Administración de Riesgos

PO-017

Introducción

La gestión de riesgos se ha convertido en un componente fundamental de cualquier organización, ya sea pública o privada, debido al entorno cada vez más complejo y dinámico en el que operan. En este contexto, una política de administración de riesgos se erige como un marco estructurado que permite identificar, evaluar y gestionar los riesgos que pueden afectar el logro de los objetivos de Rotorr-Motor de Innovación.

Esta introducción a la política de administración de riesgos abordará la importancia de esta disciplina, su relevancia en la toma de decisiones estratégicas y operativas, y los beneficios que puede aportar a nivel organizacional.

En un mundo caracterizado por la incertidumbre y la volatilidad, las organizaciones se enfrentan a una amplia gama de riesgos que pueden tener un impacto significativo en su desempeño y sostenibilidad a largo plazo. Estos riesgos pueden surgir de diversas fuentes, como cambios en el entorno económico, político o regulatorio, fluctuaciones en los mercados financieros, amenazas cibernéticas, desastres naturales, cambios normativos, entre otros.

Una política de administración de riesgos proporciona el marco y los procesos necesarios para identificar y evaluar estos riesgos, priorizarlos en función de su impacto y probabilidad, y desarrollar estrategias para mitigarlos o aprovechar las oportunidades que puedan surgir. Al adoptar un enfoque proactivo hacia la gestión de riesgos, las organizaciones pueden anticiparse a los eventos adversos, proteger sus activos y recursos, y mejorar su capacidad para adaptarse y prosperar en un entorno cambiante.

Además de proteger el valor y la reputación de Rotorr, una política de administración de riesgos puede contribuir a mejorar la eficiencia operativa, la toma de decisiones informada y la confianza de los *stakeholders*, incluidos los inversores, clientes, empleados y grupos de interés en general.

La administración de riesgos es un proceso continuo e integrado que implica la identificación, evaluación, tratamiento y monitoreo de los riesgos en toda la organización. Al establecer una política de administración de riesgos sólida y efectiva, Rotorr puede fortalecer su resiliencia y capacidad para enfrentar los desafíos del entorno empresarial actual y futuro.

Objetivo General

Garantizar la sostenibilidad y el éxito a largo plazo de Rotorr al identificar, evaluar y gestionar de manera efectiva los riesgos asociados con la innovación, el desarrollo tecnológico y la comercialización de productos y servicios, con el fin de proteger el valor y la reputación de la corporación, optimizar el uso de recursos y maximizar las oportunidades de crecimiento y competitividad en un entorno empresarial dinámico y cambiante

Objetivos Específicos

- Gestión de Riesgos Financieros: Asegurar la estabilidad financiera y la sostenibilidad de los proyectos de innovación y desarrollo mediante la evaluación y gestión de riesgos financieros asociados.

- Gestión de Riesgos Tecnológicos: Evaluar y mitigar los riesgos tecnológicos asociados con los proyectos de investigación e innovación para garantizar la viabilidad y seguridad de las soluciones desarrolladas.

- Gestión de Riesgos Operacionales: Implementar prácticas y procedimientos para minimizar los riesgos operacionales que podrían afectar la ejecución efectiva de los proyectos de Rotorr.

- Gestión de Riesgos de Cumplimiento: Asegurar el cumplimiento de las normativas legales y regulatorias relevantes en todas las actividades de Rottor, especialmente aquellas relacionadas con la protección del medio ambiente, la ética y la transparencia.

- **Gestión de Riesgos Estratégicos:** Identificar y abordar los riesgos estratégicos que podrían afectar la capacidad de la CID para cumplir con su misión y objetivos a largo plazo.

Estos objetivos de política de riesgos ayudan a la CID a mantener un enfoque equilibrado entre la innovación y la seguridad, garantizando así que sus iniciativas contribuyan positivamente al desarrollo económico y social sin comprometer la estabilidad y la integridad.

Marco Legal

Con la expedición de la Ley 1474 de 2011 en su Artículo 73, el Gobierno Nacional reglamentó que: "Cada Entidad del orden nacional, departamental y municipal deberá elaborar anualmente una estrategia de lucha contra la corrupción y de atención al ciudadano".

El Decreto 1081 de 2015 "Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República", compilatorio del Decreto 2641 de 2012 y reglamentario de los artículos 73 y 76 de la Ley 1474 de 2011, estableció como metodología para diseñar y hacer seguimiento a dicha estrategia la establecida en el Plan Anticorrupción y de Atención al Ciudadano contenida en el documento "Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano Versión 2".

A través del Decreto 124 del 26 de enero de 2016 "Por el cual se sustituye el Título IV de la Parte 1 del Libro 2 del Decreto 1081 de 2015, relativo al "Plan Anticorrupción y de Atención al Ciudadano", se estableció en su Artículo 2.1.4.1 como metodología para diseñar y hacer seguimiento a la estrategia de lucha contra la corrupción y de atención al ciudadano de que trata el artículo 73 de la Ley 1474 de 2011.

