****

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

INSTITUTO NACIONAL PARA CIEGOS

Versión 2

2020

BOGOTÁ, D.C.

**Contenido**

[Introducción 3](#_Toc47466064)

[Objetivo 3](#_Toc47466065)

[Alcance 3](#_Toc47466066)

[METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO 4](#_Toc47466067)

[**1.** **ESTABLECIMIENTO DEL CONTEXTO**: 4](#_Toc47466068)

[**1.1 Contexto Externo:** 5](#_Toc47466069)

[**1.2. Contexto Interno:** 5](#_Toc47466070)

[**1.3. Contexto del proceso:** 5](#_Toc47466071)

[**2.** **IDENTIFICACIÓN DE RIESGOS:** 6](#_Toc47466072)

[**2.1 Tipos de Riesgo** 6](#_Toc47466073)

[**2.2. Identificación de las Causas** 7](#_Toc47466074)

[**2.3. Consecuencias** 8](#_Toc47466075)

[**3.** **VALORACIÓN DE LOS RIESGOS:** 8](#_Toc47466076)

[**3.1. Análisis del riesgo Inherente** 8](#_Toc47466077)

[**3.2.** **Evaluación de Riesgos** 13](#_Toc47466078)

[**4.** **TRATAMIENTO DEL RIESGO** 17](#_Toc47466079)

[**4.1. Niveles de aceptación del riesgo:** 17](#_Toc47466080)

[**4.2. Acciones asociadas a los controles:** 18](#_Toc47466081)

[**5.** **MONITOREO Y REVISIÓN** 18](#_Toc47466082)

[**6.** **ROLES DE LAS LÍNEAS DE DEFENSA EN LA GESTIÓN DEL RIESGO** 18](#_Toc47466083)

[**6.1. ESTRATÉGICA**: 18](#_Toc47466084)

[**6.2. PRIMERA LÍNEA** 19](#_Toc47466085)

[**6.3** **SEGUNDA LÍNEA** 19](#_Toc47466086)

[**6.4. TERCERA LÍNEA** 20](#_Toc47466087)

[**7.** **ACCIONAR ANTE LOS RIESGOS MATERIALIZADOS** 21](#_Toc47466088)

[**8.** **ELIMINACIÓN RIESGOS IDENTIFICADOS** 22](#_Toc47466089)

[**REFERENCIAS** 23](#_Toc47466090)

# Introducción

El Instituto Nacional para Ciegos, establece su política de administración del riesgo tomando como referente los parámetros del Modelo Integrado de Planeación y Gestión en los procesos, así como los del Modelo Estándar de Control Interno, en lo referente a las líneas de defensa y los lineamientos de la Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública de Octubre de 2018[[1]](#footnote-1), la cual articula los riesgos de gestión, corrupción y de seguridad digital.

El presente documento establece los lineamientos que permitan la identificación, el análisis, la valoración, tratamiento y monitoreo de los riesgos que pudieran afectar la misión y el cumplimiento de los objetivos institucionales en el marco de los proyectos, planes y procesos del INCI a través de:

* La identificación y documentación de riesgos de gestión, corrupción y seguridad digital.
* El establecimiento de controles y acciones preventivas para los riesgos identificados
* La actuación correctiva y oportuna ante la materialización de los riesgos identificados.

# Objetivo

Establecer el marco general de actuación para la gestión de los riesgos a los que puede enfrentarse el Instituto Nacional para Ciegos en el desarrollo de sus acciones, a través de los lineamientos establecidos para la identificación, análisis, evaluación, tratamiento y monitoreo de los riesgos que puedan afectar la gestión y el cumplimiento de los objetivos de la institución.

# Alcance

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

# METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO

## **ESTABLECIMIENTO DEL CONTEXTO**:

Para realizar la identificación de los riesgos que puedan afectar el cumplimiento de los objetivos institucionales, se debe iniciar analizando el contexto de cada uno de los procesos del Sistema Integrado de Gestión. Para ello, debe analizar el contexto interno, externo y el del mismo proceso, ya que a partir de los factores que se definan es posible establecer las causas de los riesgos a identificar.

