TABLA DE CONTENIDO

1. OBJETIVO

Establecer herramientas conceptuales y metodológicas que contribuyan al adecuado manejo y administración de 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 del (los) riesgo(s) que se lleva a cabo determinando las causas con base en el contexto interno, externo del proceso y que pueden afectar el logro de los objetivos del proceso, continúa con el análisis, evaluación y identificación de los riesgos y termina con la valoración, monitoreo y seguimiento.

3. DEFINICIONES

Acción correctiva	Conjunto de acciones tomadas para eliminar la(s) causa(s) de una no conformidad detectada u otra situación no deseable.
Administración de riesgos	Metodología de conjunto de elementos de control que, al interrelacionarse, permiten a para las Entidades públicas desde la evaluación de aquellos eventos negativos, tanto internos como externos, la identificación de los riesgos que afectan los logros de los objetivos estratégicos y del proceso, hasta el tratamiento de cada uno de ellos. Se constituye en el componente de control que le permite a la entidad pública auto controlarse.
Análisis de riesgos	Establecimiento de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial o riesgos inherente.
Causas	Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir 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.
Causa Raíz	Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
Contexto	Parámetros internos y externos que se han de tomar en consideración para la administración del riesgo (NTC-ISO 31000). A partir de los factores que se definan es posible establecer las causas de los riesgos a identificar Permite establecer su complejidad, procesos, planeación institucional, entre otros aspectos, lo anterior para conocer y entender la entidad y su entorno, para determinar el análisis de riesgos.
Control	Medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas, u otras acciones).
Control correctivo	Medida que permite reducir o mitigar un riesgo, atacando el impacto frente a la materialización del riesgo (plan de contingencia).
Control detectivo	Medida que permite reducir o mitigar un riesgo, detectando que algo ocurre y devuelve el proceso a los controles preventivos. Ataca la probabilidad de ocurrencia del riesgo.

Control preventivo	Medida que permite reducir o mitigar un riesgo, va a las causas del riesgo. Ataca la probabilidad de ocurrencia del riesgo.
Consecuencias	Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.
Evaluación del riesgo	Etapa para mediar los resultados de la calificación del riesgo (probabilidad – impacto) antes y después de los controles, para identificar el nivel del riesgo residual para identificar el tratamiento de riesgos y por ende las acciones de control a ejecutar.
Establecimiento del Contexto	Definición de los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo (NTC ISO31000, Numeral 2.9).
Factores de riesgo	Toda característica proveniente del contexto cuya presencia o comportamiento incide en una mayor o menor probabilidad de materialización de una o varias causas asociadas a uno o varios riesgos, por lo cual son las fuentes generadoras de riesgos.
Identificación del riesgo	Etapa donde se establecen las fuentes o factores de riesgo, los riesgos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas. Se puede entender como el proceso que permite determinar qué podría suceder, por qué sucedería y de qué manera se llevaría a cabo.
Impacto	Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.
Materialización	Es el evento en el cual un riesgo se vuelve realidad y presentarse, afectando los objetivos estratégicos de la Entidad o del proceso.
Mapa de riesgos	Herramienta metodológica que permite hacer un inventario de los riesgos ordenada y sistemáticamente, definiéndolos, haciendo la descripción de cada uno de estos y las posibles consecuencias, con la información resultante de la gestión del riesgo.
Monitorear	Comprobar, supervisar, observar o registrar la forma en que se lleva a cabo una actividad con el fin de identificar posibles cambios. En concordancia con la cultura del autocontrol al interior de la entidad, los líderes de los procesos junto con su equipo realizan verificación (monitoreo) y evaluación permanente a la gestión de riesgos (gestión, corrupción y seguridad digital).
Nivel del Riesgo	Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad x Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.
Oportunidad	Eventos que pueden ayudar a mejorar la gestión, estas se identifican como parte de la comprensión de la organización y su contexto y como parte del programa de acciones correctivas y de mejora.

Plan de Acción	Conjunto de acciones tomadas para combatir la estrategia de reducir el riesgo, especificando como mínimo: responsable, fecha de implementación y fecha de seguimiento.
Probabilidad	Se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.
Riesgo	Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. **NOTA**: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
Riesgo de gestión	Posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales. Se expresa en términos de probabilidad y consecuencias.
Riesgo inherente	Es aquel al que se enfrenta una entidad en ausencia de acciones de la Dirección para modificar su probabilidad o impacto.
Riesgo residual	Nivel de riesgo que permanece luego de tomar medidas de tratamiento del riesgo.
Riesgo de corrupción	Posibilidad de que, por acción u omisión, se use el poder para poder desviar la gestión de lo público hacia un beneficio privado, ejemplos: Conflicto de intereses, extralimitación, dilación.
Riesgo de Seguridad de la Información	Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
Valoración del riesgo	Establecimiento de la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (riesgos inherentes).

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.
- Diseñar e implementar acciones para gestionar los riesgos y abordar 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, acciones de control, del monitoreo y revisión, a cargo de las tres líneas de defensa.
- Las etapas de la administración de riesgos contemplan la participación articulada y activa de los tres niveles de gestión (Central, Territorial y Local), la ciudadanía y los grupos de valor interesados en su identificación.
- 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

