PARQUES NACIONALES NATURALES DE COLOMBIA

DIRECCIÓN GENERAL
GRUPO DE CONTROL INTERNO

INFORME FINAL DE AUDITORIA INTERNA A LA IMPLEMENTACIÓN DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN

Bogotá, 25 de noviembre de 2020

1. INFORMACIÓN GENERAL

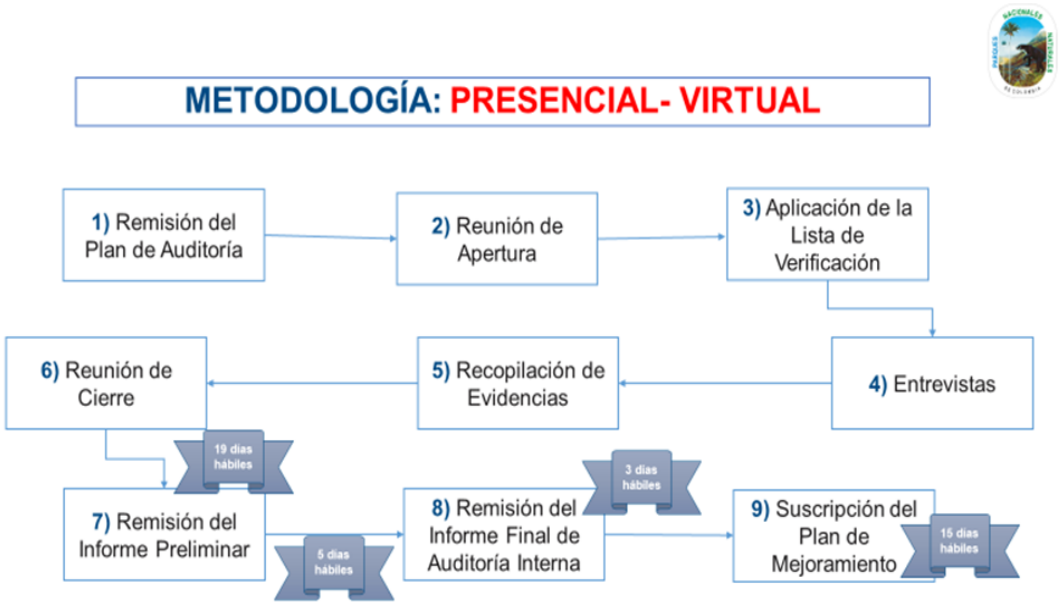
PROCESO O ACTIVIDAD:	Proceso Gestión de Tecnologías y Seguridad de la Información.
AUDITOR LÍDER:	Gladys Espitia Peña.
EQUIPO AUDITOR:	Yolanda Bernal Jiménez- Martha Inés Fernández Pacheco.
AUDITADO:	Grupo de Sistemas de Información y Radiocomunicaciones.
OBJETIVO:	Evaluar de forma sistemática, independiente, objetiva al Proceso Gestión de Tecnologías y Seguridad de la Información en la gestión desarrollada por el Grupo de Sistemas de Información y Radiocomunicaciones, en cumplimiento de las normas la implementación del Sistema de Gestión de Seguridad de la Información.
ALCANCE:	La Auditoría Interna comprende el periodo 2019 y 2020 en el proceso de implementación del Sistema de Gestión de Seguridad de la Información en Parques Nacionales Naturales de Colombia.
CRITERIOS-MARCO LEGAL:	Norma Técnica NTC-ISO/IEC Colombiana 27001:2013. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. Procedimientos.
TIPO DE AUDITORIA:	Interna de Gestión

REUNIÓN DE APERTURA						**EJECUCIÓN DE LA AUDITORÍA**				**REUNIÓN DE CIERRE**					
Día	19	**Mes**	10	**Año**	2020	**Desde**	19/10/2020 DD / MM /AA	**Hasta**	30/10/2020 DD / MM /A	**Día**	04	**Mes**	11	**Año**	2020

2. DETERMINACIÓN DE LA MUESTRA DE AUDITORÍA

Para la verificación del estado de la implementación del Sistema de Gestión de Seguridad de la Información en Parques Nacionales Naturales de Colombia, se tomó como base la Norma Técnica NTC-ISO/IEC Colombiana 27001 y se solicitó al Grupo de Sistemas de Información y Radiocomunicaciones -GSIR-los soportes de cumplimiento de los requisitos de la Norma para las vigencias 2019 y 2020.

3. METODOLOGÍA



En cumplimiento del Plan Anual de Auditorías para la vigencia 2020, el Grupo de Control Interno remitió el Plan de Auditoría al Grupo de Sistemas de Información y Radiocomunicaciones, mediante memorando 20201200008463 del 14 de octubre de 2020 en el formato ESG_FO_03 versión 5.

La reunión de apertura de la Auditoría Interna se realizó el día 19 de octubre de 2020 a través de Google Meet, en donde se expuso el objetivo, alcance y criterios a los participantes del Grupo de Sistemas de Información y Radiocomunicaciones.

Se aplicaron la lista de verificación mediante cuatro (4) solicitudes, realizadas a través de correo electrónico dirigidos a la Coordinadora del Grupo de Sistemas de Información y Radiocomunicaciones.

Con el memorando 20201200008913 del 29 de octubre de 2020, se remitió a la Coordinadora del Grupo de Sistemas de Información y Radiocomunicaciones, la reprogramación de la Reunión de Cierre de la Auditoría Interna a la Implementación del Sistema de Gestión de Seguridad de la Información.

El 3 de noviembre de 2020, se llevó a cabo una reunión virtual con la participación de la Coordinadora y los ingenieros del Grupo de Sistemas de Información y Radiocomunicaciones, la Coordinadora del Grupo de Control Interno y el equipo auditor del Grupo de Control Interno, con el propósito revisar y aclarar algunos aspectos evidenciados en la auditoría.

La reunión de cierre de la Auditoría se llevó a cabo el día 4 de noviembre de 2020, a través de Google Meet, donde se dieron a conocer las fortalezas, recomendaciones y observaciones evidenciadas en la Auditoría Interna.

4. ASPECTOS EVIDENCIADOS DURANTE EL EJERCICIO DE LA AUDITORÍA

4.1 Conocimiento de la Organización y de su Contexto

El proceso Gestión de Tecnologías y Seguridad de la Información, a través de la matriz de Contexto en el formato DE_FO_02 versión 14, analizó e identificó los factores internos y externos, para determinar la capacidad de lograr los objetivos propuestos en la implementación del Sistema de Gestión de Seguridad de la Información.