Para ello, debe diligenciar la matriz DOFA que se encuentra en la hoja Número 1 denominada Análisis de Contexto del formato “Mapa de Riesgos Institucional” la cual contiene la siguiente información:

Nombre del proceso

Objetivo del proceso:

Fecha de elaboración:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CONTEXTO EXTERNO** | **OPORTUNIDAD** | **AMENAZA** |  | **Estrategias DO** | **Estrategias FA** | **Estrategias FO** |
| Político |  |  |  |  |  |  |
| Económico y financiero |  |  |  |  |  |  |
| Social Cultural |  |  |  |  |  |  |
| Tecnológico |  |  |  |  |  |  |
| Ambiental |  |  |  |  |  |  |
| Legal y Reglamentario |  |  |  |  |  |  |
| **CONTEXTO INTERNO** | **DEBILIDAD** | **FORTALEZA** |  |  |  |  |
| Financiero |  |  |  |  |  |  |
| Personal |  |  |  |  |  |  |
| Procesos |  |  |  |  |  |  |
| Tecnología |  |  |  |  |  |  |
| Estratégico |  |  |  |  |  |  |
| Comunicación Interna |  |  |  |  |  |  |
| **CONTEXTO DEL PROCESO** | **DEBILIDAD** | **FORTALEZA** |  |  |  |  |
| Diseño del Proceso |  |  |  |  |  |  |
| Interacción con otros procesos |  |  |  |  |  |  |
| Transversalidad |  |  |  |  |  |  |
| Procedimientos Asociados |  |  |  |  |  |  |
| Responsables del Proceso |  |  |  |  |  |  |
| Comunicación Entre Procesos |  |  |  |  |  |  |
| Activos de Seguridad Digital del Proceso |  |  |  |  |  |  |

### **1.1 Contexto Externo:**

Se determinan las características o aspectos esenciales del entorno en el cual opera la entidad. Se pueden considerar los siguientes:

* Factores políticos: cambios de gobierno, legislación y políticas públicas.
* Económicos y financieros: disponibilidad de recursos.
* Sociales y Culturales: demografía, responsabilidad social, orden público
* Tecnológicos: avances en tecnología, acceso a sistemas de información externos, gobierno digital
* Ambientales: emisiones y residuos, energía, catástrofes naturales
* Legales y reglamentarios: leyes, decretos, ordenanzas y acuerdos

### **1.2. Contexto Interno:**

Se determinan las características o aspectos esenciales del ambiente en el cual la entidad busca alcanzar sus objetivos. Se pueden considerar los siguientes factores:

* Financieros: presupuesto de funcionamiento y recursos de inversión.
* Personal: competencia y disponibilidad del personal, seguridad y salud ocupacional.
* Procesos: capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.
* Tecnología: integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.
* Estratégicos: direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.
* Comunicación Interna: canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.

### 

### **1.3. Contexto del proceso:**

Se determinan las características o aspectos esenciales del proceso y sus interrelaciones. Se pueden los siguientes factores:

* Diseño del proceso: claridad en la descripción del alcance y objetivo del proceso.
* Interacciones con otros procesos: relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.
* Transversalidad: procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad.
* Procedimientos asociados: pertinencia en los procedimientos que desarrollan los procesos.
* Responsables del proceso: grado de autoridad y responsabilidad de los funcionarios frente al proceso.
* Comunicación entre los procesos: efectividad en los flujos de información determinados en la interacción de los procesos.
* Activos de seguridad digital del proceso: información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano.

## **IDENTIFICACIÓN DE RIESGOS:**

Una vez se analiza el contexto de la entidad se procede a la identificación de los riesgos que pueden afectar el cumplimiento de los objetivos.

Para el registro de esta información se utilizará la hoja número dos del formato “Mapa de Riesgos Institucional” Hoja “Matriz riesgos gestión o “matriz Riegos Corrupción”, en la cual se inicia diligenciando el nombre del proceso y su objetivo.

A continuación se sugieren algunas preguntas claves para la identificación del riesgo:

* Qué puede suceder? Identificar la afectación del cumplimiento del objetivo estratégico o del proceso según sea el caso.
* ¿Cómo puede suceder? Establecer las causas a partir de los factores determinados en el contexto.
* ¿Cuándo puede suceder? Determinar de acuerdo con el desarrollo del proceso.
* ¿Qué consecuencias tendría su materialización? Determinar los posibles efectos por la materialización del riesgo.

Para la redacción de los riesgos evite iniciar con palabras negativas como: “No…”, “Que no…”, o con palabras que denoten un factor de riesgo (causa) tales como: “ausencia de”, “falta de”, “poco(a)”, “escaso(a)”, “insuficiente”, “deficiente”, “debilidades en…”

Si el objetivo del proceso es “Adquirir con oportunidad y calidad bienes y servicios para la entidad” un riesgo puede ser: “Inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad”.´

Una vez identifique el riesgo, defina el tipo de riesgo, lo cual depende de la misión de cada entidad, de las normas que regulan su operación y de los sistemas de gestión que implemente, entre otros aspectos.

### **2.1 Tipos de Riesgo**

#### **Riesgos de Corrupción:**

Cuando por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia, del Estado, para la obtención de un beneficio particular. Los riesgos de corrupción, siempre deben gestionarse.

