



FUNCIÓN PÚBLICA

Política de Administración de Riesgos en Función Pública

Direccionamiento Estratégico

VERSIÓN 16

AGOSTO 2022

Versión	Fecha de versión	Descripción del cambio
1	2013	Actualización de acuerdo con guía de administración de riesgos y guía administración de riesgos de corrupción versión 2013
2	2013	Cambio de imagen del documento
3	2013	Cambio de imagen del documento
4	2014	Cambio de imagen del documento
5	2014	Actualización de política en Manual de Operaciones DAFP 2014
6	2016	Actualización de acuerdo con la nueva guía de administración de riesgos y guía administración de riesgos de corrupción versión 2016
7	2016	Se incluye dentro de la política los pasos de la metodología asociada a la gestión del riesgo
8	2017	Cambio de imagen del documento por cambio de gobierno
9	2017	Cambio de imagen presentación del documento
10	2018	Actualización de acuerdo con la nueva guía de administración de riesgos versión 2018
11	2018	Cambio de imagen del documento por cambio de gobierno
12	2019	Se incluyen tablas de medición de impacto riesgos de gestión, corrupción y seguridad digital
13	2020-07-29	Se incluye el tema asociado al Plan de Continuidad del Negocio (Responsabilidades, Escenarios pérdida de continuidad, criterios para evaluación impacto al negocio)
14	2020-10-01	Actualización de acuerdo con la nueva guía de administración de riesgos versión 2020
15	2021-09-22	Se revisó y actualizó la política teniendo en cuenta los lineamientos de la nueva metodología de administración de riesgos – DAFP (calificación de probabilidad e impacto, explicación al nivel de aceptación, responsabilidades frente a la gestión y materialización de riesgos). Aprobado en comité de CICCI
16	2022-08-11	Cambio de imagen del documento por cambio de gobierno

Tabla de contenido

Introducción	5
Propósito del documento	5
Glosario	5
Política de administración de riesgos	6
Objetivo de la política de riesgos	7
Alcance	7
Niveles de aceptación del riesgo	7
Responsabilidades	8
Niveles de calificación de impacto	17
Criterios para la evaluación de impacto de pérdida de continuidad	19
Acciones ante los riesgos materializados	19
Estrategia de seguimiento al plan de acción	22
Anexos	23

Gráfica

Gráfica 1. Matriz de calificación de nivel de severidad del riesgo	8
--	---

Tablas

Tabla 1. Responsabilidades de la Líneas de Defensa	8
Tabla 2. Calificación de probabilidad para riesgos proceso y seguridad digital	16
Tabla 3. Calificación de probabilidad para riesgos de corrupción	17
Tabla 4. Calificación de impacto para riesgos de proceso y seguridad digital	17
Tabla 5. Calificación del Impacto para los riesgos de Corrupción	18
Tabla 6. Criterios para la evaluación de impacto de pérdida de continuidad	19
Tabla 7. Acciones de respuesta a riesgos	19
Tabla 8. Seguimiento al mapa de riesgos y controles	21

“Función Pública se compromete a administrar adecuadamente los riesgos de gestión, de corrupción y de seguridad digital, asociados a los objetivos estratégicos, planes, proyectos y procesos institucionales, acatando la metodología propia para su gestión, determinando las acciones de control detectivos y preventivas oportunas para evitar la materialización y la actuación correctiva inmediata ante las eventualidades para mitigar las posibles consecuencias a fin de mantener los niveles de riesgo aceptables”

Introducción

La estructuración del presente documento para el DAFP está basada en la [guía para la administración del riesgo](#) vigente y el diseño de controles en entidades públicas y se establece para asegurar el cumplimiento de la misión institucional y los objetivos estratégicos y de proceso.

La política está compuesta por el objetivo, alcance, niveles de aceptación al riesgo, niveles para calificar el impacto, el tratamiento de riesgos, el seguimiento periódico según nivel de riesgo residual y responsabilidad de gestión para cada línea de defensa.

Propósito del documento

Establecer el marco general de actuación de todos los servidores públicos de la entidad para la adecuada gestión de los riesgos y los potenciales escenarios de pérdida de continuidad de negocio, mediante la identificación de acciones de control, respuestas oportunas y estrategias institucionales ante las situaciones que puedan afectar el cumplimiento de la misionalidad y el logro de objetivos institucionales, disminuyendo las potenciales consecuencias negativas, reduciendo las vulnerabilidades ante las amenazas internas y externas o mejorando las capacidades institucionales de respuesta a eventos identificados o inesperados que afecten al talento humano, la infraestructura tecnológica o los servicios esenciales de los que depende la Entidad.

