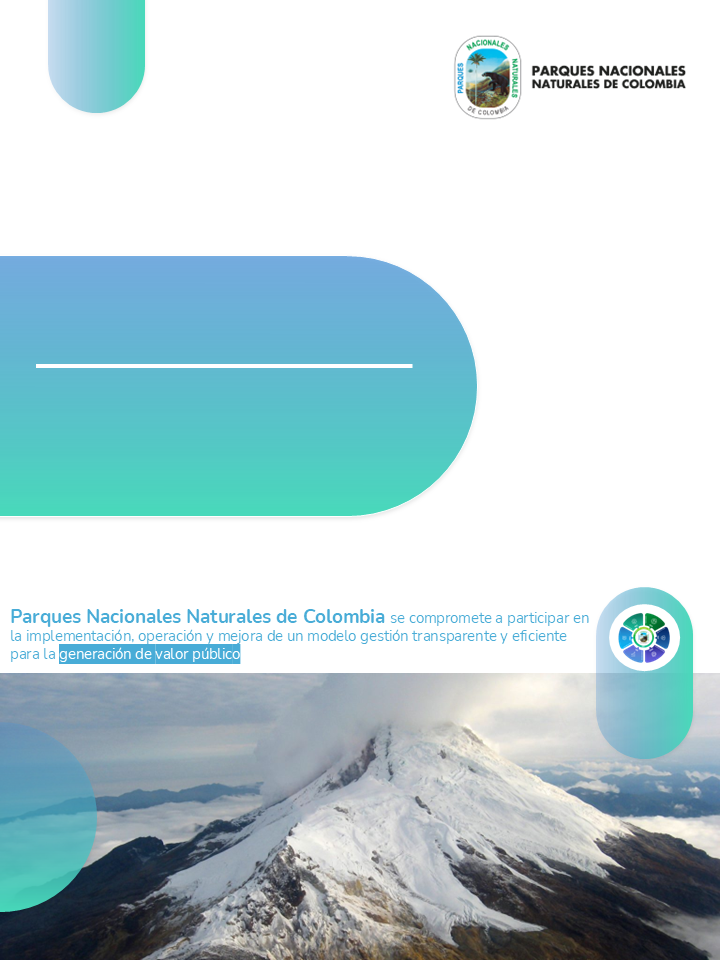


**Política Integral**

**Para la Administración del Riesgo.**

**Versión 1 Fecha 06/05/2025**

**CONTENIDO**

[DECLARACIÓN DE LA POLÍTICA 5](#_Toc198129383)

[1 INTRODUCCIÓN 5](#_Toc198129384)

[2 OBJETIVO 5](#_Toc198129385)

[3 ALCANCE 5](#_Toc198129386)

[4 DEFINICIONES, ABREVIATURAS O SIGLAS 6](#_Toc198129387)

[5 MARCO LEGAL Y TÉCNICO 7](#_Toc198129388)

[6 ROLES Y RESPONSABILIDADES 7](#_Toc198129389)

[7 COMPROMISOS DE LA ALTA DIRECCIÓN 12](#_Toc198129390)

[8 METODOLOGÍA PARA LA GESTIÓN DEL RIESGO 12](#_Toc198129391)

[8.1 Identificación del contexto 13](#_Toc198129392)

[8.1.1 Análisis de objetivos 13](#_Toc198129393)

[8.1.2 Establecimiento del Contexto 13](#_Toc198129394)

[8.2 Identificación de Puntos de Riesgo 13](#_Toc198129395)

[8.3 Identificación de Áreas de Impacto 14](#_Toc198129396)

[8.4 Identificación de Factores de Riesgo 14](#_Toc198129397)

[8.5 Identificación de Riesgos 15](#_Toc198129398)

[8.5.1 Técnicas para la Identificación de Riesgos 15](#_Toc198129399)

[8.6 RIESGOS DE GESTIÓN 16](#_Toc198129400)

[8.6.1 Descripción del riesgo 16](#_Toc198129401)

[8.6.2 Clasificación del riesgo 18](#_Toc198129402)

[8.6.3 Valoración del riesgo 19](#_Toc198129403)

[8.6.4 Evaluación del riesgo 21](#_Toc198129404)

[8.6.5 Valoración de controles 22](#_Toc198129405)

[8.6.5.1 Tipologías y atributos para el diseño de los controles 23](#_Toc198129406)

[8.6.6 Determinación riesgo residual 25](#_Toc198129407)

[8.7 RIESGO DE CORRUPCIÓN 26](#_Toc198129408)

[8.7.1 Descripción del riesgo 26](#_Toc198129409)

[8.7.2 Valoración del riesgo de corrupción 27](#_Toc198129410)

[8.7.3 Evaluación del Riesgo de Corrupción 29](#_Toc198129411)

[8.7.4 Valoración de Controles 29](#_Toc198129412)

[8.7.5 Determinación del riesgo residual 29](#_Toc198129413)

[8.8 RIESGO FISCAL 29](#_Toc198129414)

[8.8.1 Identificación del riesgo 29](#_Toc198129415)

[8.8.2 Descripción del riesgo 31](#_Toc198129416)

[8.8.3 Valoración del Riesgo Fiscal 33](#_Toc198129417)

[8.8.4 Valoración de controles 33](#_Toc198129418)

[8.8.5 Determinación del riesgo residual 34](#_Toc198129419)

[8.9 RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 34](#_Toc198129420)

[8.9.1 Identificación de los activos de seguridad de la información 34](#_Toc198129421)

[8.9.2 Identificación del riesgo de seguridad de la información 34](#_Toc198129422)

[8.9.3 Evaluación del Riesgo de Seguridad de la Información 36](#_Toc198129423)

[8.9.4 Controles para la Seguridad de la Información 36](#_Toc198129424)

[8.10 TRATAMIENTO DEL RIESGO 36](#_Toc198129425)

[8.10.1 Plan de reducción del riesgo 38](#_Toc198129426)

[9. MONITOREO Y SEGUIMIENTO DE RIESGOS 38](#_Toc198129427)

[9.1 Consideraciones generales para el Monitoreo de Riesgos 38](#_Toc198129428)

[9.2 Acciones para seguir en caso de Materialización del Riesgo 39](#_Toc198129429)

[9.3 Periodicidad del monitoreo y seguimiento al mapa de riesgos 42](#_Toc198129430)

[10 REVISIÓN Y ACTUALIZACIÓN DE LOS MAPAS DE RIESGOS 43](#_Toc198129431)

[11 COMUNICACIÓN Y CONSULTA 43](#_Toc198129432)

[12 CONTROL DE CAMBIOS 44](#_Toc198129433)

**TABLA DE TABLAS**

[Tabla 1 Responsabilidades en la gestión del riesgo 7](#_Toc198129434)

[Tabla 2 Análisis de Objetivos 13](#_Toc198129435)

[Tabla 3 Factores de Riesgo 14](#_Toc198129436)

[Tabla 4 Identificación del riesgo 15](#_Toc198129437)

[Tabla 5 Ejemplo 17](#_Toc198129438)

[Tabla 6 Clasificación de riesgos 18](#_Toc198129439)

[Tabla 7 Criterios para definir el nivel de probabilidad 20](#_Toc198129440)

[Tabla 8 Criterios para definir el nivel de impacto 20](#_Toc198129441)

[Tabla 9 Atributos para el diseño del Control 24](#_Toc198129442)

[Tabla 10 Ejemplo de aplicación de controles para determinar el riesgo residual 25](#_Toc198129443)

[Tabla 11 Posibles amenazas y vulnerabilidades 35](#_Toc198129444)

[Tabla 12 Ruta de acción en caso de materialización para riesgos de gestión 40](#_Toc198129445)

[Tabla 13 Actividades Materialización del Riesgo de Corrupción y Fiscales 40](#_Toc198129446)

[Tabla 14 Actividades Materialización del Riesgo de Seguridad de la información 41](#_Toc198129447)

[Tabla 15 Monitoreo y Seguimiento Líneas de Defensa 42](#_Toc198129448)

**TABLA DE ILUSTRACIONES**

[Ilustración 1 Estructura propuesta para la redacción del riesgo 16](#_Toc198129449)

[Ilustración 2 Relación entre los factores de riesgo y su clasificación 19](#_Toc198129450)

[Ilustración 3 Matriz de calor (niveles de severidad del riesgo) 21](#_Toc198129451)

[Ilustración 4 Matriz de calor (Zona de riesgo Alta) 22](#_Toc198129452)

[Ilustración 5 Movimiento en la matriz de calor acorde con el tipo de control 25](#_Toc198129453)

[Ilustración 6 Estructura propuesta para la redacción del riesgo 26](#_Toc198129454)

[Ilustración 7 Criterios para calificar la probabilidad 27](#_Toc198129455)

[Ilustración 8 Criterios para calificar el impacto en riesgos de corrupción 27](#_Toc198129456)

[Ilustración 9 Matriz de calor (niveles de severidad del riesgo) 29](#_Toc198129457)

[Ilustración 10 Preguntas orientadoras para puntos riesgo fiscal y causas inmediatas 30](#_Toc198129458)

[Ilustración 11 Estructura propuesta para la redacción del riesgo 31](#_Toc198129459)

[Ilustración 12 Ejemplos adicionales acorde con el objeto sobre el que recae el efecto dañoso 32](#_Toc198129460)

[Ilustración 13 Matriz de calor (niveles de severidad del riesgo) 33](#_Toc198129461)

[Ilustración 14 Estrategias para combatir el riesgo 36](#_Toc198129462)

# DECLARACIÓN DE LA POLÍTICA

Parques Nacionales Naturales de Colombia, en cumplimiento de su misión de conservación y gestión del patrimonio natural, reafirma su compromiso con los grupos de valor e interés. Reconocemos la importancia de identificar y gestionar los riesgos que pueden afectar nuestro enfoque estratégico, la calidad de nuestros servicios y el logro de los objetivos de nuestros procesos y proyectos.

Conscientes de nuestra responsabilidad, hemos implementado un conjunto de medidas de control que buscan prevenir la materialización de riesgos, mitigar sus posibles impactos y aprovechar las oportunidades que surgen de las evaluaciones realizadas por entidades de control, tanto internas como externas. Este enfoque está alineado con los requisitos normativos, legales e institucionales vigentes, garantizando que nuestras acciones sean transparentes y responsables.

La Política Integral para la Administración del Riesgo ha sido aprobada por el Comité Institucional de Control Interno en la sesión celebrada el [fecha de la sesión]. A través de esta política, buscamos fortalecer nuestra gestión y asegurar la protección efectiva de la riqueza natural de Colombia.

