1. OBJETIVO

Establecer los lineamientos que le permitan a la Agencia Nacional Digital proteger todos sus procesos de los potenciales riesgos asociados, así como establecer los mecanismos necesarios para evitar, reducir, compartir, transferir y/o mitigar los riesgos inherentes a su quehacer institucional y que pudieran afectar a las personas, las instalaciones, los bienes y los equipos de la entidad, y los objetivos institucionales

1.1. Objetivos Específicos

- Proporcionar a la administración lineamientos para un aseguramiento razonable, orientado al cumplimiento de sus objetivos
- Establecer los roles y responsabilidades de las líneas de defensa de la entidad

2. ALCANCE

La presente política aplica para la gestión de riesgos, incluyendo aquellos que se pueden derivar de los procesos definidos, igualmente se consideran los que pueden afectar la prestación de los servicios o cualquier otra actividad de la Corporación Agencia Nacional de Gobierno Digital.

3. DEFINICIONES

Con el propósito de facilitar la comprensión de la Política se deben tener en cuenta las siguientes definiciones:

a.) Administración del Riesgo: un 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.

b.) Apetito de Riesgo: es el nivel de riesgo que la Agencia puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

c.) Capacidad de riesgo: es el máximo valor del nivel de riesgo que una entidad

puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad.

d.) Gestión del Riesgo: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

e.) Identificación del Riesgo: etapa en la cual se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias.

f.) Impacto: consecuencias o efectos que pueden ocasionar a la organización la materialización del riesgo.

g.) Matriz de Riesgo: documento en el cual se plasma la representación final de la probabilidad e impacto de uno o más riesgos frente a un proceso, proyecto o programa.

h.) 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.

i.) Probabilidad: se entiende la posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de frecuencia o factibilidad.

j.) Riesgo: posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

k.) Riesgos de Corrupción: posibilidad de que por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

l.) Riegos de gestión: posibilidad de que un evento potencial afecte el cumplimiento de los objetivos de los procesos de la organización, sus definiciones estratégicas, o su operación. Estos riesgos pueden ser de carácter judicial, contractual, financiero, administrativo, imagen, asociados a la prestación de servicios, fiscales, contables y presupuestales.

m.) 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).

n.) 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 potencial2. (ver conceptos de recursos públicos, bien público e Intereses patrimoniales de naturaleza pública).

o.) Tolerancia del riesgo: es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.

4. DOCUMENTOS REFERENCIA

- Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6. Función Pública, diciembre 2022.

5. POLÍTICA GESTIÓN INTEGRAL DEL RIESGO

La Corporación Agencia Nacional de Gobierno Digital – AND, se compromete a fortalecer la cultura de prevención, por medio de una adecuada gestión de riesgos, dirigiendo sus esfuerzos hacia el establecimiento de los mecanismos necesarios para evitar, reducir/mitigar, compartir/transferir y/o asumir los riesgos relacionados con el desarrollo de todos sus procesos y que pudieran afectar negativamente a las personas, las instalaciones y/o los bienes de la entidad; para tal efecto realizará la identificación, análisis, valoración e intervención de los riesgos inherentes al que hacer institucional, contribuyendo de esta forma al logro de los objetivos y la misión de la entidad.

La Agencia, por medio de la alta dirección asigna los recursos necesarios para lograr esta gestión del riesgo, propiciando los espacios que sean necesarios para que sus colaboradores participen de forma activa en todas las actividades relacionadas con el tema, lo anterior aplicando lo establecido en la presente Política y en el procedimiento de administración de riesgos.

Así mismo, los riesgos positivos que se identifican se entienden como oportunidades de mejora y se potencializan para ser aprovechados y mejorar los resultados de nuestra gestión institucional.