- Analizar y determinar luego de cada vigencia si el riesgo sigue latente, es decir si a pesar de los controles implementados se considera que el mismo continúa, para lo cual se debe recalificar de acuerdo a las actividades establecidas y dejar constancia en un acta. Si por el contrario se considera que el riesgo ya no es latente y no debe considerarse como un riesgo, se deja mediante acta la justificación que conlleva a su eliminación del mapa de riesgos.
- En cada vigencia, se deben evaluar los riesgos y para aquellos que continúan y se recalifican se deben revisar las causas, impactos, controles existentes y acciones de control, ya que pueden surgir nuevas acciones conforme se presenten cambios del contexto en el proceso.
- Es importante verificar que todos los procesos identifiquen los riesgos pertinentes y realicen las actividades necesarias de la Administración de Riesgos, así consideren que no cuente con estos, se deben documentar todo al respecto.
- En cuanto al registro y reporte de incidentes de seguridad digital, es importante que la entidad pública cuente con el registro de los incidentes de seguridad de la información que se hayan materializado, con el fin de analizar las causas, las deficiencias de los controles implementados y las pérdidas que se pueden generar.
- El propósito fundamental del registro de incidentes es garantizar que se tomen las acciones adecuadas para evitar o disminuir su ocurrencia, retroalimentar y fortalecer la identificación y gestión de dichos riesgos y enriquecer las estadísticas sobre amenazas y vulnerabilidades y, con esta información, adoptar nuevos controles.
- El responsable de seguridad de la información deberá reportar a la Línea Estratégica (Alta dirección y Comité Institucional de Coordinación de Control Interno) y a las partes interesadas la información requerida.
- 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 (plan de contingencia) y proceder teniendo en cuenta lo descrito en el Procedimiento vigente Administración de riesgos y oportunidades código DE_PR_01.
- Los riesgos de corrupción no poseen controles correctivos “plan de contingencia”, 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.

5. DESARROLLO

El presente instructivo se genera en 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. 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 siguiente metodología:

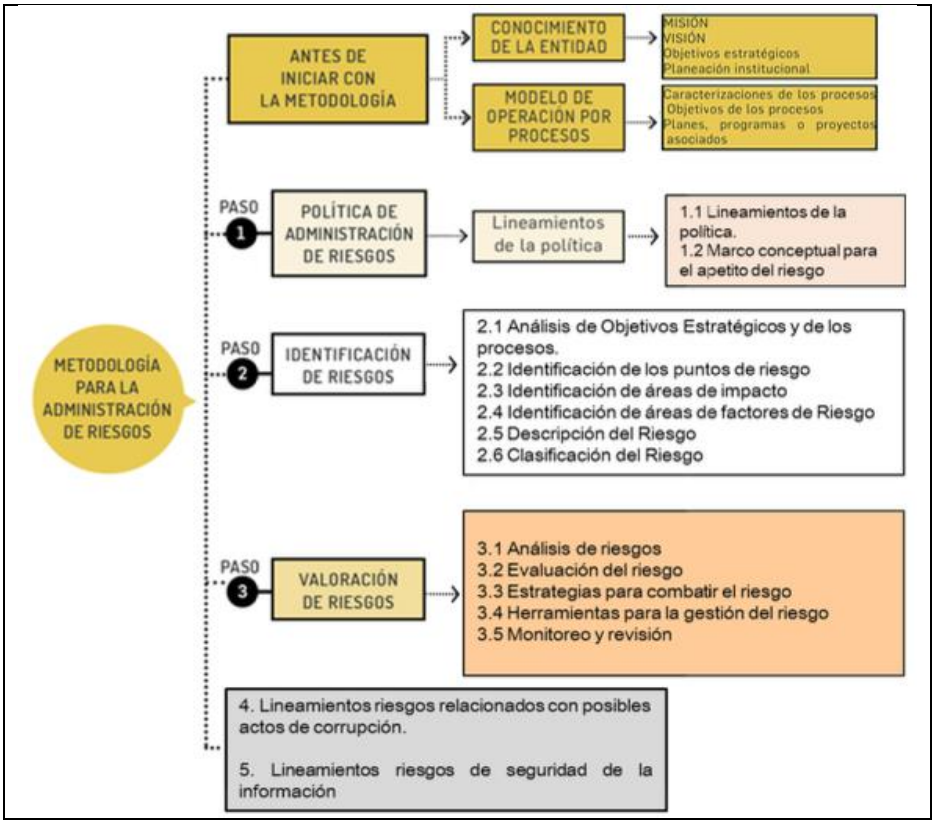

Ilustración 1. Metodología para la Administración del Riesgo
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades pública, 2020– DAFP

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, para la gestión 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. Ver documento vigente "política administración de riesgos" publicada en el Procedimiento vigente Administración de Riesgos y Oportunidades código DE_PR_01.

La Política de Administración de Riesgos debe contener los siguientes aspectos:

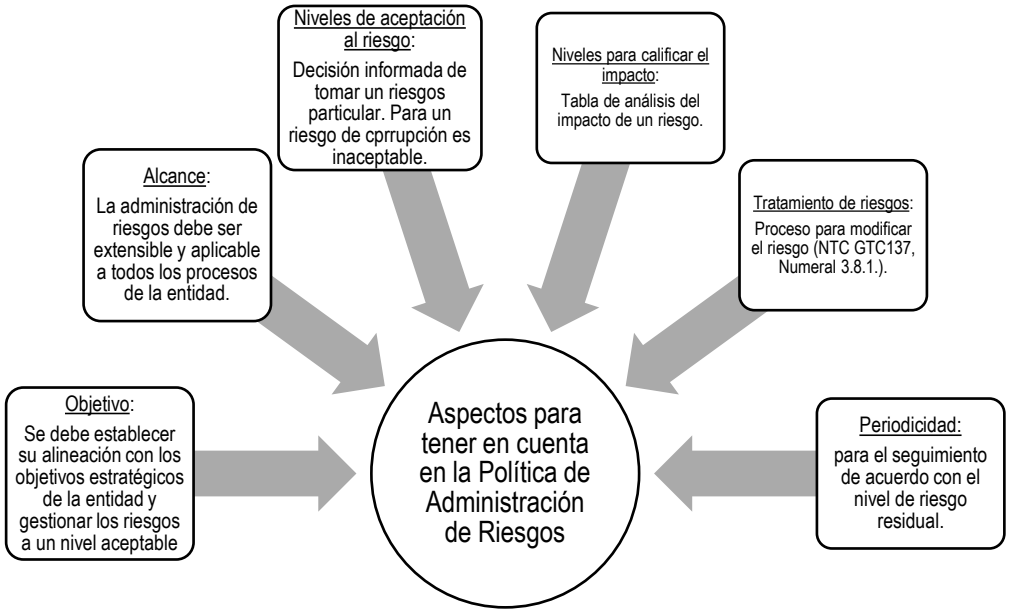

Ilustración 2. Aspectos a tener en cuenta en la Política de Administración de Riesgos