# INTRODUCCIÓN

Parques Nacionales Naturales de Colombia (PNNC) tiene la misión de conservar y administrar las áreas protegidas del país, garantizando su sostenibilidad y biodiversidad. La implementación de una política de gestión del riesgo permite anticipar, mitigar y responder a eventos que puedan afectar el cumplimiento de sus objetivos estratégicos. Esta política se fundamenta en los lineamientos establecidos en la "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas" del DAFP (versión 6, 2022) y en el Modelo Integrado de Planeación y Gestión (MIPG).

# OBJETIVO

El presente documento declara el compromiso de PNNC con sus grupos de valor y de interés al establecer los lineamientos, criterios y metodología para la administración del riesgo, en todos sus procesos y niveles de gestión, atendiendo los lineamientos normativos aplicables, que orienten la toma de decisiones y minimicen los posibles efectos adversos.

# ALCANCE

Esta política es aplicable a todos los procesos en los diferentes niveles de PNNC, desde a la Dirección General, la Dirección Territorial y el Área Protegida y Unidades de Decisión, abarcando todos los procesos y las actividades tercerizadas que puedan impactar la misión de la entidad. Además, esta política se integra de manera efectiva con el Sistema Integrado de Gestión (SIGI), asegurando una alineación coherente en nuestras operaciones.

# DEFINICIONES, ABREVIATURAS O SIGLAS

Las siguientes definiciones son tomadas o adaptadas de la “Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6”

* **Apetito de riesgo:** Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.
* **Bien Público:** Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares).
* **Causa:** Elementos internos o externos que, de manera individual o combinada, pueden contribuir a la materialización de un riesgo.
* **Causa inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo. Nota: Tratándose de riesgo fiscal, se usa el término circunstancia inmediata (Causa Inmediata, pero se asocia a la misma causa inmediata.
* **Causa Raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
* **Control:** Acción o mecanismo implementado para reducir la probabilidad o el impacto de un riesgo identificado, asegurando el cumplimiento de los objetivos institucionales.
* **Patrimonio público:** se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C340-07).
* **Probabilidad:** Nivel de posibilidad de que ocurra un evento riesgoso, determinado en función de la frecuencia con que se presentan situaciones similares dentro de un período de tiempo definido.
* **Riesgo:** Posibilidad de que un evento afecte el logro de los objetivos institucionales, derivado de fallas, deficiencias o inadecuaciones en el talento humano, los procesos, la tecnología, la infraestructura o debido a factores externos imprevistos.
* **Riesgo de Corrupción:** Posibilidad de que el poder sea utilizado, ya sea por acción u omisión, para desviar la administración de los recursos públicos en beneficio de intereses particulares.
* **Riesgo de Gestión:** Probabilidad de que deficiencias en la planificación, ejecución o supervisión de procesos impidan el cumplimiento de los objetivos estratégicos de la entidad, afectando la eficiencia, eficacia y transparencia institucional.
* **Riesgo de Seguridad de la Información:** Probabilidad de que una amenaza aproveche una vulnerabilidad en los sistemas de información, generando daño, pérdida o exposición indebida de datos, lo que puede impactar la confidencialidad, integridad y disponibilidad de la información.
* **Riesgo Fiscal:** Impacto negativo en los recursos financieros y patrimoniales de la entidad debido a eventos que afectan la correcta administración, ejecución o control del gasto público.
* **Riesgo inherente:** Nivel de riesgo que existe antes de la aplicación de controles, determinado por la combinación de la probabilidad y el impacto potencial del evento en cuestión.
* **Riesgo residual:** Nivel de riesgo que permanece después de la implementación de controles y estrategias de mitigación, reflejando la efectividad de las medidas adoptadas.
* **Tolerancia del riesgo:** Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

# MARCO LEGAL Y TÉCNICO

* **Ley 99 de 1993 (Medio Ambiente):** Establece el marco normativo para la protección del medio ambiente en Colombia, creando el Ministerio del Medio Ambiente y promoviendo el desarrollo sostenible y la participación comunitaria.
* **Decreto 2372 de 2010 (Reglamentación de Áreas Protegidas):** Regula la creación y manejo de áreas protegidas en Colombia, estableciendo criterios para su conservación y uso sostenible, con el fin de proteger la biodiversidad
* **Ley 1474 de 2011 (Estatuto Anticorrupción):** Previene y sanciona la corrupción en el sector público, promoviendo la transparencia, la rendición de cuentas y la participación ciudadana en la vigilancia de la gestión pública.
* **Modelo Integrado de Planeación y Gestión MIPG:** El MIPG es un enfoque que busca integrar la planeación, la gestión y el control en las entidades públicas de Colombia. Promueve la alineación de los objetivos institucionales con las políticas públicas, facilitando la toma de decisiones y la rendición de cuentas, y asegurando una gestión eficiente y efectiva de los recursos.
* **Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas del DAFP, versión 6 (2022):** Proporciona un marco para la identificación y gestión de riesgos en entidades públicas, ofreciendo herramientas para el diseño de controles internos que aseguren la integridad en la gestión pública.

# ROLES Y RESPONSABILIDADES

Tabla 1 Responsabilidades en la gestión del riesgo

|  |  |  |  |
| --- | --- | --- | --- |
| **Línea de Defensa** | **Descripción** | **Responsable** | **Responsabilidades frente a la Gestión integral del Riesgo** |
| **Línea estratégica** | Define el marco general para la gestión del riesgo y oportunidades, alineándose con la estrategia de PNNC. Supervisa la gestión del riesgo institucional. | * Comité Institucional de Coordinación de Control Interno. * Comité Institucional de Gestión y Desempeño. | **1. Planificar**  **\***Determinar los lineamientos para la administración de los riesgos en la entidad: Esta actividad implica establecer directrices claras y coherentes que guíen la identificación, evaluación y gestión de riesgos dentro de la entidad.  **2. Hacer**  **\*** Presentar para aprobación la Política Integral de Administración del Riesgo al comité de Coordinación de Control Interno. Una vez aprobada, se realiza seguimiento continuo para asegurar la implementación de medidas que mitiguen estos riesgos.  El Comité Institucional de Coordinación de Control aprueba la política y, con base en la información de las instancias de segunda línea, ejecuta el monitoreo y toma acciones ante incumplimientos, retrasos o posibles actos irregulares.    **3. Verificar**  **\***Evalúa el cumplimiento de la política y sus acciones de mitigación. Revisa los eventos materializados, identifica debilidades en los controles y promueve acciones de mejora continua para fortalecer la gestión del riesgo.  **4. Actuar**  **\***Evaluar el estado del sistema de control interno y aprobar acciones de fortalecimiento: Revisa los resultados del seguimiento, identifica oportunidades de mejora y aprueba ajustes o correctivos para optimizar la gestión integral del riesgo, y su integración con el sistema de control interno.  **3. Verificar**  \*Analizar la gestión del riesgo y su materialización: Evalúa el cumplimiento de la política y sus acciones de mitigación. Revisa los eventos materializados, identifica debilidades en los controles y promueve acciones de mejora continua para fortalecer la gestión del riesgo.  **\*** Revisar y aprobar los niveles de tolerancia, aceptación y severidad del riesgo: Evalúa los niveles propuestos por las dependencias responsables, asegurando que estén alineados con la capacidad institucional, la normatividad vigente y los objetivos estratégicos. Valida que dichos niveles sean pertinentes para la toma de decisiones informadas.  **4. Actuar**  **\*** Impulsar la implementación de mejoras y ajustes aprobados: Coordina con las áreas responsables la ejecución de acciones de fortalecimiento, asegurando su incorporación en los planes de acción institucionales y promoviendo su seguimiento y evaluación. |
| **Primera línea** | Desarrolla e implementa la gestión de riesgos a través de su identificación, análisis, valoración, implementación de controles, monitoreo y acciones de mejora. | * Responsables de proceso * Servidores y colaboradores de la entidad. | **1. Planificar:**  **\*** Realizar la identificación de riesgos que puedan afectar el logro de los objetivos institucionales.  **\***Formular un plan de acción que contemple la asignación de responsabilidades y recursos necesarios para abordar los riesgos y oportunidades identificados.  **2. Hacer:**  **\***Aplicar los controles, por lo que se trata de un seguimiento permanente, esto  incluye la aplicación de controles de gerencia operativa que corresponde a aquellos que son aplicados por servidores con personal a cargo (jefes, coordinadores u otro cargo)  \*Implementar un proceso sistemático para el seguimiento y análisis del mapa de riesgos.  **\***Establecer un mecanismo para la identificación continua de mejoras. **\***Realizar un inventario exhaustivo de los activos de información.  **\***Implementar controles específicos para garantizar la confidencialidad, integridad y disponibilidad de la información.  **3. Verificar:**  **\***El enlace de Calidad de Nivel Central y de la Territorial o responsable del reporte de monitoreo debe consolidar y revisar la información a reportar en el Sistema de Información SENDA,  **\***. Realizar ejercicios de autocontrol para verificar la efectividad de las medidas implementadas para el control del riesgo.  **4. Actuar:**  **\***Establecer un proceso de revisión regular de los resultados obtenidos del monitoreo de riesgos y de la gestión de mejoras.  **\***Fomentar una cultura de mejora continua, donde se incentive a los empleados a proponer cambios y se reconozcan los esfuerzos realizados para gestionar los riesgos |
| **Segunda línea** | Apoya metodológicamente a la primera línea de defensa en la gestión de riesgos.  Asegura que los controles en la gestión del riesgo, implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se han planeado.  Proporciona información a las demás líneas de defensa para el fortalecimiento en la gestión de riesgos y oportunidades. | * Jefe Oficina Asesora de Planeación. * Responsables de Riesgos según sistema | **1. Planificar:**  **\***Establecer un proceso para identificar cambios internos y externos que afecten el cumplimiento del direccionamiento estratégico.  **\***Diseñar una metodología clara para la gestión integral del riesgo  Planificar capacitaciones para los responsables de procesos sobre la metodología de para la gestión integral del riesgo.  **2. Hacer:**  **\*** Proporcionar apoyo continuo a los responsables en la implementación de la metodología de gestión de riesgos.  **\*** El jefe de planeación, o quien haga sus veces, debe realizar seguimiento periódico a todos los riesgos, generando recomendaciones y ajustes a los mapas de riesgos. Esto permite que las instancias de primera línea mejoren los riesgos y controles, y aseguren su aplicación mediante ejercicios de asesoría y acompañamiento a los líderes de proceso y sus equipos.  \* Presentar un mapa de riesgos actualizado y organizar reuniones para su análisis en instancias de toma de decisiones.  **\*** Implementar un sistema de monitoreo de riesgos y controles por la primera línea de defensa.  **3. Verificar:**  **\*** Realizar autoevaluaciones periódicas para evaluar la efectividad de la gestión de riesgos y recopilar retroalimentación.  **4. Actuar:**  **\*** Formular un plan de acción basado en los resultados de las autoevaluaciones, asignando responsabilidades y plazos para su implementación |
| **Tercera línea** | Proporciona información sobre la efectividad del Sistema de Control Interno a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa. | * Oficina de Control Interno. | **1. Planificar:**  En el marco de su Plan Anual de Auditoría puede proponer esquemas de asesoría y acompañamiento a la entidad, actividades que puede coordinar con la Oficina de Planeación o quien haga sus veces.  **2. Hacer:**  En su rol de seguimiento y evaluación, especialmente a través de la auditoría interna deben establecer la efectividad de los controles para evitar la materialización de riesgos  **3. Verificar:**  **\***Analizar los resultados de las evaluaciones y hacer recomendaciones para mejorar la política de operación en la administración del riesgo.  **4. Actuar:**  **\***Facilitar la implementación de las mejoras recomendadas en la política de operación, asignando responsabilidades y plazos claros.  **\***Realizar un seguimiento continuo para evaluar las mejoras implementadas. |