6. ESTRUCTURA INSTITUCIONAL

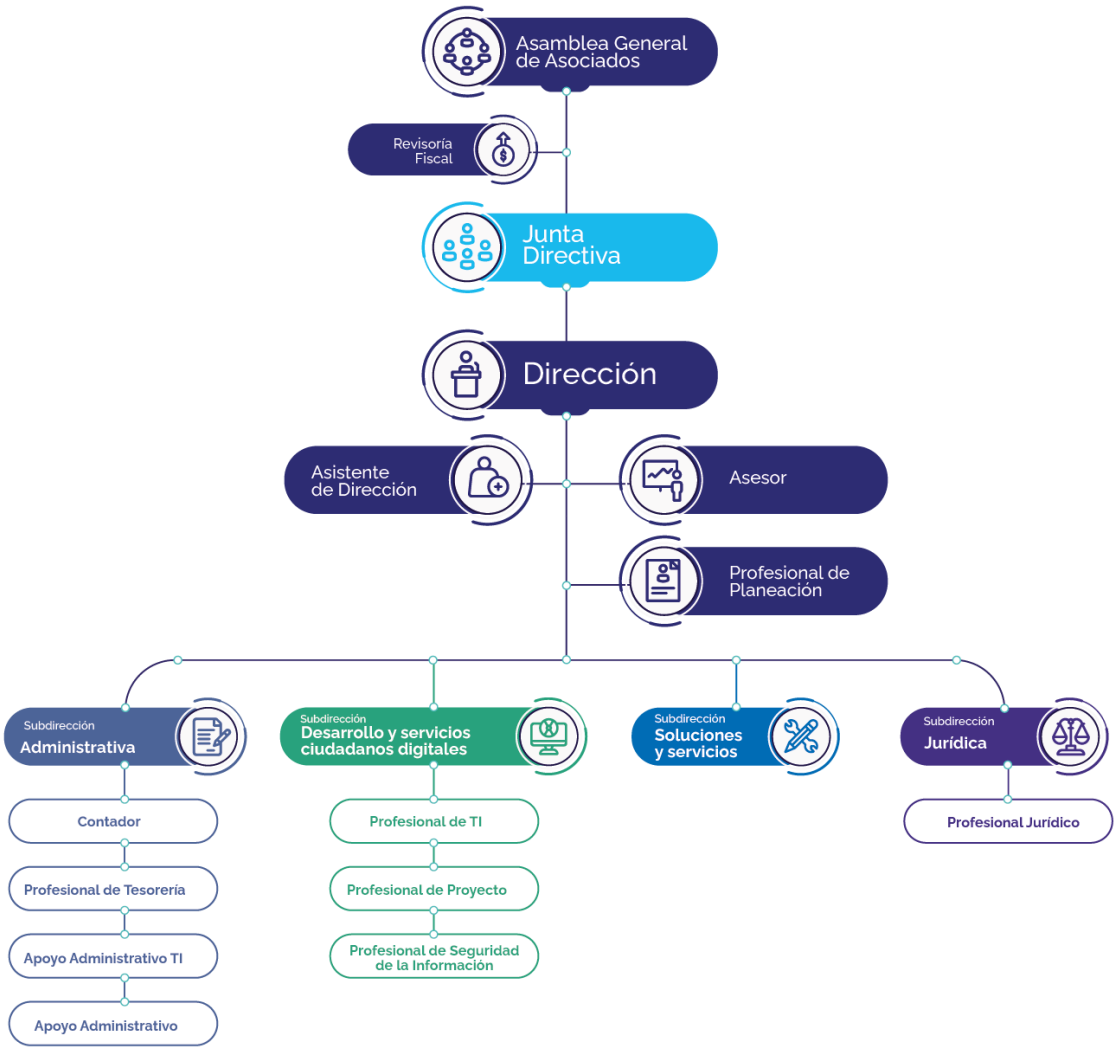


Figura 1 Estructura organizacional

Misión

La Agencia Nacional Digital –AND- es una corporación que presta servicios de asesoría y desarrollo de soluciones eficientes de transformación digital para entidades públicas y privadas, mejorando la calidad de vida de la ciudadanía.

Visión

En 2026 estaremos posicionados como la Entidad que moviliza la Transformación Digital de Colombia.

Objetivos estratégicos

1. Ampliar la cobertura en los procesos de articulación y prestación de los SCD en las entidades públicas y privadas.
2. Integrar soluciones y servicios enfocados en Ciencia, Tecnología e Innovación que aporten a la transformación digital del estado colombiano.
3. Consolidar el modelo de gestión y negocio que permita la autosostenibilidad y posicionamiento en el mercado.
4. Potenciar la AND como una entidad eficiente a través de un equipo humano competente para el logro de los objetivos organizacionales

