INSTRUCTIVO METODOLÓGICO PARA LA ADMINISTRACIÓN DE RIESGOS DE GESTIÓN

Versión 001

Contenido

OBJETIVO

Brindar lineamientos para la adecuada gestión, valoración y tratamiento de los riesgos de gestión, identificados en cada uno de los procesos que hacen parte del Sistema de Gestión de Calidad, así como fortalecer la implementación y desarrollo de la política de administración del riesgo y el cumplimiento de la misión y objetivos de la Entidad.

Lo anterior, en cumplimiento del Decreto 1083 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, la NTC ISO 9001:2015 “Norma técnica de Gestión de la Calidad”, y la “Guía para la administración del riesgo y el diseño de controles en Entidades públicas” versión 5 del 2020, del Departamento Administrativo de la Función Pública, la Entidad bajo el presente instructivo, expone la metodología para la administración de riesgos de gestión.

ALCANCE

Este documento es aplicable para la administración de los riesgos de gestión identificados y sus correspondientes desagregaciones; así como a todos los procesos, sus responsables y a todo el personal de la Entidad que participa en la operación de los procesos del Sistema de Gestión de Calidad.

GLOSARIO

De conformidad con los lineamientos metodológicos del Departamento Administrativo de la Función Pública, se enuncian algunas definiciones importantes contenidas en el presente documento:

a) Administración de riesgos: Proceso efectuado por la Alta Dirección y por todo el personal de la Entidad para proveer a la administración una protección institucional con respecto al logro de sus objetivos. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de planeación. (INTOSAI, 2000)

b) Apetito de riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar. (DAFP, 2020)

c) Capacidad de riesgo: Es el máximo valor del nivel de riesgo que la Entidad puede soportar, a partir del cual la Alta Dirección consideraría como crítico para conllevar el logro de los objetivos propuestos. (DAFP, 2020)

d) Causa Inmediata: Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo. (DAFP, 2020)

e) Causa Raíz: Causa principal o básica. Corresponde a las razones por la cuales se puede presentar el riesgo. (DAFP, 2020)

f) Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo. (DAFP, 2020)

g) Colaboradores: Funcionario público o contratista de prestación de servicios de la Agencia Nacional de Infraestructura. (Elaboración propia)

h) Consecuencia: 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. (DAFP, 2020)

i) Control: Medida que permite reducir o mitigar un riesgo. (DAFP, 2020)

j) Evento: Posibilidad[1] de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia[2] de acontecimientos externos.[3] (DAFP, 2020)

k) Impacto: Consecuencias que puede ocasionar a la Entidad la materialización del riesgo. (DAFP, 2020)

l) Líneas de defensa: Esquema que define la asignación de responsabilidades y roles para la gestión del riesgo y el control. (DAFP, 2019)

m) Mapas de riesgo: Documento que resume los resultados de las actividades de gestión de riesgos, incluye una representación gráfica en modo de mapa de calor de los resultados de la evaluación de riesgos. (DAFP, 2020)

n) Nivel de 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. (DAFP, 2020)

[1] Un evento puede consistir en algo que no está sucediendo.
[2] Un evento puede ser una o más ocurrencias y puede tener varias causas
[3] En ocasiones se puede hacer referencia a un evento como incidente o accidente.

o) Probabilidad: Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año. (DAFP, 2020)

p) Riesgo Inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad. (DAFP, 2020)

q) Riesgo Residual: El resultado de aplicar la efectividad de los controles al riesgo inherente. (DAFP, 2020)

r) Riesgos: Efecto que se causa sobre los objetivos de las Entidades, debido a eventos potenciales. (DAFP, 2020)

s) Tolerancia del riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad. (DAFP, 2020).

NORMATIVIDAD

La Entidad se rige bajo los parámetros y lineamientos metodológicos que sobre la materia imparte el Departamento Administrativo de la Función Pública - DAFP, en concordancia con el Modelo Estándar de Control Interno, los requisitos de la norma ISO 9001:2015, y lo dictado en la norma ISO 31000:2018.

Tabla 1 Normatividad asociada a los riesgos de gestión

Marco legal y normativo		
No.	**Ley/Decreto/Norma**	**Epígrafe**
1	Ley 87 de 1993	"Por la cual se establecen normas para el ejercicio del control interno en las Entidades y organismos del estado y se dictan otras disposiciones"
2	Ley 489 de 1998	"Por la cual se dictan normas sobre la organización y funcionamiento de las Entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189 de la Constitución Política y se dictan otras disposiciones."
3	Decreto 1083 de 2015	"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública."
6	Guía para la administración del riesgo Versión 5	Metodología para la Administración del Riesgo y el diseño de controles en Entidades públicas. Departamento Administrativo de la Función Pública.
7	Norma ISO 9001:2015	Norma Técnica de Calidad
8	Norma ISO 31000:2018	Norma Técnica de Gestión del Riesgo.

Fuente: Elaboración propia

DESCRIPCIÓN

2.1 ROLES Y RESPONSABILIDADES (ESQUEMA DE LÍNEAS DE DEFENSA)

Se referencian las partes o actores institucionales involucrados en la administración de riesgos, sus funciones y sus competencias, establecidos en el esquema de líneas de defensa.

a) Consejo Directivo (Línea Estratégica): Es el máximo responsable de la gestión de riesgos de la Entidad. Este órgano de Gobierno es el encargado de brindar asesoría y supervisión a las vicepresidencias y a la Presidencia de la ANI, en la gestión de los riesgos relacionados con la Agencia y los proyectos de infraestructura de transporte que esta gestiona. Por ello, el Consejo, es el responsable de aprobar y mantener actualizada la Política de Gestión Integral de Riesgos y aprueba (si aplica) el apetito a los riesgos de la ANI, herramienta que facilita identificar y gestionar los riesgos institucionales relevantes para la Entidad.

   El Consejo también debe informar anualmente a la comunidad, cómo la Agencia gestiona los riesgos, mediante el informe anual de gestión en materia de Gestión Integral de Riesgos.

b) Presidencia: al igual que el Consejo Directivo, el Presidente es el máximo responsable de verificar la gestión de riesgos de la Entidad, especialmente aquellos que por su carácter previsible pueden ser mitigados mediante esfuerzos realizados por la administración de la Entidad.

c) Vicepresidencias: Velan por la aplicación de la Política y aseguran los recursos para su implementación. Además, reportan periódicamente la adecuada gestión de los riesgos relacionados con sus vicepresidencias y establecen planes de acción para mitigar riesgos y cerrar brechas.

d) Líderes y responsables de proceso (Primera línea de defensa): Son los directos responsables de llevar a cabo la ejecución de la administración del riesgo de cada uno de los procesos en los cuales participan, al identificar, evaluar, controlar, mitigar y realizar seguimiento a sus riesgos, en procura de un mantenimiento efectivo de los controles diseñados.

e) Grupo Interno de Trabajo de Planeación (Segunda línea de defensa): Es la encargada de capacitar y asesorar a la primera línea de defensa, y de asegurarse que los controles y procesos de gestión del riesgo sean apropiados y funcionen correctamente en la Entidad.

f) Oficina de Control Interno (Tercera línea de defensa): Es la responsable de evaluar la gestión del riesgo, monitorear la exposición de la organización al riesgo, realizar recomendaciones

de forma independiente con alcance preventivo e informar los hallazgos producto de las auditorías.