Incluir fuente: Lo anterior fue tomado y adaptado de la “Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6”

# COMPROMISOS DE LA ALTA DIRECCIÓN

* Asignar los recursos financieros, humanos y tecnológicos adecuados para implementar y mantener un sistema de gestión del riesgo. Esto incluye la asignación de presupuesto y la capacitación del personal involucrado en la gestión de riesgos.
* Incorporar la gestión del riesgo en la toma de decisiones a nivel estratégico, táctico y operativo, formalizándolos juntos con sus los controles a través de procedimientos, metodologías, actos administrativos u otro documento soporte.
* Definir claramente las responsabilidades de cada línea de defensa en la gestión del riesgo. La primera línea debe gestionar los riesgos en sus operaciones diarias, la segunda línea debe supervisar y proporcionar orientación, y la tercera línea debe realizar auditorías independientes para evaluar el sistema de gestión de riesgos.
* Promover una cultura organizacional que valore el autocontrol y la responsabilidad individual en la gestión de riesgos. Esto incluye la capacitación y sensibilización del personal sobre la importancia de identificar y gestionar riesgos en su trabajo diario.
* Revisar y actualizar periódicamente la política de riesgos para reflejar cambios normativos, regulatorios y de contexto que puedan afectar a la organización.
* Asegurar que la política sea comunicada y entendida por todos los niveles de la organización.
* Implementar y mantener planes de mejora, continuidad y contingencia que respondan a los riesgos identificados.
* Asegurar que los resultados de la gestión integral del riesgo sean comunicados a todas las partes interesadas dentro de la entidad. Esto incluye la elaboración de informes periódicos y la realización de presentaciones que resalten los logros, desafíos y acciones futuras en la gestión del riesgo.

# METODOLOGÍA PARA LA GESTIÓN DEL RIESGO

Parques Nacionales Naturales de Colombia gestiona sus riesgos siguiendo los lineamientos de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (Versión 6, 2022) del Departamento Administrativo de la Función Pública (DAFP). Esta metodología está diseñada para asegurar la identificación, análisis y mitigación de los riesgos que puedan comprometer el cumplimiento de los objetivos institucionales, en armonía con el Modelo Integrado de Planeación y Gestión (MIPG).

El enfoque para la administración de riesgos parte de un análisis inicial que permite evaluar el estado actual de la estructura de riesgos y su gestión dentro de la entidad. Para ello, se adopta una perspectiva estratégica basada en la operación por procesos, lo que facilita una visión integral de los riesgos y su impacto en la entidad. Como primer paso fundamental, se lleva a cabo una identificación detallada del contexto, lo que permite comprender el entorno en el que opera la entidad y establecer bases sólidas para la gestión efectiva del riesgo.

## Identificación del contexto

### Análisis de objetivos

El análisis de los objetivos es un componente esencial en la gestión del riesgo, ya que permite identificar los factores que pueden comprometer el cumplimiento tanto de los objetivos estratégicos como de los objetivos de los procesos.

Tabla 2 Análisis de Objetivos

| **Categoría** | **Descripción** |
| --- | --- |
| **Análisis de los Objetivos Estratégicos** | La entidad debe evaluar su planeación estratégica para identificar riesgos que puedan impactar su cumplimiento, ya sea favoreciendo su éxito o generando obstáculos para su consecución. Se debe verificar que esta planeación esté alineada con la Misión y la Visión institucional, asegurando su pertinencia y correcta formulación. Además, es clave analizar la viabilidad y sostenibilidad de los objetivos estratégicos en función del contexto interno y externo. |
| **Análisis de los Objetivos del Proceso** | Los objetivos de los procesos deben revisarse conforme a los criterios establecidos en el punto anterior, garantizando su alineación con la Misión y la Visión institucional. Es fundamental que estos objetivos contribuyan de manera efectiva al cumplimiento de los objetivos estratégicos, asegurando coherencia y articulación entre los diferentes niveles de planeación. |

Fuente: Elaboración Propia – Oficina Asesora de Planeación – OAP

### Establecimiento del Contexto

El contexto hace referencia a las condiciones internas y externas que pueden influir, tanto positiva como negativamente, en el cumplimiento de la misión y los objetivos institucionales. Para su definición, es esencial considerar aspectos clave como la misión, los objetivos estratégicos, el plan de acción y la naturaleza propia de la entidad.

Cada proceso debe identificar su contexto específico, para lo cual se debe hacer el uso de la herramienta de análisis DOFA (Debilidades, Oportunidades, Fortalezas y Amenazas). Este ejercicio permite una evaluación integral del entorno, facilitando la identificación de factores críticos que pueden incidir en la gestión del riesgo.

## Identificación de Puntos de Riesgo

Los puntos de riesgo corresponden a actividades dentro del flujo del proceso donde existen indicios o evidencia de posibles eventos de riesgo operativo. Estos puntos críticos deben ser identificados y gestionados de manera proactiva para garantizar que el proceso cumpla con su propósito y minimizar cualquier afectación potencial.

Para su identificación, es recomendable realizar un mapeo detallado de los procesos, evaluando cada etapa en función de su susceptibilidad a fallas, errores o vulnerabilidades. Este análisis permitirá establecer controles efectivos que reduzcan la probabilidad de ocurrencia y el impacto de los riesgos asociados.

## Identificación de Áreas de Impacto

Las áreas de impacto representan las consecuencias que podría enfrentar la entidad en caso de materializarse un riesgo. Estas consecuencias pueden reflejarse en diferentes ámbitos, siendo los más relevantes:

* **Impacto económico o presupuestal:** Afectaciones financieras derivadas de la ocurrencia del riesgo, tales como sobrecostos, pérdidas económicas o desviaciones en la ejecución del presupuesto.
* **Impacto reputacional:** Deterioro en la imagen y credibilidad de la entidad, lo que puede afectar la confianza de los grupos de interés, la legitimidad institucional y la capacidad de gestión.

## Identificación de Factores de Riesgo

Para identificar los riesgos, es fundamental analizar las dependencias y procesos que podrían actuar como generadores de riesgo. Estos se refieren a aquellas actividades dentro de los procesos que resultan críticas para el logro de los objetivos institucionales o en las que existe evidencia o indicios de que pueden presentarse eventos de riesgo.

A continuación, se presenta una tabla con ejemplos de factores de riesgo relevantes para Parques Nacionales Naturales de Colombia (PNNC):

Tabla 3 Factores de Riesgo

| **Factor** | **Definición** | **Descripción** |
| --- | --- | --- |
| **Procesos** | Riesgos derivados de errores en la ejecución de actividades por parte de los servidores de la entidad. | - Falta de procedimientos documentados.  - Deficiencias en la divulgación de procedimientos.  - Errores en la grabación y autorización de datos.  - Fallos en cálculos para pagos internos y externos. |
| **Talento Humano** | Factores relacionados con la gestión del personal, la seguridad y salud en el trabajo, y la ética organizacional. | - Falta de capacitación en temas clave.  - Posibles actos de dolo e intención en casos de corrupción.  - Hurto de activos.  - Comportamientos no éticos de los servidores públicos.  - Fraude interno (corrupción, soborno). |
| **Tecnología** | Riesgos asociados con la infraestructura tecnológica de la entidad. | - Fallas en equipos y sistemas.  - Caídas de aplicaciones y redes.  - Errores en el funcionamiento de programas y sistemas. |
| **Infraestructura** | Eventos que pueden afectar la estructura física y los activos de la entidad. | - Derrumbes y desastres naturales.  - Incendios e inundaciones.  - Daños a activos fijos. |
| **Eventos Externos** | Situaciones externas que pueden impactar el funcionamiento de la entidad. | - Suplantación de identidad.  - Asaltos a oficinas.  - Atentados, vandalismo y alteraciones del orden público |

Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas - V6 DAFP

## Identificación de Riesgos

En esta etapa se deben determinar las fuentes o factores que pueden generar riesgos, así como los eventos de riesgo, sus causas inmediatas y su causa raíz. Para llevar a cabo este análisis, se pueden utilizar diversas herramientas, como el estudio de datos históricos, el análisis teórico, la consulta con expertos y la identificación de necesidades de las partes interesadas.

### Técnicas para la Identificación de Riesgos

La identificación de riesgos se realiza mediante el análisis del contexto interno, externo y del proceso, evaluando aquellos factores que pueden afectar el cumplimiento de los objetivos estratégicos o de los procesos. Algunos riesgos externos, que no pueden ser controlados por la entidad, pueden identificarse a través del análisis del contexto externo y ser considerados en la evaluación y gestión del riesgo.

Con base en este análisis, se identifican los riesgos asociados a eventos o situaciones que puedan obstaculizar el logro de los objetivos estratégicos o de los procesos.