4.2 Comprensión de las Necesidades y Expectativas de las Partes Interesadas

El proceso Gestión de Tecnologías y Seguridad de la Información, determinó la Matriz de Partes Interesadas Código: DE_FO_15 vigente desde el 2 de abril de 2020, en la cual se incluyen los requisitos de las partes interesadas.

Se observó, que la Agencia Nacional del Espectro, proveedor externo del proceso Gestión de Tecnologías y Seguridad de la Información, según la caracterización del proceso, no se incluyó en la matriz de partes interesadas.

Se evidenció que, dentro de la caracterización del proceso Código: GTSI_CA_01 vigente desde el 13 de octubre de 2020, no se incluyó en los requisitos asociados a normas relacionadas con sistemas de gestión, la Norma Técnica NTC-ISO/IEC Colombiana 27001: 2013.Tecnología de la Información y en el control de cambios el motivo de la actualización de la versión No.5 del documento.

4.3 Determinación del Alcance del Sistema de Gestión de la Seguridad de la Información

El Grupo de Sistemas de Información y Radiocomunicaciones informa que, "*para la determinación de los límites, la aplicabilidad del Sistema de Gestión de Seguridad de la Información y el establecimiento del alcance se tuvieron en cuenta los siguientes criterios:*

a. *En línea con la definición de los documentos del Sistema de Gestión Integrado, se determinan las cuestiones internas y externas dentro de la Matriz de Riesgos en el Análisis de Contexto y alimentan el alcance del Sistema de Gestión de Seguridad de la Información.*

b. *Los requisitos de las partes interesadas establecidos en la Matriz de Partes Interesadas.*

c. *Las interfaces y dependencias con externos, determinadas dentro de la Matriz de Partes Interesadas, el Proceso de Gestión de Tecnologías y Seguridad de Información y los procedimientos asociados".*

Se evidenció que el alcance del sistema se encuentra establecido en el numeral 2.5 del Manual del Sistema de Gestión Integrado-SGI - Código: DE_MN_01, vigente desde el 6 de octubre de 2020.

5.1 Liderazgo y Compromiso

En desarrollo de la auditoría se solicitó información sobre cómo la Alta Dirección ha demostrado liderazgo y compromiso con respecto al Sistema de Gestión de Seguridad de la Información, a lo que el Grupo de Sistemas de Información y Radiocomunicaciones respondió, que "*la Alta Dirección a través de la publicación del Manual del Sistema Integrado de Gestión manifiesta el interés y compromiso que tiene con el Sistema de Gestión de Seguridad de la Información.*

a. *A través de la Resolución 186 del 16 de junio de 2020, el Modelo Integrado de Planeación asegura la adopción del Manual del Sistema de Gestión integrado, el cual contiene la Política y Objetivos del Sistema de Gestión Integrado.*

b. *La integración de requisitos está dada a través del proceso de Gestión de Tecnologías y Seguridad de la Información definido.*

c. *La destinación de recursos humanos, físicos, financieros y tecnológicos es compromiso a través del Manual del Sistema de Gestión Integrado y está dada de acuerdo con la asignación presupuestal por cada vigencia, permitiendo contratar el recurso humano necesario y ejecutar los proyectos base para el funcionamiento del Proceso de Gestión de Tecnologías y Seguridad de la Información.*

d. *En cuanto a los procesos de comunicación, se han desarrollado algunas campañas de concientización a través de medios digitales como el correo electrónico, para la salvaguarda de la información, la apropiación de contraseñas seguras y el despliegue de doble factor de autenticación para las cuentas corporativas, con el fin de garantizar los principios básicos de la seguridad de la información (confidencialidad, disponibilidad e integridad), así mismo está en construcción la plataforma de Elearning (Moodle, https://escuelavirtual.parquesnacionales.gov.co/) y se tiene definido un plan de comunicaciones, el cual queda activo una vez aprobada política de seguridad de la información*.

   Adicionalmente, durante las reuniones del Comité Institucional de Gestión y Desempeño del 2019 y 2020, se asegura que se establezcan los lineamientos y requerimientos para el cumplimiento de los requisitos del Sistema de Gestión de Seguridad de la Información, por lo cual, durante estos Comités se ha llevado a cabo la presentación y aprobación de los documentos del Subsistema de Gestión de Seguridad de la Información.

e. *Frente al aseguramiento de los resultados previstos, se adopta la hoja metodológica de indicadores, la cual define las metas establecidas para el Sistema de Gestión de Seguridad de la Información y se mide trimestralmente.*

f. *Dentro del Plan de Comunicaciones del SGSI, se tienen proyectadas las campañas y capacitaciones enfocadas en Seguridad de la Información, las cuales contribuyen a la eficacia del SGSI. Además, se han llevado a cabo capacitaciones internas sobre la gestión de riesgos de seguridad y de manera técnica se han definido*

planes de remediación para los análisis de vulnerabilidades realizados, así mismo se ha implementado planes de mejora para los incidentes generados al sistema de gestión."

Evidencias:

- Correo de Configuración Verificación en dos pasos para las cuentas de correo.
- Guía de Configuración para Cuentas de Correo la cual tiene como objetivo principal guiar al usuario que tiene una cuenta de correo institucional de parques nacionales, en la configuración de verificación en dos pasos para su cuenta de correo como un método de seguridad adicional recomendado para la autenticación.
- Hoja Metodológica de Indicadores Código: DE_FO_03 Vigente desde: mayo/2020- reporte II y III trimestre 2020.
- Plan de sensibilización y comunicaciones en seguridad de la información-PNNC- Versión 3.4 Septiembre de 2020, documento que tiene como objetivos para la vigencia 2020:
  - Mejorar el conocimiento de los colaboradores de Parques Nacionales Naturales de Colombia en el SGSI.
  - Fortalecer las capacidades institucionales para prevenir y dar respuesta a eventos de seguridad.
  - Formar primeros respondientes en incidentes de seguridad.
- Plan Tratamiento de Vulnerabilidades de TI, el cual tiene como objetivo presentar el plan para el tratamiento de vulnerabilidades de TI, con el fin de documentar y publicar cada una de las acciones asociadas a la mitigación de riesgos de seguridad.
- Presentaciones Seguridad y Privacidad TI-Comité Julio 2020 y Gestión de Riesgos Grupo de Sistemas de Información y Radiocomunicaciones.

