



**PARQUES NACIONALES
NATURALES DE COLOMBIA**

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

GRUPO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES 2024



TABLA DE CONTENIDO

1.	3	
1.1.	3	
2.	3	
3.	3	
4.	4	
5.	4	
6.	8	
7.	14	
8.	18	
9.	18	
10.	CONTROL DE CAMBIOS	18



1. OBJETIVOS

1.1. OBJETIVO GENERAL

Definir lineamientos que puedan ser tomados como metodología para la identificación análisis y evaluación los riesgos, así como determinar los roles y responsabilidades de cada uno de los servidores públicos de la entidad frente a su propia gestión.

1.2. OBJETIVOS ESPECÍFICOS

- Determinar aspectos comunes que pueden afectar el desarrollo de las actividades de mitigación de riesgos en Parques Nacionales Naturales de Colombia.
- Suministrar mecanismos y/o metodologías que permita a todas las áreas de Parques Nacionales Naturales de Colombia gestionar de manera efectiva los riesgos generales que afectan la protección de la información de la entidad.
- Ofrecer una herramienta que después de haber identificado, analizado y evaluado los riesgos de seguridad de la información, se puedan identificar roles y responsabilidades frente al tratamiento o mejora de controles de mitigación de riesgos.
- Identificar las acciones de mejora que cada control requiere para su fortalecimiento, teniendo en cuenta los lineamientos definidos para la gestión del riesgo.
- Facilitar el monitoreo y revisión de las responsabilidades y ejecución de las actividades y controles definidos para mitigar el riesgo identificado.

2. ALCANCE

Este plan inicia con la validación y ajuste de los Riesgos de Gestión de Seguridad de la Información en el Mapa de Riesgos y Oportunidades asociado al Procedimiento administración de Riesgos y oportunidades, continúa con la gestión de los controles definidos en el Mapa de Riesgos y finaliza con la evaluación y mejora continua de los mismos.

3. PROYECTOS

El tratamiento de los riesgos de seguridad de la información que se identificaron comprende dos tipos de proyectos, el primero correspondiente a las mejoras de los controles existentes, el segundo a la inclusión de controles definidos por la norma ISO/IEC 27001:2022. Para tal fin, Se requiere:

- Adquirir herramientas tecnológicas que permitan el cifrado de información incluyendo la información contenida en copias de seguridad.
- Una revisión periódica de las vulnerabilidades que pueda tener la red, los sistemas de información de cara al ciudadano y los equipos que se usan para el trabajo cotidiano.
- Sesiones de sensibilización que permitan la óptima apropiación del Sistema de Gestión de Seguridad de la Información SGSI y sus controles, por parte de todos los servidores públicos, contratistas y terceros.
- Una revisión independiente del SGSI, en el marco de una auditoría interna.



PARQUES NACIONALES NATURALES DE COLOMBIA

4. METAS

Dentro de las metas propuestas por la entidad y a medida que se ejecute el plan de tratamiento de riesgos se propone lo siguiente:

- Trabajo conjunto de todas las áreas en la ejecución de las actividades necesarias para la mitigación de riesgos en Parques Nacionales Naturales de Colombia.
- Riesgos de seguridad de la información gestionados de forma efectiva utilizando los mecanismos como la guía del DAFP.
- Roles y responsabilidades definidos en el marco de la gestión de los riesgos de seguridad de la información (digital) identificados.
- Mejoras de controles definidos y valorados como débiles o moderados, con el fin de fortalecerlos.

5. PLAN DE GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

En concordancia con la estrategia de gestión de riesgos de la entidad, la planificación de riesgos de seguridad de la información se debe actualizar cada año, así como la definición e implementación de actividades de control. Por lo anterior, dentro del plan de gestión de riesgos se definen las siguientes fases y actividades:

FASE	ACTIVIDAD A DESARROLLAR PARA EL PLAN	TRIMESTRE 2024			
		I	II	III	IV
Planeación y análisis de riesgos	Llevar a cabo actualización de matriz de riesgos de seguridad digital para la vigencia a evaluar				
Control de los riesgos	Implementación de controles definidos en la matriz de riesgos de seguridad				
Mejora continua	Identificar los aspectos a considerar para la mejora continua del control de riesgos de seguridad de la información que impacten en la actualización de la matriz de riesgos				

6. ACCIONES

Las acciones para mitigar los riesgos se ejecutarán teniendo en cuenta dos aspectos muy importantes:

1. Acciones de mejora de los controles que al ser evaluados su solidez fue diferente a fuertes
2. Nuevos controles que se deben implementar y que apoyan la mitigación de los riesgos.