Para facilitar la identificación del riesgo, es fundamental responder las siguientes preguntas:

Tabla 4 Identificación del riesgo

| **Pregunta** | **Propósito** |
| --- | --- |
| **¿Qué puede suceder?** | Identificar los posibles eventos de riesgo que puedan afectar el cumplimiento de los objetivos estratégicos o de los procesos, considerando su impacto económico y reputacional. |
| **¿Cómo puede suceder?** | Determinar las causas inmediatas del riesgo, con base en los factores identificados en el contexto. |
| **¿Por qué puede suceder?** | Identificar la causa raíz del riesgo en función del desarrollo del proceso y el cumplimiento de sus objetivos. |

Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas - V6 DAFP

En términos generales, la descripción de un riesgo debe incluir todos los detalles necesarios para que tanto los responsables del proceso como terceros ajenos a este puedan comprenderlo de manera clara y precisa. Una identificación detallada facilita la implementación de estrategias de mitigación y control efectivas.

## RIESGOS DE GESTIÓN

El riesgo de gestión se refiere a la posibilidad de que errores, fallas o deficiencias en la planificación, ejecución o supervisión de los procesos impidan alcanzar los objetivos estratégicos de la entidad. Este tipo de riesgo no solo puede retrasar o desviar el cumplimiento de metas, sino que también puede afectar negativamente la eficiencia, la eficacia y la transparencia institucional.

En términos más simples, el riesgo de gestión ocurre cuando las decisiones estratégicas o las acciones operativas no se implementan adecuadamente. Esto puede deberse a factores como la falta de información, errores humanos, limitaciones en los recursos o deficiencias en los sistemas de control. Como resultado, la entidad puede enfrentar la pérdida de oportunidades, el uso ineficiente de recursos e incluso un daño a su reputación.

Además, el riesgo de gestión impacta no solo en los resultados finales, sino también en el funcionamiento diario de la entidad. Puede manifestarse en diversas áreas, como una distribución inadecuada de responsabilidades, decisiones tomadas con información incompleta o una supervisión insuficiente que permita la repetición de errores. Por lo tanto, es crucial abordar y gestionar estos riesgos para asegurar el éxito y la sostenibilidad de la organización.

### Descripción del riesgo

Se plantea una estructura que facilita su redacción y claridad, iniciando con la expresión "POSIBILIDAD DE" y considerando los siguientes aspectos:

Ilustración 1 Estructura propuesta para la redacción del riesgo

Diagrama

El contenido generado por IA puede ser incorrecto.  
Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – V6 DAFP

Dicha estructura permite comprender cómo se manifiesta el riesgo, así como sus causas inmediatas y principales o raíz, lo cual resulta fundamental para la definición de controles en la fase de valoración del riesgo.

Al desglosar esta estructura, se identifican los siguientes elementos:

* **Impacto:** Consecuencias que puede generar la materialización del riesgo en la entidad. Estos impactos pueden ser de tipo económico-presupuestal y/o reputacional.
* **Causa inmediata:** Circunstancias o situaciones más evidentes en las que se presenta el riesgo, sin constituir su origen principal.
* **Causa raíz:** Es la causa fundamental o subyacente del riesgo, lo que permite definir los controles adecuados en la fase de valoración. Un mismo riesgo puede estar asociado a múltiples causas o subcausas que deben analizarse.

Para una correcta identificación y definición de los riesgos, se recomienda evitar lo siguiente:

* Iniciar la redacción con expresiones negativas como “No…”, “Que no…”, o con términos que indiquen factores de riesgo (causas) tales como “ausencia de”, “falta de”, “escaso(a)”, “insuficiente”, “deficiente” o “debilidades en…”.
* Presentar el riesgo como si el evento ya estuviera ocurriendo.
* Redactar los riesgos en términos de omisiones o fallos en el control, por ejemplo: "Errores en la liquidación de la nómina por fallas en los procedimientos existentes".
* Confundir causas con riesgos, como en el caso de "Inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación".
* Definir riesgos negando la existencia de un control, por ejemplo: "Retraso en la prestación del servicio por no contar con digiturno para la atención".
* Clasificar riesgos como transversales, cuando en realidad lo que puede ser transversal son sus causas. Ejemplo: "Pérdida de expedientes".
* Ubicar como causa inmediata lo que en realidad es una causa raíz o definir riesgos que no tienen relación con el objetivo del proceso. Por ejemplo, si el propósito del proceso es “adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación”, un riesgo adecuado sería: "Posible pérdida económica por interrupciones recurrentes de la operación debido a la inoportuna adquisición de bienes y servicios".

Para ilustrar mejor la aplicación de la estructura propuesta, se presenta el siguiente ejemplo:

Tabla 5 Ejemplo

| **Proceso** | **Gestión de recursos** |
| --- | --- |
| **Objetivo del proceso** | Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos para la operación continua de la entidad. |
| **Alcance** | Inicia con el análisis de necesidades para cada uno de los procesos de la entidad (Plan Anual de Adquisiciones) y finaliza con las compras y contrataciones requeridas, conforme a las especificaciones técnicas y normativas establecidas. |
| **Redacción inicial** | Posibilidad de… |
| **Impacto (¿Qué?)** | Afectación económica |
| **Causa inmediata (¿Cómo?)** | Interrupciones recurrentes de la operación |
| **Causa raíz (¿Por qué?)** | Debido a la inoportuna adquisición de los bienes y servicios requeridos por la entidad. |

*Fuente: Adaptado de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V6 DAFP*

### Clasificación del riesgo

Este esquema facilita la agrupación de los riesgos identificados, clasificándolos en las siguientes categorías:

Tabla 6 Clasificación de riesgos

| **Clasificación** | **Descripción** |
| --- | --- |
| **Ejecución y administración de procesos** | Riesgos asociados a pérdidas ocasionadas por errores en la ejecución y gestión de procesos internos. |
| **Fraude externo** | Pérdidas derivadas de actos fraudulentos cometidos por terceros ajenos a la entidad, sin participación de su personal. |
| **Fraude interno** | Pérdidas causadas por fraude, conductas irregulares, delitos, abuso de confianza, apropiación indebida o incumplimiento de normativas internas o legales. Estas acciones involucran al menos a un miembro de la entidad y se realizan de manera intencional y/o con fines de lucro, ya sea personal o para terceros. |
| **Fallas tecnológicas** | Riesgos derivados de errores en hardware, software, telecomunicaciones o interrupciones en los servicios básicos. |
| **Relaciones laborales** | Pérdidas derivadas del incumplimiento de normativas laborales, acuerdos contractuales o regulaciones en materia de salud y seguridad en el trabajo, así como demandas por daños personales o discriminación. |
| **Usuarios, productos y prácticas** | Riesgos originados por negligencia o incumplimiento involuntario de obligaciones frente a los usuarios, afectando la prestación de servicios o el cumplimiento de compromisos profesionales. |
| **Daños a activos fijos / Eventos externos** | Pérdidas ocasionadas por daños, extravío o deterioro de activos fijos debido a desastres naturales u otros eventos externos como atentados, vandalismo o alteraciones del orden público. |

Fuente**:** *Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – V6 DAFP*

Ilustración 2 Relación entre los factores de riesgo y su clasificación

**Tabla

El contenido generado por IA puede ser incorrecto.**

Fuente**:** *Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – V6 DAFP*

### Valoración del riesgo

Se trata de determinar tanto la probabilidad de que ocurra un riesgo como el nivel de sus consecuencias o impacto, con el objetivo de establecer la zona de riesgo inicial (Riesgo Inherente). La valoración del riesgo se compone de dos elementos fundamentales:

**Análisis de riesgos:** En esta fase se identifica la probabilidad de ocurrencia del riesgo y sus posibles consecuencias.

**Probabilidad de ocurrencia:**

* Se relaciona con la frecuencia con la que se expone el proceso o actividad al punto de riesgo. Es decir, se considera el número de veces que se atraviesa ese punto crítico en el transcurso de un año. La siguiente tabla establece los criterios para definir los niveles de probabilidad:

Tabla 7 Criterios para definir el nivel de probabilidad

| **Descriptor** | **Frecuencia de la actividad** | **Probabilidad** |
| --- | --- | --- |
| Muy Baja | La actividad se ejecuta como máximo 2 veces por año | 20% |
| Baja | La actividad se ejecuta de 3 a 24 veces por año | 40% |
| Media | La actividad se ejecuta de 25 a 500 veces por año | 60% |
| Alta | La actividad se ejecuta de 501 a 5.000 veces por año | 80% |
| Muy Alta | La actividad se ejecuta más de 5.000 veces por año | 100% |

*Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – V6 DAFP*

**Niveles de calificación del impacto:**

Los impactos económicos y reputacionales se establecen como las variables clave para definir los criterios que determinan el nivel de impacto. Dentro de esta clasificación se incluyen aspectos como alteraciones en la ejecución presupuestaria, pagos por sanciones económicas, indemnizaciones a terceros y sanciones por incumplimientos legales, así como daños a la imagen institucional derivados de vulneraciones a la información o fallas en la prestación del servicio.

Tabla 8 Criterios para definir el nivel de impacto

| **Descriptor** | **Afectación Económica o Presupuestal** | **Afectación Reputacional** |
| --- | --- | --- |
| **Leve 20%** | Afectación menor a 10 SMMLV | Impacto limitado a la imagen de algún área específica de la organización. |
| **Menor 40%** | Entre 10 y 50 SMMLV | Impacto a nivel interno, reconocido por la junta directiva, accionistas o proveedores. |
| **Moderado 60%** | Entre 50 y 100 SMMLV | Impacto que afecta la imagen de la entidad frente a usuarios relevantes para el logro de los objetivos. |
| **Mayor 80%** | Entre 100 y 500 SMMLV | Impacto con efecto publicitario sostenido a nivel del sector administrativo, departamental o municipal. |
| **Catastrófico 100%** | Mayor a 500 SMMLV | Impacto que afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido en el país. |

*Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – V6 DAFP*

Cuando un riesgo presente tanto impacto económico como reputacional en distintos niveles de gravedad, se deberá considerar el de mayor nivel. Por ejemplo, si un riesgo identificado tiene un impacto económico leve y un impacto reputacional moderado, se asignará el nivel moderado, al ser el más alto de los dos.

### Evaluación del riesgo

Con base en el análisis de la probabilidad de ocurrencia de un riesgo y sus posibles consecuencias o impactos, se busca identificar la zona de riesgo inicial, también denominada **riesgo inherente**.

* **Análisis preliminar (riesgo inherente):** Este análisis consiste en determinar los niveles de severidad mediante la combinación de la probabilidad de ocurrencia y el impacto del riesgo. Para ello, se establecieron cuatro zonas de severidad representadas en una matriz de calor, de la siguiente manera:

Ilustración 3 Matriz de calor (niveles de severidad del riesgo)

**Gráfico, Gráfico de barras

El contenido generado por IA puede ser incorrecto.**

Fuente**:** Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – V6 DAFP

En esta matriz, el eje horizontal (X) representa el impacto, mientras que el eje vertical (Y) corresponde a la probabilidad de ocurrencia. La intersección entre estos valores define el nivel de riesgo inicial o inherente. A través de una escala de colores, se identifica la criticidad del riesgo de manera cualitativa:

* **Verde:** Bajo
* **Amarillo:** Moderado
* **Naranja:** Alto
* **Rojo:** Extremo

Este proceso de valoración tiene como objetivo establecer prioridades en la gestión del riesgo y orientar la toma de decisiones sobre su tratamiento.

