Contenido

1. INTRODUCCIÓN

El presente documento establece los lineamientos para la identificación, análisis, valoración, tratamiento, monitoreo y seguimiento de los riesgos que pudieran afectar la misión, el cumplimiento de los objetivos estratégicos y la gestión de los procesos, proyectos y planes institucionales. Estos lineamientos, deben ser acatados por todos los servidores públicos de la entidad en el desarrollo de sus funciones y compromisos.

Es así como la UNGRD define sus políticas de administración de riesgos tomando como referente los parámetros del Modelo Integrado de Planeación y Gestión- MIPG, la responsabilidad de las líneas de defensa definidas en el Modelo Estándar de Control Interno – MECI, los requerimientos de la Guía para la Administración del riesgo de Departamento Administrativo de la Función Pública y el Modelo de Seguridad y Privacidad de la información de la estrategia de Gobierno Digital, directrices que se desarrollan en el presente documento.

2. DEFINICIONES

- **Activo:** en el contexto de seguridad digital son elementos tales como aplicaciones, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la entidad para funcionar en el entorno digital.
- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Causa inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo**.**
- **Causa raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
- **Confidencialidad.** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados
- **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
- **Control:** medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas y otras acciones).
- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.
- **Factores de riesgo:** son las fuentes generadoras de riesgos
- **Fraude:** cualquier acto ilegal caracterizado por engaño, ocultación o violación de confianza. Estos actos no requieren la aplicación de amenaza de violencia o de fuerza física. Los fraudes son perpetrados por individuos y por organizaciones para obtener dinero, bienes o servicios, para evitar pagos o pérdidas de servicios, o para asegurarse ventajas personales o de negocio

- **Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **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.
- **Oportunidad**: evento con impacto positivo sobre las actividades, servicios u objetivos, pudiendo mejorar u optimizar el desarrollo de las funciones de la entidad y la capacidad de lograr los resultados previstos.
- **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.
- **Riesgo**: efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. *Nota*: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
- **Riesgo de corrupción**: posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Riesgo fiscal:** Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial
- **Riesgo de gestión**: posibilidad de que suceda un evento con impacto sobre las actividades, servicios u objetivos, pudiendo entorpecer el desarrollo de las funciones de la entidad y el logro de los resultados previstos.
- **Riesgo de seguridad de la información:** posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **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
- **Riesgo residual:** El resultado de aplicar la efectividad de los controles al riesgo inherente.
- **SCI:** Sistema de Control Interno
- **SGSI:** Sistema de gestión de seguridad de la información.

3. OBJETIVO

Definir los lineamientos para la gestión de riesgos en la Unidad Nacional para la Gestión del Riesgo de Desastres UNGRD, como parte integral de la gestión administrativa para el cumplimiento de su misión, objetivos estratégicos y fortalecimiento del control interno.

4. ALCANCE

La política de administración de riesgos es aplicable a todos los planes, programas, proyectos y procesos de la entidad y a todas las acciones ejecutadas por los servidores durante el ejercicio de sus funciones.

5. DESARROLLO

5.1 RESPONSABILIDADES

Línea de defensa	Responsables
Línea de Defensa Estratégica	Alta Dirección y Comité Institucional de Coordinación de Control Interno.[1]
Primera Línea de Defensa	Gerentes Públicos, Líderes de Proceso, Líderes de Proyectos/Programas y de sus equipos de trabajo y supervisores de contratos. Enlaces estratégicos y en general, colaboradores y/o servidores públicos en todos los niveles de la organización.[2]
Segunda Línea de Defensa	Oficina Asesora de Planeación e Información. Contratación, Financiera y Tecnologías de la Información.
Tercera Línea de Defensa	Oficina de Control Interno

Serán responsabilidades de las líneas de defensa las descritas a continuación, así como todas aquellas que el Comité Institucional de Coordinación de Control Interno en cumplimiento de sus funciones, defina como acciones necesarias para fortalecer y desarrollar una adecuada administración del riesgo en la entidad.