Mapa de procesos

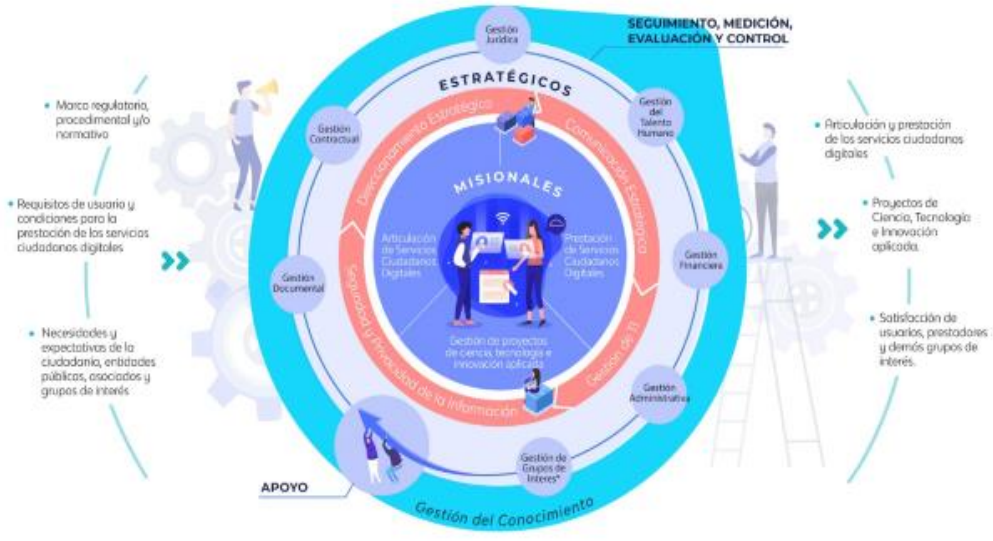


Figura 2. Mapa de procesos

7. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO EN LA AND

La AND implementa las etapas de identificación y valoración de los riesgos, teniendo como referencia la Guía para la Administración del riesgo y el diseño de

controles en entidades públicas del Departamento Administrativo de la Función Pública (DAFP)

Así mismo, la AND aplica su metodología de administración de riesgos en sus diferentes proyectos de desarrollo, reconociendo la importancia de controlar de forma organizada la ejecución de las actividades de control en sus proyectos, como también contar con un establecimiento adecuado de los riesgos que identifica, con el fin de prevenir sus materializaciones; enfocándose en el tratamiento efectivo de las causas que generan estos riesgos. Cabe mencionar, que la presente guía sirve como base para elaborar los diferentes planes de riesgos en los proyectos de Desarrollo.

A continuación, se aprecia la figura 3, que muestra de manera general la metodología aplicada en la Agencia.

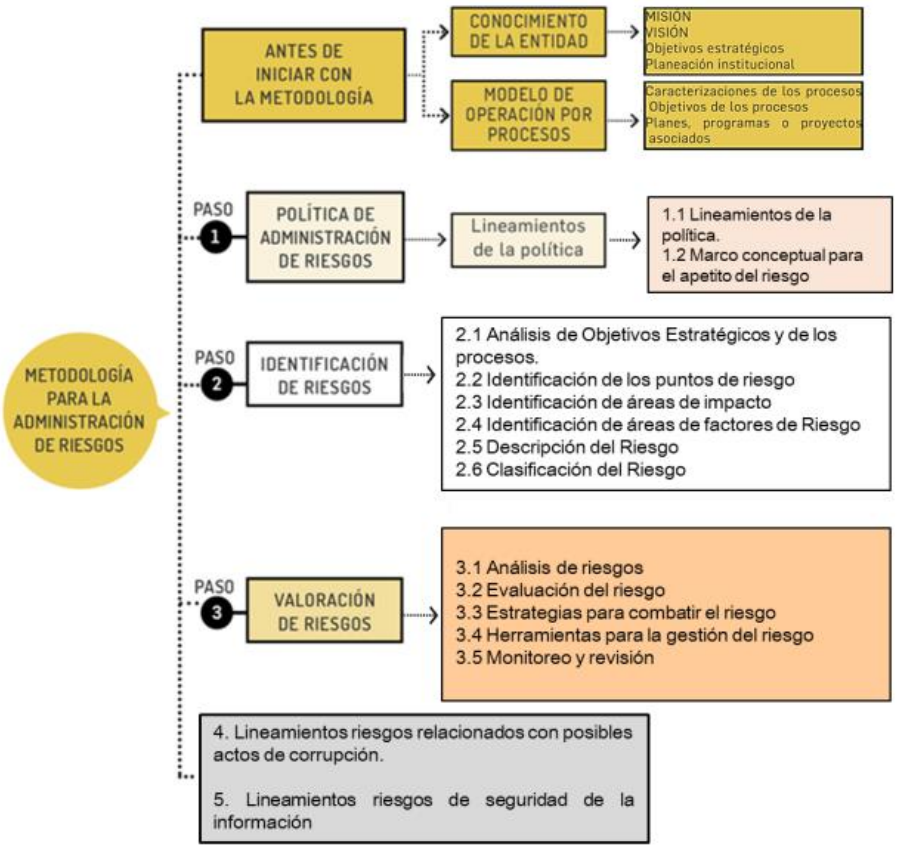


Figura 3. Metodología para la gestión del Riesgo en la AND

Fuente: Guía para la Administración del riesgo y el diseño de controles en entidades públicas versión 6, Departamento Administrativo de la Función Pública

Antes de iniciar con la metodología, es necesario contar con la información que permita llevar a cabo una contextualización de la organización, partiendo del conocimiento de la Entidad en cuanto a su misión, visión, objetivos estratégicos y su planeación institucional. En la Agencia Nacional Digital este contexto se encuentra plasmado en el Plan Estratégico Institucional el cual rige el quehacer de la Entidad.

