

Departamento Administrativo Nacional de Estadística




Sinergia Organizacional SIO

Oficina Asesora de Planeación / – OPLAN

PROCEDIMIENTO DE ADMINISTRACIÓN DE RIESGOS

Nov/2020

	PROCEDIMIENTO DE ADMINISTRACIÓN DE RIESGOS	CÓDIGO: SIO-040-PDT-002 VERSIÓN: 8 FECHA: 10/Nov/2020
PROCESO: Sinergia Organizacional	SUBPROCESO: Implementación y Mantenimiento	

1. OBJETIVO

Establecer las actividades necesarias para administrar los riesgos de gestión, corrupción y seguridad de la información del DANE-FONDANE.

2. ALCANCE

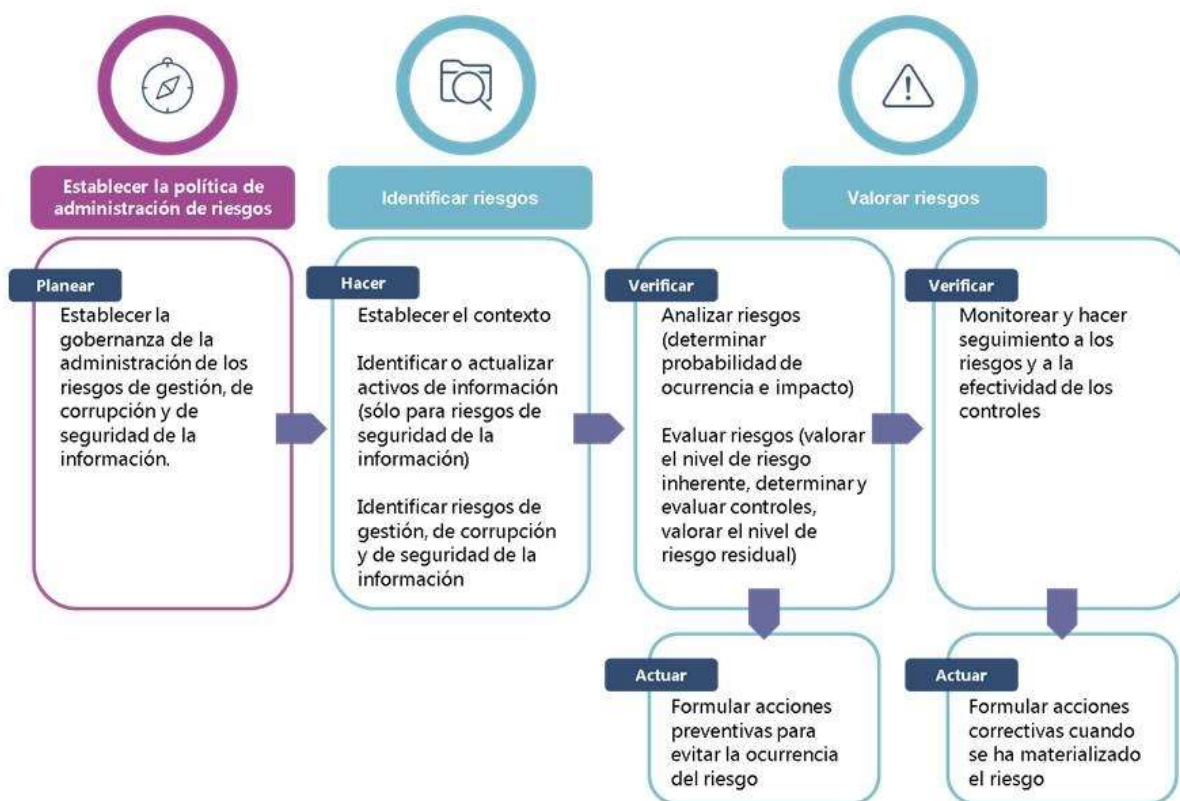
Inicia con las actividades de definir o actualizar y aprobar la política de administración de riesgos. Continúa con las actividades de establecer el contexto, identificar, modificar o trasladar riesgos, analizar y evaluar riesgos, ejecutar los controles y los planes de tratamiento, realizar el monitoreo de los riesgos, realizar el seguimiento a la administración de riesgos y finaliza con elaborar y presentar informes de riesgos.

