TABLA DE CONTENIDO

1. OBJETIVO

Establecer una orientación metodológica que permita ejercer una correcta y eficiente administración de los riesgos de la Entidad, a través de la implementación de políticas, procedimientos y controles que logren mitigar la probabilidad de ocurrencia de aquellos eventos que puedan afectar negativamente el logro de los objetivos institucionales, y se oriente a la calidad de los procesos, sus servidores y apoyar la toma de decisiones de la alta dirección.

2. ALCANCE

La administración del riesgo en el Instituto de Desarrollo urbano, vivienda y gestión territorial de Chía, cuenta con un carácter prioritario y estratégico fundamentada en el desarrollo de la operación por procesos. Inicia con la actualización del contexto estratégico para la identificación de los riesgos, el análisis, valoración, plan de manejo, consolidación, seguimiento y publicación de resultados, donde los líderes de proceso son los responsables de la identificación, valoración y tratamiento de los riesgos asociados a las actividades de los procesos.

3. TERMINOS Y DEFINICIONES[1]

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.
Apetito de 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 de 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
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.
Control: Medida que permite reducir o mitigar un riesgo.
Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados
Capacidad de riesgo: Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.
Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.
Factores de Riesgo: Son las fuentes generadoras de riesgos.
Impacto: las consecuencias que puede ocasionar a la organización la materialización del riesgo.
Integridad: Propiedad de exactitud y completitud.

[1] FUNCIÓN PÚBLICA. Guía para la administración del riesgo y el diseño de controles en Entidades públicas. Bogotá, 2020. Página 12

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

Plan Anticorrupción y de Atención al Ciudadano: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

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.

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

Nota: 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 Corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado

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 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.

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

Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

4. MARCO LEGAL

Ley 87 de 1993: Por la cual se establecen normas para el ejercicio del control interno en las Entidades y organismos del Estado y se dictan otras disposiciones.

Ley 1474 de 2011: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

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 y se dictan otras disposiciones.

Directiva presidencial 09 de 1999: Por medio de la cual se adoptan lineamientos para la implementación de la Política de lucha contra la corrupción.

Decreto 1083 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del sector de Función Pública.

Decreto 1499 de 2017: Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

5. ROLES Y RESPONSABILIDADES

5.1. Línea estratégica de defensa

Rol principal: Analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento de los planes estratégicos, así como definir el marco general para la gestión del riesgo (política de administración de riesgos) y el cumplimiento de los planes de la Entidad.

Conformada por: Alta dirección y Comité Institucional de Coordinación de Control Interno.

Aspectos claves:

- 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.
- 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.
- Evaluación de la política de gestión estratégica del Talento Humano (forma de provisión de los cargos, capacitación, código de Integridad, bienestar).

5.2. Primera línea de defensa

Rol principal: Diseñar, implementar y monitorear los controles, además de gestionar de manera directa en el día a día los riesgos de la Entidad. Así mismo, orientar el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la Entidad y emprender las acciones de mejoramiento para su logro.

Conformada por: A cargo de los líderes de proceso, programas y proyectos de la Entidad y de sus equipos de trabajo.

Aspectos claves:

- 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 su seguimiento, acorde con el diseño de dichos controles, evitando la materialización de los riesgos.
- El seguimiento a los indicadores de gestión de los procesos e institucionales, según corresponda.

- La formulación de planes de mejoramiento, su aplicación y seguimiento para resolver los hallazgos presentados.
- La coordinación con sus equipos de trabajo, 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.

5.3. Segunda línea de defensa

Rol principal: Asegurar que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente, supervisar la implementación de prácticas de gestión de riesgo eficaces; así mismo, consolidar y analizar información sobre temas clave para la Entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos, todo lo anterior enmarcado en la "autogestión"

Conformada por: Servidores que ocupan cargos del nivel directivo o asesor (media o alta gerencia), quienes realizan labores de supervisión sobre temas transversales para la entidad y rinden cuentas ante la Alta Dirección.

Aspectos claves:

- Aseguramiento de que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente, supervisan la implementación de prácticas de gestión de riesgo eficaces.
- Consolidación y análisis de información sobre temas claves para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos.
- Trabajo coordinado con las oficinas de control interno o quien haga sus veces, en el fortalecimiento del Sistema de Control Interno.
- Asesoría a la 1ª línea de defensa en temas clave para el Sistema de Control Interno: i) riesgos y controles; ii) planes de mejoramiento; iii) indicadores de gestión; iv) procesos y procedimientos.
- Establecimiento de los mecanismos para la autoevaluación requerida (auditoría interna a sistemas de gestión, seguimientos a través de herramientas objetivas, informes con información de contraste que genere acciones para la mejora).

