TABLA DE CONTENIDO

1.OBJETIVO
2.ALCANCE
3.DESARROLLO

1. OBJETIVO

Establecer lineamientos y parámetros para una adecuada gestión y control de los riesgos asociados a los procesos, planes, programas y proyectos, que le permitan a la Agencia de Desarrollo Rural - ADR asegurar de manera razonable el cumplimiento de la misión, los objetivos institucionales, la continuidad de la gestión institucional y mejora continua en los procesos.

2. ALCANCE

La Política de Administración del Riesgos de la Agencia de Desarrollo Rural - ADR, es aplicable a todos sus procesos, planes, programas y proyectos a nivel central y territorial, también para las actividades realizadas directamente o aquellas relacionadas con los procesos misionales que se adelantan a través de terceros.

Así mismo, está alineada con la planeación estratégica institucional, en la medida que permite identificar, prevenir y mitigar posibles riesgos que puedan afectar la consecución de la misión y visión institucional y los objetivos estratégicos, a la vez que, facilita la ejecución del modelo operativo de la Agencia y la operación del Sistema Integrado de Gestión.

De la misma manera, esta política será el insumo base para el componente "Gestión del Riesgo de Corrupción - Mapa de Riesgos de Corrupción" del Plan Anticorrupción y de Atención al Ciudadano, y del mapa de riesgos del Sistema de Gestión de Seguridad de la Información - Seguridad Digital, puesto que esta política incluye los lineamientos a los riesgos de seguridad de la información.

3. DESARROLLO

TERMINOS Y DEFINICIONES

A continuación, se relacionan una serie de conceptos, necesarios para la comprensión de la metodología que se desarrolla en esta política, los cuales fueron tomados de la "Guía para la administración del riesgo y el diseño de controles en entidades públicas" - Versión 5

- Activo: En una Entidad se les llama a los activos el conjunto de bienes económicos y derechos que posee. 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.

- Administración del riesgo: Comprende el conjunto de Elementos de Control y sus interrelaciones, para que la institución evalúe e intervenga aquellos eventos, tanto internos como externos, que puedan afectar de manera negativa el logro de sus objetivos institucionales. La administración del riesgo contribuye a que la entidad consolide su Sistema de Control Interno y a
que se genere una cultura de Autocontrol y autoevaluación al interior de la misma.

- Amenaza: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a la organización.

- Análisis de riesgo: Elemento de control que permite establecer la probabilidad de ocurrencia del riesgo y el impacto o consecuencias, calificándolo y evaluándolo a fin de determinar la capacidad de la entidad pública para su aceptación y manejo. Se debe llevar a cabo un uso sistemático de la información disponible para determinar qué tan frecuentemente pueden ocurrir eventos específicos y la magnitud de sus consecuencias.

- Apetito de riesgo: Es la capacidad que tiene una organización para asumir los riesgos en la búsqueda del cumplimiento de 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.

- 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.

- 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 y podría constituir 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.

- Ciberseguridad: Conjunto de medidas de protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.

- Confidencialidad: Pilar de seguridad de la información, que consiste en la propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

- 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.

- Control detectivo: Controles que están 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 decisiones correspondientes.

- Control preventivo: Controles que están diseñados para evitar un evento no deseado en el momento en el que se produce. Este tipo de controles intenta evitar la ocurrencia de los riesgos que puedan afectar el cumplimiento de los objetivos.

- Control interno: Es el proceso que por el esquema de organización y el conjunto de los planes, métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por una entidad, procura que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con las normas constitucionales y legales vigentes dentro de las políticas trazadas por la dirección y en atención a las metas u objetivos previstos.

- Corrupción: Uso del poder para desviar la gestión de lo público hacia el beneficio privado.

- Criterio de frecuencia: Criterio para medir la probabilidad de ocurrencia, analizando el número de eventos en un periodo determinado, los hechos que se han materializado y el historial de situaciones o eventos asociados al riesgo.

- DAFP: Sigla para referirse al Departamento Administrativo de la Función Pública. Disponibilidad: Pilar de seguridad de la información, que consiste en la propiedad de ser accesible y utilizable a demanda por una entidad.

- Evaluación del riesgo: Proceso utilizado para determinar las prioridades de la administración del riesgo, comparando el nivel de un determinado riesgo con respecto a un estándar determinado.

- Evento: Es un incidente o acontecimiento procedente de fuentes internas o externas que afecta la consecución de objetivos y que puede tener un impacto negativo o positivo o de ambos tipos a la vez.

- Experticia: Habilidad o conocimiento especial o habilidad o conocimiento de un experto en un tema, actividad o arte específico.

- Factor de riesgo: Son las fuentes generadoras de riesgos. Es cualquier circunstancia, situación, elemento, proceso, al que se encuentra expuesta la Entidad y que de producirse se materializa en un evento.

- Gestión del riesgo de corrupción: Proceso efectuado por la Alta Dirección de la Entidad y por todo el personal para eliminar la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

- Identificación del riesgo: Elemento de control, que posibilita conocer los eventos potenciales, estén o no bajo el control de la entidad pública, 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: Consecuencias que puede ocasionar a la organización la materialización del riesgo.

- Integridad: Pilar de seguridad de la información, que consiste en la propiedad de exactitud y completitud.

- Modelo de líneas de defensa: 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.

- Mapa de riesgos: Documento con la información resultante de la gestión del riesgo.

- Mapa de calor: Herramienta visual empleada para ubicar el nivel de riesgo, a partir del punto de intersección entre su nivel de probabilidad de ocurrencia y su nivel de impacto.

- Monitoreo: Comprobación, supervisión, observación o registro de la forma en que se lleva a cabo una actividad con el fin de identificar sus posibles cambios.

- 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 de impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general, la fórmula de cálculo del Nivel del Riesgo puede ser la Probabilidad multiplicada por el 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 como 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 período de 1 año.

- Riesgo: Posible evento que puede afectar los objetivos del proceso o alguno de los objetivos institucionales. 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 estratégico: Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad. Se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

- 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 gestión: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos.

- 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: Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento. Es el resultado de aplicar la efectividad de los controles al riesgo inherente.

