# POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

La Unidad de Búsqueda de Personas dadas por Desaparecidas en el contexto y en razón del conflicto armado (UBPD) se encuentra comprometida con el fortalecimiento de la cultura de la prevención. Por lo tanto, dentro de su Sistema de Gestión, se identifican y gestionan los riesgos institucionales que puedan afectar: El cumplimiento del mandato legal, la integralidad en el cumplimiento de la misión, el carácter humanitario y extrajudicial, los principios rectores para la búsqueda de personas desaparecidas, el manejo eficiente y transparente de los recursos, la construcción de relaciones de confianza, y la satisfacción de los derechos a la verdad y a la reparación de las víctimas, como aporte a la construcción de paz en el marco del Sistema Integral de Verdad, Justicia, Reparación y No Repetición.

## 1. OBJETIVO

Orientar las acciones para administrar de manera adecuada los riesgos a los que se enfrenta la UBPD, reduciendo los posibles efectos de su materialización y estableciendo el tratamiento de los mismos, con el propósito de disminuir la vulnerabilidad frente a situaciones que puedan interferir en el cumplimiento de sus funciones y en el logro de los objetivos de la Entidad.

## 2. ALCANCE

La Política de Administración de Riesgos de la UBPD, abarca el manejo de los riesgos de gestión asociados a cada uno de los procesos definidos por la entidad, los de seguridad de la información y seguridad digital y los correspondientes a corrupción.

El diseño, implementación y seguimiento de los riesgos de prevención de daño antijurídico seguirán los lineamientos u orientaciones dadas por la Agencia Nacional de Defensa Jurídica del Estado, y los riesgos en los procesos de contratación seguirán los lineamientos u orientaciones dadas de la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente. Estos se regirán igualmente por las demás metodologías y políticas públicas que se impartan sobre la materia y que apliquen a la UBPD dada su naturaleza humanitaria y extrajudicial. Así mismo, para los riesgos de seguridad de la información y de seguridad digital, la Oficina de Tecnología de la Información y las Comunicaciones y el Oficial de Seguridad de la Información, emitieron los correspondientes lineamientos para la gestión de estos de acuerdo con la Metodología de Gestión de Riesgos de Seguridad de la información y Seguridad Digital definida para la Entidad, la cual se encuentra en el siguiente link: https://drive.google.com/drive/u/0/folders/1g5SbZQzFCvnczLQhYr-uTDXbBQwCb0Wy

## 3. VIGENCIA

La presente rige a partir de su aprobación por parte del Comité Institucional de Coordinación de Control Interno y permanece vigente hasta una nueva actualización.

## 4. MARCO CONCEPTUAL

De conformidad con la Guía para la Administración del Riesgo[1] expedida por el Departamento Administrativo de la Función Pública, las normas técnicas para la gestión de riesgos, la normatividad aplicable y los procedimientos de la entidad, la política de Administración de Riesgos se fundamenta en los siguientes conceptos:

- Administración de riesgos[2]**:** comprende el conjunto de Elementos de Control y sus interrelaciones, para que la entidad evalúe e intervenga aquellos eventos, tanto internos como externos, que puedan afectar de manera positiva o negativa el logro de sus objetivos.

  Para efectos del presente documento, al hablar de "*administración de riesgos*" se hace referencia también a la gestión y/o manejo de riesgos.

- Análisis de riesgo[3]: elemento de control que permite establecer la probabilidad de ocurrencia de los eventos positivos y/o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la entidad pública para su aceptación y manejo.

- Activo de información[4]: se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.

- Apetito del riesgo[5]: es el nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano del Gobierno. El apetito del riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

- Calificación del riesgo[6]: estimación de la probabilidad de ocurrencia y el impacto que puede causar la materialización del riesgo.

- Capacidad del riesgo[7]: es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la entidad.

---

[1] Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5, 2020.

[2] Departamento Administrativo de la Función Pública, Guía para la administración del riesgo, 2011.

[3] Ibíd.

[4] Política General de Seguridad, Protección y Confidencialidad de la Información de la Unidad de Búsqueda de Personas Dadas por Desaparecidas en el Contexto y en Razón del Conflicto Armado –UBPD-

[5] Ibíd.

[6] Ibíd.

[7] Ibíd.

- Causa[8]: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

- Causa Inmediata[9]: circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

- Causa Raíz[10]: causa principal o básica, corresponde a las razones por las cuales se puede presentar el riesgo.

- Confidencialidad[11]: propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

- Consecuencia[12]: 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.

- Control[13]: medida que permite reducir o mitigar el riesgo.

- Controles preventivos[14]: control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

- Controles detectivos[15]: control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

- Controles correctivos[16]: control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

- Disponibilidad[17]: propiedad de ser accesible y utilizable a demanda por una entidad.

- Evaluación del riesgo [18]: proceso utilizado para determinar las prioridades de la Administración del Riesgo comparando el nivel de un determinado riesgo con respecto a un estándar determinado.

---

8 Ibìd.
9 Ibíd.
10 Ibíd.
11 Ibíd.
12 Ibíd.
13 Ibíd.
14 Ibíd.
15 Ibíd.
16 Ibíd.
17 Ibíd.
18 Departamento Administrativo de la Función Pública, Guía para la administración del riesgo, 2011.

- Eventos Potenciales[19]: hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.

- Factores de riesgo[20]: Son las fuentes generadoras de riesgo.

- Identificación del riesgo[21]: elemento de control que posibilita conocer los eventos potenciales, estén o no bajo el control de la entidad, que ponen en riesgo el logro de su misión, estableciendo los agentes generadores, las causas y los efectos de su ocurrencia. Se puede entender como el proceso que permite determinar qué podría suceder, por qué sucedería y de qué manera se llevaría a cabo.

- Impacto[22]: se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

- Integridad[23]: propiedad de exactitud y completitud.