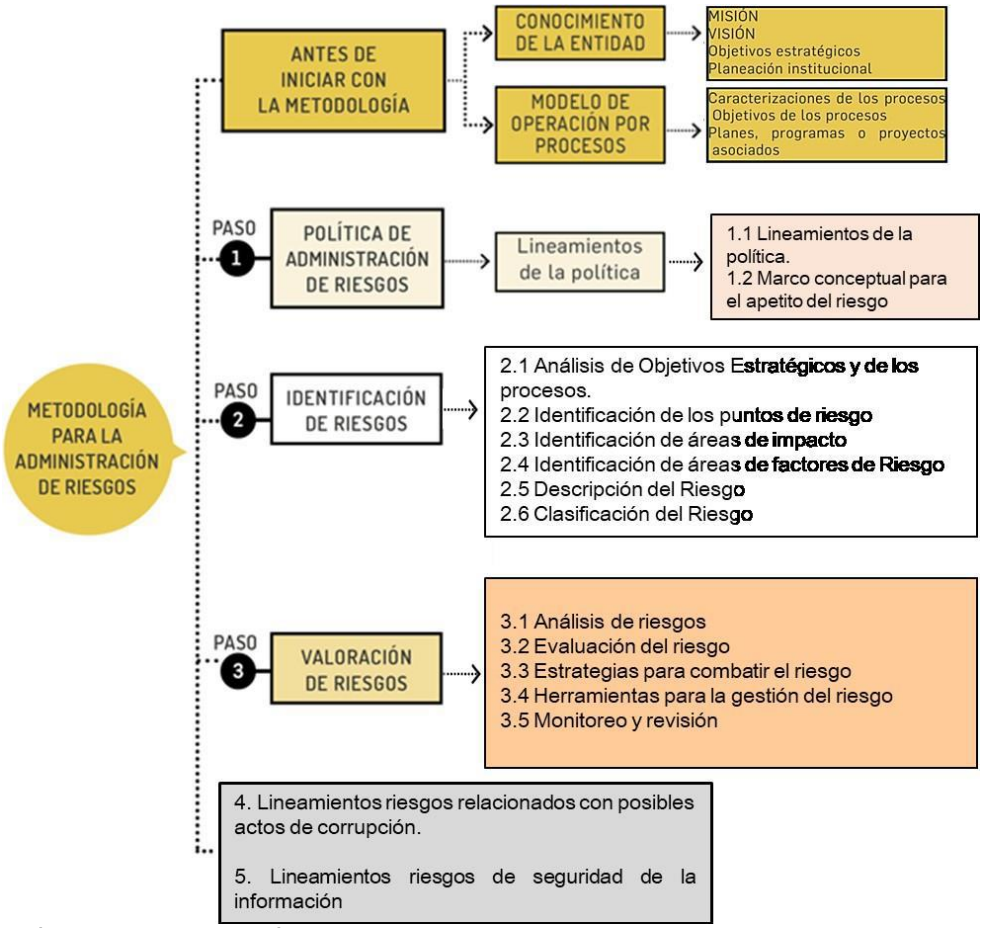
5.4. Tercera línea de defensa

Rol principal: Liderazgo estratégico, enfoque hacia la prevención, evaluación de la gestión del riesgo, relación con entes externos de control y evaluación y seguimiento.
Conformada por: Oficina de Control Interno, quienes evalúan de manera independiente y objetiva los controles de 2ª línea de defensa para asegurar su efectividad y cobertura; así mismo, evalúa los controles de 1ª línea de defensa que no se encuentren cubiertos y los que inadecuadamente son cubiertos por la 2ª línea de defensa.

Aspectos claves:

- A través de su rol de asesoría, orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Oficina Asesora de Planeación o quien haga sus veces se garantiza el cumplimento efectivo de los objetivos.
- 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.
- Formar a la alta dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos.
- Informar los hallazgos y proporcionar recomendaciones de forma independiente.

6. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO



Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades públicas" Versión 05 de Dic de 2020

7. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

El objetivo de la política de administración del riesgo en el Instituto de Desarrollo Urbano, Vivienda y Gestión Territorial de Chía (IDUVI), es preservar la eficacia estratégica y

operativa a través de la identificación, análisis, valoración, control, monitoreo y actualización de los riesgos relacionados al desarrollo de su Misión y el cumplimiento de sus objetivos institucionales.
Esta política tiene un alcance de aplicabilidad para todos los procesos del Instituto de Desarrollo Urbano, Vivienda y Gestión Territorial de Chía (IDUVI) sin exclusión alguna.
La Gestión del Riesgo está dirigida a que se establezcan acciones conducentes a reducir, evitar, transferir o compartir el riesgo con base en su evaluación.
La definición del plan de manejo del riesgo debe estar encaminada a su mitigación. No obstante, se tendrá como referencia el análisis costo/beneficio para la administración de los mismos.
Los controles y las acciones contenidas en el plan de manejo son objeto de autocontrol por parte de todos los servidores públicos y/o particulares que ejercen funciones públicas, de auto seguimiento por parte del líder de proceso, así como de evaluaciones por parte de la Oficina de Control Interno.
Los riesgos de corrupción no tendrán nivel de aceptación ya que por su naturaleza será inaceptable su ocurrencia en la entidad.