5.2 Política

Se evidenció que a través del Manual del Sistema Integrado de Gestión Código: DE_MN_01 vigente desde el 14 de octubre de 2020, se definió y adoptó la Política del Sistema de Gestión de Seguridad de la Información, la cual:

a. Está concebida de acuerdo con los criterios y propósito de la entidad.
b. Incluye los objetivos de Seguridad de la Información.
c. En el numeral 4 del Manual del Sistema de Gestión Integrado, enmarca los compromisos y requisitos aplicables a cada uno de los subsistemas incluyendo el del Subsistema de Gestión de Seguridad de la Información.
d. Incluye el compromiso para la mejora continua.

El Grupo de Sistemas de Información y Radiocomunicaciones, comunica que "*la política está publicada en la intranet y en el portal de la entidad en el siguiente enlace: https://intranet.parquesnacionales.gov.co/wp-content/uploads/2020/10/de_mn_01_-manual-del-sistema-de-gestion-integrado-sgi-_v_8.pdf".*

Igualmente, que "se *realizó comunicación interna de la política con el Grupo de Sistemas de Información y Radiocomunicaciones y se incluye dentro de la promoción de las actualizaciones del sistema de gestión integrado a cargo de la OAP para final del mes de octubre".*

Se evidenció el correo con el cual se comunicó la política al interior del Grupo de Sistemas de Información y Radiocomunicaciones.

5.3 Roles, Responsabilidades y Autoridades en la Organización

Se solicito evidencias de cómo la Alta Dirección se aseguró que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignarán y comunicarán, para lo cual Grupo de Sistemas de Información y Radiocomunicaciones respondió: "*Dentro del Manual del Sistema Integrado de Gestión se definen las responsabilidades del modelo de seguridad de la entidad, estableciendo roles y responsabilidades por cada uno de los involucrados.*

a. *El Sistema de Gestión de Seguridad de la Información está amparado por los lineamientos del Gobierno Nacional en materia de Gobierno Digital y la Norma ISO: IEC 27001:2013.*

b. *A partir de la aprobación de la Política de Seguridad de la Información, como documento primario para la implementación del Sistema de Gestión de Seguridad de la Información, se iniciará el reporte a la Alta Dirección a través del Comité Institucional de Gestión y Desempeño y demás informes definidos para tal fin."*

Se evidenció, lo señalado en el numeral 3.3 del Manual del Sistema Integrado de Gestión, la definición de los "Roles, Responsabilidades y Autoridades en la Organización" por cada dimensión y política de gestión y desempeño institucional. Para la dimensión "Gestión con valores para el resultado. Operación Interna", para las políticas de gestión y desempeño "Gobierno Digital y Seguridad Digital", los responsables son la Subdirección de Gestión y Manejo y el Grupo de Sistemas de Información y Radiocomunicaciones en calidad de Líder Estratégico y Líder Operativo.

6.1 Acciones para tratar Riesgos y Oportunidades

Se solicitó información sobre las acciones para tratar riesgos y oportunidades, a lo que el Grupo de Sistemas de Información y Radiocomunicaciones comunico que, "*dentro de la Planificación del Sistema de Seguridad de la Información, se contemplan las cuestiones referidas en los capítulos 4.1 y 4.2, para lo cual se desarrolló el Mapa de Gestión de Riesgos y Matriz de Oportunidades, con el fin de:*
a. Asegurar el cumplimiento de los resultados previstos.
b. Se definen acciones de mejora sobre cada uno de los riesgos identificados, para prevenir o reducir efectos indeseados.
c. Lograr la mejora continua".

"La política y metodología de riesgos institucional y su matriz de control, está alineada con el Modelo Integrado de Planeación y Gestión- MIPG- y adoptada para dar cubrimiento a los riesgos de corrupción, de seguridad digital y de gestión. De igual manera, se establece el Proceso de Gestión de Tecnologías y Seguridad de la Información para integrar e implementar las acciones necesarias que permitan mitigar y prevenir los riesgos identificados. Las acciones necesarias para el tratamiento de los riesgos, y los avances en la implementación del SGSI, se miden trimestralmente a través del reporte de Mapa de Riesgos y la Hoja Metodológica en el PAA".

Se evidenció en la Matriz de Riesgos y Oportunidades DE_FO_02 versión 14, el reporte correspondiente al segundo cuatrimestre de 2020 realizado por el Grupo de Sistemas de Información y Radiocomunicaciones.
La Hoja Metodológica de Indicadores Código: DE_FO_03 Vigente desde: mayo de 2020- reporte II y III trimestre 2020 en el Plan de Acción Anual -PAA.

Procedimiento de administración de riesgos y oportunidades, Código: DE_PR_01 Vigente desde el 13 de octubre de 2020.

6.1.2 Valoración de Riesgos de la Seguridad de la Información.

Se preguntó si se aplicó el proceso de valoración de riesgos de la seguridad de la información para identificar los riesgos asociados con la pérdida de confidencialidad, de integridad y de disponibilidad de información, a lo que respondió el Grupo de Sistemas de Información y Radiocomunicaciones el Grupo de Sistemas de Información y Radiocomunicaciones GSIR, "*que, se cuenta con una metodología de gestión de riesgos unificada con la entidad bajo los lineamientos del MIPG. Se enlaza al Procedimiento de Administración de Riesgos y Oportunidades de PNNC (https://intranet.parquesnacionales.gov.co/wp-content/uploads/2020/10/de_pr_01_-administracion-de-riesgos-y-oportunidades_v_11.pdf)".*

"El Grupo de Sistemas de Información y Radiocomunicaciones definió acciones de control por cada riesgo determinando las acciones a ejecutar en caso de materialización de estos, estas acciones están definidas en la matriz de riesgos."

"El Grupo de Sistemas de Información y Radiocomunicaciones identificó los riesgos asociados a seguridad de la información aplicando procesos de verificación y valoración los cuales son reportados periódicamente a través de la Matriz de Riesgos y Oportunidades. "

Se evidenció la Matriz de Riesgos en el formato DE_FO_02 versión 14, reportado por el Grupo de Sistemas de Información y Radiocomunicaciones.

6.2 Objetivos de Seguridad de la Información y Planes para lograrlos

El Grupo de Sistemas de Información y Radiocomunicaciones informó que*, "en el Manual del Sistema de Gestión Integrado, se definen los objetivos de seguridad conforme a los niveles funcionales asociados a los procesos de control; estos:*

a. *Están definidos en base a los requerimientos de seguridad de la información.*
b. Son medibles, para ello se establecen algunos indicadores Técnicos, con el objetivo de soportar técnicamente el cumplimiento de estos.
c. Teniendo en cuenta la reciente aprobación del manual del Sistema Integrado de Gestión, se tiene previsto enviar la comunicación para el conocimiento y divulgación en la entidad.
El repositorio dónde se cargan las evidencias y documentación de Seguridad de la Información, es el definido en el repositorio colaborativo de la entidad (Drive), para Matriz de Riesgos y reporte PAA".