Listado de controles identificados que, por su valoración en solidez, requieren un plan de mejora o que no existen:



**PARQUES NACIONALES
NATURALES DE COLOMBIA**

CONTROL	PLAN DE MEJORA / ACCIONES
Identificación y valoración de los activos de información	<p>Concienciación de la información que administran y genera cada una de las áreas y procesos de Parques Nacionales Naturales de Colombia.</p> <p>Realizar ejercicios periódicos de actualización e identificación de activos de información.</p> <p>Realizar actualizaciones del inventario de activos de información cada vez que se crea un nuevo formato, documento, o procedimiento, cuando se elimine o se actualice</p>
Aplicación de controles de acceso de acuerdo con perfiles definidos	<p>Generar la documentación de perfiles de acceso para cada una de las áreas de Parques Nacionales Naturales de Colombia.</p> <p>Contar con la disposición de licencias para la asignación de roles y perfiles a todos los servidores públicos y contratistas, sin importar el tiempo de ejecución de contrato para estos últimos.</p> <p>Implementar las directrices de seguridad para el acceso a la información.</p>
Control de uso de puertos USB	<p>Identificación automática en el uso de dispositivo USB no autorizados. Definición de mecanismos tecnológicos y procedimientos de autorización para extraer información.</p> <p>Socialización dentro de la entidad de las restricciones sobre el uso de USB o medios de conexión a través del puerto USB para extraer información</p> <p>Acciones correctivas aplicadas a servidores públicos o contratistas que intenten extraer información sin la debida autorización y a través de medios autorizados.</p> <p>Implementar las directrices de seguridad para el acceso a la información</p>
Definición y socialización de las rutas digitales para el almacenamiento de la información	<p>Socializar a todos los servidores públicos y contratistas, las rutas de almacenamiento.</p> <p>Restringir tecnológicamente la posibilidad de almacenamiento en rutas alternas a las definidas por el Grupo de tecnología.</p>
Ejecución de pruebas de restauración de información y almacenamiento técnico para salvaguardar la información.	<p>Realizar pruebas de restauración junto con el responsable de la información de cada una de las áreas que identifican activos de información valorados alto o muy alto en confidencialidad, integridad o disponibilidad, documentarlas con el fin de contar con pruebas de la efectividad de la ejecución de las pruebas de respaldo.</p> <p>Definir planes de cifrado para las copias de seguridad que contengan información clasificada como de reserva o confidencial, así como aquella que contenga datos sensibles.</p> <p>Aplicar política de seguridad para las copias de respaldo.</p>
Parámetros de seguridad aplicables a la administración de información asignada a funcionarios, contratistas y terceras partes.	<p>Crear acuerdos de confidencialidad y uso de información antes, durante y después de la vinculación laboral.</p> <p>Identificar perfiles de acceso a la información en cada área teniendo en cuenta las obligaciones del servidor público o contratista.</p>



**PARQUES NACIONALES
NATURALES DE COLOMBIA**

CONTROL	PLAN DE MEJORA / ACCIONES
	<p>Firmar acuerdos de transferencia de información entre entidades públicas o privadas, intercambio por convenios con entidades públicas o privadas</p> <p>Contar con la disposición de licencias para la asignación de roles y perfiles a todos los servidores públicos y contratistas, sin importar el tiempo de ejecución de contrato para estos últimos.</p> <p>Implementar las directrices de seguridad para el acceso a la información.</p>
Revisión de calidad documental por el responsable de la información.	Generar procedimientos de verificación del contenido de la información que deberá ser publicada a través de cualquier medio electrónico o físico.
Mantenimientos preventivos	Generar un documento que puede ser anexado a la hoja de vida de los equipos.
Seguimientos y pruebas a los ANS establecidos en las obligaciones contractuales	<p>Generar un plan de seguimiento y pruebas de Acuerdos de Nivel de Servicio, de acuerdo con lo establecido en las obligaciones contractuales.</p> <p>Documentar los resultados de las pruebas y dejar evidencias de estas.</p> <p>Documentar seguimientos de la operación del acuerdo de nivel de servicios, cuando estos han debido realizarse en cumplimiento de lo estipulado en las obligaciones contractuales.</p>