ROL	RESPONSABILIDAD
Línea de Defensa Estratégica: Alta Dirección y Comité Institucional de Coordinación de Control Interno	1. Establecer objetivos institucionales alineados con el propósito fundamental, metas y estrategias de la entidad. 2. Establecer las Políticas de Administración de Riesgos 3. Asumir la responsabilidad primaria del Sistema de Control Interno, de la identificación y evaluación de los cambios que podrían tener un impacto significativo en el mismo. 4. Evaluar y dar línea sobre la administración de los riesgos en la entidad.

[1] Modelo Integrado de Planeación y Gestión – Manual Operativo. Séptima Dimensión: Control Interno. Lineamientos generales para la implementación. Línea estratégica de defensa. Pág. 118. Marzo 2023 V5.

[2] En la UNGRD son Gerentes Públicos: el Secretario General, el Subdirector General y los Subdirectores Misionales. Y son Líderes de Proceso: los Jefes de Oficina y Coordinadores de Grupo.

ROL	RESPONSABILIDAD
	5. Asignar los recursos suficientes para el desarrollo de la gestión de riesgos (capital, tiempo, personal, procesos, sistemas y tecnologías), con el fin de apoyar a los responsables en la implementación de controles y seguimiento de los riesgos. 6. Definir líneas de reporte (canales de comunicación) en temas clave para la toma de decisiones, atendiendo el Esquema de Líneas de Defensa. 7. Evaluar la política de gestión estratégica del Talento Humano (forma de provisión de los cargos, capacitación, código de Integridad, bienestar).
Primera Línea de Defensa: Gerentes Públicos, Líderes de Proceso, Líderes de Proyectos/Programas y de sus equipos de trabajo y supervisores de contratos. Enlaces estratégicos y en general, colaboradores y/o servidores públicos en todos los niveles de la organización.	Los responsables de la Primera Línea de Defensa deberán: 1. Identificar y valorar los riesgos que pueden afectar el logro de los objetivos institucionales y establecer y actualizar los mapas de riesgos y oportunidades del proceso/proyecto a cargo. 2. Realizar la identificación y valoración de activos de seguridad de la información en cada proceso donde aplique la gestión del riesgo de seguridad digital. 3. Definir, diseñar y gestionar los controles a los riesgos de gestión. 4. Identificar y controlar los riesgos relacionados con posibles actos de corrupción, fraude y riesgo fiscal en el ejercicio de sus funciones y el cumplimiento de sus objetivos institucionales. 5. Implementar mecanismos para identificar, disuadir y detectar fraudes; y revisar la exposición de la entidad al fraude con el jefe de la Oficina de Control Interno de la entidad. 6. Los supervisores de contratos deben realizar seguimiento a los riesgos de estos, e informar las alertas respectivas. 7. Tener el conocimiento de las políticas, manuales, protocolos y otras herramientas que permitan tomar acciones para el autocontrol en sus puestos de trabajo. 8. Hacer el seguimiento a los indicadores de gestión de los procesos e institucionales, según corresponda. 9. Formular planes de mejoramiento, su aplicación y seguimiento para resolver los hallazgos presentados. 10. Coordinar con sus equipos de trabajo las acciones establecidas en la planeación institucional a fin de contar con la información clave para el seguimiento o autoevaluación aplicada por parte de la 2ª línea de defensa. 11. Informar al Comité Institucional de Coordinación de Control Interno la materialización de riesgo que se identifiquen en los procesos de seguimiento que se adelanten.

