



ALCALDÍA DE **LA TEBAIDA**

PLANEACIÓN

POLÍTICA DE ADMINISTRACIÓN
DEL RIESGO
ALCALDIA DE LA TEBAIDA

Vigencia 2025

| | | |
|-----|--|------------------------------|
| 1. | INTRODUCCIÓN | 3 |
| 2. | GLOSARIO | 3 |
| 3. | POLÍTICA DE ADMINISTRACIÓN DE RIESGOS..... | 5 |
| 4. | OBJETIVO DE LA POLÍTICA DE RIESGOS | 6 |
| 5. | ALCANCE..... | 6 |
| 6. | CONTEXTO ESTRATÉGICO | 6 |
| 7. | RESPONSABILIDADES | 7 |
| 8. | MARCO CONCEPTUAL PARA EL APETITO DEL RIESGO | 9 |
| 9. | IDENTIFICACIÓN DE ÁREAS DE IMPACTO | 10 |
| 10. | METODOLOGÍA..... | 10 |
| 11. | IDENTIFICACIÓN Y DESCRIPCIÓN DE RIESGO | 10 |
| 12. | VALORACIÓN DE RIESGOS..... | 11 |
| 13. | ANÁLISIS DE RIESGOS | 11 |
| 14. | DETERMINACIÓN DE LA PROBABILIDAD | 11 |
| 15. | DETERMINACIÓN DE IMPACTO | 12 |
| 16. | EVALUACIÓN DEL RIESGO | 12 |
| 17. | VALORACIÓN DE CONTROL..... | 13 |
| 18. | NIVEL DE CALIFICACIÓN DE PROBABILIDAD PARA RIESGOS DE CORRUPCIÓN | 16 |
| 19. | RIESGOS DE CORRUPCIÓN | 16 |
| 20. | ANÁLISIS DEL IMPACTO EN RIESGOS DE CORRUPCIÓN | 17 |
| 21. | CRITERIOS PARA LA EVALUACIÓN DE IMPACTO DE PÉRDIDA DE CONTINUIDAD..... | 18 |
| 22. | ACCIONES ANTE LOS RIESGOS MATERIALIZADOS..... | 19 |
| 23. | ACCIONES A SEGUIR EN CASO DE MATERIALIZACIÓN DE RIESGOS DE CORRUPCIÓN..... | 19 |
| 24. | SEGUIMIENTO A MAPA DE RIESGOS Y CONTROLES..... | 21 |
| 25. | ESTRATEGIA DE SEGUIMIENTO AL PLAN DE ACCIÓN | 22 |
| 26. | ANEXOS | ERROR! BOOKMARK NOT DEFINED. |

1. Introducción

En el presente documento, la Alcaldía de La Tebaida, en busca de una gestión eficiente y eficaz, implementa las directrices sobre la gestión de la administración del riesgo al interior de la entidad, de acuerdo con las directrices del Departamento Administrativo de la Función Pública.

Con el fin de brindar una mejora continua en cada uno de sus procesos, la Alcaldía desea generar conciencia entre los servidores públicos, sin importar el nivel, sobre la forma en que una situación de riesgo puede causar consecuencias negativas en los diferentes procesos, tanto misionales como administrativos. Por ende, se presentarán las diferentes estrategias para la gestión del riesgo.

Con el propósito de evitar reprocesos administrativos y asegurar que la gestión de la Alcaldía del Municipio de La Tebaida sea eficiente y productiva al servicio de los grupos de valor. Es importante resaltar que esta política toma como base el Modelo Integrado de Planeación y Gestión (MIPG).

Finalmente, siguiendo con la integración que nos exige el Modelo Integrado de Planeación y Gestión (MIPG), se conservan los capítulos dedicados a las políticas de transparencia, acceso a la información pública y lucha contra la corrupción. Estas áreas seguirán siendo lideradas por la Secretaría de Transparencia y el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), respectivamente, en sus roles de garantizar la integridad y seguridad de la información.