De igual manera es fundamental que la Entidad cuente con un Modelo de Operación por Procesos en el marco del cual se evidencie la estructura para la gestión en la entidad a partir de los procesos identificados y en los cuales se pueda llevar a cabo la gestión de riesgos. En la Agencia Nacional Digital, dicho modelo se encuentra descrito en el DE.MN.01 Manual del SIG AND y en la Resolución 019 de 2021 "Por la cual se adopta el SIG AND".

En este contexto, la Agencia Nacional Digital cuenta con la intranet como la herramienta por medio de la cual se encuentra la información de los diferentes procesos de la Entidad, los cuales cuentan con cartas descriptivas o caracterizaciones en las cuales se establecen los objetivos de los procesos y se enmarcan los planes o proyectos que genera la Agencia. En el caso de los proyectos de Ciencia Tecnología e Innovación aplicada, así como de Prestación y Articulación de Servicios Ciudadanos Digitales, es importante adicionar el análisis del contexto de acuerdo con la particularidad de cada proyecto (Ej. Entidad para la que se desarrolla el proyecto, población objetivo del proyecto, etc.)

8. GESTIÓN DE RIESGOS

La Agencia Nacional Digital utiliza como principal referente para la gestión de riesgos la Guía para la administración del riesgo y el diseño de controles del Departamento Administrativo de la Función Pública. De igual manera se tendrá en cuenta el anexo A de la ISO/IEC 27001:2013 para la identificación de controles de los riesgos de seguridad de la información.

Las desviaciones que se puedan presentar en el seguimiento a los procesos, indicadores, cronogramas y demás herramientas que sean utilizadas en la Agencia para la gestión de los riesgos, deberán ser tratadas a través de planes de mejoramiento, los cuales deberán ser notificados por medio de correo electrónico a Control Interno, quien realizará el seguimiento correspondiente a las actividades propuestas.

8.1 Lineamientos Riesgos relacionados con posibles actos de corrupción

Dado que, para la gestión de riesgos de corrupción, continúan vigentes los lineamientos contenidos en la versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas de 2018 del DAFP, en la Agencia Nacional Digital se continuará llevando a cabo la gestión de este tipo de riesgos de acuerdo con lo allí indicado.

8.2 Lineamientos Riesgos de Seguridad de la información

Los riesgos de seguridad de la información serán identificados, valorados y tratados de acuerdo con la metodología descrita en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP.

Nota: Al finalizar la evaluación de los riesgos identificados, el gestor de riesgos de seguridad de la información debe hacer firmar el documento de aceptación de los riesgos a los diferentes líderes de proceso, con el fin de establecer responsabilidad en la gestión de los riesgos de seguridad digital.

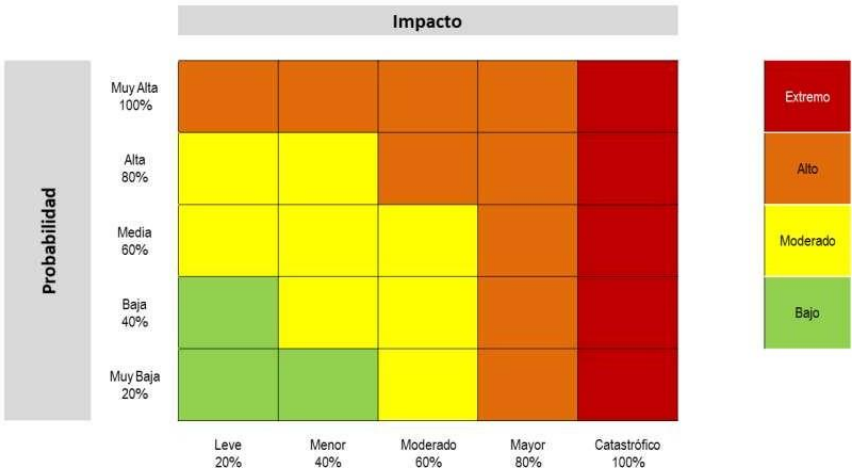
8.3 Apetito del Riesgo (Niveles de Aceptación del Riesgo)

El apetito del riesgo o el nivel del riesgo que la Agencia puede aceptar, está dado por los objetivos de la Agencia, el marco legal y disposiciones de la alta dirección. En este sentido a continuación se determina la capacidad del riesgo, el apetito del riesgo y la tolerancia del riesgo para la AND:

8.3.1 **Determinación de la Capacidad del Riesgo:** es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual se considera por la alta dirección que no sería posible el logro de los objetivos de la entidad.