8. CONTEXTO ESTRATÉGICO ORGANIZACIONAL

Para la definición del contexto estratégico organizacional es fundamental partir de la misión, los objetivos, el plan estratégico, la naturaleza de la Entidad, así como los objetivos de los procesos estratégicos, misionales, de apoyo y de evaluación; Es entonces, que el contexto estratégico es el punto de partida de una identificación eficiente de los factores tanto internos como externos, que pueden ser generadores de riesgos y que por tanto afectan negativamente en el cumplimiento de la misión y de los objetivos institucionales.
Cuando se realiza el análisis del contexto externo es necesario identificar aquellas condiciones del entorno políticas, económicas, sociales, tecnológicas, ambientales, legales, entre otras, que puedan llegar afectar tanto los objetivos de los procesos como influenciar la dinámica de los aspectos asociados a la estructura organizacional, asignación presupuestal, la gestión del talento humano, la imagen institucional, los trámites internos de la Entidad y la gestión de los procesos (Guía para la administración del riesgo y el diseño de controles en entidades públicas, 2020, p. 19)
El contexto estratégico será modificado teniendo en cuenta entre otros los siguientes factores: los resultados de los ejercicios de planeación que realice el IDUVI y afecten los objetivos del mapa estratégico, actualización o cambios en los Planes y Proyectos de la Entidad, evaluaciones del Plan Estratégico, Diagnósticos Institucionales, cambios en su estructura orgánica etc.

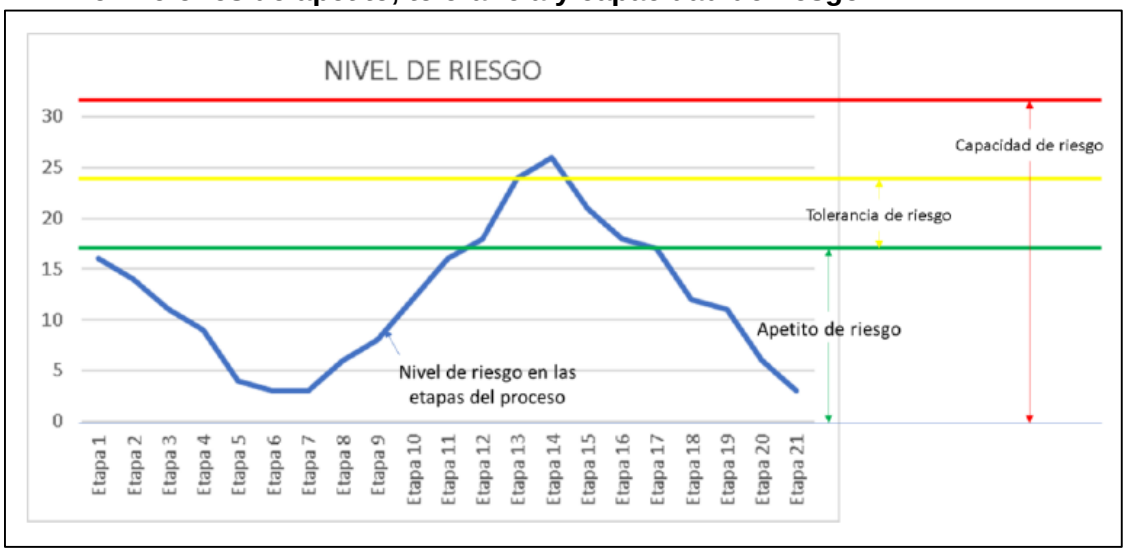
Marco conceptual para el apetito del riesgo

- **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.

Gráficamente los anteriores conceptos se relacionan así:

Definiciones de apetito, tolerancia y capacidad de riesgo



Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades públicas" Versión 05 de Dic de 2020

Determinación de la capacidad de riesgo

Para determinar la capacidad del riesgo, la Entidad, en conjunto con la alta dirección, aplica los valores de probabilidad e impacto, los cuales son sometidos a aprobación en el Comité Institucional de Gestión y Desempeño, de acuerdo con los valores establecidos en la Guía para la administración del riesgo y el diseño de controles en Entidades públicas:

a) Valor máximo de la escala que resulta de combinar la probabilidad y el impacto.
b) Valor máximo que, según el buen criterio de la alta dirección y bajo los requisitos del marco legal aplicable a la Entidad, puede ser resistido por la Entidad antes de perder total o parcialmente la capacidad de cumplir con sus objetivos. Este valor se denomina "capacidad de riesgo".

La capacidad institucional de riesgo es el máximo valor del nivel de riesgo que puede soportar la Entidad, y a partir del cual se considera por parte de la alta dirección que no sería posible el logro de los objetivos de la Entidad.

