Invest in Bogotá

MA-SIG-01

Manual de gestión de riesgos IIB.

Tabla de contenido

1. OBJETIVO GENERAL

Establecer un marco metodológico estructurado y sistemático para la evaluación, tratamiento y monitoreo de los riesgos que pueden afectar el logro de los objetivos de La Corporación, que permita incentivar el pensamiento basado en riesgos y el uso aplicado de herramientas para su adecuada gestión.

1.1 Objetivos Específicos

- Establecer una metodología integral para la gestión de riesgos alineada con la estrategia, las políticas, procesos y procedimientos de La Corporación.
- Adaptar la metodología de gestión de riesgos al nivel del día a día del empleado.
- Fomentar en La Corporación una cultura de gestión de riesgos, asegurando su vínculo con el Sistema de Gestión Integral y los ciclos de mejoramiento continuo.
- Complementar los esquemas de toma de decisión de La Corporación, con mecanismos y herramientas de análisis de gestión de riesgos.

2. ALCANCE

Este manual es aplicable a los empleados directos, contratistas y las personas relacionadas directa o indirectamente con La Corporación, de acuerdo con cada tipo y clasificación de riesgo.

3. DEFINICIONES

- **Apetito del riesgo:** Es el nivel del riesgo que La Corporación puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la alta dirección.
- **Causa:** Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo (medios, circunstancias y/o agentes que generan riesgos).
- **Cliente interno:** Área que recibe un servicio de otra área de La Corporación.
- **Confidencialidad:** Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.
- **Consecuencia:** Resultado de un evento que afecta los objetivos. Una consecuencia puede ser cierta o incierta y puede tener efectos positivos o negativos, directos o indirectos sobre los objetivos. Las consecuencias se pueden manifestar de forma cualitativa o cuantitativa.
- **Contexto externo:** Factores externos a La Corporación sobre los cuales no tiene control directo pero que pueden afectar positiva o negativamente su capacidad para alcanzar sus objetivos y metas.
- **Contexto interno:** Factores internos de La Corporación sobre los cuales tiene un control directo y pueden afectar positiva o negativamente su capacidad para alcanzar sus objetivos.
- **Control:** Medida o mecanismo que busca disminuir o mitigar el nivel de riesgo, actuando sobre las causas o sobre las consecuencias.
- **Disponibilidad:** Acceso y utilización de la información y los sistemas de tratamiento de esta, por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Entidad relacionada:** Persona u organización que recibe un servicio de La Corporación.
- **Impacto:** Magnitud de las pérdidas o daños que La Corporación podría sufrir como resultado de un riesgo específico.
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y los métodos de proceso.

- **Nivel de riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.
- **Oportunidad:** Probabilidad de que ocurra un evento y que su consecuencia sea positiva.
- **Parte interesada:** Persona o entidad que puede afectar, verse afectada, o percibirse como afectada por una decisión o actividad.
- **Probabilidad:** Medida para estimar el grado de exposición a un riesgo. Se mide según la frecuencia (número de veces en que se ha presentado el riesgo en un período determinado), o por la factibilidad (factores internos o externos que pueden facilitar que el riesgo se presente).
- **Riesgo:** Probabilidad de que un evento se materialice y pueda afectar la consecución de un objetivo.
- **Riesgo inherente:** Es aquel al que se enfrenta una entidad en ausencia de controles para modificar su probabilidad o impacto.
- **Riesgo residual:** Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.
- **Tratamiento del riesgo:** Conjunto de acciones que se toman para modificar la probabilidad y/o el impacto de un riesgo identificado.

4. PRINCIPIOS

La Corporación adopta los principios de la ISO 31000:2018, según la cual, la gestión de riesgos debe ser:

- **Integrada:** La gestión del riesgo es parte integral de todas las actividades de La Corporación.
- **Estructurada y exhaustiva**: Un enfoque estructurado y exhaustivo hacia la gestión del riesgo contribuye a resultados coherentes y comparables.
- **Adaptada:** El marco de referencia y el proceso de la gestión del riesgo se adaptan y son proporcionales a los contextos externo e interno de La Corporación relacionados con sus objetivos.
- **Inclusiva:** La participación apropiada y oportuna de las partes interesadas permite que se consideren su conocimiento, puntos de vista y percepciones. Esto resulta en una mayor toma de conciencia y una gestión del riesgo informada.
- **Dinámica:** Los riesgos pueden aparecer, cambiar o desaparecer con los cambios de los contextos externo e interno de La Corporación. La gestión del riesgo anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna.
- **Mejor información disponible:** Las entradas a la gestión del riesgo se basan en información histórica actualizada, así como en expectativas. La gestión del riesgo tiene en cuenta explícitamente cualquier limitación e incertidumbre asociada con tal información y expectativas. La información debería ser oportuna, clara y disponible para las partes interesadas pertinentes.
- **Factores humanos y culturales:** El comportamiento humano y la cultura influyen considerablemente en todos los niveles y etapas.
- **Mejora continua:** La gestión del riesgo mejora continuamente mediante aprendizaje y experiencia.