Glosario

- **Amenazas:** situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Apetito del 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 del riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

- **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.
- **CICCI:** Comité Institucional de Coordinación de Control Interno.
- **Contingencia:** posible evento futuro, condición o eventualidad.
- **Continuidad del negocio:** capacidad de una organización para continuar la entrega de productos o servicios a niveles aceptables después de una crisis.
- **Crisis:** ocurrencia o evento repentino, urgente, generalmente inesperado que requiere acción inmediata.
- **CGDI:** Comité de Gestión y Desempeño Institucional.
- **Mapa de Riesgos:** 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.
- **MIPG:** Modelo Integrado de Planeación y Gestión.
- **OTIC:** Oficina de las Tecnologías de la Información y las Comunicaciones.
- **OAC:** Oficina Asesora de Comunicaciones.
- **OAP:** Oficina Asesora de Planeación.
- **Restablecimiento:** capacidad de la Entidad para lograr una recuperación y mejora, cuando corresponda, de las operaciones, instalaciones o condiciones de vida una vez se supera la crisis.
- **SGI:** Sistema Gestión Institucional, aplicativo propio para la gestión de planeación riesgos e indicadores.
- **TIC:** Tecnologías de la Información y las Comunicaciones.
- **Vulnerabilidad:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

Política de administración de riesgos

La política de administración de riesgos del Departamento Administrativo de la Función Pública – DAFP -, tiene un carácter estratégico y está fundamentada en el [modelo integrado de planeación y gestión, la guía de administración del riesgo](#) y el diseño de controles en entidades públicas, con un enfoque preventivo de evaluación permanente de la gestión y el control, el mejoramiento continuo y con la participación de todos los servidores de la entidad.

Aplica para todos los niveles, áreas y procesos de la Entidad e involucra el contexto, la identificación, valoración, tratamiento, monitoreo, revisión, comunicación, consulta y el análisis de los siguientes riesgos:

- Los riesgos de gestión de proceso que pueda afectar el cumplimiento de la misión y objetivos institucionales.
- Los riesgos de posibles actos de corrupción a través de la prevención de la ocurrencia de eventos en los que se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- Los riesgos de seguridad digital que puedan afectar la confidencialidad, integridad y disponibilidad de la información de los procesos de la entidad.

- Los riesgos de continuidad de negocio que impiden la prestación normal de los servicios institucionales debido a eventos calificados como crisis.

Función Pública determina que el *módulo de riesgos del sistema de gestión institucional – SGI* -, es la herramienta para identificar, valorar, evaluar y administrar los riesgos de gestión, de corrupción y de seguridad digital, para lo cual la oficina asesora de planeación identifica los requerimientos funcionales, revisa periódicamente su adecuado funcionamiento, cargue de información y dispone un manual de uso para el servicio de todos los procesos.

El periodo de revisión e identificación de los riesgos institucionales se debe realizar cada vigencia, atendiendo la metodología vigente, una vez se defina el plan de acción anual, asegurando la articulación de éstos con los compromisos de cada proceso.

Objetivo de la política de riesgos

Alcanzar un nivel aceptable de riesgos residuales en todos los procesos, a través de la gestión de acciones de control, con el fin de asegurar el cumplimiento de la misión institucional, los compromisos de gobierno, los objetivos estratégicos y de procesos vigentes.

Alcance

Aplica a todos los procesos, proyectos, servicios y planes de la entidad, conforme a cada tipo y clasificación de riesgo, bajo la responsabilidad de los líderes de proceso y líneas de defensa.