Determinación del apetito de riesgo

De igual manera la alta dirección debe determinar el valor máximo deseable del nivel de riesgo que podría permitir el logro de los objetivos institucionales en condiciones normales de operación del modelo integrado de planeación y gestión. Es decir, que el apetito de riesgo equivale al nivel de riesgo que la Entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la alta dirección, no obstante, puede ser diferente para los distintos tipos de riesgos que el instituto debe o desea gestionar.

Tolerancia de riesgo

Es el valor de la máxima desviación del nivel de riesgo admitida, con respecto al valor del apetito de riesgo determinado por el Instituto, es lo que se considera tolerancia de riesgo. La tolerancia de riesgo se determina, definiendo un valor que es igual o superior al apetito de riesgo y menor o igual a la capacidad de riesgo.

Este límite o valor de la tolerancia de riesgo es definido por la alta dirección y aprobada por el órgano de gobierno respectivo y no puede ser superior al valor de la capacidad de riesgo.

La determinación de la tolerancia de riesgo es optativa para la Entidad y su uso está limitado a determinar el tipo de acciones para abordar los riesgos, dado que las acciones que se desprendan a partir del análisis de riesgos deben ser proporcionadas y razonables, lo cual se puede determinar en función del valor del nivel de riesgo residual obtenido y su comparación con el apetito y tolerancia de riesgo.

9. IDENTIFICACIÓN DEL RIESGO

El objetivo es identificar los riesgos que estén o no bajo el control de la Entidad, teniendo en cuenta el contexto estratégico en el que opera la Entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos, aplicando las siguientes fases:

9.1. Análisis de objetivos estratégicos y de los procesos

Los riesgos identificados, deben tener impacto en los objetivos estratégicos o del proceso. Es necesario revisar que estos objetivos se encuentren alineados con la Misión y Visión institucional, así como, analizar su adecuada formulación, es decir que sea especifico, medible, alcanzable, relevante y proyectado en el tiempo.

9.2. Identificación de los puntos de riesgo

Son actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades públicas" Versión 05 de Dic de 2020

9.3. Identificación de áreas de impacto

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

9.4. Identificación de áreas de factores de riesgo

Factores de riesgo que se pueden presentar en la Entidad:

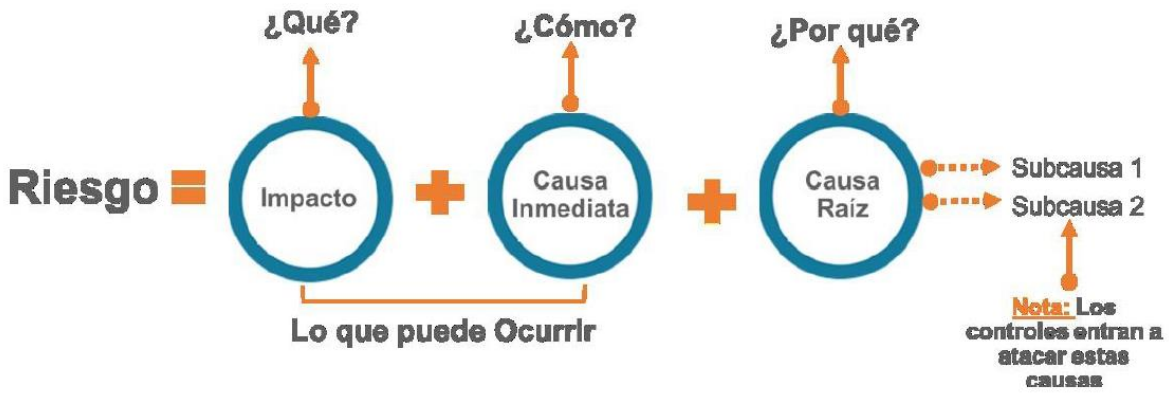
FACTOR	DEFINICIÓN	DESCRIPCIÓN
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización	- Falta de procedimientos - Errores de grabación, autorización - Errores en cálculos para pagos internos y externos - Falta de capacitación, temas relacionados con el personal.
Talento Humano	Incluye seguridad y salud en el trabajo.	- Hurto activos - Posibles comportamientos no éticos de los empleados

	Se analiza posible dolo e intención frente a la corrupción	- Fraude interno (corrupción, soborno)
Tecnología	Eventos relacionados con la infraestructura tecnológica de la Entidad	- Daño de equipos - Caída de aplicaciones - Caída de redes - Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física de la Entidad	- Derrumbes - Incendios - Inundaciones - Daños a activos fijos
Evento externo	Situaciones externas que afectan la Entidad	- Suplantación de identidad - Asalto a la oficina - Atentados, vandalismo, orden público

9.5. Descripción del riesgo

Debe contener todos los detalles necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. Se propone una estructura que facilita su redacción y claridad que inicia con la frase POSIBILIDAD DE y se analizan los siguientes aspectos:

Ilustración 6 Estructura propuesta para la redacción del riesgo



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: Es la causa principal o básica, corresponden a las razones por la 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 pueden existir más de una causa o subcausas que pueden ser analizadas.

