PARQUES NACIONALES NATURALES DE COLOMBIA	**INSTRUCTIVO** **ADMINISTRACIÓN DE RIESGOS Y OPORTUNIDADES**	Código: DE_IN_02 Versión: 14 Vigente desde: 05/04/2023

TABLA DE CONTENIDO

1. OBJETIVO

Ofrecer los lineamientos para emplear de forma adecuada la administración de riesgos y oportunidades de la entidad, como una herramienta conceptual y metodológica que contribuyan al control adecuado previniendo y mitigando los riesgos de gestión, corrupción y seguridad de la información que puedan afectar el logro de la misión y de los objetivos estratégicos y de los procesos de la entidad. De igual forma se brindan lineamientos para identificar las oportunidades y determinar las acciones para abordarlas.

2. ALCANCE

El presente instructivo aplica a los tres niveles de gestión: Central, Territorial y Local en cada uno de los procesos. Inicia con la identificación de la política de Administración de Riesgos, el contexto por proceso, continúa con el análisis, evaluación y identificación de los riesgos y termina con la valoración, monitoreo y seguimiento.

3. DEFINICIONES

Las definiciones que aplican para este instructivo corresponden a las presentes en el Procedimiento vigente administración de riesgos y oportunidades código DE_PR_01, capítulo 3. Definiciones.

4. LINEAMIENTOS GENERALES Y/O POLÍTICAS DE OPERACIÓN

- El Modelo Integrado de Planeación y Gestión – MIPG establece orientaciones para la administración de riesgos en las dimensiones: Direccionamiento Estratégico Evaluación de Resultados y Control Interno.
- Para estar conforme los requisitos de la norma ISO 9001:2015, una organización necesita diseñar, planificar e implementar acciones para abordar los riesgos y las oportunidades.
- El mapa de riesgos es una herramienta metodológica con la información resultante de la gestión del riesgo, facilita la identificación de los controles, tratamiento de riesgos (acciones de control), del monitoreo y revisión, a cargo de las tres líneas de defensa.
- Las responsabilidades sobre la administración y tratamiento de los riesgos en Parques Nacionales Naturales de Colombia se encuentran definidas en la Política vigente de Administración Integral de Riesgos documentada en el Procedimiento vigente Administración de Riesgos y Oportunidades código DE_PR_01.
- Para el desarrollo de la administración de riesgos se debe tener en cuenta los siguientes documentos:
  - Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de gestión, corrupción y seguridad digital. Dirección de Gestión y Desempeño Institucional. Función Pública. Versión 4 (riesgos de Corrupción) y Versión 5 (riesgos de Gestión y seguridad de la información), octubre 2018 y diciembre 2020.
  - Norma Técnica Colombiana NTC ISO 9001 en su versión vigente
  - Norma Técnica Colombiana NTC ISO 27001 en su versión vigente
  - Guía Estrategias para la construcción del Plan Anticorrupción y de Atención al Ciudadano, Versión 2. 2015.

- Las tres líneas de defensa tienen el rol de identificar la materialización del riesgo y en caso que sea la primera o segunda línea de defensa, deben informar a la tercera línea de defensa y poner en acción inmediatamente los controles de corrección y proceder teniendo en cuenta lo descrito en el Procedimiento vigente Administración de riesgos y oportunidades código DE_PR_01 – capítulo 6.2. Materialización de Riesgos.
- Los riesgos de corrupción no poseen controles correctivos, dado que su actuar inmediato en caso de materialización es informar al Grupo de Control Interno y Oficina de Control Disciplinario Interno para la toma de acciones según corresponda, conforme el procedimiento vigente Administración de riesgos y oportunidades DE_PR_01 capítulo 6.2. Materialización de riesgos.
- Documentar por parte de cada proceso, la hoja denominada “control de Cambios” dentro del formato vigente Mapa de riesgos DE_FO_02 y matriz de oportunidades DE_FO_11, describiendo el cambio o modificación realizada en los riesgos u oportunidad, de cada proceso, solo aplica para las modificaciones dentro del año, no para el mapa de riesgos a inicio de año.

5. DESARROLLO

El presente instructivo da respuesta a la entrada en vigencia del Modelo Integrado de Planeación y Gestión MIPG, el cuál surge de la integración de los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad en un solo sistema de gestión y en articulación de esté con el Sistema de Control Interno (Modelo Estándar de Control Interno – MECI), el cual se actualiza y alinea con los mejores estándares internacionales, como son el modelo COSO 2013, COSO ERM 2017 y el modelo de las tres líneas de defensa, el tema de riesgos. Lo anterior, con el fin de entregar a los ciudadanos lo mejor de la gestión y, en consecuencia, producir cambios en las condiciones de vida, mayor valor público en términos de bienestar, prosperidad general y fortalecer la lucha contra la corrupción. (Pública, 2018).

En tal sentido PNNC genera el presente instructivo conformado principalmente por los siguiente capítulos para la administración de riesgos: identificación, análisis, evaluación, tratamiento del riesgo y las actividades necesarias para las respectivas actualizaciones cuando apliquen y por temas tales como:

- Resultado de eficacia de las acciones de control implementadas, teniendo en cuenta los avances reportados, las evidencias de soporte y el informe de seguimiento al monitoreo generado por el Grupo de Control Interno.
- Cumplimiento del porcentaje de avance de cada una de las acciones de control planteadas de acuerdo al peso asignado.

5.1. ADMINISTRACIÓN DE RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DE LA INFORMACIÓN

Para dar inicio a la administración de riesgos de gestión, corrupción y seguridad de la información, se debe desarrollar la metodología presente en la Guía para la administración del riesgo y el diseño de controles en entidades pública, 2020– DAFP versión 5, documentada antes del capítulo que posee el primer paso de la administración de riesgos.

Antes de iniciar es necesario hacer referencia a dos orientaciones: la primera es el conocimiento de la Entidad, en términos de su misión, visión, objetivos estratégicos y planeación institucional y la segunda, es el modelo de operación por procesos, conformado por las caracterizaciones de los procesos, sus objetivos y los planes, programas o proyectos asociados. Esto con el fin determinar el análisis de riesgos y la aplicación del presente instructivo en general.

5.2. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

La política de administración de riesgos, se define como la declaración de la dirección y las intenciones generales de la entidad con respecto a la gestión del riesgo. Estableciendo lineamientos precisos acerca del tratamiento, manejo,

seguimiento a los riesgos, por lo cual la política debe contener los siguientes aspectos (Ver. **Ilustración 2.** Aspectos a tener en cuenta en la Política de Administración de Riesgos) y debe ser publicada y divulgada a las partes interesadas.

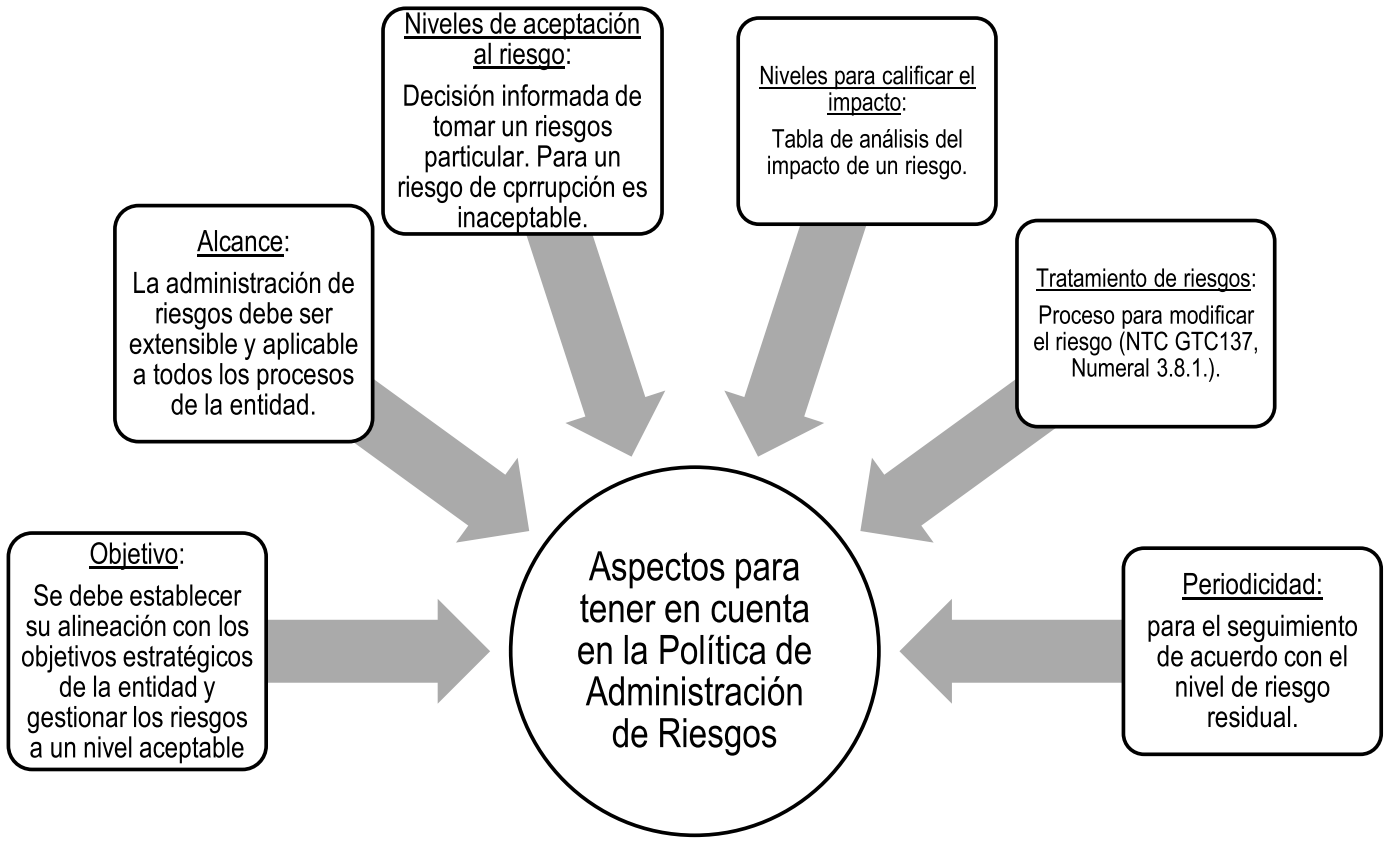

Ilustración 1. Aspectos a tener en cuenta en la Política de Administración de Riesgos

5.3. IDENTIFICACIÓN DE RIESGOS

En este componente se establecen las fuentes o factores que pueden generar un riesgo, los eventos, sus causas y consecuencias de acuerdo con las siguientes actividades:

5.3.1. Establecimiento del contexto

Se refiere a determinar los factores que afectan positiva o negativamente el cumplimiento de la misión y los objetivos del plan estratégico institucional y de los procesos de Parques Nacionales Naturales de Colombia, por lo cual es punto de partida del análisis de riesgos (gestión, corrupción, seguridad de la información y otros) dado que permite la identificación de las posibles causas que permitirían el evento de un riesgo.

