POLÍTICA DE GESTIÓN DE RIESGOS

1. OBJETIVO

Definir los lineamientos de un marco claro y accesible para identificar, evaluar, tratar y monitorear riesgos que puedan impactar a La Corporación, asegurando que todos los empleados comprendan su rol en la gestión del riesgo.

2. ALCANCE

Esta política será 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. RESPONSABLE

Esta política será responsabilidad del Gerente Administrativo y Financiero y del Profesional de Gestión de Riesgos, no obstante, todos los empleados pueden ejercer acciones colaborativas en la identificación y priorización de los riesgos de La Corporación.

4. PILARES

- **Transparencia:** Promover una cultura de reporte y registro en la gestión de riesgos, fomentando la comunicación abierta y la colaboración entre todos los niveles de La Corporación.

- **Prevención:** Adoptar medidas proactivas para mitigar los riesgos, antes de que se materialicen y causen impactos negativos.

- **Mejora continua:** Implementar un enfoque fundamental en la gestión de riesgos que implica la evaluación y evolución constante de los procesos y controles para minimizar riesgos y maximizar oportunidades.

- **Responsabilidad:** Definir roles específicos en todos los niveles de La Corporación en materia de gestión de riesgos, asegurando su compromiso y participación.

5. LINEAMIENTOS

La Corporación se compromete a:

a. Establecer un marco normativo y prescriptivo que exprese el nivel de riesgo aceptable que La Corporación pueda asumir para alcanzar sus objetivos estratégicos.

b. Identificar proactivamente los riesgos que puedan afectar el cumplimiento del propósito superior, con el propósito de asegurar la correcta identificación, definición y adecuada gestión de aquellos riesgos que puedan impactar a La Corporación.

c. Identificar las causas y consecuencias de forma consciente, rigurosa y basada en la evidencia de ser posible de cada uno de los riesgos definidos, de manera que se pueda realizar una correcta evaluación de los riesgos.

d. Evaluar la probabilidad y el impacto potencial de cada riesgo identificado, utilizando metodologías como benchmarking, buenas prácticas, datos históricos, análisis estadísticos, talleres y sesiones de trabajo, datos económicos y de mercado e informes de auditoría.

e. Mitigar de manera efectiva los riesgos mediante la implementación de planes de acción y controles internos, priorizando aquellos cuyo análisis de probabilidad e impacto puedan presentar un mayor valor de ocurrencia, de impacto o ambas, y por lo tanto representen un mayor riesgo al cumplimiento del propósito superior de La Corporación.

f. Monitorear continuamente los riesgos identificados y la efectividad de las medidas de mitigación, ajustando las estrategias cuando sea necesario.

g. Fomentar una cultura de gestión de riesgos en toda La Corporación, con el propósito de promover la toma de decisiones orientada en medición y la mitigación de riesgos, en colaboración y visión de cada uno de los diferentes equipos internos y externos y áreas.

h. Comunicar a las partes interesadas internas y externas sobre los riesgos que enfrentamos y las medidas que estamos tomando para gestionarlos.

i. Asignar los recursos financieros, humanos y tecnológicos necesarios para garantizar la implementación efectiva de esta política.

j. Realizar la asignación de responsabilidades de esta política a todos los empleados de La Corporación.

k. Capacitar periódicamente en esta política a todos empleados directos, contratistas y las personas relacionadas directa o indirectamente con La Corporación.

6. PROCESOS ASOCIADOS Y DOCUMENTOS DE REFERENCIA

- MA-SIG-01 Manual de gestión del riesgo IIB.

7. ANEXOS

Anexo 1. Identificación de riesgos
Anexo 2. Apetito al riesgo

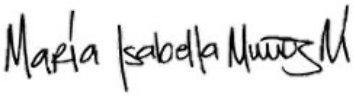
8. HISTORIAL DE CAMBIOS

Fecha	Versión	Descripción
2024	01	• Primer ejemplar.

9. APROBACIÓN

Aprobación	Nombre	Cargo	Fecha
Elaboró	Johana Agudelo Daniela García	Profesional Gestión de Riesgos Profesional en Gestión Integral	2024

Aprobación	Nombre	Cargo	Fecha
Revisó	Alexandra Beltrán Carlos Alberto Suárez	Jefe Jurídico Gerente Administrativo y financiero	
Vo.Bo.	Comité Buen Gobierno		
Aprobó	Junta Directiva		



Isabella Muñoz
Directora Ejecutiva

Aprobado por la Junta Directiva según acta 202 del 17 de diciembre del 2024.