- Modelo de líneas de defensa[24]: es un modelo de control que establece los roles y responsabilidades de todos los actores del riesgo y control en una entidad, este proporciona aseguramiento de la gestión y previene la materialización de los riesgos en todos sus ámbitos (ver numeral 6. *"Responsabilidades"*).

- Monitorear[25]: comprobar, supervisar, observar o registrar la forma en que se lleva a cabo una actividad con el fin de identificar posibles cambios.

- Nivel de riesgo[26]: 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. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

- Política o lineamiento de administración de riesgos[27]: declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.

---

19 Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5, 2020.
20 Ibíd.
21 Departamento Administrativo de la Función Pública, Guía para la administración del riesgo, 2011.
22 Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5, 2020.
23 Ibìd.
24 Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4, 2018.
25 Departamento Administrativo de la Función Pública, Guía para la administración del riesgo, 2011.
26 Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5, 2020.
27 Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4, 2018.

- Plan anticorrupción y de atención al ciudadano[28]: el Plan Anticorrupción y de Atención al Ciudadano está integrado por políticas autónomas e independientes, que gozan de metodologías para su implementación con parámetros y soportes normativos propios, no implica para las entidades realizar actividades diferentes a las que ya vienen ejecutando en desarrollo de dichas políticas. El Plan Anticorrupción y de Atención al Ciudadano lo integran las siguientes políticas:

    - Gestión del riesgo de corrupción – Mapa de riesgos de corrupción y medidas para mitigar los riesgos.
    - Racionalización de trámites (Esta política no aplica a la UBPD de acuerdo al concepto emitido por el Departamento Administrativo de Función Pública el 09 de marzo de 2020).
    - Mecanismos para mejorar la atención al ciudadano.
    - Rendición de cuentas.
    - Mecanismos para la transparencia y acceso a la información.

- Probabilidad[29]: se entiende como la posibilidad de ocurrencia del riesgo; estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

- Probabilidad Inherente[30]: número de veces que se pasa por el punto de riesgo en el periodo de un (1) año.

- Riesgo[31]: efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

- Riesgo de Seguridad de la información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consideraciones.

- Riesgo de seguridad digital[32]: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales

- Riesgo de corrupción[33]: posibilidad de que, por acción u omisión, se use del poder para desviar la gestión de lo público hacia un beneficio privado.

- Riesgo inherente[34]: nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel de riesgo inherente, dentro de unas escalas de severidad.

---

[28] Guía estrategias para la construcción del plan anticorrupción y de atención al ciudadano, Versión 2, 2015.

[29] Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5, 2020.

[30] Ibíd.

[31] Ibíd.

[32] Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4, 2018.

[33] Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5, 2020.

[34] Ibíd.

- Riesgo residual[35]: resultado de aplicar la efectividad de los controles al riesgo inherente.

- Tolerancia del riesgo[36]: es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

- Valoración del riesgo[37]: es el elemento de control que determina el nivel o grado de exposición de la entidad al impacto del riesgo, permitiendo estimar las prioridades para su tratamiento. Es el producto de confrontar los resultados de la evaluación con los controles identificados.

- Vulnerabilidad[38]: representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

- Niveles de aceptación al riesgo[39]: decisión informada de tomar un riesgo particular, en caso de tener niveles de riesgo residuales tolerables. Para riesgo de corrupción es inaceptable.

## 5. NORMATIVIDAD

Constitución Política de Colombia, en sus artículos 209 y 269, incorporó el control interno como un instrumento orientado a garantizar el logro de los objetivos de cada entidad del Estado y el cumplimiento de los principios que rigen la función pública.

Ley 87 de 1993, artículo 2°, literales a) y f), los cuales establecen que el control interno está orientado a la protección de los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afecten, y a definir y aplicar medidas para prevenirlos, así como detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.

Ley 1474 de 2011, Estatuto Anticorrupción, el cual dispone en su artículo 73 que todas las entidades deben elaborar anualmente un Plan Anticorrupción y de Atención al Ciudadano, el cual debe incluir el mapa de riesgos de corrupción, las medidas concretas para mitigar esos riesgos, las estrategias anti-tramites y los mecanismos para mejorar la atención al ciudadano.

Ley 1712 de 2014, por medio de la cual se crea la Ley de Transparencia y del derecho de Acceso a la Información Pública Nacional; en el literal g) del artículo 9 establece el deber de publicar el Plan Anticorrupción y de Atención al Ciudadano, en los sistemas de información del Estado o herramientas que lo sustituyan.

Decreto 1083 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública; señala en su artículo 2.2.21.3.2 que los elementos mínimos del Sistema de Control Interno

35 Ibíd.

36 Ibíd.

37 Departamento Administrativo de la Función Pública, Guía para la administración del riesgo, 2011.

38 Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5, 2020.

39 Departamento Administrativo de la Función Pública, Guía para la administración del riesgo, 2011.

mencionados en la Ley 87 de 1993 y demás normativa relacionada, conforman cinco (5) grupos que se interrelacionan y que constituyen los procesos fundamentales de la administración: Dirección, Planeación, Organización, Ejecución, Seguimiento y Control (Evaluación). Así mismo, señala que los responsables de fortalecer la interrelación y funcionamiento armónico de los elementos que conforman estos 5 grupos son los servidores públicos en cumplimiento de las funciones asignadas en la normativa vigente, de acuerdo con el área o dependencia de la cual hacen parte.

Decreto 1499 de 2017, que actualiza el Modelo Integrado de Planeación y Gestión - MIPG, articulando "el nuevo Sistema de Gestión, que integra los anteriores sistemas de Gestión de Calidad y de Desarrollo Administrativo, con el Sistema de Control Interno actualizado también en la séptima dimensión" [40], con el fin de "consolidar, en un solo lugar, todos los elementos que se requieren para que una organización pública funcione de manera eficiente y transparente, y que esto se refleje en la gestión del día a día" [41].