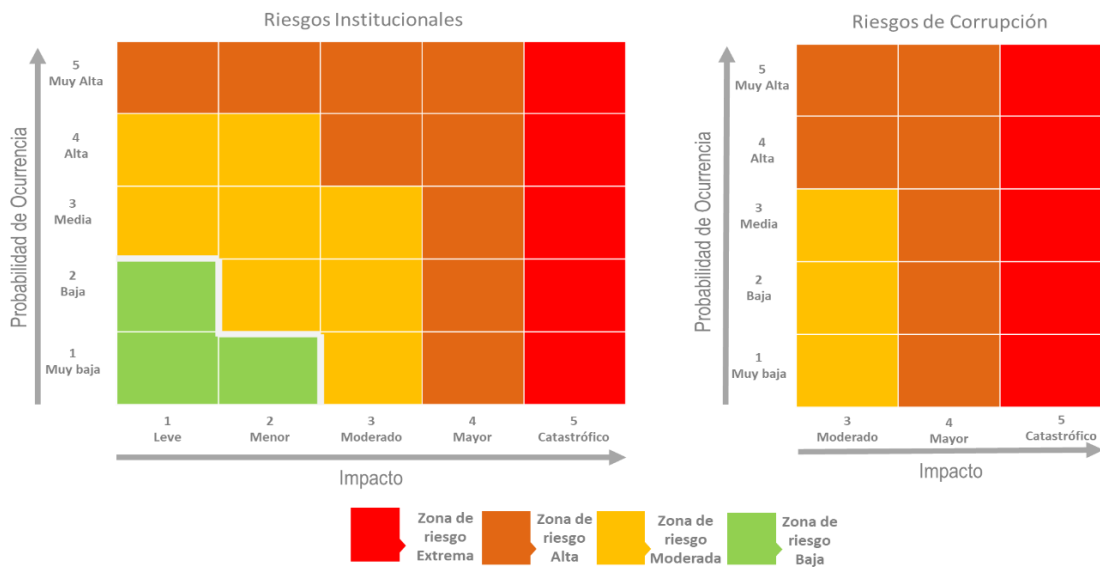
Niveles de aceptación del riesgo

Acorde con los riesgos residuales aprobados por los líderes de procesos y socializados en el comité institucional de coordinación de control interno, se debe definir la periodicidad de seguimiento y estrategia de tratamiento a los riesgos residuales aceptados.

El DAFP determina que para los riesgos residuales de gestión y seguridad digital que se encuentren en zona de riesgo baja, está dispuesto a aceptar el riesgo y no se requiere la documentación de planes de acción, sin embargo, se deben monitorear conforme a la periodicidad establecida.

Para los riesgos de corrupción no hay aceptación del riesgo, siempre deben conducir a formular acciones de fortalecimiento.

Gráfica 1. Matriz de calificación de nivel de severidad del riesgo



Responsabilidades

La responsabilidad está definida mediante las líneas de defensa y en la entidad se acogen según la siguiente tabla:

Tabla 1. Responsabilidades de la Líneas de Defensa

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
Línea Estratégica	Comité Directivo Comité de Gestión y Desempeño Institucional	<ul style="list-style-type: none"> Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información. Definir el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control. Recomendaciones de mejoras a la política de operación para la administración del riesgo.
	Comité institucional de coordinación de control interno	<ul style="list-style-type: none"> Someter a aprobación del Director de Función Pública la política de administración del riesgo previamente estructurada por parte de la oficina asesora de planeación, como segunda línea de defensa en la entidad; hacer seguimiento para su posible actualización y evaluar su eficacia frente a la gestión del riesgo institucional. Se deberá hacer especial énfasis en la prevención y detección de fraude y mala conducta. Revisar la política de administración del riesgo por lo menos una vez al año para su

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
		<p>actualización y validar su eficacia a la gestión del riesgo institucional. se deberá hacer especial énfasis en la prevención y detección de fraude y mala conducta.</p> <ul style="list-style-type: none"> • Aprobar el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control. • Analizar los riesgos, vulnerabilidades, amenazas y escenarios de pérdida de continuidad de negocio institucionales que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la entidad y capacidades para prestar servicios. • Garantizar el cumplimiento de los planes de la entidad.
<p>Primera Línea</p>	<p>Líderes de Procesos</p> <p>Responsable del proyecto</p> <p>Servidores en general</p>	<ul style="list-style-type: none"> • Asegurar que al interior de su grupo de trabajo se reconozca el concepto de “administración de riesgo” la política, metodología y marco de referencia de Función Pública aprobado por la línea estratégica. • Identificar, valorar, evaluar y actualizar cuando se requiera, los riesgos que pueden afectar los objetivos, programas, proyectos y planes asociados a su proceso y realizar seguimiento al mapa de riesgo del proceso a cargo. • Delegar, por parte del líder del proceso, el (los) profesionales que se encargaran de la identificación, monitoreo, reporte y socialización de los riesgos. • Informar a la –OAP- los cambios de responsables de reporte en caso de ausentismo laboral • Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras para su gestión. • Revisar el adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos y su documentación se evidencie en los procedimientos de los procesos. • Revisar de acuerdo con su competencia y alcance la documentación de continuidad del negocio. • Desarrollar ejercicios de autocontrol para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados y los