Para llevar a cabo esta evaluación, se presentarán los riesgos identificados (incluyendo sus causas y consecuencias) a servidores con conocimiento especializado en el proceso, quienes analizarán detalladamente la información. Luego, cada experto seleccionará la probabilidad de ocurrencia para cada causa y asignará un valor de impacto general al riesgo, basándose en su experiencia y criterio.

Por ejemplo, al evaluar un riesgo específico, se pueden obtener los siguientes valores:

* **Probabilidad inherente:** Media (60%)
* **Impacto inherente:** Mayor (80%)

Al cruzar estos datos en la matriz de calor, se determina que la zona de riesgo es **alta**, como se ilustra a continuación:

Ilustración 4 Matriz de calor (Zona de riesgo Alta)

Gráfico, Gráfico de barras

El contenido generado por IA puede ser incorrecto.

Fuente**:** Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – V6 DAFP

### Valoración de controles

Una vez identificado el riesgo inicial, se implementan acciones específicas llamadas **controles**, cuyo propósito es reducir la exposición al riesgo. Estos controles pueden incidir en la probabilidad de ocurrencia, en el impacto del riesgo o en ambos.

**Elementos clave de un control**

Cada control debe incluir los siguientes aspectos:

1. **Responsable**: Persona o cargo encargado de ejecutar el control. Si es un control automático, se debe identificar el sistema que lo realiza.
2. **Periodicidad**: Frecuencia con la que se ejecuta el control (diario, mensual, trimestral, anual, etc.).
3. **Propósito**: Acción específica que realiza el control, expresada con verbos como verificar, validar, comparar o revisar.
4. **Método de aplicación**: Descripción detallada de cómo se lleva a cabo el control.
5. **Observaciones y desviaciones**: Acciones a seguir en caso de detectar inconsistencias o desviaciones.
6. **Evidencia**: Registro que demuestra la ejecución del control.

**Ejemplo:**

Un **Profesional de Contratación**, **cada vez** que se va a realizar un contrato, **verifica** que la información suministrada por el proveedor **cumpla con los requisitos de contratación**. Esto se realiza **mediante una lista de chequeo** que compara la documentación física con los requisitos exigidos. **Si falta información, solicita al proveedor que la complete vía correo electrónico** antes de continuar con el proceso. **Como evidencia**, se conserva el formato de lista de chequeo del SGI diligenciada y los correos de solicitud de información.

#### Tipologías y atributos para el diseño de los controles

Dependiendo de su momento de aplicación en el proceso, los controles se clasifican en:

* **Controles preventivos**: Se aplican antes de que ocurra el riesgo, enfocándose en sus causas. Son los más eficientes porque reducen la probabilidad de ocurrencia.
* **Controles detectivos**: Se activan durante la ejecución de un proceso, identificando si el riesgo se está materializando. Aunque útiles, pueden generar reprocesos.
* **Controles correctivos**: Se aplican después de que el riesgo se ha materializado, buscando reducir su impacto. Su implementación suele implicar costos adicionales.

Según su forma de ejecución, los controles pueden ser:

* **Manuales**: Son realizados por personas, lo que implica un margen de error humano.
* **Automáticos**: Se ejecutan a través de sistemas o aplicaciones sin intervención humana.

Tabla Atributos para el diseño del Control

Tabla 9 Atributos para el diseño del Control

| **características** | | | **Descripción** | **Peso** |
| --- | --- | --- | --- | --- |
| **Atributos de Eficiencia** | **Tipo** | **Preventivo** | Se enfoca en evitar la ocurrencia del riesgo desde su origen, garantizando el resultado esperado. | 25% |
| **Detectivo** | Identifica cuando el riesgo se ha presentado, permitiendo corregirlo, aunque puede generar reprocesos. | 15% |
| **Correctivo** | Actúa después de que el riesgo se ha materializado, reduciendo su impacto, pero con un costo adicional en su implementación. | 10% |
| **Implementación** | **Automático** | Se ejecuta mediante un sistema o aplicación, sin intervención humana, asegurando mayor precisión y eficiencia. | 25% |
| **Manual** | Depende de la ejecución por parte de una persona, lo que puede implicar errores humanos. | 15% |
| **Atributos**  **informativos** | **Documentación** | **Documentado** | Se encuentra registrado en procedimientos, manuales, flujogramas u otros documentos del proceso. | - |
| **Sin documentar** | Se aplica en la práctica, pero no está formalmente registrado en ningún documento del proceso. | - |
| **Frecuencia** | **Continua** | Se ejecuta cada vez que ocurre la actividad asociada al riesgo. | - |
| **Aleatoria** | Se realiza de manera ocasional o en momentos específicos dentro del proceso. | - |
| **Evidencia** | **Con registro** | Deja constancia documentada de su ejecución, permitiendo su verificación. | - |
| **Sin registro** | No genera evidencia formal de su aplicación. | - |

Fuente: *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – V6 DAFP*

Cada control identificado debe evaluarse en función de su impacto en la gestión del riesgo. Para ello, es necesario analizar sus características, considerando su eficiencia y grado de formalización, con el objetivo de determinar si influye en la probabilidad de ocurrencia, en el impacto del riesgo o en ambos.

Cuanto más sólidos sean los controles implementados, mayor será la diferencia entre el riesgo inicial (inherente) y el riesgo final (residual). Esto se refleja en la matriz de calor, donde se observa cómo los diferentes tipos de controles modifican los niveles de probabilidad e impacto.

Ilustración 5 Movimiento en la matriz de calor acorde con el tipo de control

Gráfico

El contenido generado por IA puede ser incorrecto.

Fuente Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – V6 DAFP

En este sentido, un riesgo inicialmente clasificado como extremo debido a su alta probabilidad e impacto puede reducirse a un nivel moderado o bajo después de aplicar controles efectivos, como los preventivos, automáticos y documentados.

**Nota:** Para una comprensión más detallada sobre el análisis y evaluación de los controles, se recomienda consultar la *Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (versión 6)*, del Departamento Administrativo de la Función Pública, específicamente el numeral 3.2.2.3., donde se presentan ejemplos sobre la determinación del riesgo residual tras la aplicación de controles.

### Determinación riesgo residual

Después de identificar los controles existentes y evaluar su efectividad, se llevan a cabo los cálculos necesarios para determinar el riesgo residual. Este representa el nivel de riesgo restante tras la aplicación de los controles. A continuación, se presenta un ejemplo que ilustra los cálculos requeridos para su implementación.

Tabla 10 Ejemplo de aplicación de controles para determinar el riesgo residual

| **Riesgo** | **Probabilidad e Impacto Inherentes** | **Valoración de Controles** | **Cálculos Aplicados** |
| --- | --- | --- | --- |
| Posible pérdida económica por multas y sanciones impuestas por el ente regulador debido a la adquisición de bienes y servicios sin cumplir los requisitos normativos. | **Probabilidad inherente:** 60% | **Control 1 (preventivo):** 40% | 60% \* 40% = 24% → 60% - 24% = **36%** |
| **Probabilidad después del 1er control:** 36% | **Control 2 (detectivo):** 30% | 36% \* 30% = 10.8% → 36% - 10.8% = **25.2%** |
| **Probabilidad residual:** 25.2% | | |
| **Impacto inherente:** 80% | No se aplican controles adicionales al impacto. | N/A |
| **Impacto residual:** 80% | | |

**Fuente:** Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas – V6 DAFP.

**Nota:** *Es importante tener en cuenta que, en los riesgos asociados a la corrupción, solo es posible reducir la probabilidad de ocurrencia. Como se mencionó previamente en la valoración del impacto, este tipo de riesgos no pueden clasificarse como leves o menores. En consecuencia, no se contempla una disminución en la magnitud del impacto.*

## RIESGO DE CORRUPCIÓN

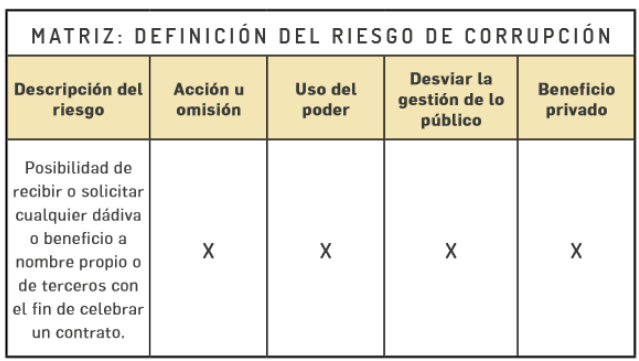
### Descripción del riesgo

Se refiere a la posibilidad de que, por acción u omisión, se abuse del poder para desviar la gestión de los asuntos públicos en beneficio privado, en contravía del interés general y de los principios de transparencia, eficiencia y equidad.

Según el CONPES No. 167 de 2013, las prácticas corruptas pueden ser llevadas a cabo por actores del sector público y/o privado con poder e influencia en la toma de decisiones y en la administración de los recursos públicos, generando impactos negativos en la confianza ciudadana y el desarrollo institucional.

Para una adecuada descripción del riesgo de corrupción, es fundamental incluir los elementos que conforman su definición, asegurando que las acciones de los servidores públicos estén alineadas con los lineamientos del Código de Integridad de la PNNC y que se prevengan los conflictos de interés que puedan comprometer la transparencia, la imparcialidad y la gestión ética de los recursos públicos. Esto implica la adopción de mecanismos de control y monitoreo que permitan identificar, mitigar y sancionar cualquier conducta que atente contra la ética pública y la legalidad.

Ilustración 6 Estructura propuesta para la redacción del riesgo



Fuente: Secretaría de Transparencia de la Presidencia de la República

### Valoración del riesgo de corrupción

* **Análisis de probabilidad**: consiste en evaluar qué tan factible es su ocurrencia, ya sea a partir de su frecuencia, que mide cuántas veces ha sucedido en un período determinado con base en antecedentes, o a través de su factibilidad, que examina los factores internos y externos que podrían propiciar su materialización, incluso si aún no ha ocurrido.