2. Glosario

- **Activo:** en el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.
- **Amenazas:** situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Apetito del riesgo:** 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 de Gobierno. El apetito del riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- **Causa inmediata:** circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.
- **Causa raíz:** causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
- **Consecuencia:** 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.
- **Confidencialidad:** propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
- **Contingencia:** posible evento futuro, condición o eventualidad.
- **Continuidad del negocio:** capacidad de una organización para continuar la entrega de productos o servicios a niveles aceptables después de una crisis.
- **Control:** medida que permite reducir o mitigar un riesgo.
- **Crisis:** ocurrencia o evento repentino, urgente, generalmente inesperado que requiere acción inmediata.
- **CIGD:** Comité Institucional de Gestión y Desempeño.
- **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad.
- **Integridad:** propiedad de exactitud y completitud.
- **Mapa de riesgos:** documento que resume los resultados de las actividades de gestión de riesgos, incluye una representación gráfica en modo de mapa de calor de los resultados de la evaluación de riesgos.
- **MIPG:** Modelo Integrado de Planeación y Gestión.
- **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

- **Restablecimiento:** capacidad de la Entidad para lograr una recuperación y mejora, cuando corresponda, de las operaciones, instalaciones o condiciones de vida una vez se supera la crisis.
- **Riesgo:** efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Los eventos potenciales 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.
- **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 consecuencias. (ISO/IEC 27000).
- **Riesgo de corrupción:** posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Riesgo Fiscal:** efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.
- **Riesgo inherente:** nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
- **Riesgo residual:** el resultado de aplicar la efectividad de los controles al riesgo inherente.
- **SGI:** Sistema Gestión Institucional, aplicativo propio para la gestión de planeación riesgos e indicadores.
- **TIC:** Tecnologías de la Información y las Comunicaciones.
- **Vulnerabilidad:** representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

3. Política de administración de riesgos

La Administración Municipal define su política del riesgo atendiendo los lineamientos establecidos en la política de operación para la administración del riesgo en la función pública, tiene un carácter estratégico y está fundamentada en el modelo integrado de planeación y gestión – MIPG, la guía para la administración del riesgo y el diseño de controles en entidades públicas, la cual plasma la identificación, análisis, valoración, evaluación, tratamiento y respuesta a los riesgos

que puedan afectar la misión institucional, el cumplimiento de los objetivos estratégicos y la gestión de los planes, programas y proyectos, con el fin de minimizar aspectos adversos ante una desviación o eventualidad que impida dar continuidad a la gestión institucional o cumplir con los compromisos adquiridos.

4. Objetivo de la Política de Riesgos

Establecer lineamientos concretos referentes a la gestión de la Administración del Riesgo, con el fin de alcanzar un nivel de riesgos residuales aceptables en todos los procesos, con el fin de dar cumplimiento en el desarrollo de la misionalidad, los compromisos de gobierno, los objetivos estratégicos y procesos vigentes de la Alcaldía de la Tebaida.

5. Alcance

La presente política de gestión de riesgos se aplicará a todos los procesos y actividades de la Alcaldía de la Tebaida incluyendo la planificación estratégica, la ejecución de proyectos, la prestación de servicios y la gestión administrativa. La política se centrará en la identificación, evaluación, tratamiento, monitoreo y comunicación de los riesgos que puedan afectar el logro de los objetivos institucionales, con el fin de garantizar la continuidad de las operaciones, la protección de los activos y el cumplimiento de las obligaciones legales.

6. CONTEXTO ESTRATÉGICO

En cada Vigencia se analiza el entorno estratégico de la Entidad a partir de los siguientes factores internos y externos, para el adecuado análisis de las causas del riesgo y gestión del mismo:

Tabla 1. Contexto Estratégico Alcaldía de La Tebaida

| CLASIFICACIÓN | FACTORES |
|------------------|--|
| CONTEXTO EXTERNO | Políticos: cambios de gobierno, legislación, políticas públicas, regulación. |
| | Económicos y financieros: Disponibilidad de capital, emisión de deuda o no pago de la misma, liquidez, mercados financieros, desempleo, competencia, disminución del presupuesto por prioridades del gobierno, austeridad en el gasto |
| | Sociales y culturales: demografía, responsabilidad social, orden público. |
| | Tecnológicos: avances en tecnología, acceso a sistemas de información externos, fallas en la infraestructura tecnológica, gobierno en línea. |
| | Medio Ambientales: emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible, contaminación por sustancias perjudiciales para la salud, mala práctica de clasificación de residuos. |