3. INSUMO (INFORMACIÓN DE ENTRADA)

- Contexto institucional.
- Documentos del Sistema Integrado de Gestión Institucional.
- Información relacionada con riesgos.
- Guía de administración de riesgos.
- Plan Estratégico Institucional.
- Política de administración de riesgos.

4. POLÍTICAS DE OPERACIÓN

- La administración de riesgos se desarrolla a través de tres etapas: establecer la política de administración de riesgos, identificar y valorar los riesgos, las cuales se resumen en la siguiente gráfica:



Fuente: Adaptado del Departamento Administrativo de la Función Pública. (2018). Guía para la administración del riesgo y el diseño de controles en entidades públicas (p. 13).

- La administración de riesgos se desarrolla siguiendo los lineamientos establecidos en la política de administración de riesgos, conforme con la normatividad legal y técnica vigente que regule la materia.
- La revisión y/o actualización anual de los riesgos de corrupción es obligatoria. Los riesgos de gestión y de seguridad de la información se actualizan cada vez que se requiera.
- La primera línea de defensa debe registrar los controles establecidos para minimizar la probabilidad de ocurrencia y/o el impacto de los riesgos en los documentos de los procesos del Sistema Integrado de Gestión. También deben crear y administrar las carpetas necesarias para acopiar y disponer las evidencias de la ejecución de los controles y verificar que las evidencias correspondan a estos controles.
- La Oficina Asesora de Planeación debe publicar los mapas de riesgos en la página web. Se debe publicar una versión consolidada y anonimizada de los riesgos de corrupción a más tardar el 31 de enero de cada año; esta versión debe haberse sometido con antelación a la consulta de la ciudadanía a través de la página web u otro medio, junto con el Plan Anticorrupción y de Atención al Ciudadano; cada vez que surjan cambios en este consolidado, deberá publicarse actualizado.
- Las fechas de corte para cada monitoreo son 30 de abril, 31 de agosto y 31 de diciembre de cada vigencia; el resultado del monitoreo de los riesgos se debe reportar a la segunda línea de defensa dentro de los diez (10) días hábiles siguientes a la fecha de corte.

- La Oficina de Control Interno debe realizar seguimiento al cumplimiento de la administración de riesgos conforme con los lineamientos establecidos en la política de administración de riesgos y la normatividad legal y técnica vigente que regule la materia.
- Los cambios realizados y aprobados a los mapas de riesgos comenzarán a operar en la fecha de inicio del cuatrimestre inmediatamente siguiente. Si ocurren cambios en los mapas de riesgos entre los meses de enero y abril, estos comienzan a operar a partir del 1 de mayo; los cambios realizados entre los meses de mayo y agosto comienzan a operar a partir del 1 de septiembre; y los cambios realizados entre los meses de septiembre y diciembre comienzan a operar a partir del 1 de enero.