Ilustración 7 Criterios para calificar la probabilidad

Tabla

El contenido generado por IA puede ser incorrecto.

Fuente Secretaría de Transparencia de la Presidencia de la República

* **Análisis del impacto:** El impacto debe evaluarse y clasificarse con base en las consecuencias identificadas durante la fase de descripción del riesgo:

Ilustración 8 Criterios para calificar el impacto en riesgos de corrupción

Tabla

El contenido generado por IA puede ser incorrecto.

Interfaz de usuario gráfica, Texto, Aplicación

El contenido generado por IA puede ser incorrecto.

Fuente: Secretaría de Transparencia de la Presidencia de la República

En el análisis de impacto de los riesgos de corrupción, solo se considerarán los niveles "moderado", "mayor" y "catastrófico", ya que estos riesgos siempre tienen una relevancia significativa. Por esta razón, no se contemplan los niveles de impacto "insignificante" y "menor", los cuales sí son aplicables a otros tipos de riesgos

### Evaluación del Riesgo de Corrupción

Con base en el análisis de la probabilidad de ocurrencia del riesgo y sus posibles consecuencias o impactos, se pretende identificar la zona de riesgo inicial, también denominada riesgo inherente.

Ilustración 9 Matriz de calor (niveles de severidad del riesgo)

Gráfico, Gráfico de barras

El contenido generado por IA puede ser incorrecto.

Fuente: Secretaría de Transparencia de la Presidencia de la República

### Valoración de Controles

Aplicar lo definido en el numeral 8.6.5

### Determinación del riesgo residual

Aplicar lo definido en el numeral 8.6.6

## RIESGO FISCAL

Su propósito es evitar la formación del núcleo esencial de la responsabilidad fiscal, que consiste en el daño al patrimonio público, manifestado en la afectación, reducción, perjuicio, menoscabo, pérdida o deterioro de los bienes, recursos.

### Identificación del riesgo

Para identificar el riesgo fiscal, es necesario determinar los puntos de riesgo y las circunstancias inmediatas. Los puntos de riesgo son actividades relacionadas con la administración y manejo de recursos públicos que pueden generar riesgo fiscal, como la gestión, adquisición, consumo, inversión, y disposición de bienes, así como la recaudación y manejo de rentas. Además, incluyen situaciones con alertas o hallazgos fiscales.

Las circunstancias inmediatas son situaciones específicas en las que se presenta el riesgo, pero no son la causa principal del mismo. Cada punto de riesgo fiscal puede estar asociado con múltiples circunstancias inmediatas.

Ilustración 10 Preguntas orientadoras para puntos riesgo fiscal y causas inmediatas

Texto

El contenido generado por IA puede ser incorrecto.

Texto

El contenido generado por IA puede ser incorrecto.

Fuente: Elaboración Dirección de Gestión y Desempeño Institucional de Función Pública, 2022

### Descripción del riesgo

Se detallan los componentes que definen el Riesgo Fiscal:

* **Efecto:** Es el daño que se produciría sobre los recursos públicos y/o los bienes e intereses patrimoniales de naturaleza pública si ocurriera el evento potencial, afectando la sostenibilidad financiera, la capacidad de inversión y la prestación de servicios esenciales por parte del Estado.
* **Evento potencial:** Son hechos inciertos o situaciones de riesgo que podrían generar daño sobre los recursos públicos o bienes e intereses patrimoniales públicos. En esta guía, el evento potencial es equivalente a la causa raíz, incluyendo fallas en la planeación financiera, inadecuada ejecución presupuestal, corrupción o debilidades en los mecanismos de control.

La descripción del riesgo debe ser clara y comprensible tanto para el líder del proceso como para personas ajenas a él. Se sugiere estructurarla iniciando con la frase **"POSIBILIDAD DE"**, seguida de un análisis integral que contemple los efectos, las causas y las medidas de mitigación.

Para una gestión efectiva del riesgo fiscal, es fundamental que las decisiones y actuaciones de los servidores públicos estén alineadas con los lineamientos del Código de Integridad de la PNNC, promoviendo principios de transparencia, responsabilidad y legalidad. Asimismo, la identificación y prevención de conflictos de interés resultan clave para evitar que intereses particulares influyan en la administración de los recursos públicos, garantizando una toma de decisiones imparcial y basada en el interés general.

El fortalecimiento de mecanismos de control, auditoría y rendición de cuentas contribuye a minimizar estos riesgos, asegurando el uso eficiente y ético de los recursos públicos en beneficio de la ciudadanía.

Ilustración 11 Estructura propuesta para la redacción del riesgo

Diagrama

El contenido generado por IA puede ser incorrecto.

Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – V6 DAFP

**Nota**: Es fundamental no confundir el riesgo fiscal con el daño fiscal, ya que la definición debe centrarse en el efecto de un evento potencial sobre los recursos y bienes públicos.

Desglosando la estructura:

* **Impacto (¿Qué?)**: Se refiere al daño potencial sobre los recursos y bienes públicos o los intereses patrimoniales de naturaleza pública.
* **Circunstancia Inmediata (¿Cómo?)**: Es la situación que origina el riesgo, aunque no es la causa principal que lo genera.
* **Circunstancia Raíz (¿Por qué?)**: Es el evento (acción u omisión) que causa directamente el riesgo, es decir, la condición necesaria para que el daño ocurra.

**Ejemplo**:

* **Proceso**: Gestión de Recursos
* **Objetivo**: Gestionar bienes, obras y servicios administrativos, de mantenimiento y asistencia logística para cumplir con la misión institucional.
* **Alcance**: Desde la consolidación del plan de necesidades de bienes hasta el suministro y prestación de servicios conforme a la disponibilidad de recursos.

Aplicando el esquema para redactar el riesgo:

* **Redacción inicia con**: Posibilidad de
* **Impacto - ¿Qué?**: Efecto dañoso sobre bienes públicos
* **Circunstancia Inmediata - ¿Cómo?**: Por pérdida, extravío o hurto de bienes muebles.
* **Circunstancia Raíz - ¿Por qué?**: Debido a la omisión en la aplicación del procedimiento para el ingreso y salida de bienes del almacén.

Este esquema ayuda a estructurar los riesgos de forma clara y precisa.

Ilustración 12 Ejemplos adicionales acorde con el objeto sobre el que recae el efecto dañoso

Una captura de pantalla de un celular

El contenido generado por IA puede ser incorrecto.

Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – V6 DAFP

### Valoración del Riesgo Fiscal

El objetivo es determinar la probabilidad de que ocurra el Riesgo Fiscal y sus posibles consecuencias o impactos:

* **Determinar la probabilidad**: Se refiere a la posibilidad de que ocurra el Riesgo Fiscal. Esta probabilidad se evalúa según la frecuencia con la que se enfrenta un punto de Riesgo Fiscal durante un año, es decir, cuántas veces se realizan actividades que impliquen Gestión Fiscal (ver tabla 7).
* **Niveles para calificar el impacto**: Debido a la naturaleza y alcance del Riesgo Fiscal, siempre tendrá un impacto económico, ya que el daño siempre afectará a un bien, recurso o interés patrimonial público. Cualquier posible consecuencia económica sobre estos activos es importante para una correcta gestión fiscal y prevención de riesgos. Sin embargo, existen diferentes niveles de impacto, dependiendo de la magnitud del daño potencial o daño fiscal (ver tabla 8).
* **Determinar el Riesgo Inherente**: A partir del análisis de la probabilidad y el impacto, se busca identificar la zona de riesgo inicial (riesgo inherente).

Ilustración 13 Matriz de calor (niveles de severidad del riesgo)

Gráfico, Gráfico de barras

El contenido generado por IA puede ser incorrecto.

Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – V6 DAFP

El cruce entre la probabilidad y el impacto determinará la zona en la que se ubica el riesgo inherente (Bajo, Moderado, Alto, Extremo).

### Valoración de controles

Aplicar lo definido en el numeral 8.6.5

### Determinación del riesgo residual

Aplicar lo definido en el numeral 8.6.6

## RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

En el caso de los riesgos relacionados con la seguridad de la información, se debe incluir el Anexo 4 "Modelo nacional de gestión de riesgo de seguridad de la información en Entidades públicas", para que los responsables analicen y determinen, dentro de sus procesos, los activos de información relacionados y los riesgos correspondientes. Los riesgos de seguridad digital se centran en la afectación de tres aspectos de un activo o grupo de activos: "Integridad, confidencialidad o disponibilidad". Para cada riesgo identificado, se deben vincular los activos del proceso y analizar las amenazas y vulnerabilidades que podrían ocasionar su materialización. Es responsabilidad de la primera línea de defensa identificar los activos en cada proceso.

### Identificación de los activos de seguridad de la información

Un activo es cualquier recurso que tenga valor para la Entidad. En el contexto de seguridad de la información, los activos incluyen elementos como aplicaciones institucionales, servicios web, redes, información en formato físico o digital, tecnologías de la información (TI) y tecnologías de operación (TO), todos ellos esenciales para el funcionamiento digital de la Entidad. Identificar estos activos por cada uno de los líderes de proceso permite determinar qué elementos deben ser protegidos para garantizar tanto la operatividad interna como la prestación de servicios a la ciudadanía, fortaleciendo así la confianza en el entorno digital.

Para identificar los activos vinculados con la seguridad de la información, se debe tener en cuenta la sección 3.1.6 del Anexo 4 del “Modelo nacional de gestión de riesgo de seguridad de la información en Entidades públicas”, publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones.

### Identificación del riesgo de seguridad de la información

Para evaluar los riesgos en seguridad de la información, es fundamental identificar las amenazas a las que están expuestos los activos de cada proceso bajo responsabilidad de la Entidad. Estas amenazas pueden ocasionar daños temporales o permanentes en los activos, procesos y sistemas de soporte. Además, algunas amenazas pueden afectar múltiples activos y generar impactos de distinta magnitud según los elementos comprometidos.

Se reconocen tres tipos principales de riesgos inherentes en la seguridad de la información:

* Pérdida de la confidencialidad
* Pérdida de la integridad
* Pérdida de la disponibilidad

Según la “Guía para la administración del riesgo y el diseño de controles en Entidades públicas” (versión 06), es necesario asociar cada riesgo con los activos o grupos de activos correspondientes dentro del proceso. Luego, se deben analizar las amenazas y vulnerabilidades que podrían provocar su materialización. Para este análisis, se debe consultar el Anexo 4 del “Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas”, donde se encuentran tablas clave, como:

* Tabla 5: Amenazas comunes
* Tabla 6: Amenazas generadas por la acción humana
* Tabla 7: Vulnerabilidades comunes

Las vulnerabilidades representan fallas o debilidades que pueden comprometer la confidencialidad, integridad y disponibilidad de los sistemas. Estas pueden identificarse mediante pruebas de vulnerabilidad, visitas, entrevistas u otros criterios que la Entidad considere adecuados. Sin embargo, la presencia de una vulnerabilidad por sí sola no implica necesariamente un riesgo, ya que esta solo representa una debilidad. Para que se convierta en una amenaza real, es necesario que exista un factor externo capaz de explotarla. Si una vulnerabilidad no tiene una amenaza asociada, es posible que no requiera la implementación de un control específico.