| | |
|-----------------------------|---|
| | <p>Comunicación Externa: Mecanismos utilizados para entrar en contacto con la ciudadanía, canales de información, adopción de herramientas de nube privada.</p> <p>Legales y reglamentarios: normatividad externa (leyes, decretos, ordenanzas y acuerdos).</p> |
| CONTEXTO INTERNO | <p>Financieros: presupuesto de funcionamiento, necesidades por parte de las dependencias, aprobación de recursos, comunicación de las dependencias intervinientes en el proceso presupuestal, recursos de inversión, infraestructura, capacidad instalada.</p> <p>Personal: competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.</p> <p>Procesos: capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento, herramientas y aplicativos internos, servidores internos,</p> <p>Tecnología: integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información, nuevos tipos de riesgos con suplantación de identidad, adopción de nube privada o pública par las labores cotidianes.</p> <p>Estratégicos: direccionamiento estratégico, planificación institucional, solicitud de información a las dependencias, información institucional, funciones y competencias de la entidad, liderazgo, trabajo en equipo.</p> <p>Comunicación Interna: Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.</p> |
| CONTEXTO DEL PROCESO | <p>Diseño del proceso: claridad en la descripción del alcance y el objetivo del proceso, planes proyectos y presupuestos articulados.</p> <p>Interacciones con otros procesos: relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes.</p> <p>Transversalidad: procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos en la entidad.</p> <p>Procedimientos asociados: pertinencia en los procedimientos que desarrollan los procesos.</p> <p>Responsables del proceso: grado de autoridad y responsabilidad de los funcionarios frente al proceso, responsabilidad compartida, control de ejecución de los procesos.</p> <p>Comunicación entre los procesos: efectividad en los flujos de información determinados en la interacción de los procesos.</p> <p>Activos de seguridad digital del proceso: información, aplicaciones, hardware entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano.</p> |

7. Responsabilidades

La responsabilidad está definida por las líneas de defensa y en la entidad se acogen según la siguiente tabla.

Tabla 2. Responsabilidades de las Líneas de Defensa

| Línea de Defensa | Responsable | Responsabilidad frente al riesgo |
|------------------|-------------|----------------------------------|
|------------------|-------------|----------------------------------|

| | | |
|-------------------------------------|--|---|
| Línea estratégica | Alta dirección - Comité institucional de gestión y desempeño | Esta línea al ser una instancia decisoria dentro del sistema de Control Interno, su rol principal es analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento de los planes institucionales y estratégicos, así como definir el marco general para la gestión del riesgo (política de administración del riesgo) y el cumplimiento de los planes de la entidad. Los aspectos clave para el Sistema de Control Interno SCI a tener en cuenta por parte de la Línea Estratégica: |
| | | Fortalecimiento del Comité Institucional de Coordinación de Control Interno incrementando su periodicidad para las reuniones. |
| | | Evaluación de la forma como funciona el Esquema de Líneas de Defensa, incluyendo la línea estratégica |
| | | Definición de líneas de reporte (canales de comunicación) en temas clave para la toma de decisiones, atendiendo el Esquema de Líneas de Defensa. |
| Subcomité de Riesgo | Definición y evaluación de la Política de Administración del Riesgo. La evaluación debe considerar su aplicación en la entidad, cambios en el entorno que puedan definir ajustes, dificultades para su desarrollo, riesgos emergentes. | |
| | Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento. | |
| Primera línea de defensa | Líderes de procesos y sus equipos de trabajo | Esta línea está bajo la responsabilidad, principalmente, de los líderes de procesos y de sus equipos de trabajo (en general servidores públicos en todos los niveles de la organización); su rol principal es el mantenimiento efectivo de controles internos, la ejecución de gestión de riesgos y controles en el día a día. Para ello, identifica, evalúa, controla y mitiga los riesgos a través del "Autocontrol". |
| | | Los aspectos clave para el Sistema de Control Interno SCI a tener en cuenta por parte de la 1ª Línea: |
| | | El conocimiento y apropiación de las políticas, procedimientos, manuales, protocolos y otras herramientas que permitan tomar acciones para el autocontrol en sus puestos de trabajo. |
| | | La identificación de riesgos y el establecimiento de controles, así como de su seguimiento, acorde con el diseño de dichos controles, evitando la materialización de los riesgos. |
| Segunda línea de defensa | Secretaría de Planeación | El seguimiento a los indicadores de gestión de los procesos e institucionales, según corresponda. |
| | | La coordinación con los líderes de procesos, de las acciones establecidas en la planeación institucional a fin de contar con información clave para el seguimiento o autoevaluación aplicada por parte de la 2ª línea de defensa. |
| | SUPERVISORES Y SERVIDORES PUBLICOS DELEGADOS | Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo. |