- 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).

- Seguridad de la información: Conjunto de técnicas y métodos encaminados a la preservación de la confidencialidad, integridad y disponibilidad de la información en cualquiera de sus estados, medios de almacenamiento y/o difusión (ISO 27000:2014 Numeral 2.33. Information security).

- Seguridad informática: Es una disciplina tecnológica que se encarga de proteger la integridad y la privacidad de la información contenida o
gestionada mediante sistemas informáticos.

- SIG: Sigla para referirse al Sistema Integrado de Gestión de la Agencia de Desarrollo Rural.

- Tolerancia al 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.

COPIA CONTROLADA

4. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO

La metodología aplicada para la administración de los riesgos de gestión es la contemplada en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas" versión 5, emitida por el Departamento Administrativo de la Función Pública, en diciembre de 2020, en lo referente a "Identificación del Riesgo" (numeral 2) y "Valoración del Riesgo" (numeral 3) y, para la gestión de los riesgos de corrupción, se aplicarán los "Lineamientos sobre los riesgos relacionados con posibles actos de corrupción" (numeral 4).

Para la administración de los riesgos de seguridad de la información, se aplicarán los lineamientos contenidos en el numeral 5 de la Guía antes mencionada, cuya metodología se vincula al Modelo de Seguridad y Privacidad de la Información (MSPI) implementado en la Entidad con el liderazgo de la Oficina de Tecnologías de la Información, el compromiso de la Alta Dirección y la participación activa de toda la Entidad para su implementación.

5. LINEAMIENTOS DE LA POLÍTICA

Para la adecuada gestión del riesgo se deben adelantar acciones y prácticas de trabajo para:

. La identificación y documentación de riesgos de gestión, de corrupción y fraude, y de seguridad de la información en los programas, proyectos, planes y procesos.

. El establecimiento de acciones de carácter preventivo para evitar la materialización de los riesgos identificados.

. La actuación correctiva y oportuna ante la materialización de los riesgos identificados.

. Que la administración del riesgo en la Entidad sea una herramienta estratégica usada como elemento para la toma de decisiones de todos los procesos institucionales.

. Que la gestión eficaz del riesgo deba ser considerada por los directivos y los líderes de proceso como un factor esencial para el logro de los objetivos de la Entidad.

. Que los resultados de la identificación de los riesgos, su valoración, la aplicación y evaluación de los controles, los planes de tratamiento formulados, las acciones de atención, casos de materialización de los riesgos y los riesgos residuales sean reconocidos y aceptados por cada uno de los propietarios de los riesgos.

. Que el riesgo residual sea documentado y sea sometido a monitoreo, revisión, y a tratamiento adicional cuando sea pertinente.

. Que los riesgos de seguridad de la información sean reportados a las autoridades o instancias respectivas que el gobierno disponga.

. Que se tengan presentes los informes de seguimiento de la Oficina de Control Interno y sean aceptados por los líderes de procesos y realizados los ajustes y/o planes de mejoramiento cuando haya lugar.

. Que se incluyan en la identificación y valoración de riesgos, los resultados de las evaluaciones realizadas por los organismos de control.

. El software utilizado por la Entidad, para administrar la Gestión del Riesgo es la Plataforma de Isolucion

6. RESPONSABILIDADES Y ROLES PARA LA GESTIÓN DEL RIESGO

Para definir las responsabilidades y roles para la gestión del riesgo y los controles, la Entidad adopta lo contemplado en la "7ª. Dimensión: Control Interno" del Modelo Integrado de Planeación y Gestión - MIPG, a través del funcionamiento de las líneas de defensa y su articulación, como se describe a continuación:

◘ Línea Estratégica: Instancia decisoria dentro del Sistema de Control Interno, está bajo la responsabilidad de la Alta Dirección, a través del Comité Institucional de Gestión y Desempeño (CIGD) y del Comité Institucional de Coordinación de Control Interno; su rol principal es 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 del riesgo) y el cumplimiento de los planes de la entidad.

◘ Primera Línea de Defensa: Esta línea, está bajo la responsabilidad de los líderes de programas, procesos y proyectos y de sus equipos de trabajo; 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".

◘ Segunda Línea de Defensa: Esta línea, está bajo la responsabilidad, principalmente, de los Jefes de Planeación o quienes hagan sus veces, coordinadores de equipos de trabajo, comité de contratación, áreas financieras, de TIC, entre otros que respondan de manera directa por el aseguramiento de la operación; su rol principal es asegurar 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; 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".

◘ Tercera Línea de Defensa: Esta línea, está bajo la responsabilidad del Jefe de control interno; desarrollará 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.

7. IDENTIFICACION DEL RIESGO

La identificación de los riesgos, que estén o no bajo el control de la Entidad, parte de la base del conocimiento del contexto y de los factores internos y externos a la Entidad, que puedan generar eventos que afecten negativamente el cumplimiento de los objetivos de la Entidad, o puedan generar oportunidades.

Para ello, se debe tener en cuenta el contexto estratégico en el que opera la Entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

De acuerdo con la “Guía para la administración del riesgo y el diseño de controles en entidades públicas” (versión 5) emitida por el Departamento Administrativo de la Función Pública, en la etapa de identificación del riesgo se aplican las siguientes fases:

- **Análisis de objetivos estratégicos y de los procesos:** Este paso es muy importante, dado que todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico o del proceso.

Tabla 1. Análisis de objetivos.

Análisis de objetivos estratégicos	Análisis de los objetivos de procesos
La entidad debe analizar los objetivos estratégicos e identificar los posibles riesgos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso. Es necesario revisar que los objetivos estratégicos se encuentren alineados con la Misión y la Visión Institucional, así como, analizar su adecuada formulación, es decir, que contengan las siguientes características mínimas: específico, medible, alcanzable, relevante y proyectado en el tiempo (SMART por sus siglas en inglés)	Los objetivos de proceso deben ser analizados con base en las características mínimas explicadas en el punto anterior, pero además, se debe revisar que los mismos estés alineados con la Misión y la Visión, es decir, asegurar que los objetivos de proceso contribuyan a los objetivos estratégicos. A continuación, encontrará un ejemplo de análisis en el proceso de contratación: La entidad debe adquirir con oportunidad y calidad técnica, en no menos del 90%, los bienes y servicios requeridos para su continua operación.