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
		<p>planes de preparación frente a la pérdida de continuidad de negocio.</p> <ul style="list-style-type: none"> • Reportar en el SGI los avances y evidencias de la gestión de los riesgos dentro de los plazos establecidos. • Realizar la medición y análisis a la gestión efectiva de los riesgos. • Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. • Informar a la oficina de planeación (segunda línea) sobre los riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo y aplicar las acciones correctivas o de mejora necesarias. • Revisar las acciones y planes de mejoramiento establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces. • En caso de la materialización de un riesgo no identificado, este debe ser gestionado en el aplicativo SGI y ser incluido en el mapa de riesgo institucional. <p>El líder del proceso debe:</p> <ul style="list-style-type: none"> • Verificar las acciones preventivas y registrar el avance junto con la evidencia en el SGI de acuerdo con la periodicidad definida. • Analizar los resultados del seguimiento y establecer acciones inmediatas ante cualquier desviación. • Evaluar con el equipo de trabajo la responsabilidad y resultados de la gestión del riesgo, así como las desviaciones según el nivel de aceptación del riesgo al interior de su dependencia y las acciones a seguir. • Comunicar al equipo de trabajo los resultados de la gestión del riesgo. • Asegurar que se documenten las acciones de corrección o prevención en el plan de mejoramiento. • Revisar y actualizar el mapa de riesgos con el acompañamiento de la OAP. <p>Los servidores en general deben:</p>

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
		<ul style="list-style-type: none"> • Participar en el diseño de los controles que tienen a cargo. • Ejecutar el control de la forma como está diseñado. • Proponer mejoras a los controles existentes. • El responsable del proyecto debe: • Realizar la identificación de los riesgos del proyecto. • Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. • Orientar a la primera línea de defensa para que identifique, valore, evalúe y gestione los riesgos y escenarios de pérdida de continuidad de negocio en los temas de su competencia. • Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad.
<p>Segunda Línea</p>	<p>Oficina Asesora de Planeación</p>	<ul style="list-style-type: none"> • Asesorar a la línea estratégica en el análisis del contexto interno y externo, la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo residual. • Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlos para su aprobación del CICC. • Capacitar al grupo de trabajo de cada dependencia en la herramienta SGI para la gestión del riesgo con la asesoría de la Dirección de Gestión y Desempeño Institucional como líder de la política de control interno. • Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de estos. • Verificar que las acciones de control se diseñen conforme a los requerimientos de la metodología. • Revisar el perfil de riesgo inherente y residual por cada proceso y pronunciarse sobre

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
		<p>cualquier riesgo que este por fuera del perfil de riesgo residual aceptado por la entidad.</p> <ul style="list-style-type: none"> • Hacer seguimiento al plan de acción establecido para la mitigación de los riesgos de los procesos registrados en el SGI. • Revisar que el cargue de información en el SGI esté acorde con lo aprobado por el líder del proceso. • Consolidar el mapa de riesgos institucional, riesgos de mayor criticidad frente al logro de los objetivos y presentarlo para análisis y seguimiento ante el CGDI. • Presentar al Comité Institucional de Coordinación de Control Interno-CICCI el resultado de la medición del nivel de eficacia de los controles para el tratamiento de los riesgos identificados en los procesos o proyectos. • Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo. • Coordinar con los líderes de proceso el responsable de reporte de seguimiento a los riesgos, controles y planes de acción en el aplicativo SGI. • Informar a la primera línea de defensa la importancia de socializar los riesgos aprobados al interior de su proceso. • Comunicar a los líderes de proceso a través de los enlaces los resultados de la gestión del riesgo. • Consolidar el mapa de riesgos institucional a partir de la información reportada por cada uno de los procesos (mapa de riesgo del proceso). • Socializar y publicar el mapa de riesgos institucional. • Participar en los ejercicios de autoevaluación de la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados. • Revisar las acciones y planes de mejoramiento establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelvan a materializar y lograr el cumplimiento a los objetivos. • Informar a la primera línea de defensa correspondiente (líder del proceso) la materialización de un riesgo no identificado, el