| | | |
|---------------------------------|-----------------------------------|--|
| Tercera línea de defensa | Oficina de Control Interno | Esta línea está bajo la responsabilidad de la (el) Jefe de control interno; desarrollaran su labor a través de los siguientes roles a saber: liderazgo estratégico, enfoque hacia la prevención, evaluación de la gestión del riesgo, relación con entes externos de control y el de evaluación y seguimiento. |
| | | Los aspectos clave para el Sistema de Control Interno SCI a tener en cuenta por parte de la 3ª Línea: |
| | | A través de su rol de asesoría, orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Secretaría de Planeación y el comité de riesgos |
| | | Monitoreo a la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo. |
| | | Asesoría proactiva y estratégica a la Alta Dirección y los líderes de proceso, en materia de control interno y sobre las responsabilidades en materia de riesgos. |
| | | Informar los hallazgos y proporcionar recomendaciones de forma independiente. |
| | | Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos. |
| | | Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa. |
| | | Seguimiento al plan de mejoramiento, su aplicación y seguimiento para resolver los hallazgos presentados. |
| | | Recomendar mejoras a la política de operación para la administración del riesgo. |

8. Marco conceptual para el apetito del riesgo

El apetito de riesgo es un factor importante dentro de la política de administración de riesgos, para comprenderlo mejor se presenta una definición conceptual para facilitar su análisis:

Nivel de riesgo: es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.

Apetito de riesgo: es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

Tolerancia del riesgo: es el valor de la máxima desviación admisible del nivel de

riesgo con respecto al valor del apetito de riesgo determinado por la entidad.

Capacidad de riesgo: es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual las altas direcciones consideran que no sería posible el logro de los objetivos de la entidad

9. Identificación de áreas de impacto

El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

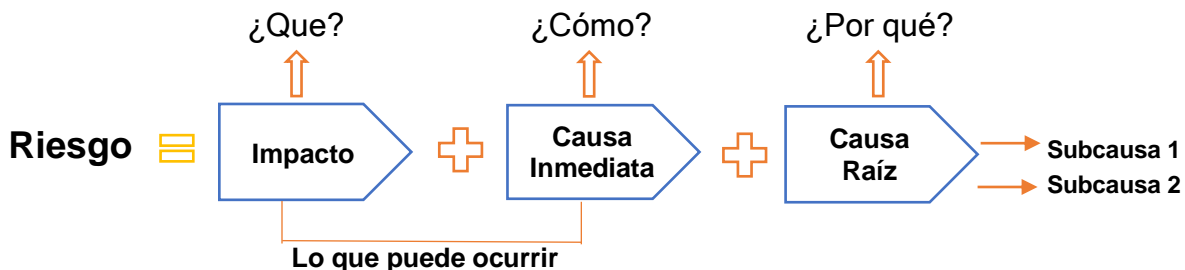
10. Metodología

La metodología para la Alcaldía de la Tebaida se define a partir de los lineamientos establecidos por el Departamento Administrativo de la Función Pública en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, V6, teniendo en cuenta las etapas de identificación, valoración y seguimiento.

11. Identificación y descripción de riesgo

Esta fase tiene como objetivo la identificación de los riesgos que están o no bajo el control de la entidad, teniendo en cuenta el contexto estratégico en el que opera la Alcaldía, las características de cada proceso considerando sus objetivos y alcance, analizando los factores de riesgos internos y externos.

Es importante que los riesgos identificados contengan los detalles necesarios para su fácil entendimiento tanto para el líder del proceso como para las personas ajenas al mismo, se toma como referencia de la Guía para la administración de riesgos, la estructura que facilita su redacción y claridad que analizan los siguientes factores:



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, v6 – Dirección de Gestión y Desempeño Institucional, noviembre 2022

La estructura anterior permite entender cómo se puede manifestar un riesgo, así como sus causas inmediatas y causas principales o raíz, esta información es fundamental para la elaboración de controles en la etapa de valoración de riesgos.

- **Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Causa Inmediata:** Circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.
- **Causa Raíz:** Causa principal o básica, corresponde a las razones por las cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo puede existir más de una causa o sub-causas que pueden ser analizadas.