De igual manera, dentro del tratamiento de riesgos se identifican controles que ayudan a optimizar y mejorar el sistema de gestión de seguridad, para tal fin tenemos:

RIESGO	DESCRIPCION	CONTROL	ACCIONES
Pérdida de confidencialidad de la información valorada como de reserva o clasificada, en uno o varios procesos	Acceso no autorizado a la información que sea confidencial o de reserva.	Aplicación de la política de control de Acceso.	<p>Aplicar los controles técnicos necesarios para controlar el acceso a la información clasificada o de reserva.</p> <p>Socializar la Política de control de acceso a todos los servidores y contratistas de la entidad.</p>
		Aplicación de la política para el uso de controles Criptográficos.	<p>Implementar la política de uso de controles criptográficos y gestión de llaves.</p> <p>Capacitar a los usuarios sobre la herramienta utilizada para el cifrado de la información.</p>
		Poner en conocimiento de todos los empleados los procesos disciplinarios.	Mediante charlas informativas socializar el proceso disciplinario y las responsabilidades de cada servidor público frente a la protección de la información clasificada o de reserva.



**PARQUES NACIONALES
NATURALES DE COLOMBIA**

RIESGO	DESCRIPCION	CONTROL	ACCIONES
		Acuerdos de confidencialidad	Firmar acuerdos de confidencialidad entre servidores públicos y la entidad, así como los contratistas y la entidad.
Pérdida de información de uno o varios procesos	Imposibilidad de recuperación de información importante para un proceso o área, que se elimine o dañe.	Aplicación de la política para el uso de controles criptográficos.	Implementar la política de uso de controles criptográficos y gestión de llaves. Capacitar a los usuarios sobre la herramienta utilizada para el cifrado de la información.
		Procedimientos para reporte y atención de incidentes.	Socializar, divulgar y aplicar el procedimiento de atención de incidentes.
		Pruebas de vulnerabilidad periódicas.	Cada Semestre realizar pruebas de vulnerabilidad a los aplicativos, la red, estaciones de trabajo y pruebas de ingeniería social.
		Socializar y sensibilizar en temas de protección de la Información y las directrices de seguridad de la información.	Realizar un sondeo al año frente a temas de seguridad y protección de la información Encuestas de seguimiento a la apropiación de los conceptos y temas tratados sobre protección y seguridad de la información.
		Etiquetado y manejo de información acorde a niveles de clasificación.	De acuerdo con el inventario de activos de información de cada área aplicar el procedimiento etiquetado la información.
		Aplicar la política y el procedimiento de gestión de usuarios.	Eliminar, modificar o adicionar permisos de acuerdo con la terminación o cambio de responsabilidades de empleo.
Pérdida de integridad de la información importante para uno o varios procesos	La veracidad de la información contenida en el activo de información se encuentra comprometida.	Etiquetado y manejo de información acorde a niveles de clasificación.	De acuerdo con el inventario de activos de información de cada área aplicar el procedimiento etiquetado la información.
		Aplicar la política y el procedimiento de gestión de usuarios.	Eliminar, modificar o adicionar permisos de acuerdo con la terminación o cambio de responsabilidades de empleo.
		Procedimientos para reporte y atención de incidentes.	Socializar, divulgar y aplicar el procedimiento de atención de incidentes.
		Socializar y sensibilizar en temas de protección de la Información y las directrices de	Realizar un sondeo al año frente a temas de seguridad y protección de la información. Encuestas de seguimiento a la apropiación de los conceptos y



**PARQUES NACIONALES
NATURALES DE COLOMBIA**

RIESGO	DESCRIPCION	CONTROL	ACCIONES
		seguridad de la información.	temas tratados sobre protección y seguridad de la información.
Indisponibilidad de la información contenida en los sistemas de información	El sistema de información presenta fallas asociadas al funcionamiento o comunicación con él	Procedimientos para reporte y atención de incidentes.	Socializar, divulgar y aplicar el procedimiento de atención de incidentes.
		Pruebas de vulnerabilidad periódicas.	Ejecución de pruebas de vulnerabilidad a los sistemas de información al menos una vez cada semestre.