Contexto externo: Se determinan las características o aspectos esenciales del entorno en el cual opera la entidad. Se pueden considerar factores como: económicos y financieros, sociales, culturales, políticos, tecnológicos, ambientales, físicos, cadena de suministro, mercado y demanda pública y legales y reglamentarios que afectan de forma positiva o negativa a la entidad **(oportunidades** (factores positivos que permiten el desarrollo de la entidad) **y amenazas (**Factores que representen algún tipo de amenaza y/o limitación para los propósitos institucionales**).**

Algunas de las preguntas que se pueden realizar al momento de analizar el **contexto externo** son:

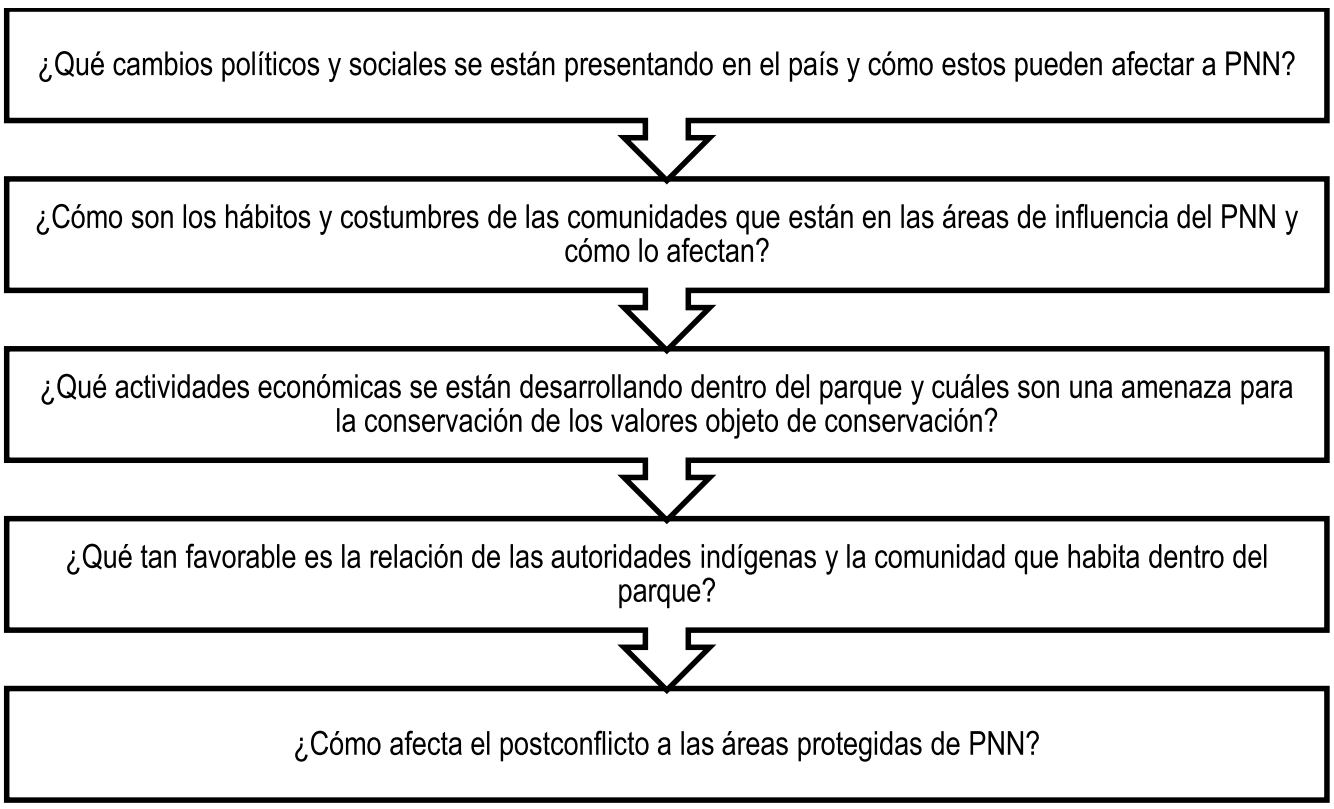

Ilustración 2. Preguntas de contexto externo

Para determinar el contexto externo, se debe considerar, sin limitarse, los siguientes **factores relacionados** con el **entorno digital**:

- Clientes, proveedores de servicios y empresas que sean competencia directa y/o se relacionen con la misión de la entidad pública analizada.
- Normativas o aspectos jurídicos que apliquen directa o indirectamente a la entidad pública; ejemplo, la ley 1581 de 2012 o la ley 1712 de 2014, circulares o regulaciones emitidas por superintendencias o ministerios, como el decreto 1078 de 2015 o el decreto 1499 de 2017.
- Dependencias económicas y financieras de otras empresas.
- Entorno cultural.
- Cualquier otro factor externo de tipo internacional, nacional (gobierno) regional o local.
- Cantidad de ciudadanos a los cuales la entidad pública brinda servicios a través del entorno digital como trámites a través de páginas web.
- Aspectos externos que pueden verse afectados con los riesgos de seguridad digital, tales como el ambiente social, económico y ambiental que tengan alguna relación con las operaciones asociadas a la entidad pública.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones.

Contexto interno: Se determinan las características o aspectos esenciales en los cuales la Entidad busca alcanzar sus objetivos. Se pueden considerar factores como: el cumplimiento de metas y planes, funciones y políticas, gobernanza y estructura de la organización, recursos humanos y económicos, procesos y procedimientos, relaciones con las partes interesadas y/o grupos de valor, conformidad legal, capacidad y habilidad, relaciones con las partes interesadas internas, subsistemas de gestión y normas, estilo y cultura de la organización, contratos, sistemas de información, que afectan positiva o negativamente a la entidad **(fortalezas y debilidades).** Así mismo se pueden considerar factores financieros, de tecnología, estratégicos y comunicación interna.

Algunas de las preguntas que se pueden realizar al momento de analizar el **contexto interno** son:

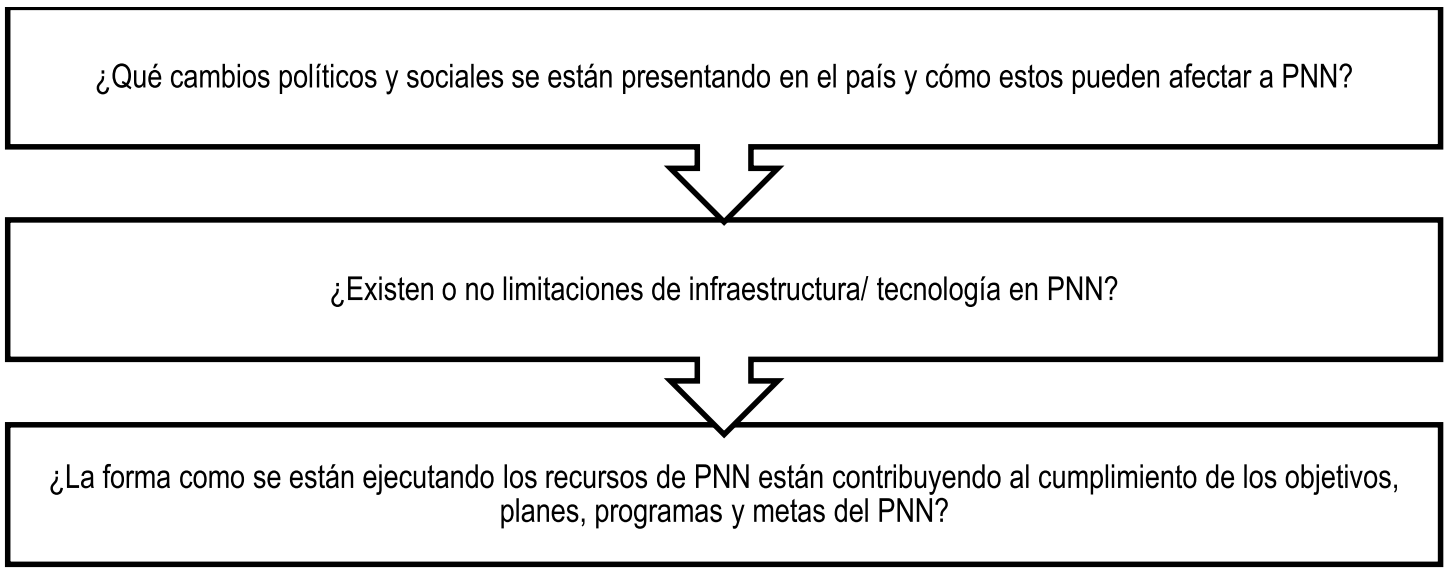

Ilustración 3. Preguntas de contexto interno

Contexto del proceso: Se determinan las características o aspectos esenciales del proceso y sus interrelaciones. Se pueden considerar factores como: para el análisis del contexto de los procesos se tendrá en cuenta los siguientes factores: diseño del proceso, interacciones con otros procesos, transversalidad, procedimientos asociados, responsables, comunicación entre los procesos y activos de seguridad digital.

Para determinar los factores de la entidad pública y los procesos se debe considerar, sin limitarse, los siguientes factores relacionados con el entorno digital:

Para la Entidad Pública	Para los Procesos
• Recursos económicos, sociales, ambientales, físicos, tecnológicos, financieros, jurídicos, entre otros. • Flujos de información y los procesos de toma de decisiones. • Empleados, contratistas. • Objetivos estratégicos y la forma de alcanzarlos. • La misión, visión, valores y cultura de la organización. • Sus políticas, procesos y procedimientos. • Sistemas de gestión (calidad, seguridad en el trabajo, seguridad de la información, riesgos, entre otros) • Toda la estructura organizacional. • Roles y responsabilidades. • Sistemas de información o servicios.	• Identificación de los procesos y su respectiva caracterización. • Detalle de las actividades que se llevan a cabo en el proceso. • Flujos de información. • Identificación y actualización de los activos en la cadena de valor de la entidad pública. • Recursos. • Alcance del proceso. • Relaciones con otros procesos de la entidad pública. • Cantidad de ciudadanos afectados por el proceso. • Procesos de gestión de riesgos que se tienen actualmente implementados. • Personal involucrado en la toma de decisiones.

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones.

A continuación, se relaciona la descripción de cada factor para cada tipo de contexto:

Tabla N.º 1. Factores internos y externos

	Factor	Descripción
CONTEXTO EXTERNO	**Económicos y Financieros**	Disminución del presupuesto por prioridades del gobierno, austeridad de gastos, disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.
	Político	Cambio de gobierno, legislación, políticas públicas, regulación, falta de continuidad de los programas establecidos.
	Legal y reglamentarios	Normatividad externa (leyes, decretos, ordenanzas y acuerdos), cambios legales y normativos que pueden afectar la misión y visión de la entidad.
	Social y culturales	Relacionamiento de la entidad con las partes interesadas: CARs, comunidades, entidades departamentales, municipales, ONGs, instituciones y grupos al margen de la demografía, responsabilidad social, orden público, también hace parte el orden público.
	Tecnológicos	Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.
	Ambientales	Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
	Otro	Otro Factor interno no identificado en el listado pero que puede estar presente en el contexto.
CONTEXTO INTERNO	**Personal**	Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.
	Procesos	Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento dentro de la entidad.
	Tecnología	Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información. (Disponibilidad de recursos tecnológicos (hardware y software) que permiten el acceso a los diferentes sistemas de información internos y externos, tales como aplicativos internet, intranet, servidores entre otros).
	Estratégicos	Lineamientos en cuanto a la planeación estratégica de la entidad, estructura organizacional, seguimiento de las metas y objetivos institucionales, informes de gestión.
	Comunicación interna	Canales utilizados y su efectividad, flujo de información necesaria para el desarrollo de las operaciones.
	Financieros	Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
	Otro	Otro Factor interno no identificado en el listado pero que puede estar presente en el contexto.
CONTE	**Diseño del proceso**	Claridad en la descripción del alcance y objetivo del proceso.