12. Valoración de riesgos

Análisis de riesgos

En este punto busca establecer la probabilidad de ocurrencia del riesgo, es decir la exposición que tiene la entidad frente al riesgo y el impacto o las consecuencias que pueden generar, con la finalidad de determinar la zona de severidad del riesgo inherente, para el diseño y efectividad de los controles.

Determinación de la Probabilidad

La probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año, es decir el número de veces que se ejecuta la acción.

Tabla 3. calificación de probabilidad para riesgos de proceso, fiscal y seguridad digital

| Probabilidad | Descripción | Nivel |
|--------------|--|-------|
| Muy Baja | La actividad se realiza máximo 2 veces al año. | 20% |
| Baja | La actividad se realiza entre 3 a 24 veces al año. | 40% |

| | | |
|----------|--|------|
| Media | La actividad se realiza entre 25 a 500 veces al año. | 60% |
| Alta | La actividad se realiza entre 501 a 5000 veces al año. | 80% |
| Muy Alta | La actividad se realiza más de 5000 veces al año. | 100% |

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, v6 – Dirección de Gestión y Desempeño Institucional, noviembre 2022

13. Determinación de Impacto

El impacto de un riesgo se refiere a las consecuencias negativas que puede generar si se materializa. Para evaluarlo, se analizarán las áreas específicas de la entidad que se verían afectadas.

Utilizando los criterios y rangos definidos en la tabla 4, que ha sido adaptada de las recomendaciones del Departamento Administrativo de la Función Pública, se clasificará el impacto de cada riesgo en los diferentes niveles.

Es importante indicar que cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, los cuales tienen diferentes niveles, se debe tomar el más alto.

Tabla 4. calificación de impacto para riesgos de proceso, fiscal y seguridad digital

| Nivel | Impacto | Descripción Económico o Presupuestal | Descripción Reputacional |
|-------|-------------|--|--|
| 20% | Leve | Pérdida económica hasta 10 SMLV | Solo de conocimiento de algunos funcionarios. |
| 40% | Menor | Pérdida económica entre 11 hasta 50 SMLV | De conocimiento general de la entidad a nivel interno, Dirección General, Comités y Proveedores. |
| 60% | Moderado | Pérdida económica entre 50 hasta 100 SMLV | Deterioro de imagen con efecto publicitario sostenido a nivel Local o Sectores Administrativos. |
| 80% | Mayor | Pérdida económica entre 100 hasta 500 SMLV | Deterioro de imagen con efecto publicitario sostenido a nivel Nacional o Territorial. |
| 100% | Catastrfico | Pérdida Económica mayor a 500 SMLV | Deterioro de imagen con efecto publicitario sostenido a nivel internacional. |

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, v6 – Dirección de Gestión y Desempeño Institucional, noviembre 2022

14. Evaluación del Riesgo

En esta etapa, una vez analizado el riesgo identificado y descrito para determinar la probabilidad y el impacto, se debe realizar el análisis de esta probabilidad e impacto identificado para determinar el nivel de severidad del riesgo inherente, a través de la combinación de probabilidad e impacto en el mapa de calor.

Para la determinación del nivel de severidad del riesgo inherente, se definen cuatro (4) zonas de severidad como se observa en la matriz de calor que se presenta a continuación:

| | | IMPACTO | | | | | | | | |
|---------------------------|------------------|-------------|--------------|-----------------|--------------|----------------------|--|--|--|----------|
| PROBABILIDAD / FRECUENCIA | MUY ALTA 100% | | | | | | | | | |
| | ALTA 80% | | | | | | | | | Extremo |
| | MEDIA 60% | | | | | | | | | Alto |
| | BAJA 40% | | | | | | | | | Moderado |
| | MUY BAJA 20% | | | | | | | | | Bajo |
| | | | | | | | | | | |
| | | LEVE 20% | MENOR 40% | MODERADO 60% | MAYOR 80% | CATASTROFICO 100% | | | | |

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, v6 – Dirección de Gestión y Desempeño Institucional, noviembre 2022

15. Valoración de control

El control es la medida que permite reducir o mitigar el riesgo, por lo tanto, es necesario identificar controles a cada riesgo a través de las entrevistas con los líderes de los procesos o servidores expertos en su quehacer. En este caso si implica el criterio del experto. Adicional los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

Estructura para la descripción del control: para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

- Responsable de ejecutar el control: identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará 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.