En este contexto, la escala que resulta de combinar la probabilidad y el impacto en la valoración de los riesgos genera los niveles de riesgo, estos son: extremo, alto, moderado y bajo, tal como se muestra en la siguiente figura:

Figura 4. Matriz de calor – Niveles de severidad del riesgo



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

En este marco, la Agencia Nacional Digital define que el valor máximo de la escala del nivel del riesgo que puede ser resistido por la entidad antes de perder total o parcialmente la capacidad de cumplir con sus objetivos, es el nivel del riesgo extremo, siendo este su capacidad de riesgo.

8.3.2 Determinación del Apetito del Riesgo: el valor máximo deseable del nivel de riesgo que podría permitir el logro de los objetivos institucionales en condiciones normales de operación del modelo integrado de planeación y gestión en la entidad. Equivale al nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

En este contexto, la Agencia Nacional Digital define que el nivel de riesgo que la entidad puede aceptar para los riesgos operativos o de gestión es el nivel alto y para los riesgos de seguridad digital es el nivel moderado.

8.3.3 Tolerancia del Riesgo: es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad. Para determinar la tolerancia de riesgo, se debe definir un valor que es igual o superior al apetito de riesgo y menor o igual a la capacidad de riesgo.

En este marco, la Agencia Nacional Digital define que la tolerancia del riesgo

para riesgos operativos o de gestión es el nivel extremo, así como para los riesgos de seguridad digital es el nivel alto.

Teniendo en cuenta todo lo anterior, en la siguiente tabla se definen las medidas de respuesta que se pueden ejecutar dependiendo del nivel de Riesgo:

Tabla 1. Medidas de Respuesta a Niveles de severidad del riesgo

Nivel del Riesgo	Medidas de Respuesta
Riesgo nivel Bajo	Aceptar el Riesgo
Riesgo nivel Moderado	Reducir el Riesgo
Riesgo nivel Alto	Reducir el Riesgo, Transferir el Riesgo o Evitar del Riesgo
Riesgo nivel Extremo	Reducir el Riesgo, Transferir el Riesgo o Evitar el Riesgo

Fuente: Guía para la Administración del riesgo y el diseño de controles en entidades públicas versión 6. Departamento Administrativo de la Función Pública

8.4 Niveles para la Calificación del Impacto

De conformidad con la Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6. Función Pública, se dispone la siguiente tabla para la calificación del impacto:

Tabla 2. Calificación del Impacto de riesgos

Nivel	Descriptor	Afectación económica	Reputacional
1	Leve 20%	ctación menor a 10 SMLMV	El riesgo afecta la imagen de algún área de la organización.
2	Menor 40 %	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y

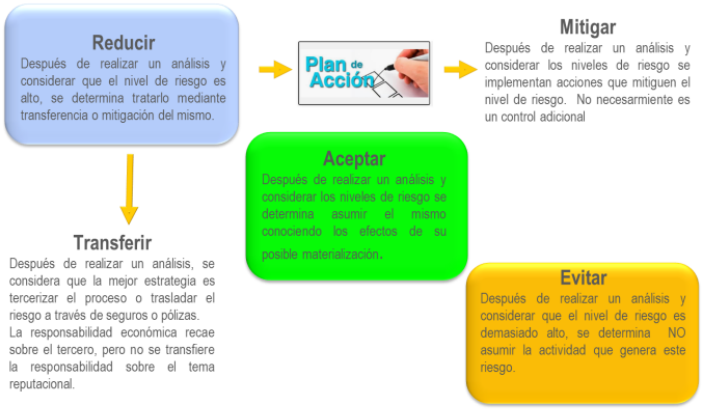
			accionistas y/o de proveedores.
3	Moderado 60 %	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
4	Mayor 80 %	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
5	Catastrófico 100 %	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: Guía para la Administración del riesgo y el diseño de controles en entidades públicas V6. Departamento Administrativo de la Función Pública

8.5 Estrategias para combatir el riesgo

Es la decisión que se toma frente a un determinado nivel de riesgo, la cual puede ser aceptar, reducir o evitar. Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente. En la siguiente ilustración se observan las tres opciones mencionadas y su relación con la necesidad de definir planes de acción dentro del respectivo mapa de riesgos.

Ilustración 17. Estrategias para combatir el Riesgo



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Fuente: Guía para la Administración del riesgo y el diseño de controles en entidades públicas versión 6, Departamento Administrativo de la Función Pública

Frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de tareas o proyectos. Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.

Nota: El plan de acción acá referido es diferente a un plan de contingencia, el cual se enmarca en el Plan de Continuidad de Negocio y se consideraría un control correctivo.

9 ESQUEMA DE LAS LÍNEAS DE DEFENSA

De conformidad con lo establecido en el MIPG, se describe la siguiente metodología, en la cual se define el esquema de las líneas de defensa adoptado por la Agencia Nacional Digital:

Línea Estratégica

Alta Dirección Comité de Gestión y Desempeño y **Comité Institucional de Coordinación de Control Interno**

Este nivel analiza los riesgos y amenazas institucionales al cumplimiento de los planes estratégicos, tendrá la responsabilidad de definir el marco general para la gestión del riesgo (política de administración del riesgo) y garantiza el cumplimiento de los planes de la entidad.