Con la expedición del 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", se realizó la articulación entre el Modelo Integrado de Planeación y Gestión MIPG y el Sistema de Control Interno.

A partir de esta actualización, surge dentro de este modelo la Dimensión de Control Interno y en su estructura se detalla el Componente de Evaluación del Riesgo orientado a identificar, evaluar y

gestionar eventos potenciales, tanto internos como externos, que puedan afectar o impedir el logro de los objetivos institucionales.

Alcance

Esta política se extiende a todos los procesos, proyectos, planes y servicios en el ámbito de la entidad, abarcando desde la fase de planificación hasta las actividades llevadas a cabo para cumplir con su misión.

En concordancia con la Política de Planeación Institucional establecida en la Dimensión dos (2) Direccionamiento Estratégico y Planeación, la Política de Seguimiento y Evaluación del Desempeño Institucional en la Dimensión Evaluación de Resultados, y el componente dos (2) del MECI en la Política de Control Interno en la Dimensión Control Interno.

Definiciones

- **Activo de Información:** En el contexto de seguridad digital, son activos elementos tales como: Aplicaciones de la organización,

servicios *web*, redes, información física o digital, Tecnologías de Información TI, tecnologías de operación TO que utiliza la organización para funcionar, en el entorno digital.

- Amenazas: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización. Peligro latente de que un evento físico de origen natural, o causado, o inducido por la acción humana de manera accidental, se presente con una severidad suficiente para causar pérdida de vidas, lesiones u otros impactos en la salud, así como también daños y pérdidas en los bienes, la infraestructura, los medios de sustento, la prestación de servicios y los recursos ambientales.

- Apetito al 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.

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

- Consecuencias: Son 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.

- **Contexto Estratégico:** Insumo básico para la identificación de los riesgos en los procesos y actividades, el análisis se realiza a partir del conocimiento de situaciones internas y externas de la institución.

- **Contexto Externo:** Ambiente externo en el cual la entidad busca alcanzar sus objetivos que puede ser, políticos, económicos y financieros, sociales y culturales, tecnológicos, ambientales, legales y reglamentarios.

- **Contexto Interno:** Ambiente interno en el cual la entidad busca alcanzar sus objetivos, el cual puede ser, financieros, personal, procesos, tecnología, estratégicos, comunicación interna.

- **Control:** Medida que permite disminuir la probabilidad de ocurrencia del riesgo, mitigar el impacto de los riesgos y/o asegurar la continuidad del servicio en caso de llegarse a materializar el riesgo.

- **Control Correctivo:** Medida que permite mitigar el impacto frente a la materialización del riesgo.

- **Control detectivo:** Medida que permite disminuir la probabilidad de ocurrencia del riesgo y detectar que algo ocurre y devuelve el proceso a los controles preventivos.

- **Controles Preventivos:** Medida que permite eliminar las causas del riesgo, para prevenir su ocurrencia o materialización.
- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.
- **Evaluación del Riesgo:** Proceso para determinar el nivel de riesgo según la probabilidad de que ocurra y la gravedad de sus posibilidades.
- **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.
- **Gestión del Riesgo:** Actividades organizadas para gestionar y controlar los riesgos en una entidad, brindando a la administración una seguridad razonable sobre el cumplimiento.
- **Impacto:** Consecuencias que puede ocasionar a la entidad la materialización del riesgo.

- **Integridad:** Propiedad de exactitud y completitud.
- **Mapa de Riesgos:** Herramienta metodológica que permite hacer un inventario de los riesgos ordenada y sistemáticamente, haciendo la descripción de cada uno de estos y las posibles consecuencias y sus acciones preventivas o correctivas.
- **Riesgo de Gestión:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- **Riesgo de 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.
- **Riesgo Residual:** El resultado de aplicar la efectividad de los controles al riesgo inherente.
- **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.

- **Control:** Medida que permite reducir o mitigar un riesgo.
- **Integridad:** Propiedad de exactitud y completitud.
- **SARLAFT:** Sistema de Administración del Riesgo de Lavado de Activos y de laFinanciación del Terrorismo.

Responsables

La gestión de los riesgos se efectúa bajo el liderazgo de la línea estratégica con la participación de todos colaboradores de Rotorr-Motor de Innovación:

Líneas de Defensa	Responsables
Línea estratégica	Dirección ejecutiva. Comité Institucional de Coordinación de Control Interno. Comité Institucional de Gestión y Desempeño.
Primera línea	Director ejecutivo. Gerencias. Jefaturas. Líderes de procesos.
Segunda línea	Gerencia Financiera y Administrativa
Tercera línea	Asesoría de Control Interno.

Línea Estratégica: Establece el marco general para la gestión del riesgo, el control y supervisa su cumplimiento. El Comité Institucional

de Coordinación de Control Interno puede solicitar y compartir información relacionada con la comunicación y consulta de los seguimientos, el monitoreo, y las estadísticas e indicadores.