Es necesario precisar que el Decreto 1499 de 2017 estableció en su artículo 2.2.22.3.4. el Ámbito de aplicación precisando que "El Modelo Integrado de Planeación y Gestión (MIPG) se adoptará por los organismos y entidades de los órdenes nacional y territorial de la rama ejecutiva del poder público. En el caso de las entidades descentralizadas con capital público y privado, el modelo aplicará en aquellas en que el Estado posea el 90% o más del capital social. Las entidades y organismos estatales sujetos a régimen especial, de conformidad con lo señalado en el artículo 40 de la Ley 489 de 1998, las ramas legislativa y judicial, la organización electoral, los organismos de control y los institutos científicos y tecnológicos, aplicarán la política de control interno prevista en la Ley 87 de 1993; así mismo, les aplicarán las demás políticas de gestión y desempeño institucional en los términos y condiciones en la medida en que les sean aplicables de acuerdo con las normas que las regulan."

En virtud del Acto Legislativo 01 de 2017, el Gobierno Nacional expidió el Decreto Ley 589 de 2017 "Por el cual se organiza la Unidad de Búsqueda de Personas dadas por Desaparecidas en el contexto y en razón del conflicto armado" , señalando conforme al parágrafo primero del artículo primero que: "La UBPD es una entidad del Sector Justicia, de naturaleza especial, con personería jurídica, autonomía administrativa y financiera, patrimonio independiente y un régimen especial en materia de administración de personal".

No obstante lo anterior, la incorporación de la Unidad dentro del sector justicia, no implica que esté sujeta a un control jerárquico o de tutela por parte del Ministerio de Justicia y del Derecho, tal como lo sostiene la Corte Constitucional en su Sentencia C-067 de 20 de junio de 2018, así:

> "(…) Desde esta perspectiva, y contrario a lo que sostienen los intervinientes, la referencia al sector justicia, no implica que la Unidad esté orgánicamente sujeta al Ministerio de Justicia y del Derecho, ya que no se consagra la existencia de una relación de adscripción o de vinculación para el ejercicio de sus funciones, circunstancia que sólo sería posible al tratarse de un organismos descentralizado, lo cual no corresponde con lo señalado ni en el Acto Legislativo 01 de 2017, ni el Decreto Ley 589 de 2017, en donde se señala que la UBPD es un organismo del orden nacional, con naturaleza jurídica especial".

[40] Presidencia de la República, Departamento Administrativo de la Función Pública. Modelo Integrado de Planeación y Gestión – MIPG. Pág. 5

[41] Ibíd.

Por lo anterior, y teniendo en cuenta la naturaleza jurídica de la UBPD y el concepto técnico emitido por el Departamento Administrativo de Función Pública del 02 de febrero de 2019 en el cual expresa claramente que "La reglamentación a aplicar frente al Sistema de Control Interno, son las disposiciones establecidas en la Ley 87 de 1993, y sus Decretos reglamentarios, específicamente el artículo 2.2.23.2 del Decreto 1499 de 2017, mediante el que se actualiza la estructura del Modelo Estándar de Control Interno MECI. "Respecto a los lineamientos o criterios para la actualización del Modelo Estándar de Control Interno, su entidad debe consultar la Dimensión 7 del Manual Operativo del Modelo Integrado de Planeación y Gestión MIPG, en donde se detalla la nueva estructura. En este sentido, dicha actualización deberá responder a la estructura de cinco componentes a saber: (i) Ambiente de control, (ii) Evaluación del riesgo, (iii) Actividades de control, (iv) Información y comunicación y (v) Actividades de monitoreo así como con la articulación con el modelo de las tres líneas de defensa", la UBPD, tomara en cuenta únicamente, lo expresado por el modelo para el Modelo Estándar de Control Interno (MECI) y lo que allí se relacione en temas de riesgos.

Decreto 648 de 2017, el cual modificó el nombre del artículo 2.2.21.3.2 del Decreto 1083 de 2015, de "Elementos de la Unidad Básica del Sistema" por "Elementos del Sistema Institucional de Control Interno".

Decreto 1393 de 2018, por el cual se establece la estructura interna de la Unidad de Búsqueda de Personas dadas por Desaparecidas en el contexto y en razón del conflicto armado (UBPD) y se determinan las funciones de sus dependencias. Esta norma precisa en el artículo el artículo 4, numeral 9, establece como función de la Oficina Asesora de Planeación "Orientar y coordinar la implementación, mantenimiento y mejora del Sistema Integrado de Gestión". Y en el 8, numeral 17, que una de las funciones para la Oficina de Control Interno es "Asesorar a las dependencias de la Unidad en la identificación y prevención de los riesgos que puedan afectar el logro de sus objetivos."

## 6. RESPONSABILIDADES

El Sistema de Control Interno está integrado por el esquema de organización y el conjunto de planes, métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por una entidad, con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y de los recursos, se lleven a cabo de acuerdo con las normas constitucionales y legales vigentes, dentro de las políticas trazadas por la alta dirección y en atención a las metas u objetivos previstos.
Adicionalmente, la estructura del MECI se acompaña por un esquema de asignación de responsabilidades, adaptado del Modelo *"Líneas de Defensa"*, el cual otorga responsabilidad a todos los niveles de la Entidad de la siguiente manera:

- Línea estratégica: Alta Dirección y Comité Institucional de Coordinación de Control Interno.
- Primera línea de defensa: Líderes de procesos o líderes operativos de proyectos de la entidad y equipos territoriales.
- Segunda línea de defensa: Jefes de planeación o quienes hagan sus veces, Subdirectora General Técnica y Territorial, coordinadores de equipos de trabajo, supervisores e interventores de contratos o proyectos, comité de riesgos, comité de contratación, áreas financieras, áreas de TIC.
- Tercera línea de defensa: Oficina de Control Interno, auditoría Interna o quien haga sus veces.