	Factor	Descripción
	Interacción con otros procesos	Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
	Transversalidad	Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
	Procesos Asociados	Pertinencia en los procedimientos que desarrollan los procesos.
	Responsables del proceso	Grado de autoridad y responsabilidad de los funcionarios frente al proceso.
	Comunicación entre los procesos	Efectividad en los flujos de información determinados en la interacción de los procesos.
	Activos de seguridad digital del proceso	Información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano. Ver conceptos básicos relacionados con el riesgo de seguridad digital en el Instructivo vigente de administración de riesgos.
	Otro	Otro Factor interno no identificado en el listado pero que puede estar presente en el contexto.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades pública, 2018 - DAFP.

El formato vigente Mapa de riesgos de gestión, corrupción y seguridad de la información Código: DE_FO_02, existe la pestaña denominada "**Análisis del contexto**" que permite realizar su identificación mediante la herramienta DOFA (debilidades, oportunidades, fortalezas y amenazas) teniendo en cuenta los procesos, el cual podrá ser actualizado de forma anual y/o cada vez que se presente un cambio.

El análisis DOFA se realiza por proceso, para lo cual es necesario tener en cuenta los planes de manejo de las Áreas protegidas en los que se identifica factores aplicables para algunos procesos y las características especiales de cada Dirección Territorial; teniendo presente que la entidad emplea para la planeación estratégica institucional el consolidado de la DOFA cuando es requerido.

Para los **riesgos de corrupción** es necesario tener en cuenta algunos factores del contexto, tales como:

En el **contexto interno**: espacios de discrecionalidad (toma de decisiones con cierta autonomía), fallas en el diseño de los procesos, normatividad compleja, excesivos costos administrativos, débiles sistemas de información, inadecuada selección de personal, ausencia de manuales, tecnología obsoleta o carente de controles, entre otros.

Por otra parte, en el **contexto externo** se deben considerar las amenazas del entorno que pueden incidir en el uso del poder para beneficio de un privado: la intervención de carteles de contratistas, organizaciones delictivas, grupos armados, participación y control social débiles, fragilidad en el control externo, recursos públicos no regulados efectivamente, entre otros.

Para los **riesgos de seguridad de la información** es necesario tener en cuenta la identificación de activos de información:

Se realizará a partir del análisis de los objetivos estratégicos y de los procesos, teniendo en cuenta que un activo es cualquier elemento que tenga valor para PNNC, sin embargo, en el contexto de seguridad digital son activos elementos tales como aplicaciones de la entidad pública, servicios Web, redes, información física o digital, Tecnologías de la Información - TI- o Tecnologías de la Operación -TO- que utiliza PNNC para su funcionamiento.

Es necesario que se identifiquen los activos y documente un inventario de activos, así podrá saber lo que se debe proteger para garantizar tanto su funcionamiento interno (BackOffice) como su funcionamiento de cara al ciudadano (FrontOffice), aumentando así su confianza en el uso del entorno digital para interactuar con el Estado.

La identificación y valoración de activos debe ser realizada por la Primera Línea de Defensa – Líderes de Proceso en cada proceso donde aplique la gestión del riesgo de seguridad digital, de acuerdo a las orientaciones del Grupo de Sistemas de Información y las Radiocomunicaciones - GTIC.

Para la generación de este inventario, PNNC debe tener en cuenta los siguientes pasos:

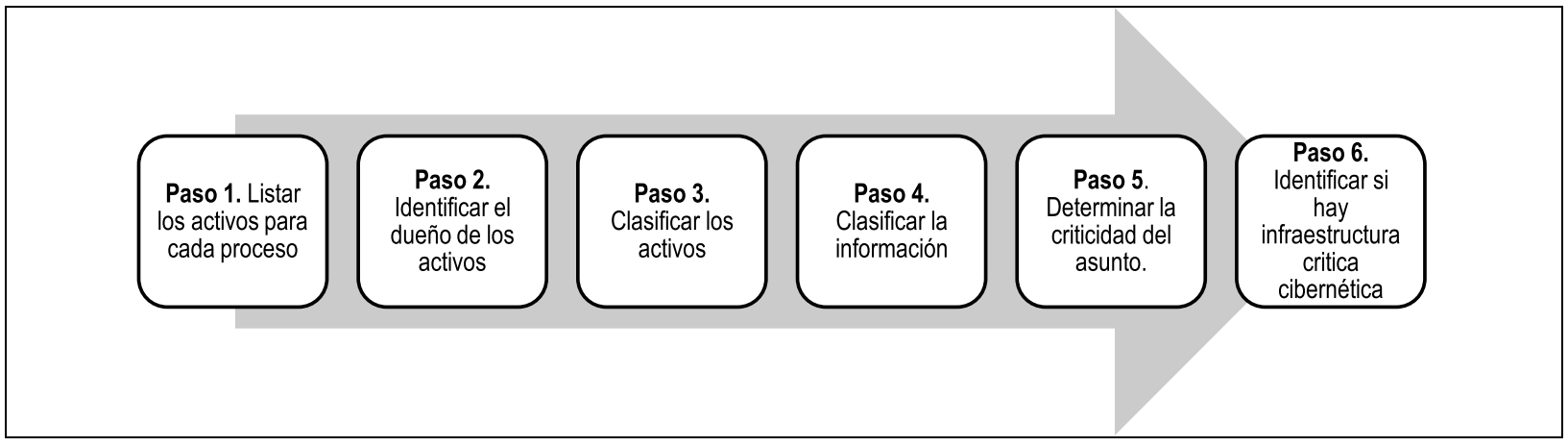

Ilustración 4. Pasos para identificar los activos

Las identificaciones de los activos de información se diligenciarán en la pestaña denominada “Activos de información” en el formato Mapa-de-riesgos de gestión, corrupción y seguridad de la información Código: DE_FO_02 y matriz-de-oportunidades código DE_FO_11, lo cual se realizará de la siguiente forma:

- **Proceso**: Selección del proceso dueño del activo de la información.
- **Riesgos**: Redacción del riesgo asociado a los activos, amenazas, vulnerabilidades, criticidad entre otros.
- **Activo**: Contiene información, la cual posee un valor y es necesario para llevar a cabo los procesos misionales y de soporte de la entidad.
- **Descripción**: Característica que define el tipo de activo conforme a la clasificación realizada.
- **Dueño del Activo**: Rol que tiene como responsabilidad velar por la protección del activo de seguridad digital.
- **Tipo de Activo**: Elemento o Activo a considerar dentro del proceso de gestión de riesgos.
- **Amenazas**: Causa potencial de un incidente no deseado, el cual puede causar daño a un sistema o a la entidad.
- **Vulnerabilidades:** Es la potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre un activo.

- **Ley 1712 de 2014**: Ley de trasparencia y de acceso a la información pública nacional Decreto 1078 de 2015 Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **Ley 1581 de 2021**: Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Criticidad Respecto a su confidencialidad**: Capacidad de divulgar información a individuos, entidades, procesos que no están autorizados.
- **Completitud o Criticidad Respecto a su Confidencialidad**: Capacidad para no proteger o divulgar la información de la entidad.
- **Completitud o Criticidad Respecto a su Disponibilidad**: Capacidad para no dejar disponible o utilizable la información a la entidad.
- **Nivel De Criticidad**: Indica que tan crítico es el riesgo al tener en cuenta su probabilidad de ocurrencia y su impacto, convirtiéndose en un criterio que permite priorizar los riesgos que se requieren gestionar.

Una vez se ejecute la identificación de los activos, la entidad definirá si gestionará los riesgos en todos los activos del inventario o solo en aquellos que tengan un nivel de criticidad Alto, esto debe estar debidamente documentando y aprobado por la Línea Estratégica – Alta dirección.

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización, identificar los activos se debe determinar las amenazas (comunes o dirigidas por el hombre) y reportarlas en el correspondiente cuadro de la pestaña “Activos de información” en el formato Mapa-de-riesgos de gestión, corrupción y seguridad de la información Código: DE_FO_02 y DE_FO_11-matriz-de-oportunidades; para ellos emplear las tablas.

Tabla N.º 2. Amenazas comunes

Tipo	Amenaza	Origen
Daño físico	Fuego	F,D,A
	Agua	F,D,A,
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
Pérdida de los servicios esenciales	Falla en el sistema de suministro de agua	E
	Falla de suministro de aire acondicionado	F,D,A,
Perturbación debida a la radiación	Radiación electromagnética	F,D,A,
	Radiación térmica	F,D,A,
Compromisos de la información	Interceptación de servicios de señales de interferencia comprometida	D
	Espionaje remoto	D

Tipo	Amenaza	Origen
Fallas técnicas	Fallas del equipo	D,F
	Mal funcionamiento del equipo	D,F
	Saturación del sistema de información	D,F
	Mal funcionamiento del software	D,F
	Incumplimiento en el mantenimiento del sistema de información	D,F
Acciones no autorizadas	Uso no autorizado del equipo	D,F
	Copia fraudulenta del software	D,F
Compromiso de las funciones	Error en el uso o abuso de derechos	D,F
	Falsificación de derechos	D

Fuente: ISO/TEC 27005-2009 – Anexo 4. Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas.

Tabla N.º 3 Amenazas dirigidas por el hombre

Fuente de amenaza	Motivación	Acciones amenazantes
Pirata informático, intruso ilegal	Reto Ego	Piratería Ingeniería Social
Criminal de la computación	Destrucción de la información Divulgación ilegal de la información.	Crimen por computador Acto fraudulento
Terrorismo	Chantaje Destrucción	Ataques contra el sistema DDos Penetración en el sistema
Espionaje industrial (inteligencia, empresas, gobiernos extranjeros, otros intereses)	Ventaja competitiva Espionaje económico	Ventaja de defensa Hurto de la información
Intrusos (empleados)	Curiosidad	Asalto a un empleado
Entrenamiento, deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Ganancia monetaria	Chantaje

Fuente: ISO/TEC 27005-2009 – Anexo 4. Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas.

Identificar las vulnerabilidades para los activos y amenazas determinadas en el correspondiente cuadro de la pestaña “Activos de información” en el formato Mapa-de-riesgos de gestión, corrupción y seguridad de la información Código: DE_FO_02 y DE_FO_11-matriz-de-oportunidades; para ello emplear la siguiente tabla.