ROL	RESPONSABILIDAD
Segunda Línea de defensa: Oficina de Asesora de Planeación e Información, Grupo de Gestión Contractual, Grupo de Apoyo Financiero y Contable y Grupo de Tecnologías de la Información.	Con el liderazgo de la Oficina Asesora de Planeación e Información los responsables de la segunda línea de defensa deberán: 1. Informar sobre la incidencia de los riesgos en el logro de objetivos y evaluar si la valoración del riesgo es la apropiada 2. Monitorear la administración de riesgos identificados por la primera línea de defensa. 3. Consolidar los monitoreos de los mapas de riesgo. 4. Aportar información que permita mejorar el Sistema de Control Interno. 5. Retroalimentar a la alta dirección sobre el monitoreo y la gestión del riesgo. 8. Asesorar y acompañar a la primera línea de defensa en la administración de riesgos de gestión, corrupción, seguridad digital, seguridad de la información, fraude y riesgo fiscal y en la recomendación de controles para mitigar los riesgos. 9. Asegurar que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente, supervisan la implementación de prácticas de gestión de riesgo eficaces. 10. Consolidar y analizar información sobre temas claves para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos. 11. Trabajar coordinadamente con la Oficinas de Control Interno en el fortalecimiento del Sistema de Control Interno. 12. Asesorar a la 1ª línea de defensa en temas clave para el Sistema de Control Interno: i) riesgos y controles; ii) planes de mejoramiento; iii) indicadores de gestión; iv) procesos y procedimientos. 13. Informar al Comité Institucional de Coordinación de Control Interno la materialización de riesgo que se identifiquen en los procesos de monitoreo y seguimiento que se adelanten.
Tercera línea de defensa: Oficina de Control Interno	Los responsables de la Tercera Línea de Defensa deberán: 1. Asesorar en metodologías para la identificación y administración de los riesgos, en coordinación con la segunda línea de defensa 2. Identificar y evaluar cambios que podrían tener un impacto significativo en el Sistema de Control Interno durante las evaluaciones periódicas de riesgos y en el curso del trabajo de auditoría interna. 3. Comunicar al Comité de Coordinación de Control Interno posibles cambios e impactos en la evaluación del riesgo, detectados en las auditorías.

ROL	RESPONSABILIDAD
	4. Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos claves de la entidad. 5. Alertar sobre la probabilidad de riesgo de fraude, riesgo fiscal y riesgo de corrupción en las áreas auditadas. 6. Asesorar y acompañar a la primera línea de defensa en la administración de riesgos de gestión, corrupción, seguridad digital, fraude y riesgo fiscal y en la recomendación de controles para mitigar los riesgos. 7. Monitorear la exposición de la entidad al riesgo y realizar recomendaciones con alcance preventivo. 8. Asesorar proactiva y estratégicamente a la Alta Dirección y los líderes de proceso, en materia de control interno y sobre las responsabilidades en materia de riesgos. 9. Formar a la alta dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos. 10. Informar los hallazgos y proporcionar recomendaciones de forma independiente.

5.2 FUNCIONALIDAD DE LA ADMINISTRACIÓN DEL RIESGO

La identificación y valoración de riesgos se integra en el desarrollo de la estrategia, la formulación de los objetivos de la entidad y la implementación de esos objetivos a través de la toma de decisiones cotidiana en cada uno de los procesos (Guía riesgos).

La administración del riesgo es un proceso dinámico, interactivo, continuo, lógico y sistemático desarrollado en cada área, en coordinación con la Oficina Asesora de Planeación e Información y la asesoría de la Oficina de Control Interno, plasmado en la herramienta denominada *"Mapa de Riesgos y Oportunidades",* para los riesgos de gestión, corrupción, fraude, fiscal y las oportunidades. También serán parte, los riesgos asociados a la integridad pública y riesgos fiscales.

Por otra parte, en la herramienta *"Matriz de Riesgos SGSI"* se realiza la identificación, control y seguimiento de los riesgos de seguridad digital, que lidera la Coordinación de Tecnologías de la Información.

Los riesgos y las oportunidades identificadas, se revisan o se actualizan anualmente y se publican en la página web de la entidad para su consulta.