#### **Tecnológicos y de seguridad digital:**

Son los relacionados con la vulnerabilidad de la capacidad tecnológica para satisfacer las necesidades actuales y futuras y el cumplimiento de la misión de la entidad. Para profundizar consultar el ANEXO 4 de la Guía de Administración del Riesgo del DAFP; “LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS” 2018

#### **Riesgos de gestión:**

Este tipo de riesgos pueden clasificarse así:

* Calidad: relacionados con los atributos de calidad establecidos en MIPG, las políticas de aseguramiento y control de calidad.
* Contractual: relacionado con los atrasos o incumplimientos de las etapas contractuales en cada vigencia.
* Comunicación: relacionado con los canales, medios y oportunidades para informar durante las diferentes etapas de un proyecto.
* Cumplimiento y conformidad: se asocian con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
* Estratégicos: asociado a la administración de la Entidad, a la misión y el cumplimiento de los objetivos estratégicos, la definición de políticas, y el diseño de lineamientos que respondan a las necesidades de los grupos de valor e interés
* Financieros: relacionado con el manejo de recursos, la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo de los bienes.
* Imagen: relacionado con la percepción y la confianza por parte de los grupos de valor frente a la Entidad
* Información: se asocia a la disponibilidad, confiabilidad e integridad de la información agregada y desagregada
* Integración: Se refiere a la integración de sistemas, áreas, entidades, etapas y elementos que se requieran coordinar para el desarrollo de un proyecto
* Operativos: riesgos provenientes del funcionamiento y operatividad de los procesos, sistemas de información, estructura de la entidad y articulación entre dependencias.
* Recurso Humano**:** Se asocia a la cualificación, competencia y disponibilidad de personal requerido para realizar un proyecto o función.

### **2.2. Identificación de las Causas**

Son las circunstancias, situaciones, factores internos o externos que generan que las probabilidades que el riesgo se presente aumenten y que solo o en combinación con otro, pueden producir su materialización.

### **2.3. Consecuencias**

Son las repercusiones que podrían generar los riesgos en caso de que ocurrieran, así como son los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas

*Luego de haber identificado el riesgo, sus causas y consecuencias es necesario verificar la consistencia entre estos. Es importante cuestionar la coherencia de las relaciones de causalidad, por lo cual es necesario preguntarse si la existencia de las causas permite que el riesgo identificado se materialice.*

## **VALORACIÓN DE LOS RIESGOS:**

Consiste en establecer 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). A continuación se detallan los elementos que lo desarrollan:

### **3.1. Análisis del riesgo Inherente**

#### **3.1.1. Calificación de la probabilidad**

Para identificar la ocurrencia del riesgo se debe calificar la probabilidad, la cual puede ser medida con criterios de: frecuencia, es decir el número de eventos en un período determinado; o factibilidad, se trata en este caso de un hecho que no se ha presentado pero es posible que se dé. Por lo anterior se definen los siguientes criterios para calificar el riesgo:

| NIVEL | DESCRIPTOR | DESCRIPCIÓN | FRECUENCIA |
| --- | --- | --- | --- |
| 5 | Casi seguro | Se espera que el evento ocurra en la mayoría de las circunstancias | Más de 1 vez al año. |
| 4 | Probable | Es viable que el evento ocurra en la mayoría de las circunstancias | Al menos 1 vez en el último año. |
| 3 | Posible | El evento podrá ocurrir en algún momento | Al menos 1 vez en los últimos 2 años. |
| 2 | Improbable | El evento puede ocurrir en algún momento | Al menos 1 vez en los últimos 5 años. |
| 1 | Rara vez | El evento puede ocurrir sólo en circunstancias excepcionales (poco comunes o anormales) | No se ha presentado en los últimos 5 años. |

#### Fuente: DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA, Guía para la administración del riesgo y el diseño de controles en entidades públicas Octubre de 2018

#### **3.1.2 Calificación del impacto**

##### **3.1.2.1. Análisis del impacto en Riesgos de corrupción:**

El análisis de impacto se realizará teniendo en cuenta solamente los niveles “moderado”, “mayor” y “catastrófico”, dado que estos riesgos siempre serán significativos.