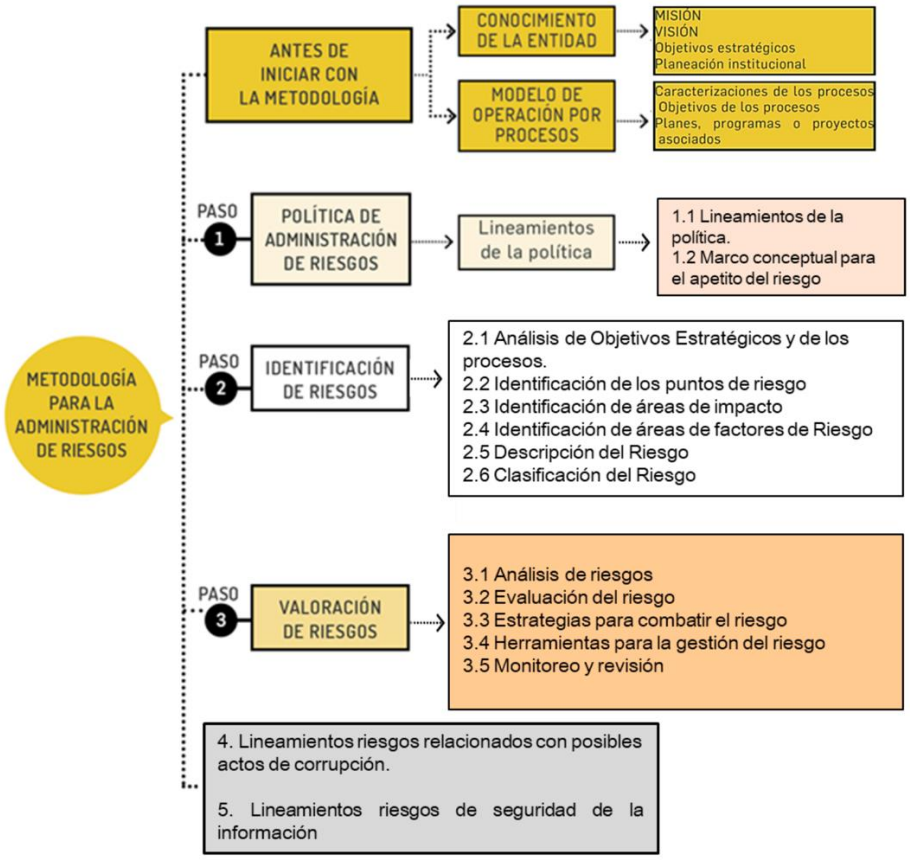
g) Colaboradores: Son los responsables de ejecutar los diferentes tipos de controles a los riesgos identificados.

h) Equipos de riesgos: Como mecanismo de gestión, son los designados por cada uno de los líderes de procesos para realizar como primera línea, la gestión que se requiera frente a la actualización y seguimiento de los mapas de riesgos de gestión.

2.2 GENERALIDADES DE LA METODOLOGÍA

La administración del riesgo en la Agencia Nacional de Infraestructura está compuesta por distintas fases, cuyo marco de referencia se construye necesariamente de manera cíclica a partir de la toma de decisiones de la Alta Dirección de la Entidad, lo que da lugar a la elaboración, implementación, monitoreo y revisión del documento de referencia para la gestión del riesgo, además de la mejora continua en el diseño de la metodología, en concordancia con la "Guía para la administración del riesgo y el diseño de controles en Entidades Públicas" versión 5, emitida por el Departamento Administrativo de la Función Pública.

Ilustración 1 Metodología para la Administración del Riesgo



Fuente: Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, Versión 5, Departamento Administrativo de la Función Pública.

2.3 CONOCIMIENTO DE LA ENTIDAD

Tal como se evidencia en la ilustración anterior, antes de iniciar con la identificación de los riesgos es importante analizar contextualmente la situación propia de la Entidad. En la Agencia Nacional de Infraestructura el contexto organizacional, con base en el Decreto 4165 de 2011 "Por el cual se cambia la naturaleza jurídica, cambia la denominación y se fijan otras disposiciones del Instituto Nacional de Concesiones – INCO", se analiza de manera interna y externa, de tal manera que se prevé los retos a los cuales se enfrenta la Entidad. El análisis externo le permite a la Agencia identificar la capacidad competitiva y las dinámicas en las que esta subsiste, mientras que el análisis del entorno interno permite determinar la capacidad o los posibles riesgos de la interrelación entre los procesos y las habilidades o fortalezas de la Entidad.

A través de la jornada de planeación estratégica se analiza el entorno interno, de acuerdo con lo establecido en el Instructivo "Elaboración, actualización y seguimiento del plan estratégico, plan de

acción y plan operativo" (SEPG-I-008). Esto da como resultado, la definición o actualización de la misión y visión institucional, los objetivos estratégicos, el plan estratégico y el plan de acción institucional, los cuales deben ser consultados por los equipos de riesgos en la página web de la Entidad, con el fin de comprender la dinámica organizacional para la identificación de los riesgos.

2.4 MODELO DE OPERACIÓN POR PROCESOS

La ANI opera bajo un modelo de operación por procesos, el cual es una herramienta para la mejora en la prestación de los servicios, que permite establecer estándares de operación organizacional enmarcados en la cadena de valor al definir los procesos a partir del entendimiento de las necesidades de los usuarios y vinculando los atributos de calidad requeridos.

Por tal razón, es necesario que los equipos de riesgos conozcan la descripción y la interrelación entre los procesos del Sistema de Gestión de Calidad, basado en el mapa de procesos y las caracterizaciones de estos, disponibles en la página web de la entidad.

2.5 POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

La Política de Administración de Riesgos (SEPG-PT-003) es la declaración de la Alta Dirección y las intenciones generales de la Entidad con respecto a la Gestión del Riesgo. Esta se establece por la Alta Dirección, con el liderazgo del Presidente de la Agencia y la participación del Comité Institucional de Coordinación de Control Interno.

Los equipos de riesgos por proceso deben consultar esta política, publicada en la página web institucional, con el fin de conocer el apetito, la tolerancia del riesgo y la capacidad de riesgo, así como los lineamientos establecidos por la Alta Dirección frente a la materia.

2.6 IDENTIFICACIÓN DE RIESGOS

En la ANI, se ha definido el sitio en SharePoint para la Gestión Integral de Riesgos el cual se puede consultar en el siguiente enlace: https://anionline.sharepoint.com/sites/GIR. El acceso a este sitio es exclusivo para los integrantes de los equipos de riesgos de la Agencia y el responsable de otorgar el respectivo permiso de ingreso es el Grupo Interno de Trabajo de Planeación.

En este se encuentra una sección para centralizar la información de la identificación, actualización y seguimiento a los mapas de riesgos. Para ello es necesario tener en cuenta el contexto estratégico, las caracterizaciones de los procesos y el formato "Mapa de riesgo por proceso y seguimiento a los riesgos" (SEPG-F-030) formalizado en el Sistema de Gestión de Calidad – SGC y publicado en la página web institucional.