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
		<p>cual debe ser gestionado en el aplicativo SGI y ser incluido en el mapa de riesgo institucional.</p> <ul style="list-style-type: none"> • Supervisar en coordinación con los demás responsables de esta segunda línea de defensa, que la primera línea identifique, analice, valore, evalúe y realice el tratamiento de los riesgos, que se adopten los controles para la mitigación de los riesgos identificados y se apliquen las acciones pertinentes para reducir la probabilidad o impacto de los riesgos. • Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos. • Evaluar que la gestión de los riesgos este acorde con la presente política de la entidad y que sean gestionados por la primera línea de defensa. • Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlos en el CICCI.
<p>Segunda Línea</p>	<p>Secretaria General</p> <p>OAP</p> <p>Jefe de la OTIC</p> <p>Gestión administrativa</p> <p>Gestión del Talento Humano</p>	<ul style="list-style-type: none"> • Orientar a la primera línea de defensa para definir la estrategia de continuidad del negocio identificando los escenarios. • Actualizar la documentación que soporta la estrategia de continuidad del negocio. • Identificar, valorar, evaluar y gestionar los riesgos de pérdida de continuidad del negocio. • Liderar mesas de trabajo para la determinación del análisis de impacto del negocio, documentación de los escenarios de riesgos y plan de continuidad de negocio institucional. • Actualizar, según se requiera, los escenarios de riesgos de continuidad y la documentación asociada al plan de continuidad de negocio bajo su responsabilidad. • Orientar y hacer seguimiento a las pruebas del plan de continuidad de negocio.
	<p>Secretaria General</p>	<ul style="list-style-type: none"> • Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo.

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
	Coordinadores de Gestión Contractual, Administrativa, Financiera, Servicio al Ciudadano, Gestión Documental, Talento Humano y Defensa Jurídica	<ul style="list-style-type: none"> • Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. • Sugerir las acciones de mejora a que haya lugar posterior al análisis, valoración, evaluación o tratamiento del riesgo. • Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad. • Participar en las pruebas del plan de continuidad del negocio y en la implementación. • El Coordinador del Grupo de Defensa Jurídica tendrá el compromiso de identificar, analizar, valorar y evaluar los riesgos y controles asociados a su gestión con enfoque en la prevención del daño antijurídico. • Comunicar al equipo de trabajo a su cargo la responsabilidad y resultados de la gestión del riesgo. • Participar en los ejercicios de autoevaluación de la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados.
	OAC	<ul style="list-style-type: none"> • Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo.
	Jefe de la OTIC, y OAP	<ul style="list-style-type: none"> • Acompañar a los líderes de procesos en la identificación, análisis, valoración, evaluación del riesgo, la definición de controles y las estrategias de continuidad de negocio asociadas a los escenarios de continuidad de negocio bajo su responsabilidad y los temas a su cargo. • Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. • Orientar a la primera línea de defensa para que identifique, valore, evalúe y gestione los riesgos y escenarios de pérdida de continuidad de negocio en los temas de su competencia. • Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
	Oficina de Gestión de Proyectos - PMO	<p>de gestión del riesgo asociado a su responsabilidad.</p> <ul style="list-style-type: none"> Participar en las pruebas del plan de continuidad del negocio y en la implementación. Identificar y documentar un manual de gerencia de proyectos para el DAFP que contenga la guía para la gerencia de los proyectos institucionales, conjunto de buenas prácticas y estándares para la dirección de los proyectos. Identificar, documentar y formalizar políticas, procedimientos, instructivos y formatos para el adecuado funcionamiento de las labores de dirección de proyectos. Generar espacios de transferencia y gestión de conocimiento que faciliten el desarrollo de competencias y habilidades en el personal encargado de la gestión de proyectos en la Entidad. Generar espacios de trabajo para que los directores de proyecto compartan recursos de conocimiento para mejorar las posibilidades de éxito de los proyectos. Apoyar a las dependencias en las actividades de formulación, planificación, seguimiento y control a la ejecución y cierre de los proyectos bajo su responsabilidad, así como la identificación, diseño de controles y gestión de los riesgos de los proyectos y sus seguimientos. Monitorizar el avance global de los proyectos de la entidad para identificar amenazas y oportunidades que puedan afectar el cumplimiento de los objetivos de proyecto. Mantener información actualizada sobre el avance, logros, dificultades y necesidades de los diferentes proyectos y presentar informes consolidados para el comité directivo institucional.
Tercera Línea	Oficina de Control Interno	<ul style="list-style-type: none"> Revisar los cambios en el "Direccionamiento estratégico" o en el entorno y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables. Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
		<p>énfasis en el diseño e idoneidad de los controles establecidos en los procesos.</p> <ul style="list-style-type: none"> • Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa. • Asesorar a la primera línea de defensa de forma coordinada con la Oficina de Planeación, en la identificación de los riesgos y diseño de controles. • Llevar a cabo el seguimiento a los riesgos y estrategia de continuidad negocio consolidados en los mapas de riesgos y plan de continuidad de conformidad con el Plan Anual de Auditoría y reportar los resultados al CICCI. • Realizar seguimiento a la implementación de mejoras sobre los lineamientos de continuidad del negocio. • Realizar seguimiento a la implementación de la estrategia de continuidad del negocio y a las pruebas efectuadas. • Recomendar mejoras a la política de operación para la administración del riesgo.