Para calificar el **impacto** a los **riesgos de corrupción** se debe partir del caso hipotético de la materialización del riesgo y tener en cuentael siguiente cuestionario, iniciando con la pregunta: “Si el riesgo se materializa podría:

1. Afectar al grupo de funcionarios del proceso
2. Afectar el cumplimiento de metas y objetivos de la dependencia
3. Afectar el cumplimiento de misión de la entidad
4. Afectar el cumplimiento de la misión del sector al que pertenece la entidad
5. Generar pérdida de confianza de la entidad, afectando su reputación
6. Generar pérdida de recursos económicos
7. Afectar la generación de los productos o la prestación de servicios
8. Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos
9. Generar pérdida de información de la entidad
10. Generar intervención de los órganos de control, de la Fiscalía u otro ente
11. Dar lugar a procesos sancionatorios
12. Dar lugar a procesos disciplinarios
13. Dar lugar a procesos fiscales
14. Dar lugar a procesos penales
15. Generar pérdida de credibilidad del sector
16. Ocasionar lesiones físicas o pérdida de vidas humanas
17. Afectar la imagen regional
18. Afectar la imagen nacional
19. Generar daño ambiental

* Si menos de cinco (5) respuestas son afirmativas la calificación del impacto es **moderado**, lo cual genera medianas consecuencias sobre la entidad
* Si el número de respuestas afirmativas esta entre seis (6) y once (11) el impacto es **mayor** y se generan altas consecuencias para la entidad.
* Si el número de respuestas afirmativas es mayor a doce (12) el impacto es **catastrófico** y se generan consecuencias desastrosas para la entidad

**3.1.2.2. Análisis del impacto en Riesgos de gestión:**

| **NIVEL** | **IMPACTO CUANTITATIVO** | **IMPACTO CUALITATIVO** |
| --- | --- | --- |
|
|  |
| **CATASTRÓFICO (5)** | - Impacto que afecte la ejecución presupuestal en un valor mayor o igual al 50%. - Pérdida de cobertura en la prestación de los servicios de la entidad en un valor mayor o igual al 50%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor mayor o igual al 50%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor mayor o igual al 50% del presupuesto general de la entidad. | - Interrupción de las operaciones de la entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de información crítica para la entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados. |
| **MAYOR (4)** | - Impacto que afecte la ejecución presupuestal en un valor igual o mayor a 20%. - Pérdida de cobertura en la prestación de los servicios de la entidad igual o mayor a 20%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor igual o mayor a 20%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor igual o mayor a 20% del presupuesto general de la entidad. | - Interrupción de las operaciones de la entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación |
| **MODERADO (3)** | - Impacto que afecte la ejecución presupuestal en un valor ≥5%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad. | - Interrupción de las operaciones de la entidad por un (1) día.  - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. - Inoportunidad en la información, ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias. |
| **MENOR (2)** | - Impacto que afecte la ejecución presupuestal en un valor mayor o igual a 1%.  - Pérdida de cobertura en la prestación de los servicios de la entidad mayor o igual a 5%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor mayor o igual a 1%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor mayor o igual a 1% del presupuesto general de la entidad. | - Interrupción de las operaciones de la entidad por algunas horas. - Reclamaciones o quejas de los usuarios, que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos. |
| **INSIGNIFICANTE (1)** | - Impacto que afecte la ejecución presupuestal en un valor mayor o igual a 0,5%. - Pérdida de cobertura en la prestación de los servicios de la entidad mayor o igual a 1%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor mayor o igual a 0,5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor mayor o igual a 0,5% del presupuesto general de la entidad. | - No hay interrupción de las operaciones de la entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa. |

#### Fuente: DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA, Guía para la administración del riesgo y el diseño de controles en entidades públicas Octubre de 2018

##### **3.1.2.3. Análisis del impacto en Riesgos de seguridad digital**:

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

#### Fuente: DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA, Guía para la administración del riesgo y el diseño de controles en entidades públicas Octubre de 2018

#### **Zona del Riesgo Inherente:**

Para definir el nivel del riesgo, se utiliza el **Mapa de calor** y se inicia ubicando la valoración de la probabilidad (Rara vez, Improbable, Posible, Probable ó Casi seguro). Posteriormente se determina el impacto en las columnas correspondientes. (Insignificante, Menor, Moderado, Mayor ó Catastrófico). Finalmente, se define el punto de intersección de las dos; que corresponderá al nivel de riesgo.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **PROBABILIDAD** | Casi seguro 5 |  |  |  |  |  |  | **Extremo** |
| Probable 4 |  |  |  |  |  |  | **Alto** |
| Posible 3 |  |  |  |  |  |  | **Moderado** |
| Improbable 2 |  |  |  |  |  |  | **Bajo** |
| Rara vez 1 |  |  |  |  |  |  |  |
|  |  | 1 | 2 | 3 | 4 | 5 |  |  |
|  |  | Insignificante | Menor | Moderado | Mayor | Catastrófico |  |  |
|  |  | **IMPACTO** | | | | |  |  |

Fuente: Secretaría de Transparencia de la Presidencia de la República.

### **Evaluación de Riesgos**

#### **3.2.1. Identificación de controles**

Las actividades de control son aquellas medidas orientadas a prevenir y detectar la materialización de los riesgos y deben estar documentadas. De esta forma, se garantiza que sean ejecutadas por responsables claros y que hagan parte de la operación normal de la Entidad.