5. DEFINICIONES

- **Activo:** Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854 2016, pág. 56).
- **Administración del riesgo:** Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la entidad un aseguramiento razonable con respecto al logro de los objetivos. (DAFP 2018).
- **Amenaza:** Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización. (ISO/IEC 27000:2016).
- **Control:** Medida que modifica el riesgo. (NTC ISO 31000:2011). Medios para gestionar el riesgo e incluye políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal. (MGRSD 2018).
- **Daño antijurídico:** Perjuicio causado a una persona natural o jurídica, como consecuencia de una acción, omisión o exceso en el ejercicio de una actividad pública, que provoque que el afectado soporte una carga u obligación, superior a la que social o legalmente estaba obligado.
- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad. (DAFP 2018).
- **Impacto:** Se entiende como las consecuencias ocasionadas por la materialización del riesgo. (DAFP 2018).
- **Infraestructura crítica cibernética nacional:** Aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública. (CONPES 3854, pág. 29).
- **Integridad:** Propiedad de exactitud y completitud. (DAFP 2018).
- **Política de administración de riesgos:** Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo. (NTC ISO 31000:2011).
- **Primera línea de defensa:** En el DANE – FONDANE, está conformada por los líderes de procesos, directores territoriales, responsables de programas, de proyectos y sus equipos de trabajo (servidores públicos y contratistas a nivel nacional).
- **Probabilidad:** Es la posibilidad de ocurrencia de un riesgo, la cual puede ser medida con criterios de frecuencia o factibilidad. (DAFP 2018).
- **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. (DAFP 2018).
- **Riesgo de gestión:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias. (DAFP 2018).
- **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 27000:2016).
- **Riesgo de seguridad digital:** Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas. (DAFP 2018).
- **Riesgo inherente:** Es aquel al que se enfrenta la entidad en ausencia de controles que modifiquen su probabilidad de ocurrencia o impacto. (DAFP 2018).
- **Riesgo residual:** Es el riesgo que permanece luego de haber diseñado, implementado y valorado la efectividad de los controles. (Basado en DAFP 2018).
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas. (ISO/IEC 27000:2016).

- **Segunda línea de defensa:** En el DANE – FONDANE, está conformada por la Oficina Asesora de Planeación, el Comité de Seguridad de la Información, el responsable de seguridad de la información y la Oficina Asesora Jurídica.
- **Seguridad digital:** Es la situación de normalidad y de tranquilidad en el entorno digital (cibespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país. (CONPES 3854 2016, pág. 29).
- **Servicio esencial:** Servicio prestado por el gobierno o por cualquier organización o entidad, es aquel servicio cuya modificación o interrupción puede poner en riesgo la seguridad, la salud o la vida de los ciudadanos. (Plan Sectorial de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia PSPICCN V 1.0. 2019).
- **Tercera línea de defensa:** En el DANE – FONDANE, está conformada por la Oficina de Control Interno.
- **Vulnerabilidad:** Es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas. (Basado en DAFP 2018).

6. DESCRIPCIÓN DE ACTIVIDADES

Nº	Actividad	Descripción	Responsable Cargo y/o grupo responsable/ Dependencia	Registro Resultado (Documento Evidencia)	Puntos de Control
1	Definir o actualizar la política de administración de riesgos.	Establecer los lineamientos y el marco general de actuación en la administración de riesgos de gestión, de corrupción y de seguridad de la información.	Oficina Asesora de Planeación Comité de Seguridad de la Información	Propuesta de política de administración de riesgos	Verificar que la política de administración de riesgos contenga todos los elementos requeridos en la normatividad vigente que rige la materia.
2	Aprobar la política de administración de riesgos.	Revisar, ajustar de ser necesario y aprobar, la política de administración de riesgos.	Alta dirección	Acta del Comité de Coordinación de Control Interno	
3	Establecer el contexto	Identificar los cambios en el direccionamiento estratégico y en el contexto de la entidad (amenazas y vulnerabilidades) y cómo estos pueden generar nuevos riesgos o modificar los existentes en sus procesos.	Primera línea de defensa	Formatos mapa de riesgos de gestión, de seguridad de la información y de corrupción (este último cuando aplique) diligenciados.	
4	¿Se van a identificar nuevos riesgos o a modificar los existentes?	SI: Continúa en la actividad No. 6. NO: Continúa en la actividad No. 5.	Primera línea de defensa		
5	Justificar por qué no se detectan riesgos o no se	Explicar de forma convincente el motivo o razón por el cual no se detectan o modifican los riesgos (gestión, corrupción, seguridad	Primera línea de defensa	Ayuda de memoria con lista de asistencia o	