5. DESARROLLO

5.1 Componentes

i. **Apetito al riesgo:** Se definirá claramente el nivel de riesgo que La Corporación está dispuesta a asumir en función de sus objetivos y nivel de tolerancia permisible.

ii. **Identificación del riesgo:** Se establecerán métodos sistemáticos para identificar los riesgos internos y externos que puedan afectar el logro de los objetivos.
iii. **Evaluación del riesgo:** Se utilizarán herramientas y técnicas cuantitativas y cualitativas para evaluar la probabilidad y el impacto de los riesgos identificados.
iv. **Tratamiento de riesgos:** Se definirán las estrategias de tratamiento de riesgos, incluyendo la transferencia, la mitigación y la aceptación.
v. **Monitoreo y control:** Se establecerán mecanismos para monitorear los riesgos identificados y evaluar la efectividad de las medidas de control implementadas.
vi. **Comunicación:** Se establecerán canales de comunicación efectivos para informar a los interesados sobre los riesgos y las acciones tomadas para su adecuada gestión.

5.2 Partes Interesadas

a. **Miembros fundadores:** Alcaldía Mayor de Bogotá y Cámara de Comercio de Bogotá.
b. **Junta Directiva:** Órgano directivo de La Corporación que, en desarrollo de sus funciones legales y estatutarias, es responsable de orientar la política estratégica de Invest In Bogotá, monitorear y evaluar la gestión adelantada por la alta gerencia, fijar la arquitectura de gobierno, control, así como las principales políticas de administración de riesgos y de desarrollo organizacional, velando por el cumplimiento de éstas por parte de la alta gerencia y de toda La Corporación.
c. **Cliente interno:** Área que recibe un servicio de otra área de La Corporación.
d. **Entidad relacionada:** Persona u organización que recibe un servicio de La Corporación.
e. **Empleados:** Personas vinculadas a La Corporación mediante contrato de trabajo.
f. **Proveedores:** Personas naturales o jurídicas que suministran bienes o servicios a La Corporación.

5.3 Roles y responsabilidades

Junta Directiva:

- Aprobar la política de gestión del riesgo.
- Definir el apetito de riesgo.
- Garantizar que La Corporación disponga de un adecuado proceso de gestión de riesgos.
- Prevenir y gestionar situaciones críticas.
- Conocer y hacer seguimiento periódico de los principales riesgos de La Corporación.

Comité de Buen Gobierno:

- Validar la política de gestión del riesgo y presentarla a la Junta Directiva.
- Supervisar la gestión del riesgo y perfil del riesgo.
- Informar a la Junta Directiva asuntos relacionados con la gestión del riesgo.
- Conocer el avance en la implementación de medidas de tratamiento para los riesgos más relevantes y emitir sus comentarios y recomendaciones sobre dichas medidas y sobre el perfil del riesgo de La Corporación.

Dirección Ejecutiva:

- Someter a validación del comité de buen gobierno, la política de gestión de riesgos.
- Someter a aprobación de la Junta Directiva de la Corporación, la política de gestión de riesgos.
- Promover la cultura de gestión de riesgos en La Corporación.

- Garantizar que la política de gestión de riesgos se materialice en normas y procedimientos claros, orientando el comportamiento de todos los involucrados.

Gerencia Administrativa y Financiera:

- Aprobar el manual de gestión de riesgos asegurando que se ajusten a las características de La Corporación.
- Consolidar el perfil de riesgo de La Corporación.
- Acompañar el informe de Dirección Ejecutiva a la junta directiva por lo menos una (1) vez al año sobre la implementación, desarrollo y avances en la gestión de riesgos.
- Gestionar con eficiencia los recursos humanos, físicos, tecnológicos, financieros y de información, suficientes e idóneos para el correcto funcionamiento del proceso de gestión de riesgos.
- Definir la estrategia de apropiación de la cultura de gestión de riesgos en La Corporación.

Líderes de proceso:

- Mantener el perfil de riesgo de sus procesos dentro de los parámetros aceptados por La Corporación.
- Reportar los eventos de riesgo materializados en las áreas a cargo.
- Participar en el proceso de identificación, análisis, evaluación y tratamiento de riesgos.
- Asegurar que los controles sean ejecutados por el personal bajo su responsabilidad.
- Liderar la gestión de riesgos en cada uno de sus procesos.
- Asegurar la adhesión a las normas y procedimientos de gestión de riesgos en todas las actividades de La Corporación.
- Diseñar controles o planes de acción que mitiguen el impacto de los riesgos en los procesos que están bajo su responsabilidad.
- Validar la eficacia de los planes de tratamiento implementados.
- Revisar, por lo menos una vez al año, la eficacia de los controles asociados a los riesgos identificados.
- Promover la asistencia y asistir a las capacitaciones que programa La Corporación sobre la gestión de riesgos.
- Diseñar, elaborar, desarrollar y ejecutar los controles y planes de tratamiento de riesgos.

Profesional Gestión de Riesgos:

- Diseñar y proponer la política, metodologías y estándares de gestión de riesgo y someterlas a aprobación.
- Asegurar la adhesión de la implementación y cumplimiento de la política, lineamientos y procesos de la gestión de riesgos.
- Desarrollar la estrategia de apropiación de la cultura de gestión de riesgos en La Corporación.
- Preparar los informes y reportes sobre la gestión de riesgos de la Corporación bajo requerimiento.
- Brindar soporte metodológico a las áreas para la ejecución de las actividades del ciclo de gestión de riesgos.
- Realizar el seguimiento a la eficacia de los procesos, procedimientos y controles establecidos dentro de la gestión de riesgos.
- Diseñar y programar los planes de capacitación para los empleados de La Corporación, relacionados con la gestión de riesgos.

- Validar que los planes de tratamiento diseñados por los líderes de procesos cumplen con los lineamientos establecidos en el manual de gestión de riesgos.