A continuación, se presentan las posibles amenazas y vulnerabilidades que pueden generar riesgos en un activo de información, considerando su tipo específico:

Tabla 11 Posibles amenazas y vulnerabilidades

| **Tipo de activo** | **Ejemplo de vulnerabilidades** | **Ejemplo de amenazas** |
| --- | --- | --- |
| **Hardware** | Defectos de Fabrica | Fallas por mal funcionamiento del sistema de información por fallas generadas por el fabricante en el uso o aplicación de producto y/o Servicio |
| Ausencia de esquemas de reemplazo periódico | Destrucción de equipos o medios |
| Ausencia de un eficiente control de cambios en la configuración | Error en el uso |
| Susceptibilidad a variaciones de temperatura | Pérdida del suministro de energía |
| Almacenamiento de medios sin protección | Hurto de medios o documentos |
| **Amenaza Informática** | Ausencia de parches de auditoría | Abuso de derechos |
| Ausencia de documentación | Error en el uso |
| Tablas de contraseñas sin protección | Falsificación de derechos |
| Ausencia de control de cambios eficaz | Manipulación con software |
| **Red** | Arquitectura de red insegura | Espionaje remoto |
| Envío de contraseñas en texto claro | Espionaje remoto |
| Gestión inadecuada de la red | Saturación del sistema de información |
| **Fallas Humanas** | Ausencia de personal | Incumplimiento en la disponibilidad del personal |
| Falta de conciencia acerca de la seguridad | Error en el uso |
| Ausencia de políticas para el uso correcto del correo electrónico | Uso no autorizado del equipo |
| **Entidad** | Ausencia de auditorías | Abuso de derechos |
| Ausencia de procedimiento formal para el registro y retiro de usuarios | Abuso de derechos |
| Ausencia de procedimientos de control de cambios | Incumplimiento en el mantenimiento del sistema de información |
| Ausencia de procedimientos para el manejo de la información | Error en el uso |

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

### Evaluación del Riesgo de Seguridad de la Información

En esta fase, es necesario aplicar los lineamientos establecidos para medir la probabilidad e impacto del riesgo, de acuerdo con lo indicado en la sección 8.7.3 de la presente guía.

### Controles para la Seguridad de la Información

Para gestionar y mitigar los riesgos en seguridad de la información, Parques Nacionales Naturales de Colombia adopta los criterios definidos en el Anexo A de la norma ISO 27001:2022. Estos controles también están incluidos en el Anexo 4 del “Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas”.

## TRATAMIENTO DEL RIESGO

La gestión del riesgo implica determinar la acción a tomar frente a un nivel de riesgo específico, pudiendo optar por aceptarlo, reducirlo o evitarlo. Esta decisión se basará en un análisis del riesgo inherente y residual, así como en la implementación de controles adecuados.

Según la Secretaría de Transparencia, en el contexto de los riesgos de corrupción, no existen niveles de aceptación o tolerancia. Por lo tanto, todas las situaciones de riesgo deben ser tratadas, y se debe esforzar por mantener los riesgos en un nivel moderado.

En lo que respecta a los riesgos de seguridad de la información, solo se consideran tolerables aquellos que se encuentren en el nivel residual dentro de la zona de riesgo bajo.

La siguiente ilustración muestra las estrategias de gestión de riesgos disponibles y su relación con la necesidad de establecer planes de reducción dentro del mapa de riesgos.

Ilustración 14 Estrategias para combatir el riesgo

Diagrama, Texto

El contenido generado por IA puede ser incorrecto.

Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas – V6 DAFP

Los líderes de proceso deben analizar las alternativas disponibles para el tratamiento del riesgo, basándose en la presente política. Para ello, deben considerar su relevancia, los posibles efectos sobre la entidad, su probabilidad e impacto, así como la relación costo-beneficio de las medidas a implementar. La decisión sobre el tratamiento del riesgo se toma con base en el nivel de riesgo residual.

Las opciones de tratamiento del riesgo incluyen:

* **Aceptar el riesgo:** Asumirlo plenamente, con conocimiento de sus posibles consecuencias, conociendo los efectos de su posible materialización.
* **Reducir el riesgo:** Gestionarlo mediante su transferencia o mitigación.
* **Evitar el riesgo:** Optar por no realizar la actividad que lo genera.

**Estrategia de reducción del riesgo**

* **Transferir**: Tras evaluar la situación, se determina que la opción más adecuada es delegar el proceso a un tercero o trasladar el riesgo mediante seguros o pólizas. Aunque la carga económica recae en el tercero, la responsabilidad reputacional sigue siendo de la entidad.
* **Mitigar**: Tras analizar los niveles de riesgo, se implementan controles destinados a reducir su impacto y probabilidad de ocurrencia.

### Plan de reducción del riesgo

Es un conjunto de acciones que refuerzan los controles existentes y aportan valor a la gestión preventiva y a la debida diligencia. Para abordar el tratamiento del riesgo de manera más específica, es necesario consolidar un plan de reducción detallado según el riesgo y sus causas. Este plan debe incluir los siguientes elementos:

* **Actividades:** Son las acciones diseñadas para tratar el riesgo, enfocadas en su mitigación. Se deben evaluar opciones viables y efectivas, como la implementación de políticas, definición de estándares, optimización de procesos y procedimientos, o mejoras en la infraestructura. Estas actividades deben ser claras, contar con plazos definidos y disponer de mecanismos de verificación. Se recomienda incluir entre una (1) y tres (3) actividades por riesgo.
* **Responsables:** Se debe asignar roles o personas encargadas de ejecutar cada actividad dentro del plan de acción. Es fundamental que cuenten con la autoridad y los recursos necesarios para garantizar su implementación efectiva.
* **Fechas de ejecución:** Para cada actividad, se debe establecer un periodo de implementación, indicando los plazos mínimos y máximos o la periodicidad con la que se deben llevar a cabo.

**Evidencias o soportes:** Se deben definir los medios que permitan verificar de manera objetiva el cumplimiento de cada acción. Estas evidencias deben estar directamente relacionadas con las actividades planteadas, ya que representan la materialización de estas.

# MONITOREO Y SEGUIMIENTO DE RIESGOS

## Consideraciones generales para el Monitoreo de Riesgos

Una vez diseñado y validado el mapa de riesgos, es fundamental realizar su seguimiento continuo, dado que los riesgos siempre representan una posible amenaza. Para **PNNC**, esta actividad es clave y está a cargo de los líderes de proceso junto con sus equipos, asegurando así una gestión eficiente de los riesgos.

El monitoreo en **PNNC** es permanente y no se limita a los informes de segunda y tercera línea. Para ello, es fundamental garantizar el acceso a las evidencias de los controles y planes de reducción, considerando la periodicidad establecida, ya sea con fechas fijas o con revisiones mensuales, trimestrales, cuatrimestrales, semestrales o anuales, según corresponda. Este seguimiento permite verificar si las actividades se han ejecutado conforme a lo planificado y evaluar su efectividad de manera objetiva.

El monitoreo de riesgos debe realizarse a través del Sistema de Información SENDA, utilizando el módulo de riesgos, específicamente en el apartado de Monitoreo. Este módulo ha sido diseñado en alineación directa con los lineamientos establecidos en la Guía para la Administración del Riesgo, lo que garantiza que cada una de las etapas del proceso (identificación, análisis, evaluación, tratamiento, seguimiento y comunicación) se desarrollen de forma estructurada y conforme a la normativa vigente.

Cabe destacar que SENDA incorpora dentro de su plataforma las guías oficiales, facilitando así el acceso a los marcos metodológicos necesarios para la correcta implementación del modelo.

En esta fase, el líder del proceso, junto con su equipo como Primera Línea de Defensa, debe:

* Verificar que los controles sean efectivos tanto en su diseño como en su implementación.
* Ajustar o establecer nuevos controles según sea necesario.
* Recopilar información adicional para optimizar la valoración del riesgo.
* Analizar y extraer aprendizajes a partir de eventos, cambios, tendencias, logros y fallos.
* Identificar lecciones aprendidas para fortalecer la gestión del riesgo.
* Detectar variaciones en el contexto interno y externo que puedan afectar la entidad.
* Reconocer nuevos riesgos y evaluar su incorporación en el mapa de riesgos.
* Implementar los planes de reducción
* En caso de materialización de un riesgo, se deberá informar de inmediato por correo electrónico a la Oficina Asesora de Planeación (para riesgos fiscales y de gestión) y a la Oficina de Control Interno y Planeación (para riesgos de corrupción), con el fin de activar las acciones necesarias y reiniciar el ciclo de gestión del riesgo.

El monitoreo continuo, para el caso de la seguridad de la información además implica la implementación de herramientas de análisis en tiempo real, auditorías periódicas y pruebas específicas que permitan identificar brechas de seguridad antes de que puedan ser explotadas, todo, de acuerdo con los controles de la norma ISO 27001:2022. Lo anterior, permite que PNNC técnicamente pueda anticiparse a posibles incidentes y reforzar sus mecanismos de defensa en función de las amenazas emergentes y/o recurrentes.

Estas acciones permiten determinar si es necesario modificar, actualizar o mantener los factores de riesgo en sus condiciones actuales, así como mejorar su identificación, análisis y evaluación

## Acciones para seguir en caso de Materialización del Riesgo

El riesgo siempre está presente en el desarrollo de cualquier actividad, ya sea realizada por una entidad, un grupo empresarial, una sociedad o una persona. Por ello, es fundamental mantenerse en alerta constante, revisar periódicamente procesos, procedimientos, controles y objetivos. Sin embargo, a pesar de todos los esfuerzos, un riesgo puede llegar a materializarse, y **PNNC** no es la excepción.

Ante esta situación, es crucial actuar de manera inmediata para minimizar el impacto y prevenir su recurrencia. En este contexto, a continuación, se presentan las acciones prioritarias que deben ejecutarse en caso de que ocurra un evento que derive en la materialización de un riesgo.

