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 la integralidad del Sistema de Verdad, Justicia, Reparación y No Repetición, el cumplimiento de su misión, su mandato legal, su carácter humanitario y extrajudicial, los principios, 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.

1. OBJETIVO

Orientar las acciones para administrar de manera adecuada los riesgos a los que se enfrenta la UBPD, mitigando los posibles efectos de su materialización y estableciendo el tratamiento de los mismos, con el propósito de orientar las acciones necesarias que conduzcan a 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 digital, así como los correspondientes a corrupción, de acuerdo con lo establecido en el artículo 73 de la Ley 1474 de 2011.

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 la naturaleza humanitaria y extrajudicial. Así mismo para los riesgos de seguridad digital la Oficina de Tecnología de la Información y las Comunicaciones emitirá los correspondientes lineamientos.

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

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

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.

- Calificación del riesgo[4]: estimación de la probabilidad de ocurrencia y el impacto que puede causar la materialización del riesgo.

- Causa[5]: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

- Consecuencia[6]: 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: medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

- Controles preventivos: diseñados para evitar un evento no deseado en el momento en que se produce. Este tipo de controles intentan evitar la ocurrencia de los riesgos que puedan afectar el cumplimiento de los objetivos[7].

- Controles detectivos: diseñados para identificar un evento o resultado no previsto después de que se haya producido. Buscan detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes[8].

- Evaluación del riesgo: combinación de la probabilidad de ocurrencia de un riesgo con el impacto de su materialización, que permite determinar el grado de exposición de la entidad.

---

[2] Ibíd.
[3] Ibíd.
[4] Ibíd.
[5] Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4, 2018.
[6] Ibíd.
[7] Ibíd
[8] Ibíd

- Evento[9]: incidente o situación que ocurre en un lugar determinado durante un periodo de tiempo determinado. Este puede ser cierto o incierto y su ocurrencia puede ser única o ser parte de una serie.

- Identificación del riesgo[10]: 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[11]: se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

- Mitigación: moderación, aplacamiento, disminución o suavización de un riesgo.

- Modelo de líneas de defensa[12]: 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[13]: comprobar, supervisar, observar o registrar la forma en que se lleva a cabo una actividad con el fin de identificar posibles cambios.

- Política o lineamiento de administración de riesgos[14]: declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.

- Plan de restablecimiento: hace referencia a la descripción de actividades a desarrollar ante la materialización de un riesgo.

- Plan de tratamiento: corresponde a la selección y aplicación de medidas para modificar el riesgo y prevenir su materialización.

- Probabilidad[15]: se entiende como la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de frecuencia, si se ha materializado (por ejemplo: número de veces en un tiempo determinado), o de factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque este no se haya materializado.

[9] Departamento Administrativo de la Función Pública, Guía para la administración del riesgo, 2011.
[10] Ibíd.
[11] Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4, 2018.
[12] Ibíd.
[13] Departamento Administrativo de la Función Pública, Guía para la administración del riesgo, 2011.
[14] Departamento Administrativo de la Función Pública, Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4, 2018.
[15] Ibíd.

- Riesgo[16]: posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

- Riesgo de gestión[17]: posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- Riesgo de Seguridad Digital[18]: combinación de amenazas y vulnerabilidades en el ambiente 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. El riesgo de seguridad digital es de naturaleza dinámica. Incluye aspectos relacionados con el ambiente físico y digital, las personas involucradas en las actividades y los procesos organizacionales que las soportan

- Riesgo de corrupción[19]: posibilidad de que, por acción u omisión, se use del poder para desviar la gestión de lo público hacia un beneficio privado.

- Riesgo inherente[20]: es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

- Riesgo residual[21]: nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.

- Valoración del riesgo[22]: 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.

- Niveles de aceptación al riesgo[23]: 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 1991, 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

[16] Ibíd.
[17] Ibíd.
[18] Consejo Nacional de política Económica y social CONPES -Documento CONPES 3854–Política Nacional de Seguridad Digital 2016
[19] Ibíd.
[20] Ibíd.
[21] Ibíd.
[22] Departamento Administrativo de la Función Pública, Guía para la administración del riesgo, 2011.
[23] Departamento Administrativo de la Función Pública, Guía para la administración del riesgo, 2011.

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 trámites 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 en los sistemas de información del Estado o herramientas que lo sustituyan el plan Anticorrupción y de Atención al Ciudadano.