Adicionalmente, la [matriz de responsabilidad y autoridad](#) de Función Pública define los cargos que pueden identificar, valorar, evaluar y definir controles y reportar los riesgos institucionales en el módulo de riesgos del SGI, por lo cual dicha matriz hace parte de este documento.

<https://www.funcionpublica.gov.co/web/intranet/manuales-proceso-direccionamiento-estrategico>

Nivel de calificación de probabilidad para riesgos de proceso y seguridad digital

Tabla 2. Calificación de probabilidad para riesgos proceso y seguridad digital

Nivel	Probabilidad	Descripción
100%	Muy Alta	La actividad se realiza más de 1500 veces al año.
80%	Alta	La actividad se realiza entre 366 a 1500 veces al año.
60%	Media	La actividad se realiza entre 13 a 365 veces al año.
40%	Baja	La actividad se realiza entre 5 a 12 veces al año.
20%	Muy Baja	La actividad se realiza máximo 4 veces al año.

Fuente: Oficina Asesora de Planeación

Nivel de calificación de probabilidad para riesgos de corrupción

Tabla 3. Calificación de probabilidad para riesgos de corrupción

Nivel		Probabilidad	Descripción
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 públicas, v4 - Dirección de Gestión y Desempeño Institucional, octubre 2018

Niveles de calificación de impacto

La calificación del impacto para los riesgos de gestión y de seguridad de la información se tendrá en cuenta la siguiente escala, de acuerdo con la realidad de Función Pública.

Tabla 4. Calificación de impacto para riesgos de proceso y seguridad digital

Nivel	Impacto	Descripción Económica o Presupuestal	Descripción Reputacional
100%	Catastrófico	Pérdida económica superior a 1500 SMLV	Deterioro de imagen con efecto publicitario sostenido a nivel internacional.
80%	Mayor	Pérdida económica de 319 hasta 1500 SMLV	Deterioro de imagen con efecto publicitario sostenido a nivel Nacional o Territorial.
60%	Moderado	Pérdida económica de 21 hasta 318 SMLV	Deterioro de imagen con efecto publicitario sostenido a nivel Local o Sectores Administrativos.
40%	Menor	Pérdida económica de 11 hasta 20 SMLV	De conocimiento general de la entidad a nivel interno, Dirección General, Comités y Proveedores.
20%	Leve	Pérdida económica hasta 10 SMLV	Solo de conocimiento de algunos funcionarios.

Fuente: Oficina Asesora de Planeación

La calificación del impacto para los riesgos de corrupción se realiza aplicando la siguiente tabla de valoración establecida por Secretaría de Transparencia de la Presidencia de la República. Cada riesgo identificado es valorado de acuerdo con las preguntas, la tabla y la calificación obtenida se compara con la tabla de medición de impacto de riesgo de corrupción para obtener el nivel de impacto del riesgo.