Nota: Es importante aclarar que los riesgos identificados aplican para todas las áreas y procesos por ende la ejecución de los controles dependerá de manera conjunta entre los responsables mencionados y los jefes de todas las áreas con su equipo de trabajo. En especial se aplica para todas las áreas que han identificado activos de información en un nivel alto o muy alto de confidencialidad, integridad o disponibilidad.

7. PRODUCTOS

Dentro de los productos que se deben generar en el transcurso de la aplicación del plan de tratamiento de riesgos de seguridad de la información se encuentran:

- Mejoras definidas para los controles que su nivel de solidez fue diferente a fuerte, con su respectiva evidencia que a continuación se listan.
- Controles nuevos diseñados, generando las actividades previstas y con las evidencias o productos que a continuación se listan.

Productos esperados de las acciones de mejora de los controles que su nivel de madurez fue débil o moderado:

CONTROL	PLAN MEJORA	RESPONSABLES	EVIDENCIA
Identificación y valoración de los activos de información	<p>Concienciación de la información que administran y genera cada una de las áreas y procesos de la Entidad.</p> <p>Realizar ejercicios periódicos de actualización e identificación de activos de información.</p> <p>Realizar actualizaciones del inventario de activos de información cada vez que se crea un nuevo formato, documento, o procedimientos, cuando se elimine o se actualice.</p>	Responsables de áreas y procesos de la entidad	Inventario de Activos de Información debidamente diligenciado y con las valoraciones correspondientes por parte de todas las áreas de la entidad.



**PARQUES NACIONALES
NATURALES DE COLOMBIA**

CONTROL	PLAN MEJORA	RESPONSABLES	EVIDENCIA
Aplicación de controles de acceso de acuerdo con perfiles definidos	<p>Generar la documentación de perfiles de acceso para cada una de las áreas de la entidad.</p> <p>Contar con la disposición de licencias para la asignación de roles y perfiles a todos los servidores públicos y contratistas, sin importar el tiempo de ejecución de contrato para estos últimos</p> <p>Implementar las directrices de seguridad para el acceso a la información.</p>	Responsables de áreas y procesos de la entidad	<p>Perfiles definidos por área</p> <p>Protocolo de configuraciones de acceso a la información implementado para todos los servidores públicos y contratistas</p>
Control de uso de Puertos USB	<p>Identificación automática en el uso de dispositivo USB no autorizados.</p> <p>Definición de mecanismos tecnológicos y procedimientos de autorización para extraer información.</p> <p>Socialización dentro de la entidad de las restricciones sobre el uso de USB o medios de conexión a través del puerto USB para extraer información.</p> <p>Acciones correctivas aplicadas a servidores públicos o contratistas que intenten extraer información sin la debida autorización y a través de medios autorizados.</p> <p>Implementar las directrices de seguridad para el acceso a la Información.</p>	<p>Grupo Tecnologías de la Información y las Comunicaciones</p> <p>Jefes de áreas</p> <p>Todos los servidores públicos y contratistas</p> <p>Persona asignada con las responsabilidades de Seguridad de la Información</p>	<p>USB bloqueadas y alertas configuradas por intentos de descarga, debidamente documentadas y socializadas con las áreas y procesos</p> <p>Política de control de Acceso</p> <p>Socialización de implicaciones disciplinarias o jurídicas frente al uso de información privilegiada sin el debido proceso y autorización</p>
Definición y socialización de las rutas digitales para el almacenamiento de la información	<p>Socializar a todos los servidores públicos y contratistas, las rutas de almacenamiento.</p> <p>Restringir tecnológicamente la posibilidad de almacenamiento en rutas</p>	<p>Grupo Tecnologías de la Información y las Comunicaciones</p> <p>Jefes de áreas</p> <p>Todos los servidores públicos y contratistas</p>	Información de la entidad almacenada en los repositorios definidos