5.3 HERRAMIENTAS PARA ADMINISTRACIÓN DE RIESGOS

Para llevar a cabo la administración de los riesgos, se utilizan las herramientas descritas a continuación:

5.3.1 Procedimiento de administración de riesgos y oportunidades UNGRD

El documento PR-1300-SIPG-11 *Administración de riesgos y oportunidades* describe las actividades en relación con las fases descritas en el numeral 5.3, que inicia con el contexto organizacional y termina con la consolidación y cargue del mapa de riesgos y oportunidades en la herramienta tecnológica.

5.3.2 Mapa de Riesgos y Oportunidades

Contiene los siguientes elementos:

- Contexto estratégico
- Identificación del riesgo u oportunidad
- Análisis del Riesgo
- Valoración de Controles
- Valoración del Riesgo
- Seguimiento y Monitoreo

Esta herramienta contiene las siguientes orientaciones para facilitar su diligenciamiento: tablas de escala de los niveles de probabilidad, impacto en riesgos y oportunidades, listado de preguntas para determinar el impacto de los riesgos de corrupción y mapas de calor.

5.3.3 Matriz de Riesgos SGSI

Contiene los siguientes componentes:

- Contexto y definiciones
- Inventario de activos
- Identificación del riesgo
- Valoración del riesgo inherente
- Valoración de controles
- Valoración del riesgo residual
- Plan de tratamiento

En cuanto a la valoración de los riesgos se pueden presentar los siguientes niveles o zonas de Riesgo: “Extrema”, “Alta”, “Moderada” y “Baja” determinadas por la probabilidad e impacto asignados a cada Riesgo.

5.4 METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO

La UNGRD, teniendo en cuenta las orientaciones metodológicas establecidas en las guías o herramientas dispuestas para tal fin por el Departamento Administrativo de la Función Pública – DAFP, la Secretaría de Transparencia de la Presidencia de la República y el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, acoge los lineamientos que

considera pertinentes acorde a la dinámica y necesidades de la entidad, estableciendo como metodología para la administración del riesgo el desarrollo de seis fases:

FASE	ASPECTOS POR CONSIDERAR
Fase 1 – Establecimiento del contexto	1.1. Objetivos estratégicos 1.2. Responsabilidades de las líneas de defensa frente al manejo de riesgos 1.3. Mecanismos de comunicación para dar a conocer la política de riesgos a todos los niveles de la entidad. 1.4. Contexto organizacional: debe tenerse en cuenta lo desarrollado en los procesos de planeación (ej. Plan estratégico, plan de acción), que se diligencia en el formato identificación contexto interno y externo (FR-1300-PE-12). 1.5. Contexto del proceso 1.6. Identificación de activos de información.
Fase 2 – Identificación de riesgos	2.1. Identificación de riesgos inherentes
Fase 3 – Análisis y valoración de riesgos	3.1. Análisis de probabilidad e impacto 3.2. Valoración del riesgo
Fase 4 – Identificación y evaluación de controles	4.1. Identificación de controles. Debe definir los siguientes elementos: nombre del control, responsable, periodicidad, propósito, cómo se realiza y evidencias. 4.2. Evaluación de controles, de acuerdo con las siguientes preguntas: 1. ¿Existen manuales, instructivos o procedimientos para el manejo del control? 2. ¿Está definido el responsable de la ejecución del control y seguimiento? 3. ¿El control es automático? 4. ¿El control es manual? 5. ¿La frecuencia de ejecución del control y seguimiento es adecuada? 6. ¿Se cuenta con evidencias de la ejecución y seguimiento del control? 7. ¿En el tiempo que lleva la herramienta ha demostrado ser efectiva?

FASE	ASPECTOS POR CONSIDERAR
Fase 5 – Tratamiento de los riesgos	5.1. Definir medida de tratamiento del riesgo (aceptar, reducir, evitar, compartir) 5.2. Establecer niveles de aceptación de riesgo residual. 5.3. Elaborar plan de tratamiento de riesgos en caso de que le aplique.
Fase 6 – Monitoreo y seguimiento	6.1. Periodicidad de monitoreo y seguimiento a los controles y planes de tratamiento. 6.2. Validar efectividad de los controles.