2.7 ANÁLISIS DE OBJETIVOS ESTRATÉGICOS Y DE LOS PROCESOS

La identificación del riesgo se realiza a partir de las actividades definidas en la caracterización de cada uno de los procesos las cuales, como se mencionó con anterioridad, deben ser revisadas con

el fin de asegurar que atiendan al contexto organizacional y a los objetivos estratégicos institucionales, dado que todos los riesgos que se identifiquen deben tener impacto en el cumplimiento de los objetivos estratégicos o del objetivo del proceso.

Para ello, una vez ingresado al sitio de SharePoint para la Gestión Integral de Riesgos y seleccionado el proceso al que se pertenece, en la primera parte del formato (SEPG-F-030) denominada "Características del proceso" se debe transcribir el objetivo, las actividades y las partes interesadas internas y externas, las cuales se encuentran en la caracterización del proceso.

Tabla 2 Características del mapa de riesgos por proceso y seguimientos a los riesgos

CARACTERÍSTICAS DEL PROCESO		
ACTIVIDADES DEL PROCESO	PARTES INTERESADAS (INTERNAS)	PARTES INTERESADAS (EXTERNAS)

Fuente: Elaboración propia, con el Mapa de riesgos por proceso y seguimientos a los riesgos SEPG-F-030.

Una vez definidos estos parámetros, se debe realizar una identificación o tipificación preliminar del riesgo para su correcta descripción en la segunda parte del formato denominada "Puntos, áreas y factores de riesgo".

Tabla 3 Puntos, áreas y factores del mapa de riesgos por proceso y seguimientos a los riesgos

PUNTOS, ÁREAS Y FACTORES DE RIESGO		
PUNTO DE RIESGO	ÁREAS DE IMPACTO	FACTORES DE RIESGO

Fuente: Elaboración propia, con el Mapa de riesgos por proceso y seguimientos a los riesgos SEPG-F-030.

2.8 IDENTIFICACIÓN DE LOS PUNTOS DE RIESGOS

Los puntos de riesgos son actividades dentro del flujo del proceso en las cuales existe alguna posibilidad de que puedan ocurrir eventos de riesgo relacionados con la gestión y que por ende deben ser controlados para asegurar que el proceso cumpla con su objetivo. Estos puntos se deben identificar para cada una de las actividades del proceso, con el fin de determinar de forma preliminar si existe algún indicio de riesgo, seleccionando una opción de la lista desplegable en el formato. Tal como se evidencia en la siguiente ilustración, los puntos de riesgos son: insumos, procesos, productos, resultados e impactos.

Ilustración 2 Puntos de riesgos en la cadena de valor público

Fuente: Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, Versión 5, Departamento Administrativo de la Función Pública.

2.9 IDENTIFICACIÓN DE ÁREAS DE IMPACTO

El área de impacto, la cual se define como la consecuencia a la cual se vería expuesta la Entidad en caso de materializarse un riesgo. Las áreas de impacto son: económica, reputacional, o económica y reputacional. Según aplique se debe seleccionar la opción en la lista desplegable.

Dentro del área de impacto económica se encuentran afectaciones tales como la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal, entre otros. Por su parte, dentro del área de impacto reputacional se encuentra todo lo relacionado con la afectación a la imagen institucional por asuntos tales como fallas en la prestación del servicio, vulneraciones a la información, entre otros.

2.10 IDENTIFICACIÓN DE ÁREAS DE FACTORES DE RIESGO

Los factores de riesgo son aquellas fuentes que generan riesgos. Se debe seleccionar en la lista desplegable el factor más pertinente de acuerdo con la especificidad de cada actividad, a continuación, se desarrolla cada uno de ellos.

Tabla 4 Factores de riesgo

Factor	Definición	Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización	Falta de procedimientos.
		Errores de grabación, autorización.
		Errores en cálculos para pagos internos y externos.
		Falta de capacitación, temas relacionados con el personal.
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.	Hurtos activos.
		Posibles comportamientos no éticos de los empleados.
		Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la Entidad	Daño de equipos.
		Caída de aplicaciones.
		Caída de redes.
		Errores en programas.
Infraestructura	Eventos relacionados con la infraestructura física de la Entidad.	Derrumbes.
		Incendios.
		Inundaciones.
		Daños a activos fijos.
Evento externo	Situaciones externas que	Suplantación de identidad.
		Asalto a la oficina.
		Atentados, vandalismo, orden público.

Fuente: Elaboración propia, con base en la Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, Versión 5, Departamento Administrativo de la Función Pública

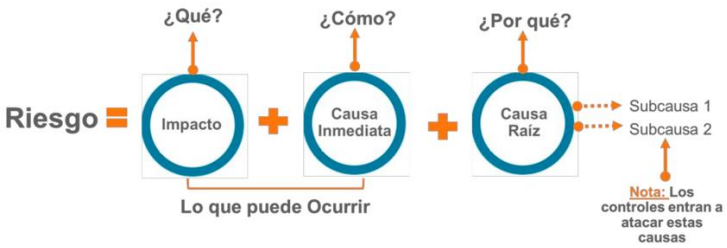
2.11 DESCRIPCIÓN DEL RIESGO

Una vez identificados los puntos, áreas y factores del riesgo, el siguiente paso es elaborar su descripción. Para facilitar el ejercicio, se recomienda tener 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, la satisfacción de un usuario, entre otros. A continuación, se listan algunos aspectos a tener en cuenta:

- Resultados de las auditorías internas y externas.
- Resultados de las actividades de rendición de cuentas.
- Medición del desempeño institucional en periodos anteriores.
- Medición de la satisfacción de grupos de valor en periodos anteriores.
- Medición de indicadores de los procesos.
- Medición de los servicios y tratamiento no conforme.
- Resultados de la evaluación de las obligaciones de cumplimiento legal y otros.
- Situaciones latentes que puedan generar impactos negativos.
- Otros eventos identificados.

La descripción del riesgo debe contener todos los detalles que sean necesarios para que sea de fácil entendimiento para personas ajenas al proceso. La estructura para describir el riesgo debe iniciar con la expresión "Posibilidad de" y continuar como se detalla en la siguiente ilustración.

Ilustración 3 Elementos de la descripción del riesgo



Fuente: Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, Versión 5, Departamento Administrativo de la Función Pública.

Esta descripción se debe realizar en la parte del formato denominada "Descripción del riesgo" en el cual se encuentra dividido cada uno de los elementos anteriormente señalados, con el fin de facilitar su redacción. A continuación, se desglosan cada uno de ellos:

- **Impacto:** Consecuencias que puede ocasionar a la Entidad la materialización del riesgo.
- **Causa inmediata:** Circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo. Estas no constituyen la causa principal o la causa base para que se presente el riesgo.
- **Causa raíz:** Causa principal o básica. Es la razón principal por la cual se puede presentar el riesgo, de modo que esta debe corresponder a la actividad del proceso que está siendo analizada. Es la base para la definición de controles en la etapa de valoración del riesgo.