Responsabilidad Frente al Riesgo:

- Definir el marco general para la gestión del riesgo y el control y supervisar su cumplimiento.
- Establecer y aprobar la Política de Administración del Riesgo, incluyendo los niveles de responsabilidad y autoridad.
- Definir y hacer seguimiento a los niveles de aceptación del riesgo.
- Analizar los cambios en el entorno que puedan tener un impacto significativo en la operación de la corporación y que puedan generar cambios en la estructura de riesgos y controles.
- Realizar seguimiento y análisis periódico a los riesgos institucionales.
- Evaluar el estado del sistema de control interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento del mismo.

Primera Línea de Defensa: Reforzará la cultura de gestión de riesgos en el ámbito institucional, bajo un enfoque estratégico, revisando las necesidades de adaptación al cambio y definiendo o actualizando la Política de Administración del Riesgo. Cada proceso designará al menos un (1) gestor de riesgos por proceso, quienes, en su rol de primera línea de defensa, son responsables de la identificación, análisis, valoración, diseño de controles, evaluación del riesgo, determinación del plan de tratamiento; también son responsables de llevar a cabo el seguimiento inicial y recopilar evidencias.

Responsabilidad Frente al Riesgo

- Desarrollar e implementar procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.
- Identificar y valorar los riesgos que pueden afectar los programas, proyectos, planes y procesos a su cargo y actualizarlo cuando se requiera.
- Actualizar los riesgos de corrupción y/o reporte de la materialización de los riesgos sobre presuntos hechos de corrupción.
- Actualizar los riesgos y/o controles asociados cuando la Asesoría de Control Interno genere una alerta sobre la materialización de los riesgos.

- Definir, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados, alineado con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo en su proceso.
- Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar.
- Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles.
- Implementar el procedimiento transversal de activos de información para identificación de los riesgos de seguridad de la información.
- Informar a la (segunda línea de defensa) sobre la identificación y materialización de los riesgos en los programas, proyectos, planes y/o procesos a su cargo.

Segunda Línea de Defensa: Orienta y fortalece el conocimiento en la gestión del riesgo, verificación y evaluación de controles en las diferentes tipologías de riesgos, intensidad y frecuencia de los controles, según corresponda.

Responsabilidad Frente al Riesgo

- Elaborar e impartir lineamientos respecto al manejo del inventario y registro de activos de información.
- Elaborar e impartir lineamientos para la conservación, preservación y el uso adecuado del patrimonio documental de Rotorr y verificar su cumplimiento.
- Promover y verificar el cumplimiento de las normas en materia de transparencia y acceso a la información.
- Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis y valoración de riesgos de seguridad de la información.
- Monitorear los riesgos identificados y controles establecidos por la primera línea de defensa, acorde con la estructura de los temas a su cargo.
- Apoyar, guiar y capacitar a los líderes de procesos para que puedan identificar, analizar y evaluar los riesgos, así como definir los controles necesarios en sus áreas, con un enfoque en prevención.
- Supervisar que la primera línea de defensa identifique, evalúe y gestione los riesgos en los temas de su competencia.

Tercera Línea de Defensa: Radica en la auditoría interna enfocada en los riesgos, con el fin de asegurar la eficacia del gobierno corporativo. Su función consiste en evaluar la gestión del riesgo y el control interno, además de analizar el desempeño de las dos primeras líneas de defensa.

Responsabilidad Frente al Riesgo

- Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos.
- Analizar el comportamiento de los riesgos consolidados en el mapa de riesgos de conformidad con el Programa Anual de Auditoría Interna y reportar los resultados al Comité Institucional de Coordinación de Control Interno.
- Recomendar mejoras a la Política de Administración del Riesgo.
- Generar a través de su rol de asesoría, una orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la gerencia Financiera y Administrativa.
- Evaluar el análisis al monitoreo de la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo.

- Brindar un nivel de asesoría proactiva y estratégica, frente a la segunda y primera línea de defensa.
- Informar los hallazgos y proporcionar recomendaciones de forma.