	modifican los existentes	de la información. Finaliza el procedimiento.		correo electrónico	
6	¿Se van a identificar nuevos riesgos de seguridad de la información o modificar los existentes?	SI: Continúa en la actividad No. 7. NO: Continúa en la actividad No. 8.	Primera línea de defensa		
7	Identificar o actualizar y clasificar el inventario de activos de información	Elaborar o actualizar y clasificar el inventario de activos de información conforme con la documentación vigente. El responsable de seguridad de la información asesorará de forma proactiva en esta actividad	Primera línea de defensa	Inventario de activos de información	
8	Identificar, modificar o trasladar riesgos	Identificar o modificar y clasificar los riesgos que pueden ocurrir y que puedan afectar el cumplimiento de la misión y de los objetivos de los procesos, utilizando el formato mapa de riesgos de gestión, de corrupción o de seguridad de la información, según aplique. Para trasladar un riesgo de un proceso a otro, se requiere que haya un acuerdo entre los respectivos responsables y gestionar los cambios necesarios ante la Oficina Asesora de Planeación, enviando las evidencias (ayuda de memoria con lista de asistencia) de las decisiones tomadas mediante correo electrónico dirigido al coordinador del GIT Gestión Organizacional. La Oficina Asesora de Planeación y el responsable de seguridad de la información asesorarán de forma proactiva estas actividades.	Primera línea de defensa	Para identificar, modificar :Formatos mapa de riesgos de gestión, de seguridad de la información y de corrupción (este último cuando aplique) diligenciados. Para trasladar: Correo electrónico con evidencias	
9	Analizar y evaluar los riesgos	Establecer la probabilidad de ocurrencia de los riesgos y el nivel de impacto que podrían tener si llegaran a materializarse, con el fin de estimar el riesgo inherente. Para lo anterior, se debe diligenciar el formato de probabilidad de ocurrencia e impacto que se encuentra el formato mapa de riesgos de gestión, de corrupción o de seguridad de la información,	Primera línea de defensa	Formatos mapa de riesgos de gestión, de seguridad de la información y de corrupción (este último cuando aplique) diligenciados.	

		<p>según aplique.</p> <p>La Oficina Asesora de Planeación y el responsable de seguridad de la información asesorarán de forma proactiva estas actividades.</p>			
10	Determinar y evaluar controles	<p>Establecer y evaluar controles, tanto en su diseño como en su ejecución utilizando el formato mapa de riesgos de gestión, de corrupción o de seguridad de la información, según aplique.</p> <p>La Oficina Asesora de Planeación y el responsable de seguridad de la información asesorarán de forma proactiva estas actividades.</p> <p>La Oficina Asesora Jurídica asesorará en el establecimiento de controles adecuados para minimizar las vulnerabilidades que puedan generar daño antijurídico.</p>	Primera línea de defensa	<p>Formatos mapa de riesgos de gestión, de seguridad de la información y de corrupción (este último cuando aplique) diligenciados</p>	<p>Verificar que los controles se encuentren documentados en los procedimientos.</p>
11	Determinar el nivel de riesgo residual y formular acciones de tratamiento	<p>Determinar el nivel de riesgo residual, utilizando el formato mapa de riesgos de gestión, de corrupción o de seguridad de la información, según aplique.</p> <p>Formular acciones de tratamiento con acciones preventivas para evitar la materialización de riesgos teniendo en cuenta los niveles de aceptación del riesgo que se encuentran en la política de administración de riesgos.</p> <p>La Oficina Asesora de Planeación y el responsable de seguridad de la información asesorarán de forma proactiva estas actividades.</p>	Primera línea de defensa	<p>Formatos mapa de riesgos de gestión, de seguridad de la información y de corrupción (este último cuando aplique) diligenciados</p>	<p>Verificar que la suscripción de los planes de tratamiento se realice de conformidad con los lineamientos de la Oficina de Control Interno.</p>
12	Aprobar y socializar los riesgos	<p>Enviar aprobación de los riesgos mediante correo electrónico dirigido al Coordinador del GIT Gestión Organizacional (para riesgos de gestión y de corrupción) y al responsable de seguridad de la información (para riesgos de seguridad de la información), adjuntando el formato mapa de riesgos respectivo diligenciado.</p> <p>Socializar los riesgos a quienes</p>	Primera línea de defensa	<p>Formatos mapa de riesgos de gestión, de seguridad de la información y de corrupción (este último cuando aplique) diligenciados</p> <p>Correo electrónico</p>	