Tabla 5. Calificación del Impacto para los riesgos de Corrupción

No.	Pregunta: Si el riesgo de corrupción se materializa podría		Respuesta	
	Si	No	Si	No
1	¿Afectar al grupo de funcionarios del proceso?			
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?			
3	¿Afectar el cumplimiento de misión de la entidad?			
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?			
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?			
6	¿Generar pérdida de recursos económicos?			
7	¿Afectar la generación de los productos o la prestación de servicios?			
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?			
9	¿Generar pérdida de información de la entidad?			
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?			
11	¿Dar lugar a procesos sancionatorios?			
12	¿Dar lugar a procesos disciplinarios?			
13	¿Dar lugar a procesos fiscales?			
14	¿Dar lugar a procesos penales?			
15	¿Generar pérdida de credibilidad del sector?			
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?			
17	¿Afectar la imagen regional?			
18	¿Afectar la imagen nacional?			
19	¿Generar daño ambiental?			
Nivel	Descriptor	Descripción	Respuestas afirmativas	
1	Moderado	Genera medianas consecuencias sobre la entidad.	1 a 5	
2	Mayor	Genera altas consecuencias sobre la entidad.	6 a 11	
3	Catastrófico	Genera consecuencias desastrosas para la entidad.	12 a 19	

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas v5.

Criterios para la evaluación de impacto de pérdida de continuidad

La determinación de las prioridades de recuperación de servicios en caso de materialización de escenarios de pérdida de continuidad de negocio se realiza mediante la valoración del impacto percibido por los líderes de los procesos. Mediante mesa de trabajo los participantes califican los impactos en cada variable y definen el orden de recuperación de los servicios asignando la secuencia de reactivación de los mismos primero a los servicios con mayor impacto y de manera secuencia a los servicios con menor impacto percibido.

Tabla 6. Criterios para la evaluación de impacto de pérdida de continuidad

Criterio	Descripción
Financiero	Nivel de pérdidas económicas
Reputacional	Nivel de pérdida de la confianza de los grupos de valor en la entidad
Legal / Regulatorio	Nivel de incumplimiento de normas y regulaciones a las que está sometida la entidad
Contractual	Impactos asociados al incumplimiento de cláusulas en obligaciones contractuales
Misional	Nivel de incumplimiento o impacto percibido por imposibilidad de cumplir los objetivos y obligaciones misionales.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas v5

De igual manera, en el instructivo de análisis de impacto al negocio se amplía esta información:

<https://www.funcionpublica.gov.co/web/intranet/manuales-proceso-direccionamiento-estrategico>

Acciones ante los riesgos materializados

Cuando se materializan riesgos identificados en la matriz de riesgos institucionales se deben aplicar las acciones descritas en la tabla “acciones de respuesta a riesgos”.

Tabla 7. Acciones de respuesta a riesgos

Tipo de Riesgo	Responsable	Acción
Riesgo de Corrupción	Líder de Proceso	<ul style="list-style-type: none"> Informar a la Oficina Asesora de Planeación como segunda línea de defensa en el tema de riesgos sobre el posible hecho encontrado y marcar en el SGI la alerta de posible materialización.

Tipo de Riesgo	Responsable	Acción
		<ul style="list-style-type: none"> • Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), determinar la aplicabilidad del proceso disciplinario. • Identificar las acciones correctivas necesarias y documentarlas en el <i>plan de mejoramiento</i>. • Efectuar el análisis de causas y determinar acciones preventivas y de mejora. • Revisar los controles existentes y actualizar el mapa de riesgos.
	Oficina de Control Interno	<ul style="list-style-type: none"> • Informar al líder del proceso y a la segunda línea de defensa, quienes analizarán la situación y definirán las acciones a que haya lugar. • Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), determinar la aplicabilidad del proceso disciplinario. • Informar a discreción los posibles actos de corrupción al ente de control.
Riesgos de Gestión y Seguridad digital	Líder de Proceso	<ul style="list-style-type: none"> • Informar a la Oficina Asesora de Planeación como segunda línea de defensa, el evento o materialización de un riesgo. • Proceder de manera inmediata a aplicar el <i>plan de contingencia o de tratamiento de incidentes de seguridad de la información</i> que permita la continuidad del servicio o el restablecimiento de este (si es el caso) y documentar en el plan de mejoramiento. • Realizar los correctivos necesarios frente al cliente e iniciar el análisis de causas y determinar acciones correctivas, preventivas, y de mejora, así como la revisión de los controles existente, documentar en el plan de mejoramiento institucional y actualizar el mapa de riesgos. • Dar cumplimiento al procedimiento plan de mejoramiento.