5.5 ELEMENTOS PARA TENER EN CUENTA EN EL MAPA DE RIESGOS

a. Riesgos de gestión y corrupción se tiene en cuenta las siguientes tablas de probabilidad e impacto:

Tabla de probabilidad

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

Tabla de impacto

NIVEL	DESCRIPTOR	DESCRIPCIÓN
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencia o efectos mínimos sobre la entidad
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad.
5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

b. Riesgos de corrupción

En la descripción de los riesgos de corrupción deben concurrir todos los componentes:

Acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado.

Para determinar el impacto, sigue las siguientes preguntas:

Nº	Si el riesgo de corrupción se materializa podría…
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 o servicios o los 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?

c. Riesgos fiscales

El elemento medular de la responsabilidad fiscal, que es el daño al patrimonio público, representando en el menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos, o a los intereses patrimoniales del Estado (Decreto 403, 2020, art.6), se pueden tener en cuenta en el mapa de riesgos y oportunidades. Las bases de la responsabilidad fiscal están consignadas en la Ley 610 de 2000.

Para estos riesgos, se tendrá en cuenta lo estipulado en la guía de administración de riesgos del Departamento Administrativo de la Función Pública y demás instrumentos técnicos que en la materia se puedan aplicar.

d. Riesgos de seguridad de la información

Se debe tener en cuenta la Guía Metodológica Gestión de Riesgos para SGSI (G-1101-GTI-01,) cuyo objetivo es proporcionar las directrices para la identificación, análisis, evaluación y tratamiento de los riesgos de seguridad de la información de manera tal que los responsables

analicen y establezcan, en el marco de sus procesos, los activos de información asociados y se identifiquen los riesgos correspondientes.

5.6 TRATAMIENTO DE RIESGOS

Para la adecuada administración de los riesgos identificados se tendrán en cuenta las siguientes directrices:

a. Aquellos riesgos que, debido a su naturaleza, sobrepasen la capacidad del proceso/programa/proyecto en torno a la ejecución de medidas de tratamiento de los mismos, los gerentes públicos, líderes de proceso, líderes de proyectos/programas y de sus equipos de trabajo, supervisores de contratos, como primera línea de defensa, deberán presentarlos ante el Comité Institucional de Coordinación de Control Interno para recibir orientación al respecto.

b. La gestión de riesgos de seguridad de la información se realiza para los activos de información de la entidad valorados con un nivel de criticidad alto o extremo y su tratamiento se da de acuerdo con el plan de tratamiento de riesgos de seguridad definido por la entidad.

c. Cuando las condiciones externas y/o internas que originaron el riesgo, cambien o desaparezcan ocasionando la eliminación del riesgo, se documentará la situación en el Mapa de Riesgos y Oportunidades donde quedará el registro hasta el inicio de la siguiente vigencia en aras de tener la trazabilidad de la situación presentada. Se documentaría por correo a siplag@gestiondelriesgo justificando la inactivación.

d. Para hacer modificaciones a un riesgo u oportunidad incorporado en el Mapa de Riesgos y Oportunidades, deberá el líder del proceso notificar al correo siplag@gestiondelriesgo.gov.co con la descripción de los cambios. Si el riesgo o la oportunidad no aplica, se deberá dar la justificación y se clasificará como inactivo en la columna “Estado” del Mapa de Riesgos y Oportunidades.

e. **Nivel de aceptación del riesgo.** Para el tratamiento de los riesgos residuales (es decir, después de la aplicación de controles) se tendrá en cuenta:

- Riesgos valorados como MODERADO o BAJO: deben mantenerse monitoreados en aras que se mantengan en dicho nivel. No será necesario la formulación de planes de acción o de mitigación.
- Riesgos valorados como EXTREMO y ALTO: deberá formular planes de acción o mitigación para el tratamiento del riesgo.
- Las oportunidades valoradas como EXTREMA o ALTA serán establecidas en el mapa de riesgos y oportunidades y deberá tener al menos un control. Si se considera necesario, se formulará un plan de tratamiento.

