FND Federación Nacional de Departamentos

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

2025

TABLA DE CONTENIDO

1. OBJETIVO

Establecer las bases y disposiciones de la FND para identificar, analizar, evaluar, tratar y hacer seguimiento a los riesgos a los que está expuesta la entidad (gestión, corrupción, soborno, seguridad, privacidad de la información, seguridad digital, así como cualquier otro tipo de riesgo que se identifique o que deba prevenirse en atención a la normatividad interna o externa aplicable a la entidad); a través del diseño y ejecución de controles efectivos, lo que le permite asegurar razonablemente el logro de la misión, visión, objetivos estratégicos y objetivos de los procesos.

De acuerdo con lo anterior, por medio de la presente política se define una metodología para la administración del riesgo orientada minimizar su ocurrencia y mitigar su impacto ante una eventual materialización, buscando la consecución de los objetivos institucionales; así como posibilitar la mejora continua en el proceso de toma de decisiones, teniendo en cuenta los siguientes aspectos:

- Fomentar la cultura de la prevención del riesgo en todos los niveles de la FND.
- Mantener los controles que permitan el adecuado aprovechamiento de los recursos destinados a la ejecución de los procesos siempre bajo las mejores condiciones de eficacia, eficiencia y efectividad.
- Gestionar de forma anticipada las vulnerabilidades o eventos que puedan afectar el logro de los objetivos institucionales.

2. ALCANCE

La Política de Administración de Riesgos de la FND se aplicará para prevenir y mitigar los riesgos relativos a gestión, corrupción, soborno, seguridad, privacidad de la información y seguridad digital, así como cualquier otro tipo de riesgo que se identifique o que deba prevenirse en atención a la normatividad interna o externa aplicable a la entidad, en todos sus procesos y niveles.

Aplica desde la identificación, el análisis y evaluación de los riesgos, el diseño y aplicación de controles sólidos y efectivos para su mitigación, hasta el seguimiento y monitoreo periódico de los mismos como medida de autoevaluación, autocontrol y evaluación independiente.

3. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

La política de administración de riesgos de la FND tiene un carácter estratégico. Está fundamentada, como insumo, en el modelo integrado de planeación y gestión, y en la guía para la administración del riesgo y el diseño de controles en entidades públicas. Esta política se basa en un enfoque preventivo de evaluación permanente de la gestión y el control, promoviendo el mejoramiento continuo con la participación de todos los colaboradores de la entidad.

Aplica para todos los niveles, áreas y procesos de la Entidad e involucra el contexto, la identificación, valoración, tratamiento, monitoreo, revisión, comunicación, consulta y el análisis de los siguientes riesgos:

- Los riesgos de gestión de proceso que pueda afectar el cumplimiento de la misión y objetivos institucionales.
- Los riesgos de posibles actos de corrupción y/o soborno a través de la prevención de la ocurrencia de eventos en los que se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- Los riesgos de seguridad de la información que puedan afectar la confidencialidad, integridad y disponibilidad de la información de los procesos de la entidad.
- Los riesgos de continuidad de negocio que impiden la prestación normal de los servicios institucionales debido a eventos calificados como crisis.

4. DEFINICIONES

Para efectos de lo dispuesto en la presente Política, las siguientes definiciones tienen el significado específico que a continuación se indica:

Administración del riesgo: Conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.

Amenaza: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización el cual puede ser un factor no controlable por la FND.

Auditoría interna: Es una actividad independiente y objetiva de aseguramiento y consulta, para agregar valor y mejorar la gestión de la organización.

Análisis de riesgo: Es el proceso través del cual se establece la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona

de riesgo inicial (Riesgo Inherente).

Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo; entendido paralelamente como evento de interrupción.

Causa raíz: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

Clasificación del riesgo: Es el nivel de riesgo que la FND puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la FND debe o desea gestionar.

Control: Medida que se toma para modificar la exposición al riesgo, bien sea para disminuir la probabilidad de ocurrencia del evento o para disminuir su impacto.

Control correctivo: Medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones); está orientado a disminuir el nivel de impacto del riesgo.

Control preventivo: Medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones); está orientado a disminuir la probabilidad de ocurrencia del riesgo.

Efecto: Situaciones resultantes de la materialización del riesgo que impactan en el proceso, la FND, sus grupos de valor y demás partes interesadas.

Evaluación del riesgo: Proceso general de identificación, análisis y valoración de los riesgos.

Identificación del riesgo: Etapa del proceso para encontrar, reconocer y describir el riesgo.

Impacto: Los efectos que puede ocasionar a la organización la materialización del riesgo.

Líneas de defensa MIPG: El modelo de las Líneas de Defensa proporciona una manera simple y efectiva para mejorar las comunicaciones en la gestión de riesgos y control mediante la aclaración de las funciones y deberes esenciales relacionados.

Matriz de riesgos: Documento que permite inventariar, estandarizar y agrupar (estimar, tipificar y asignar) los principales riesgos que influyen en la consecución de los objetivos, para luego definir acciones de mitigación y seguimiento.

Monitoreo del riesgo: Verificación, supervisión, observación crítica o determinación continúa del estado del riesgo con el fin de identificar cambios del nivel de desempeño requerido o esperado de cada una de las etapas de administración, así como el nivel de cumplimiento y efectividad de los controles y acciones definidas.

Nivel del 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.

Probabilidad: Grado en el cual es probable que ocurra un evento.

Riesgo: Contingencia o incertidumbre ante eventos futuros que puedan influir positiva o negativamente en los resultados esperados. Se hace referencia al riesgo en términos del impacto de un evento en la consecución de los objetivos.

Riesgo de corrupción: Posibilidad de que, por acción u omisión, se use el poder para poder desviar la gestión de lo público hacia un beneficio privado[1]. **Riesgo Inherente**: Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto[2].

Riesgo de seguridad digital: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad que cause una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC27000)

Riesgo materializado: Es la ocurrencia de un evento que genera un impacto negativo, identificado o no previamente como un riesgo.

Riesgo residual: Es el nivel de riesgo que permanece luego de aplicar la efectividad de los controles al riesgo inherente.

Tratamiento del riesgo: Es el proceso para modificar el riesgo, el tratamiento del

[1] Definición tomada de la Guía para la administración del riesgo y el diseño de controles en entidades públicas elaborada por el DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA.
[2] Ibídem.

riesgo puede implicar: evitar el riesgo decidiendo no iniciar o continuar la actividad que lo causó; tomar o incrementar el riesgo para conseguir una oportunidad; suprimir la fuente del riesgo; cambiar la probabilidad; cambiar los efectos; compartir el riesgo con otra parte o partes o retener el riesgo mediante una decisión informada (ISO/IEC27000). En lo que respecta a los riesgos de corrupción se debe tener en cuenta que no procede la aceptación del riesgo.