Ejecutores de procesos:

Todos los empleados de La Corporación son responsables de:

1. Cumplir con las políticas y directrices de la gestión de riesgos.
2. Incorporar el autocontrol en la gestión de riesgos.
3. Apropiar y practicar a diario la cultura de gestión de riesgos.
4. Aplicar los controles diseñados en los procesos a su cargo que presenten algún factor de riesgo.
5. Notificar, respecto de los riesgos que identifique, al jefe inmediato y al profesional de gestión de riesgos.
6. Asistir y participar en las capacitaciones de gestión de riesgos, a las cuales seas convocados.

5.4 Metodología

Mediante este manual, se define la metodología de gestión de riesgos de La Corporación tomando como referencia el modelo apoyado en la norma ISO 31000:2018.

Los numerales siguientes presentan cada una de las etapas a desarrollar durante la gestión del riesgo. En la descripción de cada etapa se detallarán los aspectos conceptuales y operativos que deben tenerse en cuenta; la explicación del desarrollo de cada etapa se realizará de acuerdo con el tipo de riesgo.

Las matrices, controles y planes de gestión de riesgos, se registrarán en la herramienta que La Corporación designe y se realizará de acuerdo con el IN-SIG-02 Instructivo de la herramienta para la gestión de riesgos.

5.4.1 Apetito al riesgo

El apetito al riesgo se define como el nivel de riesgo que La Corporación está dispuesta a asumir para alcanzar sus objetivos estratégicos y operativos. Este concepto refleja el balance entre los riesgos y las oportunidades que La Corporación considera aceptables, teniendo en cuenta su perfil organizacional y su capacidad para gestionar dichos riesgos.
El apetito al riesgo será determinado siguiendo las directrices establecidas en el Anexo 3 de la POL-SIG-04 Política de Gestión del Riesgo. De acuerdo con los lineamientos definidos, se realizarán los ajustes necesarios a los niveles de aceptación del riesgo. Estos niveles serán calibrados para garantizar su alineación con la estrategia de La Corporación.

5.4.2 Identificación del riesgo

El propósito de la identificación de riesgos es encontrar, reconocer y describir los riesgos que pueden ayudar o impedir a La Corporación lograr sus objetivos, para la identificación de riesgos, es importante contar con información pertinente, apropiada y actualizada. La Corporación, debe identificar los riesgos, tanto si sus fuentes están o no bajo su control, incluyendo el análisis del contexto interno y externo y deben tener en cuenta los siguientes apartados:

- La identificación se realizará a partir de los objetivos estratégicos y de gestión, también se tendrán en cuenta los riesgos estratégicos, operacionales, financieros y de cumplimiento, con el fin de determinar los eventos que potencialmente puedan afectar el cumplimiento de la estrategia de La Corporación.
- El profesional de gestión de riesgos realizará el acompañamiento metodológico en los ejercicios de identificación de los riesgos de gestión en todos los niveles.
- Es responsabilidad de las gerencias identificar los riesgos y oportunidades que pueden afectar sus objetivos estratégicos y de gestión.

Así mismo, deberá como mínimo incluir los siguientes factores:

i. las fuentes de riesgos tangibles e intangibles;
ii. las causas y los eventos;
iii. las amenazas y las oportunidades;
iv. las vulnerabilidades y las capacidades;
v. los cambios en los contextos interno y externo;
vi. los indicadores de riesgos emergentes;
vii. la naturaleza y el valor de los activos y los recursos;
viii. las consecuencias y sus impactos en los objetivos;
ix. las limitaciones de conocimiento y la confiabilidad de la información;
x. los factores relacionados con el tiempo;
xi. los sesgos, los supuestos y las creencias de las personas involucradas.

Finalmente, el desarrollo de al menos las siguientes preguntas clave:

i. ¿Qué podría salir mal en este proceso?
ii. ¿Dónde están los puntos críticos o vulnerabilidades?

5.4.2.1 Contexto de La Corporación

La identificación del contexto interno y externo hace referencia a las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento del propósito de La Corporación. La definición del contexto estratégico contribuye al control de La Corporación frente a la exposición al riesgo, lo cual facilita la formulación de controles para lograr el cumplimiento de los objetivos institucionales.

La etapa del establecimiento del contexto consiste en analizar el entorno interno y externo para determinar qué factores de este pueden llegar a afectar el logro de los objetivos y por ende dar origen a riesgos y oportunidades, los cuales deben ser identificados y gestionados; la identificación del contexto en Invest in Bogotá se realiza en la formulación del PL-DE-01 Plan Estratégico.

Para realizar el análisis del contexto en IIB es necesario definir 3 dimensiones:

- **Contexto externo**

Todos aquellos factores, eventos y condiciones a nivel local, regional, nacional o internacional que se encuentran fuera de los límites de La Corporación y que pueden influir significativamente en su funcionamiento y desempeño, tales como:

i. Sociales
ii. Culturales
iii. Políticos
iv. Legales
v. Reglamentarios
vi. Financieros
vii. Tecnológicos
viii. Económicos
ix. Ambientales

Situaciones clave y tendencias que puedan afectar los objetivos de La Corporación.
Las relaciones, percepciones, valores, necesidades y expectativas de las partes interesadas externas.
Las relaciones contractuales y los compromisos adquiridos, entre otras.

- **Contexto interno**

Factores, elementos y condiciones que se encuentran dentro de La Corporación y que influyen directamente en su funcionamiento y desempeño, tales como:

i. Propósito de La Corporación.
ii. Junta directiva y estructura de La Corporación.
iii. Normas y directrices adoptados por La Corporación.
iv. Las políticas, la estrategia y los objetivos.
v. Cultura de La Corporación.
vi. Capacidades, recursos y conocimientos (por ejemplo, capital, tiempo, personas, propiedad intelectual, procesos, sistemas y tecnologías).
vii. Los datos, los sistemas de información y el flujo de información.
viii. Las relaciones con las partes interesadas internas, teniendo en cuenta sus percepciones y valores.
ix. Los compromisos contractuales y otros compromisos.
x. Las relaciones entre las distintas instancias de La Corporación.