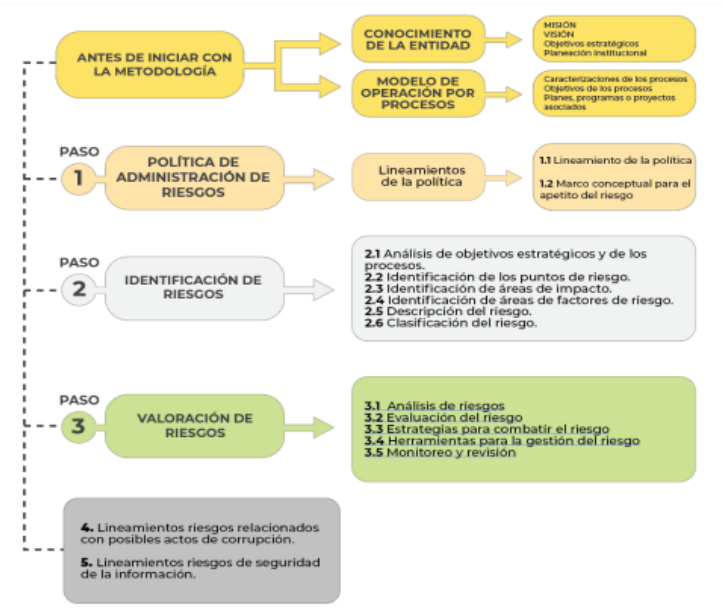
Tipología de Riesgos	Primera Línea de Defensa	Segunda Línea de Defensa	Tercera Línea de Defensa	Línea Estratégica
Gestión	Todos los procesos	Gerencia Financiera y Administrativa		Dirección ejecutiva Comité institucional de coordinación decontrol interno. Comité institucional de gestión y desempeño.
Corrupción	Todos los procesos	Gerencia Financiera y Administrativa		
Seguridad de la información	Todos los procesos	Gerencia Financiera y Administrativa		
Contratación	Participes del proceso de contratación	Gerencia Financiera y Administrativa	CI	
SARLAFT	Participes delproceso de contratación / Procesos misionales			
Seguridad y Salud en el Trabajo	Talento Humano	Gerencia Financiera y Administrativa		

Metodología Administración de Riesgos

En Rotorr-Motor de Innovación, se sigue la metodología de la guía para la administración del riesgo y el diseño de controles en entidades públicas, elaborada por el Departamento Administrativo de la Función Pública, para llevar a cabo el proceso de gestión del riesgo. Esto se realiza a través del modelo de operación por procesos y en concordancia con las estrategias establecidas por la línea estratégica, con el fin de mitigar y prevenir los riesgos. Una estrategia fundamental en este proceso es la determinación y asignación de parámetros de calificación, apetito y nivel de aceptación específicos para cada tipo de riesgo.

Los riesgos de gestión son identificados, analizados, evaluados y tratados, en el marco de los objetivos de procesos y proyectos.

Metodología Administración de Riesgos DAFP



Calificación de Probabilidad

Se evalúa la posibilidad de que el riesgo se materialice, la cual se cuantifica en términos de frecuencia o viabilidad. La frecuencia implica examinar la cantidad de eventos en un periodo determinado.

Nivel	Frecuencia	Cálculo de Probabilidad	Probabilidad %
1	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año.	Muy Baja	20 %
2	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año.	Baja	40 %
3	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.	Media	60 %
4	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año.	Alta	80 %
5	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año.	Muy Alta	100 %

Calificación de Impacto

Se considera en el marco de los efectos adversos económicos y reputación:

Nivel	Afectación Económica	Reputación	Cálculo de Impacto	Impacto %
1	Afectación menora 10 SMLMV	El riesgo afecta la imagen de algún área de la corporación.	Leve	20 %
2	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la corporación internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de	Menor	40 %

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

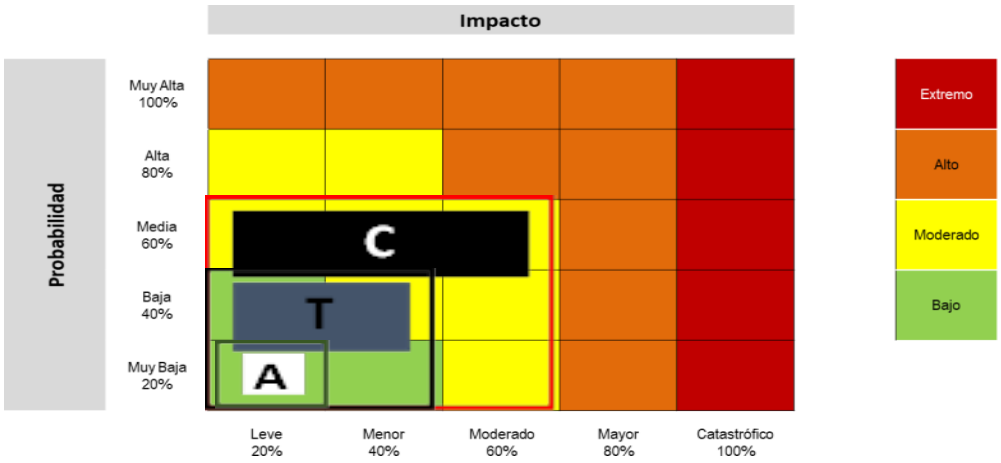
La calificación de impacto de obtiene a través de la tabla de preguntas que determina la guía para la administración del riesgo y el diseño de controles en entidades públicas, elaborado por el Departamento Administrativo de la Función Pública.