Valoración del riesgo: Es la etapa en la cual se establece la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (riesgo inherente). Posteriormente, se confrontan los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (riesgo residual).

5. RESPONSABILIDAD FRENTE A LA GESTIÓN DEL RIESGO DE ACUERDO CON EL ESQUEMA DE LÍNEAS DE DEFENSA

El Modelo Integrado de Planeación y Gestión – MIPG, a través del Modelo Estándar de Control Interno (MECI) establece una estructura de control para la gestión institucional, siendo uno de los elementos fundamentales de esta estructura el esquema de responsabilidades de las líneas de defensa, el cual proporciona una manera efectiva para mejorar la gestión de los riesgos y los controles mediante la aclaración de las funciones y deberes.

En la siguiente tabla se explica la aplicación de los roles y responsabilidades del esquema de líneas de defensa para la FND:

5.1 Tabla 1. Responsabilidades de las líneas de defensa

LÍNEA DE DEFENSA	RESPONSABLE	RESPONSABILIDAD FRENTE A LA GESTIÓN DEL RIESGO
LÍNEA ESTRATÉGICA	• La Alta Dirección (Director Ejecutivo y su equipo directivo)	• Promover la administración de riesgos como un componente fundamental dentro de la operación de la FND.
	• El Comité Institucional de Coordinación de Control Interno.	• Analizar los riesgos y amenazas institucionales que puedan afectar el cumplimiento de los objetivos estratégicos, planes, programas, metas, compromisos de la FND y capacidades para prestar servicios, a partir de la información aportada por las instancias de 2ª línea identificadas.
	• Comité Institucional de Gestión y Desempeño	• Definir, aprobar y evaluar la Política de Administración del Riesgo de la Entidad. • Aprobar el nivel de aceptación del riesgo para la FND y asegurar que sea coherente con los objetivos estratégicos establecidos, el modelo de negocio y la capacidad de riesgo.
PRIMERA LÍNEA DE DEFENSA	• Líderes de procesos, programas y proyectos y sus equipos. • Los colaboradores de la FND en todos los niveles.	• Identificar, valorar, evaluar, controlar y mitigar los riesgos a través del autocontrol. • Establecer y revisar el contexto institucional (interno y externo), así como de definir las partes interesadas para su proceso. • Mantener efectivamente los controles internos y los controles del día a día. • Conocer y apropiar las políticas, procedimientos, tips, información entre otras herramientas para el autocontrol. • Identificar los riesgos de los procesos, programas y proyectos a su cargo, establecer los controles, hacer el seguimiento acorde con el diseño de los controles para evitar su materialización. • Asegurar que la construcción de los riesgos asociados al proceso se realice de forma participativa. • Realizar seguimiento de los riesgos del proceso a través del medio que el proceso de Gestión Integral Organizacional disponga para tal fin. • Informar las materializaciones de los riesgos a la Oficina de Planeación (segunda línea de defensa) y a la Oficina de Control Interno (tercera línea de defensa) Revisar las acciones y planes de mejoramiento establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces.

		• Evaluar con el equipo de trabajo la responsabilidad y resultados de la gestión del riesgo, así como las desviaciones según el nivel de aceptación del riesgo al interior de su dependencia y las acciones a seguir.
SEGUNDA LÍNEA DE DEFENSA	• Jefe de Oficina de Planeación • Responsable de temas transversales para la FND y que reporta ante el Representante Legal • Coordinador de Tecnología • Jefe de Contratación. • Secretaría General • Jefe de Talento Humano • Subdirectores y Jefes.	• Generar propuestas sobre la metodología y Políticas para la Administración del Riesgo de la FND y presentarlas para aprobación del Comité Institucional de Gestión y Desempeño. • Coordinar, liderar, capacitar y asesorar a la primera línea de defensa en la aplicación de la metodología y políticas desarrolladas. • Consolidar la gestión del riesgo y llevar ante la línea estratégica alertas sobre eventos y cambios en el entorno. • Consolidar el mapa de riesgos institucionales y socializarlo con las partes interesadas. • Asegurar que los controles y actividades de gestión del riesgo de la primera línea de defensa sean apropiados funcionen correctamente. • Acompañar la implementación de prácticas eficaces para la gestión de los riesgos y para el diseño e implementación de controles. • Evaluar y efectuar seguimiento a los controles aplicados. • Establecer el nivel del riesgo adecuado para la FND, consistente con los objetivos estratégicos y el modelo de negocio y presentar a las instancias correspondientes, cada vez que corresponda. • Evaluar el cumplimiento de los controles asociados a las políticas de seguridad de la información (Coordinación de Tecnología) • Monitorear la gestión contractual y generar alertas sobre retrasos, incumplimientos u otras situaciones de riesgo (Jefe de Contratación) • Realizar seguimiento a las PQRD generando alertas sobre incumplimientos, quejas en la prestación del servicio o tutelas (Secretaria General) • Monitorear temas claves relacionados con el Talento Humano (capacitación, bienestar, incentivos, convivencia laboral, código de integridad), generando alertas sobre incumplimientos, situaciones críticas que afectan el clima laboral y posibles afectaciones del código de integridad. (Jefe de Talento Humano) • Monitorear el Plan Estratégico de Tecnologías de Información PETI, generando alertas sobre retrasos, incumplimientos y otras situaciones de riesgos detectadas en materia de tecnología (Coordinador de Tecnología) • Monitoreo de 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	• Jefe de la Oficina de Control Interno	• Realizar seguimiento de manera independiente y objetiva al cumplimiento de los objetivos institucionales y de procesos, a través de la adecuada gestión de riesgos • En su rol de asesoría, realizar orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Oficina de planeación y desarrollo corporativo. • Asesorar a la alta dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos. • Informar los hallazgos sobre la gestión de riesgo y proporcionar recomendaciones de forma independiente. • Generar alertas sobre retrasos, incumplimientos u otras situaciones de riesgo detectadas, a partir de sus seguimientos y procesos de auditoría interna. • Formar a la alta dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos.

6. INSTITUCIONALIDAD

El modelo integrado de planeación y gestión (MIPG) define para su operación articulada la creación en todas las entidades del Comité Institucional de Gestión y Desempeño, regulado por el Decreto 1499 de 2017 y del Comité Institucional de Coordinación de Control Interno, reglamentado a través del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017, en este marco general, para una adecuada gestión del riesgo, dicha institucionalidad entra a funcionar de la siguiente forma:

- Comité Institucional de Gestión y Desempeño: Analiza la gestión del riesgo y se aplican las mejoras que considere pertinentes.
- Comité Institucional de Coordinación de Control Interno: Traslada el análisis de eventos y riesgos críticos.