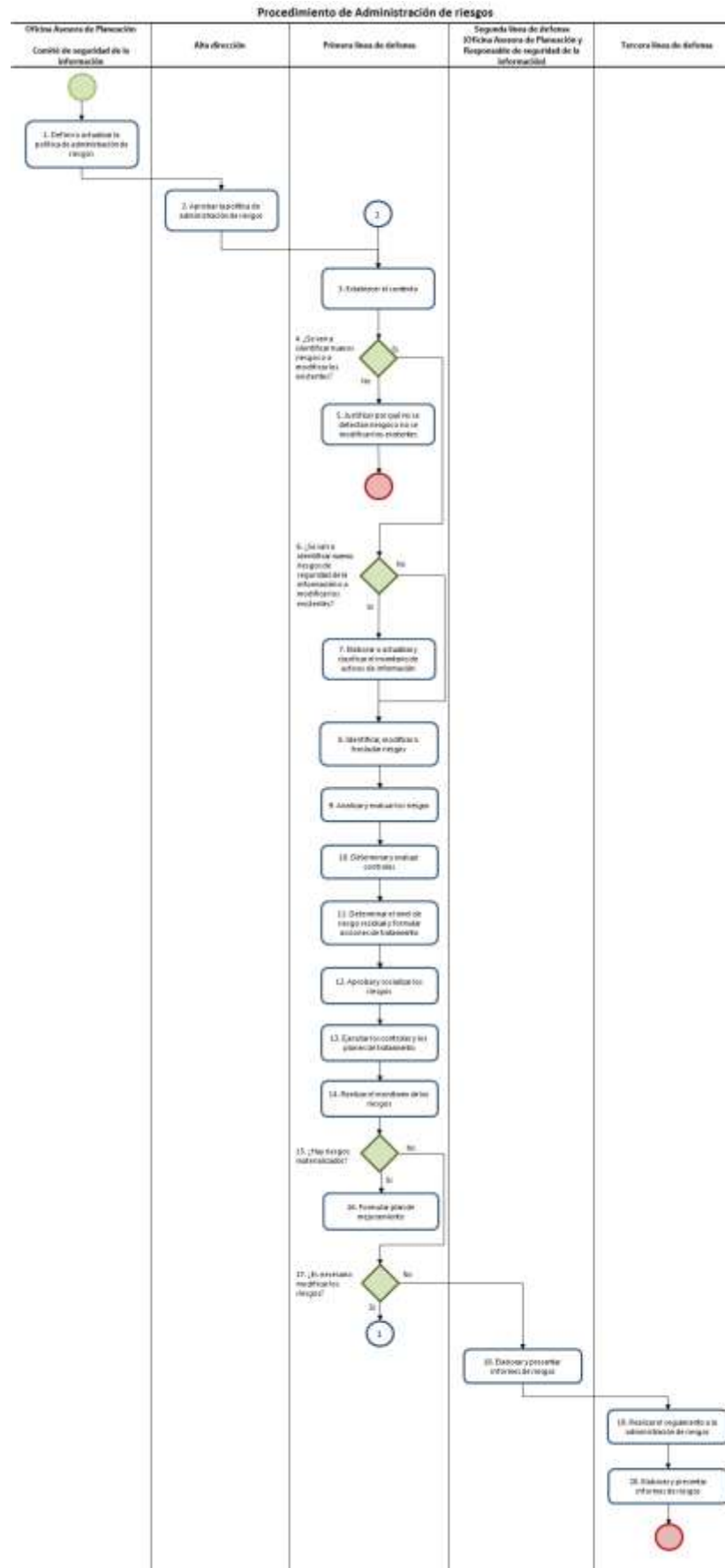
		intervienen o participan en el proceso, especialmente a los encargados de ejecutar los controles en DANE Central y territoriales.		Registros de la socialización	
13	Ejecutar los controles y los planes de tratamiento	<p>Ejecutar los controles establecidos para minimizar la probabilidad de ocurrencia y/o el impacto de los riesgos, según la periodicidad indicada, así como las acciones establecidas en los planes de tratamiento y generar las evidencias correspondientes.</p> <p>Nota: Se deben recopilar las evidencias de la ejecución de los controles y de los planes de tratamiento en el sitio que se disponga para presentarlas cuando sean requeridas.</p>	Primera línea de defensa	Evidencias de la ejecución de los controles y de los planes de tratamiento	Verificar que las evidencias correspondan a los controles identificados en el mapa de riesgos y a las acciones establecidas en los planes de tratamiento.
14	Realizar el monitoreo de los riesgos	<p>Realizar el monitoreo cuatrimestral utilizando el formato mapa de riesgos de gestión, de corrupción o de seguridad de la información, según aplique, considerando los siguientes aspectos:</p> <ul style="list-style-type: none"> • Las amenazas y vulnerabilidades que generan los riesgos. • La materialización de los riesgos. • La ejecución y efectividad de los controles. <p>Reportar los resultados del monitoreo a la segunda línea de defensa con la misma periodicidad, a través de correo electrónico dirigido al Coordinador del GIT Gestión Organizacional (para riesgos de gestión y de corrupción) y al responsable de seguridad de la información (para riesgos de seguridad de la información).</p> <p>La Oficina Asesora de Planeación y el responsable de seguridad de la información asesorarán de forma proactiva estas actividades.</p>	Primera línea de defensa	Correo electrónico con los resultados del monitoreo	
15	¿Hay riesgos materializados?	SI: Continúa en la actividad No. 16.	Primera línea de defensa		