Tabla N.º 4 Tabla de vulnerabilidades comunes

Tipo	Vulnerabilidades
Hadware	Mantenimiento insuficiente
	Ausencia de esquema de reemplazo periódico
	Sensibilidad a la radiación electromagnética
	Susceptibilidad a las variaciones de temperatura (o al polvo suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no controlada
Software	Ausencia o insuficiencia de pruebas de software
	Ausencia de terminación de sesión
	Ausencia de registros de auditoria
	Asignación errada de los derechos de acceso
	Interfaz del usuario compleja
	Ausencia de documentación
	Fechas incorrectas
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseñas sin protección
	Sotware nuevo o inmaduro
Red	Ausencia de pruebas de envío o recepción de mensaje
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia de personal
	Entrenamiento insuficiente
	Falta de conciencia en seguridad
	Ausencia de políticas de uso aceptable
	Trabajo no supervisado de personal externo o de limpieza

Tipo	Vulnerabilidades
Lugar	Uso inadecuado de los controles de acceso al edificio
	Áreas susceptibles a inundación
	Red electica inestable
	Ausencia de protección en puertas y ventanas
Organización	Ausencia de procedimiento de registro / retiro de usuarios
	Ausencia de proceso para supervisión de derechos de acceso
	Ausencia de control de los activos que se encuentran fuera de las instalaciones.
	Ausencia de acuerdo de nivel de servicio (ANS o SLA)
	Ausencia de mecanismos de monitoreo para brechas en la seguridad.
	Ausencia de procedimientos y/o políticas en general (esto aplica para muchas actividades que la entidad no tenga documentadas y formalizadas como uso aceptable de activos, control de cambios, valoración de riesgos, escritorio y pantalla limpia entre otros)

Fuente: ISO/TEC 27005-2009 – Anexo 4. Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas.

5.3.2. Identificación del riesgo

El propósito es determinar las causas con base en el contexto interno, externo y del proceso que pueden afectar el logro de los objetivos. Algunas causas externas no controlables por la entidad se podrán evidenciar en el análisis del contexto externo, para tener en cuenta en el análisis y valoración del riesgo.

A partir del análisis del contexto de cada uno de los procesos, se identifican y definen las situaciones de riesgo de la gestión, corrupción y seguridad de la información que pueden afectar el desarrollo de los objetivos del proceso o los estratégicos.

Posteriormente se describe la forma como se documenta la identificación del riesgo en el formato DE_FO_02 Mapa de riesgos.

Las preguntas claves para la identificación del **riesgo de gestión**:

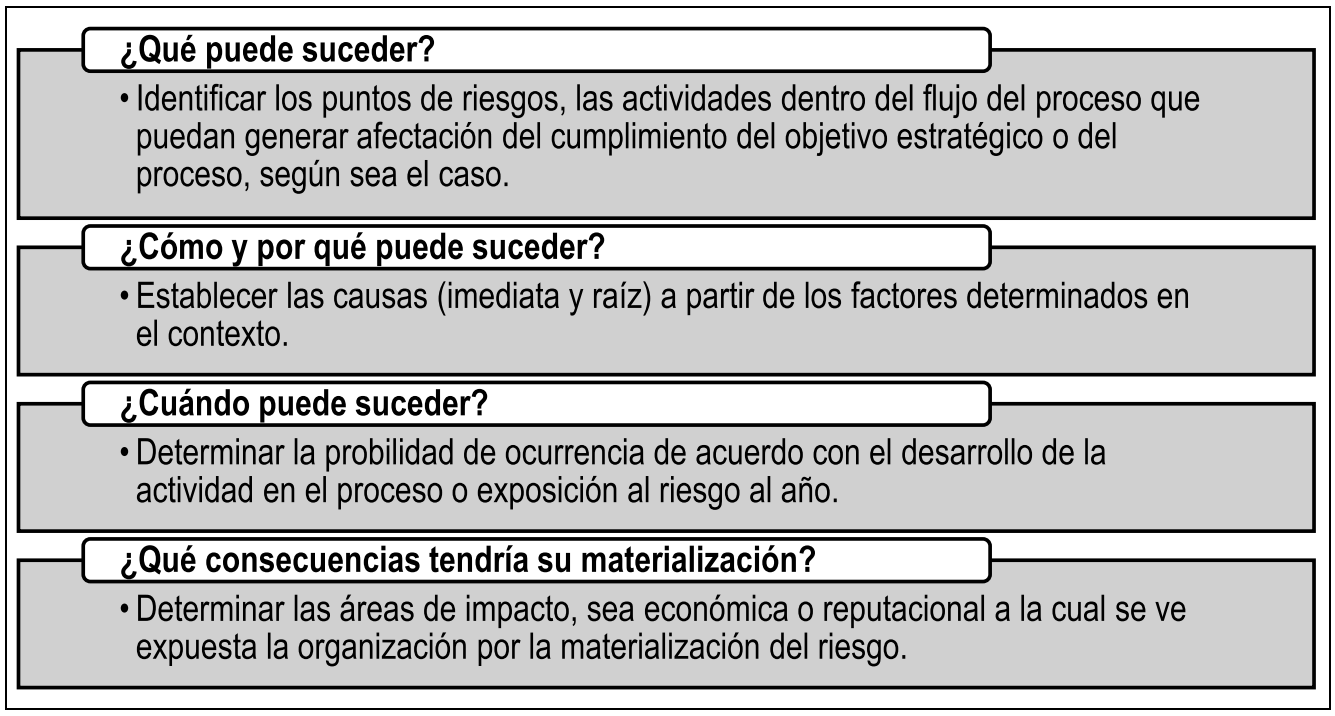

Ilustración 5. Preguntas clave para la identificación de riesgos

Para facilitar el proceso de identificación de los riesgos se recomienda tener en cuenta el conocimiento previo de aquellas situaciones que puedan obstaculizar el cumplimiento de los objetivos, la obtención de un resultado, la generación de procesos transparentes, el cumplimiento de requisitos legales o la satisfacción del usuario.

Para la identificación del riesgo de **gestión o seguridad de la información,** es necesario definir los siguientes parámetros:

- Contener todos los detalles que sean necesarios y que sean fácil de entender tanto por el Líder del proceso como para las personas ajenas al proceso.
- Iniciar con la frase POSIBILIDAD DE.
- Redacción que permite dar respuesta a la sumatoria de: ¿Qué? (impacto), ¿Cómo? (Causa inmediata) y ¿Por qué? (causa raíz incluye sub causas si aplica).
- Evitar la subjetividad y permitir entender cómo se puede manifestar el riesgo, así como su causa inmediata y causa raíz.
- No describir como riesgos omisiones ni desviaciones de control.
- No describir causas como riesgos.
- No describir riesgos como la negación de un control.

En lo que respecta a **los riesgos de corrupción** es recomendable realizar un análisis de hechos de corrupción presentados en los últimos años en la entidad, quejas, denuncias e investigaciones adelantadas; así como los actos de corrupción presentados en entidades similares. Así mismo se considera en el análisis los resultados de auditorías internas, externas y fiscales.

Su identificación debe evitar que se presenten confusiones y se debe utilizar la matriz “definición del riesgo de Corrupción” (Fuente: Secretaria de Transparencia de la Presidencia de la República), presente en el capítulo 2.2. Identificación del Riesgo, en la Guía para la administración del riesgo y el diseño de controles en entidades pública, 2018 – DAFP, vigente para riesgos de corrupción, la cual incorpora cada uno de los componentes de su contexto.

Si en la descripción del riesgo, las casillas son contestadas todas afirmativamente (es decir con una equis), en la matriz de definición del riesgo de corrupción, se trata de un riesgo de corrupción.

Se señalan algunos de los procesos y procedimientos susceptibles de actos de corrupción a partir de los cuales se puede identificar **riesgos de corrupción**, presente en el capítulo 2.2.2, Identificación del Riesgo, en la Guía para la administración del riesgo y el diseño de controles en entidades pública, 2018 – DAFP, vigente para riesgos de corrupción.

Durante el proceso de identificación del riesgo se puede hacer una "clasificación del riesgo", con el fin de establecer con mayor facilidad el análisis del impacto, tener presente que esta clasificación es independiente del riesgo (gestión, corrupción y seguridad de la información). Para la clasificación básica para **riesgos de Corrupción** tener presente la tabla 2.2.2, Tipología de riesgos, en la Guía para la administración del riesgo y el diseño de controles en entidades pública, 2018 – DAFP, vigente para riesgos de corrupción y para los **riesgos de gestión y seguridad de la información** tener presente la tabla 2. Clasificación del riesgo, en el capítulo 2.6., Clasificación del riesgo, en la Guía para la administración del riesgo y el diseño de controles en entidades pública, 2020 – DAFP, vigente para riesgos de gestión.

5.3.3. Documentación de la identificación del riesgo

5.3.3.1. Riesgos de gestión – Seguridad de la Información.

A continuación, se relaciona los pasos a realizar para la identificación de riesgos, en el formato vigente Mapa de riesgos de gestión, corrupción y seguridad de la información Código: DE_FO_02, pestañas Riesgos de Gestión.

Paso 1. Seleccionar el proceso de acuerdo con el mapa de procesos. **Nota**. El número del riesgo será asignado en el momento de la consolidación de los riesgos, por la Oficina Asesora de Planeación y dado que los riesgos de Gestión, corrupción y seguridad de la información se registran en hojas independientes y poseen numeración independiente.

Paso 2. Área de Impacto de la Entidad: Identifique el impacto al cual está expuesta la entidad en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional, o los dos casos.

Paso 3. Registre la causa inmediata, como aquellas circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.

Paso 4. Registre la causa(s) raíz, la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo pueden existir más de una causa o subcausas que pueden ser analizadas. Consecuencia(s) que se pueden presentar en caso de materialización del riesgo.

Paso 5. Identifique el riesgo Iniciando con la frase POSIBILIDAD DE (área de impacto de la Entidad), POR (Causa raíz), DEBIDO A (dando respuesta a lo que puede ocurrir (Impacto + causa inmediata) + causa(s) raíz (riesgo)), para este paso se debe tener en cuenta el concepto de riesgo de gestión y seguridad de la información presentes en el capítulo 3 Definiciones y los lineamientos de redacción del capítulo 5.3.2., al igual la siguiente estructura.

Nota. Las palabras en mayúscula son conectores obligatorios que deben estar presente en la redacción del riesgo.

Ilustración 6. Estructura de la redacción de un riesgo

Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Paso 6. Clasificación del riesgo: Con el objetivo de agrupar los riesgos identificados seleccionar la categoría correspondiente teniendo presente la tabla 2. Clasificación del riesgo, en el capítulo 2.6., Clasificación del riesgo, en la Guía para la administración del riesgo y el diseño de controles en entidades pública, 2020 – DAFP, vigente para riesgos de gestión.

5.3.3.2. Riesgos de corrupción

A continuación, se relaciona los pasos a realizar para la identificación de riesgos, en el formato vigente Mapa de riesgos de gestión, corrupción y seguridad de la información Código: DE_FO_02, pestaña “Riesgos corrupción”.

Paso 1. Seleccionar el proceso de acuerdo con el mapa de procesos. **Nota**. El número del riesgo será asignado en el momento de la consolidación de los riesgos, por la Oficina Asesora de Planeación y dado que los riesgos de Gestión, corrupción y seguridad de la información se registran en hojas independientes y poseen numeración independiente.

Paso 2. Registre el objetivo del proceso de acuerdo con la caracterización vigente del proceso.

Paso 3. Registre el riesgo específico para el proceso en la casilla “riesgo”, para este paso se debe tener en cuenta el concepto de riesgo de gestión y seguridad de la información presentes en el capítulo 3 Definiciones y los lineamientos de redacción del capítulo 5.3.2. – Riesgos de corrupción, la redacción debe iniciar con “posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de” seguido por la actividad o acción respuesta a lo que puede ocurrir (riesgo).