Se debe tener en cuenta que para un mismo riesgo puede existir más de una causa o subcausas que pueden ser analizadas, para lo cual se sugiere el uso de la metodología de árbol de problemas, especialmente porque permite identificar el problema, efecto y causas secundarias que deben ser controladas.
Recomendaciones para la redacción del riesgo:

a. No describir como riesgos omisiones ni desviaciones del control. Ejemplo: Errores en la liquidación de la nómina por fallas en los procedimientos existentes.
b. No describir causas como riesgos. Ejemplo: Inadecuado funcionamiento de la plataforma estratégica donde se realiza el seguimiento a la planeación.
c. No describir riesgos como la negación de un control. Ejemplo: Retrasos en la prestación del servicio por no contar con digiturno para la atención.

d. No existen riesgos transversales, lo que pueden existir son causas transversales. Puede ser un riesgo asociado a la gestión documental, a la gestión contractual o jurídica y en cada proceso sus controles son diferentes. Ejemplo: Pérdida de expedientes.
e. No describir riesgos como la negación de un control. Ejemplo: Retrasos en la prestación del servicio por no contar con digiturno para la atención.

2.12 CLASIFICACIÓN DEL RIESGO

Realizada la identificación y la descripción del riesgo, el paso siguiente es clasificarlo dentro de las categorías que se exponen en la siguiente ilustración, para lo cual se deberá seleccionar la opción que más corresponda en la lista desplegable del formato trabajado.

Tabla 5 Clasificación del riesgo

Clasificación	Definición	Factor asociado
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.	Procesos
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).	Evento externo
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.	Talento humano
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.	Tecnología
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	Varios factores
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.	Varios factores
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.	Infraestructura y evento externo

Fuente: Elaboración propia, con base en la Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, Versión 5, Departamento Administrativo de la Función Pública

Para facilitar la clasificación del riesgo, se debe tener presente que existe una relación directa entre estas categorías y los factores de riesgo expuestos, tal como se ilustra a continuación:

Ilustración 4 Relación entre factores de riesgo y clasificación del riesgo

Fuente: Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, Versión 5, Departamento Administrativo de la Función Pública

2.13 VALORACIÓN DE RIESGOS

Una vez identificado, descrito y clasificado el riesgo, se debe proceder con su valoración, la cual contempla dos etapas: el análisis del riesgo, en la cual se debe establecer la probabilidad de ocurrencia del riesgo y su nivel de impacto, con el propósito de estimar la zona de riesgo inicial, denominada riesgo inherente y; la evaluación del riesgo, en donde se confrontan los resultados de análisis de riesgo inicial, frente a los diferentes tipos de controles establecidos, con el fin de determinar la zona final del riesgo, denominada zona riesgo residual.

2.14 ANÁLISIS DEL RIESGO

Esta etapa el equipo de riesgos debe diligenciar la parte denominada “Riesgo inherente” del formato del mapa de riesgos por proceso SEPG-F-030, el cual se busca establecer la probabilidad de ocurrencia del riesgo y sus posibles consecuencias.

Tabla 6 Riesgo inherente riesgos de gestión y seguridad digital

RIESGO INHERENTE					
Frecuencia de la actividad (Al año)	PROBABILIDAD	Afectación económica	Pérdida reputacional	IMPACTO	NIVEL DE RIESGO INHERENTE

Fuente: Elaboración propia, con el Mapa de riesgos por proceso y seguimientos a los riesgos SEPG-F-030.

2.15 PROBABILIDAD

La probabilidad es entendida como la posibilidad de ocurrencia del riesgo. Está asociada a la frecuencia con la cual se lleva a cabo la actividad del proceso que se está analizando, es decir, la probabilidad debe corresponder al número de veces que se realiza la actividad asociada con el riesgo en el periodo de un año, dado que esto le indica al proceso el número de veces en que se ve expuesto al riesgo. La frecuencia se puede determinar utilizando como recurso datos históricos, actividades programadas en el plan operativo, metodologías de estándares estadísticos, entre otras fuentes de información.

Una vez se identifique la frecuencia del riesgo, se debe asociar la escala que más se ajusta con el número de veces en que se ejecuta la actividad al año, en la lista desplegable y en la columna para la probabilidad inherente dispuesta en el formato, la cual corresponde que se muestra en la tabla expuesta a continuación:

Tabla 7 Probabilidad

TABLA DE PROBABILIDAD			
			Frecuencia de la actividad
Probabilidad	Muy baja (20%)	(0-20%)	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año
	Baja (40%)	(21-40%)	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año
	Media (60%)	(41-60%)	La actividad que conlleva el riesgo se ejecuta de 25 a 499 veces por año
	Alta (80%)	(61-80%)	La actividad que conlleva el riesgo se ejecuta de 500 a 5000 veces por año
	Muy alta (100%)	(81- 100%)	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año

Fuente: Elaboración propia, con base en la Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, Versión 5, Departamento Administrativo de la Función Pública.

2.16 IMPACTO

Una vez identificada la probabilidad, se debe realizar un análisis del impacto como segunda unidad de medida del análisis de riesgo. Para ello, debe entenderse como impacto las consecuencias que trae para la Entidad la materialización del riesgo. Los impactos contemplan dos variables principales: impactos económicos e impactos reputacionales. Por esta razón, debe seleccionarse en la lista desplegable el criterio más objetivo de acuerdo con la tabla expuesta a continuación y teniendo en cuenta el área de impacto seleccionada en el numeral 4.9

Tabla 8 Impacto

	TABLA DE IMPACTO			
			Afectación económica o presupuestal	Pérdida reputacional
Impacto	Leve (20%)	(0-20%)	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la entidad
	Menor (40%)	(21-40%)	Afectación entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente; de conocimiento general a nivel interno, junta directiva, accionistas y/o de proveedores
	Moderado (60%)	(41-60%)	Afectación entre 51 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia, frente al logro de los objetivos.
	Mayor (80%)	(61-80%)	Afectación entre 101 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental y/o municipal.
	Catastrófico (100%)	(81- 100%)	Afectación mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país.

Fuente: Elaboración propia, con base en la Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, Versión 5, Departamento Administrativo de la Función Pública.

De otra parte, se debe tener en cuenta que, si en el riesgo analizado inicialmente se contempló las áreas de impacto económica y reputacional, se debe analizar en qué escala se encuentra cada una, referenciarlas en las listas desplegables del formato y finalmente tomar el nivel de impacto más alto entre estas dos.

2.17 EVALUACIÓN DEL RIESGO

A partir del análisis y la determinación de la probabilidad de ocurrencia del riesgo y su impacto en caso de materialización, se debe identificar la zona de riesgo inicial, también denominada zona de riesgo inherente.

2.18 RIESGO INHERENTE

El riesgo inherente es el nivel de riesgo propio de la actividad, es decir, es el nivel de exposición al riesgo que tiene la Entidad, bajo un escenario sin controles. Para hallar el nivel de severidad del riesgo inherente, es necesario ir a la hoja de Excel del formato denominada “Mapa de calor” (ver Tabla No. 9). Este instrumento facilita el análisis gráfico ya que contiene las cuatro (4) posibles zonas de riesgo, también denominadas niveles de severidad del riesgo: Extremo, alto, moderado y bajo.