5.3. IDENTIFICACIÓN DE RIESGOS

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

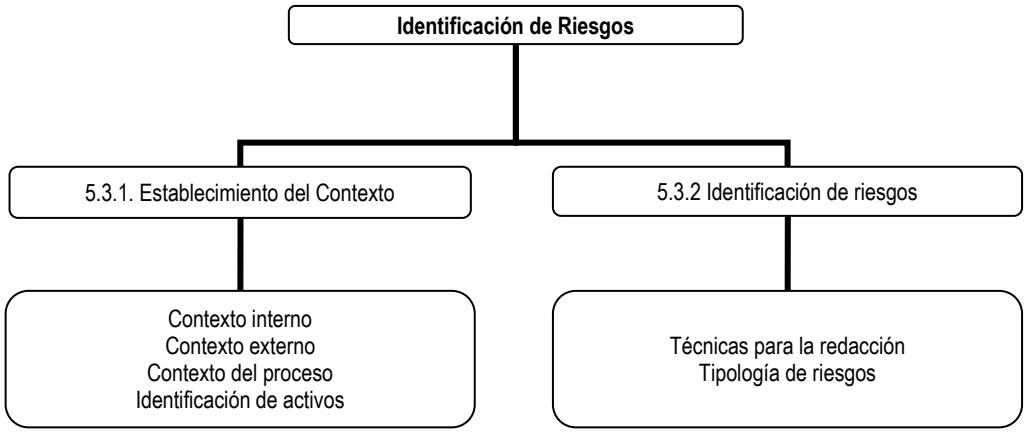

Ilustración 3. Mapa conceptual Identificación de Riesgos

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. Para el desarrollo de este componente se debe tener en cuenta el contexto de los procesos.

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:

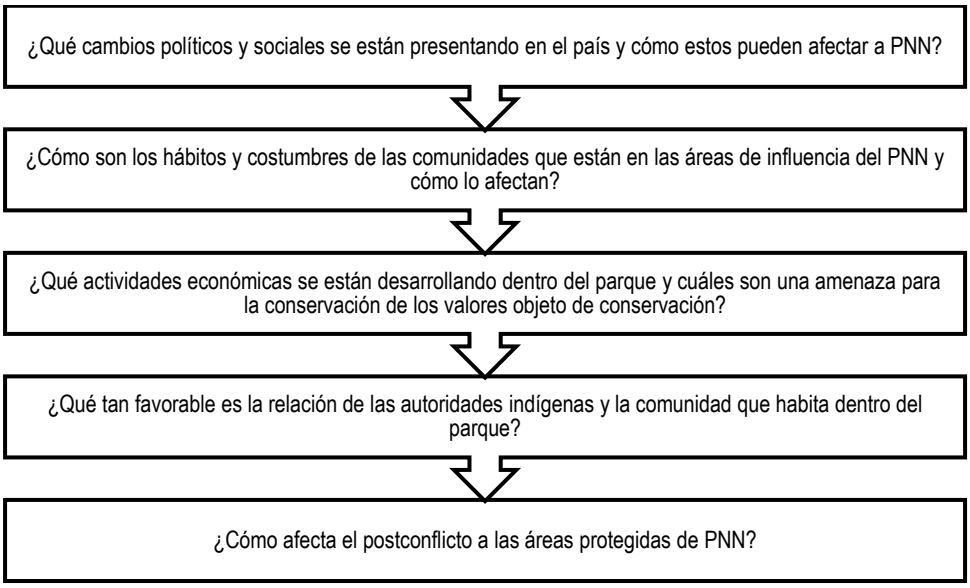

Ilustración 4. Preguntas de contexto externo

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:

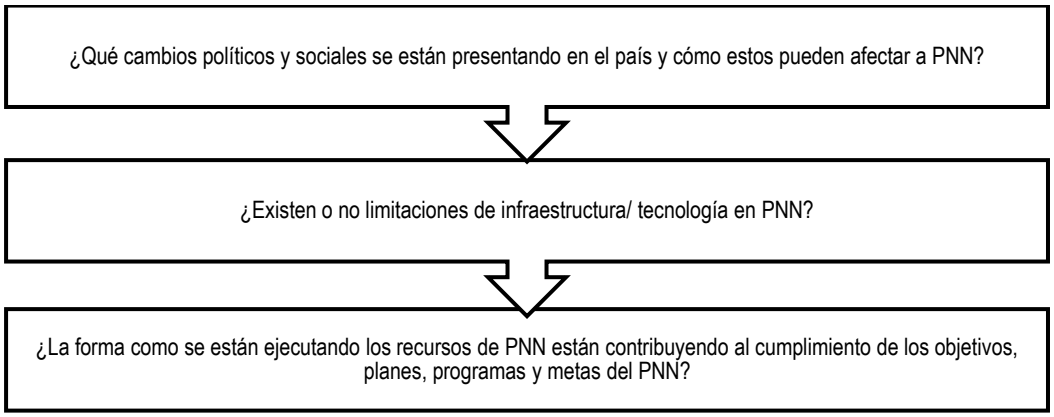

Ilustración 5. Preguntas de contexto interno

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.
CO NTE	**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 DE_FO_02 Mapa de riesgos, 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; adicionalmente la entidad emplea para la planeación estratégica 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:

*S*e realizará a partir del análisis de los objetivos estratégicos y de proceso, 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 Radiocomunicaciones.