Anexo 1. Identificación de riesgos

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.

El ejercicio de identificación de los riesgos de gestión para los procesos se realiza por parte de los líderes de proceso, en compañía de los miembros de su equipo que considere pertinentes y del profesional de gestión de riesgos, con base en la posible afectación a los objetivos de cada proceso.

Para mitigar los riesgos asociados con corrupción y seguridad de la información, se sugiere implementar un paso adicional en el proceso. Este paso específico será detallado al final del presente anexo.

Este anexo introduce el uso de diversas herramientas técnicas y estadísticas que facilitarán la identificación de los riesgos como:

i. **Lluvia de ideas:** Es una técnica creativa y colaborativa que se utiliza para generar un gran número de ideas sobre un tema o problema específico.

El objetivo principal de esta técnica es crear un espacio libre de crítica para que todos participen y la innovación pueda prosperar.

La lluvia de ideas estimula la creatividad y convoca a la participación de todos, lo que la convierte en una gran herramienta para generar una amplia variedad de ideas en poco tiempo. En especial, es útil cuando se busca solucionar un problema que te resulta muy cercano. En ocasiones, escuchar puntos de vista externos puede generar impulso para alcanzar una solución.

Pasos:

1. Definir el problema o tema a abordar.
2. Establecer reglas básicas.
   - No criticar ninguna idea.
   - Alentar una diversidad amplia de ideas.
   - No temer compartir ideas poco realistas o poco convencionales.
3. Generar ideas durante un tiempo determinado, se sugiere que sea entre 15 y 20 minutos.
4. Organizar y categorizar las ideas: Una buena práctica es utilizar notas adhesivas para mantener el anonimato de los participantes, además permiten documentar fácilmente las ideas y trasladarlas a un tablero para agruparlas.
5. Se identifican los riesgos con mayor probabilidad de ocurrencia e impacto.

Tiempo: Dependerá del tamaño del grupo, se sugiere que se realice en sesiones entre 30 y 60 minutos.
Número de personas por sesión: Se sugiere que se realice en grupos entre 5 a 10 personas donde se involucren diversos niveles de cargos y al menos un representante de cada una de las áreas involucradas en el proceso, aún si no pertenecen a una misma área.

ii. **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. Definir el horizonte de tiempo en el que se desarrollará el escenario y el alcance.
2. Identificar los factores de generación de incertidumbre.
3. Construir narrativas de escenarios.
4. Evaluar las implicaciones de cada escenario.
5. Se identifican los riesgos con mayor probabilidad de ocurrencia e impacto.

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.

iii. **Entrevistas estructuradas o semiestructuradas:** Son útiles cuando es difícil hacer que las personas se reúnan para una sesión de lluvia de ideas o cuando el flujo libre de una discusión en un grupo no es el adecuado para las situaciones o las personas implicadas, así mismo, es útil cuando se tratan temas técnicos específicos, cuyo manejo lo hacen pocas personas en La Corporación o incluso se hace consultoría con externos. Son una herramienta fundamental en la investigación cualitativa, y su diseño puede variar según el nivel de estructura que se le otorgue, es importante generar preguntas abiertas y evitar los sesgos.

Pasos:

1. Definir el objetivo de la entrevista y los tipos de riesgos a identificar.
2. Identificar a los expertos clave en el área de interés, estas serán las personas por entrevistar.
3. Desarrollar un conjunto de preguntas abiertas y cerradas que cubran los diferentes tipos de riesgos (financieros, operativos, legales, etc.).
4. Realizar las entrevistas de manera estructurada, siguiendo el guion y permitiendo que los entrevistados amplíen sus respuestas.
5. Transcribir las entrevistas y analizar las respuestas para identificar los riesgos recurrentes y las percepciones clave.
6. Se identifican los riesgos con mayor probabilidad de ocurrencia e impacto.

Tiempo: El tiempo de cada entrevista puede variar, pero se sugiere hacer entrevistas de 30 a 60 minutos.
Número de personas por sesión: Se sugiere entrevistar entre 2 y 3 expertos, de forma individual.

iv. **Técnica *What if*? (¿Qué pasa sí?):** Consiste en plantear diferentes escenarios hipotéticos para prever posibles resultados y consecuencias de una acción o decisión. El facilitador y el equipo utilizan frases normales del tipo “que pasaría si” en combinación con las indicaciones para investigar como un proceso, un servicio o una actividad se verán afectados por las desviaciones con respecto al comportamiento de las operaciones normales.