Tabla 9 Mapa de calor

			MAPA DE CALOR				
			Impacto				
			Leve (20%)	Menor (40%)	Moderado (60%)	Mayor (80%)	Catastrófico (100%)
			(0-20%)	(21-40%)	(41-60%)	(61-80%)	(81-100%)
Probabilidad	Muy alta (100%)	(81- 100%)	Alto	Alto	Alto	Alto	Extremo
	Alta (80%)	(61-80%)	Moderado	Moderado	Alto	Alto	Extremo
	Media (60%)	(41-60%)	Moderado	Moderado	Moderado	Alto	Extremo
	Baja (40%)	(21-40%)	Bajo	Moderado	Moderado	Alto	Extremo
	Muy baja (20%)	(0-20%)	Bajo	Bajo	Moderado	Alto	Extremo

Fuente: Elaboración propia, con base en la Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, Versión 5, Departamento Administrativo de la Función Pública.

Posteriormente, se debe realizar un cruce entre el nivel de probabilidad y el nivel de impacto determinados previamente. A continuación, se presenta un ejemplo para hallar el nivel de riesgo inherente, con una probabilidad media (60%), un impacto mayor (80%) lo que da como resultado un nivel de riesgo alto.

Tabla 10 Ejemplo Riesgo Inherente

			MAPA DE CALOR				
			Impacto				
			Leve (20%)	Menor (40%)	Moderado (60%)	Mayor (80%)	Catastrófico (100%)
			(0-20%)	(21-40%)	(41-60%)	(61-80%)	(81-100%)
Probabilidad	Muy alta (100%)	(81- 100%)	Alto	Alto	Alto	Alto	Extremo
	Alta (80%)	(61-80%)	Moderado	Moderado	Alto	Alto	Extremo
	Media (60%)	(41-60%)	Moderado	Moderado	Moderado	Alto	Extremo
	Baja (40%)	(21-40%)	Bajo	Moderado	Moderado	Alto	Extremo
	Muy baja (20%)	(0-20%)	Bajo	Bajo	Moderado	Alto	Extremo

Fuente: Elaboración propia, con base en la Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, Versión 5, Departamento Administrativo de la Función Pública.

La escala determinada para la probabilidad e impacto del riesgo, deben seleccionarse en la lista desplegable de la hoja de Excel “Mapa de riesgos” del mismo formato con código SEPG-F-030. Se debe hacer lo propio con los niveles de probabilidad e impacto correspondientes a la escala seleccionada, y con el nivel de riesgo inherente identificado.

Lo anterior, permite analizar desde un panorama general los riesgos que deben priorizarse según la zona en que quedaron ubicados (zona de riesgo bajo, moderado, alto o extremo) facilitando al líder

del proceso, y en general a la Alta Dirección, la evaluación de prioridades, la determinación de controles, la decisión del tratamiento al riesgo y la implementación de planes de mitigación.

2.19 DESCRIPCIÓN DE CONTROLES

Posterior a la valoración del riesgo, se deben implementar controles que disminuyan la probabilidad o impacto del riesgo. Un control es la medida que permite reducir o mitigar el riesgo. La identificación de controles debe realizarse en la parte del formato denominada "Descripción del control" para cada uno de los riesgos identificados, a través de mesas de trabajo al interior de cada equipo de riesgos, utilizando el criterio de experto, documentos formalizados en el Sistema de Gestión de Calidad, entre otras herramientas. Los responsables de implementar, realizar seguimiento y actualizar los controles definidos, son los líderes de proceso con el apoyo de su equipo de riesgos.

Tabla 11 Descripción del control

DESCRIPCIÓN DEL CONTROL				
RESPONSABLE	ACCIÓN	COMPLEMENTO	No.	CONTROL

Fuente: Elaboración propia, con el Mapa de riesgos por proceso y seguimientos a los riesgos SEPG-F-030.

La redacción del control debe tener en cuenta la estructura que se menciona a continuación, la cual facilitará identificar sus diferentes atributos:

Descripción del control = Responsable + Acción + Complemento.

- Responsable: Se debe relacionar el cargo del coordinador, gerente, o jefe del área responsable de ejecutar el control. Para los casos en los cuales el control lo ejecuta un servidor público en específico se debe relacionar su cargo, de lo contrario, se debe generalizar a todos los colabores del área asignados.
- Acción: Se debe iniciar con verbos en infinitivo que indiquen la acción que se realiza como parte del control. Por ejemplo: Verificar, validar, revisar, cotejar, entre otros.
- Complemento: Se deben indicar todos los detalles que permitan entender claramente el objeto del control. Dentro de estos es obligatorio definir la periodicidad establecida para la ejecución del control, el propósito del control, la herramienta utilizada o la explicación de cómo se realiza la acción del control y la evidencia resultante de su ejecución.

Esta información debe incluirse en cada una de las casillas con el mismo nombre, establecidas en la parte del formato mencionada. Una vez diligenciadas, en la celda de la columna "Control" se podrá evidenciar su redacción definitiva.

2.20 ATRIBUTOS DEL CONTROL

2.20.1 TIPOS DE CONTROLES

Posterior a la descripción del control, en la casilla "Tipo de control" debe seleccionarse la tipología a la que corresponde, de acuerdo con la siguiente tabla:

Tabla 12 Tipos de controles

Tipo de control	Descripción	Etapa en la que se ejecuta
Control Preventivo	El control va dirigido a las causas del riesgo. Permite disminuir la probabilidad de que el riesgo ocurra. Busca establecer las condiciones que aseguren el resultado final esperado.	El control se ejecuta en la entrada del proceso, es decir, antes de que se realice la actividad originadora del riesgo.
Control Detectivo	El control permite detectar alguna anomalía, irregularidad o desviación en el desarrollo de la actividad. Permite disminuir la probabilidad de que el riesgo ocurra. Detecta el riesgo, pero genera reprocesos.	El control se ejecuta en las interrelaciones del proceso, es decir, durante la ejecución de la actividad originadora del riesgo.
Control Correctivo	El control se ejecuta después de que se ha materializado el riesgo. Permite disminuir el impacto de su materialización. Tienen costos implícitos.	El control se ejecuta en las salidas del proceso, es decir, una vez finalizada la actividad originadora del riesgo.

Fuente: Elaboración propia, con base en la Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, Versión 5, Departamento Administrativo de la Función Pública.

2.20.2 TIPOS DE IMPLEMENTACIÓN DEL CONTROL

Posteriormente, en la casilla "Implementación" se debe seleccionar en la lista desplegable la forma en la cual se implementará el control, de acuerdo con la siguiente tabla:

Tabla 13 Tipos de implementación del control

Tipo de implementación	Descripción
Control Manual	El control es ejecutado directamente por los colaboradores de la Entidad.
Control Automático	El control es ejecutado por un sistema tecnológico.