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

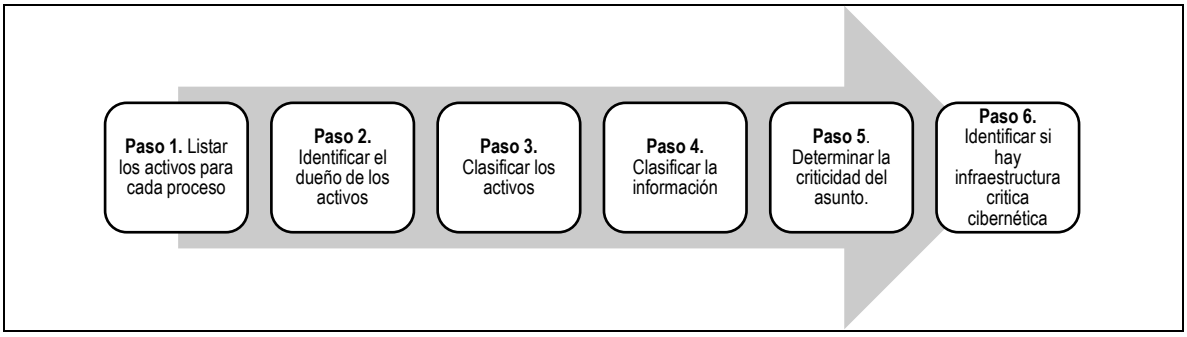

Ilustración 6. Pasos para identificar los activos

Las identificaciones de los activos de información se diligenciarán en la pestaña denominada “Activos de información” en el formato DE_FO_02_Mapa-de-riesgos y DE_FO_11-matriz-de-oportunidades, 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 DE_FO_02_Mapa-de-riesgos 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
Fallas técnicas	Fallas del equipo	D,F
	Mal funcionamiento del equipo	D,F

Tipo	Amenaza	Origen
	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 autorizada 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 DE_FO_02_Mapa-de-riesgos 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
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

Tipo	Vulnerabilidades
	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**:

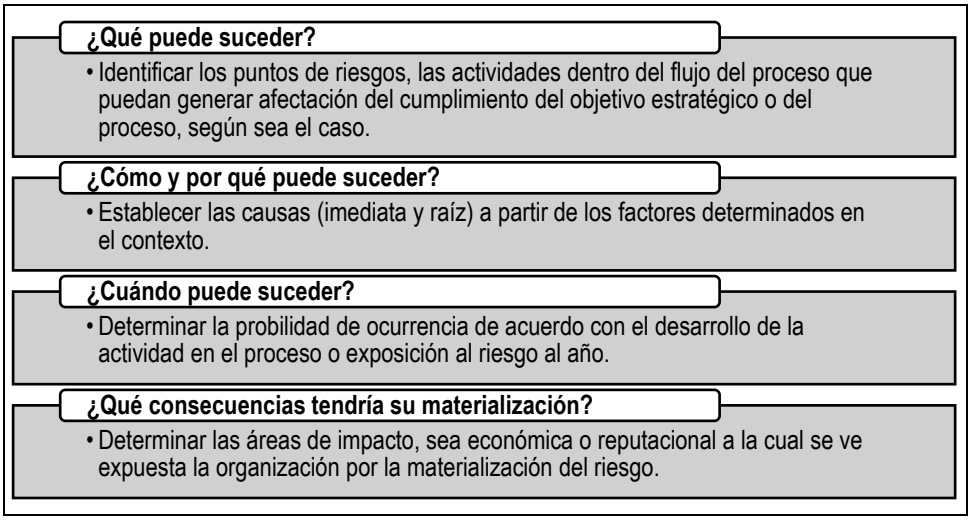

Ilustración 7. Preguntas clave para la identificación de riesgos

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 siguiente matriz (Tabla Nº 5 Matriz definición del riesgo de Corrupción), que 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), se trata de un riesgo de corrupción:

Tabla N.º 5. Matriz definición del riesgo de corrupción

MATRIZ: DEFINICIÓN DEL RIESGO DE CORRUPCIÓN				
Descripción del riesgo	**Acción y omisión**	**Uso del poder**	**Desviar la gestión de lo público**	**Beneficio privado**
Ejemplo: Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

Fuente: Secretaria de Transparencia de la Presidencia de la República

A manera de ilustración se señalan algunos de los procesos y procedimientos susceptibles de actos de corrupción a partir de los cuales se puede identificar **riesgos de corrupción**[1]:

Tabla N.º 6. Ejemplo de procesos susceptibles de actos de corrupción

Direccionamiento Estratégico (Alta Dirección).	• Concentración de autoridad o exceso de poder. • Extralimitación de funciones. • Ausencia de canales de comunicación. Amiguismo y clientelismo.
Financiero (Está relacionado con áreas de Planeación y Presupuesto).	• Inclusión de gastos no autorizados. • Inversiones de dineros públicos en entidades de dudosa solidez financiera, a cambio de beneficios indebidos para servidores públicos encargados de su administración. • Inexistencia de registros auxiliares que permitan identificar y controlar los rubros de inversión. • Archivos contables con vacíos de información. • Afectar rubros que no corresponden con el objeto del gasto en beneficio propio o a cambio de una retribución económica.
De contratación (Como proceso o los procedimientos ligados a éste).	• Estudios previos o de factibilidad superficiales. • Estudios previos o de factibilidad manipulados por personal interesado en el futuro proceso de contratación. (Estableciendo necesidades inexistentes o aspectos que benefician a una firma en particular). • Pliegos de condiciones hechos a la medida de una firma en particular. • Disposiciones establecidas en los pliegos de condiciones que permiten a los participantes direccionar los procesos hacia un grupo en particular, como la media geométrica. • Restricción de la participación a través de visitas obligatorias innecesarias, establecidas en el pliego de condiciones. • Adendas que cambian condiciones generales del proceso para favorecer a grupos determinados. • Urgencia manifiesta inexistente. • Concentrar las labores de supervisión de múltiples contratos en poco personal. • Contratar con compañías de papel, las cuales son especialmente creadas para participar procesos específicos, que no cuentan con experiencia, pero si con músculo financiero.
De información y documentación.	• Concentración de información de determinadas actividades o procesos en una persona. • Sistemas de información susceptibles de manipulación o adulteración. • Ocultar a la ciudadanía la información considerada pública. • Deficiencias en el manejo documental y de archivo

[1] *Estrategias para la construcción del plan anticorrupción y de atención al ciudadano.*

