comunicaciones debe afianzar y fomentar el liderazgo y gobernanza tecnológica, a través del fortalecimiento de procesos, procedimientos, estándares y buenas prácticas. Con el cumplimiento de estas acciones, se recomienda expedir un acto administrativo que reafirme lo establecido en el Decreto 415 de 2016, Título 35, artículo 2.2.35.3, numeral 7; “Liderar los procesos de adquisición de bienes y servicios de tecnología, mediante la definición de criterios de optimización y métodos que direccionen la toma de decisiones de inversión en tecnologías de la información buscando el beneficio económico y de los servicios de la entidad.”.

6. CONCLUSIONES

- En la auditoria efectuada al Proceso de Gestión de Tecnologías y Seguridad de la Información, se identificaron dieciséis (16) No conformidades y una (1) Observación que evidencian debilidades en el seguimiento a los controles implementados, la falta de implementación de políticas de gestión y la falta de uso y apropiación de los procedimientos establecidos por el Proceso y los usuarios en general.

- Los planes de recuperación ante desastres, denotan una debilidad que expone de manera directa o indirecta a la Entidad, con un impacto negativo a nivel operativo por la posibilidad de materialización de un riesgo que pueda requerir una acción correctiva.

- La falta de control en las adquisiciones de Tecnologías, dificultan o impiden al Proceso garantizar su oportunidad, confiabilidad, compatibilidad y seguridad. De igual manera se debe llevar un estricto control y seguimiento de los proyectos de inversión ejecutados por la Entidad y que están relacionados con la adquisición de nuevas Tecnologías como una estrategia más de control, sin olvidar que esta información es un insumo vital para los informes de ejecución presupuestal.

- Producto de la auditoría se encontró que no existe un inventario de activos de información institucional, por lo que se determina una no conformidad. En razón a lo anterior el Proceso de Gestión de Tecnologías y Seguridad de la Información tiene la responsabilidad de adelantar las actividades necesarias para el levantamiento de los activos de información, con el fin de aplicar los controles y planes de recuperación que garanticen su conservación y restauración. Esta tarea se debe adelantar de manera articulada con el Proceso de Gestión Documental, y debe ejecutarse al interior de todas las unidades de decisión y las direcciones territoriales, alineando los activos identificados con la Tabla de Retención Documental.

- En la revisión de control de inventarios, se resalta a nivel general la adecuada gestión de licencias por volumen adquiridas en la Entidad, no obstante, se evidenció que algunas actividades se encuentran desactualizadas, especialmente en el movimiento de personal. Por ello, en aras de mantener la mejora continua es importante actualizar dichos soportes o registros establecidos en el procedimiento.

- El Proceso de Gestión de Tecnologías y Seguridad de la Información debe validar la pertinencia de la documentación que a la fecha se encuentra publicada en la intranet y evaluar ese valor agregado que aporta al Proceso.

- El Proceso de Gestión de Tecnologías y Seguridad de la Información debe actualizar toda la documentación que se encuentra relacionada en el Modelo Integrado de Planeación y Gestión y que se articula al indicador establecido para las vigencias 2022 y 2023.

Aprobado por:

NERY LONDOÑO ZAPATA
Coordinadora Grupo de Control Interno (Encargada)

Elaborado por:
Raymon Guillermo Sales Contreras – funcionario.
Carlos Fredy Rey Camacho – Contratista.