No.	Pregunta: Si el riesgo de corrupción se materializa podría ...	Respuesta	
		Sí	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 detraimiento 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 en el 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 preguntas(s) generar un impacto moderado.Responder afirmativamente de seis a once preguntas(s) generar un impacto mayor. Responder afirmativamente de doce a diecinueve preguntas(s) generar un impactocatastrófico.		10 (Nivel de impacto Mayor)	10

Definición de Apetito, Tolerancia y Capacidad de Riesgo

- Apetito: Riesgos en zona bajo.
- Tolerancia: Riesgos en zona moderado.Capacidad: Riesgos en zona moderado.



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 las siguientes estrategias:

Aceptar	Reducir	Evitar	Mitigar	Transferir
Después de analizar y evaluar los niveles de riesgo, se decide asumirlo, entendiendo los posibles	Después de realizar un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante	Después de realizar un análisis y considerar que el nivel de riesgo es	Después de realizar un análisis y considerar los niveles de riesgo, se implementan acciones que mitiguen el nivel	Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través

efectos.	transferencia o mitigación del mismo.	demasiado o alto, se determina no asumir la actividad que genera este riesgo.	de riesgo. No necesariamente es un control adición.	de seguros y pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputación.

- Aceptar el Riesgo: Si el nivel de riesgo residual se ubica en riesgo bajo.
- Reducir o Evitar el Riesgo: Si el nivel de riesgo residual se ubica en riesgo moderado.
- Mitigar o Transferir: Si el nivel de riesgo residual se ubica en riesgo alta o extrema, aplica también para riesgos aun no identificados.

La calificación de impacto de obtiene a través de la tabla de preguntas que determina la guía para la administración del riesgo y el diseño de controles en entidades públicas, elaborado por el Departamento Administrativo de la Función Pública.

Gestión de Riesgos por Procesos

Gestionar riesgos por procesos implica identificar, evaluar y controlar los riesgos específicos asociados a las actividades y operaciones de una organización. Aquí hay algunas acciones clave que suelen incluirse en la gestión de riesgos por procesos:

Identificar los riesgos potenciales asociados a cada proceso dentro de Rotorr. Se pueden utilizar técnicas como listas de verificación, análisis de causa raíz, entrevistas y revisiones documentales para identificar riesgos específicos, una vez identificados, es crucial evaluar la probabilidad y el impacto de cada riesgo. Esto puede realizarse utilizando matrices de riesgo que consideren factores como la severidad del impacto y la probabilidad de ocurrencia.

Para comprender mejor los riesgos identificados, es útil realizar un análisis de causa raíz para determinar las causas fundamentales que podrían desencadenar esos riesgos. Basado en la evaluación de riesgos, se deben desarrollar estrategias efectivas para mitigar o reducir la probabilidad de ocurrencia y/o el impacto de los riesgos identificados. Esto puede incluir la implementación de controles preventivos, procedimientos de emergencia, etc.

Establecer mecanismos para monitorear continuamente los riesgos identificados y las estrategias de mitigación implementadas. Esto

puede implicar la revisión periódica de procesos, la recopilación de datos relevantes y la actualización de estrategias según sea necesario.

Comunicación y Sensibilización: Todos los involucrados en el proceso deben estar conscientes de los riesgos identificados y las medidas de mitigación establecidas. La comunicación efectiva ayuda a garantizar que todos comprendan su papel y responsabilidad en la gestión de riesgos. Finalmente, es importante aprender de los incidentes pasados y las experiencias para mejorar continuamente el proceso de gestión de riesgos. Esto puede incluir realizar revisiones post-implementación, análisis de lecciones aprendidas y ajustes a las estrategias de gestión de riesgos.

Implementar estas acciones en la gestión de riesgos por procesos, ayuda a Rotorr a identificar, evaluar y manejar de manera efectiva los riesgos potenciales que podrían afectar sus operaciones y objetivos estratégicos.

Gestión de Riesgos de Corrupción

En el marco del Plan Anticorrupción y de Atención al Ciudadano establecido en la Ley 1474 de 2011 (artículo 73) y el Decreto 124 de 2016 (artículo 2.1.4.1.).

- 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.

- Los riesgos de corrupción se establecen sobre procesos.

- El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe darlugar a ambigüedades o confusiones con la causa generadora de los mismos.

- Establecer políticas y normativas claras contra la corrupción, incluyendo códigos de conducta ética y políticas de conflicto de intereses. Estas políticas deben ser comunicadas de manera efectiva a todos los empleados y partes interesadas.

- Implementar controles internos sólidos para la gestión financiera, compras y contrataciones. Esto incluye la separación de funciones, auditorías internas regulares y la revisión de procesos críticos para identificar posibles puntos vulnerables.

- Promover una cultura organizacional basada en la transparencia y la rendición de cuentas. Esto incluye la divulgación proactiva de información relevante y la responsabilización de los responsables de la toma de decisiones.

- Capacitar a los empleados en los riesgos de corrupción y las políticas anticorrupción de la organización. Esto puede incluir

talleres, cursos y campañas de sensibilización sobre ética y conducta profesional.

- Establecer un canal de denuncias, seguro y confidencial para que los empleados puedan reportar actividades sospechosas o violaciones a las políticas anticorrupción sin temor a represalias.