		NO: Continúa en la actividad No. 17.			
16	Formular plan de mejoramiento	Cuando se materialice un riesgo se debe formular un plan de mejoramiento con acciones correctivas tendientes a evitar que vuelva a ocurrir. Si el riesgo materializado es de corrupción, además de la formulación del plan de mejoramiento, el hecho deberá ponerse en conocimiento del superior inmediato y de la Oficina de Control Interno Disciplinario. La Oficina Asesora de Planeación y el responsable de seguridad de la información asesorarán de forma proactiva estas actividades.	Primera línea de defensa Grupo1	Plan de mejoramiento	Verificar que la suscripción de los planes de mejoramiento se realice de conformidad con los lineamientos de la Oficina de Control Interno.
17	¿Es necesario modificar los riesgos?	SI: Continúa en la actividad No. 3. NO: Continúa en la actividad No. 18.	Primera línea de defensa		
18	Elaborar y presentar reportes de riesgos	Elaborar reportes cuatrimestrales para la Línea estratégica sobre los riesgos, su severidad y materialización.	Segunda línea de defensa (Oficina Asesora de Planeación y Responsable de seguridad de la información)	Reportes de riesgos	
19	Realizar el seguimiento a la administración de riesgos	Realizar actividades de monitoreo y revisión a las etapas de la administración de riesgos, con el fin de presentar recomendaciones relacionadas con: <ul style="list-style-type: none"> • Cambios en el direccionamiento estratégico o en el contexto y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados. • La identificación de riesgos significativos que afectan el cumplimiento de los objetivos de los procesos. • El adecuado diseño y ejecución de los controles para la mitigación de los riesgos establecidos por parte de 	Tercera línea de defensa	Informes de riesgos	

		<p>la primera línea de defensa (es decir, que se encuentren documentados y actualizados en los procedimientos) y realizar recomendaciones y seguimiento para el fortalecimiento de los mismos.</p> <ul style="list-style-type: none">• El perfil de riesgos inherente y residual.• Cualquier riesgo que se encuentre por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad no sea coherente con los resultados de las auditorías realizadas.• Seguimiento al cumplimiento de los planes de tratamiento o mejoramiento relacionados con la administración del riesgo.			
		<p>Elaborar informes cuatrimestrales para la Línea estratégica relacionados con el seguimiento a la administración de riesgos.</p>			