9.6. Clasificación del riesgo

CATEGORIA	DESCRIPCIÓN
Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en *hardware*, *software*, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

10. Valoración del riesgo

La valoración del riesgo se desarrolla mediante dos elementos: El análisis y la evaluación de los riesgos.

10.1. Análisis del riesgo

Busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo inherente).

10.1.1. Determinar la probabilidad:

La probabilidad está asociada a la exposición al riesgo del proceso o actividad que se esté analizando; de tal forma que la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

	Frecuencia de la Actividad	Probabilidad frente al riesgo
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades públicas" Versión 05 de Dic de 2020

10.1.2. Determinar el impacto

Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales. Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferente nivel, se debe tomar el nivel más alto.

Criterios para definir el nivel de impacto

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

Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades públicas" Versión 05 de Dic de 2020

10.2. Evaluación de riesgos

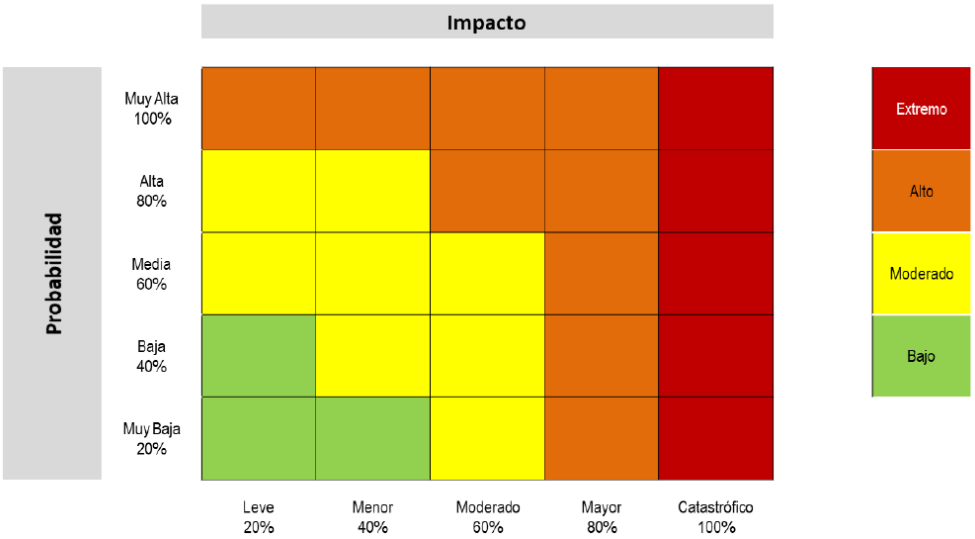
A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

10.2.1. Análisis preliminar (riesgo inherente):

Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor.

En cumplimiento a lo anterior, debe tenerse en cuenta el análisis de objetivos del proceso junto con los objetivos estratégicos de tal manera que se identifique todos los activos que deben protegerse para garantizar el funcionamiento interno con el funcionamiento de cara al ciudadano.

MATRIZ DE CALOR (Niveles de severidad del riesgo)



Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades públicas" Versión 05 de Dic de 2020

10.2.2. Valoración de controles:

En primer lugar, conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso si aplica el criterio experto.

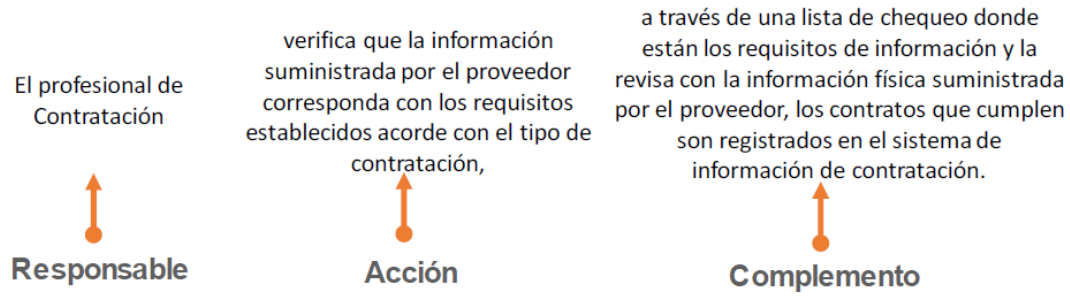
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