De investigación y sanción	• Fallos amañados. Dilatación de los procesos con el propósito de obtener el vencimiento de términos o la prescripción del mismo. • Desconocimiento de la ley, mediante interpretaciones subjetivas de las normas vigentes para evitar o postergar su aplicación. • Exceder las facultades legales en los fallos. • Soborno (Cohecho).
De actividades regulatorias	• Decisiones ajustadas a intereses particulares. • Tráfico de influencias, (amiguismo, persona influyente). • Soborno (Cohecho).
De trámites y/o servicios internos y externos.	• Cobro por realización del trámite, (Concusión). • Tráfico de influencias, (amiguismo, persona influyente). • Falta de información sobre el estado del proceso del trámite al interior de la entidad.
De reconocimiento de un derecho, como la expedición de licencias y/o permisos	• Cobrar por el trámite, (Concusión). • Imposibilitar el otorgamiento de una licencia o permiso. • Ofrecer beneficios económicos para acelerar la expedición de una licencia o para su obtención sin el cumplimiento de todos los requisitos legales. • Tráfico de influencias, (amiguismo, persona influyente).

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

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). A continuación, se presenta la clasificación básica para riesgos de Corrupción en la tabla Nº7y para los riesgos de gestión y seguridad de la información en la Tabla Nº8:

Tabla Nº 7. Tipología del riesgo de corrupción

Riesgos Estratégicos	Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad.
Riesgos Gerenciales	Posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.
Riesgos Operativos	Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.
Riesgos Financieros	Posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.
Riesgos Tecnológicos	Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.
Riesgos de Cumplimiento	Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento por desacato a la normatividad legal y las obligaciones contractuales. Riesgos de Imagen o reputacional: posibilidad de ocurrencia

	de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes y partes interesadas
Riesgos ambientales	Efecto de la incertidumbre frente a la ocurrencia de eventos que pueden afectar el desempeño ambiental de la entidad.
Riesgo de corrupción	Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
Riesgos de Seguridad Digital	Posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

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

Tabla Nº 8. Tipología de los riesgos de gestión y Seguridad de la información

Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.
Ambiental	Impacto sobre el medio ambiente, por forma natural o por acción humana.

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

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 DE_FO_02 Mapa de riesgos, 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, como 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.

Paso 5. Identifique el riesgo Iniciando con la frase POSIBILIDAD DE y dando respuesta a lo que puede ocurrir (Impacto + causa inmediata) + causa(s) raíz, 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.

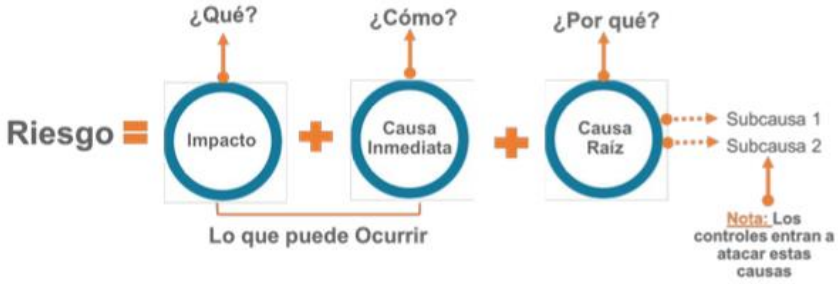

Ilustración 8. Estructura de la redacción de un riesgo
Fuente: Adaptado del Curso Riesgo Operativo de la Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Paso 6. Clasificación del riesgo: Con el objetivo de agrupar los riesgos identificados seleccionar la categoría correspondiente empleando la **Tabla Nº 8** Tipología de los riesgos de gestión y Seguridad de la información.

5.3.3.2. Riesgos de corrupción

A continuación, se relaciona los pasos a realizar para la identificación de riesgos, en el formato vigente DE_FO_02 Mapa de riesgos, pestaña mapa de riesgos.

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.

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: De acuerdo con el riesgo identificado, clasificar teniendo en cuenta la Tabla Nº 7 Tipología del riesgo 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, utilizando la siguiente tabla (columna Frecuencia de la actividad), se registra el número de veces que desarrolla la actividad.

Tabla 9. Criterios de para definir el nivel de probabilidad – riesgos de gestión y seguridad de la información

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

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

Paso 2. Probabilidad Inherente, dado el resultado al paso anterior identifique en la primera columna de la Tabla 10. 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 siguiente tabla, 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.

Tabla 10. Criterios para definir el nivel de impacto – riesgos de gestión y seguridad de la información

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.
Menor 40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

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

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, el análisis se debe realizar de arriba hacia abajo.

Tabla N.º 11. Probabilidad riesgos de corrupción

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	Probable	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	Posible	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	Improbable	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	Rara vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

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

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”.

A continuación, se presente un ejemplo de calificación de las preguntas para determinar el impacto de los riesgos de corrupción:

Tabla N.º 12. Criterios para calificar el impacto - **riesgos de corrupción**

N.º	PREGUNTA	RESPUESTA	
	SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRIA…	SI	NO
1	¿Afectar el grupo de funcionarios del proceso?	1	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	1	
3	¿Afectar el cumplimiento de misión de la entidad?	1	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		1
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	1	
6	¿Generar pérdida de recursos económicos?	1	
7	¿Afectar la generación de los productos o la prestación de servicios?	1	
8	¿Da lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		1
9	¿Genera perdida de información de la entidad?	1	
10	¿Genera intervención de los órganos de control, de la Fiscalía y otro ente?	1	
11	¿Dar lugar a procesos sancionatorios?	1	
12	¿Dar lugar a procesos disciplinarios?	1	
13	¿Dar lugar a procesos fiscales?	1	
14	¿Dar lugar a procesos penales?		1
15	¿Generar pérdida de credibilidad del sector?		1
16	¿Ocasionar lesiones físicas o pérdidas de vidas humanas?		1
17	¿Afectar la imagen regional?		1
18	¿Afectar la imagen nacional?		1
19	¿Generar daño ambiental?		1
Responder afirmativamente de UNA a CINCO preguntas(s) genera un impacto moderado. Responder afirmativamente de SEIS a **ONCE** preguntas(s) genera un impacto mayor. Responder afirmativamente de DOCE a DIECINUEVE preguntas(s) genera un impacto catastrófico		**11**	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad		
CATASTRÓFICO	Genera consecuencias desastrosas para la entidad		

Nivel de impacto Mayor

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

Para este ejemplo se tuvo un total de respuestas afirmativas de "11", lo que indica que el impacto del riesgo es **MAYOR**.