Fuente: Función Pública, 2020

Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 pág. 28

La entidad debe analizar los objetivos estratégicos y revisar que se encuentren alineados con la misión y la visión institucionales, así como su desdoble hacia los objetivos de los procesos.

Así mismo, la entidad debe analizar los objetivos de proceso, los cuales deben estar igualmente, alineados con la misión y la visión y asegurar que contribuyan al cumplimiento de los objetivos estratégicos.

- **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.

7.1 RIESGOS DE GESTIÓN

7.1.1 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.

7.1.2 Identificación de áreas de factores de riesgo:
Son las fuentes generadoras de riesgos.
Algunos ejemplos de factores de riesgo que puede tener una entidad, se mencionan en la siguiente tabla:

Tabla 2. Factores de Riesgo

COPIA CONTROLADA

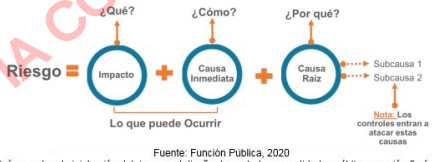
Factor	Definición		Descripción
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores de la organización.		Falta de procedimientos
			Errores de grabación, autorización
			Errores en cálculos para pagos internos y externos
			Falta de capacitación, temas relacionados con el personal
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.		Hurto activos
			Posibles comportamientos no éticos de los empleados
			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

Fuente: Función Pública, 2020
Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 pág. 31

COPIA CONTROLADA

7.1.3 Descripción del riesgo:
La descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. El DAFP propone una estructura que facilita su redacción y claridad que inicia con la frase POSIBILIDAD DE y se analizan los siguientes aspectos:

Figura 1. Estructura propuesta para la redacción del riesgo



Fuente: Función Pública, 2020
Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 pág.32

La anterior estructura evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, esta es información esencial para la definición de controles en la etapa de valoración del riesgo.

Al desglosar la estructura propuesta se tiene:

- **Impacto**: las consecuencias que puede ocasionar a la Entidad 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.

Ejemplo:

Proceso: Gestión Contractual

Objetivo: Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación

Alcance: Inicia con el análisis de necesidades para cada uno de los procesos de la entidad (plan anual de adquisiciones) y termina con las compras y contratación requeridas bajo las especificaciones técnicas y normativas establecidas.

Atendiendo el esquema propuesto para la redacción del riesgo, tenemos:

Redacción inicia con: Posibilidad de

Impacto - ¿Qué?: Afectación Económica

Causa Inmediata - ¿Cómo?: Por multa y sanción del ente regulador

Causa Raíz - ¿Por qué?: Debido a adquisición de bienes y servicios fuera de los requerimientos normativos.

Nota:
Para los Riesgos de Seguridad de la Información se podrán identificar los siguientes tres (3) riesgos inherentes:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

7.1.4 Clasificación del riesgo:
Permite agrupar los riesgos identificados. Se clasifica cada uno de los riesgos en las siguientes categorías:

Tabla 3. Clasificación de riesgos

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.

Fuente: Función Pública, 2020
Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 Pág. 35

Figura 2. Relación entre los factores de riesgo y clasificación del riesgo

Fuente: Función Pública, 2020
Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 Pág. 36

7.1.5 Valoración del Riesgo de Gestión

Consiste en establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente).

Los elementos que desarrollan la valoración del riesgo son el análisis de los riesgos (zona de riesgo inicial: Riesgo Inherente) y su evaluación (zona de riesgo final: Riesgo Residual), elementos que se describen a continuación:

- **Análisis de riesgos**: Se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

- **Probabilidad de ocurrencia del riesgo**: La probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo. Así las cosas, la probabilidad inherente será el número de veces que se pasa por el punto del riesgo en el periodo de 1 año, en la siguiente tabla se establecen los criterios para definir el nivel de probabilidad.

COPIA CONTROLADA

Tabla 4. Criterios para definir el nivel de probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 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: Función Pública, 2020
Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 Pág. 39

- **Niveles para calificar el Impacto**: Se definen los impactos económicos y reputacionales como las variables principales para establecer los criterios que determinan el nivel de impacto.

Las afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal; así como afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio, se agrupan en impacto económico y reputacional.

La siguiente tabla muestra los criterios establecidos en la Guía del DAFP para definir el nivel de impacto:

Tabla 5. 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 accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Fuente: Función Pública, 2020
Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 Pág. 40

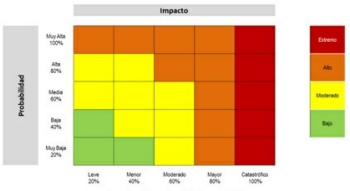
Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto. Por ejemplo: para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado.

7.1.6 Evaluación del Riesgo

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

- **Análisis preliminar (riesgo inherente)**: Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. El DAFP definió 4 zonas de severidad en una matriz de calor, así:

Figura 3. Matriz de calor (niveles de severidad del riesgo)



Fuente: Función Pública, 2020
Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 Pág. 42

El eje X (horizontal) muestra el impacto y el eje Y (vertical) la probabilidad de ocurrencia. La intersección de los datos de probabilidad e impacto, corresponde al nivel de riesgo inicial o inherente. Los colores hacen visible qué tan crítico es el riesgo en términos cualitativos, ubicando la intersección en verde si es **Bajo**, amarillo si es **Moderado**, naranja si es **Alto** o rojo si es **Extremo**.

Esta valoración del riesgo se hace con el fin de establecer prioridades para su manejo y tomar decisiones en cuanto a su tratamiento.

La forma de llevar a cabo esta valoración, consistirá en presentar a los servidores que por su conocimiento del proceso se consideren expertos, los riesgos identificados (riesgo, causas y consecuencias) para que revisen detalladamente esta información. A continuación, el servidor seleccionará la probabilidad de ocurrencia para cada una de las causas y un valor de impacto general para el riesgo, según su conocimiento y experticia.