10.2.2.1. Estructura de 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:

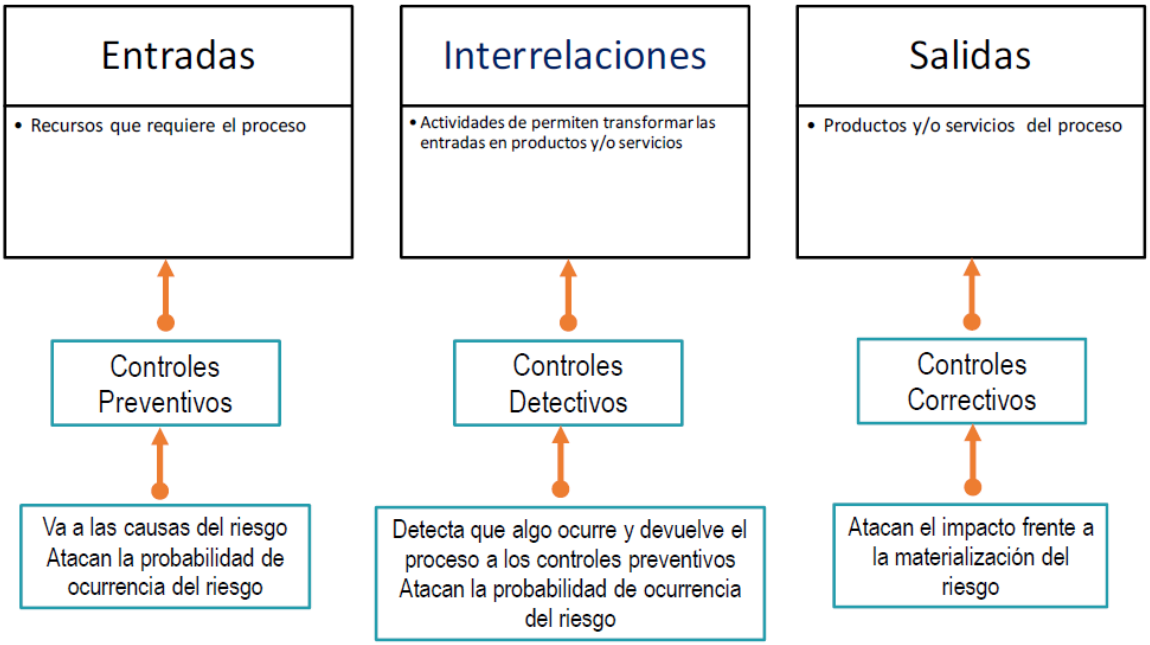
- **Responsable de ejecutar el control:** identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
- **Acción:** se determina mediante verbos que indican la acción que deben realizar como parte del control.
- **Complemento**: corresponde a los detalles que permiten identificar claramente el objeto del control.

Ejemplo:



10.2.2.2. Tipología de controles y los procesos:

Para realizar con más precisión la tipología y la clasificación del tipo de control, es necesario conocer y ejecutar el proceso, para así establecer en qué momento se activa un control y definir su tipo.



Acorde con lo anterior, tenemos las siguientes tipologías de controles:

- **Control preventivo:** control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.
- **Control detectivo:** control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- **Control correctivo:** control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

Así mismo, de acuerdo con la forma como se ejecutan tenemos:

- **Control manual:** controles que son ejecutados por personas.
- **Control automático:** son ejecutados por un sistema.

10.2.2.3. Análisis y evaluación de los controles – Atributos:

A continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización.

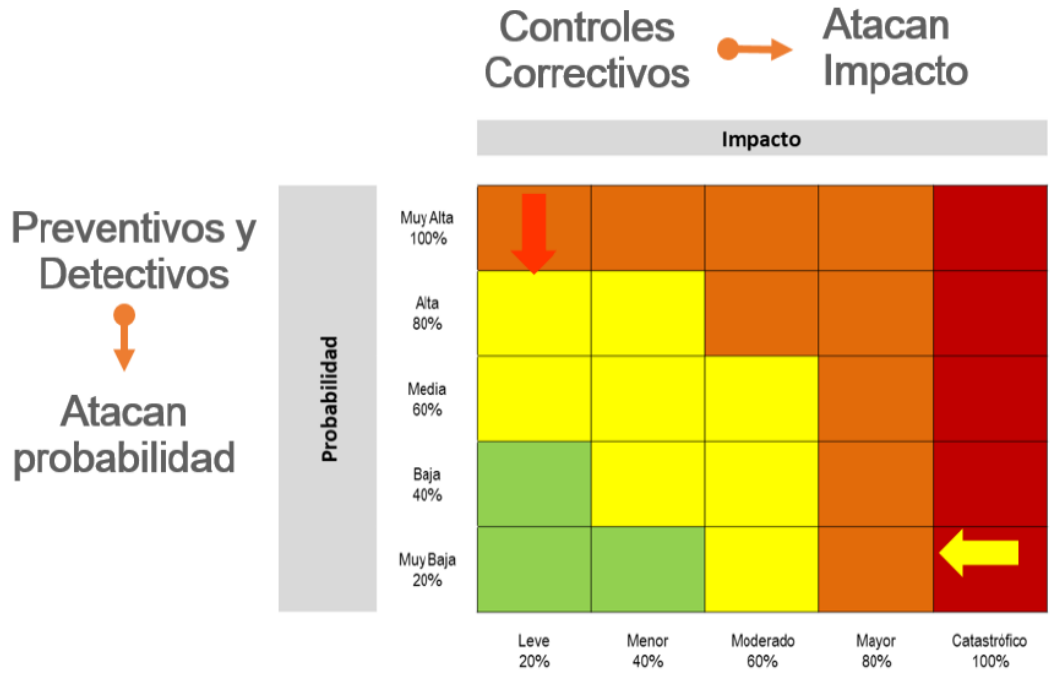
Características			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado	25%