Se evidenció:

El Manual del Sistema de Gestión Integrado, Código: DE_MN_01 versión 8, vigente desde el 14 de octubre de 2020, numeral 4.1, Objetivos Subsistema Privacidad y Seguridad de la Información:

- Gestionar adecuadamente la seguridad de la información, la gestión de activos, la gestión de riesgos y la continuidad en la prestación de los servicios ofrecidos.
- Mantener la confidencialidad, integridad, disponibilidad y control sobre la información administrada por Parques Nacionales Naturales de Colombia mediante la construcción de lineamientos, aplicación de estrategias y aplicación de mecanismos técnicos y tecnológicos.
- Apalancar la implementación del Sistema de Gestión de Seguridad de la Información de la entidad de acuerdo con los requerimientos establecidos en el modelo de seguridad de la estrategia de Gobierno en Línea.
- Establecer lineamientos para la implementación y/o adopción de mejores prácticas de seguridad en la entidad.
- Optimizar la gestión de la seguridad de la información al interior de la entidad.

El Grupo de Control Interno preguntó si, la organización determinó lo que se va a hacer y que recursos se requerirán cuándo se hizo la planificación para lograr los objetivos de la seguridad de la información, a lo cual el Grupo de Sistemas de Información y Radiocomunicaciones, respondió:

"Dentro de la planificación del Sistema de Gestión de Seguridad de la Información, se determinan las fases y actividades para su implementación, adicionalmente en el presupuesto anual se solicitan los recursos requeridos tanto humanos como financieros, las metas y resultados están proyectados en la hoja metodológica del Sistema de Gestión de Seguridad de la Información".

Se evidenció:
Plan Operacional Sistema de Gestión de Seguridad de la Información.
Planificación presupuesto 2021.
https://drive.google.com/drive/folders/1iWaNZ6gIPLPVDTqliqFpWqgVtbrqBUfr
Sistema de Gestión de Seguridad de la Información 2019 con el Plan de Implementación Modelo de Seguridad.
Presupuesto 2020.

7.1 Recursos

El Grupo de Sistemas de Información y Radiocomunicaciones, manifiesta*: "Parques Nacionales Naturales de Colombia, a través de la Subdirección de Manejo de Áreas Protegidas, en cabeza del Grupo de Sistemas de Información y Radiocomunicaciones definió los recursos necesarios de acuerdo con su plan de acción para la vigencia 2020, donde se tuvo en cuenta la gestión del sistema de seguridad de la Información y el personal para gestionar el sistema; esta definición está dada por la apropiación presupuestal en donde se contempla la contratación del personal de tecnología de la información y recursos tecnológicos".*

El Presupuesto para el Grupo de Sistemas de Información y Radiocomunicaciones en la vigencia 2019 ascendió a $6.105.396.617, el compromiso ascendió al 93.12% frente a la apropiación, las obligaciones y los pagos fueron del 57.58% frente a los compromisos realizados y la reserva de apropiación fue del 42.42% frente a los compromisos registrados.

Para la vigencia del año 2020, el presupuesto ascendió a $7.750.970.405.54 con corte a 31 de octubre de 2020, la ejecución se presenta así: Compromisos registrados el 41.92% y las obligaciones y pagos se encuentran en el 54% de los compromisos registrados. Teniendo en cuenta el presupuesto asignado para el Grupo de Sistemas de Información y Radiocomunicaciones se encuentra pendiente de ejecutar a 31 de octubre de 2020, el 58.08%. Es necesario revisar los proyectos pendientes por comprometer.

VIGENCIA	DEPENDENCIA	APROPIACIÓN VIGENTE	COMPROMISOS	OBLIGACIÓN	PAGOS	RESERVAS DE APROPIACIÓN
2019	Total, recursos Grupo de Sistema de Información y Radiocomunicaciones	6,105,396,617.00	5,685,559,400.35	3,273,956,922.75	3,273,956,922.75	2,411,602,477.60
	Porcentaje ejecutado año 2019		93.12	57.58		42.42
2020	Total, recursos Grupo de Sistema de Información y Radiocomunicaciones	7,750,970,405.54	3,249,429,620.60	1,754,734,879.54	1,754,734,879.54	
	Porcentaje ejecutado a octubre 2020		41.92	54.00		

Fuente: Grupo de Gestión Financiera

Por lo anterior, se evidenció, que Parques Nacionales Naturales de Colombia determinó y proporcionó los recursos para la implementación y el mantenimiento para las vigencias 2019 y 2020.

7.2 Competencia

El Grupo de Sistemas de Información y Radiocomunicaciones, informa que: "*Las competencias necesarias para el personal que realiza trabajo y que afecta el desempeño del Modelo de Seguridad y Privacidad de la Información (MSPI), se determinan de acuerdo con el procedimiento de contratación definido por Parques Nacionales Naturales de Colombia -PNNC; adicional a esto, el Grupo de Sistemas de Información y Radiocomunicaciones plantea los perfiles requeridos, los cuales se evalúan conforme a los estudios previos para la contratación de éstos".*

La contratación del personal por prestación de servicios se realiza a través del SECOP, el cual contiene la información de contratación en cumplimiento a la Ley 80 de 1993.

Se evidenció el estudio previo de contratista para la seguridad de la información, donde se define la descripción de la necesidad que se pretende satisfacer con la contratación, la descripción del objeto, obligaciones, actividades y productos a entregar, plazo de ejecución, presupuesto oficial estimado, entre otras. En el cual se determina la competencia necesaria de las personas que lo realizan, basándose en la formación académica y experiencia. La información de los contratos de prestación de servicios y su ejecución se encuentran en el SECOP.
En reunión celebrada con el Grupo de Sistemas de Información y Radiocomunicaciones, el 3 de noviembre de 2020, informaron que son nueve (9) personas las que intervienen en este proceso y todas están contratadas mediante contrato de prestación de servicios, tres (3) en el Nivel Central y uno (1) por cada Dirección Territorial.