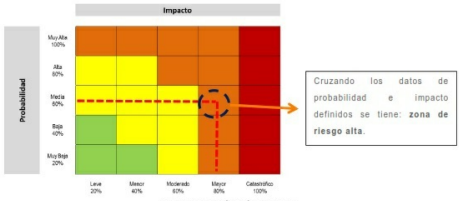
Por ejemplo, para un riesgo determinado, se obtiene la siguiente valoración, en términos de probabilidad de ocurrencia, e impacto:

Probabilidad Inherente: Media 60%

Impacto Inherente: Mayor 80%

Al cruzar los datos de probabilidad e impacto definidos, se tiene: **zona de riesgo alta**, tal como se muestra a continuación:

Figura 4. Matriz de calor (Zona de riesgo Alta)



Fuente: Función Pública, 2020
Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5 Pág. 43

COPIA CONTROLADA

7.1.7 Valoración de Controles

A partir del análisis del riesgo inicial, se identifica e implementa una o más acciones específicas, denominadas controles, que contribuyan a modificar la exposición al riesgo desde la primera línea de defensa, ya sea en la valoración de probabilidad de impacto o en la valoración de impacto.

Estructura para la descripción del control: Para una adecuada redacción del control se propone una estructura que facilita 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 aplicado bajo la estructura propuesta para la redacción del control

Responsable: El profesional de Contratación

Acción: verifica que la información suministrada por el proveedor corresponda con los requisitos establecidos acorde con el tipo de contratación,

Complemento: a través de una lista de chequeo donde están los requisitos de información y la revisa con la información física suministrada por el proveedor, los contratos que cumplen son registrados en el sistema de información de contratación.

Se tienen las siguientes tipologías de controles, teniendo en cuenta las características relacionadas con la eficiencia y la formalización. A continuación, se presenta la descripción y peso asociados a cada uno así:

• **Control preventivo**: control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, va hacia las causas del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado. Peso: **25%**

• **Control detectivo**: control accionado durante la ejecución del proceso. Estos controles detectan el riesgo y devuelve el proceso a los controles preventivos, pero generan reprocesos. Peso:**15%**

• **Control correctivo**: control accionado en la salida del proceso y después de que se materializa el riesgo. Permiten reducir el impacto de la materialización del riesgo. Estos controles tienen costos implícitos. Peso:**10%**

De acuerdo con la forma como se ejecutan tenemos:

• **Control manual**: controles que son ejecutados por personas, tiene implícito el error humano. Peso:**15%**

• **Control 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. Peso: **25%**

Tabla 6. Atributos para el diseño del Control

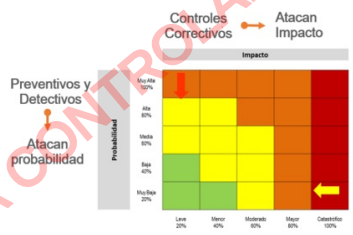
Características			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten 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.	-
		Aleatoria	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.	-

Fuente: Función Pública, 2020
Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, versión: 5 Pág. 45

Cada control identificado deberá ser valorado en términos de su efectividad sobre el riesgo, de tal forma que para cada control será necesario analizar sus atributos, teniendo en cuenta las características relacionadas con la eficiencia y la formalización, a fin de determinar si modifica a la variable de probabilidad de ocurrencia, a la variable de impacto o ambos.

Teniendo en cuenta que, es a partir de los controles que se dará el movimiento en la matriz de calor, en la siguiente figura, se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

Figura 5. Movimiento en la matriz de calor acorde con el tipo de control



Fuente: Función Pública, 2020
Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, versión: 5 Pág. 47

COPIA CONTROLADA

Como resultado de la evaluación de riesgos y análisis de los controles se originará una calificación residual para la probabilidad de ocurrencia, el impacto o ambos, determinado por el tipo de control, ocasionando el desplazamiento del riesgo dentro del mapa de calor, en sentido favorable a la Entidad.

Nota: Para mayor comprensión del análisis y evaluación de los controles, remitirse a la Guía para la administración del riesgo y el diseño de controles en entidades públicas (versión 5), emitida en diciembre de 2020 por el Departamento Administrativo de la Función Pública, numeral 3.2.2.3., en el cual se describen unos ejemplos con los que se indica cómo se determina el nivel de riesgo (riesgo residual), descrito como el resultado de aplicar la efectividad de los controles al riesgo inherente o riesgo inicial

7.2 RIESGOS DE CORRUPCIÓN

7.2.1 Descripción del riesgo:
Es la probabilidad de que, por acción u omisión, se use se use el poder para desviar la gestión de lo público hacia un beneficio privado.
"Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos" (Conpes No.167 de 2013).

Es necesario que en la descripción del riesgo concurran los componentes de su definición, así:

Figura 6. Estructura propuesta para la redacción del riesgo

ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO.

MATRIZ: DEFINICIÓN DEL RIESGO DE CORRUPCIÓN				
Descripción del riesgo	**Acción u omisión**	**Uso del poder**	**Desviar la gestión de lo público**	**Beneficio privado**
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

Fuente: Función Pública, 2020
Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, versión: 5 Pág. 64

7.2.2 Valoración del Riesgo de Corrupción

- **Análisis de la probabilidad:** Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado pero es posible que suceda.

Tabla 7. Criterios para calificar la probabilidad

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

Fuente: Función Pública, 2020
Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, versión: 5 Pág. 67

- **Análisis del Impacto:** El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo

Tabla 8. Criterios para calificar el impacto en riesgos de corrupción

N.°	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA...	RESPUESTA SÍ	RESPUESTA NO
1	¿Afectar al grupo de funcionarios del proceso?	X	
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?	X	
3	¿Afectar el cumplimiento de misión de la entidad?	X	
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		X
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?	X	
6	¿Generar pérdida de recursos económicos?	X	
7	¿Afectar la generación de los productos o la prestación de servicios?	X	
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos?		X
9	¿Generar pérdida de información de la entidad?		X
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?	X	
11	¿Dar lugar a procesos sancionatorios?	X	
12	¿Dar lugar a procesos disciplinarios?	X	
13	¿Dar lugar a procesos fiscales?	X	
14	¿Dar lugar a procesos penales?		X
15	¿Generar pérdida de credibilidad del sector?		X
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		X
17	¿Afectar la imagen regional?		X
18	¿Afectar la imagen nacional?		X
19	¿Generar daño ambiental?		X
Responder afirmativamente de UNA a CINCO pregunta(s) 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.		10	
MODERADO	Genera medianas consecuencias sobre la entidad		
MAYOR	Genera altas consecuencias sobre la entidad.		