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".

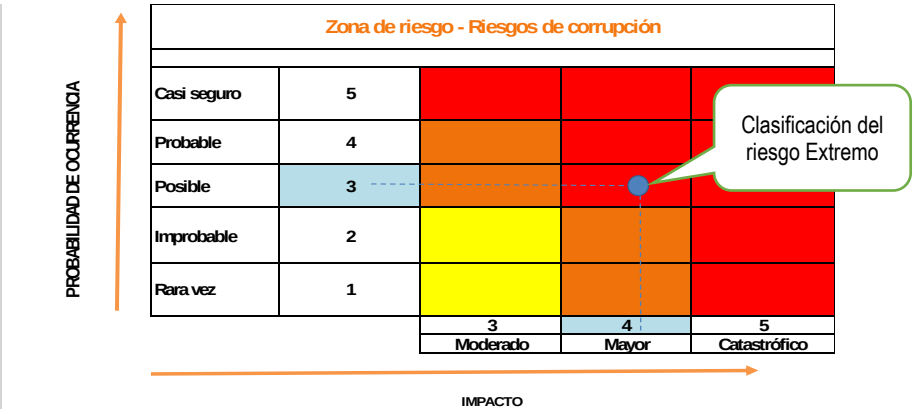

Ilustración 9. Ejemplo Clasificación del riesgo (probabilidad – impacto)

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).

Al momento de definir las actividades de control por parte de la primera línea de defensa, es importante considerar que los controles estén bien diseñados, es decir, que efectivamente estos mitigan las causas que hacen que el riesgo se materialice, aunque sabemos que la mayoría de los controles se encuentran en los documentos asociados a cada proceso, lo cual será verificado por la segunda línea de defensa como la Oficina Asesora de Planeación para los riesgos de gestión y de corrupción y lo propio desarrollará el Grupo de Tecnología de la Información y Comunicaciones para los riesgos de Seguridad de la información, esto con la finalidad de generar advertencia sobre su necesidad de actualización y/o ingreso de nueva documentación en respuesta al control de los riesgos.

A continuación, se debe recordar que los controles se ejecutan con el fin de prevenir la materialización de los riesgos, reducir o mitigar el riesgo previamente identificados, disminuyendo así la probabilidad o el impacto, según sea el caso.

Se relaciona algunos ejemplos de tipos de control:

Tabla N.º 13. Descripción resumen de los controles

DESCRIPCIÓN DE LOS CONTROLES	
Tipo de control	**Controles relacionados**
Controles de gestión	Seguimiento a los objetivos del plan institucional, reportes y seguimiento plan de acción anual (PAA)
	Seguimiento a cronogramas de trabajo

DESCRIPCIÓN DE LOS CONTROLES	
Tipo de control	**Controles relacionados**
	Evaluación del desempeño
	Generación de informes de gestión o reportes
	Monitoreo de riesgos
	Reportes y seguimiento en aplicativos (SULA, SICO SMART)
Controles de operación	Aplicación de listas de chequeo formatos, pólizas, personal capacitado.
	Aplicación de procedimientos, manuales, guías, instructivos (internos y/o externos)
	Capacitación del personal
	Verificación de firmas
	Copias de seguridad, contingencias y respaldo
	Custodia de bienes
	Envío de comunicaciones escritas informando o solicitando información.
	Uso de consecutivos
Controles legales	Leyes, decretos, control de términos

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.

Al momento de definir si un control o los controles mitigan de manera adecuada el riesgo, se deben considerar aspectos como la redacción del (los) mismo(s) y evitar controles ambiguos, dado que deben dar la mayor información posible para conocer la forma como la primera línea de defensa está evitando la materialización de un riesgo y facilitar la identificación de la tipología y otros atributos para su valoración, los siguiente pasos aplican para el diligenciamiento en el formato vigente DE_FO_02 Mapa de riesgos tanto para **los riesgos de gestión, corrupción y seguridad de la información**:

Tabla N.º 14. 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" se debe colocar entre paréntesis "*Plan de contingencia*", teniendo presente que esto corresponde 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.

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, por lo cual se recomienda emplear la ilustración 10. Ciclo del proceso y las tipologías de controles.

NOTA. Para los riesgos con determinación como "Correctivos" se debe colocar entre paréntesis "*Plan de contingencia*", teniendo presente que esto corresponde a la acción 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

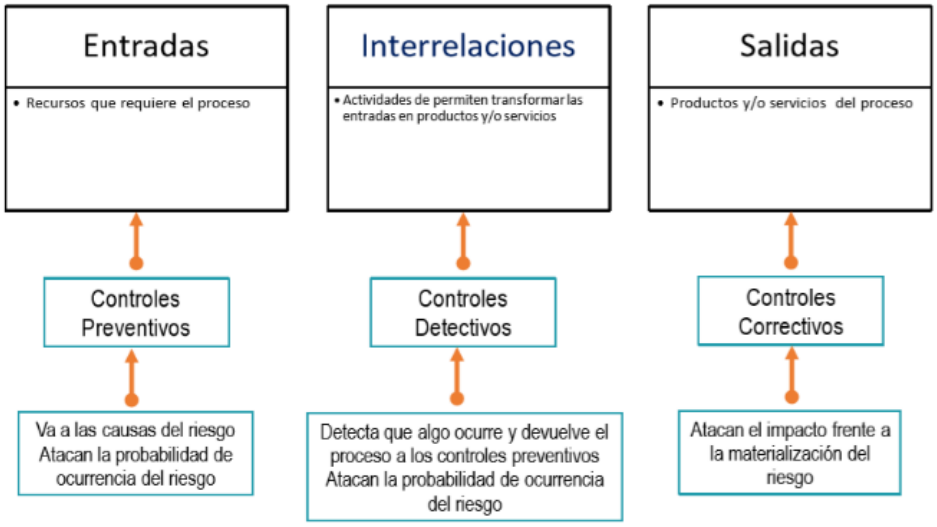

Ilustración 10. Ciclo del proceso y las tipologías de controles

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

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 observar en la siguiente tabla, teniendo presente que el diligenciamiento de estas casillas automáticamente genera la calificación de la Evaluación del Riesgo - Nivel del Riesgo Residual.**Tabla Nº 15.** Atributos de para el diseño del control