7. NIVEL DE ACEPTACIÓN DEL RIESGO (APETITO DEL RIESGO)

El nivel de aceptación al riesgo es definido como el nivel de riesgo que la Entidad está dispuesta a asumir sin necesidad de establecer controles adicionales tendientes a disminuir su probabilidad de ocurrencia o su impacto.

Por su parte, el nivel de aceptación del riesgo debe ser adecuadamente comunicado en todos los niveles de la FND; esto con el fin de que sea considerado en el marco de la toma de decisiones.

Para el caso de la FND de acuerdo con sus estatutos, el contexto de sus actuaciones, su misionalidad y la naturaleza de los procesos que desarrolla ha definido el nivel de aceptación del riesgo de acuerdo con los siguientes criterios:

7.1. La FND tiene como objetivo mantener su riesgo residual "bajo" o "moderado", el cual le permitirá, mitigar la incertidumbre y de este modo generar condiciones que le permitan alcanzar el logro de sus objetivos.

7.2. Con respecto a la capacidad del riesgo, serán considerados los riesgos que se encuentren en la zona de riesgo residual "alto" o "extremo", y para los riesgos de corrupción y/o soborno, "alto", "extremo" y "moderado", esto implica que, a diferencia de lo anterior, se deberán ejecutar planes de mejoramiento que permitan mitigar, compartir o eliminar el riesgo, basados en la ejecución de actividades orientadas al fortalecimiento o generación de nuevos controles para contrarrestar los impactos que pueden suceder tras la materialización de un evento.

En la siguiente tabla se presentan los niveles de riesgo y los criterios de decisión para la aceptación de los riesgos de acuerdo con su nivel.

7.3 Tabla 2. Clasificación de niveles de riesgo

	Nivel del Riesgo Residual	Criterio de aceptación del riesgo
	Riesgo Extremo	El riesgo en este nivel no se acepta. En ninguna circunstancia la entidad deberá mantener un riesgo con este nivel, pues afecta el logro de los objetivos de la entidad. De identificarse deben establecerse medidas de intervención inmediatas para mitigación.
	Riesgo Alto	El riesgo en este nivel no se acepta. Es necesario que la entidad implemente acciones prioritarias a corto plazo para su mitigación, debido al alto impacto que tendría su materialización sobre el logro de los objetivos de la entidad.
	Riesgo Moderado	El riesgo en este nivel se tolera. Deberá evaluarse la pertinencia de implementar medidas de intervención sobre el riesgo para disminuir su calificación a una zona asumible.

	Riesgo Bajo	El riesgo en este nivel se acepta. El riesgo no presenta una gravedad significativa, por lo que no amerita la aplicación de acciones adicionales. El riesgo se debe gestionar mediante monitoreo periódico. Ningún riesgo de corrupción puede aceptarse

Fuente: Matriz institucional de riesgos FND

8. METODOLOGÍA PARA LA GESTIÓN DEL RIESGO

La FND ha definido la siguiente metodología para la gestión de los riesgos de la FND, tomando como insumo y adaptando los lineamientos establecidos por el Departamento Administrativo de la Función Pública -DAFP - en la Guía para Administración del Riesgo y Diseño de Controles. La metodología se desarrolla a través de las siguientes etapas:

- ✓ Establecimiento del contexto.
- ✓ Identificación del riesgo.
- ✓ Análisis del riesgo.
- ✓ Evaluación del riesgo.
- ✓ Tratamiento del riesgo.
- ✓ Monitoreo y revisión.

Nota: Para la gestión de los riesgos de seguridad y privacidad de la información y seguridad digital se debe consultar el anexo 1 de la presente política.

8.1. ESTABLECIMIENTO DEL CONTEXTO

Son las condiciones internas y externas, que pueden generar eventos de oportunidades o afectar negativamente el cumplimiento de la misión, visión, objetivos estratégicos y objetivos de los procesos de la FND. Definir el contexto institucional contribuye al autoconocimiento de la FND frente a la exposición al riesgo, ya que permite identificar las situaciones generadoras de riesgos.

El establecimiento del contexto permite a la FND articular los objetivos frente a las características del entorno interno y externo en el cual opera, los cuales deberán ser considerados posteriormente en la gestión del riesgo.

El contexto de la FND se determinó a partir del Plan Estratégico 2021-2025, por

medio de diferentes matrices, como la DOFA, la cual permite identificar los aspectos clave a considerar para definir el alcance de los objetivos y potencializar las fortalezas y oportunidades, así como también minimizar el riesgo asociado a las debilidades y amenazas; para lo cual se evaluó con el líder de cada proceso las fortalezas y debilidades en relación con las oportunidades y amenazas que ellos identifican en la operación. Adicionalmente, se elaboró una matriz PESTEL en la cual se analizaron los factores políticos, económicos, sociales, tecnológicos, ambientales y legales que podían afectar la organización, se identificaron las posibles amenazas y oportunidades y cuál sería su impacto en la FND. Se identificaron los principales grupos de interés o stakeholders, se elaboró una matriz MEFI (Matriz de evaluación de factores internos), una matriz MEFE (matriz de evaluación de factores externos) y la matriz MIME, en la cual se realiza la evaluación de los factores internos y externos.

El contexto institucional de la FND se revisará considerando los cambios administrativos que puedan afectar la operación. Esta revisión se realizará cada vez que se actualicen las matrices mencionadas anteriormente, como parte de la planeación estratégica de la FND. Este ejercicio será ejecutado por los líderes de proceso, quienes asegurarán la participación de sus equipos de trabajo, con el apoyo y dirección de la Dirección Ejecutiva y la Oficina de Planeación y Desarrollo Corporativo.

8.1.1. Factores de riesgo del proceso y establecimiento del contexto a nivel de procesos

Todos los procesos deberán estar debidamente documentados y actualizados; así las cosas, los siguientes son elementos mínimos que se deberán considerar y documentar en el establecimiento del contexto en cada uno de los procesos del mapa de procesos de la Federación Nacional de Departamentos.