Paso 4. Identifique el nivel de gestión en el cual se pudiese llegar a materializar el riesgo, el cual puede ser nivel central, dirección territorial y área protegida, solo en conjunto.

Paso 5. Descripción del riesgo: De manera breve ampliar la información relacionada con el riesgo de tal forma que permita tener una mayor comprensión al lector del riesgo identificado.

Paso 6. Establecer las causas: Determinar los agentes generadores del riesgo, teniendo en cuenta que las causas son medios, circunstancias, situaciones o agentes generadores del riesgo y son parte del contexto identificado previamente en el proceso.

Es importante tener en cuenta que en el mapa de riesgos se debe registrar únicamente las causas que realmente origina el riesgo y pueden ser controladas por el proceso y/o entidad, ya que se pueden identificar muchas causas, pero solo algunas de ellas conllevan a la materialización del riesgo (como mínimo una causa).

IMPORTANTE

- La(s) causa(s) debe estar asociada(s) directamente al riesgo.
- Para definir las causas es importante realizar el ejercicio con las personas que manejan la temática asociada con el riesgo identificado, es decir con los responsables del monitoreo conforme la segunda línea de defensa, lo cual se reflejará en la actualización del contexto.

Paso 7. Efecto/Consecuencia: Efectos generados por la ocurrencia de un riesgo que afecta los objetivos estratégicos o un proceso de la entidad. Normalmente estas consecuencias están asociadas con pérdidas económicas, daños físicos, deterioro de la imagen corporativa, interrupción del servicio, desconfianza de las partes interesadas, impacto sobre los valores objeto de conservación, efectos sociales, entre otros.

Paso 8. Tipología de Riesgo: Seleccionar de acuerdo con el riesgo identificado, clasificar teniendo presente la tabla 2.2.2, Tipología de riesgos, en la Guía para la administración del riesgo y el diseño de controles en entidades pública, 2018 – DAFP, vigente para riesgos de corrupción.

5.3.4. VALORACIÓN DEL RIESGO

El paso de valoración del riesgo incluye dos etapas que la desarrollan: el análisis y la evaluación de los riesgos que se describen a continuación:

5.3.4.1. Análisis del riesgo – Riesgo de Gestión – Seguridad de la información

El propósito de este componente es establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial **(riesgo inherente),** es decir calificar el riesgo identificado antes de aplicar los controles.

Para esto es necesario recordar los siguientes conceptos:

Paso 1. Frecuencia con la que se realiza la actividad, Determinar la probabilidad de ocurrencia mediante la identificación de la exposición al riesgo, por el número de veces que se pasa por el punto de riesgo en el periodo de 1 año, se registra el número de veces que desarrolla la actividad, empleando la tabla No 1 del procedimiento vigente Administración de riesgos y oportunidades código DE_PR_01.

Paso 2. Probabilidad Inherente, dado el resultado al paso anterior identifique en la primera columna de la Tabla 3. Criterios para definir el nivel de impacto – riesgos de gestión y seguridad de la información del procedimiento vigente Administración de riesgos y oportunidades código DE_PR_01. Criterios de para definir el nivel de probabilidad – riesgos de gestión y seguridad de la información y seleccione el nivel de probabilidad la cual automáticamente identifica el % de la siguiente columna.

Paso 3. Criterios de Impacto: Determinar el criterio de la afectación económica o reputacional, empleando la tabla 3. Criterios para definir el nivel de impacto – riesgos de gestión y seguridad de la información del procedimiento vigente Administración de riesgos y oportunidades código DE_PR_01, teniendo presente cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto. El diligenciamiento de esta casilla genera el reporte automático de las dos siguientes casillas, por lo cual determina el porcentaje y la Zona de Riesgo Inherente.

En la aplicación de los criterios para determinar el impacto de los riesgos de seguridad de la información se debe tener en cuenta que:

- Las variables confidencialidad, integridad y disponibilidad se definen de acuerdo con el modelo de seguridad y privacidad de la información de la estrategia de Gobierno Digital (GD) del Ministerio de Tecnologías de la Información y las Comunicaciones.
- La variable población se define teniendo en cuenta el establecimiento del contexto externo de la entidad, es decir, que la consideración de población va a estar asociada a las personas a las cuales se les prestan servicios o trámites en el entorno digital y que de una u otra forma pueden verse afectadas por la materialización de algún riesgo en los activos identificados. Los porcentajes en las escalas pueden variar, según la entidad y su contexto.
- La variable presupuesta es la consideración de presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal.
- La variable ambiental estará también alineada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital. Esta variable puede no ser utilizada en la mayoría de los casos, pero debe tenerse en cuenta, ya que en alguna eventualidad puede existir afectación ambiental.
- Para los riesgos de seguridad de la información la probabilidad y el impacto se determinan con base a la amenaza, no en las vulnerabilidades.

Fuente: Elaboración conjunta entre la Dirección de Gestión y Desempeño Institucional de Función Pública y el Ministerio TIC, 2018.

5.3.4.2. Análisis del riesgo – Riesgo de Corrupción

El propósito de este componente es establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial **(riesgo inherente),** es decir calificar el riesgo identificado antes de aplicar controles.

Paso 1. Identificar la Probabilidad a partir de las siguientes especificaciones, teniendo en cuenta la que más se asemeje a la realidad de la situación del riesgo, empleando la Tabla 2. Criterios para definir el nivel de probabilidad – riesgos de corrupción del procedimiento vigente Administración de riesgos y oportunidades código DE_PR_01.

Para este caso se analiza qué tan posible es que ocurra el riesgo, expresado en términos de **frecuencia** teniendo en cuenta el siguiente concepto:

- **Frecuencia**: implica analizar el número de eventos en un periodo determinado; se aplica para hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo.

Paso 2. Calificar el Impacto para la cual se tendrá en cuenta solamente los niveles “moderado”, “mayor” y “catastrófico”, dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, para esta actividad se contempla 19 preguntas estipuladas por el Departamento Administrativo de Función Pública -DAFP, dichas preguntas se deben responder en su totalidad, diligenciando con un 1 según el caso, en la columna “Si” o “No” en la hoja denominado “*Impacto R. Corrupción*” y conforme su respuesta se identifica el nivel de impacto para el riesgo, de la siguiente forma:

- Responder afirmativamente de UNA a CINCO preguntas (s) genera un impacto moderado.
- Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor.
- Responder afirmativamente de DOCE a DIECINUEVE preguntas (s) genera un impacto catastrófico.

Dentro del formato vigente DE_FO_02, la información correspondiente al impacto para un riesgo de corrupción se diligencia en la hoja denominado "*Impacto R. Corrupción*" y el resultado obtenido se debe diligenciar en la casilla denominada "impacto" del riesgo inherente, en la hoja "mapa de Riesgo".

Se presenta un ejemplo de calificación de las preguntas para determinar el impacto de los riesgos de corrupción, en la Tabla 4. Criterios para calificar el impacto en riesgos de corrupción, en el procedimiento vigente Administración de riesgos y oportunidades código DE_PR_01.

Paso 3. Zona del riesgo: conforme la calificación obtenida en probabilidad e impacto, identificar la calificación del riesgo inherente teniendo en cuenta el mapa de calor presente en la hoja denominada "Matriz RG-RC-RSD" en el formato vigente DE_FO_02 Mapa de riesgos, en la gráfica denominada "*Zona de riesgo - Riesgos de corrupción*".

A continuación, se presenta un ejemplo según la tabla probabilidad y el resultado obtenido de las preguntas de impacto, para un riesgo de corrupción se obtuvo posible y mayor respectivamente, se identifica una clasificación "extremo".

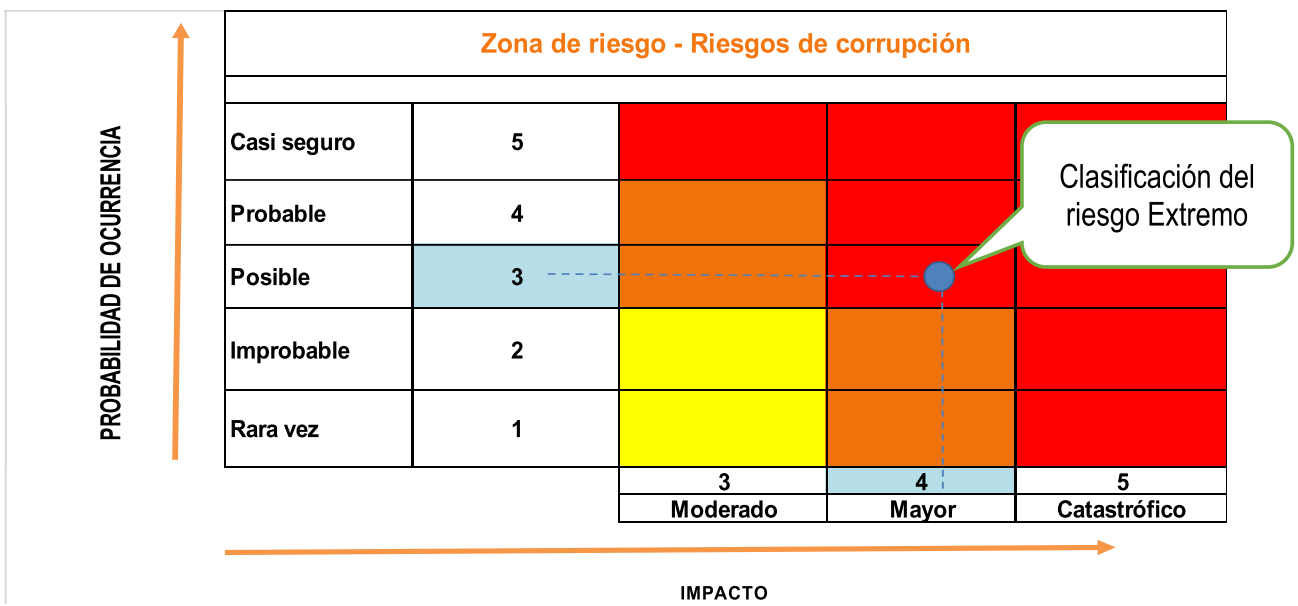

Ilustración 7. Ejemplo Clasificación del riesgo (probabilidad – impacto)

5.3.5. Evaluación del riesgo

El propósito de la valoración del riesgo es confrontar los resultados del análisis de riesgo inicial frente a los controles existentes establecidos, con el fin de determinar la zona de riesgo final (RIESGO RESIDUAL).

NOTA: Para cada riesgo se debe relacionar como mínimo un control y como máximo tres controles, por lo tanto, se deben priorizar los controles que contribuyen a evitar la materialización del riesgo.