7.3 Toma de Conciencia

El Grupo de Sistemas de Información y Radiocomunicaciones, informa que*: "Parques Nacionales Naturales de Colombia ha dispuesto campañas de concientización a través del medio digital (Correo electrónico). Se encuentra en implementación la plataforma E-learning (https://escuelavirtual.parquesnacionales.gov.co/) con el fin de optimizar los procesos de aprendizaje y concientización. Estos procesos se proyectan desde el plan de comunicaciones".*

"Para la contribución a la eficacia del Sistema de Gestión de la Seguridad de la Información, se genera un informe de gestión mensual, el cual abarca todos los elementos en materia de seguridad e infraestructura, de tal manera que se evidencian todos los controles técnicos implementados, estos comenzaron a alimentar el sistema, una vez adoptada y aprobada la política del Sistema de Gestión de la Seguridad de la Información. Así mismo, se realiza seguimiento al Modelo de Seguridad y Privacidad de la Información a través de las hojas metodológicas de indicadores y los planes de acción definidos en la matriz de riesgos".

"Aunado a lo anterior, desde infraestructura tecnológica, redes y seguridad se ha venido garantizando la operación segura de los servicios tecnológicos de PNNC, conforme a los elementos brindados desde el área y la Subdirección de Manejo de Áreas Protegidas a Nivel Nacional, con herramientas base para la gestión y cumplimiento de los objetivos misionales, el apoyo al desempeño, la protección de la información y facilidades de acceso de los usuarios externos e internos a los sistemas de información de la entidad".

Se evidenció el Plan de Sensibilización y Comunicaciones en Seguridad de la Información de septiembre de 2020 y las 7 campañas que han sido enviadas a través del correo electrónico, como son: seguridad, confidencialidad e integridad; nuevas funcionalidades herramienta Meet; fortalece tus capacidades en el uso de herramientas de Google; ten presente que una cuenta de correo tiene 30 GB de espacio de almacenamiento por lo tanto se debe dar buen uso al mismo; protege tus datos no te dejes engañar.

7. 4 Comunicación

El Grupo de Sistemas de Información y Radiocomunicaciones, comunicó que "*La estrategia adoptada por el Grupo de Sistemas de Información y Radiocomunicaciones para las comunicaciones internas y externas del Sistema de Gestión de la Seguridad de la Información ha sido la utilización de los medios digitales de Parques Nacionales Naturales de Colombia, la creación de un curso en la escuela Moodle de PNNC (en construcción) y espacios en los comités de gestión para la divulgación y oficialización de los documentos y campañas realizadas por correo electrónico*".

El Grupo de Sistemas de Información y Radiocomunicaciones remitió la presentación sobre la Seguridad y Privacidad de Tecnología de la Información, en la cual definen que es la seguridad de la información, la política de seguridad de la información, fuentes de compromiso, que hacemos desde el Grupo de Sistemas de Información y Radiocomunicaciones, los Tips para proteger la información y por qué se debe proteger la información, así mismo las propuestas de campaña de sensibilización tales como: enforce de contraseñas – correo, implementación de Token de autenticación, implementación de certificados digitales PC y ataque de ingeniería Social.

7.5 Información Documentada

7.5.1 Generalidades

Parques Nacionales Naturales de Colombia, determinó para la eficacia del Sistema de Seguridad de la Información, la expedición de la Política MIPG y el Manual del Sistema de Gestión Integrado, el cual declara las Políticas de Seguridad de la Información que viene apoyada por el Plan Operacional de Seguridad de la Información y se mide específicamente con la aplicación de la Hoja Metodológica de Indicadores para el reporte, control y seguimiento del modelo.

Como evidencias el Grupo de Seguridad de Información y Radiocomunicaciones remitió:

La Resolución 0186 del 16 de junio de 2020 "Por la cual se modifica parcialmente la Resolución 0361 del 9 de octubre de 2019 y se adopten otras disposiciones". En el artículo 1, se adopta el modelo integrado de planeación y gestión – MIPG. En el Sistema de Gestión Integrado de PNNC se encuentra el subsistema de Seguridad de la Información.

Además, remite el Manual del Sistema de Gestión Integrado Versión 8, vigente desde el 14 de octubre de 2020; el Plan Operacional del Sistema de Gestión de la Seguridad de la Información (SGSI) – Plan de seguridad y privacidad de la información cuyo objetivo es apoyar el establecimiento del Sistema de Gestión de Seguridad y Privacidad de la Información de la entidad, acorde a los requerimientos del modelo de seguridad de la estrategia de gobierno digital los requerimientos del negocio y en cumplimiento de las disposiciones legales vigentes.

Se verificó el Balance del Segundo y Tercer Trimestre 2020 – Plan de Acción Anual, proceso:" Porcentaje de implementación del Plan de Seguridad y Privacidad de la Información", con un avance del 72% y 90%, en los siguientes enlaces:
https://www.parquesnacionales.gov.co/portal/wp-content/uploads/2013/08/BALANCE-PAA-2%C2%B0-TRIMESTRE-2020.pdf
https://www.parquesnacionales.gov.co/portal/wp-content/uploads/2013/08/balance-de-metas-paa_-iii_trimestre_2020.pdf

7.5.2 Creación y Actualización

El Grupo de Sistemas de Información y Radiocomunicaciones, informa que: "*Los controles establecidos se rigen por el manual del sistema de gestión integrado y los controles de la Norma ISO 27001:2013, a partir de la adopción del Modelo de Seguridad y Privacidad de la Información, así mismo, se establece una hoja de controles, con las cuales se determina el nivel de adopción de cada uno de ellos asociados a las políticas de seguridad".*

El Grupo de Sistemas de Información y Radiocomunicaciones presentó una matriz de controles de Seguridad de la Información en la cual se observó: el dominio, el objetivo del control, la descripción del control, el nivel de cumplimiento (diagnóstico inicial-madurez-porcentaje).

Se dispone de las siguientes políticas de seguridad, las cuales fueron elaboradas el 1 de septiembre de 2019 y se encuentran en trámite de aprobación: de uso de internet, redes sociales, relacionamiento con proveedores, destrucción de la información, acceso remoto, gestión de cambios, gestión de riesgos de seguridad de la información, escritorio y pantalla limpios, cumplimiento, continuidad de las operaciones y recuperaciones, uso de controles criptográfi-

cos, dispositivos móviles, intercambio de información, registro y auditoría de eventos, separación de entornos, protección software malicioso, respaldo de información, control de acceso físico a áreas seguras, gestión de usuarios privilegiados, acceso lógico, uso aceptable de activos, gestión de incidentes de seguridad y sistema de gestión de seguridad de la información.

De acuerdo con la información recibida en reunión del 3 de noviembre de 2020, por parte de la Coordinadora y profesionales del Grupo de Sistemas de Información y Radiocomunicaciones, estas políticas no han sido aprobadas por cuanto, la política del Sistema de Gestión de Seguridad de la Información, tan solo se aprobó el 14 de octubre de 2020 en el Comité Institucional de Gestión y Desempeño. Por lo anterior, la aprobación de estas políticas se realizará por parte de la responsable del Proceso Gestión de Tecnologías y Seguridad de la Información y la Coordinadora del Grupo de Sistemas de Información y Radiocomunicaciones.