- **Contexto por proceso**

Se refiere al entorno específico y las condiciones en las que se desarrolla un conjunto de acciones dentro de un proceso de La Corporación.

i. Entorno físico o virtual donde se realiza el proceso.
ii. Roles y responsabilidades de las personas involucradas.
iii. Sistemas, como datos, conocimiento y documentos necesarios para llevar a cabo el proceso.
iv. Transversalidad.
v. Interacciones con otros procesos.
vi. Reglas y normas.
vii. Comunicación entre los procesos.

La Corporación, a través de los procesos, realizará el análisis del contexto anualmente o cada vez se presente un cambio relevante en el contexto, para establecer cuáles de ellos podrían afectar el logro de los objetivos estratégicos o de los procesos. Es responsabilidad de la dirección ejecutiva y/o la gerencia

Administrativa y Financiera realizar el análisis de contexto en la periodicidad ante descrita y dejar constancia por escrito.

Un cambio relevante, se refiere, entre otros, a:

1. **Cambios en la legislación:** Nuevas leyes o regulaciones que impacten la inversión extranjera directa o las políticas fiscales que pueden alterar significativamente el entorno operativo de La Corporación.
2. **Innovaciones tecnológicas:** La adopción de nuevas tecnologías para mejorar la eficiencia en la promoción y gestión de inversiones, como plataformas digitales para la gestión de proyectos o análisis de datos avanzados.
3. **Reestructuración organizacional:** Cambios en la estructura interna, como la creación de nuevas áreas/cargos o la fusión con otras entidades; esto puede influir en la efectividad y alcance de La Corporación.
4. **Variaciones en el financiamiento**: Alteraciones en la disponibilidad de fondos, ya sea por cambios en las políticas gubernamentales o en las contribuciones del sector privado, que pueden afectar la capacidad de La Corporación para llevar a cabo sus actividades.
5. **Cambios en el mercado:** Fluctuaciones económicas o cambios en las tendencias de inversión globales pueden requerir ajustes estratégicos importantes.
6. **Eventos de fuerza mayor o caso fortuito:** Situaciones imprevisibles e irresistibles que escapan del manejo de La Corporación.

Para el análisis de contexto, se debe realizar una clasificación DOFA para cada uno de los factores antes enunciados y de cómo se presenta el mismo frente a La Corporación o frente al proceso analizado.

La clasificación de los factores se realiza teniendo en cuenta los siguientes parámetros:

i. **Debilidad:** Son los aspectos negativos internos, es decir, las limitaciones, deficiencias o áreas de mejora de La Corporación.
ii. **Fortaleza:** Son los aspectos positivos internos, es decir, las capacidades, recursos y ventajas competitivas que posee La Corporación.
iii. **Amenaza:** Son los factores externos negativos que pueden representar un riesgo para La Corporación.
iv. **Oportunidad:** Son los factores externos positivos que pueden aprovecharse para el crecimiento y desarrollo de La Corporación.

Nota*: Para los riesgos de Seguridad de la información el concepto debilidad se asocia al concepto de vulnerabilidad de los activos de la información.*

A partir del resultado del análisis de contexto, las debilidades y amenazas resultantes, son fuentes generadoras de riesgos frente a los objetivos, por su parte las oportunidades y fortalezas resultantes son fuentes generadoras de oportunidades frente al logro de los objetivos.

5.4.2.2 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 de proceso, como para personas ajenas al proceso, debido a esto, la descripción se realizará de la siguiente forma:

Ejemplos:

1. "Extralimitación de funciones en las decisiones institucionales en beneficio propio o de un tercero".
2. "Pérdida, deterioro o adulteración de documentos de los expedientes relacionados con X trámite en el archivo central".
3. "Pérdida del conocimiento y experticia del personal de los procesos misionales con ocasión de los procesos de selección del personal".
4. "CRM no disponible para la operación de La Corporación".

5.4.2.3 Clasificación del riesgo

Para calificar los riesgos de La Corporación es importante tener en cuenta la tipología de los riesgos que se presenta a continuación:

Tabla 1. Tipos de riesgo

Tipo de riesgo	Descripción	Ejemplo
Riesgos estratégicos	Estos riesgos están relacionados con el propósito de La Corporación y su capacidad para alcanzar sus objetivos a largo plazo. Se refieren a decisiones estratégicas, cambios en el mercado, nuevas tecnologías y otros factores que pueden afectar la viabilidad del negocio.	Cambios en las regulaciones, entrada de nuevos competidores, cambios en las preferencias de los clientes, fallos en el lanzamiento de nuevos servicios, cambios en el entorno legal, político, económico o social.
Riesgos operacionales	Son aquellos riesgos asociados a las actividades diarias de La Corporación. Se relacionan con los procesos internos, los sistemas de información, la infraestructura, los recursos humanos, financieros, de sostenibilidad y de seguridad y salud en el trabajo.	Errores humanos, fluctuaciones en los tipos de interés, variaciones en los tipos de cambio, insolvencia de clientes, pérdidas por inversiones, inflación, eventos externos, Ingeniería social, malware, pishing, pérdida de dispositivos, etc.
Riesgos financieros	Los riesgos financieros son aquellos eventos o condiciones que tienen el potencial de afectar negativamente la situación financiera de una empresa, entre ellos se encuentran los riesgos de mercado, crédito y liquidez.	Fluctuaciones en tasas de interés que afectan el valor de activos y pasivos, volatilidad en tipos de cambio que impacta operaciones internacionales, cambios en precios de materias primas que afectan costos operativos, Incumplimiento de pago por parte de clientes o contrapartes, deterioro de la calidad crediticia de deudores, incapacidad para cumplir obligaciones financieras a corto plazo, dificultad para convertir activos en efectivo.