Factores de riesgo del proceso	Descripción
Diseño del proceso	Claridad en la descripción del alcance (misión y visión). Objetivos estratégicos vinculados al proceso. Objetivo del proceso y características claves. Actividades clave utilizadas por el proceso para el

Factores de riesgo del proceso	Descripción
	cumplimiento del objetivo. Sistemas de información utilizados en la operación.
Interacciones con otros procesos	Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes. Proveedores o terceros que soportan el proceso.
Procedimientos asociados	Pertinencia en los procedimientos que desarrollan los procesos. Caracterización del proceso.
Responsable del proceso	Grado de autoridad y responsabilidad de los colaboradores frente al proceso. Estructura organizacional que soporta el proceso.
Comunicación entre los procesos	Efectividad en los flujos de información determinados en la interacción de los procesos, así como la toma de decisiones.

8.2. Establecimiento del contexto interno

Es el ambiente interno en el cual la FND busca alcanzar sus objetivos. Es importante que la administración del riesgo este alineada con la cultura, los procesos, la estructura y la estrategia de la FND. Para este análisis, realizado en el marco de la planeación estratégica, se tuvieron en cuenta los factores internos como las debilidades y fortalezas identificadas.

8.3. Establecimiento del contexto externo

Es el ambiente externo en el cual la FND busca alcanzar sus objetivos. Entenderlo es importante para garantizar que los objetivos y las precauciones de las partes interesadas externas se tomen en consideración en el momento de tomar decisiones.

Para el análisis de contexto externo, realizado en el marco de la planeación estratégica, se tuvieron en cuenta los factores externos como las oportunidades y amenazas.

9. IDENTIFICACIÓN DEL RIESGO

El proceso de identificación de riesgos en la FND es participativo y cuenta con el apoyo de la Oficina de Planeación y Desarrollo Corporativo. Su objetivo es analizar las actividades ejecutadas por el proceso e identificar los posibles riesgos asociados. Es fundamental realizar una identificación adecuada de los riesgos para garantizar un entendimiento claro por parte de todos los actores involucrados.

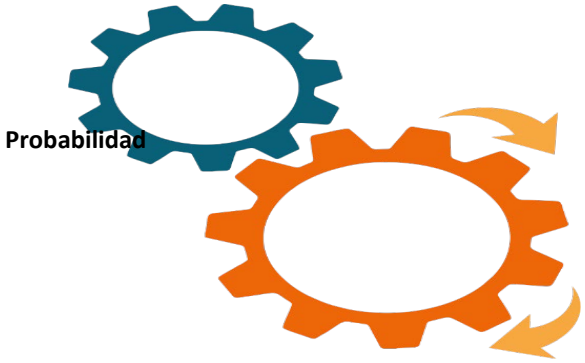
En este orden de ideas, para identificar un riesgo, es necesario realizar los siguientes pasos:

i. Revisar el objeto y alcance del proceso.
ii. Determinar las características o requisitos que deben cumplir los productos y/o servicios identificados.
iii. Revisar antecedentes del proceso.
iv. Determinar los riesgos (puntos de riesgos, áreas de impacto y áreas de factores de riesgo).
v. Describir del riesgo.
vi. Clasificar del riesgo.
vii. Describir de la posible materialización del riesgo.
viii. Identificar las causas del riesgo
ix. Identificar los efectos del riesgo.

El desarrollo estos pasos se encuentra en el procedimiento de Gestión y Administración del Riesgo.

10. CRITERIOS PARA EL ANÁLISIS Y EVALUACIÓN DEL RIESGO

La FND ha definido los criterios para el análisis y la evaluación de los riesgos en función de su tamaño, la naturaleza de las actividades misionales, los recursos que administra y las características de los procesos institucionales (estratégicos, misionales y de apoyo). Los criterios de análisis y evaluación permiten determinar de manera objetiva el nivel para cada riesgo identificado a través del establecimiento para criterios de probabilidad y criterios de impacto frente a los cuales los riesgos son evaluados por parte de los equipos de trabajo.



10.1. ANÁLISIS DEL RIESGO

Esta etapa busca establecer la probabilidad de ocurrencia e impacto de cada riesgo, calificándolos y evaluándolos para obtener información cuantitativa y cualitativa que permita establecer el nivel de riesgo inherente.

La forma en que deberá realizarse el cálculo de la probabilidad inherente de cada uno de los anteriores puntos se encuentra en el procedimiento de Gestión y Administración del Riesgo. En ese procedimiento la clasificación del riesgo inherente podrá variar dependiendo si se trata de un riesgo totalmente nuevo o si se trata de un riesgo previamente identificado.

10.1.1. Cálculo de la probabilidad inherente

La probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de un año.

La selección para clasificación de la probabilidad inherente se basará en la siguiente tabla:

10.1.1.1 Tabla de clasificación de la probabilidad

	Frecuencia de la actividad – Probabilidad	Nivel de exposición
Muy alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año y/o se materializó al menos una vez en los últimos 4 meses.	**5 – 100%**
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año y/ se materializó al menos una vez en los últimos 8 meses.	**4 – 80%**
Media	La actividad que conlleva el riesgo se ejecuta 24 a 499 veces por año y/o se materializó al menos una vez en los últimos 12 meses.	**3 – 60%**
Baja	La actividad que conlleva a que el riesgo se ejecuta de 3 a 23 veces por año y/o se materializó al menos una vez en los últimos 16 meses.	**2 – 40%**
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año y/o no se ha materializado en los últimos 24 meses.	**1 – 20%**

10.1.2. Clasificación del impacto inherente

Para identificar el impacto y asignarlo al riesgo, se debe ubicar en la siguiente tabla los efectos en la columna correspondiente al tipo de impacto y seleccionar el nivel que le represente el mayor impacto, especulando siempre en el peor escenario, en

caso de que el riesgo se llegase a materializar siendo el criterio suficiente para la selección.

10.1.2.1. Tabla de criterios para definir el nivel de impacto

		Económica	Reputacional
1 – 20%	**Leve/ insignificante**	Afectación menor a 10 SMLMV	El riesgo afecta la imagen de algún proceso de la FND.
2 – 40%	**Menor**	Entre 11 y 50 SMLMV	El riesgo afecta la imagen de la FND internamente, de conocimiento general nivel interno, de Consejo Directivo y Asamblea de Gobernadores y/o de proveedores.
3 – 60%	**Moderado**	Entre 51 y 100 SMLMV	El riesgo afecta la imagen de la FND frente algunos usuarios de relevancia de cara al logro de los objetivos.
4 – 80%	**Mayor**	Entre 101 y 500 SMLMV	El riesgo afecta la imagen de la FND con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental.
5 – 100%	**Catastrófico**	Mayor a 500 SMLMV	El riesgo afecta la imagen de la FND a nivel nacional, con efecto publicitario sostenido a nivel país.