Se establecerá una tipología de controles, clasificados según su momento de aplicación y su naturaleza.

- **Controles preventivos:** Se implementan antes de que ocurra el riesgo, con el objetivo de evitar su materialización. Actúan sobre las causas raíz del riesgo.
- **Controles detectivos:** Se ejecutan durante la realización del proceso para identificar el riesgo en sus etapas iniciales y minimizar sus consecuencias.
- **Controles correctivos:** Se aplican después de que el riesgo se ha materializado, con el fin de reducir su impacto y evitar que vuelva a ocurrir.

Adicionalmente, los controles pueden ser:

- **Manuales:** Realizados por personas, como revisiones o verificación.
- **Automáticos:** Realizados por sistemas o aplicaciones, como validaciones de datos, alertas automáticas.

Es importante mencionar que los controles preventivos y detectivos reducen probabilidad de ocurrencia y los correctivos atacan el impacto, teniendo en cuenta la siguiente valoración porcentual:

Tabla 5. Valoración de controles

| 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 puede generar reproceso | 15% |
| | | Correctivo | Dado que permiten reducir el impacto de la materialización del riesgo, tienen 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 error humano. | 15% |
| Atributos de Formalización | Documentación | Documentado | Controles que están documentados en el proceso, ya sea en 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 | Este atributo identifica a los controles que se ejecutan siempre que se realiza la actividad originadora del riesgo | - |

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, v6 – Dirección de Gestión y Desempeño Institucional, noviembre 2022

Para calcular el riesgo inherente se debe realizar la siguiente operación:

RIESGO INHERENTE * CONTROL = EL RESULTADO SE RESTA NUEVAMENTE AL RIESGO INHERENTE ES DE DECIR: RIESGO INHERENTE – RESULTADO = A RIESGO RESIDUAL.

Nivel de riesgo (riesgo residual): es el resultado de aplicar la efectividad de los controles al riesgo inherente. Para la aplicación de los controles se debe tener en **cuenta que los estos mitigan el riesgo de forma acumulativa, esto quiere decir que** una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

Nota: En caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente, es importante señalar que no será posible su movimiento en la matriz para el impacto.

Riesgo de corrupción

Posibilidad de que, por acción u omisión, se une el poder para desviar la gestión de lo público hacia un beneficio privado.

La definición del escenario de riesgo de corrupción debe tener la siguiente estructura:

Acción u Omisión + Uso del Poder + Desviación de la Gestión de lo Público + Beneficio Privado

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. Está asociado con la selección del parámetro de impacto.

16. Nivel de calificación de probabilidad para riesgos de corrupción

Tabla 6. Calificación de Probabilidad para riesgos de corrupción

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

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, v6 - Dirección de Gestión y Desempeño Institucional, noviembre 2022.

17. Riesgos de corrupción

En cuanto al impacto para los riesgos de corrupción se realiza aplicando la tabla de valoración establecida por la Secretaría de Transparencia de la Presidencia de la República. El riesgo identificado es valorado teniendo en cuenta las preguntas, la

tabla y la calificación obtenida se compara con la medición de impacto de riesgo de corrupción para obtener el nivel de impacto del riesgo.

Tabla 7. Calificación del Impacto para los riesgos de Corrupción

| 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 la misión del sector al que pertenece la entidad? | | | |
| 4 | ¿Generar pérdida de confianza de la entidad, afectando su reputación? | | | |
| 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? | | | |
| Nivel | Descriptor | Descripción | Respuestas afirmativas | |
| 1 | Moderado | Genera medianas consecuencias sobre la entidad. | 1 a 6 | |
| 2 | Mayor | Genera altas consecuencias sobre la entidad. | 6 a 11 | |
| 3 | Catastrófico | Genera consecuencias desastrosas para la entidad | 12 a 19 | |

Fuente: Secretaría de Transparencia de la Presidencia de la República

Nota: Si la pregunta numero 16 es afirmativa, el riesgo se considera catas tórico. Por cada riesgo de corrupción identificado, se debe de diligencia una tabla.