Tipo de Riesgo	Responsable	Acción
Riesgos de Gestión y Seguridad digital	Oficina de Control Interno	<ul style="list-style-type: none"> • Informar al líder del proceso sobre el hecho encontrado • Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos. • Verificar que se tomen las acciones y se actualice el mapa de riesgos correspondiente. • Si la materialización de los riesgos es el resultado de una auditoría realizada por la Oficina de Control Interno, esta verificará el cumplimiento del plan de mejoramiento y realizará el seguimiento de acuerdo con el procedimiento.
Riesgos de continuidad de negocio	Comité de crisis	<ul style="list-style-type: none"> • Activar el plan de continuidad de negocio

Tabla 8. Seguimiento al mapa de riesgos y controles

Tipo de Riesgo	Zona de Riesgo Residual	Estrategia de Tratamiento - Controles
Riesgos de Gestión, y Seguridad digital	Baja	Se realiza seguimiento a los controles con periodicidad SEMESTRAL y se registran sus avances en el módulo de riesgos- SGI.
	Moderada	Se realiza seguimiento a los controles con periodicidad TRIMESTRAL y se registran sus avances en el módulo de riesgos- SGI.
	Alta	Se realiza seguimiento a los controles con periodicidad BIMESTRAL y se registran sus avances en el módulo de riesgos- SGI
	Extrema	Se realiza seguimiento a los controles con periodicidad MENSUAL y se registra en el módulo de riesgos – SGI.
Riesgos de Corrupción	Todos los riesgos de corrupción, independiente de la zona de riesgo en la que se encuentran debe tener un seguimiento MENSUAL y se registra en el módulo de riesgos – SGI.	

Estrategia de seguimiento al plan de acción

Tipo de Riesgo	Zona de Riesgo Residual o severidad	Estrategia de Tratamiento – Plan de Acción
Riesgos de Gestión, y Seguridad digital	Baja	No se debe realizar plan de acción por que está dentro del nivel de aceptación del riesgo por Función Pública.
	Moderada Alta Extrema	<p>El líder del proceso define acciones que permita mitigar el riesgo residual. Asimismo, determina la fecha de inicio y finalización de estas y establece los seguimientos que va a realizar durante la ejecución de la acción correspondiente a su avance, el cual se debe reportar junto con el seguimiento al mapa de riesgo y controles.</p> <p>Después de haber implementado la acción debe realizar un seguimiento con el fin de evaluar la efectividad del plan de acción.</p>

Anexos

Para una mayor comprensión de la política de operación para la administración del riesgo, se define que los anexos son parte fundamental de este documento técnico, por tanto, se recomienda su consulta y conocimiento por parte de todos los servidores públicos de la Entidad.

- Manual operativo MIPG
https://www.funcionpublica.gov.co/documents/34645357/34702994/Modelo_integrado_planeacion_gestion.pdf/7f3d55ea-4ad6-3bdc-3f05-a23d287ca69b?t=1615223466439
- Manual Metodología de riesgos
https://www.funcionpublica.gov.co/documents/34645357/34702994/Manual_metodologia_riesgos.pdf.pptx/8b3d4a02-7c0d-41a7-b609-3752cb063bc8?t=1536162961916
- Guía para la Administración del riesgo de FP
https://www.funcionpublica.gov.co/documents/34645357/34702994/Guia_externa_administracion_riesgo_direccionamiento_estrategico.pdf/0330fa64-0a6a-4772-887f-27aae325afa5?t=1614199851989
- Matriz de autoridad y responsabilidad
<https://www.funcionpublica.gov.co/web/intranet/manuales-proceso-direccionamiento-estrategico>
- Manual del usuario – módulo de riesgos SGI
https://www.funcionpublica.gov.co/documents/34645357/34702994/Manual_usuario_sgi_modulo_riegos_direccionamiento.pdf/e9a51e27-30af-4045-b0b2-53713707d456?t=1536164158725
- Plan de Continuidad
<https://www.funcionpublica.gov.co/plan-de-continuidad>
- Procedimiento Administración del plan de mejoramiento institucional
<https://www.funcionpublica.gov.co/web/intranet/procedimiento-administracion-plan-mejoramiento-institucional>



Política de Administración de Riesgos

VERSIÓN 16

Direccionamiento Estratégico

AGOSTO de 2022

Departamento Administrativo de la Función Pública

Carrera 6 n.º 12-62, Bogotá, D.C., Colombia

Conmutador: 601 7395656 – 601 7395657

Web: www.funcionpublica.gov.co

eva@funcionpublica.gov.co

Bogotá, D.C., Colombia.