ARCHIVO GENERAL DE LA NACIÓN COLOMBIA

LINEAMIENTOS DE POLÍTICA DE ADMINISTRACIÓN Y GESTIÓN DE RIESGOS DEL ARCHIVO GENERAL DE LA NACIÓN

MARZO DE 2022

La cultura es de todos Mincultura

Introducción

La Administración del Riesgo comprende el conjunto de elementos de control y sus interrelaciones, para que la entidad identifique, evalúe y gestione eventos potenciales, tanto internos como externos, que puedan afectar el logro de los objetivos institucionales, contribuye a que la entidad consolide su Sistema de Control Interno y a generar una cultura de autocontrol y autoevaluación al interior de esta.

La administración de riesgos contribuye a minimizar la ocurrencia de hechos que puedan afectar el cumplimiento de la misionalidad del Archivo General de la Nación, por ello se encuentra alineado y armonizado con el Modelo Integrado de Planeación y Gestión MIPG y la Guía para la Gestión del Riesgo vigente establecida por el Departamento Administrativo de la Función Pública, la cual articula los riesgos de gestión, corrupción y de seguridad digital y la estructura del Sistema Integrado de Gestión.

1. Objetivo

Establecer los elementos y el marco general de actuación para la gestión integral de los riesgos, de toda naturaleza, a los que se enfrenta la Entidad y orientar las acciones necesarias que conduzcan a disminuir la vulnerabilidad frente a situaciones que puedan interferir en el logro de su misionalidad y objetivos institucionales y establecer la respuesta oportuna a amenazas externas que puedan generar eventos de riesgo.

2. Alcance

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

3. Glosario

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.

CICCI: Comité Institucional de Coordinación de Control Interno.

Factores de Riesgo: Fuente generadora de los eventos de riesgos operativos.

Riesgos Operativos: Posibilidad de incurrir en pérdidas por errores, fallas, deficiencias en el Talento Humano, Procesos, Tecnología, Infraestructura y Eventos Externos.

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.

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.

Riesgo de corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviarla gestión de lo público hacia un beneficio privado.

Gestión del riesgo: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización 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.

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

Probabilidad: Se entiende como la posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de Frecuencia o Factibilidad.

Impacto: Se entiende como las consecuencias que pueden ocasionar a la organización la materialización del riesgo.

Riesgo inherente: Es aquel riesgo al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

Riesgo residual: Nivel de riesgo permanente luego de tomar medidas de tratamiento del riesgo.

Mapa de Riesgos: Documento con la información resultante de la gestión del riesgo.

Plan anticorrupción y de Atención al Ciudadano: plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

Confidencialidad: propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

Control: medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

Vulnerabilidad: es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

Amenazas: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Integridad: propiedad de exactitud y completitud.

Disponibilidad: propiedad de ser accesible y utilizable a demanda por una entidad.

Tolerancia al riesgo: son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.

Metodología General Ajustada- MGA: es una aplicación informática que sigue un orden lógico para el registro de la información más relevante resultado del proceso de formulación y estructuración de los proyectos de inversión pública.

4. Responsabilidades

La responsabilidad está definida mediante las líneas de defensa determinadas dentro de MIPG y en el Archivo General de la Nación se acogen según la siguiente tabla:

RESPONSABILIDADES FRENTE A LOS RIESGOS

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
Línea Estratégica	Comité Directivo Comité de Gestión y Desempeño Institucional (CGDI) Comité Institucional de Coordinación de Control Interno (CICCI)	•Definir y aprobar el marco general para la gestión del riesgo y el control. • Analizar los riesgos, vulnerabilidades y amenazas institucionales para el cumplimiento de los objetivos estratégicos, planes institucionales, metas y compromisos de la entidad. • Definir y aprobar la política para la administración del riesgo. • Garantizar el cumplimiento de los planes de la entidad.
Primera Línea	A cargo de los gerentes públicos y líderes de los procesos, programas y proyectos.	• Identificar, valorar, evaluar y actualizar cuando se requiera, los riesgos que pueden afectar los objetivos, programas, proyectos y planes asociados a su proceso. • Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras para su gestión. • 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. • Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados.