Los siguientes pasos aplican para el diligenciamiento en el formato vigente Mapa de riesgos de gestión, corrupción y seguridad de la información Código: DE_FO_02, tanto para **los riesgos de gestión, corrupción y seguridad de la información**:

Tabla N.º 5. Pasos para establecer el control que mitigue el riesgo

Nº	INFORMACIÓN	DESCIPCIÓN
PASO 1	**Responsable**	Persona asignada para ejecutar el control. Debe tener la autoridad, competencias y conocimientos para ejecutar el control dentro del proceso y sus responsabilidades deben ser adecuadamente segregadas o redistribuidas entre diferentes individuos del proceso, para reducir así el riesgo de error o de actuaciones irregulares o fraudulentas. Si ese responsable quisiera hacer algo indebido, por sí solo, no lo podría hacer. Si la respuesta es que cumple con esto, quiere decir que el control está bien diseñado, si la respuesta es que no cumple, tenemos que identificar la situación y mejorar el diseño del control con relación a la persona responsable de su ejecución, por ejemplo: Profesional temático del AP, o GPM, entre otros. En caso de que sean controles automáticos se identificará el sistema que realiza la actividad. **NOTA.** Para los riesgos de gestión incluir en Nº de control.
PASO 2	**Periodicidad**	El control debe tener una periodicidad específica para su realización (diario, mensual, trimestral, anual, etc.) y su ejecución debe ser consistente y oportuna para la mitigación del riesgo.
PASO 3	**Propósito**	El control debe tener un propósito que indique para qué se realiza, y que ese propósito conlleve a prevenir las causas que generan el riesgo (verificar, validar, conciliar, comparar, revisar, cotejar) o detectar la materialización del riesgo, con el objetivo de llevar a cabo los ajustes y correctivos en el diseño del control o en su ejecución. El solo hecho de establecer un procedimiento o contar con una política por sí sola, no va a prevenir o detectar la materialización del riesgo o una de sus causas, adicionalmente informar el manejo de las desviaciones del control para mitigar los riesgos de corrupción.
PASO 5	**Cómo se realiza la actividad del control**	Indicar mediante verbos la acción del cómo se realiza, de tal forma que se pueda evaluar si la fuente u origen de la información que sirve para ejecutar el control es confiable para la mitigación del riesgo. Es necesario informar que se hace en caso de desviación de la actividad, es decir que no se cumpla la actividad.
PASO 6	**Evidencia de la ejecución del control**	El control debe dejar evidencia de su ejecución. Esta evidencia ayuda a que se pueda revisar como se llevó a cabo el control y evaluar que el control realmente fue ejecutado de acuerdo con los parámetros establecidos

NOTA. Para los riesgos con determinación como “Correctivos”, tener presente que estos controles corresponden a las acciones que se activan una vez el riesgo se materialice, las cuales son independientes de los lineamientos y políticas de operación contempladas en el procedimiento vigente Administración de riesgos y oportunidades código DE_PR_01, capítulo 6.2. Materialización de un riesgo.

5.3.5.1. Valoración de los controles – Riesgos de gestión y seguridad de la Información

Para la adecuada mitigación de los riesgos no basta con que un control esté bien diseñado, sino que este se debe ejecutar por parte del (los) responsable(s) tal como se formuló inicialmente y así contribuir en evitar la mitigación del riesgo.

Paso 7. Determinar la afectación del control: teniendo en cuenta la tipología de los controles determinar si estos afectan el impacto o probabilidad de un riesgo, y se recomienda conocer el ciclo del proceso y las tipologías de controles, para identificar si es un control preventivo, detectivo o correctivo.

Paso 8. Calificar cada uno de los atributos de los controles, seleccionado para cada una de las características de los atributos del diseño del control relacionados con eficiencia y la formalización como se puede observaren la tabla 6 atributos para el diseño del control, presente, en la Guía para la administración del riesgo y el diseño de controles en entidades pública, 2020 – DAFP, vigente para riesgos de gestión, teniendo presente que el diligenciamiento de estas casillas automáticamente genera la calificación de la Evaluación del Riesgo - Nivel del Riesgo Residual.

Para la aplicación de los controles se debe tener en cuenta que los estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control, es decir se toma el porcentaje de la probabilidad inherente y el porcentaje de del primer control se multiplica y su resultado es restado es restado al porcentaje de la probabilidad inherente y su valor se tomara como dato correspondiente al el porcentaje de la probabilidad inherente y así sucesivamente para determinar la *Probabilidad Residual*.

NOTA: Se recomienda tener presente que, en caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente, es importante señalar que no será posible su movimiento en la matriz para el impacto.

Paso 9. Identificar el tratamiento a desarrollar como estrategia para combatir el riesgo, a través de una decisión que se toma frente a un determinado nivel de riesgo, la cual puede ser aceptar, reducir o evitar. A partir del valor del riesgo residual y empleando la siguiente tabla. El tratamiento es por el riesgo.

Para identificar la estratégica para combatir el riesgo de gestión o seguridad de la información, emplear la Tabla 5. Estrategias para combatir los riesgos de gestión y de seguridad de la información, del procedimiento vigente Administración de riesgos y oportunidades código DE_PR_01.

5.3.5.2. Valoración de los controles – Riesgos de corrupción

Paso 7. Calificar el peso o participación de cada variable en el diseño del control para la mitigación del riesgo, para lo cual se realizará un análisis y evaluación del diseño de control, mediante la aplicación de (6) variables establecidas por el Departamento de la Función Pública – DAFP, con las preguntas y opciones de respuesta presentes en las tablas 6 (Análisis y evaluación de los controles para la mitigación de los riesgos) y 7 (Peso o participación de cada variable en el diseño del control para la mitigación del riesgo), en el capítulo 3.2., Evaluación de riesgos, en la Guía para la administración del riesgo y el diseño de controles en entidades pública, 2018 – DAFP, vigente para riesgos de corrupción.

Paso 8. Identifique el Rango de calificación del diseño del control,el resultado de estas seis (6) variables permite determinar si el control se encuentra bien diseñado, para lo cual se tiene en cuenta la siguiente calificación:

Tabla N.º 6. Resultados de la evaluación del diseño del control.

RANGO DE CALIFICACIÓN DEL DISEÑO DEL CONTROL	RESULTADO - PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
Fuerte	Calificación entre 96 y 100
Moderado	Calificación entre 86 y 95
Débil	Calificación entre 0 y 85

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2018 - DAFP.

Si el resultado de las calificaciones del control, o el promedio en el diseño de los controles, está por debajo de 96%, se debe establecer un plan de mejoramiento que permita tener un control o controles bien diseñados.

Paso 9. Determinar el Rango de calificación de la ejecución: Resultados de la evaluación de la ejecución del control, por parte de la primera línea de defensa debe asegurarse que el control se ejecute, por ende, al momento de determinar si el control se desarrolla, inicialmente, el responsable del proceso debe llevar a cabo una confirmación y posteriormente se confirma con las actividades de evaluación realizadas por la auditoría interna o control interno.

Tabla N.º 7. Resultados de la evaluación de la ejecución del control.

RANGO DE CALIFICACIÓN DE LA EJECUCIÓN	RESULTADO - PESO DE LA EJECUCIÓN DEL CONTROL
Fuerte	El control se ejecuta de manera consistente por parte del responsable
Moderado	El control se ejecuta algunas veces por parte del responsable.
Débil	El control no se ejecuta por parte del responsable

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades pública, 2018 - DAFP.

Paso 10. Determinar la Solidez individual de cada control. Dado que la calificación de los riesgos inherentes y residuales se efectúa al riesgo y no a cada causa, es necesario consolidar un conjunto de los controles asociados a la causa para evaluar estos de manera individual y en conjunto, ayudan al tratamiento de estos.

En la evaluación del diseño y ejecución de los controles, las dos variables son importantes y significativas en el tratamiento de los riesgos y sus causas, por lo que la calificación del control corresponde a las dos variables indicadas previamente, como se observa en la siguiente tabla.

Tabla N.º 8. Análisis y evaluación de los controles para la mitigación de los riesgos.

PESO DEL DISEÑO DE CADA CONTROL	PESO DE LA EJECUCION DE CADA CONTROL	SOLIDEZ INDIVIDUAL DE CADA CONTROL FUERTE:10 MODERADO:50 DEBIL:0	DEBE ESTABLECER ACCIONES PARA FORTALECER EL CONTROL SI / NO
	fuerte (siempre se ejecuta)	fuerte + fuerte = fuerte	No

PESO DEL DISEÑO DE CADA CONTROL	PESO DE LA EJECUCION DE CADA CONTROL	SOLIDEZ INDIVIDUAL DE CADA CONTROL FUERTE:10 MODERADO:50 DEBIL:0	DEBE ESTABLECER ACCIONES PARA FORTALECER EL CONTROL SI / NO
fuerte: calificación entre 96 y 100”	moderado (algunas veces)	fuerte + moderado = moderado	Si
	débil (no se ejecuta)	fuerte + débil = débil	Si
moderado: calificación entre 86 y 95	fuerte (siempre se ejecuta)	fuerte + fuerte = fuerte	Si
	moderado (algunas veces)	fuerte + moderado = moderado	Si
	débil (no se ejecuta)	fuerte + débil = débil	Si
débil: calificación entre 0 y 85	fuerte (siempre se ejecuta)	fuerte + fuerte = fuerte	Si
	moderado (algunas veces)	fuerte + moderado = moderado	Si
	débil (no se ejecuta)	fuerte + débil = débil	Si

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades pública, 2018 - DAFP.

Paso 11. Determinar la calificación de la solidez del conjunto de controles. Dado que un riesgo puede tener varias causas, a su vez varios controles y la calificación se realiza al riesgo, es importante evaluar el conjunto de controles asociados al riesgo.

La solidez del conjunto de controles se obtiene calculando el promedio aritmético simple de los controles por cada riesgo, es decir si tenemos dos controles para un riesgo y un control posee una calificación fuerte (100) y otro moderado (95) la suma de los dos nos generá que la calificación es moderado ((100+95)/2=97,5).

Tabla N.º 9. Calificación de la solidez del conjunto de controles.

CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE CONTROLES	
Fuerte	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100.
Moderado	El promedio de la solidez individual de cada control al sumarlos y ponderarlos está entre 50 y 99.
Debil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es menor a 50.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades pública, 2018 -DAFP.

Paso 12. Nivel de riesgo (riesgo residual) realizar un desplazamiento del riesgo inherente para calcular el riesgo residual. Esta etapa busca establecer tanto la probabilidad de ocurrencia del riesgo como la consecuencia o impacto final, teniendo en cuenta la calificación realizada a los controles existentes para gestionarlos e identificar el control que permite conocer el riesgo residual, para el cálculo del riesgo residual se realizará de acuerdo con la siguiente tabla, para la cual tenemos que identificar si la solidez de los controles me permite disminuir probabilidad e impacto, de forma directa (es decir fueron creados con este propósito) o inderecto (su propósito fue otro pero permite la dismunición de la probabilidad o el impacto):

Tabla N.º 10. Resultados de los posibles desplazamientos de la probabilidad y del impacto de los riesgos

SOLIDEZ DEL CONJUNTO DE LOS CONTROLES	CONTROLES AYUDAN A DISMINUIR LA PROBABILIDAD	CONTROLES AYUDAN A DISMINUIR IMPACTO	# COLUMNAS EN LA MATRIZ DE RIESGO QUE SE DESPLAZA EN EL EJE DE LA PROBABILIDAD	# COLUMNAS EN LA MATRIZ DE RIESGO QUE SE DESPLAZA EN EL EJE DE IMPACTO
Fuerte	directamente	directamente	2	2
Fuerte	directamente	indirectamente	2	1
Fuerte	directamente	no disminuye	2	0
Fuerte	no disminuye	directamente	0	2
moderado	directamente	directamente	1	1
moderado	directamente	indirectamente	1	0
moderado	directamente	no disminuye	1	0
moderado	no disminuye	directamente	0	1

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades pública, 2018 - DAFP.