Fuente: Elaboración propia, con base en la Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, Versión 5, Departamento Administrativo de la Función Pública

2.20.3 ATRIBUTOS INFORMATIVOS DE LA IMPLEMENTACIÓN DEL CONTROL

Seguido de los tipos de implementación del control, se debe identificar y seleccionar los atributos informativos de su implementación, según correspondan, los cuales se relacionan a continuación:

Tabla 14 Atributos informativos de implementación del control

Tipo de implementación	Opción	Descripción
Documentación	Documentado	Controles documentados en el Sistema Integrado de Gestión.
	Sin documentar	Controles que se ejecutan, pero que NO están documentados en el Sistemas Integrado de Gestión.
Frecuencia	Continua	El control se aplica siempre que se realiza la actividad relacionada con el riesgo.
	Aleatoria	El control NO se aplica cada vez que se realiza la actividad relacionada con el riesgo, sino aleatoriamente.
Evidencia	Con registro	El control deja un registro que permite evidenciar su ejecución.
	Sin registro	El control no deja registro de su ejecución.

Fuente: Elaboración propia, con base en la Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, Versión 5, Departamento Administrativo de la Función Pública

2.21 VALORACIÓN DEL CONTROL

2.21.1 CALIFICACIÓN DEL CONTROL

Definidos los atributos del control, en la casilla “Calificación del control” del mencionado formato, de manera automática se realizarán los cálculos que determinan el peso porcentual del control, de acuerdo con la siguiente tabla:

Tabla 15 Calificación del control por sus atributos

CARACTERISTICAS			PESO
ATRIBUDOS DE EFICIENCIA	Tipo	Preventivo	25%
		Detectivo	15%
		Correctivo	10%
	Implementación	Automático	25%
		Manual	15%
Valoración del control			Total %

Fuente: Elaboración propia, con base en la Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, Versión 5, Departamento Administrativo de la Función Pública

Los atributos de información, si bien se constituyen como variables inherentes a los controles, no tienen peso alguno en su calificación, pues no influyen en su efectividad y por lo tanto funcionan únicamente como elementos descriptivos de índole cualitativa que permite caracterizarlos de una mejor manera.

2.21.2 PROBABILIDAD E IMPACTO RESIDUAL

Para calcular la reducción de la probabilidad y el impacto del riesgo, se requiere realizar una serie de operaciones, teniendo en cuenta los controles diseñados, su tipo y su calificación. Los controles preventivos y detectivos disminuyen la probabilidad, mientras que los controles correctivos disminuyen el impacto.

Para hallar la probabilidad residual, en los casos frente a los cuales el riesgo sólo tiene un (1) control preventivo o detectivo, la operación es la siguiente:

Tabla 16 Cálculo para la probabilidad residual con un solo control

Probabilidad Residual (Un sólo control preventivo o detectivo)		
Pasos	**Fórmulas**	**Ejemplo**
		Probabilidad inherente = 80% Calificación control No. 1 = 40%
Paso 1: Casilla "Probabilidad x Control"	% de probabilidad inherente[1] * % de la calificación del control preventivo o correctivo[2] = Valor 1	80% * 40% = 32%
Paso 2: Casilla "Probabilidad después del control"	% de probabilidad inherente - Valor 1 = % de probabilidad residual (definitiva)	80% - 32% = 48%

Fuente: Elaboración propia, con base en la Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, Versión 5, Departamento Administrativo de la Función Pública

Frente al cálculo del impacto residual, en los casos frente a los cuales el riesgo sólo se tiene un (1) control correctivo, la operación es la siguiente:

Tabla 17 Cálculo para el impacto residual con un solo control

Impacto Residual (Un solo control correctivo)		
Pasos	**Fórmulas**	**Ejemplo**
		Impacto inherente = 60% Calificación control No. 1 = 25%
Paso 1: Casilla "Impacto x Control"	% de impacto inherente * % de la calificación del control correctivo = Valor 1	60% * 25% = 15%
Paso 2: Casilla "Impacto después del control"	% de impacto inherente - Valor 1 = % de impacto residual (definitiva)	60% - 15% = 45%

Fuente: Elaboración propia, con base en la Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, Versión 5, Departamento Administrativo de la Función Pública

Este cálculo se debe realizar manualmente en las casillas indicadas. Por su parte, en el caso de que se haya diseñado más de un control, lo primero será realizar la operación señalada y posteriormente, para los demás controles, hacer lo propio tomando como referencia el resultado de la probabilidad o impacto, según corresponda, dada en el control inmediatamente anterior.
Para entenderlo con mayor facilidad, a continuación, se relacionan los diferentes pasos para determinar la probabilidad residual, en los casos frente a los cuales el riesgo tiene dos (2) o más controles detectivos o preventivos, con su respectivo ejemplo:

Tabla 18 Cálculo para la probabilidad residual con dos o más controles

Probabilidad Residual (Dos o más controles correctivos)		
Pasos	**Fórmulas**	**Ejemplo** **Probabilidad inherente = 80%** **Calificación control No. 1 = 40%** **Calificación control No. 2 = 30%**
Paso 1 (Control 1): Casilla "Probabilidad x Control"	% de probabilidad inherente * % de la calificación del control preventivo o correctivo no. 1 = Valor 1	80% * 40% = 32%
Paso 2 (Control 1): Casilla "Probabilidad después del control"	% de probabilidad inherente - Valor 1 = % de probabilidad residual (resultado 1)	80% - 32% = 48%
Paso 3 (Control 2): Casilla "Probabilidad x Control"	% de probabilidad residual (resultado 1) * % calificación del segundo control preventivo o correctivo = Valor 2	48% * 30% = 14,4%
Paso 4 (Control 2): Casilla "Probabilidad después del control"	% de probabilidad residual (resultado 1) - Valor 2 = % de probabilidad residual (definitiva)	48% - 14,4% = 33,60%

Fuente: Elaboración propia, con base en la Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, Versión 5, Departamento Administrativo de la Función Pública

Frente al cálculo para el impacto residual, en los casos en los cuales el riesgo sólo tenga más de un control tiene un (1) control correctivo, la operación es la siguiente:

Tabla 19 Cálculo para el impacto residual con dos o más controles

Impacto Residual (Dos o más controles correctivos)		
Pasos	**Fórmulas**	**Ejemplo** **Impacto inherente = 60%** **Calificación control No. 1 = 25%** **Calificación control No. 2 = 25%**
Paso 1 (Control 1): Casilla "Impacto x Control"	% de impacto inherente * % de la calificación del control correctivo no. 1 = Valor 1	60% * 25% = 15%
Paso 2 (Control 1): Casilla "Impacto después del control"	% de impacto inherente - Valor 1 = % de Impacto residual (resultado 1)	60% - 15% = 45%
Paso 3 (Control 2): Casilla "Impacto x Control"	% de impacto residual (resultado 1) * % calificación del segundo control correctivo no. 2 = Valor 2	45% * 25% = 11,25%
Paso 4 (Control 2): Casilla "Impacto después del control"	% de probabilidad residual (resultado 1) - Valor 2 = % de Probabilidad residual (definitiva)	45% - 11,25% = 33,75%

Fuente: Elaboración propia, con base en la Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, Versión 5, Departamento Administrativo de la Función Pública

La operación anterior, tanto para la probabilidad como para el impacto, se debe realizar igualmente de forma manual y por cada uno de los controles diseñados repitiéndola según su número.

2.22 NIVEL DE RIESGO RESIDUAL

Ejecutadas las operaciones, los valores definitivos deben ubicarse en las tablas de probabilidad e impacto de la hoja de Excel del formato denominada "Tablas" y seleccionar su escala, según corresponda, en la lista desplegable de las casillas "Probabilidad residual" e "Impacto residual".