1ª Línea de Defensa

Medidas de Control Interno: (controles del día a día). Ejecutados por el equipo de trabajo.

Controles de Gerencia Operativa:

(Ejecutados por un Jefe)

- ✓ La gestión operacional se encarga del mantenimiento efectivo de controles internos, ejecutar procedimientos de riesgo y el control sobre una base del día a día.
- ✓ La gestión operacional identifica, evalúa, controla y mitiga los riesgos.

2

2ª Línea de Defensa

Media y Alta Gerencia:

Jefes de planeación o quienes hagan sus veces, coordinadores de equipos de trabajo, comités de riesgos (donde existan), Comité de contratación, áreas financieras, de TIC, entre otros que generen información para el Aseguramiento de la operación.

- ✓ Asegura 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.
- ✓ Consolidan y analizan información sobre temas clave para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos.

3

3ª Línea de Defensa

- ✓ Desarrolla los componentes de Control Interno:
  1. Liderazgo Estratégico
  2. Enfoque Hacia la Prevención
  3. Evaluación de la Gestión de Riesgo
  4. Relación con Entes Externos de Control.
  5. Evaluación y Seguimiento.

10.1 ROLES Y RESPONSABILIDADES

Línea estratégica

Responsable	Responsabilidad frente al riesgo
Alta Dirección. Comité de Gestión y Desempeño y Comité Institucional de Coordinación de Control Interno	• Aprobar la Política de Gestión Integral del riesgo. • Definir y hacer seguimiento a los niveles de aceptación (apetito al riesgo). • Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la Agencia y que puedan generar cambios en la estructura de los riesgos identificados y en sus actividades de control. • Realizar seguimiento y análisis periódico a los riesgos institucionales. • Revisar la exposición de la entidad a los riesgos de corrupción y fraude de acuerdo con los informes del canal de denuncias PQRSD. • Monitorear el tratamiento de las denuncias de riesgos de corrupción y fraude desde el Comité Institucional de Coordinación de Control Interno. • Realimentar en el Comité Institucional de Gestión y Desempeño los ajustes que se deban hacer frente a la gestión del riesgo. • Evaluar el estado del sistema de control interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento de este. • Monitorear el cumplimiento de los estándares de conducta y la práctica de los principios y valores de los funcionarios públicos por medio del Comité Institucional de Coordinación de Control Interno.
Director(a)	• Aprobar las directrices determinadas de la Administración de Riesgos aplicables a la entidad. • Definir el marco general para la administración del riesgo • Presentar los cambios en el Direccionamiento Estratégico y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados. • Hacer seguimiento en el Comité Institucional de Coordinación de Control Interno en la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por Control Interno.

Primera línea de defensa

Responsable	Responsabilidad frente al riesgo
Líderes de procesos Gerentes de proyecto	• Realizar el análisis de contexto y análisis de causas, relacionados con cada mapa de riesgos que lidera. • Identificar y valorar los riesgos que pueden afectar los programas, proyectos, planes y procesos a su cargo y actualizarlos cuando se requiera. • Realizar la evaluación del riesgo inherente y riesgo residual, aplicando las actividades de control que correspondan. • Definir, aplicar y hacer seguimiento a las actividades de control para tratar los riesgos identificados, alineados con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo en su proceso o proyecto. • Aprobar los riesgos formulados o actualizados • Supervisar la ejecución de las actividades de control aplicadas 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, con base en la evaluación del diseño de actividades de control. • Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de las actividades de control. • Informar a Planeación o quien haga sus veces (segunda línea) sobre los riesgos materializados en los programas, planes y/o procesos a su cargo. En el caso de los proyectos de desarrollo, el Gerente debe informar al cliente en las reuniones de seguimiento programadas, y coordinar con Control Interno (tercera línea) el establecimiento del plan de mejoramiento respectivo. • Diligenciar el mapa de riesgos del proceso o proyecto liderado, el cual debe ser aprobado por la AND (en el caso de los proyectos, requiere aprobación del cliente) y mantenerlo actualizada, en caso de requerir asesoría por parte de Planeación, realizar la solicitud correspondiente. • Los líderes de Procesos, Proyectos, propietarios y responsables de Activos de Información son los encargados de realizar la gestión del Riesgo sobre dichos Activos de Información. El Oficial de Seguridad de la Información debe promover y apoyar la ejecución de esta actividad, basado en la metodología aprobada para tal fin.