**PARQUES NACIONALES
NATURALES DE COLOMBIA**

CONTROL	PLAN MEJORA	RESPONSABLES	EVIDENCIA
	alternas a las definidas por la oficina de tecnología.		
Identificación y valoración de los activos de información	<p>Concienciación de la información que administran y genera cada una de las áreas y procesos de la Entidad.</p> <p>Realizar ejercicios periódicos de actualización e identificación de activos de información Realizar actualizaciones del inventario de activos de información cada vez que se crea un nuevo formato, documento, o procedimientos, cuando se elimine o se actualice</p>	Responsables de áreas y procesos de la Entidad	Inventario de Activos de Información debidamente diligenciado y con las valoraciones correspondientes por parte de todas las áreas de la Entidad
Ejecución de pruebas de restauración de información y almacenamiento técnico para salvaguardar la información.	<p>Realizar pruebas de restauración junto con el responsable de la información de cada una de las áreas que identifican activos de información valorados alto o muy alto en confidencialidad, integridad o disponibilidad, documentarlas con el fin de contar con pruebas de la efectividad de la ejecución de las pruebas de respaldo. Definir planes de cifrado para las copias de seguridad que contengan información clasificada como de reserva o confidencial, así como aquella que contenga datos sensibles. Aplicar política de seguridad para las copias de respaldo</p>	<p>Grupo Tecnologías de la Información y las Comunicaciones</p> <p>Responsables de información (jefes de área, servidores públicos y contratistas)</p>	<p>Pruebas de restauración Debidamente documentadas y realizadas con los propietarios de la información</p> <p>Plan de copias de seguridad donde se incluya al menos una prueba de restauración con cada área en el año.</p>
Parámetros de seguridad	Crear acuerdos de confidencialidad y uso	Grupo de Contratos	Acuerdos de confidencialidad



**PARQUES NACIONALES
NATURALES DE COLOMBIA**

CONTROL	PLAN MEJORA	RESPONSABLES	EVIDENCIA
<p>aplicables a la administración de información asignada a funcionarios, contratistas y terceras partes.</p>	<p>de información antes, durante y después de la vinculación laboral.</p> <p>Identificar perfiles de acceso a la información en cada área teniendo en cuenta las obligaciones del servidor público o contratista.</p> <p>Firmar acuerdos de transferencia de información entre entidades públicas o privadas, intercambio por convenios con entidades públicas o privadas</p> <p>Contar con la disposición de licencias para la asignación de roles y perfiles a todos los servidores públicos y contratistas, sin importar el tiempo de ejecución de contrato para estos últimos</p> <p>Implementar las directrices de seguridad para el acceso a la información</p>	<p>Talento Humano</p> <p>Grupo Tecnologías de la Información y las Comunicaciones</p>	<p>debidamente firmados</p> <p>Acuerdos de transferencia de información debidamente firmados</p> <p>Usuarios activos conforme a planta y contratistas en funcionamiento</p>
<p>Revisión de calidad documental por el responsable de la información.</p>	<p>Generar procedimientos de verificación del contenido de la información que deberá ser publicada a través de cualquier medio electrónico o físico</p>	<p>Responsables de área que deben publicar, transferir o compartir información.</p>	<p>Modificaciones en el proceso de publicación, donde se evidencie la revisión de calidad</p> <p>Seguimientos documentados por parte de control de cambios en la documentación.</p>
<p>Mantenimientos preventivos</p>	<p>Generar un documento que puede ser anexado a la hoja</p>	<p>Grupo Tecnologías de la Información y las Comunicaciones</p>	<p>Información documentada de los mantenimientos</p>



**PARQUES NACIONALES
NATURALES DE COLOMBIA**

CONTROL	PLAN MEJORA	RESPONSABLES	EVIDENCIA
	de vida de los equipos		realizados en el año, por cada equipo.
Seguimientos y pruebas a los ANS establecidos en las obligaciones contractuales	<p>Generar un plan de seguimiento y pruebas de Acuerdos de Nivel de Servicio, de acuerdo con lo establecido en las obligaciones contractuales</p> <p>Documentar los resultados de las pruebas y dejar evidencias de estas.</p> <p>Documentar seguimientos de la operación del acuerdo de nivel de servicios, cuando estos han debido realizarse en cumplimiento de lo estipulado en las obligaciones contractuales</p>	Grupo Tecnologías de la Información y las Comunicaciones	<p>Plan de seguimientos y pruebas a proveedores de servicios esenciales en tecnología</p> <p>Documentación de las pruebas realizadas a la prestación por parte de terceros de servicios esenciales en Tecnología</p>