10.1.2.2 Tabla de clasificación del impacto de riesgos de corrupción y soborno

	Clasificación del impacto	Nivel de Exposición
Catastrófico	El riesgo afecta la imagen de la FND a nivel nacional, con efecto publicitario sostenido a nivel país.	**5**
Mayor	El riesgo afecta la imagen de la FND con efecto publicitario sostenido a nivel de sector administrativo o nivel departamental.	**4**
Moderado	El riesgo afecta la imagen de la FND con algunos usuarios de relevancia frente al logro de los objetivos.	**3**

10.2 Medición del riesgo inherente

En este punto se busca determinar el resultado de la calificación según los criterios definidos anteriormente, los cuales establecen un grado de exposición al riesgo, de esta forma se define el riesgo inherente, para esto, se debe cruzar el resultado obtenido en la probabilidad e impacto y ubicarlo en la zona correspondiente obteniendo así el nivel de riesgo.

Es importante destacar, que se utilizará un solo mapa de calor para determinar la calificación de los diferentes tipos de riesgos, buscando la simplificación de la metodología, pero sin perder en ningún momento lo estricto de la evaluación en cada caso. Para los riesgos de corrupción y/o soborno en el análisis de impacto se realizará teniendo en cuenta los niveles “moderado”, “mayor” y “catastrófico”, dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los

niveles de impacto “menor” e “insignificante”.

10.3 Mapa de calor

A continuación, se presentan el mapa de las zonas de calor para los riesgos, los cuales muestran las zonas de calor en las que se puede ubicar un riesgo una vez calificado en cuanto a su probabilidad e impacto.

MATRIZ DE CALIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS					
Probabilidad	**Impacto**				
	Leve (1)	**Menor (2)**	**Moderado (3)**	**Mayor (4)**	**Catastrófico (5)**
MUY BAJA (1)	B	B	M	A	E
BAJA (2)	B	M	M	A	E
MEDIA (3)	M	M	M	A	E
ALTA (4)	M	M	A	A	E
MUY ALTA (5)	A	A	A	A	E

11. VALORACIÓN DE RIESGOS

Esta etapa busca establecer para cada riesgo, la probabilidad de ocurrencia e impacto de sus efectos, calificándolos y evaluándolos con el fin de obtener información cuantitativa y cualitativa para establecer el nivel de riesgo residual.

11.1 Identificación, diseño y valoración de controles

Los controles son las acciones orientadas a modificar el riesgo y que permiten determinar su tratamiento por parte de la entidad, puede ser minimizando la probabilidad de ocurrencia o el impacto del riesgo; la administración del riesgo contribuirá a la gestión de la FND en la medida en que los controles se identifiquen, documenten, apliquen y sean efectivos para prevenir o mitigar los riesgos. Es de este modo, previo a la determinación de la probabilidad e impacto del riesgo

residual, se deben listar los controles existentes para administrar el riesgo identificado; este ejercicio permite conocer los mecanismos con los que se cuenta para controlar el riesgo, todo lo anterior deberá ser acorde con las condiciones reales de operación.

Nota: El desarrollo de cómo se deberán identificar, diseñar y evaluar los controles se encuentran en el procedimiento de Gestión y Administración del Riesgo.

11.2 Medición del riesgo residual

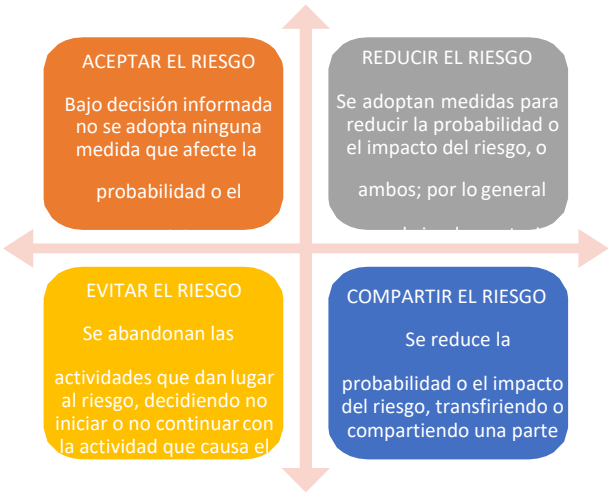
Dado lo anterior se procede, partiendo del resultado de la determinación del riesgo inherente y la calificación de los controles a modificar la calificación en el mapa de riesgo inherente según lo determinado en el procedimiento de Gestión y Administración del Riesgo.

Para la calificación del riesgo residual se utilizarán las mismas tablas de calificación de probabilidad e impacto mencionadas previamente en el riesgo inherente en la presente política, así como el mismo mapa de calor.

12. TRATAMIENTO DEL RIESGO

El tratamiento del riesgo se define como las medidas que toma la entidad para prevenir, mitigar, transferir o eliminar el riesgo de acuerdo con las posibilidades de gestión, capacidades de recursos y la naturaleza del riesgo. Las opciones de tratamiento adaptadas a la FND según la Guía para Administración del Riesgo y Diseño de Controles, del DAFP, se muestran en la siguiente figura.

Figura: Opciones de tratamiento de riesgo



Fuente: Guía Administración del riesgos - DAFP

El tratamiento del riesgo incluye el diseño y ejecución de las actividades de control que tienen como objetivo prevenir, detectar o mitigar la materialización del riesgo.

13. MONITOREO Y REVISIÓN

En esta fase se debe verificar el continuo estado del riesgo (todas las clases) con el fin de identificar cambios a nivel de desempeño requerido o esperado de cada una de las etapas de administración, así como el nivel de cumplimiento y efectividad de los controles con una periodicidad de ejecución cuatrimestral (día 30 del mes de abril y día 31 de los meses de agosto y diciembre).

El desarrollo de los criterios y aspectos clave para monitorear el riesgo se encuentran en el procedimiento de Gestión y Administración del Riesgo.

14. MAPA DE RIESGOS

Como producto de la aplicación de la metodología anterior se obtendrán los mapas de riesgo. El mapa de riesgos es la consolidación de la información generada a lo largo de las etapas de administración de riesgos, dentro de esta consolidación se destacan cuatro mapas fundamentales:

14.1 Mapa de riesgos de gestión

Este mapa construye aquellos riesgos que fueron clasificados dentro de la etapa de identificación general como “Riesgos de Gestión”.

14.2 Mapa de riesgos de corrupción

Este mapa construye aquellos riesgos que fueron clasificados dentro de la etapa de identificación general como “Riesgos de Corrupción”.

14.3 Mapa de riesgos de soborno

Este mapa construye aquellos riesgos que fueron clasificados dentro de la etapa de identificación general como “Riesgos de soborno”.