Tipo de riesgo	Descripción	Ejemplo
Riesgos de cumplimiento	El riesgo de cumplimiento es la posibilidad de sufrir consecuencias negativas (como sanciones legales, pérdidas financieras o daño reputacional) debido al incumplimiento de leyes, regulaciones, códigos de conducta o estándares de buenas prácticas que se aplican a La Corporación, entre ellos se encuentran los riesgos en materia legal, ética, contractual, corrupción, auditorías, LAFT entre otros.	Incumplimiento de leyes y regulaciones aplicables, cambios en el marco normativo que requieren adaptación, sanciones por parte de organismos reguladores, exposición a transacciones ilícitas, conflictos de interés no gestionados

5.4.3 Evaluación del riesgo

La evaluación de riesgo es un proceso sistemático que busca identificar, evaluar y gestionar las potenciales amenazas que pueden afectar a un proyecto, La Corporación o una actividad específica. En otras palabras, es una herramienta que nos permite anticiparnos a posibles problemas y tomar medidas para minimizar sus consecuencias, es importante porque nos permite tomar decisiones informadas y estratégicas al conocer la probabilidad e impacto de ocurrencia, ayuda a identificar y mitigar los riesgos antes de que se materialicen evitando pérdidas económicas y daños a la reputación, también permite identificar áreas de mejora en los procesos y sistemas de La Corporación.

5.4.3.1 Análisis de causas y consecuencias

El análisis de causas, en el contexto de la gestión de riesgos, es una herramienta fundamental para ir más allá de la identificación de riesgos. Su objetivo es descubrir las raíces subyacentes de un problema y así poder implementar soluciones más efectivas y duraderas.

¿Por qué es importante?

1. **Prevención:** Al conocer la causa raíz, se pueden implementar medidas para prevenir que el riesgo vuelva a ocurrir.
2. **Mejora continua:** Permite identificar debilidades en los procesos y sistemas, facilitando la mejora continua.
3. **Asignación de responsabilidades:** Ayuda a determinar quiénes son los responsables de cada causa y, por lo tanto, de implementar las acciones correctivas.
4. **Optimización de recursos:** Al dirigir las acciones a la causa raíz, se optimizan los recursos y se evitan soluciones superficiales.

¿Cómo realizar el análisis de causas?

Se sugiere la metodología de los 5 porqués, esta es una herramienta sencilla pero poderosa para identificar la causa raíz de un problema. Consiste en hacerse repetidamente la pregunta "¿por qué?" hasta llegar a la raíz del problema.

Pasos a seguir:

1. **Definir el problema:** Es importante ser específico, en lugar de decir "el equipo no funciona", especificar: "La impresora no imprime en color", también debe ser objetivo, se deben evitar juicios de valor y enfocarse en los hechos.
2. **Preguntar "¿por qué?" cinco veces:**

Ejemplo:

Problema: Mi computador se apaga solo.

¿Por qué se apaga solo? Porque se sobrecalienta.
¿Por qué se sobrecalienta? Porque el ventilador no funciona correctamente.
¿Por qué el ventilador no funciona correctamente? Porque está obstruido con polvo.
¿Por qué está obstruido con polvo? Porque no se ha limpiado en mucho tiempo.
¿Por qué no se ha limpiado en mucho tiempo? Porque no existe un programa de mantenimiento regular para los equipos.

3. **Identificar la causa raíz:**

La última respuesta, en este caso "Porque no existe un programa de mantenimiento regular para los equipos", es la causa raíz del problema.

Las causas identificadas deben registrarse en la H02-MA-SIG-01 Matriz de gestión de riesgos.

¿Cómo determinar las consecuencias?

Los riesgos, una vez materializados, desencadenan una serie de efectos que pueden ser tanto beneficiosos como perjudiciales para La Corporación. Entre los primeros destacan las oportunidades de aprendizaje y desarrollo. Por otro lado, entre los segundos se encuentran las pérdidas económicas y los daños a la reputación, las consecuencias deben determinarse en el peor escenario, se sugiere emplear:

Análisis de escenarios: Es una herramienta estratégica que nos permite visualizar y evaluar diferentes futuros posibles para un proyecto, una empresa o una situación determinada. En lugar de intentar predecir un único futuro, esta técnica nos ayuda a identificar una variedad de escenarios que podrían ocurrir, considerando diferentes variables y factores que podrían influir en los resultados.

Pasos:
1. Preguntarse, ¿Qué pasaría si?
2. Construir narrativas de escenarios.
3. Evaluar las consecuencias en cada escenario.

Tiempo: Variable, depende de la complejidad del tema, se sugieren sesiones de mínimo 1 hora. Es posible que se requieran varias sesiones.
Número de personas por sesión: Se sugiere que sean grupos entre 5 a 10 personas, deben ser expertos en el tema a tratar y debe existir un facilitador quien debe guiar el proceso y asegurar que se aborden todos los aspectos relevantes.

Las consecuencias identificadas deben registrarse en la H02-MA-SIG-01 Matriz de gestión de riesgos.