Características			Descripción	Peso
Atributos de Eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona., tiene implícito el error humano.	15%
*Atributos de Formalización	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin Documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso	-
	Frecuencia	Continua	Este atributo identifica a los controles que se ejecutan siempre que se realiza la actividad originadora del riesgo.	-
		Aleatoria	Este atributo identifica a los controles que no siempre se ejecutan cuando se realiza la actividad originadora del riesgo	-
	Evidencia	Con Registro	El control deja un registro que permite evidenciar la ejecución del control	-
		Sin Registro	El control no deja registro de la ejecución del control	-

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

***NOTA:** Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.

Dado que el Nivel de riesgo (riesgo residual): es el resultado de aplicar la efectividad de los controles al riesgo inherente. 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

Tabla 16. Estrategias para combatir los riesgos de gestión y de seguridad digital

TRATAMIENTO DEL RIESGOS	DESCRIPCIÓN
Aceptar el Riesgo	Después de realizar un análisis y considerar los niveles de riesgo, se considera asumir el mismo, conociendo los efectos de su posible materialización.
Reducir el Riesgo	Después de realizar un análisis y considerar los niveles de riesgo es alto, se determina tratarlo mediante transferir o mitigación del mismo. TRANSFERENCIA: Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional. MITIGAR: Después de realizar un análisis y considerar los niveles de riesgo, se implementan acción que mitiguen el nivel de riesgo. No necesariamente es un control adicional. **NOTA**: Para la opción de reducir, se empleará un plan de acción, para el cual 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. El plan de acción acá referido es diferente a un plan de contingencia, el cual se enmarca dentro del Plan de Continuidad de Negocio[2] y se consideraría un control correctivo.
Evitar el Riesgo	Después de realizar un análisis y considerar que el nivel de riesgo es demasiado alto, se determina NO asumir la actividad que genera este riesgo.

Fuente: Guía para la Administración del riesgo y el diseño de controles en entidades públicas, del Departamento Administrativo de la Función Pública – 2020

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 siguientes preguntas y opciones de respuesta:

Tabla N.º 17. Criterios de Evaluación- Opciones de Respuesta- **Peso de Evaluación**

[2] De acuerdo con la Guía para la preparación de las TIC para la continuidad del negocio emitida por el Ministerio TIC lo define como procedimientos documentados que guían y orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido de operación una vez presentada o tras la interrupción para garantizar la continuidad de las funciones críticas del negocio.

CRITERIO DE EVALUACION	ASPECTO A EVALUAR EN EL DISEÑO DEL CONTROL	OPCIONES DE RESPUESTA	
1. Responsable	¿Existe un responsable asignado a la ejecución del control?	Asignado = 5	No asignado= 0
	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Adecuado = 15	Inadecuado = 0
2. Periodicidad	¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna = 15	Inoportuna = 0
3. Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, Ej.: verificar, validar, cotejar, comparar, revisar, etc.?	Prevenir = 15 Detectar = 10	No es un control = 0
4. Cómo se realiza la actividad de control	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	Confiable =15	No confiable = 0
5. Qué pasa con las observaciones o desviaciones	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y resuelven oportunamente = 15	No se investigan y resuelven oportunamente=0
6. Evidencia de la ejecución del control	¿Se deja evidencia o rastro de la ejecución del control que permita a cualquier tercero con la evidencia llegar a la misma conclusión?	Completa = 10	Incompleta = 5 No existe = 0

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

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 18. 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

RANGO DE CALIFICACIÓN DEL DISEÑO DEL CONTROL	RESULTADO - PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
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 19. 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 20. 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: calificación entre 96 y 100”	fuerte (siempre se ejecuta)	fuerte + fuerte = fuerte	No
	moderado (algunas veces)	fuerte + moderado = moderado	Si

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
	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 21. 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 22. 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").

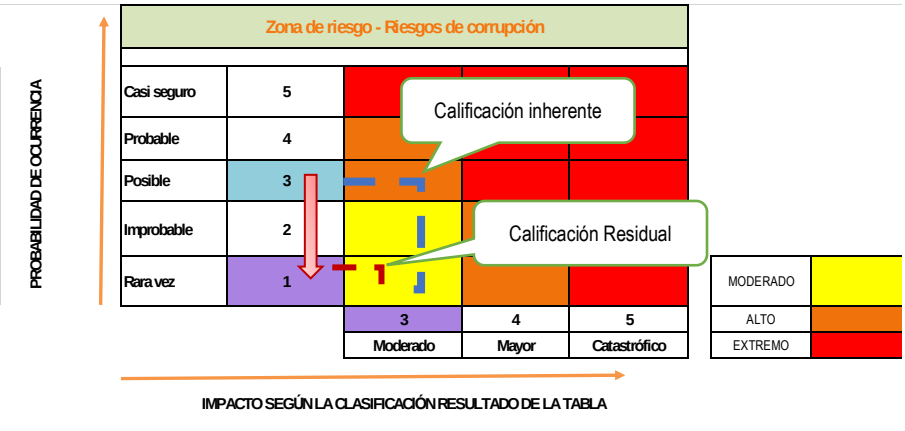

Ilustración 11. Riesgo Residual

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.

A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo, y partiendo de lo que establezca la política de administración del riesgo, los dueños 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.