A continuación, se relacionan los roles y responsabilidades de cada línea de defensa en el Modelo Estándar de Control Interno.

| Líneas de Defensa en el Modelo Estándar de Control Interno |
|---|
| **LÍNEA ESTRATÉGICA** |
| A cargo de la Alta Dirección y Comité Institucional de Coordinación de Control Interno<br><br>***Responsabilidades:***<br><br>- *Define el marco general para la gestión del riesgo y el control.*<br>- *Analiza los riesgos y amenazas institucionales al cumplimiento de los planes estratégicos (objetivos, metas, indicadores).*<br>- Tiene la responsabilidad de definir el marco general para la gestión del riesgo (Política de Administración de Riesgos) y garantiza el cumplimiento de los planes de la Entidad. |

| 1ª. Línea de Defensa | 2ª. Línea de Defensa | 3ª. Línea de Defensa |
|---|---|---|
| A cargo de los *líderes de procesos o líderes operativos de proyectos de la entidad y equipos territoriales.*<br><br>***Responsabilidades:***<br><br>- *La gestión operacional se encarga del mantenimiento efectivo de controles internos, ejecutar procedimientos de riesgo y el control sobre una base del día a día. La gestión operacional identifica, evalúa, controla y mitiga los riesgos.*<br>- *Son responsables de implementar acciones correctivas, igualmente detecta las deficiencias de control* | A cargo de servidores con responsabilidades de monitoreo y evaluación de controles y riesgos: Oficina Asesora de Planeación, Subdirectora General Técnica y Territorial, coordinadores de grupos de trabajo, supervisores e interventores de contratos o proyectos, comité de contratación (cuando aplique), áreas financieras, Oficina de TIC, Oficial de Seguridad de la Información, entre otros que generen información para el aseguramiento de la operación.<br><br>***Responsabilidades:***<br><br>- *Asegura que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente.*<br>- Ejerce el control y la gestión de riesgos, las funciones de cumplimiento, seguridad, calidad y otras similares.<br>- Supervisa la implementación de prácticas de gestión de riesgo eficaces por parte de la primera línea, y ayuda a los responsables de riesgos a distribuir la información adecuada sobre | A cargo de la **Oficina de Control Interno**, Auditoría Interna o quién haga sus veces.<br><br>***Responsabilidades:***<br><br>- *Proporciona información sobre la efectividad del SCI., la operación de la primera y segunda línea de defensa con un enfoque basado en riesgos.*<br>- *La función de la auditoría interna, a través de un enfoque basado en el riesgo, proporciona aseguramiento sobre la eficacia de gobierno, gestión de riesgos y control interno a la alta dirección de la entidad, incluidas las maneras en que funciona la primera y segunda línea de defensa.* |

| | | |
|---|---|---|
| | riesgos a todos los servidores de la Entidad. | |

Fuente: Adaptado de Declaración de Posición. Las tres líneas de defensa para una efectiva gestión de riesgos y control. Instituto Internacional de Auditores IIA 2013

Para la implementación del Modelo Estándar de Control Interno, los roles y responsabilidades para la administración de riesgos están dados por el modelo de las líneas de defensa, así[42]:

| Líneas de Defensa | Responsable | Responsabilidad frente al riesgo |
|---|---|---|
| Línea Estratégica | Alta Dirección<br><br>Comité Institucional de Coordinación de Control Interno - CICCI | Establecer y aprobar la Política de Administración del Riesgo la cual incluye los niveles de responsabilidad y autoridad.<br><br>Definir y hacer seguimiento a los niveles de aceptación del riesgo.<br><br>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.<br><br>Realizar seguimiento y análisis periódico a los riesgos institucionales<br><br>El Comité Institucional de Coordinación de Control Interno, evalúa y da línea sobre la administración de los riesgos en la UBPD.<br><br>Presentar al Comité Institucional de Coordinación de Control los ajustes que se deban hacer frente a la gestión del riesgo.<br><br>Evaluar el estado del sistema de control interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento del mismo. |
| Primera Línea | A cargo de los líderes de procesos, líderes operativos de proyectos de la entidad y equipos territoriales.<br><br>Se encarga del mantenimiento efectivo de controles internos, ejecutar procedimientos de riesgo y el control sobre una base del día a día. La gestión operacional identifica, evalúa, controla y mitiga los riesgos. | Identificar y valorar los riesgos que pueden afectar los planes, proyectos y procesos a su cargo y actualizarlos cuando se requieran.<br><br>Gestionar los riesgos con base en la política de administración del riesgo e implementar las metodologías y lineamientos para ello.<br><br>Elaborar los mapas de riesgo, incluidos los riesgos de corrupción<br><br>Definir, aplicar y hacer monitoreo a los controles para mitigar los riesgos identificados y proponer mejoras a la gestión del riesgo en su proceso.<br><br>Monitorear la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, evaluar la eficiencia, eficacia y efectividad de los controles y determinar las acciones de mejora a que |

[42] "Guía para la administración del riesgo y el diseño de controles en entidades públicas" Versión 4. Departamento Administrativo de la Función Pública. Año 2018.