Productos esperados para los controles definidos como acciones de mejora o nuevos:

CONTROL	ACCIONES	EVIDENCIA
Aplicación de la política de control de Acceso	<p>Aplicar los controles técnicos necesarios para controlar el acceso a la información clasificada o de reserva</p> <p>Socializar la Política de control de acceso a todos los servidores y contratistas de la entidad.</p>	<p>Política de Control de Acceso</p> <p>Controles aplicados</p> <p>Listados de asistencia</p> <p>Piezas de divulgación</p>
Aplicación de la política para el uso de controles criptográficos	<p>Implementar la política de uso de controles criptográficos y gestión de llaves</p> <p>Capacitar a los usuarios sobre la herramienta utilizada para el cifrado de la información</p>	<p>Política para el uso de controles criptográficos</p> <p>Aplicativo configurado</p> <p>Listados de asistencia</p> <p>Piezas de divulgación</p>
Poner en conocimiento de todos los empleados los procesos disciplinarios	Mediante charlas informativas socializar el proceso disciplinario y las responsabilidades de cada servidor público frente a la	<p>Listados de asistencia</p> <p>Piezas de divulgación</p>



**PARQUES NACIONALES
NATURALES DE COLOMBIA**

CONTROL	ACCIONES	EVIDENCIA
	protección de la información clasificada o de reserva.	
Acuerdos de confidencialidad	Firmar acuerdos de confidencialidad entre servidores públicos y la entidad, así como los contratistas la entidad	Acuerdos firmados por todos los servidores públicos y contratistas o proveedores
Aplicación de la política para el uso de controles criptográficos	Implementar la política de uso de controles criptográficos y gestión de llaves Capacitar a los usuarios sobre la herramienta utilizada para el cifrado de la información	Política para el uso de controles criptográficos Aplicativo configurado Listados de asistencia Piezas de divulgación
Procedimiento para reporte y atención de incidentes	Socializar, divulgar y aplicar el procedimiento de atención de incidentes	Procedimiento para reporte y atención de incidentes Aplicativo configurado Listados de asistencia Piezas de divulgación Incidentes documentados
Pruebas de vulnerabilidad periódicas	Cada semestre realizar pruebas de vulnerabilidad a los aplicativos, la red, estaciones de trabajo y pruebas de ingeniería social	Pruebas planificadas ejecutadas y documentadas Planes de remediación y ejecución de estos
Socializar y sensibilizar en temas de protección de la Información y las directrices de seguridad de la información	Realizar un sondeo al año frente a temas de seguridad y protección de la información Encuestas de seguimiento a la apropiación de los conceptos y temas tratados sobre protección y seguridad de la información	Plan de sensibilización en temas de seguridad de la información Listados de asistencia Piezas de divulgación Encuestas de sondeo y seguimiento diligenciadas y documentadas
Etiquetado y manejo de Información acorde a niveles de clasificación	De acuerdo con el inventario de activos de información de cada área aplicar el procedimiento etiquetado la información	Procedimiento de etiquetado socializado Documentos con marca de agua, de forma impresa o digital Archivadores y carpetas etiquetados
Aplicar la política y el procedimiento de gestión de usuarios	Eliminar, modificar o adicionar permisos de acuerdo con la terminación o cambio de responsabilidades de empleo	Política de gestión de usuarios Procedimiento de gestión de usuarios



**PARQUES NACIONALES
NATURALES DE COLOMBIA**

CONTROL	ACCIONES	EVIDENCIA
		Usuarios actualizados en el directorio activo

8. CRONOGRAMA

De acuerdo con las actividades definidas se presenta el cronograma para la vigencia al 2024.