Segunda Línea de defensa

Responsable	Responsabilidad frente al riesgo
Persona o equipo asignado para realizar las funciones de Planeación en la AND.	• 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. • Consolidar el Mapa de riesgos institucional y presentar en el comité de gestión y desempeño los riesgos de mayor criticidad frente al logro de los objetivos para análisis y seguimiento. • Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos y proyectos. • Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles. • Presentar a la Línea Estratégica alertas sobre eventos y cambios en el entorno
Profesional asignado como Oficial de seguridad de la información	Evaluar el cumplimiento de los controles asociados a las Políticas de Seguridad de la Información
Subdirector jurídico	• Monitorear la gestión contractual y generar alertas sobre retrasos, incumplimientos u otras situaciones de riesgo detectadas • Monitorear la gestión jurídica, generando alertas sobre retrasos, incumplimientos u otras situaciones de riesgo detectadas en esta materia
Subdirector administrativo / Profesional asignado	• Hacer monitoreo a las PQRD generando alertas sobre incumplimientos, quejas en la prestación del servicio, tutelas u otras situaciones de riesgo detectadas • Monitorear temas clave del ciclo del servidor (capacitación, bienestar, incentivos, convivencia laboral, código integridad), generando alertas sobre incumplimientos, situaciones críticas que afectan en clima laboral y posibles afectaciones al código de integridad • Monitorear en Plan Estratégico de Tecnologías de la Información - PETI
Gerentes de proyectos	• Monitorear aspectos estructurales de los temas bajo su gestión, generando alertas sobre retrasos, incumplimientos u otras situaciones de riesgo detectadas acorde con las materias a su cargo

Tercera Línea de defensa

Responsable	Responsabilidad frente al riesgo
Persona o equipo asignado para realizar las funciones de Control Interno	• Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de las actividades de control establecidas en los procesos y proyectos. • Proporcionar aseguramiento objetivo en los procesos y proyectos identificados no cubiertos por la primera y segunda línea de defensa. • Acompañar de forma coordinada con el equipo de Planeación, a la primera línea de defensa en la identificación de los riesgos institucionales y en el diseño de las actividades de control. • Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos de conformidad con el Programa Anual de Auditoría. • Recomendar mejoras a la política y guía de administración del riesgo. • Comunicar a la Alta Dirección sobre posibles materializaciones de riesgos críticos en la Agencia. • Realizar acompañamiento a los Gerentes de Proyecto de desarrollo, sobre la aplicación correcta de la presente política. • Evaluar la eficacia de las actividades de control establecidas por la primera línea de defensa en los diferentes mapas de riesgo.

11.Seguimiento y Registro de riesgos materializados

El seguimiento de los riesgos identificados se realizará con base en el nivel de riesgo residual de acuerdo con las escalas descritas en la matriz de calor residual, así:

Nivel de Riesgo Residual	Periodicidad de Seguimiento
Extremo	Mensual
Alto	Trimestral
Moderado	Semestral
Bajo	Anual

El seguimiento principal estará en cabeza de los líderes de procesos, gerentes de proyectos y el equipo de trabajo que se designe para este fin, posteriormente desde el rol de Planeación, se realizará el seguimiento de

acuerdo con la periodicidad descrita en la tabla anterior, en el caso que sea necesario, se realizarán las recomendaciones necesarias en relación con el diseño y ejecución de los controles incluidos los controles que mitigan los riesgos estratégicos o institucionales.

Anualmente se revisará el mapa de riesgos completo, tomando como base las auditorías realizadas por Control Interno, los organismos de control y las notificaciones de materialización realizadas por los líderes de procesos y gerentes de proyecto, con el objetivo de actualizar el mapa de riesgos institucional conforme a los cambios presentados en cada vigencia. Adicional, en este seguimiento se realizará la verificación de la efectividad de los controles identificados en los riesgos de los procesos y proyectos.

El reporte de los eventos de riesgos materializados será enviado mediante correo electrónico por el Líder del proceso o gerente de proyecto, al equipo asignado con funciones de Planeación, el cuál debe informar la situación presentada (incluyendo el análisis de causas respectivo), fecha inicio y fin del suceso, fecha de reporte, riesgo al cual está asociado, proceso o proyecto en donde se identificó el suceso, impacto, acciones adelantadas, actividades de control relacionadas y consecuencias. Este reporte debe realizarse cuando el evento del riesgo materializado se presente.

Partiendo del análisis de causas del evento materializado, se debe formular un plan de mejora que indique la corrección o actividades de mitigación de este.

Los colaboradores con rol y funciones de Planeación deben validar, consolidar y analizar los eventos de riesgos materializados reportados por los procesos o proyectos, y presentar en los casos requeridos, ante el Comité de Gestión y Desempeño aquellos que deban ser de su conocimiento y revisión. A través del Comité de Coordinación de Control Interno se realizará la verificación de la gestión realizada a los riesgos materializados.