7. DIAGRAMA DE FLUJO

- [Ver Archivo original del Flujograma](#)



8. REGISTROS (Documento evidencia)

Código	Nombre	Almacenamiento Físico	Almacenamiento Magnético
SIO-O4O-PDT-OO2-f-001	Formato de Mapa de Riesgo de Gestión		X
SIO-O4O-PDT-OO2-f-002	Formato Mapa de Riesgos de Corrupción		X
SIO-O4O-PDT-OO2-f-003	Formato Mapa de Riesgos de Seguridad de la Información		X

9. ANEXOS

- [Guía para la administración del riesgo y el diseño en entidades públicas V4 -DAFP](#)

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
3	04/Jul/2013	Actualización del Documento
4	16/May/2014	Se modifica el alcance del procedimiento incluyendo las Territoriales y los proyectos, se incluyen nuevas políticas de operación, se modifican las actividades establecidas y se incluyen nuevas definiciones.
5	07/Jun/2016	Se incluyen documentos externos que emiten lineamientos como Información de entrada, se incluyen nuevos conceptos relacionados y se aclaran algunos existentes y se aclaran algunas políticas de operación, dando cumplimiento al Decreto 124 del 26 de enero de 2016 sobre Riesgos de Corrupción. Así mismo, se incluyen nuevos formatos para el desarrollo de algunas etapas en la administración de riesgos.
6	23/Mar/2017	Se ajusta el documento en cuanto a: 1. Se especifica la definición del mapa de riesgos institucional. 2. Inclusión de las responsabilidades territoriales en medición de controles y en la etapa de monitoreo mediante la herramienta tablero de control de riesgos. 3. Se flexibiliza el envío de información tanto al correo institucional (SDI) como al correo del responsable de riesgos asignado por la OPLAN y opcional al Jefe de OPLAN. 4. Se puntualiza cuando se pueden ajustar los riesgos (crear, eliminar, trasladar). 5. Se especifica la responsabilidad de los líderes e integrantes de la MPTMC en la revisión del mapa de riesgos publicado y cualquier ajuste solicitado a este documento. 6. Se dejan todos los registros con almacenamiento magnético. 7. Se unifica en todo el documento el nombre del formato PDE-040-LIN-001-r004-Evaluación de Controles de Administración del Riesgo. 8. Actualización del diagrama de flujo (responsable territorial y medición de controles)
7	09/Jul/2018	Se ajusta el documento en cuanto a: 1. Se puntualiza sobre las fechas de recepción de los reportes de monitoreo. 2. Se especifican los periodos de recepción de los seguimientos realizados por la Oficina de Control Interno. 3. Se puntualizan las responsabilidades de la verificación de la publicación de los seguimientos realizados por la Oficina de Control Interno.

8	09/Nov/2020	<p>1. En el marco del rediseño del mapa de procesos el procedimiento pasa del proceso Planeación y Direccionamiento Estratégico/subproceso Sistema Integrado de Gestión Institucional al proceso de Sinergia Organizacional/subproceso Implementación y Mantenimiento.</p> <p>2. Se ajusta todos los items del procedimiento (objetivo, alcance, insumos, política de operación, definiciones, descripción de actividades, etc.) teniendo en cuenta los lineamientos de la Guía de Administración del Riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública y de la nueva forma de operar basada en la política de administración de riesgos del DANE-FONDANE</p>
---	-------------	---

ELABORÓ	REVISÓ	APROBÓ
Nombre: Sandra Patricia Burgos Chaquer Cargo: Profesional Especializado Fecha: 10/Nov/2020	Nombre: Hernan David Gonzalez Carrillo Cargo: Profesional Especializado Fecha: 10/Nov/2020	Nombre: Lina Paola Cardozo Orjuela Cargo: Jefe Oficina Asesora de Planeación Fecha: 10/Nov/2020

Si este documento es impreso se considera copia no controlada