CONTROL	PLAN MEJORA	RESPONSABLE	CRONOGRAMA	
			INICIO	FIN
Identificación y valoración de los activos de información	<p>Concienciación de la información que administran y genera cada una de las áreas y procesos de la entidad</p> <p>Realizar ejercicios periódicos de actualización e identificación de activos de información</p> <p>Realizar actualizaciones del inventario de activos de información cada vez que se crea un nuevo formato, documento, o procedimientos, cuando se elimine o se actualice</p>	Responsables de Áreas y procesos de la entidad	01/02/2024	30/04/2024
Aplicación de controles de acceso de acuerdo con perfiles definidos	<p>Generar la documentación de perfiles de acceso para cada una de las áreas de la entidad</p> <p>Contar con la disposición de licencias para la asignación de roles y perfiles a todos los servidores públicos y contratistas, sin importar el tiempo de ejecución de contrato para estos últimos</p> <p>Implementar las directrices de seguridad para el acceso a la información</p>	Responsables de Áreas y procesos de la entidad	01/02/2024	30/12/2024
Control de uso de puertos USB	<p>Identificación automática en el uso de dispositivo USB no autorizados.</p> <p>Definición de mecanismos tecnológicos y procedimientos de autorización para extraer información</p> <p>Socialización dentro de la entidad de las restricciones sobre el uso de USB o medios de conexión a través del puerto USB para extraer información</p>	<p>Grupo de Tecnologías de la Información y las Comunicaciones</p> <p>jefes de áreas</p> <p>Todos los servidores públicos y contratistas</p> <p>Persona asignada</p>	01/05/2024	30/12/2024



**PARQUES NACIONALES
NATURALES DE COLOMBIA**

CONTROL	PLAN MEJORA	RESPONSABLE	CRONOGRAMA	
			INICIO	FIN
	<p>acciones correctivas aplicadas a servidores públicos o contratistas que intenten extraer información sin la debida autorización y a través de medios autorizados.</p> <p>Implementar las directrices de seguridad para el acceso a la Información</p>	<p>con las responsabilidades de Seguridad de la Información</p>		
Definición y socialización de las rutas digitales para el almacenamiento de la información	<p>Socializar a todos los servidores públicos y contratistas, las rutas de almacenamiento.</p> <p>Restringir tecnológicamente la posibilidad de almacenamiento en rutas alternas a las definidas por el Grupo de tecnologías de la Información y las Comunicaciones</p>	<p>Grupo de Tecnologías de la Información y las Comunicaciones</p> <p>jefes de áreas</p> <p>Todos los servidores públicos y contratistas</p>	01/03/2024	30/04/2024
Identificación y valoración de los activos de información	<p>Concienciación de la información que administran y genera cada una de las áreas y procesos de la Entidad</p> <p>Realizar ejercicios periódicos de actualización e identificación de activos de información</p> <p>Realizar actualizaciones del inventario de activos de información cada vez que se crea un nuevo formato, documento, o procedimientos, cuando se elimine o se actualice</p>	<p>Responsables de Áreas y procesos de la entidad</p>	01/02/2024	30/11/2024
Ejecución de pruebas de restauración de información y almacenamiento técnico para salvaguardar la información.	<p>Realizar pruebas de restauración junto con el responsable de la información de cada una de las áreas que identifican activos de información valorados alto o muy alto en confidencialidad, integridad o disponibilidad, documentarlas con el fin de contar con pruebas de la efectividad de la ejecución de las pruebas de respaldo.</p> <p>Definir planes de cifrado para las copias de seguridad que contengan</p>	<p>Grupo de Tecnologías de la Información y las Comunicaciones</p> <p>Responsables de información (jefes de área, servidores públicos y contratistas)</p>	01/03/2024	30/12/2024