Los resultados de la identificación de los riesgos de gestión se registran en la matriz gestión de riesgos de La Corporación.

Pasos:

1. Definir el alcance, lo que delimita el proyecto, proceso o área a analizar.
2. Generación de preguntas: Se formula una serie de preguntas comenzando con "¿Qué pasaría si...?" que desafíen las suposiciones actuales y exploren diferentes escenarios.
   Ejemplos: "¿Qué pasaría si alguno de nuestros oficiales de inversión se enferma estando en un viaje?", "¿Qué pasaría si hay un ciberataque a La Corporación?", "¿Qué pasaría si cambia la legislación ambiental?".
3. Se recomienda realizar una lluvia de ideas, ya que esto promueve un ambiente creativo donde los participantes pueden generar libremente ideas y respuestas a las preguntas.
4. Se evalúan las posibles consecuencias de cada escenario, tanto positivas como negativas.
5. Se identifican los riesgos con mayor probabilidad de ocurrencia e impacto.

Riesgos de corrupción

La identificación de los riesgos de corrupción realiza de la misma manera que para los riesgos de gestión, sin embargo, es necesario validar que el riesgo identificado corresponda con la definición del riesgo de corrupción mediante la utilización del esquema guía de validación de riesgos de corrupción que se presenta a continuación. Si el riesgo identificado no cumple con **todas** las características definidas en dicha matriz, no se considera riesgo de corrupción. A continuación, se presenta el esquema guía de validación de riesgos de corrupción:

Tabla 1. 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 dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato	X	X	X	X

Fuente: Secretaría de transparencia de la presidencia de la república

Acción u omisión: Una acción en este sentido es cualquier acto deliberado que facilite o promueva la corrupción, una omisión, por su parte, es la falta de acción ante una situación que podría dar lugar a corrupción.

Uso del poder: Capacidad que tiene una persona o grupo para influir en decisiones, procesos o recursos de manera indebida, con el fin de obtener un beneficio personal o para terceros, en detrimento del interés general.
Desviar la gestión de lo público: Utilizar de manera indebida el poder o los recursos públicos para obtener un beneficio personal o para favorecer a un grupo específico, en lugar de servir al interés general.

Beneficio privado: Cualquier ventaja personal o de un grupo reducido que se obtiene a costa del interés general. Es decir, es cualquier ganancia, ya sea económica, política o de otro tipo, que se logra de manera ilícita al aprovechar una posición de poder o influencia dentro de una institución pública o privada.

Riesgos de seguridad de la información

Es un proceso fundamental que consiste en detectar y evaluar las posibles amenazas que podrían comprometer la confidencialidad, integridad o disponibilidad de los activos de información de La Corporación. En otras palabras, es como realizar un inventario de los peligros a los que está expuesta nuestra información más valiosa.

Para seguridad digital, se debe realizar la identificación de los activos de seguridad de información, un activo es cualquier elemento que tenga valor para La Corporación, sin embargo, en el contexto de seguridad digital, son activos elementos que utiliza La Corporación para funcionar en el entorno digital tales como: aplicaciones de La Corporación, servicios web, redes, información física o digital, tecnologías de información -TI, tecnologías de operación -TO. Para identificar estos activos, La Corporación debe cumplir con los siguientes pasos:

- Hacer un listado de los activos de información por cada proceso (Inventario activos de información).
- Identificar los dueños de los activos.
- Calificar los activos.
- Clasificar la información.
- Determinar la criticidad del activo.

Para cada activo evaluado como crítico se identificarán los riesgos de seguridad de la Información.
Los riesgos de seguridad de la información pueden ser de tres tipos según al atributo de la seguridad de la Información que impacte:

a. Pérdida de la Confidencialidad.
b. Pérdida de la Integridad.
c. Pérdida de la Disponibilidad.

La identificación y valoración de activos de información debe ser realizada por los líderes de proceso, en cada proceso donde aplique la gestión del riesgo de seguridad de la información, siendo un ejercicio orientado por el profesional de Gestión del conocimiento, el profesional de TI de La Corporación y con el acompañamiento del profesional de riesgos.

Así mismo los activos de información pueden ser clasificados en diferentes tipos de acuerdo con su naturaleza. En la siguiente tabla se presenta la clasificación de los tipos de activos de seguridad de la información.