		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos	15%
		Correctivo	Dado que 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 el error humano.	15%
Atributos informativos	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	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatorio	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-

	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.
Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor que corresponde a la figura 14 se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

Movimiento en la matriz de calor acorde con el tipo de control



Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades públicas" Versión 05 de Dic de 2020

10.2.3. Nivel de riesgo (riesgo residual)

En esta etapa se obtiene el riesgo residual, el cual es el resultado de aplicar la efectividad de los controles al riesgo inherente.

De acuerdo con lo estipulado en la Guía para la administración del riesgo y el diseño de controles en Entidades públicas 2020, para la aplicación de los controles se debe tener en cuenta que 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.

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

Aplicación de controles para establecer el riesgo residual

Riesgo	Datos relacionados con la probabilidad e impacto inherentes		Datos valoración de controles		Cálculos requeridos
Posibilidad de pérdida económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.	Probabilidad inherente	60%	Valoración control 1 preventivo	40%	60%* 40% = 24% 60% - 24% = **36%**
	Valor probabilidad para aplicar 2º control	36%	Valoración control 2 detectivo	30%	36%* 30% = 10,8% 36% - 10,8% = **25,2%**
	Probabilidad Residual	**25,2 %**			
	Impacto Inherente	80%			
	No se tienen controles para aplicar al impacto	N/A	N/A	N/A	N/A
	Impacto Residual	**80%**			

Fuente: Guía para la administración del riesgo y el diseño de controles en Entidades públicas Versión 5 - diciembre de 2020. Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020

10.3. Estrategias para combatir el riesgo

Decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar. Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.

Los líderes de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la Entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento.

- **Aceptar:** Después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo conociendo los efectos de su posible materialización.
- **Evitar:** Después de realizar un análisis y considerar que el nivel de riesgo es demasiado alto, se determina NO asumir la actividad que genera este riesgo.
- **Reducir:** Después de realizar un análisis y considerar que el nivel de riesgo es alto, se decide tratarlos mediante transferencia o mitigación del riesgo.
    - **Transferir:** Después de realizar un análisis se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.
    - **Mitigar:** Después de realizar un análisis y considerar los niveles de riesgo se implementan acciones que mitiguen el nivel de riesgo. No necesariamente es un control adicional.

10.4. Herramientas para la gestión del riesgo

Se contará con el mapa de riesgos como herramienta para la gestión del riesgo.

10.4.1. Gestión de eventos

Un evento es un riesgo materializado, se pueden considerar incidentes que generan o podrían generar pérdidas a la entidad, se debe contar con una base histórica de eventos que permita revisar si el riesgo fue identificado y qué sucedió con los controles. En caso de que el riesgo no se hubiese identificado, se debe incluir y dar el tratamiento correspondiente de acuerdo con la metodología.

10.4.2. Indicadores claves de riesgo

Hace referencia a colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados riesgos.

10.5. Monitoreo y revisión

Se adelanta, teniendo en cuenta la dimensión 7 Control interno del Modelo integrado de planeación y gestión – MIPG referente a las líneas de defensa mediante las cuales se identifica la responsabilidad de la gestión del riesgo y control.

El proceso debe revisar y actualizar el mapa de riesgos cuando se presenten cambios en su objetivo, alcance y/o actividades, o cuando el contexto estratégico presente un cambio significativo que requiera la revisión completa de los riesgos gestionados, teniendo como mínimo una revisión y/o actualización anual a partir de la última fecha de revisión.

Los riesgos pueden actualizarse de manera individual, cuando se identifique la necesidad por medio de auditorías internas, revisión por la dirección, auditorías externas o resultado de las acciones de seguimiento y autocontrol ejecutadas por los líderes de proceso.

Si como resultado de la autoevaluación o auto seguimiento por parte del líder del proceso y/o del seguimiento por parte de la OCI un riesgo se materializa, es fuente para la realización de una acción correctiva y debe ser incluida en el plan de mejoramiento, de acuerdo con los lineamientos contenidos en procedimiento Acciones correctivas preventivas y de mejora para evitar o disminuir la probabilidad de que vuelva a suceder.