- Realizar la debida diligencia exhaustiva en terceros, proveedores y socios comerciales para asegurar que cumplan con estándares éticos y legales adecuados.

- Implementar sistemas de monitoreo y análisis de datos para detectar patrones o comportamientos inusuales que puedan indicar posibles casos de corrupción.

- Realizar auditorías externas e independientes periódicas para evaluar el cumplimiento de las políticas anticorrupción y la efectividad de los controles internos.

- Participación y compromiso de la alta dirección: Fomentar el compromiso y liderazgo de la alta dirección en la promoción de una cultura ética y en la implementación de medidas anticorrupción efectivas.

- Revisar regularmente las políticas y procedimientos anticorrupción, así como los resultados obtenidos de las acciones implementadas, con el objetivo de identificar áreas de mejora y ajustar las estrategias según sea necesario.

Implementar estas acciones no solo ayuda a reducir los riesgos de corrupción dentro de Rotorr, sino que también fortalece la reputación, la confianza de los empleados y las relaciones con clientes y partes interesadas externas.

Gestión de Seguridad de la Información

- Establecer políticas claras y procedimientos documentados que regulen el uso, acceso, almacenamiento y transmisión de la información dentro de la organización. Esto incluye políticas de clasificación de la información, gestión de contraseñas, acceso remoto, entre otros.

- Realizar evaluaciones periódicas de riesgos de seguridad de la información para identificar y evaluar las amenazas potenciales, vulnerabilidades y consecuencias asociadas. Basado en esto, implementar controles adecuados para mitigar esos riesgos.

- Implementar controles de acceso adecuados para garantizar que solo las personas autorizadas tengan acceso a la información relevante para sus funciones. Esto incluye la autenticación multifactor, control de privilegios y la revisión regular de los accesos.

- Capacitar y sensibilizar a los empleados sobre las políticas y prácticas de seguridad de la información. Esto puede incluir programas de formación en seguridad, simulacros de phishing y sesiones informativas regulares.

- Implementar tecnologías adecuadas para proteger la información, como *firewalls*, sistemas de detección y prevención de intrusiones (IDS/IPS), antivirus, cifrado de datos, entre otros. Además, mantener estos sistemas actualizados y configurados correctamente.

- Establecer un plan de respuesta a incidentes de seguridad de la información que detalle los procedimientos a seguir en caso de violaciones de seguridad, incluyendo la notificación adecuada a las partes afectadas y la investigación de las causas subyacentes.

- Realizar auditorías internas y externas periódicas para evaluar la efectividad de los controles de seguridad de la información y asegurar el cumplimiento de las políticas establecidas.

- Evaluar y gestionar los riesgos de seguridad de la información asociados con proveedores externos y terceros que tienen acceso a información crítica de la organización.

- Implementar un ciclo de mejora continua en la gestión de seguridad de la información, revisando regularmente las políticas, procedimientos y controles para adaptarse a nuevos riesgos y amenazas emergentes.

La gestión efectiva de la seguridad de la información no solo protege los datos críticos de Rotorr, sino que también fortalece la confianza de los clientes, socios y empleados, minimizando el impacto de posibles incidentes de seguridad y asegurando la continuidad del negocio.

Gestión de Riesgos de Contratación

- Dar cumplimiento al manual de contratación de Rotorr.

- Realizar una evaluación inicial de los riesgos potenciales asociados con la contratación, considerando aspectos como integridad, cumplimiento normativo, seguridad, capacidad financiera, entre otros.

- Realizar una debida diligencia exhaustiva sobre los candidatos o contratistas, proveedores o empleados. Esto implica verificar antecedentes, referencias laborales, historial financiero, cumplimiento normativo, y cualquier otro aspecto relevante para la relación contractual.

Definición de criterios de selección:

- Establecer criterios claros y objetivos para la selección de contratistas, proveedores o empleados. Estos criterios deben estar alineados con los objetivos estratégicos y los requisitos específicos del proyecto o servicio a contratar.

- Elaborar contratos claros y detallados que definan los derechos, responsabilidades, términos y condiciones de la relación contractual. Es importante incluir cláusulas relacionadas con la

gestión de riesgos, la responsabilidad por incumplimientos y las medidas de mitigación previstas.

- Implementar un sistema de monitoreo continuo de los contratistas, proveedores o empleados para asegurar que cumplan con los compromisos contractuales y los estándares esperados durante toda la duración de la relación contractual.

- Realizar auditorías periódicas a los contratistas, proveedores o empleados para evaluar el cumplimiento de los términos contractuales, así como los estándares éticos, legales y de seguridad requeridos.

- Establecer un canal de denuncias seguro y confidencial para que los empleados puedan reportar irregularidades, incumplimientos o incidentes relacionados con los contratistas, proveedores o empleados.

- Capacitar a los empleados involucrados en el proceso de contratación sobre la importancia de la gestión de riesgos y la debida diligencia en la selección de contratistas, proveedores o empleados.