Nivel de impacto MAYOR

COPIA CONTROLADA

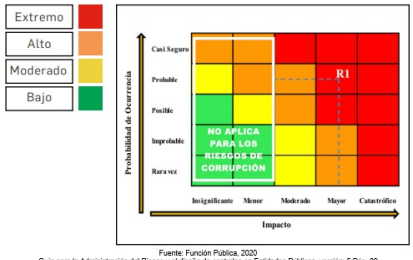
Fuente: Función Pública, 2020
Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, versión: 5 Pág. 68

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.

7.2.3 Evaluación del Riesgo

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

Figura 7. Matriz de calor (niveles de severidad del riesgo)



Fuente: Función Pública, 2020
Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, versión: 5 Pág. 69

7.2.4 Valoración de Controles

Al momento de definir si un control o controles mitigan de manera adecuada el riesgo se deben considerar, desde la redacción del mismo, las siguientes variables:

Tabla 9. Variables diseño de controles

CRITERIO DE EVALUACIÓN	ASPECTO A EVALUAR EN EL DISEÑO DEL CONTROL	OPCIONES DE RESPUESTA		
1. Responsable	¿Existe un responsable asignado a la ejecución del control?	Asignado		No asignado
		15		0
	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Adecuado		Inadecuado
		15		0
2. Periodicidad	¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna		Inoportuna
		15		0
3. Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, Ej.: verificar, validar, cotejar, comparar, revisar, etc.?	Prevenir	detectar	No es un control
		15	10	0
4. Cómo se realiza la actividad de control	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	Confiable		No confiable
		15		0
5. Qué pasa con las observaciones o desviaciones	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y resuelven oportunamente		No se investigan y resuelven oportunamente.
		15		0
6. Evidencia de la ejecución del control	¿Se deja evidencia o rastro de la ejecución del control que permita a cualquier tercero con la evidencia llegar a la misma conclusión?	Completa	Incompleta	No existe
		10	5	0

Fuente: Función Pública, 2018
Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, versión: 4 Pág. 61

- Resultados de la evaluación del diseño del control: El resultado de cada variable de diseño, a excepción de la evidencia, va a afectar la calificación del diseño del control, ya que deben cumplirse todas las variables para que un control se evalúe como bien diseñado.

Tabla 10. Rango calificación diseño del Control

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

Fuente: Función Pública, 2018
Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, versión: 4 Pág. 62

Si el resultado de las calificaciones del control, o el promedio en el diseño de los controles, está por debajo de 96%, se debe establecer un plan de acción que permita tener un control o controles bien diseñados.

- Resultados de la evaluación de la ejecución del control: Aunque un control esté bien diseñado, este debe ejecutarse de manera consistente, de tal forma que se pueda mitigar el riesgo. No basta solo con tener controles bien diseñados, debe asegurarse por parte de la primera línea de defensa que el control se ejecute.

COPIA CONTROLADA

Tabla 11. Rango calificación ejecución del Control

RANGO DE CALIFICACIÓN DE LA EJECUCIÓN	RESULTADO - PESO DE LA EJECUCIÓN DEL CONTROL -
Fuerte	El control se ejecuta de manera consistente por parte del responsable.
Moderado	El control se ejecuta algunas veces por parte del responsable.
Débil	El control no se ejecuta por parte del responsable.

Fuente: Función Pública, 2018
Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, versión: 4 Pág. 62

- Análisis y evaluación de los controles para la mitigación de los riesgos: Se consolida el conjunto de los controles asociados a las causas, para evaluar si estos de manera individual y en conjunto sí ayudan al tratamiento de los riesgos, considerando tanto el diseño, ejecución individual y promedio de los controles.
La calificación de la solidez de cada control asumirá la calificación del diseño o ejecución con menor calificación entre fuerte, moderado y débil, tal como se detalla en la siguiente tabla:

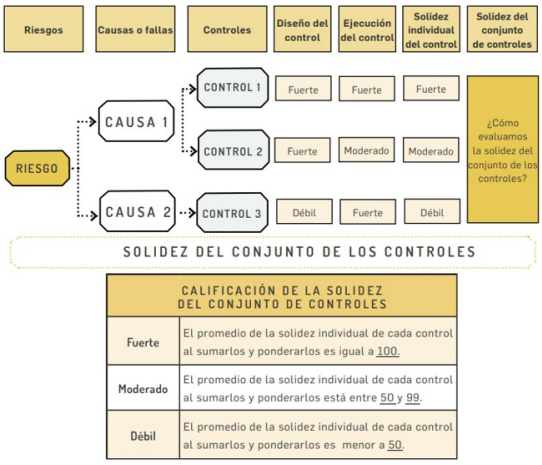
Tabla 12. Solidez individual de cada Control

PESO DEL DISEÑO DE CADA CONTROL	PESO DE LA EJECUCIÓN DE CADA CONTROL	SOLIDEZ INDIVIDUAL DE CADA CONTROL FUERTE:100 MODERADO:50 DÉBIL:0	DEBE ESTABLECER ACCIONES PARA FORTALECER EL CONTROL SÍ / NO
fuerte: calificación entre 96 y 100"	fuerte (siempre se ejecuta)	fuerte + fuerte = fuerte	No
	moderado (algunas veces)	fuerte + moderado = moderado	Sí
	débil (no se ejecuta)	fuerte + débil = débil	Sí
moderado: calificación entre 86 y 95	fuerte (siempre se ejecuta)	moderado + fuerte = moderado	Sí
	moderado (algunas veces)	moderado + moderado = moderado	Sí
	débil (no se ejecuta)	moderado + débil = débil	Sí
débil: calificación entre 0 y 85	fuerte (siempre se ejecuta)	débil + fuerte = débil	Sí
	moderado (algunas veces)	débil + moderado = débil	Sí
	débil (no se ejecuta)	débil + débil = débil	Sí

Fuente: Función Pública, 2018
Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, versión: 4 Pág. 63

- Solidez del conjunto de controles para la adecuada mitigación del riesgo: Dado que un riesgo puede tener varias causas, a su vez varios controles y la calificación se realiza al riesgo, es importante evaluar el conjunto de controles asociados al riesgo.

