PARQUES NACIONALES NATURALES DE COLOMBIA

DIRECCIÓN GENERAL
GRUPO DE CONTROL INTERNO

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

Bogotá, 7 de octubre 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:	Raimond 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 D / MM /AA	**Hasta**	24/07/2023 DD / MM /AA	**Día**	21	**Mes**	07	**Año**	2023

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.

3. DESCRIPCIÓN GENERAL DE LAS NO CONFORMIDADES /OBSERVACIONES

- 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.

- 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 del procedimiento GTSI_PR_03 V2, ya que este indica el paso a paso que se debe llevar a cabo para gestionar las solicitudes de cambio de TI, que son trasversales a todas las Tecnologías en general de la Entidad, incluso la actividad No 2 de este mismo procedimiento tiene como punto de control, el diligenciamiento del formato de Solicitud de Cambios RFC código GTSI_FO_17.

- 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

- 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.

- 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.

- 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".

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

- 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.

4. CONCLUSIONES

- La Arquitectura Empresarial (AE), es un enfoque integral y sistemático para diseñar, planificar y gestionar la estructura y operación de una organización. Su objetivo es alinear de manera estratégica los procesos, la tecnología, los recursos humanos y otros elementos clave para lograr los objetivos de la Entidad. En ese sentido, la AE se convierte en el articulador de todos los procesos, para alinear los objetivos hacia la misión y visión de la entidad.

- El eje central del Proceso de Gestión de Tecnologías y Seguridad de la Información, gira en torno al aseguramiento de los activos de información de la Entidad, por ello, atender las Observaciones y No conformidades reveladas en la auditoría interna; con respecto a la protección de los activos de información, debe darse de manera articulada con los procesos que tienen un impacto directo o indirecto con los activos de información, es decir que sin excepción, todos los procesos de la Entidad tienen un grado de responsabilidad en esta tarea.

5. RECOMENDACIONES

- Realizar un 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 Arquitecta-tura 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.”.

Aprobado por:

GLADYS ESPITIA PEÑA
Coordinadora Grupo de Control Interno