**PARQUES NACIONALES
NATURALES DE COLOMBIA**

CONTROL	PLAN MEJORA	RESPONSABLE	CRONOGRAMA	
			INICIO	FIN
	<p>información clasificada como de reserva o confidencial, así como aquella que contenga datos sensibles.</p> <p>Aplicar política de seguridad para las copias de respaldo</p>			
<p>Parámetros de seguridad aplicables a la administración de información asignada a funcionarios, contratistas y terceras partes.</p>	<p>Crear acuerdos de confidencialidad y uso de información antes, durante y después de la vinculación laboral.</p> <p>Identificar perfiles de acceso a la información en cada área teniendo en cuenta las obligaciones del servidor público o contratista.</p> <p>Firmar acuerdos de transferencia de información entre entidades públicas o privadas, intercambio por convenios con entidades públicas o privadas</p> <p>Contar con la disposición de licencias para la asignación de roles y perfiles a todos los servidores públicos y contratistas, sin importar el tiempo de ejecución de contrato para estos últimos</p>	<p>Contractual</p> <p>Talento Humano</p> <p>Grupo de Tecnologías de la Información y las Comunicaciones</p>	01/02/2024	30/03/2024
<p>Revisión de calidad documental por el responsable de la información</p>	<p>Generar procedimientos de verificación del contenido de la información que deberá ser publicada a través de cualquier medio electrónico o físico</p>	<p>Responsables de área que deben publicar, transferir o compartir información</p>	01/03/2024	30/12/2024
<p>Mantenimientos preventivos</p>	<p>Generar un documento que puede ser anexado a la hoja de vida de los equipos</p>	<p>Grupo de Tecnologías de la Información y las Comunicaciones</p>	01/02/2024	30/04/2024
<p>Seguimientos y pruebas a los ANS establecidos en las obligaciones contractuales</p>	<p>Generar un plan de seguimiento y pruebas de Acuerdos de Nivel de Servicio, de acuerdo con lo establecido en las obligaciones contractuales</p> <p>Documentar los resultados de las pruebas y dejar evidencias de estas.</p> <p>Documentar seguimientos</p>	<p>Grupo de Tecnologías de la Información y las Comunicaciones</p>	01/03/2024	30/12/2024



PARQUES NACIONALES NATURALES DE COLOMBIA

CONTROL	PLAN MEJORA	RESPONSABLE	CRONOGRAMA	
			INICIO	FIN
	de la operación del acuerdo de nivel de servicios, cuando estos han debido realizarse en cumplimiento de lo estipulado en las obligaciones contractuales			



9. PLAN DE COMPRAS

Dentro de los planes de adquisiciones se encuentran los siguientes temas:

- Plan de adquisiciones para copias de seguridad

Plan de Compras	Control	Entregable	Costo
Plan de adquisiciones para copias de seguridad	Ejecución de pruebas de restauración de información y almacenamiento técnico para salvaguardar la información	Documentación de seguimiento sobre pruebas restauración de las copias de seguridad realizadas	\$300.000.000

10. MAPA DE RIESGOS

Descripción del Riesgo: Incumplimiento de las acciones de implementación para los controles descritas en el plan de tratamiento de riesgos de seguridad de la información

Causas:

- Mecanismos insuficientes en la socialización de los controles a los propietarios de la información
- Demoras en la aplicación de los controles por parte de los custodios, responsables y propietarios de la información
- Demoras en los tiempos de contratación
- Falta de personal responsable de hacer seguimiento al plan de tratamiento de riesgos de seguridad de la información

Consecuencias:

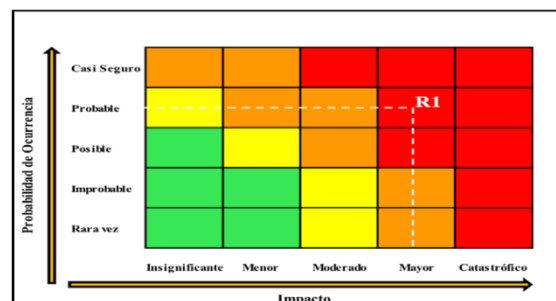
- Posible materialización de riesgos de seguridad de la información
- Atraso en la ejecución de actividades e implementación de controles que prevengan la materialización de los riesgos de seguridad de la información
- Afectación de la imagen institucional
- Incumplimientos que ocasionen sanciones legales o penales.

Tipo de riesgo: Estratégico

Probabilidad de ocurrencia: Probable

Impacto: Moderado

Zona de riesgo: Alta



Fuente: Adaptado de Instituto de Auditores Internos. COSO ERM. 2017.



11. CONTROL DE CAMBIOS

FECHA DE VIGENCIA VERSIÓN ANTERIOR	VERSIÓN ANTERIOR	MOTIVO DE LA ACTUALIZACIÓN

CRÉDITOS		
Elaboró	Nombre	Fernando Bolívar Buitrago
	Cargo	Profesional TI Contratista
	Fecha	07/12/2023
Revisó	Nombre	Carlos Arturo Sáenz Barón
	Cargo	Coordinador Grupo Tecnologías de la Información y las Comunicaciones
	Fecha:	19/12/2023
Aprobó	Nombre	Carlos Arturo Sáenz Barón
	Cargo	Coordinador Grupo Tecnologías de la Información y las Comunicaciones
	Fecha:	19/12/2023