Figura 8. Solidez del conjunto de controles



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

Fuente: Función Pública, 2018
Guía para la Administración del Riesgo y el diseño de controles en Entidades Públicas, versión: 4 Pág. 64

7.2.5 Nivel de Riesgo Residual

Desplazamiento del riesgo inherente para calcular el riesgo residual Dado que ningún riesgo con una medida de tratamiento se evita o elimina, el desplazamiento de un riesgo inherente en su probabilidad o impacto para el cálculo del riesgo residual se realizará de acuerdo con la siguiente tabla.

Tabla 13. Posible desplazamiento despalzamiento de la Probabilidad

SOLIDEZ DEL CONJUNTO DE LOS CONTROLES.	CONTROLES AYUDAN A DISMINUIR LA PROBABILIDAD	CONTROLES AYUDAN A DISMINUIR IMPACTO	# COLUMNAS EN LA MATRIZ DE RIESGO QUE SE DESPLAZA EN EL EJE DE LA PROBABILIDAD	# COLUMNAS EN LA MATRIZ DE RIESGO QUE SE DESPLAZA EN EL EJE DE IMPACTO
fuerte	directamente	no disminuye	2	0
moderado	directamente	no disminuye	1	0

Fuente Oficina de Planeación - ADR
Ajustado - Guía para la Administración del Riesgos y el Diseño de Controles para Entidades Públicas, Versión: 4, Pag.66

Nota:
- Si la solidez del conjunto de los controles es débil, este no disminuirá ningún cuadrante de impacto o probabilidad asociado al riesgo.
- Tratándose de riesgos de corrupción únicamente hay disminución de probabilidad. Es decir, para el impacto no opera el desplazamiento.

Una vez realizado el análisis y evaluación de los controles para la mitigación de los riesgos, procedemos a la elaboración del mapa de riesgo residual (después de los controles).

COPIA CONTROLADA

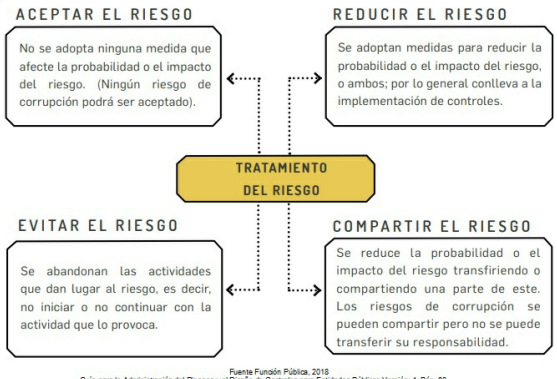
8. TRATAMIENTO DEL RIESGO

Es la respuesta establecida por la **Primera Línea de Defensa** para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción.

Para el caso de los Riesgos de Gestión y de los Riesgos de Seguridad de la Información se consideran ACEPTABLES aquellos ubicados en Nivel de Riesgo Bajo . Para los riesgos asociados a posibles actos de corrupción, es claro que este tipo de riesgos NO ADMITEN ACEPTACIÓN DEL RIESGO.

En todos los casos para los riesgos de corrupción la respuesta será evitar, compartir o reducir el riesgo. El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías.

Figura 9. Tratamiento del Riesgo



Fuente Función Pública, 2018
Guía para la Administración del Riesgos y el Diseño de Controles para Entidades Públicas Versión: 4, Pág. 68

Zona de riesgo BAJO: ACEPTABLE. **Aceptar el riesgo.** Se asumirá el riesgo y se administra por medio de las actividades propias del proyecto o proceso asociado y se realiza un reporte cuatrimestral de seguimiento del riesgo a través del formato F-SIG-003 Seguimiento Mapa de Riesgos por proceso, de conformidad con las fechas de corte definidas en el numeral 10. Periodicidad para el Seguimiento, de la presente política.

Zona de riesgo MODERADO: NO ACEPTABLE. **Reducir el riesgo.** Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo, las cuales se documentan como Acciones para abordar Riesgos.

Se hace seguimiento cuatrimestral y se registra sus avances en el formato F-SIG-003 Seguimiento Mapa de Riesgos por proceso, de conformidad con las fechas de corte definidas en el numeral 10. Periodicidad para el Seguimiento, de la presente política.

Zona de riesgo ALTO: NO ACEPTABLE. **Reducir el riesgo – Evitar el riesgo – Compartir o transferir el riesgo.** Se establecen acciones de control preventivas que permitan MITIGAR la materialización del riesgo.

Cuando se opta por la medida de tratamiento "Reducir el riesgo", en el caso de riesgos en zona Alta, las actividades de control definidas (preventivas y/o detectivas) deben propender por bajar el nivel de riesgo a la zona baja, las cuales se documentan como Acciones para abordar Riesgos.

Se monitorea cuatrimestralmente y se registra en el formato F-SIG-003 Seguimiento Mapa de Riesgos por proceso, de conformidad con las fechas de corte definidas en el numeral 10. Periodicidad para el Seguimiento, de la presente política.