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 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 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" [24], 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" [25].

Es necesario precisar que este Decreto 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

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

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”.

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, 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. y su articulación con el modelo de las tres líneas de defensa”, la UBPD, tomara en cuenta únicamente, lo expresado por el modelo para el tema de Control Interno 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 su artículo 8 el 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.” y el artículo 4 del numeral 9 establece como función de la Oficina Asesora de Planeación “ Orientar y coordinar la implementación, mantenimiento y mejora del Sistema Integrado de Gestión”.

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.
- Segunda línea de defensa: jefes de Planeación o quienes haga sus veces, 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 ***Responsabilidades:*** - *Define el marco general para la gestión del riesgo y el control.* - *Analiza los riesgos y amenazas institucionales al cumplimiento de los planes estratégicos (objetivos, metas, indicadores).* - 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.*	A cargo de servidores con responsabilidades de monitoreo y evaluación de controles y riesgos: Oficina Asesora de Planeación, coordinadores de equipos de trabajo, supervisores e interventores de contratos o proyectos, comité de contratación (cuando aplique), áreas financieras, Oficina de TIC, entre otros	A cargo de la **Oficina de Control Interno**, Auditoría Interna o quién haga sus veces.

Responsabilidades: - *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.* - *Son responsables de implementar acciones correctivas, igualmente detecta las deficiencias de control*	que generen información para el Aseguramiento de la operación. ***Responsabilidades:*** - *Asegura que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente.* - Ejerce el control y la gestión de riesgos, las funciones de cumplimiento, seguridad, calidad y otras similares. - 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 riesgos a todos los servidores de la Entidad.	***Responsabilidades:*** - *Proporciona información sobre la efectividad del SCI., la operación de la primera y segunda línea de defensa con un enfoque basado en riesgos.* - *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.*

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[26]:

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
	Alta dirección	Establecer y aprobar la Política de administración del riesgo la cual incluye los niveles de responsabilidad y autoridad. Definir y hacer seguimiento a los niveles de aceptación del riesgo. Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la

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

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
Línea Estratégica	Comité Institucional de Coordinación de Control Interno - CICCI	entidad y que puedan generar cambios en la estructura de riesgos y controles. Realizar seguimiento y análisis periódico a los riesgos institucionales El Comité Institucional de Coordinación de Control Interno, evalúa y da línea sobre la administración de los riesgos en la UBPD. Presentar al Comité Institucional de Coordinación de Control 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.
Primera Línea	A cargo de los líderes de procesos o líderes operativos de proyectos de la entidad 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. Son responsables de implementar acciones correctivas, igualmente detecta las deficiencias de control	Identificar y valorar los riesgos que pueden afectar los proyectos, planes y procesos a su cargo y actualizarlos cuando se requieran. Gestionar los riesgos con base en la política de administración del riesgo e implementar las metodologías y lineamientos para ello. Elaborar los mapas de riesgo, incluidos los riesgos de corrupción Definir, aplicar y hacer monitoreo a los controles para mitigar los riesgos identificados y proponer mejoras a la gestión del riesgo en su proceso. 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 haya lugar, así como realizar monitoreo a las acciones de mejora establecidas. Informar a la Oficina Asesora de Planeación (segunda línea) sobre los riesgos materializados en los proyectos, planes y/o procesos a su cargo.

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
		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. 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, Secretario General, coordinadores de equipos 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. 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 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. 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 Está a cargo de Oficina de Tecnología de Información y Comunicaciones, Secretario General, coordinadores de equipos de trabajo, supervisores e interventores de contratos o proyectos, áreas financieras,	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. 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.

Líneas de Defensa	Responsable	Responsabilidad frente al riesgo
	comités de contratación (cuando aplique).	
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. 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. 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. Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos de la entidad Alertar sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas Alertar sobre la identificación y materialización de riesgos de corrupción, gestión y seguridad digital. 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 de Administración del Riesgo de la Función Pública 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

"La identificación del riesgo se lleva a cabo determinando las causas con base en el contexto interno, externo y del proceso que pueden afectar el logro de los objetivos institucionales. Algunas causas externas no controlables por la entidad se podrán evidenciar en el análisis del contexto externo, para ser tenidas en cuenta en el análisis y valoración del riesgo. A partir de este contexto se identifica el riesgo, el cual estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del proceso o los estratégicos." [27]

9. ANÁLISIS Y EVALUACIÓN 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.

La calificación del riesgo se debe realizar de acuerdo con los siguientes rangos:

PROBABILIDAD			
Descriptor	**Criterios Factibilidad**	**Criterios de Frecuencia**	**Valoración**
Casi Seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año	**5**
Probable	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año.	**4**
Posible	El evento podrá ocurrir en algún momento	Al menos 1 vez en los últimos 2 años.	**3**
Improbable	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años.	**2**
Rara Vez	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.	**1**

Fuente: Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas – DAFP; octubre 2018.