7.5.3 Control de la Información Documentada

"El Grupo de Sistemas de Información y Radiocomunicaciones, implementa herramientas de almacenamiento y protección de la información en data center y nube, para albergar la información generada por los usuarios de Parques Nacionales Naturales de Colombia, tanto a nivel local, cómo en los sistemas de información. Estos sistemas, están monitoreados y respaldados, de acuerdo con la Política de Respaldo de Información."

"La información es procesada y controlada por el Grupo de Procesos Corporativos, quienes estandarizan y normalizan la información institucional, adicionalmente, la información la publican las dependencias en la intranet y medios públicos de la entidad (página web), esta información está protegida por los repositorios, los cuales tiene acceso a través el manejo de perfiles de usuarios".

Evidencias. El Grupo de Sistemas de Información y Radiocomunicaciones cuenta con la política de control de acceso lógico, la cual establece los lineamientos generales para controlar el acceso a los activos de información y a los activos de tratamiento de la información. La política de respaldo de información preserva la información de la Institución o en poder restaurarla en tiempo y forma en caso de pérdida. La política de gestión de cambios para garantizar los lineamientos generales de la entidad con relación a la Tecnología de la Información.

El procedimiento gestión copias de seguridad GAINF_PR_03 Versión 5, presenta la última actualización el 11 de diciembre de 2018. Se revisó la actividad 5 que dice: "Realizar, etiquetar, probar y almacenar e Backup físicamente en el sitio definido según lo estipulado en el instructivo de copias de seguridad". Punto de control - Formato de asignación de bienes y servicios tecnológicos para funcionarios y contratistas - copias de seguridad GAINF_FO_26. Se observó que están diligenciando el formato correctamente y es el documento soporte para la creación del usuario.

La política de intercambio de información es para garantizar la seguridad de la información que se intercambia o transfiere dentro de la entidad y con cualquier entidad externa a la misma haciendo uso de cualquier recurso de comunicación. Se encuentra en proceso de aprobación. La política aún no cuenta con un procedimiento de control para la información de origen externo. La información que se encuentra en el DRIVE es información restringida.

8.1 Planificación y Control Operacional

"La planificación, implementación y control de los procesos del Modelo de Seguridad y Privacidad de la Información, se determinan a través del autodiagnóstico realizado a la entidad, planificados por medio del Plan Operacional de Seguridad y Privacidad de la Información y establecidos en la Hoja Metodológica de Indicadores, con la cual se controla el avance en el cumplimiento de la norma."

"De acuerdo con el Plan Operacional se planifican los procesos de control para cumplir con los requisitos del modelo de seguridad de la información, para apalancar este proceso se está implementado un sistema de control y gestión sobre el modelo Sistema de Gestión del Sistema de Información para implementar procesos de control sobre cambios".

Se evidenció el Plan de Seguridad y Privacidad de la Información 2019 cuyo objetivo es establecer un plan que apoye el establecimiento del Sistema de Gestión de Seguridad y Privacidad de la información de la entidad, acorde a los requerimientos del modelo de seguridad de la estrategia de Gobierno Digital los requerimientos del negocio y en cumplimiento de las disposiciones legales vigentes.

Igualmente, se verificó el Balance del Segundo y Tercer Trimestre 2020 – Plan de Acción Anual, proceso:" Porcentaje de implementación del Plan de Seguridad y Privacidad de la Información", con un avance del 72% y 90%, en los siguientes enlaces:
https://www.parquesnacionales.gov.co/portal/wp-content/uploads/2013/08/BALANCE-PAA-2%C2%B0-TRIMESTRE-2020.pdf
https://www.parquesnacionales.gov.co/portal/wp-content/uploads/2013/08/balance-de-metas-paa_-iii_trimestre_2020.pdf

Sobre cómo se controlan los procesos contratados externamente, el Grupo de Sistemas de Información y Radiocomunicaciones comunicó que los "*procesos contratados externamente están apalancados contractualmente y están cobijados por los elementos legales definidos por la entidad para la gestión de seguridad. Así mismo, están cubiertos por el Proceso de Gestión Contractual de la entidad, por lo cual, se lleva a cabo la supervisión y control bajo los lineamientos entregados por la Subdirección Administrativa y Financiera y la Política de Relacionamiento con Proveedores establecida por el Grupo de Seguridad de Información y Radiocomunicaciones, la cual tiene como objetivo mantener la seguridad de los activos de información que deban ser accedidos por proveedores"*. Esta política, se encuentra pendiente de aprobación.

El Grupo de Sistemas de Información y Radiocomunicaciones, presenta el Acta del 14 de abril de 2020, suscrita entre PNNC y PASSWORD Consulting Services SAS, en la cual se presenta el Plan del Proyecto: Adquisición de la plataforma, administración y modelo de seguridad de la información para Parques Nacionales Naturales de Col., así mismo el formato del acuerdo de confidencialidad y/o propiedad intelectual (terceros) firmado el 7 de octubre de 2020, entre PNNC y PASSWORD Consulting Services SAS.

8.2 Valoración de Riesgos de la Seguridad de la Información

"Trimestralmente se realiza la valoración e informe de la gestión de los riesgos y la información derivada de los reportes se encuentra publicada en la página Web de la entidad".

Evidencia: Matriz e riesgos y oportunidades. en el formato DE_FO_02 versión 14, que se encuentra diligenciada con corte a 30 de agosto de 2020. Las observaciones y los comentarios a los riesgos se encuentran en el Informe de Seguimiento a la Gestión del Riesgo del segundo cuatrimestre de 2020, publicado en la página web.

9. Evaluación De Desempeño

9.1 Seguimiento, Medición, Análisis y Evaluación

"La medición y evaluación del Sistema de Gestión de Seguridad de la Información se hace a través de Hoja Metodológica de Indicadores, la cual es reportada a través del Plan de Acción Anual (PAA)".