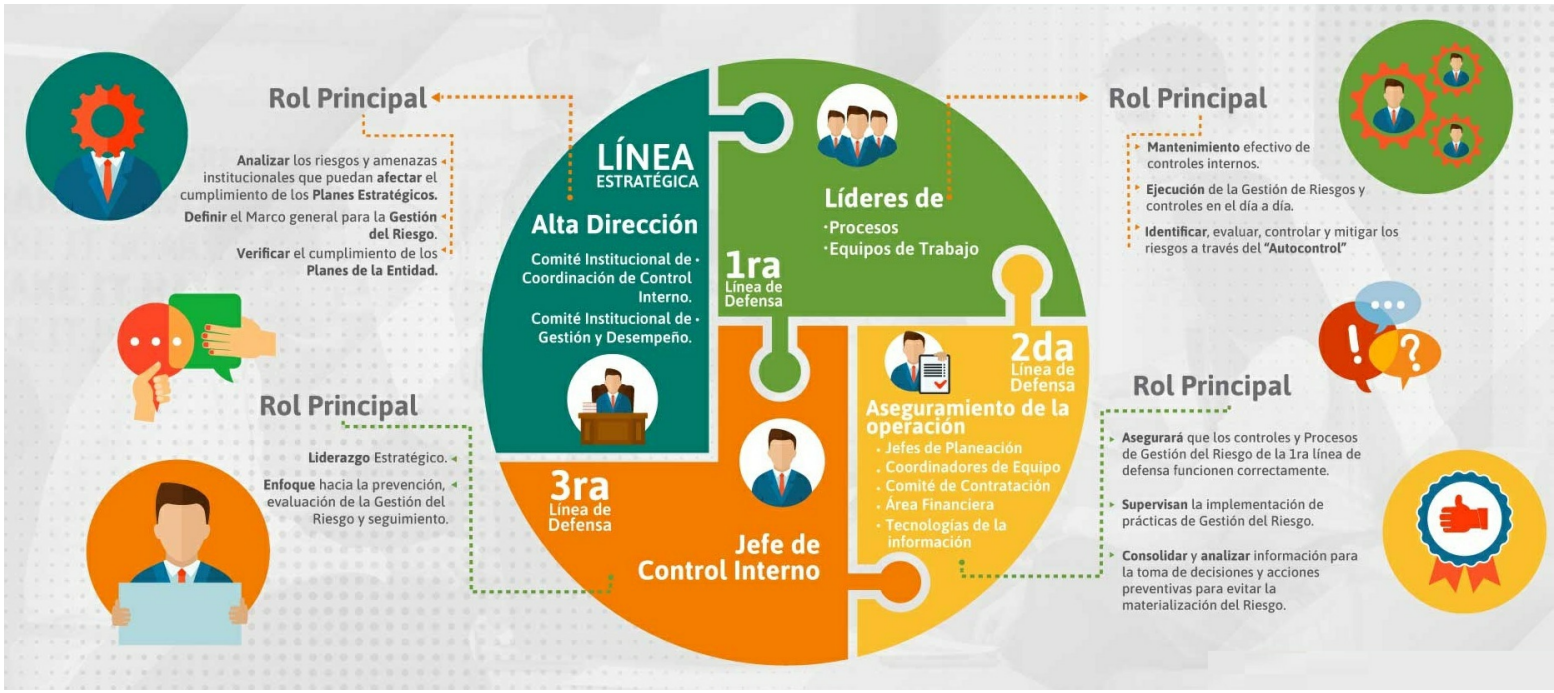
Zona de riesgo EXTREMO: NO ACEPTABLE. **Reducir el riesgo – Evitar el riesgo – Compartir o transferir el riesgo.** Se establecen acciones de Control Preventivas y correctivas que permitan MITIGAR la materialización del riesgo. El seguimiento será cuatrimestral y se registra en el formato F-SIG-003 Seguimiento Mapa de Riesgos por proceso, de conformidad con las fechas de corte definidas en el numeral 10 Periodicidad para el Seguimiento, de la presente política.

Para los riesgos asociados a posibles actos de corrupción se deben definir los lineamientos para su tratamiento, es decir que siempre deben tratarse y gestionarse. Es claro que este tipo de riesgos no admiten aceptación del riesgo.

9. MONITOREO Y REVISIÓN

La entidad debe asegurar el logro de sus objetivos anticipándose a los eventos negativos relacionados con la gestión de la entidad. El monitoreo y revisión de la gestión de riesgos está alineado con la dimensión 7 "Control interno" del MIPG, desarrollando a través de las líneas de defensa la responsabilidad de la gestión del riesgo y control. Las líneas de defensa, 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.

Figura 10. Lineas de Defensa ADR



La revisión al contenido de la matriz de riesgos de la entidad (Instrumento de riesgos – "Mapa de Riesgos") se realizará una vez al año o cuando las circunstancias lo ameriten, a partir de modificaciones o cambios sustanciales en el contexto estratégico, modificaciones de proceso o procedimientos, o cualquier hecho interno o externo que afecte la operación de la entidad, con el fin de identificar acciones pertinentes o actualizaciones.

Mediante el monitoreo y revisión, se:

- Evalúa que los controles sean eficaces y eficientes en el diseño y la operación.
- Detecta cambios en el contexto externo e interno que puedan exigir revisión de los controles y planes de tratamiento del riesgo, y establecer un orden de prioridades.

En la realización del monitoreo y revisión de los riesgos, se debe incluir:

- Las auditorías Internas llevadas a cabo por la Oficina de Control Interno y los informes de seguimiento.
- Los informes de seguimiento a los riesgos realizados por la Oficina de Control Interno.

Además, esta actividad permite la identificación de nuevos riesgos.

A su vez, las acciones de tratamiento resultantes del proceso de valoración de los riesgos pueden tener la participación de varios responsables, y están en capacidad de reportar, a los líderes de procesos los resultados de la implementación de dichas acciones.

COPIA CONTROLADA

10. PERIODICIDAD PARA EL SEGUIMIENTO

Para hacer seguimiento a la eficacia y efectividad de las acciones de tratamiento adoptadas se deben definir indicadores que permitan medir la eficiencia y efectividad (si aplica).

Los líderes de los procesos (primera línea de defensa) en conjunto con sus equipos deben monitorear los riesgos de gestión y corrupción cuatrimestralmente, revisando que su contexto y valoración no presente cambios y si es del caso ajustarlo. Las modificaciones de los riesgos de corrupción se presentarán al Comité Institucional de Gestión y Desempeño y se publicarán nuevamente.