[27] "Guía para la administración del riesgo y el diseño de controles en entidades públicas" Versión 4. Departamento Administrativo de la Función Pública. Año 2018. Pág. 22.

Cuando la UBPD no cuente con datos históricos sobre el número de eventos que se hayan materializado en un periodo de tiempo, se debe calificar el nivel de probabilidad en términos de factibilidad.

IMPACTO			
Des.	**Impacto (Consecuencias) Cuantitativo**	**Impacto (Consecuencias) Cualitativo**	**Valor del impacto**
CATASTRÓFICO	Impacto que afecte la ejecución presupuestal en un valor ≥50%	Interrupción de las operaciones de la Entidad por más de cinco (5) días.	**5**
	Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%.	Intervención por parte de un ente de control u otro ente regulador.	
	Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50%.	Pérdida de Información crítica para la entidad que no se puede recuperar.	
	Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad.	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	Impacto que afecte la ejecución presupuestal en un valor ≥20%	Interrupción de las operaciones de la Entidad por más de dos (2) días.	4
	Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%.	Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta.	
	Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20%.	Sanción por parte del ente de control u otro ente regulador.	

IMPACTO			
Des.	**Impacto (Consecuencias) Cuantitativo**	**Impacto (Consecuencias) Cualitativo**	**Valor del impacto**
	Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad.	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 del servicio a los usuarios o ciudadanos.	
MODERADO	Impacto que afecte la ejecución presupuestal en un valor ≥5%	Interrupción de las operaciones de la Entidad por un (1) día.	**3**
	Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%.	Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad.	
	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.	Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos.	
		Inoportunidad en la información ocasionando retrasos en la atención a los usuarios.	
		Reproceso de actividades y aumento de carga operativa.	
		Investigaciones penales o fiscales	
MENOR	Impacto que afecte la ejecución presupuestal en un valor ≥1%	Interrupción de las operaciones de la Entidad por algunas horas.	**2**
	Pérdida de cobertura en la prestación de los servicios de la entidad ≥5%.	Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias.	
	Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥1%		

IMPACTO			
Des.	**Impacto (Consecuencias) Cuantitativo**	**Impacto (Consecuencias) Cualitativo**	**Valor del impacto**
	Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1% del presupuesto general de la entidad.	Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.	
	Impacto que afecte la ejecución presupuestal en un valor ≥1%		
INSIGNIFICANTE	Impacto que afecte la ejecución presupuestal en un valor ≥0,5%	No hay interrupción de las operaciones de la entidad.	
	Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%.	No se generan sanciones económicas o administrativas.	**1**
	Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥0,5%	No se afecta la imagen institucional de forma significativa.	
	Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5% del presupuesto general de la entidad.		

Fuente: Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas – DAFP; octubre 2018.

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[28], los criterios para calificar el impacto de riesgos de corrupción 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?		

[28] Departamento Administrativo de la Función Pública, Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Versión 4. 2018, pág. 46.

No.	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA…	RESPUESTA	
		SI	NO
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. Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor. 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 4. 2018. Departamento Administrativo de la Función Pública.

Por cada riesgo de corrupción identificado, se debe diligenciar la tabla anterior

La evaluación del riesgo se determina combinando la probabilidad con el impacto en el mapa de calor (Ilustración 1), dando como resultado el nivel donde se encuentra el riesgo:

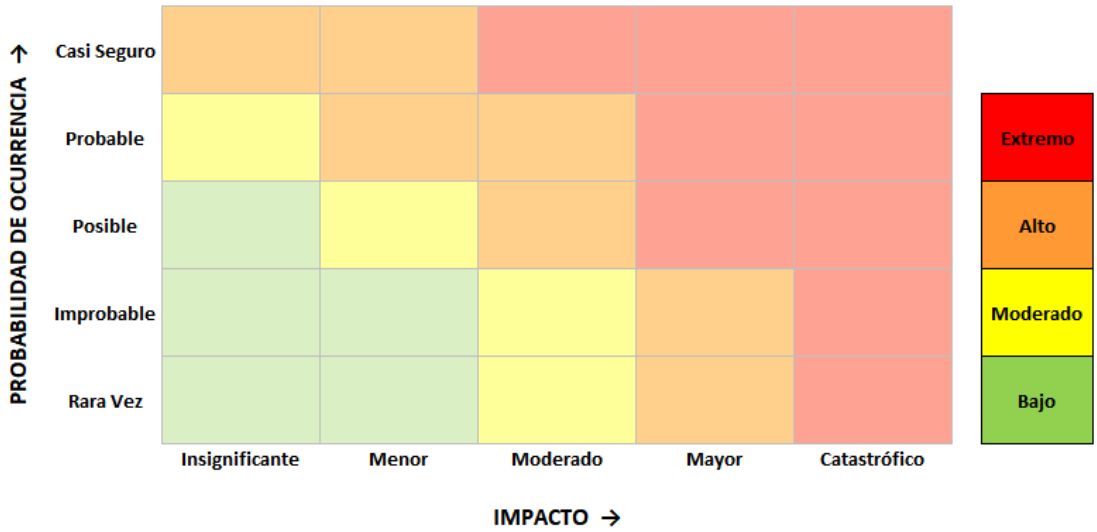

Ilustración 1. Mapa de Calor. "Fuente: Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas – DAFP; octubre 2018.".

Para el caso de los riesgos de corrupción, para 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

10. VALORACIÓN DE RIESGOS

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 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.

Las actividades de control se clasifican como preventivos y detectivos:

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.

11. TRATAMIENTO DE RIESGOS

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

i. **Evitar el riesgo.** *"Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca"*[29].

ii. **Reducir el riesgo.** *"Implica tomar medidas encaminadas a disminuir tanto la probabilidad como el impacto. La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Se consigue generalmente mediante la optimización de los procedimientos y la implementación de controles"*[30].

iii. **Compartir o transferir el riesgo.** *"Se reduce la probabilidad o impacto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra organización, como en los contratos a riesgo compartido. Es así como, por ejemplo, la información de gran importancia se puede duplicar y almacenar* en un lugar distante y de ubicación segura, en lugar de dejarla concentrada en un solo lugar"[31].

iv. **Aceptar el riesgo**. *"No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (ningún riesgo de corrupción podrá ser aceptado). Esto debería aplicar para riesgos inherentes en la zona de calificación de riesgo bajo*" [32].

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

[29] Ibíd.
[30] "Guía para la administración del riesgo" Departamento Administrativo de la Función Pública. Año 2011.
[31] Ibíd.
[32]"Guía para la administración del riesgo y el diseño de controles en entidades públicas" Versión 4. Departamento Administrativo de la Función Pública. Año 2018.

- 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 acciones de control.

- Riesgos de corrupción Ningún riesgo de corrupción podrá ser aceptado, por lo tanto, para estos riesgos se adoptarán medidas para evitar, reducir o compartir el riesgo, de tal manera que se formularán actividades de control sobre las cuales los líderes de proceso realizarán monitoreo y registro cuatrimestral, según lo definido en la Guía para la Gestión del Riesgo de Corrupción.

El plan de tratamiento del riesgo corresponderá a las acciones para fortalecer el control, "establecidas por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción" [33].

12. 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 y monitoreo. 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. Está a cargo de la Oficina Asesora de Planeación, Oficina de Tecnología de Información y Comunicaciones, Secretario General, coordinadores de equipos de trabajo, supervisores e interventores de contratos o proyectos, áreas financieras,

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

Línea de defensa	Monitoreo y Revisión
	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. 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 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 4. Departamento Administrativo de la Función Pública. Año 2018

13. 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. • 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.

Tratamiento de Riesgos Materializados	
	• 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. • 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.

14. EVALUACIÓN

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

15. 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 y a los controles establecido, 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.

16. 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.

17. DIVULGACIÓN

La política de administración del riesgo y el mapa de riesgos institucional se divulgará 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.

Revisó: Miembros del Comité Institucional de Control Interno en la sesión 06 del día 6 de noviembre de 2019
Aprobó: Miembros del Comité Institucional de Control Interno en la sesión 06 del día 6 de noviembre de 2019