| | | |
|---|---|---|
| | Son responsables de implementar acciones correctivas, igualmente detecta las deficiencias de control | haya lugar, así como realizar monitoreo a las acciones de mejora establecidas.<br><br>Informar a la Oficina Asesora de Planeación (segunda línea) sobre los riesgos materializados en los planes, proyectos y/o procesos a su cargo.<br><br>Reportar a la Oficina de Control Interno (tercera línea de defensa) sobre los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado.<br><br>Contar con los responsables de los riesgos en todos los procesos y/o áreas funcionales. |
| Segunda Línea | A cargo de servidores con responsabilidades de monitoreo y evaluación de controles y riesgos: Está a cargo de la Oficina Asesora de Planeación, Secretaria General, Subdirectora General Técnica y Territorial, coordinadores de grupos de trabajo, supervisores e interventores de contratos o proyectos, áreas financieras, comités de contratación (cuando aplique). | Informar sobre la incidencia de los riesgos en el logro de objetivos y evaluar si la valoración del riesgo es la apropiada.<br><br>Consolidar y socializar el mapa de riesgos institucional (riesgos de mayor criticidad frente al logro de los objetivos) y presentarlo para análisis y seguimiento ante el Comité<br><br>Orientar a los líderes de procesos y a su equipo de trabajo en la identificación y valoración de los riesgos a su cargo, de acuerdo con la metodología y lineamientos establecidos por la Entidad e incorporando los riesgos de corrupción.<br><br>Monitorear los controles y acciones establecidos por la primera línea de defensa de acuerdo con la información suministrada por los líderes de procesos. |
| Segunda Línea | A cargo de servidores con responsabilidades de monitoreo y evaluación de controles y riesgos<br>está a cargo de Oficina de Tecnología de Información y Comunicaciones, Oficial de Seguridad de la Información, Secretario General, coordinadores de equipos de trabajo, supervisores e interventores de contratos o proyectos, áreas financieras, comités de contratación (cuando aplique). | Orientar a los líderes de proceso en la identificación y valoración de los riesgos de seguridad digital, de acuerdo con los lineamientos establecidos en la Entidad para este fin.<br><br>Monitorear los controles y acciones de los riesgos de seguridad digital establecidos por la primera línea de defensa de acuerdo con la información suministrada por los líderes de procesos. |
| Tercera Línea | A cargo de la Oficina de Control Interno | Evaluar de forma independiente y objetiva la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primera y segunda línea de defensa cumplan con sus responsabilidades en la |

| | | |
|---|---|---|
| | | gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción.<br><br>Dar a conocer a toda la entidad el Plan Anual de Auditorías basado en riesgos y los resultados de la evaluación de la gestión del riesgo.<br><br>Identificar y evaluar cambios que podrían tener un impacto significativo en el Sistema de Control Interno durante las evaluaciones periódicas de riesgos y en el curso del trabajo de auditoría interna, e informar al Comité Institucional de Coordinación de Control Interno.<br><br>Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos de la entidad.<br><br>Alertar sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas.<br><br>Alertar sobre la identificación y materialización de riesgos de corrupción, gestión y seguridad digital.<br><br>Recomendar mejoras a la política de administración del riesgo. |

## 7. ADMINISTRACIÓN DEL RIESGO

Los riesgos en la UBPD se identifican por procesos, entendiendo que, si en el marco de los planes o proyectos se identifican riesgos, estos se deben enmarcar dentro de los procesos de la Entidad según corresponda.

La Política de Administración de Riesgos se opera a través de los instrumentos que se diseñen en la Entidad para la administración de riesgos, que incorpora las directrices de la Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas – DAFP; Versión 5. Diciembre. 2020 y las normas internacionales para la gestión de riesgos, en las etapas de contexto estratégico, identificación, análisis, evaluación, monitoreo y revisión, y seguimiento.

Las siguientes son las directrices establecidas en la Unidad de Búsqueda de Personas dadas por Desaparecidas – UBPD para la gestión de sus riesgos, basados en la Guía para la administración del riesgo y el diseño de controles en entidades públicas (riesgos de gestión y corrupción).

## 8. IDENTIFICACIÓN DE RIESGOS

*"En la identificación de riesgos se tiene como objetivo identificar los riesgos que estén o no bajo el control de la organización, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos."*[43]

[43] Departamento Administrativo de la Función Pública. Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Versión 5. Año 2020. Pág. 27.

Los riesgos de corrupción se establecen sobre procesos. Con el fin de facilitar su identificación y evitar confusiones con los riesgos de gestión, se utiliza la siguiente matriz en la cual, si se marcan los cuatro componentes de su definición, podemos decir que hablamos de un riesgo de corrupción.

| Matriz de definición de riesgos de corrupción | | | | |
|---|---|---|---|---|
| Descripción del riesgo | Acción u omisión | Uso del poder | Desviar la gestión de lo publico | Beneficio Privado |
| (Ejemplo) Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato. | X | X | X | X |

**Fuente:** Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas – DAFP Versión 5; diciembre 2020.

## 1. VALORACIÓN DE RIESGOS

### 9.1. ANÁLISIS DE RIESGOS

El análisis busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo (riesgo inherente) y las acciones que se van a implementar. En el análisis del riesgo se deben considerar los aspectos de calificación y evaluación del riesgo; además dependerá de la información obtenida, de la identificación de riesgos y de la disponibilidad de datos históricos y aportes de los servidores de la organización.

Para determinar la probabilidad se entiende como la posibilidad de ocurrencia del riesgo y 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 pasa por el punto de riesgo en el periodo de un año.

En la siguiente tabla se establecen los criterios para definir el nivel de probabilidad de los riesgos de gestión y seguridad digital:

| | FRECUENCIA DE LA ACTIVIDAD | PROBABILIDAD |
|---|---|---|
| **Muy Baja** | La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año | 20% |
| **Baja** | La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año | 40% |
| **Media** | La actividad que conlleva el riesgo se ejecuta de 24 a 500 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% |

**Fuente:** Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de

Controles en Entidades Públicas – DAFP Versión 5; diciembre 2020.