##### **Clasificación de los controles**

* Control preventivo: Estos controles se orientan a eliminar las causas del riesgo para evitar que ocurran, como por ejemplo, revisar el cumplimiento de los requisitos contractuales en el proceso de selección del contratista.
* Control correctivo: Este tipo de controles permiten enfrentar un evento no deseado una vez que se ha presentado y permiten continuar con la operación normal de la Entidad. Aplicar un mecanismo para la protección de archivos físicos después de que han sido vulnerados.

Las medidas de control preventivo ayudan a minimizar la probabilidad de ocurrencia, mientras que las correctivas contribuyen a minimizar el impacto del riesgo.

Al momento de definir las actividades de control por parte de la primera línea de defensa, es importante considerar que los controles estén bien diseñados, es decir, que efectivamente estos mitigan las causas que hacen que el riesgo se materialice. Para ello se debe tener en cuenta:

* Tener definido el responsable de llevar a cabo la actividad de control.
* Indicar cuál es el propósito del control.
* Indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control.
* Tener una periodicidad definida para su ejecución.
* Establecer el cómo se realiza la actividad de control.
* Dejar evidencia de la ejecución del control.

#### **Valoración de los controles:**

Para la adecuada mitigación de los riesgos no basta con que un control esté bien diseñado, el control debe ejecutarse por parte de los responsables tal como se diseñó, ya que un control que no se ejecute, o un control que se ejecute y esté mal diseñado, no va a contribuir con la mitigación del riesgo.

La siguiente tabla detalla las variables establecidas para el análisis y evaluación del diseño del control que se encuentran dentro del formato mapa de riesgos institucional:

| Criterio de Evaluación | Aspecto a evaluar en el diseño del control | Opción de respuesta | Puntaje | Opción de respuesta | Puntaje |
| --- | --- | --- | --- | --- | --- |
| Responsable | ¿Existe un responsable asignado a la ejecución del control? | Asignado | 15 | No asignado | 0 |
| Responsable | ¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control? | Adecuado | 15 | Inadecuado | 0 |
| Periodicidad | ¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna? | Oportuna | 15 | Inoportuna | 0 |
| Propósito | Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, Ej.: verificar, validar, cotejar, comparar, revisar, etc. | Prevenir  Detectar | 15  10 | No es un control | 0 |
| ¿Cómo se realiza la actividad de control? | La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo | Confiable | 15 | No confiable | 0 |
| Qué pasa con las observaciones o desviaciones | ¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna | Se investigan y resuelven oportunamente | 15 | No se investigan y resuelven oportunamente | 0 |
| Evidencia de la ejecución del control | ¿Se deja evidencia o rastro de la ejecución del control que permita a cualquier tercero con la evidencia llegar a la misma conclusión? | Completa | 10 | Incompleta/no existe | 5/0 |

#### Fuente: DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA, Guía para la administración del riesgo y el diseño de controles en entidades públicas Octubre de 2018

1. **Calificación y peso del diseño de cada control:**

El resultado de cada variable de diseño afecta la calificación del diseño del control así:

| TOTAL EVALUACIÓN DEL DISEÑO DEL CONTROL | RANGO DE CALIFICACIÓN PESO DISEÑO DEL CONTROL |
| --- | --- |
| Calificación entre 96 y 100 | Fuerte |
| Calificación entre 86 y 95 | Moderado |
| Calificación entre 0 y 85 | Débil |

#### Fuente: DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA, Guía para la administración del riesgo y el diseño de controles en entidades públicas Octubre de 2018

1. **Calificación de la solidez individual del control:**

En la evaluación del diseño y ejecución de los controles las dos variables son importantes y significativas en el tratamiento de los riesgos y sus causas, ***por lo que siempre la calificación de la solidez de cada control asumirá la calificación del diseño o ejecución con menor calificación entre fuerte, moderado y débil***, tal como se detalla en la siguiente tabla:

| PESO DEL DISEÑO DE CADA CONTROL | PESO DE LA EJECUCIÓN DE CADA CONTROL | SOLIDEZ INDIVIDUAL DE CADA CONTROL: Fuerte: 100 Moderado: 50 Débil: 0 | SE DEBEN ESTABLECER ACCIONES PARA FORTALECER EL CONTROL |
| --- | --- | --- | --- |
| Fuerte:  calificación  entre 96 y 100 | fuerte (siempre se ejecuta) | fuerte + fuerte = fuerte |  |
| moderado (algunas veces) | fuerte + moderado = moderado | X |
| débil (no se ejecuta) | fuerte + débil = débil | X |
| Moderado:  calificación  entre 86 y 95 | fuerte (siempre se ejecuta) | moderado + fuerte = moderado | X |
| moderado (algunas veces) | moderado + moderado = moderado | X |
| débil (no se ejecuta) | moderado + débil = débil | X |
| Débil:  calificación entre  0 y 85 | fuerte (siempre se ejecuta) | débil + fuerte = débil | X |
| moderado (algunas veces) | débil + moderado = débil | X |
| débil (no se ejecuta) | débil + débil = débil | X |