14.4 Mapa de riesgos consolidado

Integra la totalidad de los riesgos de la Entidad.

DIDIER ~~TAVERA AMADO~~
Director Ejecutivo

Elaboró: **Oficina de Planeación**
Revisó: Dar. Lina Zapata Bueno
Secretaria Privada Dirección Ejecutiva
Aprobó: Comité de Gestión y Desempeño.
Sesión No. 2 del 22 de agosto de 2025

15. CONTROL DE CAMBIOS

No. Versión	Ítem del cambio	Motivo del cambio	Fecha del cambio
1	Versión inicial de documento		20/12/2022
2	1. Objetivo 2. Alcance 3. Definición 4. Responsabilidad 5. Institucionalidad 6. Nivel de aceptación del riesgo 8. Establecimiento del contexto. 9. Criterios de identificación del riesgo. 11. Análisis del riesgo 12. Valoración de los riesgos 14. Monitoreo y revisión 15. Mapa de riesgos	1. Se amplía el objeto de la política incorporando también los riesgos de corrupción, soborno y seguridad de la información. Se amplía la redacción del objetivo. 2. Se amplía la incorporando los riesgos de corrupción, soborno y seguridad de la información. 3. Se incorpora la definición de amenazas, apetito del riesgo, causa, causa raíz, control correctivo, control preventivo, efecto, identificación del riesgo, monitoreo del riesgo, riesgo inherente, riesgo residual, tratamiento de riesgo, valoración del riesgo. 4. Se complementan las responsabilidades de cada una de las líneas de defensa. 5. Se incorpora un numeral para definir la institucionalidad del tema de riesgos en cabeza del comité institucional de gestión y desempeño y el Comité de Coordinación de Control Interno. 6. Se incorpora lo correspondiente al novel de aceptación del riesgo para los riesgos de corrupción y soborno. 8. Se incorpora lo relacionado con el establecimiento del contexto. 9. Se incorpora lo relacionado con los criterios para la identificación del riesgo. 11. Se incluye un numeral relacionado con el análisis del riesgo. 12. Se ajusta el texto en este numeral. 14. Se incorpora numeral de monitoreo y revisión. 15. Se incorpora numeral de mapas de riesgos.	02/11/2023
3	5. 5.1 Tabla 1. Responsabilidades de las líneas de defensa.	5. Se ajustan las responsabilidades de la segunda y tercera línea conforme a preguntas de FURAG. Se ajustan responsabilidades, dividiendo la primera línea estratégica.	22/08/2025

	7. Nivel de aceptación del riesgo	7. - Se modifica el nivel de aceptación del riesgo, tolerando el nivel de riesgo Moderado para loa riesgos de gestión. - En cuanto a los riesgos de seguridad digital se tolera la clasificación de riesgos Moderada, tal como lo contempla el anexo de la presente política. Conforme a lo anterior, se suprime la Expresión (…) Seguridad Digital (…) de este numeral.	
	8. Metodología para la Gestión del Riesgo	8. Se incluye nota dentro del numeral para la gestión de los riesgos de seguridad y privacidad de la información y seguridad digital, para la cual, se debe consultar el anexo 1 de la presente política.	
	12. 12.1.1 Tabla de clasificación de la probabilidad 13. Anexo Se realizan cambios de forma general del documento.	12. Se ajusta conforme a la tabla de la guía de administración de riesgos de la Función pública. 13. Se adiciona anexo relacionado con la gestión de riesgos de seguridad y privacidad de la información y de seguridad digital. Se modifican por cambios en la ortografía y redacción.	

16. CUADRO DE APROBACIONES

Elaboró: Colaboradores proceso GIO Oficina Asesora de Planeación **Fecha:** 18/05/2023	**Revisó:** Lideres de proceso **Fecha:** 04/07/2023 **Revisó**: Colaborador SIG/Oficina de Planeación **Fecha:** 22/08/2025	**Aprobó:** Comité de Gestión y Desempeño **Fecha:** 31/07/2023

ANEXO PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y DE SEGURIDAD DÍGITAL

En el contexto actual de transformación digital y constante evolución tecnológica, la seguridad de la información y la privacidad se han convertido en pilares fundamentales para la sostenibilidad y la reputación de cualquier organización. La Federación Nacional de Departamentos, comprometida con la protección de los datos y la integridad de sus sistemas de información, reconoce la necesidad de identificar, evaluar y mitigar los riesgos asociados con la seguridad y privacidad de la información, así como con la seguridad digital.

Este anexo tiene como objetivo proporcionar una visión integral de los riesgos de seguridad y privacidad de la información, y de seguridad digital a los que la organización está expuesta. Se describen las amenazas potenciales, las vulnerabilidades inherentes a nuestros sistemas y procesos, y las posibles consecuencias de no gestionar adecuadamente estos riesgos. Además, se establecen las medidas de control y mitigación necesarias para minimizar el impacto de estos riesgos en nuestras operaciones.

El enfoque adoptado en este anexo está alineado con las mejores prácticas y estándares internacionales, tales como ISO/IEC 27001:2022, garantizando un marco robusto para la gestión de riesgos de seguridad y privacidad de la información. Se busca no solo cumplir con las obligaciones legales y reglamentarias aplicables, sino también fomentar una cultura organizacional orientada a la seguridad y protección de la información.

A lo largo de este documento, se detallarán las diferentes categorías de riesgos, se proporcionarán ejemplos de escenarios de riesgo, y se presentarán las estrategias de mitigación recomendadas. Al hacerlo, pretendemos equipar a nuestros colaboradores con el conocimiento y las herramientas necesarias para identificar y abordar los riesgos de manera proactiva, asegurando así la resiliencia y continuidad de nuestras operaciones.

En la Federación Nacional de Departamentos se busca reducir todos los riesgos en la medida de lo posible y someter a tratamiento todas aquellas conductas, operaciones y/o actividades que obtengan una evaluación de riesgo residual (riesgo final evaluado) superior a **MODERADA.** Pese a lo anterior, si el proceso lo estima conveniente se puede realizar tratamiento a los riesgos residuales con calificación moderada.