Para los riesgos de corrupción los criterios están definidos en la siguiente tabla:

| Nivel | Descriptor | Descriptor | 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 una vez en el último año. |
| 3 | **Posible** | El evento podrá ocurrir en algún momento. | Al menos una vez en los últimos 2 años. |
| 2 | **Improbable** | El evento puede ocurrir en algún momento. | Al menos una vez en los últimos 5 años. |
| 1 | **Rara Vez** | El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales) | No se ha presentado en los últimos 5 años. |

**Fuente:** Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas – DAFP Versión 5; diciembre 2020.

Para determinar el impacto se definen los impactos económicos y reputacionales como las variables principales, cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto, en la siguiente tabla se establecen los criterios para definir el nivel de impacto en los riesgos de gestión:

| | AFECTACIÓN ECONÓMICA | AFECTACIÓN REPUTACIONAL |
|---|---|---|
| **Leve 20%** | Afectación menor a 10 SMLMV. | El riesgo afecta la imagen de algún área de la organización. |
| **Menor 40%** | Entre 10 y 50 SMLMV. | El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores. |
| **Moderado 60%** | Entre 50 y 100 SMLMV. | El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos. |
| **Mayor 80%** | Entre 100 y 500 SMLMV. | El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal. |
| **Catastrófico 100%** | Mayor a 500 SMLMV. | El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país. |

**Fuente:** Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas – DAFP; Versión 5; diciembre 2020.

Para el caso de los riesgos de corrupción, según lo definido en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas[44], los criterios para calificar el impacto son:

| No. | PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA… | RESPUESTA | |
|---|---|---|---|
| | | SI | NO |
| 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? | | |

| | | |
|---|---|---|
| Responder afirmativamente de UNA a CINCO preguntas genera un impacto moderado.<br>Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor.<br>Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico. | | |

| | | | |
|---|---|---|---|
| MODERADO | Genera medianas consecuencias sobre la entidad | | |
| MAYOR | Genera altas consecuencias sobre la entidad. | | |
| CATASTRÓFICO | Genera consecuencias desastrosas para la entidad. | | |

Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Versión 5. 2020. Departamento Administrativo de la Función Pública.

Nota: Si la respuesta a la pregunta 16 es afirmativa, el riesgo se considera catastrófico. Por cada riesgo de corrupción identificado, se debe diligenciar la tabla anterior.

Para el caso de los riesgos de seguridad de la información y seguridad digital el análisis del impacto se desarrollará de acuerdo con lo establecido en la Metodología de Gestión de Riesgos de Seguridad de la Información y Seguridad Digital definida para la Entidad.

[44] Departamento Administrativo de la Función Pública, Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Versión 5. 2020, pág. 72.

### 9.2. EVALUACIÓN DE RIESGOS

Para los riesgos de gestión y seguridad digital, la evaluación del riesgo se determina combinando la probabilidad con el impacto en el mapa de calor (Ilustración 1), dando como resultado el nivel de severidad donde se encuentra el riesgo.

Para el caso de los riesgos de corrupción, en la evaluación no aplican los niveles de impacto insignificante y menor, ya que el análisis de impacto se realiza solo teniendo en cuenta los niveles "moderado", "mayor" y "catastrófico", debido a que estos riesgos siempre son significativos.

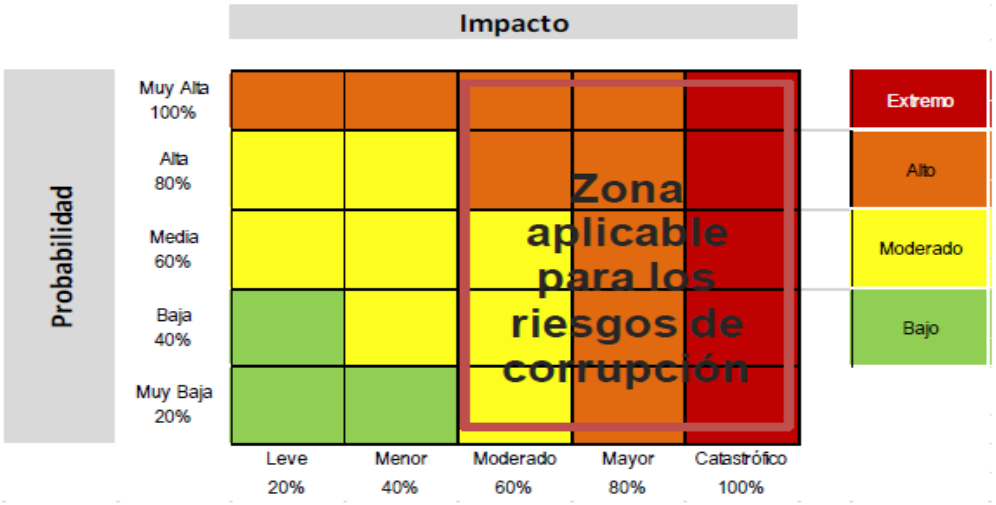



*Ilustración 1. Mapa de Calor. "Fuente: Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas – DAFP; Versión 5. Diciembre. 2020".*

La valoración del riesgo es el producto de confrontar los resultados de la evaluación del riesgo inicial (riesgo inherente) frente a los controles establecidos, con el fin de determinar la zona de riesgo final (riesgo residual). Esto se hace con el objetivo de establecer prioridades para su manejo y para la fijación de políticas.

Al momento de definir las actividades de control se debe validar que estas mitigan el riesgo, para lo cual se establece la siguiente estructura, tipología y atributos para los riesgos de gestión:

**Responsable de ejecutar el control:** identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificara el sistema que realiza la actividad.