Paso 13. Resultados del mapa de riesgo residual. Una vez realizado el análisis y evaluación de los controles para la mitigación de los riesgos, procedemos a determinar el valor del riesgo residual (después de los controles).

A continuación se presente un ejemplo, dentro del riesgo que se obtuvo un nivel inherente "*alto*" (resultado de una probabilidad "posible – 3" y un impacto "Moderado – 3", la solidez de los controles fue "fuerte" y se identificó que ayuda directamente a disminuir la probabilidad y no disminuye el impacto, por ende se desplazan dos ejes de la probabilidad y cero en el impacto, conforme a lo anterior el nivel del riesgo residual pasa a ser" "*moderado*" (resultado de una probabilidad "rara vez – 1" y un impacto "moderado – 3").

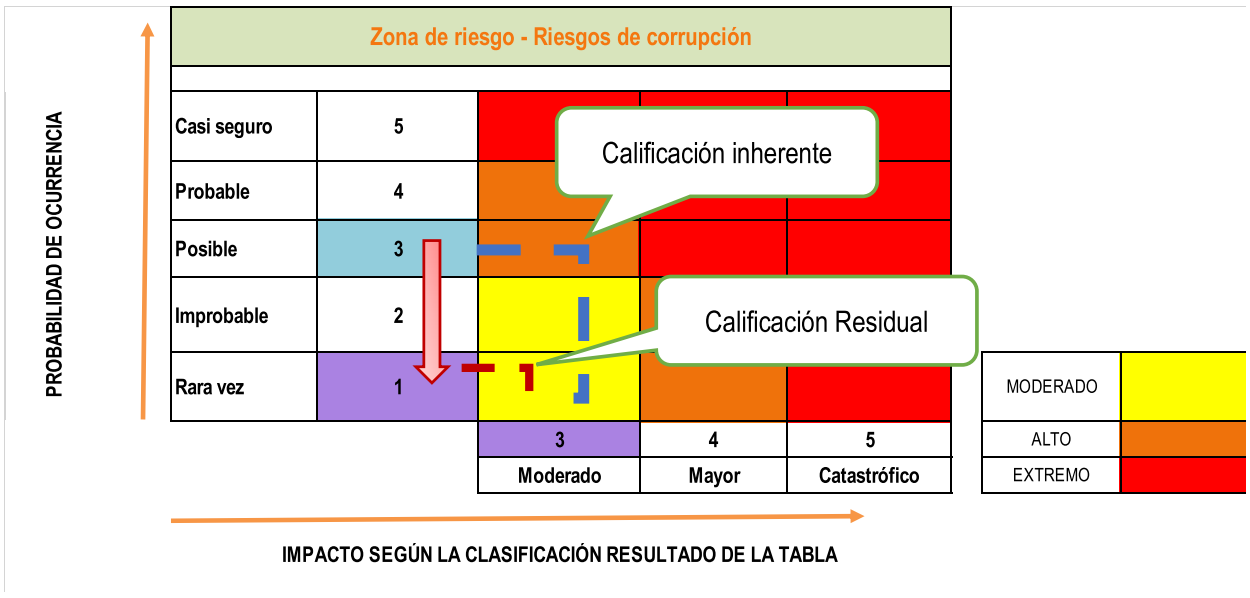

Ilustración 9. Riesgo Residual

Paso 14. Tratamiento del riesgo: A partir del nivel de riesgo y la zona de riesgo residual, se debe proceder a formular las acciones de tratamiento teniendo en cuenta las causas identificadas previamente en el componente de identificación del riesgo, estableciendo fechas de ejecución y responsables.

¿Qué es tratamiento del riesgo?

Es la respuesta establecida por la primera línea de defensa para la mitigación de los riesgos de corrupción.

Para identificar la estratégica para combatir el riesgo de corrupción, emplear la Tabla 6. Tratamiento de riesgos de corrupción, del procedimiento vigente Administración de riesgos y oportunidades código DE_PR_01.

A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, y partiendo de lo que establezca la política vigente de administración del riesgo, los líderes de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento. En todos los casos para los riesgos de corrupción la respuesta será evitar, compartir o reducir el riesgo, nunca se puede aceptar.

NOTA: Una vez analizados los riesgos asociados a posibles actos de corrupción o de deficiencias administrativas, las entidades públicas deben implementar acciones de control orientadas a reducir o eliminar los riesgos que se puedan presentar. Los trámites que presenten riesgos de corrupción deben ser incluidos en el proceso de priorización para implementar acciones de racionalización con el fin de que estas se constituyan en controles a dichos riesgos. Así mismo, se debe tener en cuenta en el análisis que no toda causa de corrupción genera acciones de racionalización, debido a que un trámite puede ser ágil y transparente pero el agente incide en el procedimiento para favorecer sus intereses personales, de manera que la causa de corrupción no es inherente al procedimiento del trámite, sino a factores como presión externa o fallas de integridad (triángulo de la corrupción).

5.3.6. Herramientas para la Gestión del Riesgo

Las actividades o acciones, independientemente de la clasificación y tipología del riesgo a tratar, deben tener una adecuada combinación para prevenir que la situación de riesgo se origine. Ahora, en caso de que la situación de riesgos se presente, esta debe ser detectada de manera oportuna.

5.3.6.1. Plan de acción – Riesgos de Gestión – seguridad de la información

Frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de tareas o proyectos.

Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.

Paso 1. Acción o actividad: Documentar la(s) acción(es) / actividad(es) por cada riesgo, teniendo en cuenta que el objetivo de estas es trabajar las causas identificada, por lo cual deben iniciar con un verbo.

Paso 2. Peso porcentual de la acción o actividad: Determine para cada acción o actividad el peso porcentual, de tal forma que todas las acciones o actividades, de cada riesgo sumen el 100%. **Nota**: El peso porcentual facilitará determinar el % de avance del monitoreo y seguimiento.

Paso 3. Producto / Evidencia de la acción o actividad: Identificar el(los) registro(s) que evidencia (n) la implementación de cada una de la(s) acción(es) o actividad(es) establecida(s).

Paso 4. Responsable: Indicar el nombre de quién posee la responsabilidad de ejecutar la acción o actividad, teniendo en cuenta que está en cabeza de los jefes, coordinadores, subdirectores, directores territoriales, aunque la acción o actividad a ejecutar esté delegada en un funcionario y/o contratista, de igual forma se puede indicar el nombre de la dependencia que ejecuta y quién reporta la información de ejecución de la acción o actividad.

Paso 5. Fecha de inicio: Indicar fecha en la que se inicia la ejecución de la(s) acción(es) o actividad(es).

Paso 6. Fecha de finalización: Indicar la fecha de finalización de ejecución de la(s) acción(es) o actividad(es).

Paso 7. Meta de la acción o actividad(es): Para cada acción o actividad, identificar una meta la cual será ejecutable de forma anual o cuatrimestral y la precisión su frecuencia se recomienda documentar en la acción o actividad.

5.3.6.2. Tratamiento del riesgo – Riesgo de corrupción

Se deben generar acciones o actividades para las causas identificadas, de forma adicionales a los controles establecidos, para fortalecer su prevención y mitigar que el riesgo se presente, es necesario que dichas acciones contribuyan a contrarrestar la causa identificada.

Por otra parte, si la causa de un riesgo incluye a terceros, la acción o actividad, debe establecerse teniendo en cuenta el alcance del proceso y de la entidad, conforme a su competencia.

Paso 1. Acción o actividad: Documentar la(s) acción(es) o actividad(es) por cada riesgo, teniendo en cuenta que el objetivo de estas es trabajar las causas identificada, por lo cual deben iniciar con un verbo, adicionalmente si su ejecución no es constante indicar la frecuencia para ayudar a determinar si la meta es anual, semestral u otra.

Paso 2. Peso porcentual de la acción o actividad(es): Determine para cada acción o actividad, el peso porcentual, de tal forma que todas las acciones o actividades de cada riesgo sumen el 100%. **Nota**: El peso porcentual facilitará determinar el % de avance del monitoreo y seguimiento.

Paso 3. Registro/Evidencia de la acción o actividad: Identificar el(los) registro(s) que evidencia (n) la implementación de cada una de las acciones o actividades establecidas.

Paso 4. Responsable: Indicar el nombre de quién posee la responsabilidad de ejecutar la acción o actividad, teniendo en cuenta que está en cabeza de los jefes, coordinadores, subdirectores, directores territoriales, aunque la acción o actividad, a ejecutar esté delegada en un funcionario y/o contratista, de igual forma se puede indicar el nombre de la dependencia que ejecuta y quién reportará la ejecución.

Paso 5. Fecha de inicio: Indicar fecha en la que se inicia la ejecución de la(s) acción(es) o actividad(es).

Paso 6. Fecha de finalización: Indicar la fecha de finalización de ejecución de la(s) acción(es) o actividad(es).

Paso 7. Meta: Identificar una meta la cual será ejecutable de forma anual o cuatrimestral y la precisión su frecuencia se debe documentar en la acción o actividad.

5.4. Monitoreo, revisión y seguimiento

5.4.1. Monitoreo y revisión

Mediante el monitoreo y revisión se asegura el logro de sus objetivos anticipándose a los eventos negativos relacionados con la gestión de la entidad. El modelo integrado de planeación y gestión (MIPG) en la dimensión 7 “Control Interno” desarrolla a través de las líneas de defensa la responsabilidad de la gestión del riesgo y control que está distribuida en diferentes servidores de la entidad como se puede observar en el procedimiento vigente Administración de riesgos y oportunidades DE_PR_01.

Los líderes de los procesos, los jefes, directores territoriales en conjunto con sus equipos de trabajo deben monitorear y revisar conforme la política de administración de riesgos, las acciones (plan de acción (mapa de riesgos gestión y seguridad de la información) o tratamiento del riesgo (mapa de riesgos de corrupción)) y los controle existentes (mapa de riesgos de Corrupción) definidos en el mapa de riesgos de gestión, de corrupción y de seguridad digital, según aplique. La información de este monitoreo se amplía en procedimiento vigente Administración de riesgos y oportunidades DE_PR_01. La Oficina Asesora de Planeación genera un monitoreo aleatorio y consolida el mapa de riesgos y oportunidades con las evidencias de ejecución de las acciones (plan de acción, tratamiento de riesgos y controles existentes) remitidas por los procesos y compartido en el DRIVE e informa al Grupo de Control Interno conforme el cronograma proyectado para cada vigencia.

Paso 1. Fecha: Reportar fecha (día/mes/año) en la que se documenta el monitoreo.

Paso 2. Descripción del monitoreo: En este espacio se registra el avance de la acción o actividad, el cual debe ser coherente con lo establecido o programado en el mapa de riegos (plan de acción, tratamiento del riesgo o control). Debe ser coherente con las evidencias que fueron adjuntadas dado que es el soporten del avance o ejecución de las acciones o actividades.

> **Nota**. Las evidencias deben corresponder al registro/evidencia descritas (plan de acción, tratamiento del riesgo o control), adicionalmente se debe registrar el nombre de las evidencias tal cual como se reporta en el DRIVE o están presente en la URL registrada.

Paso 3. Preguntas de autocontrol (solo para controles en riesgos de gestión y corrupción): Registrar una respuesta para las dos preguntas: 1. se generó o requirió una alerta y 2. se materializó el riesgo, mediante un si o un no, y una breve justificación o descripción que soporte la respuesta, principalmente en caso de una respuesta afirmativa.