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías, por lo cual se debe seleccionar una de ellas:

Tabla N.º 23. Tratamiento de Riesgo

OPCIONES DE TRATAMIENTO	DESCRIPCIÓN
Evitar el riesgo	Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.
Compartir el riesgo	Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir pero no se puede transferir su responsabilidad.
Reducir el riesgo	Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.

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

NOTA: Para el tratamiento de los riesgos la opción de **COMPARTIR**, consiste en reducir su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que

permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar, la tercerización.

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 de control, 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: Documentar la(s) acción(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: Determine para cada acción el peso porcentual, de tal forma que todas las acciones de control 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: Identificar el(los) registro(s) que evidencia (n) la implementación de cada una de las acciones establecidas.

Paso 4. Responsable: Indicar el nombre de quién posee la responsabilidad de ejecutar la acción de control, teniendo en cuenta que está en cabeza de los jefes, coordinadores, subdirectores, directores territoriales, aunque la acción de control 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 de control.

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

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

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

5.3.6.2. Tratamiento del riesgo – Riesgo de corrupción

Se deben generar acciones de control para las causas identificadas, que no poseen controles y cuando se requiere pueden ser adicionales al control que posea una causa para fortalecer su acción, es necesario que dichas acciones contribuyan a contrarrestar la causa identificada y cuando se considere necesario también se pueden identificar acciones de control diseñadas para identificar un evento o resultado no previsto después de que se haya producido, es decir detectan la situación no deseada para que se corrija y se tomen las acciones correspondientes.

Por otra parte, si la causa de un riesgo incluye a terceros, la acción de control debe establecerse teniendo en cuenta el alcance de la entidad puede adelantar conforme a su competencia.

Paso 1. Acción de control: Documentar la(s) acción(es) de control (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 de control**:** Determine para cada acción de control el peso porcentual, de tal forma que todas las acciones de control 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 de control: Identificar el(los) registro(s) que evidencia (n) la implementación de cada una de las acciones de control establecidas.

Paso 4. Responsable: Indicar el nombre de quién posee la responsabilidad de ejecutar la acción de control, teniendo en cuenta que está en cabeza de los jefes, coordinadores, subdirectores, directores territoriales, aunque la acción de control 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 de control.

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

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

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 de control.

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 esta 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 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, el cual debe ser coherente con lo establecido o programado en el mapa de riegos (plan de acción, tratamiento del riesgo o control existente). Debe ser coherente con las evidencias que fueron adjuntadas dado que es el soporten del avance o ejecución de las acciones de control, **Nota**. Las evidencias deben corresponder al registro/evidencia descritas (plan de acción, tratamiento del riesgo o control existente), adicionalmente se debe registrar el nombre de las evidencias tal cual como se reporta en el DRIVE. **Nota**: El monitoreo de los controles existentes se realizará **únicamente** para los **riesgos de corrupción.**

Paso 3. % avance (de acuerdo al peso porcentual de la acción): Registrar el porcentaje del avance para cada una de las acciones de control, teniendo en cuenta que la acción de control tiene una ejecución anual, coherente con el cumplimiento de la meta establecida para la acción de control. **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*". **Nota**. Para los controles existentes del Mapa de Riesgos de corrupción no aplica por cuanto no se tiene identificado un valor.

> **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 de control 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 y determinar para el próximo monitoreo una nueva acción.

5.4.2. 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.

Paso 1. Fecha: Corresponde a la fecha (día/mes/año) en la que se realiza el seguimiento.

Paso 2. Descripción Monitoreo: Texto que determina el análisis de las causas, así como la evaluación de la eficacia y efectividad de los controles existentes y las acciones de control establecidas, para ello se debe hacer una revisión y análisis de las evidencias que soportan la ejecución de las acciones establecidas y describir dicho seguimiento en la columna correspondiente. La información ampliada del seguimiento se evidencia en el informe que el Grupo de Control Interno elabora y publica cuatrimestralmente y presenta a la alta dirección, en el cual genera las alertas correspondientes y solicita el plan de mejoramiento que surja como resultado del seguimiento en caso de aplicar.

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 control de 100%, **por ejemplo**, para una oportunidad en el cual solo la compone una acción de control 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%. 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. 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
20/10/2021	10	Se incluyeron los parámetros para la identificación de riesgos de seguridad de la información, dentro del capítulo 5.3.1. Establecimiento del contexto. Se actualiza el formato Mapa de riesgos incluyendo la nueva hoja de "Inventario activos de información – riesgos seguridad de la información" en cumplimiento de la guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020.
07/12/2021	11	Se ajustó el nombre del Grupo de Gestión Sistemas de Información y Radiocomunicaciones – GSIR, por el Grupo de Tecnologías de la Información y Comunicación – TIC en cumplimiento de la Resolución 310 de

FECHA DE VIGENCIA VERSIÓN ANTERIOR	VERSIÓN ANTERIOR	MOTIVO DE LA ACTUALIZACIÓN
		2 de diciembre de 2021, en los lugares que se encontraba nombrado dicho grupo dentro del Instructivo. Se aclaró en el capítulo 5.4. monitoreo, revisión y seguimiento que se realizará también monitoreo, revisión y seguimiento a los controles existentes del mapa de Riesgos de Corrupción en cumplimiento de la Guía para la Administración del riesgo y el diseño de controles en entidades públicas, del Departamento Administrativo de la Función Pública – 2020.

CRÉDITOS		
Elaboró	Nombre	Mireya Cubillos Briana Lizeth Cabrera –Mónica Sandoval
	Cargo	Funcionaria – Oficina Asesora de Planeación Contratistas – Oficina Asesora de Planeación
	Fecha	17/02/2022
Revisó	Nombre	Andrea del Pilar Moreno Hernández
	Cargo	Jefe Oficina Asesora de Planeación
	Fecha:	17/02/2022
Aprobó	Nombre	Andrea del Pilar Moreno Hernández
	Cargo	Jefe Oficina Asesora de Planeación
	Fecha:	17/02/2022