11. Gestión de los riesgos relacionados con posibles actos de corrupción

El riesgo de corrupción se define como la posibilidad de que por acción u omisión se use el poder para desviar la gestión de lo público hacia un beneficio privado.

En la descripción del riesgo deben concurrir los siguientes componentes:

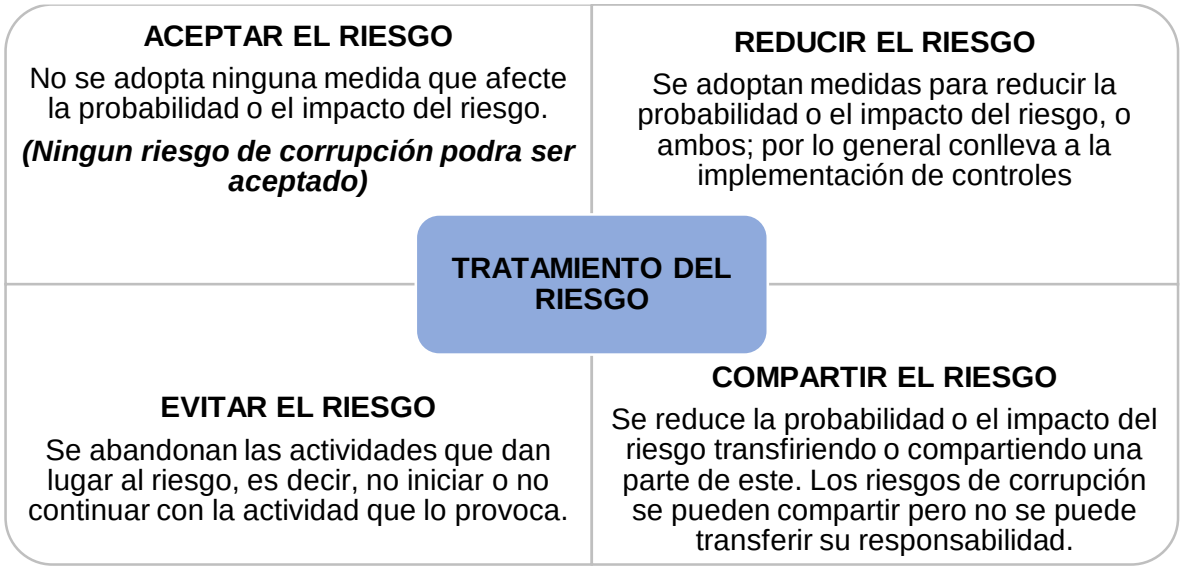
Acción u omisión	+	*Uso del poder*	+	*Desviación de la gestión de lo público*	+	*El beneficio privado*

Se elabora anualmente por el líder de cada proceso, junto con su equipo de trabajo y la consolidación está a cargo de la oficina de planeación quien a su vez debe velar por que este sea publicado en la página web de la entidad, en la sección de Transparencia y acceso a la información pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año.

- **Ajustes y modificaciones:** Se podrán realizar ajustes y modificaciones necesarias orientadas a mejorar el mapa de riesgos de corrupción; y en este caso, deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.
- **Monitoreo:** Estará a cargo de los líderes de los procesos, junto con su equipo, quienes deben realizar monitoreo y evaluación permanente a la gestión de riesgos de corrupción.
- **Seguimiento:** A cargo del jefe de control interno o quien haga sus veces. Dentro de sus procesos de auditoria interna debe analizar las causas los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de 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.
Así mismo, es importante tener en cuenta que para los riesgos de corrupción solamente hay disminución de la probabilidad, y que el impacto sigue siendo igual.

Tratamiento del riesgo



Fuente: Departamento administrativo de la Función pública

BIBLIOGRAFIA

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA – DAFP (2020). Guía para la administración del riesgo y el diseño de controles en entidades Públicas. V5

DEPARTAMENTO NACIONAL DE PLANEACIÓN – DNP (2015) Estrategias para la construcción del Plan Anticorrupción y de Atención al ciudadano.

CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN
1	**30/11/2015**	Creación del documento acorde con los lineamientos para el Sistema de gestión de la calidad.
2	**30/09/2016**	Modificación de calificación y valoración de los controles, se incluye el tratamiento de riesgos de seguridad digital e identificación de activos.
3	**22/02/2019**	Actualización de la Guía para la administración de los riesgos de gestión, corrupción y seguridad digital, y el diseño de controles en entidades públicas, se hicieron cambios en la guía de administración del riesgo de la entidad.
4	**28/09/2021**	Se actualiza el documento de acuerdo a Guía para la administración del riesgo y el diseño de controles en entidades públicas – versión 5.

APROBACIÓN

PROYECTÓ Y REVISÓ	APROBÓ
Cargo: Profesional Universitario – Encargado del SGC	**Cargo:** jefe Oficina Asesora de Planeación
Firmado en original **Firma:**	Firmado en original **Firma:**