- Realizar revisiones periódicas del proceso de gestión de riesgos en la contratación para identificar áreas de mejora y ajustar las prácticas y políticas según sea necesario.

- Integración con la gestión de riesgos global de la organización:

- Asegurar que el proceso de gestión de riesgos en la contratación esté alineado y sea coherente con la estrategia global de gestión de riesgos de la organización, garantizando una gestión integrada y efectiva.

- Gestión de Riesgos SARLAFT.

- Establecer políticas y procedimientos detallados que definan claramente cómo Rotorr identificará, evaluará y mitigará los riesgos de lavado de activos y financiación del terrorismo.

- Incluir en estas políticas los criterios para la clasificación de clientes y transacciones de alto riesgo, así como los procesos para el monitoreo continuo de estas actividades.

- Realizar debida diligencia mejorada (enhanced due diligence, EDD) en clientes y transacciones identificados como de alto riesgo. Esto puede incluir verificaciones adicionales de la identidad del cliente, fuentes de fondos y propósito de la relación comercial.

- Implementar sistemas y herramientas de monitoreo continuo de transacciones y actividades financieras.

- Utilizar tecnología y análisis de datos para identificar patrones y comportamientos sospechosos que puedan indicar actividades de lavado de dinero o financiación del terrorismo.

- Capacitar regularmente al personal en los riesgos de lavado de activos y financiación del terrorismo, así como en las políticas y procedimientos SARLAFT de Rotorr
- Asegurar que todos los empleados estén conscientes de su rol y responsabilidades en la prevención y detección de actividades ilícitas.
- Reportar actividades sospechosas a las autoridades competentes.
- Realizar auditorías internas regulares para evaluar la efectividad del SARLAFT implementado y asegurar el cumplimiento de las políticas y procedimientos establecidos.
- Revisar periódicamente los riesgos identificados y actualizar las medidas de mitigación según sea necesario.
- Colaborar con otras entidades del sector financiero y con las autoridades reguladoras para compartir información y mejores prácticas en la gestión de riesgos SARLAFT.
- Participar en grupos de trabajo y redes de información sobre prevención de lavado de activos y financiación del terrorismo.
- Implementar estas acciones ayudará a Rotorr a fortalecer su capacidad para identificar, evaluar y mitigar los riesgos relacionados con el lavado de activos y la financiación del terrorismo, cumpliendo

así con las obligaciones regulatorias y protegiendo la integridad y reputación de la organización.

Gestión de Riesgos SGSST

- Identificar y evaluar los Riesgos para la Seguridad y Salud de los trabajadores en el lugar de trabajo. Esto incluye riesgos físicos, químicos, biológicos, ergonómicos y psicosociales.
- Evaluar la probabilidad y severidad de los riesgos identificados para determinar el nivel de riesgo asociado a cada uno.
- Implementar medidas preventivas y de control para mitigar los riesgos identificados. Estas medidas pueden incluir controles técnicos, medidas administrativas y uso de equipos de protección personal (EPP).
- Capacitar a los trabajadores sobre los riesgos específicos asociados a sus tareas y funciones, así como sobre las medidas de control y seguridad aplicables.
- Monitorear continuamente las condiciones de trabajo y revisar periódicamente las evaluaciones de riesgos para asegurar que las medidas de control sean efectivas y estén actualizadas.

- Cumplir con las normativas y regulaciones locales e internacionales relacionadas con la SGSST, asegurando que la organización esté alineada con los estándares mínimos de seguridad laboral.

- Fomentar la participación activa de los trabajadores en la identificación y evaluación de riesgos, así como en la implementación y revisión de medidas de control.

- Investigar incidentes y accidentes laborales para identificar causas subyacentes y tomar medidas correctivas para prevenir su recurrencia.

- Fomentar una cultura organizacional donde la Seguridad y la Salud en el trabajo sean prioridades, promoviendo la comunicación abierta y la responsabilidad compartida.

  Realizar auditorías internas y externas periódicas para evaluar el desempeño de la gestión de riesgos en SGSST y asegurar el cumplimiento de estándares y regulaciones.

La gestión efectiva de riesgos en SGSST no solo protege a los trabajadores de accidentes y enfermedades laborales, sino que también contribuye a mejorar la productividad, reducir costos relacionados con la salud y aumentar la moral y la satisfacción laboral en la corporación.

Aceptación del Riesgo

La aceptación de riesgos dentro del MIPG no solo ayuda a las organizaciones a manejar eficazmente las incertidumbres inherentes a sus actividades, sino que también promueve una cultura organizacional que valora la toma de decisiones informadas y la gestión responsable de riesgos. Al integrar la aceptación de riesgos en el proceso de planeación y gestión, las organizaciones pueden optimizar sus recursos y focalizar sus esfuerzos en áreas donde la mitigación de riesgos genere el mayor valor agregado.