#### Fuente: DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA, Guía para la administración del riesgo y el diseño de controles en entidades públicas Octubre de 2018

1. **Calificación de controles y su solidez:**

Dado que un riesgo puede tener varias causas y a su vez varios controles y la calificación se le realiza al riesgo, es importante evaluar el conjunto de controles asociados al riesgo, así:

| RANGO DE CALIFICACIÓN CONTROLES | SOLIDEZ DEL CONJUNTO DE CONTROLES |
| --- | --- |
| Fuerte | El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100 |
| Moderado | El promedio de la solidez individual de cada control al sumarlos y ponderarlos está entre 50 y 99. |
| Débil | El promedio de la solidez individual de cada control al sumarlos y ponderarlos es menor a 50. |

#### Fuente: DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA, Guía para la administración del riesgo y el diseño de controles en entidades públicas Octubre de 2018

1. **Riesgo residual (Después de Controles)**

Dado que ningún riesgo se evita o elimina con una medida de tratamiento, se debe calcular el riesgo residual, para lo cual se mide el nivel de desplazamiento del riesgo inherente en su probabilidad o impacto. Este cálculo se realizará de acuerdo con la siguiente tabla:

| Solidez del conjunto de los controles | Controles ayudan a disminuir la probabilidad | Controles ayudan a disminuir impacto | # columnas que se desplaza el riesgo en el eje vertical del mapa de calor | # columnas que se desplaza el riesgo en el eje horizontal del mapa de calor |
| --- | --- | --- | --- | --- |
| Fuerte | Directamente | Directamente | 2 | 2 |
| Fuerte | Directamente | Indirectamente | 2 | 1 |
| Fuerte | Directamente | No disminuye | 2 | 0 |
| Fuerte | No disminuye | Directamente | 0 | 2 |
| Moderado | Directamente | Directamente | 1 | 1 |
| Moderado | Directamente | Indirectamente | 1 | 0 |
| Moderado | Directamente | No disminuye | 1 | 0 |
| Moderado | No disminuye | Directamente | 0 | 1 |

#### Fuente: DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA, Guía para la administración del riesgo y el diseño de controles en entidades públicas Octubre de 2018

Si la solidez del conjunto de los controles es débil, este no disminuirá ningún cuadrante de impacto o probabilidad asociado al riesgo.

Tratándose de **riesgos de corrupción** únicamente hay disminución de probabilidad, en impacto no opera el desplazamiento.

Una vez realizado el análisis y evaluación de los controles para la mitigación de los riesgos, se procede a definir la nueva calificación de impacto y probabilidad y por lo tanto la nueva zona de riesgo en la cual se ubica el riesgo residual (Ver Numeral 3.1.3. Zona del Riesgo Inherente página 13 del presente documento)

## **TRATAMIENTO DEL RIESGO**

Consiste en evaluar las opciones para la mitigación de los riesgos considerando su importancia, probabilidad e impacto. Las acciones pueden ser establecidas con base en los siguientes criterios:

“**Asumir el riesgo**: Cuando un riesgo se ubica en la zona baja del mapa de calor, se acepta el riesgo, es decir que no será necesario adoptar medidas que afecten la probabilidad o impacto del riesgo. Este criterio aplica también para aquellos riesgos a los que no se les puedan establecer controles. Es importante tener en cuenta que ningún riesgo de corrupción puede ser aceptado.

**Evitar el riesgo**: En este caso se debe decidir no realizar o no continuar con la actividad que origina el riesgo y aplica cuando los riesgos son demasiado extremos.

**Compartir o transferir el riesgo**: El riesgo puede ser compartido o transferido con otras organizaciones cuando se considere que no se cuenta con la capacidad o experticia suficiente para gestionarlo. Las formas más comunes de compartir o transferir un riesgo son mediante seguros o tercerización. Los mecanismos de transferencia del riesgo deben respaldarse bajo un acuerdo contractual.