5.4.3.2 Determinación de la probabilidad de ocurrencia e impacto de un riesgo

El primer paso en este proceso es comprender a fondo la naturaleza y el alcance de los riesgos a los que está expuesta La Corporación. Para ello, es crucial diferenciar entre el riesgo inherente y el riesgo residual.

El **riesgo inherente**, se refiere al nivel de riesgo que existe antes de aplicar cualquier control, representa la exposición natural al riesgo de una actividad, proceso o situación sin considerar ninguna acción que pueda reducir su probabilidad o impacto; es útil para identificar y evaluar la magnitud de los riesgos en estado bruto.

El riesgo residual, es el riesgo que persiste después de que se han aplicado controles y medidas de mitigación.

De acuerdo con lo anterior, el paso a seguir es la determinación de la probabilidad de ocurrencia del riesgo inherente, este es el proceso de estimar cuán probable es que un riesgo específico ocurra. Es una parte fundamental del análisis de riesgo, ya que nos permite evaluar la frecuencia con la que un evento puede suceder, es responsabilidad de cada gerencia determinar la probabilidad de ocurrencia para cada uno de los riesgos identificados, de acuerdo con la siguiente tabla:

Tabla 2. Probabilidad de ocurrencia

PROBABILIDAD	CUANTITATIVO	FRECUENCIA
Raro	1	Al menos una vez cada 3 años / Menor o igual al 5% de probabilidad que ocurra.
Poco frecuente	2	Una vez al año / Mayor a 5% o menor o igual al 25% de probabilidad de que ocurra.
Posible	3	Una vez por semestre / Mayor a 25% o menor o igual al 50% de probabilidad de que ocurra.
Frecuente	4	Al menos una vez al mes o entre / Mayor a 50% o menor o igual al 75% de probabilidad de que ocurra.
Casi seguro	5	Al menos una vez cada semana / Se espera que ocurra el evento en una probabilidad mayor al 75%

5.4.3.3 Determinación del impacto del riesgo

La determinación del impacto es un proceso clave en la gestión de riesgos que consiste en evaluar y cuantificar las consecuencias negativas que podría tener la materialización de un riesgo específico. En otras palabras, es responder a la pregunta: "¿Qué tan malo sería si este riesgo ocurriera?".

Tabla 3. Impacto

SEVERIDAD	CUANTITATIVO	OPERACIONAL	LEGAL / CUMPLIMIENTO	ECONÓMICO	REPUTACIONAL
INSIGNIFICANTE	1	• Leves demoras en la programación de reuniones con inversores y o emprendedores. • Interrupciones técnicas breves y fácilmente solucionables en presentaciones virtuales. • Inconvenientes menores en la logística de eventos pequeños con inversionistas, con aliados apoyados o con emprendedores. • Fallos logísticos menores que no afectan la satisfacción del inversionista o asistente. • Fallos administrativos en la oportunidad de la respuesta a solicitudes.	Requerimientos recibidos por el sistema de PQRS de La Corporación.	Mayor a 0% y menor o igual a 1% del patrimonio.	• Impacto limitado al ámbito interno de La Corporación. • Sin afectación a la confianza de grupos de interés. • Sin mención en medios de comunicación.
BAJO	2	• Cancelación de una reunión individual con inversionista potencial o emprendedor. • Reprogramación de presentaciones virtuales por inconvenientes técnicos. • Retrasos en eventos corporativos de mediana escala con inversionistas, con aliados apoyados o con emprendedores. • Interrupciones temporales en el sistema CRM afectando el seguimiento a inversores, tomadores de decisión o emprendedores.	Observaciones y/o hallazgos por parte de los entes de control cuyo nivel de evaluación sea leve o bajo.	Mayor del 1% y menor o igual al 3% del patrimonio.	• Impacto general al ámbito interno de La Corporación. • Sin afectación a la confianza de grupos de interés. • Con mención baja en medios de comunicación.
MODERADO	3	• Cancelación de ronda de reuniones con múltiples inversionistas en un sector específico. • Problemas logísticos en evento empresarial de gran escala con inversionistas, con aliados apoyados o con emprendedores. • Caída de plataformas de La Corporación, tales como páginas web por 24 horas. • Pérdida temporal de información con respaldo disponible sobre proyectos en curso. • Cambio en el alcance de proyectos ciudad promovidos por La Corporación.	Observaciones y/o hallazgos por parte de los entes de control cuyo nivel de evaluación sea medio.	Mayor del 3% y menor o igual al 5% del patrimonio.	• Afectación moderada a la confianza de grupos de interés. • Con mención moderada en diferentes medios de comunicación.
MAYOR	4	• Reprogramación de evento de gran escala con inversionistas, con aliados apoyados o con emprendedores debido a fallas graves. • Pérdida de información crítica sobre inversiones en curso sin respaldo inmediato. • Problemas técnicos que afectan la realización de un evento importante. • Incumplimiento de compromisos con patrocinadores internacionales. • Cancelación en el alcance de proyectos ciudad promovidos por La Corporación.	Observaciones y/o hallazgos por parte de los entes de control cuyo nivel de evaluación sea alto. Demandas, acciones populares, acciones de grupo u otro instrumento legal que implique indemnizaciones o multas o sanciones por incumplimiento de la normatividad.	Mayor del 6% y menor o igual al 8% del patrimonio.	• Impacto significativo en la confianza de grupos de interés clave. • Con mención alta en diferentes medios de comunicación.
CATASTRÓFICO	5	• Pérdida definitiva de bases de datos de inversionistas, tomadores de decisión o emprendedores. • Incapacidad para operar los sistemas críticos por más de una semana. • Cancelación de un evento de gran escala de alto impacto con inversionistas o emprendedores.	Intervención total o parcial de La Corporación. Suspensión temporal o total de la operación.	Mayor al 8% del patrimonio.	• Afectación severa a la confianza de todos los grupos de interés y partes relacionadas. • La noticia se convierte en tendencia.