Se verificó el Balance del Segundo y Tercer Trimestre 2020 – Plan de Acción Anual, proceso: Porcentaje de implementación del Plan de Seguridad y Privacidad de la Información, con un avance del 72% y 90%, en los siguientes enlaces:
https://www.parquesnacionales.gov.co/portal/wp-content/uploads/2013/08/BALANCE-PAA-2%C2%B0-TRIMESTRE-2020.pdf
https://www.parquesnacionales.gov.co/portal/wp-content/uploads/2013/08/balance-de-metas-paa_-iii_trimestre_2020.pdf

9.2 Auditoría Interna.

El Plan Anual de Auditoria 2020, se encuentra en ejecución con la auditoría de la Implementación del Sistema de Gestión de Seguridad de la Información para los periodos 2019- 2020 y el Plan de Mejoramiento por Proceso - Gestión se suscribirá una vez se presente el Informe Final la Auditoría a la líder del proceso.

9.3 Revisión Por La Dirección

"Teniendo en cuenta que el Sistema de Gestión de Seguridad de la Información se adoptó durante el mes de octubre de 2020, no se ha presentado información para la revisión por la Dirección".

El Grupo de Control Interno evidenció, el acta de la Revisión por la Dirección del año 2019, en la cual no se encontró información relacionada con el Grupo de Sistemas de Información y Radiocomunicaciones.

10. Mejora

10.1 No Conformidades y Acciones Correctivas

Se evidenció el Plan de Mejoramiento por Proceso - Gestión resultado de la auditoría al proceso de Gestión Documental. A la fecha de la auditoria el Grupo de Sistemas de Información y Radiocomunicaciones presenta un plan de mejoramiento con una acción de corrección y una acción correctiva las cuales tienen fecha de vencimiento del 15 de diciembre de 2020.

4.1 ASPECTOS POSITIVOS: FORTALEZAS

- ✓ Se destaca el compromiso y el amplio concomimiento sobre el Sistema de Seguridad de la Información por parte de la Coordinadora, contratistas y profesionales del Grupo de Sistemas de Información y Radiocomunicaciones que lidera la implementación en la Entidad.

- ✓ Es de resaltar la disponibilidad, la actitud y el respeto de la Coordinadora y su equipo de trabajo para atender la Auditoría Interna.

- ✓ La contextualización de las respuestas, como la evidencias y su organización, por parte del Grupo de Sistemas de Información y Radiocomunicaciones, facilitaron el ejercicio de Auditoría Interna, permitiendo un conocimiento amplio del estado de la Implementación del Sistema de Gestión de Seguridad de la Información.

4.2 LIMITACIONES

No se presentaron limitaciones en el alcance y desarrollo de la auditoría interna que no permitieran 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:
4.4 Sistema de Gestión de la Seguridad de la Información	Se solicitó Plan de Trabajo para las vigencias 2019 y 2020, que permita visualizar el desarrollo de la implementación del Sistema de Seguridad de la Información en PNNC. Igualmente, se preguntó cómo la organización estableció, implementó, mantiene y mejora continuamente el sistema de gestión de la seguridad de la información, de acuerdo con los requisitos de la NTC ISO 27001:2013. El Grupo de Sistemas de Información y Radiocomunicaciones informó que "*de acuerdo con los requisitos de la norma ISO 27001:2013, el Sistema de Gestión de Seguridad de la Información se establece a partir de la Oficialización de la Resolución 186 del 16 de junio de 2020, por medio de la cual se adopta el Modelo Integrado de Planeación y Gestión - MIPG; y la publicación de la declaración de la política del SGSI en el Manual del Sistema de Gestión Integrado del 10 de octubre de 2020; así mismo, para la implementación, mantenimiento y mejora continua y teniendo en cuenta la reciente adopción de la política a través de resolución, el Grupo de Sistemas de Información y Radiocomunicaciones inició la implementación desde el Plan de Seguridad y Privacidad de la Información, además adquirió y está implementando un Sistema de Gestión para el control y seguimiento del modelo SGSI, adicional a*

	esto se adopta una hoja metodológica a través de la cual se reporta el seguimiento y cumplimiento periódico del SGSI". No se evidenció en el Plan de Implementación del Modelo de Seguridad (Plan de Trabajo) el seguimiento, los cambios y ajustes realizados durante los años 2019 y 2020 a las actividades programadas, como tampoco, la presentación de estos cambios al Comité Institucional de Gestión y Desempeño. (Observación No. 1) Se evidenció la siguiente documentación: Plan de Implementación del Modelo de Seguridad, el cual, no está actualizado con los cambios y ajustes realizados durante los años 2019 y 2020, ni los seguimientos realizados por el Comité Institucional de Gestión y Desempeño. El Manual del Sistema de Gestión Integrado Código: DE_MN_01 versión 8, vigente desde el 14 de octubre de 2020. El Plan de Seguridad y Privacidad de la Información 2020, el cual tiene como objetivo apoyar el establecimiento del Sistema de Gestión de Seguridad y Privacidad de la Información de Parques Nacionales Naturales de Colombia, acorde a los requerimientos del modelo de seguridad de la estrategia de gobierno digital, los requerimientos del negocio y en cumplimiento de las disposiciones legales vigentes e incluye el Plan de Implementación del Modelo de Seguridad. Resolución No.186 de 2020, "Por la cual se modifica parcialmente la Resolución 0361 del 9 de octubre de 2019 y se adoptan otras disposiciones" Hoja Metodológica de Indicadores Código: DE_FO_03 Vigente desde: mayo de 2020. Reporte II y III trimestre 2020.
OBSERVACION / NO CONFORMIDAD: **OBSERVACIÓN No.1** No se evidenció en el Plan de Implementación del Modelo de Seguridad (Plan de Trabajo) el seguimiento, los cambios y ajustes realizados durante los años 2019 y 2020 a las actividades programadas, como tampoco, la presentación de estos cambios al Comité Institucional de Gestión y Desempeño, conforme el literal b) de la Resolución No.361 del 9 de octubre de 2020 que, señala dentro de las funciones del Comité "Revisar las acciones y estrategias adoptadas para la operación del Modelo Integrado de Planeación y Gestión - MIPG".	

