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 negativamente a las personas, las instalaciones, los bienes y los equipos de la entidad.

1.1. Objetivos Específicos

- Manejar de forma adecuada la incertidumbre que se puede presentar en la ejecución de las diferentes actividades, siendo necesario realizar una gestión del Riesgo organizada.
- Proporcionar a la administración un aseguramiento razonable, orientado al cumplimiento de sus objetivos.

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.) Riesgos de Seguridad Digital: 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.

n.) 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 5. Función Pública, diciembre 2020.

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 su guía interna de tratamiento de riesgos, que incluye en una sola metodología lo relacionado con riesgos de gestión u operativos, corrupción y seguridad digital.

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. GESTIÓN DE RIESGOS

La Agencia Nacional Digital, dispone de la SM.GU.01 Guía para la Administración de Riesgos por medio de la cual se describen los lineamientos para la identificación, análisis, valoración, evaluación, tratamiento, seguimiento y comunicación de los riesgos que se puedan materializar en los procesos y proyectos adelantados por la Agencia.

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.

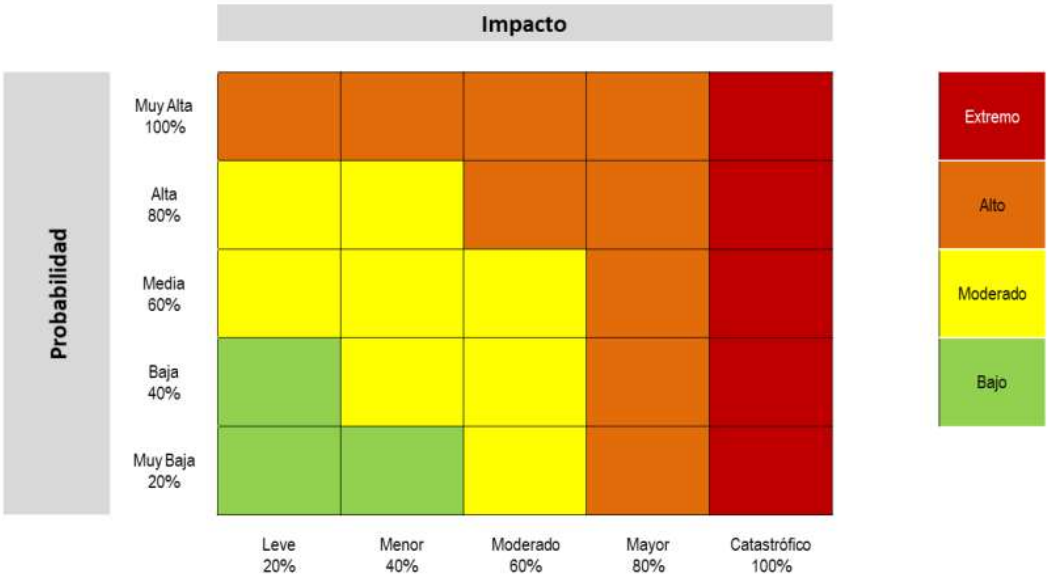
6.1. Apetito del Riesgo (Niveles de Aceptación del Riesgo)

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:

6.1.1. 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 el siguiente gráfico:

Gráfico 1. Matriz de calor – Niveles de severidad del riesgo



Fuente: DAFP

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.

6.1.2. 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. En cuanto a los riesgos de corrupción el nivel aceptado por la entidad es el nivel bajo, siendo estos el apetito del riesgo de la Agencia.

6.1.3. 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. En cuanto a los riesgos de corrupción el nivel de tolerancia continúa siendo el nivel bajo.

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	Aceptar el Riesgo o 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: DAFP

6.2. 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 5. Función Pública, diciembre 2020, 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%	Afectación 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 algún área de la organización.
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: DAFP

7. ESQUEMA DE LAS LÍNEAS DE DEFENSA

De conformidad con lo establecido en 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.

1

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)

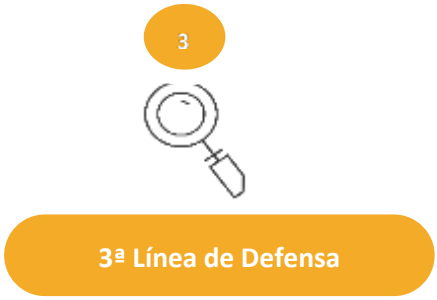
- ✓ La gestión operacional se encarga del mantenimiento efectivo de controles internos, ejecutar procedimientos de riesgo y el control sobre una base del día a día.
- ✓ La gestión operacional identifica, evalúa, controla y mitiga los riesgos.

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.



- ✓ 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.

Así mismo, a través de la SM.GU.01 Guía para la Administración de Riesgos se establecen las responsabilidades de cada línea de defensa frente a la Gestión de Riesgos, las cuales quedan consignadas en el Formato para la estructura de la segunda línea de defensa, adaptado desde el Manual Operativo de MIPG Versión 2, donde se describen las responsabilidades y roles distribuidos a través de cada funcionario o área específica frente a la gestión del riesgo y control de la Agencia Nacional Digital.

8. CUMPLIMIENTO

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

9. 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.

10. 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.

JOHAN SEBASTIAN ESLAVA GARZÓN
Director

Revisó y aprobó: Comité Institucional de Coordinación de Control Interno, sesión 11 de octubre de 2021
Elaboró: Johanna Catherine Laverde Moncada – Profesional de Planeación
Anyela Méndez Santos – Profesional Control Interno, Contratista