5.4.3.4 Priorización del riesgo

Al multiplicar el impacto por la probabilidad, obtenemos un valor numérico que representa el riesgo total asociado a ese evento. Esta cifra nos permite comparar diferentes riesgos y priorizar las acciones a tomar.

Tabla 4. Mapa de calor

PROBABILIDAD	CASI SEGURO	5	5	10	15	20	25
	FRECUENTE	4	4	8	12	16	20
	POSIBLE	3	3	6	9	12	15
	POCO FRECUENTE	2	2	4	6	8	10
	RARO	1	1	2	3	4	5
			1	2	3	4	5
			INSIGNIFICANTE	BAJO	MODERADO	MAYOR	CATASTRÓFICO
			IMPACTO				

De acuerdo con el valor numérico obtenido, se ubica dentro del mapa de calor.

Nivel	Acción
BAJO	Aceptable sin acción adicional, genera menores efectos que pueden ser fácilmente remediados.
MODERADO	Se requiere una pronta atención, se requiere establecer actividades con el objetivo de disminuir su impacto o probabilidad.
CRÍTICO	Se requiere plan de acción inmediato.

Es fundamental evaluar el riesgo en dos etapas: primero, el riesgo inherente, y luego, el riesgo residual una vez implementadas las medidas de control.

5.4.4 Controles

Los controles son las acciones específicas que se basan o están relacionadas directamente con las causas y la evaluación del riesgo, para su establecimiento y correcta documentación, cada uno de ellos debe dar respuesta como mínimo a las siguientes preguntas:

- ¿Qué se garantiza o asegura con la aplicación del control?
- ¿Qué actividad se ejecuta?
- ¿Cómo se ejecuta esa actividad?
- ¿Qué evidencia genera la aplicación del control?

Los controles serán evaluados de acuerdo con los siguientes criterios:

Tabla 5. Criterios de Evaluación

Categoría	Descripción	Definición	Desplazamiento	
			Probabilidad	Impacto
Totalmente Efectivo	Los controles han sido diseñados, operan sin deficiencias, y han	Aquí se incluirán exclusivamente los controles que, después de una evaluación exhaustiva tanto en términos de diseño como de operatividad, no presenten ninguna deficiencia y que, además,	2	2

Categoría	Descripción	Definición	Desplazamiento	
			Probabilidad	Impacto
	sido evaluados en los últimos 6 meses.	sean sometidos a pruebas semestrales de manera sistemática.		
Parcialmente Efectivo	Se implementan controles, pero presentan deficiencias en cuanto a la documentación del control y/o excepciones en operatividad justificadas, o la última evaluación de los controles se realizó hace más de 6 meses.	En esta categoría se sitúan los controles que, después de una evaluación, revelan deficiencias en cuanto a la documentación del control y/o excepciones en operatividad justificadas. Además, estos controles no están sujetos a evaluaciones semestrales, sino que se someten a un ciclo de revisión que abarca un período mayor a 6 meses. Excepciones en operatividad justificadas, se refiere a una situación en la que, a pesar de que un control está diseñado para funcionar de manera específica, ocasionalmente no se ejecuta de acuerdo con su diseño debido a circunstancias específicas y justificadas. Estas excepciones pueden ocurrir debido a razones temporales, eventos imprevistos o situaciones excepcionales, pero deben estar respaldadas por una justificación válida. Algunos ejemplos de excepciones justificadas pueden incluir: - Circunstancias de contingencia y/o emergencia. - Falta temporal de personal. - Cambios en el entorno tecnológico. - Cambios en la estructura organizativa.	1	1
No Evaluado	Los controles existen y son implementados, pero no se ha evaluado su diseño y/u operatividad.	Esta categoría abarca todos los controles que han sido identificados mediante indagaciones y discusiones con los responsables de los procesos y que forman parte integral del sistema de control interno del proceso.	1	0
Inefectivo	Los controles existentes han sido evaluados y presentan deficiencias en su diseño y/u operatividad.	Una deficiencia de control se define como una debilidad o fallo que reduce su capacidad para mitigar los riesgos asociados. a) Las deficiencias en diseño, se definen como una debilidad en componentes como: - Inadecuada segregación de funciones. - Desalineación con riesgo asociado. - La frecuencia y/o naturaleza impide identificar un error oportunamente. b) Las deficiencias en operatividad, se definen como una debilidad en la ejecución o implementación efectiva de los controles diseñados. Esto puede incluir: - Falta de evidencia en la ejecución del control. - El control no fue ejecutado en la frecuencia diseñada.	0	0

Categoría	Descripción	Definición	Desplazamiento	
			Probabilidad	Impacto
		- El control no fue ejecutado bajo la segregación de funciones diseñado. - El control no gestiona las excepciones identificadas.		
Ninguno	No existen controles para mitigar el evento de riesgo.	No existen controles para mitigar el evento de riesgo.	0	0

El **riesgo residual** es la cantidad de riesgo que permanece después de que se han implementado medidas de control para mitigar un riesgo identificado, para esto, se realiza la evaluación de controles y se hacen los desplazamientos correspondientes de acuerdo con la categoría del control.