CRITERIO – MARCO LEGAL	DESCRIPCION DE LA SITUACION:
6.1.3 Tratamiento de Riesgos de la Seguridad de la Información	Sobre el tratamiento de Riesgos, el Grupo de Sistemas de Información y Radiocomunicaciones, responde "*que se cuenta con una metodología para la definición y el tratamiento de los riesgos de seguridad de la información adoptada por la entidad. El Procedimiento de administración de riesgos y oportunidades Código: DE_PR_01*

	Vigente desde el 13 de octubre de 2020.Se definen los controles aplicables de acuerdo con los objetivos trazados y conforme al Anexo A de la Norma". Se evidenció la matriz denominada "Seguimiento a Controles de Seguridad de la Información" documento que incluye los controles definidos y aplicables a Parques Nacionales Naturales de Colombia del Anexo A de la Norma Técnica ISO:27001, y contiene la siguiente información diligenciada: Dominio, objetivo del control, control, nivel de cumplimiento- Diagnóstico inicial (madurez- %). Para dar claridad, a esta respuesta, en reunión virtual realizada el 3 de noviembre, con la Coordinadora y los profesionales del Grupo de Sistemas de Información y Radiocomunicaciones, expresaron que a la fecha no disponen de la información, que a través de la hoja metodológica de indicadores no es posible realizar el seguimiento a los controles identificados según Anexo A de la Norma ISO 27001, que se está implementando el sistema de gestión de seguridad de la información, el cual sistematiza la especificación, avance y seguimiento de los controles de seguridad de la información. El Grupo de Control Interno, requirió la siguiente información, para evidenciar las acciones programadas y los seguimientos realizados por el Grupo de Sistemas de Información y Radiocomunicaciones, a la matriz de "Seguimiento a Controles de Seguridad de la Información "y con el objetivo de que estos controles cumplan con los requisitos de la Norma Técnica NTC-ISO/IEC Colombiana 27001:2013: a) Comentarios, recomendación o acción de mejora b) Acción c) Responsable, d) Seguimiento e) Fecha del último seguimiento, f) Nivel de cumplimiento (madurez-%) A lo cual respondió el Grupo Seguridad de Información y Radiocomunicaciones, "*como parte integral del seguimiento a controles y del Modelo de Seguridad y Privacidad de la Información-MSPI- se cuenta actualmente con la Hoja Metodológica de Indicadores, la cual hace seguimiento al modelo integral; así mismo, las evidencias en su mayoría reposan dentro del manual del sistema integrado de gestión y las políticas derivadas de cada control. Adicionalmente, se está implementando el sistema de gestión de seguridad de la información, el cual sistematiza la especificación, avance y seguimiento de los controles de seguridad de la información; esta información soportará la evidencia entregada por medio de la matriz de controles previamente".* Para dar claridad, a esta respuesta, en reunión virtual realizada el 3 de noviembre, con la Coordinadora y los profesionales del Grupo de Sistemas de Información y

	Radiocomunicaciones, expresaron que a la fecha no disponen de la información, que a través de la hoja metodológica de indicadores no es posible realizar seguimiento a los controles identificados en el Anexo A de la Norma ISO 27001; que se está implementando un sistema de control y gestión de la información, el cual sistematiza la especificación, avance y seguimiento de los controles de seguridad de la información. Igualmente, el Grupo de Control Interno, solicitó el acto administrativo mediante el cual se creó el comité de riesgos, actas del comité de riesgos según numeral 2.4 "estructura organizacional del modelo de Seguridad y Privacidad" del Plan de Seguridad y Privacidad de la Información 2019 y las evidencias de la función de informar a la Alta Dirección sobre aspectos relacionados con la gestión de riesgos. En reunión virtual realizada el 3 de noviembre, con la Coordinadora y los profesionales de Grupo de Sistemas de Información y Radiocomunicaciones, se solicitó respuesta por cuanto, no la había obtenido el Grupo de Control Interno, expusieron que el Comité de Riesgos, no se ha constituido, la estructura Organizacional del Modelo del Sistema y Protección de la Información- MSPI, está en proyecto para la siguiente vigencia, sobre lo cual es importante se revise y actualice la documentación del Sistema de Seguridad de la Información. El Grupo de Sistemas de Información y Radiocomunicaciones, respondió que "*Teniendo en cuenta que la declaración de la Política de Seguridad de la Información a través del Manual del Sistema de Gestión Integrado se llevó a cabo durante el último mes, el cronograma se retrasó y aún no se ha llevado a cabo la creación del comité. Este numeral, aún está en proyecto y se llevará a cabo la modificación de fechas para poder cumplir con el compromiso. De igual manera, se proyecta la estructura organizacional del Modelo de Seguridad y Privacidad de la Información, para la siguiente vigencia, en concordancia con la aprobación de la política. Finalmente, en la Revisión por la Dirección de noviembre de 2020, el Grupo de Sistemas de Información y Radiocomunicaciones debe entregar las diapositivas el 9 de noviembre, para aportar la información en esta primera Revisión por la Dirección".*
OBSERVACION / NO CONFORMIDAD: **OBSERVACIÓN No.2** No se evidenciaron las acciones programadas y los seguimientos realizados, contenidos en la matriz de "Seguimiento a Controles de Seguridad de la Información", con el objetivo de que estos controles cumplan con los requisitos de la Norma Técnica NTC-ISO/IEC Colombiana 27001:2013. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI)y del Modelo de Seguridad y Privacidad de la Información.	

5. RECOMENDACIONES

- Incluir en la matriz de partes interesadas el proveedor externo denominado la Agencia Nacional del Espectro, según la caracterización del proceso Gestión de Tecnologías y Seguridad de la Información.

- Incluir en la caracterización del proceso Gestión de Tecnologías y Seguridad de la Información dentro de los requisitos asociados a normas relacionadas con sistemas de gestión, la Norma Técnica NTC-ISO/IEC Colombiana 27001: 2013.Tecnología de la Información.

- Incluir en el control de cambios de la caracterización del proceso Gestión de Tecnologías y Seguridad de la Información, el motivo de la actualización de la Versión No.5 del documento.

- Para la vigencia 2021 aplicar el procedimiento Planificación de Cambios Código: DE_PR_06, el cual tiene como objetivo "Establecer los lineamientos para identificar, analizar, implementar y hacer seguimiento a los cambios, que puedan afectar la integridad del Sistema Integrado de Gestión, de una manera planificada y controlada".

- Revisar y actualizar la información del Sistema de Gestión de Seguridad de la Información.

6. CONCLUSIONES

- Se verificó la Implementación del Sistema de Gestión de Seguridad de la Información, conforme los requisitos de la Norma Técnica NTC-ISO/IEC Colombiana 27001:2013. Tecnología de la Información.

- Se destaca el trabajo realizado por el Grupo de Sistemas de Información y Radiocomunicaciones, en el avance de la Implementación del Sistema de Gestión de Seguridad de la Información.

- Resultado de la auditoría Interna a la Implementación del Sistema de Gestión de Seguridad de la Información se presentaron dos (2) Observaciones al Proceso Gestión de Tecnologías y Seguridad de la Información.

Aprobado por:

GLADYS ESPITIA PEÑA
Coordinadora Grupo de Control Interno

Elaborado por: Yolanda Bernal Jiménez
Martha Inés Fernández Pacheco