18. Análisis del impacto en riesgos de corrupción

Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles “moderado”, “mayor” y “catastrófico”, dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que sí aplican para los demás riesgos. Por último, ubique en el mapa de calor el punto de intersección resultante de la probabilidad y el impacto para establecer el nivel del riesgo inherente.

| RESULTADOS DE LA CALIFICACIÓN DEL RIESGO DE CORRUPCIÓN | | | | |
|--|---------|------------------------------|-------|--------------|
| PROBABILIDAD | PUNTAJE | Zona de Riesgo de Corrupción | | |
| Casi seguro | 5 | | | |
| Probable | 4 | | | |
| Posible | 3 | | | |
| Imposible | 2 | | | |
| Rara vez | 1 | | | |
| Impacto | | Moderado | Mayor | Catastrófico |

Fuente: Secretaría de Transparencia de la Presidencia de la República

IMPORTANTE: Aunque se utilice el mismo mapa de calor para los riesgos de gestión y corrupción, a estos últimos solo se les aplican las columnas de impacto Moderado, Mayor y Catastrófico.

19. Criterios para la evaluación de impacto de pérdida de continuidad

La determinación de las prioridades de recuperación de servicios en caso de materialización de escenarios de pérdida de continuidad de negocio se realiza mediante la valoración del impacto percibido por los líderes de los procesos. Mediante mesa de trabajo los participantes califican los impactos en cada variable y definen el orden de recuperación de los servicios asignando la secuencia de reactivación de los mismos primero a los servicios con mayor impacto y de manera secuencial a los servicios con menor impacto percibido.

Tabla 8. Criterios para la evaluación de impacto de pérdida de continuidad

| Criterio | Descripción |
|----------|-------------|
|----------|-------------|

| | |
|-----------------------|---|
| Financiero | Nivel de pérdidas económicas |
| Reputacional | Nivel de pérdida de la confianza de los grupos de valor. |
| Legal/ Regulatorio | Nivel de incumplimiento de normas y regulaciones que está sometida la entidad. |
| Contractual | Impactos asociados al incumplimiento de cláusulas en obligaciones contractuales. |
| Misional | Nivel de incumplimiento o impacto percibido por imposibilidad de cumplir los objetivos y obligaciones misionales. |

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas v6

20. Acciones ante los riesgos materializados

Ante la materialización de un riesgo se deberá medir el impacto y las consecuencias que puede ocasionar afectaciones a los objetivos de la Entidad, se revisarán y ajustarán los controles asociados determinando el grado de efectividad, eficiencia o eficacia, que garantice la mitigación de la ocurrencia. Para adelantar el análisis del riesgo y sus controles se deben considerar los siguientes aspectos:

- **Calificación del riesgo:** se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo.
- **Bajo el criterio de probabilidad:** el riesgo se debe medir a partir de la cantidad de veces que se ejecuta cada una de sus acciones.

Se deberán tomar las medidas encaminadas a prevenir la ocurrencia como primera alternativa a considerar, se logra cuando al interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de ajustes en los controles y acciones emprendidas.

21. Acciones a seguir en caso de materialización de riesgos de corrupción

En el evento de materializarse un riesgo de corrupción, es necesario realizar los ajustes necesarios con acciones, tales como:

- Informar a las autoridades de la ocurrencia del hecho de corrupción.
- Revisar el mapa de riesgos de corrupción, en particular, las causas, riesgos y controles.
- Verificar si se tomaron las acciones y se actualizó el mapa de riesgos de corrupción.
- Llevar a cabo un monitoreo permanente.

La Oficina de Control Interno debe asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma oportuna y efectiva.

Las acciones adelantadas se refieren a:

- Determinar la efectividad de los controles.
- Mejorar la valoración de los riesgos.
- Mejorar los controles.
- Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción.
- Determinar si se adelantaron acciones de monitoreo.
- Revisar las acciones del monitoreo.

Cuando se materializan riesgos identificados en la matriz de riesgos institucionales se deben aplicar las acciones descritas en la tabla “acciones de respuesta a riesgos”.