Riesgo residual	Probabilidad	Impacto	Aceptación del Riesgo	Apetito	Estrategia
Corrupción Contratación Asociados al proceso Gestión financiera SARLAFT	Baja	Moderado Mayor Catastrófico	Bajo	Tolerancia 0	Evitar Mitigar
Gestión Seguridad de la información Seguridad y Salud en elTrabajo	Muy baja Baja Media	Leve Menor Moderado	Moderado Bajo	Tolerancia 0 Aversión Cautela	Aceptar Reducir Evitar Mitigar Transferir

Gestión de Eventos

En el contexto de la gestión de riesgos, un evento se define como cualquier situación o suceso que podría afectar las operaciones normales de una organización y potencialmente resultar en pérdidas económicas, daño a la reputación, interrupción de servicios, entre otros impactos adversos. Estos eventos son considerados como la manifestación concreta de riesgos previamente identificados y evaluados en los procesos de gestión de riesgos.

Tipos de Eventos en la Gestión de Riesgos

Los eventos pueden categorizarse en diversas formas según su naturaleza y origen:

- Incidentes Operativos: Tales como, interrupciones en la cadena de suministro, fallos en sistemas críticos, o errores humanos que resultan en pérdidas financieras o de datos.

- Eventos de Seguridad: Incluyendo ciberataques, violaciones de datos, o incidentes de seguridad física que comprometen la integridad de la organización y su capacidad para operar de manera segura.

- Eventos Regulatorios y Legales: Tales como, cambios en las regulaciones, litigios o sanciones legales que pueden afectar la reputación y el cumplimiento normativo de la entidad.

- Eventos de Mercado y Económicos: Como fluctuaciones en los mercados financieros, cambios en las condiciones económicas globales, o eventos geopolíticos que impactan en la estabilidad financiera y operativa de la organización

En caso de que el riesgo no se hubiese identificado, se debe incluir y dar el tratamiento correspondiente; en caso de riesgos identificados que presentan materialización, el proceso procede de acuerdo con la metodología que se menciona en el procedimiento administración del riesgo.

Nivel de Confianza de los Controles

La primera línea de defensa debe asegurar que los controles de riesgos y puntos de control estén adecuadamente establecidos en documentos reconocidos como procedimientos, siguiendo la estructura establecida que incluye el responsable, la periodicidad, el propósito, cómo se lleva a cabo la actividad, observaciones y desviaciones, y evidencia. Además, es crucial tener en cuenta las observaciones derivadas del análisis de los resultados de la evaluación

del nivel de confianza en los controles, las cuales son compartidas por la segunda línea de defensa a través del informe de gestión de riesgos.

Los controles considerados y existentes son:

- Preventivos.
- Detectivos.
- Correctivos

Materialización de Riesgos

Para evitar la materialización de riesgos y fortalecer la capacidad de Rotorr, para gestionarlos de manera efectiva, se implementan diversas medidas generales. Estas acciones están diseñadas para prevenir la ocurrencia de eventos adversos y mitigar su impacto potencial.

- Realizar evaluaciones regulares de riesgos para identificar y entender los posibles riesgos que enfrenta la corporación. Esto incluye considerar tanto los riesgos internos como los externos que podrían afectar los objetivos y operaciones de Rotorr.
- Implementar controles preventivos adecuados para mitigar los riesgos identificados antes de que se materialicen.

- Capacitar a los empleados sobre los riesgos específicos relacionados con sus funciones y responsabilidades. Promover una cultura organizacional que valore la gestión de riesgos y la seguridad, incluyendo la formación en políticas de cumplimiento y procedimientos de emergencia.

- Implementar sistemas de monitoreo continuo para identificar señales tempranas de posibles riesgos y eventos adversos. Esto podría incluir monitoreo de sistemas de seguridad, auditorías internas y revisiones periódicas de cumplimiento normativo.

- Mantener actualizados los controles preventivos y ajustarlos según sea necesario para abordar nuevos riesgos o cambios en el entorno operativo de la corporación. Esto garantiza que los controles sigan siendo efectivos y relevantes.

- Establecer requisitos claros de gestión de riesgos para proveedores y terceros. Evaluar regularmente su desempeño y asegurarse de que cumplan con los estándares de seguridad y calidad esperados.

- Realizar revisiones periódicas de la gestión de riesgos y las medidas preventivas implementadas.

- Identificar áreas de mejora y tomar acciones correctivas para fortalecer la capacidad de la organización para prevenir y mitigar riesgos.

Implementar estas medidas generales no solo ayuda a evitar la materialización de riesgos, sino que también fortalece la capacidad de Rotorr, para gestionar eficazmente los riesgos que podrían afectar sus operaciones y objetivos estratégicos.

Recursos Financieros

La Gerencia Financiera y Administrativa de Rotorr apropiará anualmente, en su respectivo presupuesto, los recursos necesarios para el efectivo cumplimiento de las obligaciones emanadas de la Política de Administración de Riesgos.

Los recursos presupuestales se ejecutarán de conformidad con los programas y proyectos diseñados.