El adecuado manejo de los riesgos por activos de información favorece el desarrollo y crecimiento de la Federación Nacional de Departamentos. Con el fin de asegurar dicho manejo es importante que se establezca en la organización, la identificación, análisis, valoración y definición de las alternativas de acciones de mitigación de los riesgos, esto en desarrollo de los siguientes elementos:

- Identificación de Activos

- Identificación del riesgo del Activo
- Identificación de Amenazas y Vulnerabilidades
- Clasificación y Valoración del Riesgo
- Selección del Mecanismo de Control
- Administración de riesgos

A continuación, se detallan cada una de las etapas usadas como metodología para el análisis y evaluación de riesgo por activos:

Identificación de Activos

El primer paso en la apreciación de riesgos es la identificación de todos los activos dentro del alcance del Sistema de Gestión de Seguridad de la Información, sus dependencias directas, su ubicación, los servicios o procesos en los que están implicados, y el propietario del riesgo. El registro de inventario de activos sirve como base para el análisis y evaluación de riesgos, además de ser necesario para controlar los recursos implicados en el alcance del sistema.

Se entiende por activo cualquier recurso o elemento que tiene valor para la organización, tales como aplicaciones, servicios web, redes, hardware, información física o digital, recurso humano, entre otros.

Identificación del Riesgo del Activo

El riesgo es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. La Federación Nacional de Departamentos, analiza y examina los riesgos teniendo en cuenta los tres (3) principios fundamentales de seguridad de la información para asegurar la confidencialidad, integridad y disponibilidad.

- **Confidencialidad:** Asegurar que la información sea accesible solo para aquellos autorizados a tener acceso.
- **Integridad:** Salvaguardar la exactitud y completitud de la información y los métodos de procesamiento.
- **Disponibilidad:** Asegurar que los usuarios autorizados tengan acceso a la información y a los activos asociados cuando lo requieran.

Cada proceso dentro de la organización debe identificar los activos que tiene a cargo e identificar el o los tipos de riesgos (Pérdida de Integridad, Pérdida de Confidencialidad y/o Pérdida de Disponibilidad) asociados para cada uno de los activos, indicando una breve descripción del riesgo identificado, por ejemplo:

Activo	Tipo de Riesgo	Descripción del Riesgo

Base de Datos de la Nómina.	Pérdida de la Integridad	La falta de políticas de seguridad digital, ausencia de políticas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada, lo cual causaría la pérdida de la integridad de la base de datos de nómina.

Identificación de Amenazas y Vulnerabilidades

Para cada riesgo asociado al activo de información se deben incluir las posibles amenazas y vulnerabilidades que podrían causar su materialización. Para tal efecto se dispondrá de un formato para la evaluación y análisis de riesgos por activos, en donde se detalle el listado de las amenazas comunes, amenazas dirigidas por el hombre y vulnerabilidades frente a los riesgos y activo del proceso teniendo como referencia el catálogo de amenazas y vulnerabilidades comunes indicados en el anexo "Lineamientos para la gestión del riesgo de seguridad digital en entidades públicas", el cual hace parte de la “Guía para la Administración del Riesgo y el diseño de controles en entidades públicas” expedida por el DAFP.

Cada proceso dentro de la organización debe identificar las amenazas, vulnerabilidades y consecuencias asociadas a los riesgos identificados para cada activo que tiene a cargo.

Clasificación del Riesgo

Teniendo como referencia la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas emitida por el DAFP, los riesgos identificados se clasifican en las siguientes categorías:

Daños a activos fijos/eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.
Ejecución y Administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fallas tecnológicas	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.

Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.

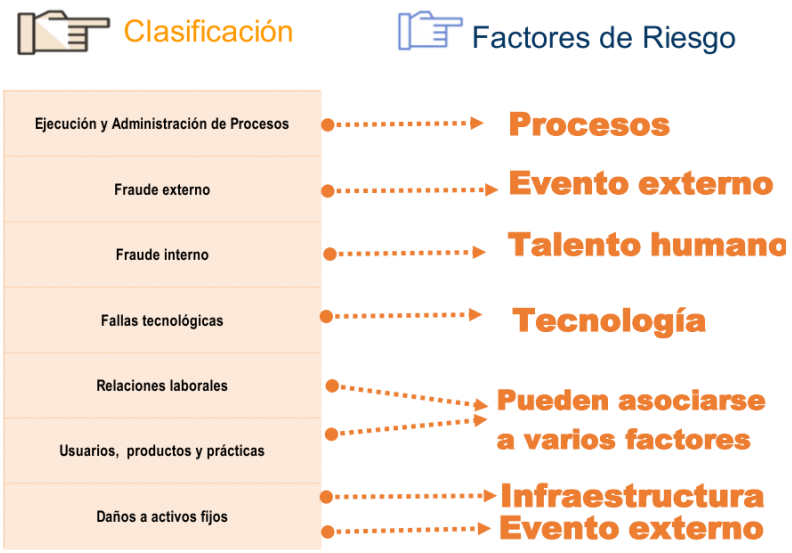


Gráfico 1. Relación entre factores de riesgo y clasificación del riesgo. Tomado como referencia de la guía administración del Riesgo V.6 DAFP

Valoración del del Riesgo Inherente

La probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo (Actividades en las que potencialmente se genera riesgo) en el periodo de 1 año.

La **Probabilidad**, corresponde con la estimación en términos escalares de las frecuencias con las que se ejecutan las actividades que conllevan el riesgo, los cuales se clasifican según los criterios que se definen a continuación:

Criterios para definir el nivel de probabilidad		
Escala	**Frecuencia de la Actividad**	**Probabilidad**
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva a que el riesgo se ejecuta de 3 a 23 veces por año.	40%
Media	La actividad que conlleva el riesgo se ejecuta 24 a 499 veces por año.	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año.	100%

El **Impacto**, corresponde con la estimación en términos escalares de las afectaciones a nivel reputacional y/o económicas que puede tener la Federación Nacional de Departamentos, las cuales se clasifican según los criterios que se definen a continuación:

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto, así, por ejemplo: para un riesgo identificado se define un impacto o económico en nivel insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado.

Criterios para definir el nivel de impacto		
Escala	**Reputacional**	**Afectación Económica**
Leve / Insignificante	El riesgo afecta la imagen de algún área de la organización.	Afectación menor a 2 SMLMV.
Menor	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.	Entre 2 y 5 SMLMV

Criterios para definir el nivel de impacto		
Escala	**Reputacional**	**Afectación Económica**
Moderado	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.	Entre 5 y 10 SMLMV
Mayor	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.	Entre 10 y 50 SMLMV
Catastrófico	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país	Mayor a 50 SMLMV

A partir del análisis de la probabilidad de ocurrencia del riesgo e impacto, se realiza la valoración de la zona de riesgo **INHERENTE**, la cual consiste en determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto, tomando como referencia 4 zonas de severidad en la matriz de calor que se detalla a continuación:

Probabilidad	**Impacto**				
	Leve (1)	**Menor (2)**	**Moderado (3)**	**Mayor (4)**	**Catastrófico (5)**
Muy Alta (5)	**Alta**	**Alta**	**Extrema**	**Extrema**	**Extrema**
Alta (4)	**Moderada**	**Alta**	**Alta**	**Extrema**	**Extrema**
Media (3)	**Baja**	**Moderada**	**Alta**	**Extrema**	**Extrema**
Baja (2)	**Baja**	**Baja**	**Moderada**	**Alta**	**Extrema**
Muy Baja (1)	**Baja**	**Baja**	**Moderada**	**Alta**	**Alta**

Identificación de Controles

Una vez obtenido el Riesgo Inherente, se deben definir los mecanismos de control con los que se están mitigando/tratando los riesgos identificados y valorados inicialmente. Para lo cual, se deben seleccionar aquellas medidas definidas mediante actividades de control establecidas en los anexos de la ISO 27001:2022.