**Reducir el riesgo**: Implica la implementación de controles para minimizar la probabilidad de ocurrencia e impacto del riesgo o ambos.”[[2]](#footnote-2)

### **4.1. Niveles de aceptación del riesgo:**

| **Zona de riesgo** | **Significado** | **Nivel de aceptación** | **Tratamiento** |
| --- | --- | --- | --- |
| Extrema | En caso de materializarse, el riesgo genera impactos graves significativos para la Entidad. | No aceptable | Las acciones que se emprendan para tratar el riesgo extremo deben orientarse a evitar, reducir, compartir o transferir el riesgo. |
| Alta | En caso de materializarse, el riesgo genera impactos graves para la Entidad. | No aceptable | Considerando el impacto de estos riesgos, las acciones deben estar enfocadas a evitar, reducir, compartir o transferir el riesgo. |
| Moderada | En caso de materializarse, el riesgo genera impactos mínimos para la Entidad. | No aceptable | Las acciones deben estar enfocadas a reducir la probabilidad de ocurrencia del riesgo. |
| Baja | En caso de materializarse, el riesgo genera impactos sustancialmente leves para la Entidad. | Aceptable | El riesgo catalogado en nivel bajo se asume y es necesario realizar seguimiento continuo del riesgo. |

Fuente: Guía para la Gestión del Riesgo y diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública 2018.

**4.2. Acciones asociadas a los controles:**

Se formulan acciones orientadas a mitigar los riesgos teniendo en cuenta:

* Fecha inicial y fecha final de la actividad que se va a adelantar
* Actividad: Identificar la acción que se va a adelantar
* Responsable de la actividad: quien va a realizar la actividad
* Soporte Registro: Es la evidencia de la acción
* Indicador: Miden el índice de cumplimiento de las actividades establecidas

## **MONITOREO Y REVISIÓN**

Se debe monitorear y revisar la gestión de riesgos porque la entidad debe asegurar el logro de sus objetivos anticipándose a los eventos negativos relacionados con la gestión de la entidad y así mismo el avance en el desarrollo de las acciones asociadas a los controles establecidas; teniendo en cuenta que se debe contar siempre con las evidencias de lo que se realice.

Para el caso de los riesgos de gestión se realizará un seguimiento cada tres meses y para los riesgos de corrupción cada cuatro meses.

## **ROLES DE LAS LÍNEAS DE DEFENSA EN LA GESTIÓN DEL RIESGO**

El Modelo Integrado de Planeación y Gestión (MIPG) en la dimensión 7 “Control interno” desarrolla a través de las líneas de defensa la responsabilidad de la gestión del riesgo y control.

A continuación se detallan los roles y responsabilidades de todos los actores de la gestión del riesgo y el control en la entidad para proporcionar aseguramiento de la gestión y previniendo la materialización.

## **6.1. ESTRATÉGICA**:

#### ALTA DIRECCIÓN Y COMITÉ INSTITUCIONAL DE COORDINACIÓN DE CONTROL INTERNO:

* Establecer y aprobar la política de administración del riesgo la cual incluye los niveles de aceptación o tolerancia al riesgo.
* Supervisar el cumplimiento de la política de administración del riesgo
* Revisar el adecuado análisis y articulación de los objetivos institucionales con los objetivos de los procesos que sirvieron de base para llevar a cabo la identificación de los riesgos.
* Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles
* Realizar seguimiento y análisis periódico a los riesgos institucionales
* Retroalimentar al Comité Institucional de Gestión y Desempeño sobre 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 del mismo.

### **6.2. PRIMERA LÍNEA**

#### GERENTES PÚBLICOS Y LIDERES DE PROCESO, PROGRAMA O PROYECTO:

* Identificar, analizar, valorar, monitorear y evaluar los riesgos que pueden afectar los proyectos, planes y procesos a su cargo y actualizarlo cuando se requiera.
* Orientar el desarrollo e implementación de políticas y procedimientos y asegurar que sean compatibles con las metas y objetivos de la entidad y emprender las acciones de mejora para su logro.
* Diseñar, implementar y monitorear los controles además de gestionar de manera directa en el día a día los riesgos de la entidad.
* Definir, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados y proponer mejoras a la gestión del riesgo de los procesos.
* Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar
* Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles
* Informar a la oficina de planeación (segunda línea) sobre los riesgos materializados en los proyectos, planes y/o procesos a su cargo
* Reportar a la Oficina de Planeación, los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado.

### **SEGUNDA LÍNEA**

#### OFICINA ASESORA DE PLANEACIÓN, SUPERVISORES DE CONTRATOS, COORDINADORES DE OTROS SISTEMAS DE GESTIÓN Y COMITÉS INSTITUCIONALES

* Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición y aplicación 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 (riesgos de mayor criticidad frente al logro de los objetivos) y presentarlo para análisis y seguimiento ante el Comité Institucional de Gestión y Desempeño.
* Presentar al Comité Institucional de Control Interno, el seguimiento a la eficacia de los controles en las áreas identificadas en los diferentes niveles de operación de la entidad.
* Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis y valoración del riesgo.
* Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos.
* Supervisar en coordinación con los demás responsables de esta segunda línea de defensa que la primera línea identifique, evalué y gestione los riesgos y controles para que se generen acciones.
* Evaluar que los riesgos sean consistentes con la presente política de la entidad y que sean monitoreados por la primera línea de defensa.
* Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles.
* Identificar cambios en los riesgos, especialmente aquellos ubicados en zona baja y presentarlo para aprobación del Comité Institucional de Coordinación de Control Interno.