Posteriormente se debe realizar el cruce de ambas escalas en hoja “Mapa de calor” del formato de Excel, donde se encontrará la tabla con el mismo nombre y seleccionar el nivel de severidad encontrado en la casilla “Nivel de riesgo residual”.

2.23 ESTRATEGIAS PARA COMBATIR EL RIESGO

2.23.1 OPCIÓN DE TRATAMIENTO Y PLAN DE MITIGACIÓN

Los líderes de proceso deben evaluar la opción de tratamiento que se le dará al riesgo, es decir, la estrategia que se implementará para combatirlo. Este análisis se realiza partiendo de la política de administración de riesgos de la Entidad y teniendo en cuenta aspectos tales como la probabilidad e impacto residual, los efectos que el riesgo pueda tener sobre la Entidad, eventos presentados con relación al riesgo, oportunidades de mejora para diseñar controles adicionales, entre otros.
La estrategia por implementar se debe asociar en la parte del formato denominada “Tratamiento del riesgo”. En la casilla “Tratamiento” se deberá escoger de la lista desplegable la decisión que se tomará respecto al nivel de riesgo residual, la cual será elegida por el equipo y aprobada por el líder del proceso. Dicha decisión puede ser: reducir, aceptar o evitar.

a) **Reducir el riesgo:** Se adoptan medidas para reducir la probabilidad residual, el impacto residual, o ambos; por lo general conlleva a la programación de acciones de mitigación apropiadas para combatir el riesgo y con una adecuada segregación de funciones.

   Por regla general, cuando el nivel de riesgo sea alto o extremo, se deberá contemplar esta opción de tratamiento como prioritaria. No obstante, esto debe analizarse, como se mencionó anteriormente, de acuerdo con la especificidad de cada riesgo y la posibilidad de reducir la probabilidad residual o el impacto residual, en caso contrario, se debe analizar otra opción de tratamiento con su debida justificación en la casilla “observaciones”.

   Cuando se elija la opción “Reducir” se debe seleccionar en la casilla “Forma de reducción” alguna de las siguientes opciones:

   i) Mitigar: Se contempla una o más acciones que mitiguen el nivel de riesgo residual, es decir, estas deben estar relacionadas directamente con la mitigación de la probabilidad o el impacto residual y, por ende, con el riesgo mismo. Estas acciones deben ser específicas, claras, realizables y medibles. Además, se deben programar en el plan operativo del área responsable de su implementación, con el fin de realizarle un adecuado seguimiento.

   ii) Transferir: Se contemplan acciones para tercerizar la actividad o trasladar el riesgo a través de seguros o pólizas. Sin embargo, en caso de una posible materialización, si bien el impacto económico recae sobre el tercero, el impacto reputacional lo termina asumiendo la Entidad.

En cualquiera de las dos opciones descritas con anterioridad, las acciones se deben programar en la parte del formato denominada “Plan de mitigación del riesgo” en la cual se debe establecer su responsable, fecha de implementación y fecha de seguimiento.

Ilustración 5 Elementos mínimos para el plan de mitigación

Fuente: Elaboración propia, con base en la Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, Versión 5, Departamento Administrativo de la Función Pública

b) Aceptar el riesgo: Se determina no realizar acciones de mitigación que reduzcan la probabilidad o el impacto residual del riesgo, teniendo en cuenta el nivel de riesgo residual y los efectos de su posible materialización. En caso de que se seleccione en la lista desplegable esta opción de tratamiento, se deberá dejar la debida justificación en la casilla “observaciones”.

c) Evitar el riesgo: Se decide NO realizar la(s) actividad(des) relacionadas con el riesgo, es decir, no iniciar o continuar con la actividad que lo genera. Al igual que en la opción anterior, en caso de que se seleccione “evitar” en la lista desplegable como la opción de tratamiento, se deberá dejar la debida justificación en la casilla “observaciones” y realizar los trámites pertinentes a los que haya lugar.

2.24 HERRAMIENTAS PARA LA GESTIÓN DEL RIESGO

2.24.1 INDICADOR DEL RIESGO

Existen diversas herramientas para generar alertas respecto a la materialización del riesgo o considerar aspectos relacionados con este y que den cuenta de una posible afectación a la Entidad. Para el efecto, se debe diseñar un indicador que esté directamente relacionado con la causa inmediata o causa raíz del riesgo, con sus diferentes aspectos, dentro de los cuales se encuentran: el nombre del indicador, fórmula, descripción, meta, periodicidad y fuente de medición, así como demás que se consideren pertinentes. Esta información se debe relacionar en las casillas con su mismo nombre, en el formato con código SEPG-F-030.

Para lo anterior, es importante considerar el “Manual de indicadores de gestión” (SEPG-M-003). Además, cabe aclarar que el indicador NO necesariamente define la materialización del riesgo, pero sí sugiere que algo no funciona adecuadamente y por lo tanto se debe analizar y abordar.

2.24.2 APROBACIÓN DEL MAPA DE RIESGOS

Como producto de la aplicación de la metodología aquí dispuesta, se contará con los mapas de riesgos por cada uno de los procesos de la Entidad. Para ello, al finalizar el ejercicio el equipo de riesgos deberá proceder con la validación y aprobación del respectivo mapa por parte del líder del proceso, a través de memorando dirigido al Grupo Interno de Trabajo de Planeación, de la Vicepresidencia de Planeación, Riesgos y Entorno, anexando el formato SEPG-F-030 en archivo de Excel, el cual será enviado previamente por el equipo del G.I.T. Planeación a través de correo electrónico para evitar cambios en la formulación del formato.

Posteriormente, el equipo de riesgos del G.I.T. Planeación deberá seleccionar las columnas más importantes del mapa de riesgos, que sean de interés general para la ciudadanía, y enviar el formato definitivo al G.I.T. Tecnologías de la Información y las Telecomunicaciones a través del correo electrónico dirigido a la mesa de servicio, con el fin de que este se publique en la página web institucional para consulta de las partes interesadas y de la ciudadanía en general. Los memorandos de aprobación, así como los respectivos mapas de riesgos, serán cargados de igual manera en el Sitio de SharePoint de la Gestión Integral de Riesgos por parte del G.I.T Planeación.

2.24.3 SOCIALIZACIÓN DEL MAPA DE RIESGOS

El mapa de riesgos de cada uno de los procesos tendrá que ser divulgado por parte de la primera línea de defensa a los colaboradores que hagan parte de este. La respectiva evidencia será enviada al G.I.T. Planeación para su consolidación y cargue en el Sitio de SharePoint de la Gestión Integral de Riesgos.

Además, el G.I.T. Planeación deberá promover la cultura de gestión del riesgo, a través de socializaciones, campañas, capacitaciones, mesas de trabajo y asesorías, con el fin de mejorar continuamente la ejecución de los procesos, el diseño de mecanismos para la gestión del conocimiento, y la apropiación del enfoque basado en riesgos.

2.25 MONITOREO Y REVISIÓN

2.25.1 SEGUIMIENTO Y MONITOREO DEL MAPA DE RIESGOS

Como siguiente aspecto en la administración del riesgo, el seguimiento y monitoreo permiten observar y recolectar información de la situación específica de la gestión de riesgos, en aras de la toma de decisiones frente al aumento de afectaciones generadas por un riesgo.