**Acción:** se determina mediante verbos que indican la acción que deben realizar como parte del control.

**Complemento:** corresponde a los detalles que permiten identificar claramente el objeto del control.

Acorde a lo anterior se presenta la siguiente tabla donde se muestran los atributos de eficiencia e informativos que deben tener los controles para la correcta mitigación de los riesgos de gestión:

| Características | | | Descripción | Peso |
|---|---|---|---|---|
| Atributos de eficiencia | Tipo | Preventivo | Va hacia las causas del riesgo, aseguran el resultado final esperado. | 25% |
| | | Detectivo | Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos. | 15% |
| | | Correctivo | Dado que permite reducir el impacto de la materialización del riesgo, tiene un costo en su implementación. | 10% |
| | Implementación | Automático | Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización. | 25% |
| | | Manual | Controles que son ejecutados por una persona, tiene implícito el error humano. | 15% |
| Atributos informativos | Documentación | Documentado | Controles que están documentados en el proceso, ya sean manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso. | - |
| | | Sin documentar | Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso. | - |
| | Frecuencia | Continua | El control se aplica siempre que se realiza la actividad que conlleva al riesgo. | - |
| | | Aleatoria | El control se aplica aleatoriamente a la actividad que conlleva el riesgo. | - |
| | Evidencia | Con registro | El control deja un registro, permite evidenciar la ejecución del control. | - |
| | | Sin registro | El control no deja registro de la ejecución del control. | - |

*Fuente: Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas – DAFP; Versión 5. Diciembre. 2020*

En el caso de los riesgos de corrupción al momento de definir las actividades de control se debe validar que estas mitigan el riesgo, para lo cual en su diseño se deben incluir las siguientes variables:

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

El líder del proceso, a partir de la metodología e instrumentos definidos, debe asegurar que las actividades de control se encuentran bien diseñadas y que éstas se ejecutan tal como han sido definidas, lo cual será revisado mediante las actividades de monitoreo de la segunda línea de defensa y, de auditoría interna o evaluación independiente realizadas por la Oficina de Control Interno.

Para el caso de los riesgos de seguridad de la información y seguridad digital, los atributos de la valoración de los controles se desarrollarán de acuerdo con lo establecido en la Metodología de Gestión de Riesgos de Seguridad de la Información y Seguridad Digital definida para la Entidad.

La forma en que estas actividades de control afectan la probabilidad y/o el impacto determina la ubicación final del riesgo en el mapa de calor (Ilustración 1), lo cual se conoce como riesgo residual.

## 10. ESTRATEGIAS PARA COMBATIR EL RIESGO

Luego de valorar el riesgo, el líder del proceso debe decidir si evita, reduce, comparte, transfiere o asume el riesgo, partiendo del riesgo residual de la siguiente manera:

i) **Evitar el riesgo.** *"Después de realizar un análisis y considerar que el nivel de riesgo es demasiado alto, se determina NO asumir la actividad que genera este riesgo"*[45].

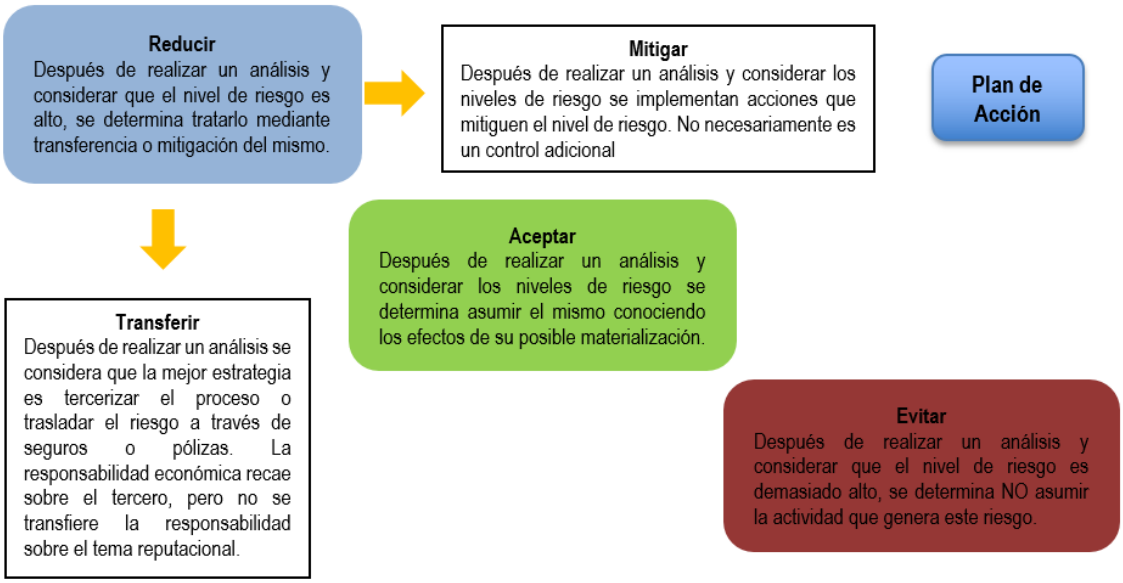
ii) **Reducir el riesgo.** *"Después de realizar un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante transferencia o mitigación del mismo "*[46].

a) **Mitigar el riesgo:** "*Después de realizar un análisis y considerar los niveles de riesgo se implementan acciones que mitiguen el nivel del riesgo. No necesariamente es un control adicional*" [47].

[45] Departamento Administrativo de la Función Pública, Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Versión 5. 2020, pág. 57.
[46] Ibíd.
[47] Ibíd.

b) **Transferir el riesgo:** "*Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional*" [48].

iii) **Aceptar el riesgo**. *"Después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo conociendo los efectos de su posible materialización "* [49].




De esta manera se establecen los niveles de aceptación del riesgo (Apetito del riesgo):

- Riesgos ubicados en la **zona de riesgo baja** se asumirá el riesgo y los líderes de proceso realizarán seguimiento trimestral con el fin de validar que la calificación de probabilidad e impacto no ha tenido cambios. La administración de los riesgos en esta zona se realizará a través de las actividades propias del proceso.

- La UBPD no aceptará los riesgos ubicados en la zona de riesgo "moderado", "alto" y "extremo", por lo tanto, se adoptarán medidas para evitar, reducir o compartir el riesgo, de tal manera que se formularán planes de acción.

- Ningún riesgo de corrupción podrá ser aceptado, por lo tanto, para estos riesgos se adoptarán medidas para evitarlos, reducirlos o compartirlos, de tal manera que se formularán actividades de control sobre

[48] Ibíd.
[49] Ibíd.

las cuales los líderes de proceso realizarán monitoreo y registro cuatrimestral, según lo definido en la Guía Estrategias para la construcción del plan anticorrupción y de atención al ciudadano.