Los controles pueden ser:

- Preventivos (mitigan la probabilidad del riesgo)

- Correctivos y detectivos (mitigan el impacto de la materialización del riesgo)

La totalidad de las causas identificadas deben ser mitigadas a través de los controles, los cuales deberán ser tomadas de la base de controles de la ISO 27001:2022, Anexo A. Cada control debe ser analizado para determinar su solidez. Se debe incluir una breve descripción de la aplicación del control al interior del proceso. Para una adecuada redacción de la descripción del control, se deberá tener en cuenta lo definido en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas del DAFP.

Valoración del Control y Relación del control respecto de los atributos informativos.

Un control se define como la medida que permite reducir o mitigar el riesgo, por lo cual, para la valoración de controles se debe tener en cuenta que:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

A través del ciclo de los procesos es posible establecer cuándo se activa y ejecuta un control, y de esta forma establecer su tipología. Para lo anterior, se debe tener en cuenta lo definido en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas del DAFP, respecto a las 3 fases globales del ciclo de un proceso.

Valoración del Riesgo Residual.

La valoración del riesgo residual es el resultado de aplicar la efectividad de los controles al riesgo inherente. La aplicación de los controles mitiga el riesgo de forma acumulativa. Para la calificación del riesgo residual se utilizarán las mismas tablas de calificación de probabilidad e impacto mencionadas previamente en el riesgo inherente, así como el mismo mapa de calor, según lo definido en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas del DAFP.

Apetito del riesgo

Teniendo en cuenta lo indicado en la política de administración de riesgos, en donde se detalla que el nivel de aceptación al riesgo es definido como el nivel de riesgo que la Entidad está dispuesta a asumir sin necesidad de establecer controles adicionales tendientes a disminuir su probabilidad de ocurrencia o su impacto y que el nivel de aceptación del riesgo debe ser adecuadamente comunicado en todos los niveles de la FND, serán considerados los riesgos que se encuentren en la zona de riesgo residual “alto” o “extremo”, para los riesgos de seguridad de la información y

seguridad digital, implicando que, se elaboren y ejecuten planes de mejoramiento que permitan mitigar, compartir o eliminar el riesgo, basados en la ejecución de actividades orientadas al fortalecimiento o generación de nuevos controles para contrarrestar los impactos que pueden suceder tras la materialización de un evento.

	Nivel del Riesgo Residual	Criterio de aceptación del riesgo
	Riesgo Extremo	El riesgo en este nivel no se acepta. En ninguna circunstancia la entidad deberá mantener un riesgo con este nivel, pues afecta el logro de los objetivos de la entidad. De identificarse deben establecerse medidas de intervención inmediatas para mitigación.
	Riesgo Alto	El riesgo en este nivel no se acepta. Es necesario que la entidad implemente acciones prioritarias a corto plazo para su mitigación, debido al alto impacto que tendría su materialización sobre el logro de los objetivos de la entidad.
	Riesgo Moderado	El riesgo en este nivel se acepta. Sin embargo, si el proceso lo considera pertinente, podrá implementar acciones a corto plazo para su mitigación, teniendo en cuenta el impacto que podría tener su materialización sobre el logro de los objetivos de la entidad.
	Riesgo Bajo	El riesgo en este nivel se acepta. El riesgo no presenta una gravedad significativa, por lo que no amerita la aplicación de acciones adicionales. El riesgo se debe gestionar mediante monitoreo periódico. Ningún riesgo de corrupción puede aceptarse

Tratamiento del Riesgo (Plan de Acción)

Para los riesgos cuyo resultado de la evaluación del riesgo residual sea diferente de bajo o Moderado una vez implementados los controles (Anexo de la ISO 27001:2022), se debe definir planes de acción con el objetivo de mitigarlos, centrando la atención y recursos en estos.

Los riesgos evaluados como bajos y Moderados se consideran aceptables por parte de la FND, teniendo en cuenta la situación y contexto actual y los recursos disponibles. Sin embargo, si el proceso lo estima conveniente puede realizar tratamiento a los riesgos residuales con calificación moderada

Las acciones sobre los riesgos objetivo de tratamiento deberán incluir acciones como, implementación de nuevos controles, revisión y mejora de la efectividad de los controles existentes, eliminación del riesgo mediante la decisión de la modificación de la naturaleza de la actividad/proceso que origina el riesgo o cesando la misma.

A partir de los resultados del riesgo intrínseco, se decide qué medidas son necesarias para reducir, en lo posible el riesgo de los activos. El responsable del sistema junto con la Coordinación de Tecnología y Planeación, serán los responsables de asegurar la implantación de las contramedidas, las cuales puede consistir en i) reducir el riesgo, ii) transferir el riesgo a terceros, iii) eliminar los activos o procesos involucrados en dicho riesgo, iv) asumir el riesgo.

El establecimiento de las medidas puede verse condicionado por el coste de las medidas, el impacto, su dificultad de implantación y el mantenimiento.

El tratamiento del riesgo deberá realizarse a partir de lo determinado en el numeral 12 de la política de administración del riesgo y de la ejecución de actividades que surjan como resultado de los procedimientos definidos desde la Coordinación de Tecnología.

Ejecución del tratamiento del riesgo.

Los responsables de la mejora o implementación de los planes deberán realizar las acciones de tratamiento de acuerdo con lo formulado. La Coordinación de Tecnología junto con la Oficina Asesora de Planeación y Desarrollo Corporativo son los responsables de hacer seguimiento a la implementación de los planes.

Materialización del riesgo

La materialización de los riesgos de Seguridad y Privacidad de la información y Seguridad Digital serán identificados a partir de un registro o reporte de un incidente de seguridad registrado a través de la mesa de ayuda de la FND.