Los líderes de proceso (primera línea de defensa) reportan cuatrimestralmente a la Oficina de Planeación (segunda línea de defensa) el estado de avance del tratamiento del riesgo en la operación, a través del formato F-SIG-003 Seguimiento Mapa de Riesgos por Proceso.

- **Primer seguimiento,** con corte al 30 de abril (período comprendido entre el 1° de enero y el 30 de abril): El reporte de avance se debe realizar los 5 primeros días hábiles del mes de mayo.
- **Segundo seguimiento,** con corte al 31 de agosto (período comprendido entre el 1° de mayo y el 31 de agosto): El reporte de avance se debe realizar los 5 primeros días hábiles del mes de septiembre.
- **Tercer seguimiento,** con corte al 31 de diciembre (período comprendido entre el 1° de septiembre y el 31 de diciembre): El reporte de avance se debe realizar los 15 primeros días calendario del mes de diciembre y actualizar el reporte los 5 primeros días hábiles del mes de enero.

Le corresponde igualmente a la Oficina de Planeación (segunda línea de defensa) adelantar el monitoreo una vez al año, para que el Comité Institucional de Coordinación de Control Interno analice los riesgos asociados a la operación de la ADR, identificados para las acciones desarrolladas en forma directa o tercerizada.

El seguimiento a la elaboración, divulgación, monitoreo y control será realizado por la Oficina de Control Interno (tercera línea de defensa) tres (3) veces al año en las siguientes fechas:

- **Primer seguimiento,** con corte al 30 de abril: La publicación debe surtirse dentro de los diez (10) primeros días hábiles del mes de mayo
- **Segundo seguimiento,** con corte al 31 de agosto: La publicación debe surtirse dentro de los diez (10) primeros días hábiles del mes de septiembre.
- **Tercer seguimiento,** con corte al 31 de diciembre: La publicación debe surtirse dentro de los diez (10) primeros días hábiles del mes de enero.

En cuanto al seguimiento a los riesgos de gestión, este se realizará con las auditorías a los procesos por parte de la Oficina de Control Interno de acuerdo con la programación establecida en el respectivo Plan Anual de Auditoria.

11. MATERIALIZACIÓN DE RIESGOS

11.1 Materialización de riesgos de corrupción

La entidad establece las acciones a seguir por el líder de proceso ante la materialización del **riesgo de corrupción**, así:

- Informar al responsable del Proceso de Direccionamiento Estratégico sobre el hecho encontrado.
- En caso de materializarse un riesgo que afecte la imagen de la Entidad o reputacional de la misma, se deben seguir los lineamientos contenidos en el Manual Guía Comunicaciones en situación de Crisis y Manejo de Medios de Comunicación código: MO-COM-001 que se encuentra en el aplicativo Isolución.
- Informar a las autoridades de la ocurrencia del hecho de corrupción, realizando la denuncia ante la instancia de control correspondiente (cuando se requiera)
- Identificar las acciones correctivas necesarias y documentarlas en el plan de mejoramiento
- Revisar el Mapa de Riesgos de Corrupción, en particular las causas, riesgos y controles y actualizar el mapa de riesgos
- Verificar si se tomaron las acciones y se actualizó el Mapa de Riesgos de Corrupción.
- Realizar un monitoreo permanente.

Ante la materialización del riesgo, se procede de manera inmediata a aplicar el plan de contingencia que permita la continuidad del servicio o el restablecimiento del mismo (si es el caso), y documentarlo en el Plan de mejoramiento.

11.2 Materialización de riesgos de gestión

Con el fin de determinar el manejo de la materialización de riesgo de gestión, es necesario:

- Diligenciar el formato "Plan de Contingencia para Riesgos Materializados" (F-SIG-001) en el cual se deben definir, entre otros: Objetivo, Alcance y Plan de acción.
- Se requiere la revisión del Mapa de Riesgos de Gestión en lo referente a causa, riesgo y control. De ser necesario, realizar los ajustes a los que haya a lugar.

11.3 Materialización de riesgos de Seguridad Digital

La entidad establece las acciones tomando como referencia el Anexo 4 de la "Guía para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de Gestión, Corrupción y Seguridad Digital" (Versión 4)", emitida por el DAFP en octubre de 2018. Para efectos del presente modelo se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad digital:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

Para cada riesgo, se deben asociar el grupo de activos o activos específicos del proceso, conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización, así mediante la ejecución del Plan de Tratamiento de Riesgos de Seguridad

Digital - ADR, para el análisis, valoración y tratamiento de riesgos de Seguridad, alineados con las políticas de seguridad y privacidad de la información y en el caso de materialización del riesgo de seguridad digital se realizara la gestión del incidente de la seguridad de la información en conformidad con el procedimiento PR – OST – 004

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
1	21/Sep/2017	Ajuste general del documento por emisión de la Guía de Administración del Riegos V2. de la Función Pública en octubre de 2018.
2	30/Nov/2018	Modificación general del documento para eliminar la descripción metodológica. Cambio de las descripciones de frecuencia. Cambio de la tabla de impacto para los riegos de seguridad digital
3	23/Sep/2020	Cumplimiento lineamientos guia administración del riesgo
4	26/Oct/2021	En cumplimiento a los lineamientos de la Guia Administración del Riesgo versión 5 de Diciembre del 2020
5	08/Sep/2022	En cumplimiento a los Lineamientos de la Guía Administración del Riesgo versión 5 de Diciembre del 2020 para los Riesgos de Gestión y relación de los lineamientos que aún son vigentes de la versión 4 para Riesgos de Corrupción y atendiendo las observaciones de la Oficina de Control Interno en su Seguimiento a la Gestión del Riesgo.

ELABORÓ	REVISÓ	APROBÓ
Nombre: Wendy Nirvana Tovar Rojas	**Nombre:** Felipe Enrique Guerra Olivella	**Nombre:** Cesar Augusto Castaño Jaramillo
Cargo: Contratista	**Cargo:** Jefe Oficina de Planeacion	**Cargo:** Presidente Encargado
Fecha: 08/Sep/2022	**Fecha:** 08/Sep/2022	**Fecha:** 12/Sep/2022

COPIA CONTROLADA