**Riesgos de Gestión**

Tabla 12 Ruta de acción en caso de materialización para riesgos de gestión

| **Línea de Defensa** | **Conducto regular** | **Actividades** |
| --- | --- | --- |
| **Primera Línea** | Jefes de área o líder del proceso y su equipo de trabajo | - Analizar la materialización del riesgo y sus causas en mesa de trabajo con la OAP. - Ejecutar el plan de contingencia, documentarlo y registrar el evento en el Sistema de Información SENDA con sus evidencias.  -Formular Plan de Mejoramiento, documentar e implementar las correcciones - Revisar el mapa de riesgos, las causas, controles existentes y los planes de tratamiento. - Evaluar el contexto interno, externo y del proceso. - Determinar la efectividad de los controles y analizar si es necesario modificar o crear nuevos controles. |
| **Segunda Línea** | OAP | - Revisar la información registrada en el sistema SENDA/Módulo de Riesgos. - Brindar asesoría y apoyo en la revisión y actualización del mapa de riesgos. - Evaluar los planes de tratamiento y definir medidas para evitar la repetición del riesgo. - Comunicar al líder del proceso sobre los riesgos detectados para su respectivo análisis y tratamiento. |

Fuente: Elaboración Propia – Oficina asesora de Planeación – OAP

**Riesgos de Corrupción y Fiscales**

Tabla 13 Actividades Materialización del Riesgo de Corrupción y Fiscales

| **Línea de Defensa** | **Conducto regular** | **Actividades** |
| --- | --- | --- |
| **Primera Línea** | Jefes de área o líder del proceso y su equipo de trabajo | - Implementar el plan de contingencia, documentarlo y reportarlo en el sistema SENDA. - Notificar a la OAP sobre la materialización del riesgo. - Aplicar correcciones y gestionar las consecuencias. - Revisar el mapa de riesgos de corrupción y fiscales, junto con sus controles y planes de tratamiento. - Evaluar el contexto interno, externo y del proceso. - Analizar la materialización del riesgo con la OAP y, si es necesario, con la Oficina de Control Interno. - Determinar la efectividad de los controles y definir si se requieren nuevas medidas. |
| **Segunda Línea** | Oficina Asesora de Planeación | - Analizar la información del formulario de materialización de riesgos. - Brindar asesoría en la actualización del mapa de riesgos. - Revisar los planes de tratamiento y proponer acciones para evitar la repetición del riesgo. - Confirmar si el reporte corresponde realmente a un riesgo de corrupción y validar si se requiere llevar a instancias disciplinarias. - Asegurar que el líder del proceso haya tomado acciones y actualizado el mapa de riesgos. |
| **Tercera Línea** | OCI | - Verificar que las decisiones tomadas sean proporcionales al impacto del riesgo materializado. - Convocar al Comité de Coordinación del Sistema de Control Interno cuando sea necesario. - Informar sobre hechos detectados y facilitar la investigación. - Coordinar acciones con el líder del proceso para revisar controles. - Reportar a la Contraloría General de la República los riesgos fiscales identificados a través del Sistema de Alertas de Control Interno – SACI.  Reportar a la Secretaría de Transparencia del Departamento Administrativo de la Presidencia de la República, los riesgos de corrupción. |

Fuente: Elaboración Propia – Oficina asesora de Planeación – OAP

**Riesgos de Seguridad de la Información**

Tabla 14 Actividades Materialización del Riesgo de Seguridad de la información

| **Línea de Defensa** | **Conducto regular** | **Actividades** |
| --- | --- | --- |
| **Primera Línea** | Jefes de área o líder del proceso y su equipo de trabajo | - Implementar el plan de contingencia, documentarlo y registrar el evento en el Sistema SENDA. - Notificar a la OAP sobre la materialización del riesgo. - Analizar el evento y sus causas en mesa de trabajo con la OAP y el líder del proceso - Gestionar correcciones y mitigar las consecuencias. - Revisar el mapa de riesgos de seguridad de la información y evaluar los controles existentes. - Analizar la conveniencia de actualizar el mapa de riesgos. - Verificar la efectividad de los controles y determinar si es necesario implementar nuevos. |
| **Segunda Línea** | Grupo de Tecnologías de la Información y Comunicaciones | - Evaluar la información registrada en SENDA. - Brindar asesoría en la revisión y actualización del mapa de riesgos. - Analizar los planes de tratamiento y establecer medidas para evitar la repetición del riesgo. |

Fuente: Elaboración Propia – Oficina asesora de Planeación – OAP

## Periodicidad del monitoreo y seguimiento al mapa de riesgos

La supervisión de la implementación de los controles y las acciones del plan de reducción es responsabilidad de la primera línea de defensa y del proceso de seguimiento. Por su parte, el control del mapa de riesgos institucional recae en la segunda y tercera línea de defensa, según lo indicado en la siguiente tabla:

Tabla 15 Monitoreo y Seguimiento Líneas de Defensa

| **Línea de defensa** | **Riesgos** | **Ene** | **Feb** | **Mar** | **Abr** | **May** | | **Jun** | **Jul** | **Ago** | **Sep** | | **Oct** | **Nov** | **Dic** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **1ra línea** | **Todos los tipos de riesgo** | **Monitoreo Permanente** (Depende de la periodicidad de la ejecución de los controles) | | | | | | | | | | | | | |
| **2da línea** | **Riesgos de Gestión Fiscales, Seguridad de la Información TI** | **1er seguimiento** (Corte: 30 de abril, informe elaborado en las dos semanas siguientes) | | | | | **2do seguimiento** (Corte: 31 de agosto, informe elaborado en las dos semanas siguientes) | | | | | **3er seguimiento** (Corte: 31 de diciembre, informe elaborado en las dos semanas siguientes) | | | |
| **Riesgos de corrupción** | **1er seguimiento** (Corte: 30 de abril, informe elaborado en las dos semanas siguientes) | | | | **2do seguimiento** (Corte: 31 de agosto, informe elaborado en las dos semanas siguientes) | | | | | **3er seguimiento** (Corte: 31 de diciembre, informe elaborado en las dos semanas siguientes) | | | | |
| **3ra línea** | **1er seguimiento** (Corte: 30 de abril, publicación del informe en los primeros 10 días de mayo) | | | | **2do seguimiento** (Corte: 31 de agosto, publicación del informe en los primeros 10 días de septiembre) | | | | | **3er seguimiento** (Corte: 31 de diciembre, publicación del informe en los primeros 10 días de enero) | | | | |

Fuente: Elaboración Propia – Oficina asesora de Planeación – OAP

# REVISIÓN Y ACTUALIZACIÓN DE LOS MAPAS DE RIESGOS

Los mapas de riesgos se revisan y actualizan cuando se presentan cambios en los objetivos, el alcance o las actividades de un proceso, o si el contexto estratégico experimenta modificaciones significativas que requieran una reevaluación de los riesgos gestionados. Como mínimo, deben ser revisados y/o actualizados anualmente a partir de la última fecha de revisión.

Los riesgos identificados pueden actualizarse de manera individual cuando sea necesario, utilizando insumos como No conformidades de auditorías internas y externas, revisiones por la dirección, así como los resultados de acciones de seguimiento y autocontrol realizadas por los líderes y responsables de cada proceso. Además, los informes de seguimiento de la segunda y tercera línea de defensa pueden evidenciar la necesidad de realizar ajustes a los mapas de riesgos, incorporando retroalimentaciones específicas sobre la identificación del riesgo, la planificación de tratamientos y los controles existentes.

# COMUNICACIÓN Y CONSULTA

La comunicación y consulta con las partes interesadas, tanto internas como externas, deben desarrollarse en todas las etapas del proceso de gestión del riesgo y las oportunidades. En este sentido, Parques Nacionales Naturales de Colombia establece las siguientes actividades:

* **Política de Gestión de Riesgos:** La Alta Dirección será responsable de establecer y actualizar esta política, garantizando su socialización en todos los niveles de la entidad a través de los Comités Institucional de Gestión y Desempeño. Esto permitirá que las tres líneas de defensa comprendan claramente sus roles, responsabilidades y niveles de autoridad en la gestión del riesgo.
* **Divulgación del Mapa de Riesgos:** Este documento deberá estar disponible en el sistema de información SENDA Módulo de Riesgos, permitiendo su consulta por parte de la comunidad de PNNC. Así, los colaboradores podrán revisar y aportar su conocimiento en la identificación, análisis y valoración de riesgos, así como en la ejecución de las acciones definidas para su tratamiento.
* **Rol del líder de proceso:** Como parte de la primera línea de defensa, los líderes de proceso deberán compartir con sus equipos los riesgos identificados, los controles implementados y las acciones de mitigación. Esto contribuirá a generar conciencia y comprensión sobre la toma de decisiones y la importancia de las acciones adoptadas, fortaleciendo la cultura de gestión del riesgo dentro de la entidad.
* **Fomento de la cultura de gestión del riesgo:** La Oficina Asesora de Planeación (OAP) y la Oficina de Control Interno (OCI) promoverán esta cultura a nivel institucional mediante divulgaciones, capacitaciones, mesas de trabajo y asesorías, con el propósito de mejorar el conocimiento y la apropiación del enfoque basado en riesgos.
* **Comunicación de acciones de tratamiento de riesgos:** Cuando las acciones de mitigación involucren a partes interesadas o terceros, los líderes y responsables de cada proceso serán los encargados de divulgarlas.
* **Mapa de Riesgos de Corrupción:** La OAP será la encargada de consolidar este mapa y de facilitar el proceso de gestión de riesgos de corrupción en coordinación con las diferentes dependencias.
* **Divulgación del Mapa de Riesgos de Corrupción:** Su consulta estará disponible para partes interesadas y la comunidad en general a través de la página web de la entidad, en la sección de Transparencia y Acceso a la Información Pública, conforme a lo establecido en el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015. Este documento revisado deberá publicarse a más tardar el 31 de enero de cada año o en un medio de fácil acceso para la ciudadanía.

# CONTROL DE CAMBIOS

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Fecha** | **Versión** | **Elaboró** | **Revisó** | **Aprobó** | **Motivo de la actualización** |
| 02/04/2025 | 1 | Hugo Alvarez – Contratista OAP  Marcela Borda - Contratista OAP  Diana Ramírez – Profesional Universitario OAP  Pedro Pardo - Contratista OAP  Daniela Carvajal - Contratista OAP | Nancy Gómez - Contratista OCI  Gladys Espitia- Jefe OCI | Comité de Control Interno 06-05-2025 | Creación de la política integral para la administración del riesgo |