El plan de acción como mínimo debe especificar: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento estos deben ser, "establecidos por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción" [50].

## 11. MONITOREO Y REVISIÓN DEL RIESGO

Es el paso que asegura el logro de los objetivos institucionales mediante la previsión de los eventos negativos asociados a la gestión de la entidad, y se desarrolla a través de un esquema de asignación de responsabilidades y roles de la siguiente manera:

| Línea de defensa | Monitoreo y Revisión |
|---|---|
| Línea estratégica | Define el marco general para la gestión del riesgo y el control, y supervisa su cumplimiento. Está a cargo de la Alta Dirección y el Comité Institucional de Coordinación de Control Interno. |
| 1ª Línea de defensa | Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.<br><br>Está a cargo de los líderes de procesos o líderes operativos de proyectos quienes deben realizar monitoreo a las actividades de control formuladas realizando el registro y reporte de los avances a la Oficina Asesora de Planeación. |
| 2ª Línea de defensa | Asegura que las actividades de control y los procesos de gestión de riesgos implementados por la primera línea de defensa estén diseñados apropiadamente y funcionen como se pretende.<br><br>Está a cargo de la Oficina Asesora de Planeación, Oficina de Tecnología de Información y Comunicaciones, Oficial de Seguridad de la Información, Secretario General, coordinadores de equipos de trabajo, supervisores e interventores de contratos o proyectos, áreas financieras, comités de contratación (cuando aplique), estos deben monitorear la gestión del riesgo y control ejecutada por la primera línea de defensa, informando las observaciones pertinentes respecto a lo reportado con el fin de fortalecer el cumplimiento de las etapas de administración de riesgos y remitir a la (3ª línea de defensa), el resultado consolidado del monitoreo validado como segunda línea de defensa. |
| 3ª línea de defensa | Proporciona información sobre la efectividad del Sistema de Control Interno, a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa.<br><br>Una vez recibidos los resultados presentados por la 2ª línea de defensa, de acuerdo con lo definido en el plan anual de auditoría, la Oficina de Control Interno evaluará el diseño y |

[50] Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5, 2020.

| | |
|---|---|
| | ejecución de los controles con el fin de presentar un informe de evaluación a la gestión de riesgos ante la línea estratégica (Comité Institucional de Coordinación de Control Interno). |

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas" Versión 5. Departamento Administrativo de la Función Pública. Año 2020

## 12. TRATAMIENTO DE RIESGOS MATERIALIZADOS

En el evento de materialización de un riesgo, las líneas de defensa deberán emprender acciones en el marco de sus responsabilidades, así:

| Tratamiento de Riesgos Materializados | |
|---|---|
| 1ª Línea de defensa | ● Informar y remitir a la segunda línea de defensa el respectivo plan de mejora que incluya *la ejecución de la corrección* que permitió restablecer la situación y las acciones a adelantar para la actualización del mapa de riesgos.<br>● Cuando se trate de un riesgo de corrupción, realizar la denuncia ante la instancia de control correspondiente, una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normativa asociada al hecho de corrupción materializado). |
| 2ª Línea de defensa | ● Orientar a los líderes de proceso en la actualización del mapa de riesgos. |
| 3ª Línea de defensa | ● Cuando en el marco de un ejercicio de evaluación independiente o seguimiento, la Oficina de Control Interno identifique la materialización de un riesgo, deberá informar a los líderes de proceso sobre el hecho detectado, los cuales emprenderán las acciones descritas para la primera línea de defensa en este numeral.<br>● Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso para revisar el mapa de riesgos.<br>● En articulación con la segunda línea de defensa, informar a la línea estratégica (Comité Institucional de Coordinación de Control Interno) sobre el estado de los riesgos materializados. |

## 13. EVALUACIÓN

La evaluación de la política de administración de riesgos se realizará cada vez que se requiera por parte de la alta dirección.

## 14. MONITOREO Y REVISIÓN

El monitoreo y revisión al mapa de riesgos institucional, estará a cargo de los líderes de los procesos, en conjunto con su equipo de trabajo (primera línea de defensa) y de los líderes de cada uno de los tipos de riesgos en la Entidad (segunda línea de defensa), su finalidad principal es monitorear permanentemente la gestión del riesgo y la efectividad de los controles, y de esta manera, sugerir los correctivos y ajustes cuando sea necesario para asegurar un efectivo manejo de riesgo.

El monitoreo al mapa de riesgos de gestión y a los controles establecidos, se realizará como mínimo (1) vez al año, salvo en los casos que los lineamientos u orientaciones establezcan los respectivos seguimientos. Los ciclos de control establecidos se revisarán y ajustarán si es necesario, para adaptarlos a los cambios, situaciones o circunstancias por las que pueda atravesar la Entidad.

Para el caso de los riesgos de corrupción el monitoreo se realizará cuatrimestralmente desde el inicio de cada vigencia.

## 15. SEGUIMIENTO Y EVALUACIÓN INDEPENDIENTE

La Oficina de Control Interno en su rol de evaluación de la gestión del riesgo, realizará el seguimiento al mapa de riesgos institucional, atendiendo la normatividad aplicable.

## 16. DIVULGACIÓN

La Política de Administración del Riesgo y el Mapa de Riesgos Institucional se divulgarán en la Entidad, a través de los canales y medios de comunicación establecidos por el líder de la administración del riesgo en la Entidad. La socialización al interior de las dependencias estará a cargo de los líderes de proceso.

Para el caso del mapa de riesgos de corrupción, este será publicado en la página web de la entidad, a más tardar el 31 de enero de cada vigencia.

Revisó: Miembros del Comité Institucional de Control Interno en la sesión 09 del día 25 de agosto de 2021
Aprobó: Miembros del Comité Institucional de Control Interno en la sesión 09 del día 25 de agosto de 2021