Bajo ese contexto y de acuerdo con lo establecido en el numeral 4.1 relacionado con el esquema de líneas de defensa, le corresponderá realizar anualmente a la primera línea de defensa el seguimiento de su mapa de riesgos en la parte denominada “Etapa de seguimiento” del formato "Mapa de riesgo por proceso y seguimiento a los riesgos" (SEPG-F-030), así como el reporte de eventos en el formato “Matriz de eventos de riesgo” (SEPG-F-078). Ambos dispuestos por el G.I.T.

Planeación, en el sitio de SharePoint de la Gestión Integral de Riesgos, quien además establecerá y comunicará previamente la fecha para su realización a través de correo electrónico o memorando.

2.26 MATRIZ DE EVENTOS DE RIESGO

Únicamente en el caso de identificar eventos asociados con los riesgos del proceso, se deberá diligenciar la "Matriz de eventos de riesgo" (SEPG-F-078). Un evento se define como 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. La anterior definición indica la necesidad de analizar todos aquellos posibles incidentes relacionados con la actividad generadora del riesgo, y por ende con el riesgo per se, que produzcan o hayan producido alguna alerta de materialización con respecto a la causa inmediata y la causa raíz definidas.

Dentro del formato SEPG-F-078, en primer lugar, se debe asociar la siguiente información relacionada con el evento identificado: fecha en la que se presentó el evento; fuente de información a través de la cual se identificó el evento tales como informes de auditoría, informes de Entes de Control, PQRS, denuncias, oficios, memorandos, correos electrónicos, entre otros; descripción detallada del evento; tipo de evento, que deberá seleccionarse en la lista desplegable; ID del riesgo relacionado con el evento, el cual se encuentra en el mapa de riesgos del proceso (formato SEPG-F-030).

Posteriormente, en la misma matriz, se debe relacionar las características del evento, a saber: causas internas que provocaron el evento; el tipo de impacto generado con ocasión del evento, el cual puede ser económico, reputacional, o económico y reputacional, y debe seleccionarse en la lista desplegable; y la descripción detallada del impacto generado por el evento. En caso dado que el impacto generado por el evento sea de tipo reputacional, es necesario seleccionar dentro de la casilla "impacto reputacional (si aplica)" la escala a la cual corresponde, de lo contrario deberá dejarse la opción "no aplica". De igual manera, si el impacto generado es de tipo económico se debe relacionar la cuantía afectada y, si aplica, la cuantía recuperada; de lo contrario deberá diligenciarse estas casillas con "no aplica".

2.27 INFORME DE SEGUIMIENTO

Posterior al análisis de la matriz de eventos de riesgo, el paso siguiente será diligenciar el informe de seguimiento. Este se encuentra en las columnas finales del mismo formato SEPG-F-030 "Mapa de riesgos por proceso y seguimiento a los riesgos". En este se deberá diligenciar, en primer lugar, la fecha de corte del seguimiento la cual será indicada por el G.I.T. Planeación. Posteriormente, para el seguimiento a los controles, deberá indicarse la frecuencia del riesgo, es decir, únicamente en números las veces en que se llevó a cabo la actividad relacionada con el riesgo en el periodo de seguimiento, la cual debe atender a la frecuencia seleccionada en el numeral 4.15 al momento de determinar la probabilidad inherente.

Paso seguido, se debe indicar, en números, la cantidad de eventos registrados en la "Matriz de eventos de riesgo" (SEPG-F-078). Como resultado de este paso, en la casilla "Desempeño del

control" se calculará automáticamente el porcentaje de efectividad de los controles dispuestos para el riesgo analizado. Esta información se deberá detallar y analizar en la casilla "Análisis de la información reportada".

A continuación, para el seguimiento de los indicadores, deberá diligenciarse el resultado de cada uno de estos, de acuerdo con la información suministrada en el numeral 4.26 (indicador clave del riesgo). Esta información se deberá detallar y analizar en la casilla "Análisis de la información reportada y evidencias" teniendo presente la meta definida en primera instancia.

El seguimiento al plan de mitigación únicamente aplica para los riesgos a los cuales se les programó alguna acción de mitigación en el numeral 4.24 (opción de tratamiento), caso en el cual deberá indicarse el porcentaje de su cumplimiento, de acuerdo con las fechas inicialmente previstas; si la acción está incluida en el plan operativo para facilitar su seguimiento. Esta información se deberá detallar y analizar en la casilla "Análisis de la información reportada y evidencias".

Posteriormente, deberá reportarse la materialización del riesgo cuando a ello hubiera lugar de acuerdo con la información dispuesta y analizada en la "Matriz de eventos de riesgo" (SEPG-F-078), describiendo las causas de su materialización y la acción propuesta para mitigarlo. En caso contrario, en la casilla "Materialización del riesgo" deberá seleccionarse en la lista desplegable la opción "El riesgo no se materializó" y en las demás indicar que "No aplica".
Finalmente, y de forma general con base en el seguimiento realizado, es necesario indicar si se identificaron nuevos riesgos y/u oportunidades de mejora en la gestión, la descripción de los riesgos, la definición de los controles y en los indicadores clave de riesgo.

Todas las evidencias de los eventos identificados, la ejecución de controles, el resultado del indicador clave del riesgo, el cumplimiento de la acción de mitigación cuando aplique, y la materialización del riesgo cuando a ello hubiere lugar, por cada uno de los riesgos dispuestos en el mapa del proceso, deberán cargarse en la carpeta dispuesta por el G.I.T. Planeación en el sitio de SharePoint de la Gestión Integral de Riesgos. La "Matriz de eventos de riesgo" (SEPG-F-078) y el informe de seguimiento realizado en el formato SEPG-F-030 deberán remitirse al G.I.T. Planeación a través de memorando por parte del líder del proceso, con lo cual se entenderá su aprobación.

2.28 ACTUALIZACIÓN DEL MAPA DE RIESGOS

El mapa de riesgos de gestión por cada proceso deberá actualizarse de forma anual o cada vez que se requiera por el líder del proceso, teniendo en cuenta lo dispuesto en el presente instructivo (desde identificación del riesgo, hasta indicador clave del riesgo).

CONTROL DE CAMBIOS		
VERSIÓN	**FECHA**	**DESCRIPCIÓN DEL CAMBIO**
001	08/09/2022	Creación del instructivo para la administración de riesgos conforme a los lineamientos de la guía de riesgos del DAFP V5.

APROBACIÓN			
	Nombre	**Cargo**	**Aprobación**
Elaborado	Juan Sebastián Barreto Montoya	Contratista – GIT Planeación	Documento aprobado mediante Radicado No. 20226010109703
Elaborado	Jessika del Pilar Junca Ortiz	Contratista – GIT Planeación	
Revisado	Héctor Eduardo Vanegas Gámez	Gestor T1 - 12 - GIT Planeación	
Aprobado	Diana Catalina Chirivi González	Coordinadora - GIT Planeación	
Vo.Bo. SGC	Cristian Leandro Muñoz Claros	Contratista – GIT Planeación	