		• Informar a la Oficina de Planeación (segunda línea) sobre los riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo. • Realizar y reportar el monitoreo correspondiente a los riesgos con oportunidad y en los medios y formatos que la Entidad disponga para el efecto.
Segunda Línea	Jefe Oficina Asesora de Planeación. Jefe Oficina Asesora Jurídica Supervisores e interventores de los contratos y proyectos. Coordinadores de Grupo. Comité de Contratación	• Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo residual. • 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 CICCI el resultado de la medición del nivel de eficacia de los controles para el tratamiento de los riesgos identificados en las áreas en los diferentes niveles de operación de la entidad. • Acompañar, orientar y asesorar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo. • Supervisar en coordinación con los demás responsables de esta segunda línea de defensa, que la primera línea identifique, analice, valore, evalué 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 monitoreados 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 para su aprobación del CICI. • Monitorear los riesgos identificados y controles definidos por la primera línea de defensa acorde con la estructura de los temas a su cargo. • Realizar el seguimiento al mapa de riesgos de su proceso. • Reportar o delegar a un profesional de la dependencia o grupo a su cargo, el registro de los avances en la gestión del riesgo.

		• Proponer 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.
Tercera Línea	Jefe Oficina de Control Interno.	• Revisar los cambios en el "Direccionamiento estratégico" o en el entorno y cómo estos puedan 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. • Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar. • Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, además de incluir los riesgos de corrupción. • Revisar el adecuado diseño y ejecución 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. • Revisar el perfil de riesgo inherente y residual por cada proceso consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas. • Para mitigar los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos y los planes de mejora como resultado de las auditorías efectuadas, además, que se lleven a cabo de manera oportuna, se establezcan las causas raíz del problema y se evite, en lo posible, la repetición de hallazgos y la materialización de los riesgos. • Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados.

Tabla 1. Fuente: Elaboración propia

5. Niveles de Aceptación y Periodicidad de Monitoreo o Seguimiento a los Riesgos

En el esquema que se detalla a continuación se establece el manejo (nivel de aceptación y periodicidad del monitoreo o seguimiento) que debe darse a los riesgos inherentes (antes de controles) de acuerdo con la zona de riesgo en la que se encuentre ubicado.

MATRIZ DE ACEPTACIÓN DEL RIESGO

Tipo de Riesgo	Zona de Riesgo	Nivel de Aceptación
Riesgos de Gestión	Bajo	Se **ACEPTA** el riesgo y se administra por medio de las actividades propias delproceso asociado. Se realiza seguimiento **TRIMESTRAL**.
	Moderado	Se establecen acciones de control preventivas que permitan **REDUCIR** la probabilidad de ocurrencia del riesgo, se hace seguimiento TRIMESTRA**L.**
	Alto y Extremo	Se debe incluir el riesgo tanto en el Mapa de riesgo del Proceso como en el Mapa de Riesgo Institucional y se establecen acciones de Control Preventivas que permitan **EVITAR** la materialización del riesgo o **COMPARTIR** el riesgo. Se monitorea **MENSUALMENTE.**
Riesgos de Corrupción	Bajo	Ningún riesgo de corrupción podrá ser aceptado en esta zona.
	Moderado	Se establecen acciones de control preventivas que permitan **REDUCIR** la probabilidad de ocurrencia del riesgo. Periodicidad **TRIMESTRAL**
	Alto y Extremo	Se adoptan medidas para: **REDUCIR** la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. **EVITAR** Se abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo. **COMPARTIR** una parte del riesgo para reducir la probabilidad o el impacto de este. Periodicidad TRIMESTRAL

Tabla 2. Fuente: Elaboración propia

El jefe de Control Interno del Archivo General de la Nación debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles, teniendo en cuenta los siguientes cortes:

Primer seguimiento: Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.

Segundo seguimiento: Con corte al 31 de agosto. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.

Tercer seguimiento: Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

6. Niveles para Calificar el Impacto

Los criterios para valorar el impacto de los riesgos serán los contenidos en la guía para la administración del riesgo vigente del DAFP así:

6.1 Niveles para Calificar el Impacto - Riesgos de Gestión

CALIFICACIÓN DEL IMPACTO DEL RIESGO

NIVEL	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
CATASTRÓFICO	- Impacto que afecte la ejecución presupuestal en un valor ≥50%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de información crítica para la entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
MAYOR	- Impacto que afecte la ejecución presupuestal en un valor ≥20%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.