Paso 4. % avance (de acuerdo al peso porcentual de la acción): Registrar el porcentaje del avance para cada una de las acciones o actividades, teniendo en cuenta que la acción tiene una ejecución anual, coherente con el cumplimiento de la meta establecida para la acción o actividad.

Nota: el porcentaje de avance es acumulativo y su valor máximo no puede superar el porcentaje programado en la columna "*Peso porcentual de la acción*".

Ejemplo. El peso porcentual el cual se asigna teniendo en cuenta los **tres** períodos de reporte anual (es decir cuatrimestralmente), cuando se ejecución es estable en el año se recomienda dividir el peso en tres, es decir el líder del proceso debe verificar que la suma en conjunto de todas las acciones de control de 100%, **por ejemplo**, para un riesgo en el cual solo lo compone una acción o actividad, que pese el 100%: 100/3 = 33.33, este 33.33% correspondería al porcentaje de cumplimiento de la acción para cada periodo a reportar en caso de que cumpla con lo establecido, por lo cual en el primer cuatrimestre se reporta 33.33% y para el segundo cuatrimestre 66.66% y el tercer y último cuatrimestre 100%. Otro ejemplo a tener en cuenta es un riesgo con una sola acción la cual se cumple al 100% en el primer reporte se deberá justificar con las evidencias para el respectivo seguimiento del Grupo de Control Interno.

5.4.2. Monitoreo

La Oficina Asesora de Planeación como segunda línea de defensa para riesgos de gestión y corrupción, debe asegura que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende y por ende monitorear la gestión de riesgo ejecutada por la primera línea de defensa, por tal motivo realizará de forma aleatoria un monitoreo que será reportado en el formato Mapa de riesgos de gestión, corrupción y seguridad de la información Código: DE_FO_02:

Paso 1. De respuesta a la siguiente pregunta resultado del Monitoreo: "¿Se ejecutan controles de acuerdo con lo planificado?" de forma afirmativa o negativa y generé un breve texto que justifique la respuesta de la pregunta y que es resultado del análisis de la información reportada en los controles y las acciones o actividades establecidas, para frente a las evidencias que soportan la ejecución de los controles y las acciones establecidas.

5.4.3. Seguimiento

El seguimiento lo realiza el Grupo de Control interno conforme lo señala la Ley 1474 en su artículo 73, el Decreto 124 del 2016, el Decreto 648 del 2017 y el Modelo Integral de Planeación y Gestión -MIPG y Política de Administración de Riesgos, el cual quedará consignado en el informe de seguimiento a la Gestión de riesgos, el monitoreo al seguimiento, publicado en el portal web de la entidad en el Link de Transparencia y acceso a la información pública y divulgado al interior de la entidad.

Paso 1. La información del seguimiento y monitoreo, se evidencia en el informe de seguimiento a la Gestión de riesgos, que genera el Grupo de Control Interno como resultado del análisis de las causas, así como la evaluación de la eficacia y efectividad de los controles y las acciones o actividades establecidas, determinado mediante la revisión y análisis de las evidencias que soportan la ejecución de los controles como mecanismo principal de prevención del riesgo y las acciones complementarias, establecidas para el tratamiento o plan de acción de los riesgos; dicho informe genera las alertas correspondientes, incluyendo un plan de mejoramiento que surja como resultado del seguimiento en caso de aplicar y se publica cuatrimestralmente y se presenta a la alta dirección.

5.5. METODOLOGÍA PARA ABORDAR LAS OPORTUNIDADES

De acuerdo a la definición de la norma NTC ISO 9000:2015, el "riesgo es el efecto de la incertidumbre, un efecto es una desviación de lo esperado ya sea positivo o negativo.

Las oportunidades pueden surgir como resultado de una situación favorable para lograr un resultado previsto, así como impactar de manera positiva el logro de los objetivos estratégicos y de los procesos. Por ejemplo, se puede identificar oportunidades que permitan mejorar la prestación de los servicios de la entidad, o una oportunidad que permita mejorar la satisfacción de los usuarios, entre otros.

Para identificar las oportunidades de mejora se debe tener en cuenta el contexto, así como las necesidades y expectativas de las partes interesadas. Otro aspecto a tener en cuenta, es que a partir de un riesgo también puede surgir una oportunidad.

Para identificar las oportunidades se debe diligenciar el Formato vigente la matriz de oportunidades DE_FO_11:

Paso 1. Proceso: Seleccione el proceso al que corresponde. **Nota**. El número de la oportunidad será asignado en el momento de la consolidación, por la Oficina Asesora de Planeación.

Paso 2. Oportunidad: Describa la oportunidad identificada, teniendo en cuenta el contexto, las necesidades, expectativas y riesgos, tener en cuenta que la ejecución de una función o el cumplimiento de una norma no es una oportunidad, de igual forma una acción o control de riesgo no corresponde a una oportunidad.

Paso 3. Beneficios a obtener a partir de la implementación de la oportunidad: Documente brevemente cuál es el objetivo o logro esperado a obtener con la ejecución de la oportunidad.

Paso 4. Acciones para abordar la oportunidad: Describa la(s) acción(es) que se adelantará(n) para abordar la oportunidad, siendo clara la forma de ejecutar la actividad puede ser una acción o varias.

Paso 5. Responsable: Diligencia el nombre de la dependencia responsable de ejecutar la oportunidad, teniendo presente que quién posee la responsabilidad de ejecutar la(s) acción(es), teniendo en cuenta que está en cabeza de los jefes, coordinadores, subdirectores, directores territoriales, aunque la acción a ejecutar esté delegada en un funcionario y/o contratista.

Paso 5. Peso porcentual: Para cada acción que compone la oportunidad se deberá asignar un peso porcentual de tal forma que la suma de las acciones del 100%, lo cual facilitará determinar el % de avance en el seguimiento.

Paso6. Registro/ evidencia: En esta columna se debe relacionar el (los) registro(s) que evidencia la implementación de la acción establecida.

Paso 9. Fecha de inicio: Relacione la fecha de inicio de la acción.

Paso 10. Fecha de finalización: Relacione la fecha de finalización de la acción.

Monitoreo y Descripción.

Paso 11. Fecha corresponde a la fecha (día/mes/año) en la que se realiza el reporte de ejecución por parte del responsable.

Paso 12. Descripción del monitoreo*:* En este espacio se registra el avance por cada una de las acciones establecidas de manera cuatrimestral, el cual debe ser coherente con las evidencias adjuntadas y que soporten el avance de la(s) acción(es), adicionalmente se debe registrar el nombre de las evidencias como se encuentra en el DRIVE. **Nota**. Las Evidencias deben corresponder al registro/evidencia descritas con anterioridad.

Paso 13. % avance (de acuerdo al peso porcentual de la acción): Registrar el porcentaje del peso porcentual del avance para cada una de las acciones de control que compone la oportunidad, teniendo en cuenta que la acción de control tiene una ejecución anual.

El peso porcentual el cual se asigna teniendo en cuenta los **tres** períodos de reporte anual, cuando se ejecución es estable en el año se recomienda dividir el peso en tres, es decir el líder del proceso debe verificar que la suma en conjunto de todas las acciones de 100%, **por ejemplo**, para una oportunidad en el cual solo la compone una acción que pese el 100%: 100/3 = 33.33, este 33.33% correspondería al porcentaje de cumplimiento de la acción para cada periodo a reportar en caso de que cumpla con lo establecido, por lo cual en el primer cuatrimestre se reporta 33.33% y para el segundo cuatrimestre 66.66% y el tercer y último cuatrimestre 100%.

Nota. Si la acción cumple al 100% en el primer reporte se deberá justificar con las evidencias para el respectivo seguimiento de la oficina de Control Interno y determinar para el próximo monitoreo una nueva acción.

Seguimiento

El seguimiento lo realiza el Grupo de Control interno teniendo presente los siguientes pasos.

Paso 14. Fecha: Corresponde a la fecha (día/mes/año) en la que se realiza el seguimiento.

Paso 15. Descripción Monitoreo: Texto que determina el análisis de la eficacia de la acción de la oportunidad identificada, para ello se debe hacer una revisión y análisis de las evidencias que soportan la ejecución de la(s) acción(es) establecida(s) y describir dicho seguimiento en la columna correspondiente.

Nota. La información ampliada del seguimiento debe contemplarse en el informe que el Grupo de Control Interno presenta a la alta dirección generando las alertas correspondientes que surjan como resultado del seguimiento.

6. CONTROL DE CAMBIOS

FECHA DE VIGENCIA VERSIÓN ANTERIOR	VERSIÓN ANTERIOR	MOTIVO DE LA ACTUALIZACIÓN
18/02/2022	12	Se ajustaron: objetivo, alcance y lineamientos generales y/o políticas de operación del instructivo, dado que se actualizó dejando únicamente los lineamientos de como generar las herramientas para la administración de riesgos y oportunidades de la oportunidad, lo anterior dado las observaciones recibidas en asesoría por el Departamento Administrativo de la Función Pública. Se incluyó el lineamiento sobre el diligenciamiento del “control de cambios”, por parte de cada proceso, en la hoja para tal fil dentro del formato vigente Mapa de riesgos DE_FO_02 y matriz de oportunidades DE_FO_11, y que

FECHA DE VIGENCIA VERSIÓN ANTERIOR	VERSIÓN ANTERIOR	MOTIVO DE LA ACTUALIZACIÓN
18/02/2022	12	solo aplica para las modificaciones dentro del año, no para el mapa de riesgos a inicio de año. Se actualizó el desarrollo del instructivo en concordancia con el ajuste del objetivo del instructivo, se ajustó separando “control existente” y la acción o actividad del “plan de acción o plan de tratamiento” para que no existan confusiones.
13/12/2022	13	Se ajustó dentro de capítulo de desarrollo, algunos temas se te eliminaron algunas imágenes y tablas citando las Guía para la administración del riesgo y el diseño de controles en entidades pública, 2020 y 2018 – DAFP. En el Capitulo 5.4.1., se eliminó que el reporte de los controles es solo para los riesgos de corrupción, dado que ahora aplica para riesgos de gestión y corrupción, y se incluyeron las preguntas que ahora son parte del formato Mapa de riesgos de gestión, corrupción y seguridad de la información Código: DE_FO_02, en las etapas de monitoreo de la primera línea de defensa. Se incluyó el nuevo capitulo 5.4.2. para el monitoreo realizado por la Oficina Asesora de Planeación y se eliminó del capítulo 5.4.3., ajustes que se generaron dada la actualización del formato Mapa de riesgos de gestión, corrupción y seguridad de la información Código: DE_FO_02 y se aclara que toda la información el Grupo de Control Interno será reportada en el Informe correspondiente.

CRÉDITOS		
Elaboró	Nombre	Mónica Sandoval
	Cargo	Contratista – Oficina Asesora de Planeación
	Fecha	30/03/2023
Revisó	Nombre	Diana Carolina Oviedo León
	Cargo	Jefe Oficina Asesora de Planeación
	Fecha:	31/03/2023
Aprobó	Nombre	Diana Carolina Oviedo León
	Cargo	Jefe Oficina Asesora de Planeación
	Fecha:	31/03/2023