Tabla 9. Acciones de respuesta a riesgos

| Tipo de riesgo | Responsable | Acción |
|--|----------------------------|---|
| Riesgo de corrupción | Líder del Proceso | <ul style="list-style-type: none"> • Comunicar a la Oficina Asesora de Planeación como segunda línea de defensa en el tema de riesgos sobre el posible hecho encontrado • Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), determinar la aplicabilidad del proceso disciplinario. • Identificar las acciones correctivas necesarias y documentarlas en el plan de mejoramiento. • Efectuar el análisis de causas y determinar acciones preventivas y de mejora. Revisar los controles existentes y actualizar el mapa de riesgos. |
| | Oficina de Control Interno | <ul style="list-style-type: none"> • Informar al líder del proceso y a la segunda línea de defensa, quienes analizarán la situación y definirán las acciones a que haya lugar. • Una vez surtido el conducto regular establecido por la entidad y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), determinar la aplicabilidad del proceso disciplinario. • Informar a discreción los posibles actos de corrupción al ente de control. |
| Riesgos de Gestión y Seguridad Digital | Líder del Proceso | <ul style="list-style-type: none"> • Informar a la Oficina Asesora de Planeación como segunda línea de defensa, el evento o materialización de un riesgo. • Proceder de manera inmediata a aplicar el plan de contingencia o de tratamiento de incidentes de seguridad de la información que permita la continuidad del servicio o el restablecimiento de este |

| | | |
|--|-----------------------------------|---|
| | | <p>(si es el caso) y documentar en el plan de mejoramiento.</p> <ul style="list-style-type: none"> Realizar los correctivos necesarios frente al cliente e iniciar el análisis de causas y determinar acciones correctivas, preventivas, y de mejora, así como la revisión de los controles existente, documentar en el plan de mejoramiento institucional y actualizar el mapa de riesgos. Dar cumplimiento al procedimiento plan de mejoramiento |
| Riesgos de Gestión y Seguridad Digita | Oficina de Control Interno | <ul style="list-style-type: none"> Comunicar al líder del proceso sobre el hecho encontrado. 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. Realizar la verificación de las acciones que se tomen y que actualice el mapa de riesgos correspondiente. Si la materialización de los riesgos es el resultado de una auditoría realizada por la Oficina de Control Interno, esta verificará el cumplimiento del plan de mejoramiento y realizará el seguimiento de acuerdo con el procedimiento. |
| Riesgos de Continuidad del Negocio | Subcomité de Riesgo | Activar Plan de Acción o Contingencia. |

22. Seguimiento a mapa de riesgos y controles

Tabla 10. Seguimiento riesgos y controles

| Tipo de Riesgo | Zona de Riesgo Residual | Estrategia de Tratamiento de Controles |
|---|--------------------------------|---|
| Riesgos de Gestión y Seguridad Digital | BAJA | Se realiza seguimiento a los controles con periodicidad SEMESTRAL y se registran sus avances |
| | MODERADA | Se realiza seguimiento a los controles con periodicidad TRIMESTRAL y se registran sus avances |
| | ALTA | Se realiza seguimiento a los controles con periodicidad BIMESTRAL y se registran sus avances |

| | | |
|------------------------------|---|---|
| | EXTREMA | Se realiza seguimiento a los controles con periodicidad MENSUAL |
| Riesgos de Corrupción | Todos los riesgos de corrupción, independiente de la zona de riesgo en la que se encuentran debe tener un seguimiento MENSUAL | |

23. Estrategia de seguimiento al plan de acción

Tabla 11. Seguimiento plan de acción

| Tipo de Riesgo | Zona de Riesgo Residual | Estrategia de Tratamiento de Controles |
|---|-----------------------------|--|
| Riesgos de Gestión y Seguridad Digital | BAJA | No se debe realizar plan de acción porque está dentro del nivel de aceptación del riesgo por la entidad. |
| | MODERADA ALTA EXTREMA | <p>El líder del proceso define acciones que permita mitigar el riesgo residual. Asimismo, determina la fecha de inicio y finalización de estas y establece los seguimientos que va a realizar durante la ejecución de la acción correspondiente a su avance, el cual se debe reportar junto con el seguimiento al mapa de riesgo y controles.</p> <p>Después de haber implementado la acción debe realizar un seguimiento con el fin de evaluar la efectividad del plan de acción.</p> |

24. Referencias

- Guía de administración de riesgos del DAFP

https://www1.funcionpublica.gov.co/documents/28587410/34299967/Guia_administracion_riesgos_capitulo_riesgo_fiscal.pdf

- Instructivo metodología de Riesgos

[Instructivo de la metodología de riesgos para los usuarios del Sistema de Gestión Institucional](#)

- Manual Operativo del Modelo Integrado de Planeación y Gestión

https://www1.funcionpublica.gov.co/documents/34645357/34702994/Modelo_integrado_planeacion_gestion.pdf/7f3d55ea-4ad6-3bdc-3f05-a23d287ca69b?t=1615223466439