### **6.4. TERCERA LÍNEA**

#### OFICINA DE CONTROL INTERNO

* Realizar evaluación independiente al cumplimiento y efectividad de la Política de Administración del Riesgo, los mecanismos de evaluación del riesgo y la efectividad de los controles, en cumplimiento de su rol “Evaluación de la Gestión del Riesgo”.
* Alertar sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas.
* Evaluar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a los cambios que pueden afectar el Sistema de Control Interno para el cumplimiento de los objetivos.
* Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos.
* Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa.
* Asesorar de forma coordinada con la Oficina de Planeación, a la primera línea de defensa en la identificación de los riesgos institucionales y diseño de controles.
* Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos de conformidad con el Plan Anual de Auditoria y reportar los resultados al Comité Institucional de Coordinación de Control Interno.

## **ACCIONAR ANTE LOS RIESGOS MATERIALIZADOS**

El Departamento Administrativo de la Función Pública ha establecido unos lineamientos para tratar el riesgo materializado, los cuales involucran a la Asesoría de Control Interno y a los líderes de los procesos y se encuentran en la siguiente tabla:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Detectado por** | **Riesgo de corrupción** | **Riesgo de gestión** | | | |
|
| **Zona extrema** | **Zona alta** | **Zona moderada** | **Zona baja** |
| Oficina de Control Interno | 1. Convocar al Comité de Coordinación de Control Interno e informar sobre los hechos detectados, desde donde se tomarán las decisiones para iniciar la investigación de los hechos. | 1.          Informar al líder del proceso sobre el hecho encontrado. | | | 1. Informar al líder del proceso sobre el hecho. |
| 2. Dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante el ente de control respectivo. | 2.          Orientar al líder del proceso para que realice la revisión, análisis y acciones correspondientes para resolver el hecho. | | |  |
| 3.          Facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos y sus controles asociados. | 3.          Verificar que se tomaron las acciones y que se actualizó el mapa de riesgos correspondiente. | | | 2. Orientar técnicamente sobre las acciones determinadas en la política de riesgos institucional. |
| 4.          Verificar que se tomaron las acciones y se actualizó el mapa de riesgos. | 4.          Convocar al Comité de Coordinación de Control Interno e informar sobre la actualización realizada. | | |  |

Fuente: Guía para la Administración del Riesgo, Departamento Administrativo de la Función Pública 2014

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  | | | |
| **Detectado por** | **Riesgo de corrupción** | **Riesgo de gestión** | | | |
| **Zona extrema** | **Zona alta** | **Zona moderada** | **Zona baja** |
| Líder del proceso u otro(s) funcionario(s) que participa(n) o interactúa(n) con el proceso | 1. Informar a la Alta Dirección sobre el hecho encontrado. 2. De considerarlo necesario, realizar la denuncia ante el ente de control respectivo 3. Iniciar con las acciones correctivas necesarias. 4. Realizar el análisis de causas y determinar acciones preventivas y de mejora.   5. Análisis y actualización del mapa de riesgos. | 1. Tomar las acciones correctivas necesarias, dependiendo del riesgo materializado. 2. Iniciar el análisis de causas y determinar acciones preventivas y de mejora. 3. Analizar y actualizar el mapa de riesgos. 4. Informar a la Alta Dirección sobre el hallazgo y las acciones tomadas. | | | Aplicar las orientaciones de la política de riesgos institucional.    (Verificar los niveles de aceptación del riesgo). |

Fuente: Guía para la Administración del Riesgo, Departamento Administrativo de la Función Pública 2014

## **ELIMINACIÓN RIESGOS IDENTIFICADOS**

Los riesgos de gestión que se encuentren en nivel de aceptación BAJO, que soporten documentación de sus controles en sus procedimientos, evidencien su implementación y no presenten materialización durante la vigencia, no se incluirán en el mapa de riesgos.

## **REFERENCIAS**

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA, Guía para la administración del riesgo y el diseño de controles en entidades públicas Octubre de 2018, VERSIÓN 4 DIRECCIÓN DE GESTIÓN Y DESEMPEÑO INSTITUCIONAL,

1. <https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/->document\_library/bGsp2IjUBdeu/view\_file/34316499 [↑](#footnote-ref-1)
2. Fuente: Guía para la Gestión del Riesgo y diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública 2018. [↑](#footnote-ref-2)