MODERADO	- Impacto que afecte la ejecución presupuestal en un valor ≥5%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. - Inoportunidad en la información, ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias.
MENOR	- Impacto que afecte la ejecución presupuestal en un valor ≥1%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥5%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥1%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por algunas horas. - Reclamaciones o quejas de los usuarios, que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
INSIGNIFICANTE	- Impacto que afecte la ejecución presupuestal en un valor ≥0,5%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥0,5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5% del presupuesto general de la entidad.	- No hay interrupción de las operaciones de la entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa.

Tabla 4. Fuente: Elaboración propia

6.2 Niveles para Calificar los Riesgos de Seguridad Digital

CALIFICACIÓN DEL RIESGO DE SEGURIDAD DIGITAL

NIVEL	VALOR	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
INSIGNIFICANTE	1	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. No hay afectación medioambiental.	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad.
MENOR	2	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de ≥X días de recuperación.	Afectación leve de la integridad. Afectación leve de la disponibilidad. Afectación leve de la confidencialidad.
MODERADO	3	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de ≥X semanas de recuperación.	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.
MAYOR	4	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación importante del medio ambiente que requiere de ≥X meses de recuperación.	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros.
CATASTRÓFICO	5	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación muy grave del medio ambiente que requiere de ≥X meses de recuperación.	Afectación muy grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación muy grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.

Tabla 5. Fuente: Elaboración propia

6.3 Criterios para calificar el impacto de Riesgos de corrupción

La calificación obtenida se compara con la tabla de medición de impacto de riesgo de corrupción para obtener el nivel de impacto del riesgo.

CALIFICACIÓN DEL RIESGO DE CORRUPCIÓN

Calificación de Riesgo de Corrupción Impacto		
Respuestas Afirmativas	**Descripción**	**Nivel**
Entre 1 y 5	Moderado: Genera medianas consecuencias sobre la entidad	3
Entre 6-11	Mayor: Genera altas consecuencias sobre la Entidad	4
Entre 12 y 19	Catastrófico	5

Tabla 6. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas VERSIÓN 5

La medición del impacto de los riesgos de corrupción se realiza aplicando la siguiente tabla de valoración.

VALORACIÓN RIESGO DE CORRUPCIÓN

No.	Si el riesgo de corrupción se materializa podría...	Respuesta
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?	
19	¿Generar daño ambiental?	

Tabla 7. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas VERSIÓN 5

7. Tratamiento de Riesgos

De llegarse a presentar la materialización de algún riesgo, el líder de proceso deberá realizar los análisis de las causas y hará los ajustes en los mapas correspondientes. A su vez se debe diligenciar el formato ESC-FO-01 PLAN DE MEJORAMIENTO, donde se propondrán las acciones de mejora del caso.

ACCIONES PARA TRATAMIENTO DE RIESGOS

TIPO DE RIESGO	ACCIÓN
CORRUPCIÓN	➢ Informar a las autoridades de la ocurrencia del hecho de corrupción. ➢ Revisar el Mapa de Riesgos de Corrupción, en particular las causas, riesgos y controles. ➢ Verificar si se tomaron acciones y se actualizó el Mapa de Riesgos de Corrupción. ➢ Realizar un monitoreo permanente. ➢ Identificar e implementar acciones correctivas necesarias y establecer Plan de mejoramiento para efectuar el análisis de causas y determinar acciones preventivas y de mejora. ➢ Definir nuevos controles asociados al riesgo teniendo en cuenta el plan de mejoramiento definido.
GESTIÓN Y SEGURIDAD DIGITAL	➢ Hacer una descripción detallada de lo ocurrido y del impacto generado en el proceso. ➢ Revisar el mapa de Riesgos del proceso en particular las causas, riesgos y controles. Se debe tener en cuenta que en el análisis del riesgo varía la probabilidad. ➢ Tomar acciones para evitar que se repita la materialización del riesgo detectado y actualizar el mapa de riesgos y sus acciones de seguimiento contempladas. ➢ Realizar un monitoreo permanente.

Tabla 8. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas VERSIÓN 5

8. Periodicidad de la actualización al Mapa de Riesgos

El mapa de riesgos del Archivo General de la Nación se actualizará cada dos años o antes en caso de ser materializado alguno de los riesgos contemplados allí o si el líder del proceso así lo solicita.

Esta política es aprobada el 31 de marzo de 2022.

Firmado digitalmente por ENRIQUE SERRANO LOPEZ

Enrique Serrano López
Director General
Archivo General de la Nación