f. Los riesgos de corrupción y fraude, por su naturaleza, son inaceptables y por lo tanto no aplica que se ubiquen en zona baja (color verde).

g. En caso de materializarse un riesgo los responsables de la Primera Línea de Defensa (gerentes públicos, líderes de proceso, líderes de proyectos/programas, supervisores de contrato) deberán:

- Informar por escrito al *Comité Institucional de Coordinación de Control Interno* por intermedio del Secretario Técnico del Comité (Jefe Oficina de Control Interno). Desde allí, si es necesario, se analizará la situación y se darán las orientaciones al respecto.
- Implementar una acción correctiva conforme con el *procedimiento de acciones correctivas y de mejora* definido en el Siplag, pudiendo valerse de la segunda línea de defensa para su formulación.
- Actualizar el mapa de riesgos y se procede conforme al literal d.
- Según sea el caso, reportar a las autoridades competentes los riesgos materializados de corrupción.

5.7 MONITOREO

Con el liderazgo de la Oficina Asesora de Planeación e Información y el Grupo de Tecnologías de la Información en su rol de segunda línea de defensa, se hará monitoreo cuatrimestralmente con corte a 30 de abril, 31 de agosto y 31 de diciembre, teniendo en cuenta el procedimiento de administración de riesgos y oportunidades PR-1300-SIPG-11.

5.8 SEGUIMIENTO Y EVALUACIÓN

La Oficina de Control Interno, como tercera línea de defensa, en su rol de evaluación de la gestión del riesgo, debe realizar seguimientos cuatrimestrales con cortes a 30 de abril, 31 de agosto y 31 de diciembre. Los resultados de dichos seguimientos serán publicados en la página web de la UNGRD o en un lugar de fácil acceso al ciudadano en los plazos establecidos en la Ley 1474 de 2011 y demás decretos reglamentarios y en la ley 1712 de 2014.

ELABORÓ	REVISÓ	APROBÓ
Ítalo Prieto Téllez Sylvia Ribero Corzo	Maritza Herrera Molina	Olmedo de Jesús López Martínez
Profesionales Oficina Asesora de Planeación e Información / Grupo de Tecnologías de la Información/ Talento Humano	Coordinadora Grupo Talento Humano / Coordinador Grupo de Tecnologías de la Información/	Director General

6. CONTROL DE CAMBIOS DEL DOCUMENTO

VERSIÓN	DESCRIPCIÓN DEL CAMBIO	FECHA
01	Emisión Inicial	16/06/2020
02	Se actualizan algunas definiciones acordes a lo establecido en la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 del DAFP. Se ajusta el alcance omitiendo la diferenciación de riesgos relacionados con seguridad de la información. Se actualizan roles y responsabilidades de las líneas de defensa. Se elimina la especificación de los riesgos de gestión ambiental, dado que el manual aplica a toda la entidad.	26/10/2021
03	Se ajustó los responsables de la segunda línea de defensa; en las líneas de defensa se complementó las responsabilidades y se agrega lo relacionado con fraude y riesgo fiscal; en la sección de metodología, se complementó aspectos para tener en cuenta en la fase de contexto y se incluyó la sección de monitoreo. Se incluyó detalle de los riesgos de corrupción (redacción); tablas de probabilidad e impacto de los riesgos de gestión y corrupción. En relación a SGSI, se actualizó los ítems de la matriz de seguimiento y lo relacionado a los riesgos de seguridad de la información literal d del punto 5.5. En 5.6 literal b, se ajustó riesgos de información (antes de seguridad digital). 5.8 se ajusta la normativa de los plazos del seguimiento y evaluación establecidos en la Ley 1474 de 2011 y demás decretos reglamentarios, y en la Ley 1712 de 2014.	18/12/2023