12. MONITOREO

Primera línea de defensa
A través de autocontrol los funcionarios y contratistas de la primera línea de defensa realizan constante verificación de la gestión los controles y planes de mitigación del riesgo. Se deberá realizar el reporte de seguimiento de manera cuatrimestral para riesgos de corrupción y semestral para riesgos de gestión y de seguridad de la información.

Segunda línea de defensa
De acuerdo con la información reportada por la primera línea de defensa,

Planeación analiza las situaciones asociadas a la gestión de riesgos en el marco de cambios, o necesidades de mejora que se deban gestionar en los riesgos de la entidad, informando a la primera línea sobre lo observado en los respectivos reportes.

Tercera línea de defensa
Este monitoreo lo gestiona el (la) profesional de Control Interno, quién realizará evaluación al cumplimiento de las acciones establecidas en los mapas de riesgos. De acuerdo con la programación de Plan anual de auditorías se analizará la efectividad de los controles asociados a los riesgos

13. COMUNICACIÓN

Los colaboradores con rol y funciones de Planeación y Control Interno coordinarán las acciones necesarias para promover la comunicación de información que promueva la cultura de gestión integral de los riesgos en la AND.

De igual forma, Planeación coordinará la divulgación y publicación de las de riesgos, de acuerdo con las necesidades de divulgación y las partes interesadas a quienes se dirija la publicación, principalmente considerando: la página web y la intranet.

Respecto a los riesgos de Seguridad de la Información, todas las novedades se comunicarán al Oficial de Seguridad de la Información y se dejará la documentación asociada, que puede ser por correo electrónico u oficio, de igual manera el/la Oficial deberá presentar en el Comité de Gestión y Desempeño dichas novedades.

14.CUMPLIMIENTO

La presente Política se debe aplicar en todos los procesos y por todos los colaboradores de la Agencia.

15.VIGENCIA DE LA POLÍTICA

La política se revisará y actualizará, cuando se presenten cambios organizacionales, del entorno, operativos o normativos que afecten a la Entidad. Así mismo, se revisará cuando ocurran cambios de alcance que obliguen a su fortalecimiento, o de acuerdo con los resultados de las actividades de seguimiento y control definidos. De igual manera, cuando sea necesario incluir las observaciones o recomendaciones presentadas por

control interno en los informes de seguimientos, o los resultados de las evaluaciones llevadas a cabo por los organismos de control.

16. CONTROL DE CAMBIOS

REVISIÓN No.	FECHA	DESCRIPCIÓN DEL CAMBIO
1	25/09/2018	Emisión del Documento
2	16/12/2019	Actualización del documento de acuerdo con el contexto de la Agencia.
3	11/10/2021	Actualización del objetivo, cambio del numeral de los objetivos específicos, inclusión de definiciones, inclusión del punto 6 y 7, de acuerdo con la última versión de la Guía para la administración del riesgo y el diseño de controles en entidades públicas (versión 5). Función Pública, diciembre 2020 y ajuste del numeral 9.
4	27/06/2024	• Ajuste en redacción del objetivo de la política incluyendo la relación con los objetivos institucionales • Ajuste en redacción de objetivos específicos • Ampliación de definiciones (riesgo seguridad digital y riesgo fiscal) • Referenciación de Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 6 • Eliminación de referenciación de la Guía para la administración de riesgos de la Agencia Nacional Digital. La información allí dispuesta se consolidó en la actual política • Se incluye la misión, visión y objetivos estratégicos de la entidad • Se ajusta redacción sobre apetito y tolerancia de riesgo para riesgos de corrupción • Se incluye la sección de estrategias para compartir el riesgo (reducir, aceptar, mitigar, transferir y evitar • Se incluye el capítulo de roles y responsabilidades para cada una de las líneas de defensa. Este capítulo estaba incluido en la Guía para la administración del riesgo de la entidad. • Se incluyen roles para profesional asignado a oficial de seguridad de la información, al subdirector jurídico, y al subdirector

		administrativo, en el marco de los requisitos que evalúa el Formulario Único de reporte de Avances en la Gestión FURAG. • Se incluye capítulo de seguimiento y registro de riesgos materializados • Se incluye capítulo de monitoreo de riesgos • Se ajusta la redacción del capítulo 12 "Comunicación"

Firmado digitalmente por CLAVIJO CUINEME LUIS ALBERTO
Fecha: 2024.07.17 11:15:14 -05'00'

LUIS ALBERTO CLAVIJO CUINEME
Director (E)

Revisó: Anyela Méndez Santos – Asesora de Seguimiento y Evaluación
Giovanny Montenegro – Profesional de Planeación
Comité Institucional de Coordinación de Control Interno - Sesión Extraordinaria 27 de junio de 2024
Elaboró: Carlos Quitián – Profesional de Planeación