5.4.5 Tratamiento de riesgos

El tratamiento de riesgos consiste en buscar y aplicar acciones para abordar los riesgos identificados dentro de La Corporación. Esto incluye la formulación de opciones para el tratamiento, la selección de las más adecuadas, la planificación e implementación de estas acciones, y la evaluación de su efectividad.

5.4.5.1 Tipos de tratamiento de riesgos

- **Aceptar:** La Corporación está dispuesta a asumir el riesgo, esto aplica para los riesgos en verde, es decir, con una severidad del riesgo residual mayor o igual a 1 y menor a 8, el líder de proceso define si establece planes de tratamiento.
- **Mitigar:** Para los riesgos cuya severidad residual sea mayor o igual a 8 es obligatorio establecer planes de tratamiento.
- **Transferir:** Se realiza con pólizas o terceros, tercerización de la contratación del personal.
- **Evitar:** La Corporación no acepta el riesgo, se encuentra fuera del apetito de riesgo.

5.4.5.2 Actividades y planes de acción

De acuerdo con el tipo de tratamiento de riesgos, se procede a realizar actividades y planes de acción para los riesgos en los que el tratamiento sea mitigar, estas actividades pueden derivar en controles para el siguiente ciclo de gestión de riesgos.

Debe contener como mínimo:

- Acciones para mitigar el riesgo.
- Actividades.
- Responsables.
- Cronograma de implementación.

5.4.6 Monitoreo de los riesgos

El monitoreo de riesgos es un proceso dinámico y evolutivo que implica una revisión periódica de los riesgos identificados. En La Corporación, dicha periodicidad es anual o de acuerdo con la consideración de la Junta Directiva o la Dirección Ejecutiva, donde se evalúa la vigencia y eficacia de las medidas de

control establecidas, incorporando nueva información y adaptando las estrategias de gestión de riesgos a las cambiantes condiciones del entorno, así mismo se hará seguimiento a los indicadores asignados a los riesgos que de materializarse podrían generar mayor impacto, el seguimiento se realizará de forma trimestral.

5.4.7 Comunicación en la gestión de riesgos

La comunicación efectiva en la gestión de riesgos es fundamental para garantizar la transparencia, la colaboración y la toma de decisiones informadas en La Corporación.

Se realizará bajo las modalidades que La Corporación tiene para informarle a los trabajadores directos e indirectos y su periodicidad dependerá de la aplicación y roles y responsabilidades definidos en este manual.

5.4.7.1 Capacitación

Se realizará capacitación a todo el personal involucrado de acuerdo con su rol en la gestión de riesgos, mediante talleres, charlas y actividades con el fin de mejorar el conocimiento y las habilidades de los empleados apoyado en material didáctico que facilite la comprensión de los conceptos clave.

5.4.7.2 Inducción

En el ingreso del personal, se incluirá en la inducción la gestión de riesgos con el fin de que el nuevo personal se incorpore de forma adecuada a su rol.

5.4.7.3 Informes periódicos

Se realizarán informes concisos sobre los riesgos identificados en La Corporación, donde se incluirá información estadística del comportamiento de estos, con periodicidad semestral.

5.4.7.4 Comunicación individual

Se mantendrá una comunicación fluida con los responsables de cada área para abordar sus inquietudes y proporcionar la información necesaria.

6. DOCUMENTOS REFERENCIA

- POL-SIG-04 Política de gestión de riesgos.
- H02-MA-SIG-01 Matriz de gestión de riesgos.
- IN-SIG-02 Instructivo de la herramienta para la gestión de riesgos.

7. HISTORIAL DE CAMBIOS

Fecha	Versión	Descripción
Abril 10 de 2014	01	• Creación del Manual.
Diciembre 17 de 2012	03	• Se incluyó la metodología de los riesgos de gestión ambiental, de seguridad y salud en el trabajo.
Noviembre 26 de 2019	04	• Se incluyó el análisis del contexto interno y externo. • La metodología relacionada con los riesgos de la seguridad de la información. • Se ajustó la definición de términos relacionado con el riesgo de la planeación estratégica.
Enero 27 de 2022	05	• Se incluye metodología lineamientos de la Guía de Administración del Riesgo del Departamento Administrativo de la Función Pública en su versión 5, en respuesta a lo que en materia de gestión del riesgo dispone el Modelo Integral de Planeación y Gestión en su manual operativo (MIPG) versión 3, y la base técnica de la norma ISO 31000 en su versión 2018.
Diciembre 30 de 2024	06	• Se creó la POL-SIG-04 Política de Gestión de Riesgos. • Se actualizó el nombre del documento a Manual de gestión de riesgos IIB. • Se realizó una revisión integral del Manual de Gestión de Riesgos que derivó en una restructuración del documento. • Los cambios fundamentales comprendieron: la incorporación de un nuevo capítulo dedicado a controles; la actualización y precisión de definiciones clave; la redefinición de roles y responsabilidades, incluyendo el cargo y funciones del Profesional de Gestión de Riesgos ; el reajuste de los niveles de aceptación del riesgo; la simplificación y modificación de las categorías de clasificación de riesgos; y la incorporación de los conceptos de riesgo inherente y residual en la metodología de gestión de riesgos.

8. APROBACIÓN

Aprobación	Nombre	Cargo	Fecha
Elaboró	Johana Agudelo	Profesional en Gestión de Riesgos	Diciembre 30 de 2024
Revisó	Daniela García	Profesional en Gestión Integral	
Aprobó	Carlos Alberto Suárez	Gerente Administrativo y Financiero	

Carlos Alberto Suárez
Gerente Administrativo y Financiero