Tabla 2. Tipos de activos de seguridad de la información

TIPO DE ACTIVO	DESCRIPCIÓN
DATOS/ INFORMACIÓN	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal

TIPO DE ACTIVO	DESCRIPCIÓN
	o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
SOFTWARE	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades.
SERVICIOS	Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información.
COMPONENTES DE RED	Servicio brindado por parte de La Corporación para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software).
PERSONAS	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades.
INFRAESTRUCTURA	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para La Corporación.
PROCESOS	Procedimientos, buenas prácticas, directrices, políticas y lineamientos de La Corporación para la realización o ejecución de sus funciones misionales.

Posteriormente a la identificación de los riesgos de Seguridad de la Información para cada activo crítico, se agrupan los activos por tipo de riesgo para realizar el análisis de las amenazas y vulnerabilidades que podrían causar su materialización.

Las amenazas, se definen como situaciones o fuentes que pueden generar daños a los activos y materializar los riesgos de Seguridad de la Información.

Las amenazas se clasifican en:

- **Deliberadas (D):** En donde existe la intención de generar daño, por ejemplo, piratería, falsificación de credenciales, hurto de información.
- **Fortuitas (F):** Las cuales pueden presentarse por efecto de errores involuntarios.
- **Ambientales (A):** Las cuales se pueden presentar como efecto, eventos naturales o como efecto colateral de otro evento.

La identificación de vulnerabilidades es un paso fundamental en cualquier estrategia de seguridad de la información. Consiste en detectar las debilidades o fallos en sistemas, aplicaciones, redes o procesos que podrían ser explotados por atacantes con intenciones maliciosas.

Las vulnerabilidades se clasifican en:

- **Vulnerabilidades de software:** Son debilidades o errores presentes en el código fuente de una aplicación o sistema operativo que pueden ser explotados por atacantes para obtener acceso no autorizado, modificar datos o causar daños.
- **Vulnerabilidades de la configuración:** Son debilidades o errores presentes en el código fuente de una aplicación o sistema operativo que pueden ser explotados por atacantes para obtener acceso no autorizado, modificar datos o causar daños.
- **Vulnerabilidades humanas:** Son debilidades que surgen del comportamiento de los usuarios, como errores humanos o la susceptibilidad a ataques de ingeniería social.

Matriz de identificación de peligros:

Tabla 3. Matriz de identificación del riesgo

N°. Riesgo	Proceso	Descripción del riesgo	Tipo de riesgo	Causas	Consecuencias	Responsable de seguimiento	Contexto		
							Interno	Externo	Proceso

- **N°:** Número consecutivo para identificar cada riesgo y facilitar su seguimiento.
- **Riesgo:** Una descripción clara y concisa del riesgo específico, utilizando un lenguaje sencillo y evitando tecnicismos excesivos.
- **Proceso:** El proceso al que pertenece el riesgo.
- **Descripción del riesgo:** Una explicación más detallada del riesgo, incluyendo los eventos o condiciones que podrían desencadenarlo.
- **Tipo de riesgo:** La categoría a la que pertenece el riesgo.
- **Causas:** Los factores que contribuyen a que el riesgo se materialice.
- **Consecuencias:** El impacto potencial del riesgo en caso de que ocurra.
- **Responsable de seguimiento:** El cargo del responsable del riesgo y las acciones de mitigación.
- **Contexto:** Seleccione con una X, si el riesgo se identificó partiendo del contexto interno, externo o del proceso.

Anexo 2. Apetito al riesgo

¿Por qué es importante determinar el apetito al riesgo?

1. Ayuda a La Corporación a tomar decisiones que estén alineadas con su visión a largo plazo.
2. Permite identificar y gestionar los riesgos de manera más efectiva.
3. Facilita la comunicación sobre la tolerancia al riesgo dentro de La Corporación.
4. Proporciona un marco de referencia para evaluar nuevas oportunidades.

Definiciones:

Apetito al riesgo: Es el nivel de riesgo que La Corporación está dispuesta a asumir para alcanzar sus objetivos estratégicos y operativos. Representa el balance entre riesgo y oportunidad que una empresa considera aceptable, dado su perfil y capacidad para gestionar esos riesgos.

Tolerancia: Es el nivel máximo de variación o desviación que La Corporación está dispuesta a aceptar en relación con un objetivo específico. En otras palabras, es el límite a partir del cual se considera que un riesgo es excesivo y debe ser mitigado.

Capacidad: Es la habilidad de La Corporación para absorber pérdidas o impactos negativos derivados de la materialización de un riesgo. Se relaciona con la solidez financiera, los recursos disponibles y la capacidad de recuperación de La Corporación.

Lineamientos:

La Dirección Ejecutiva, determinará el apetito riesgo de La Corporación, el cual se basará en los siguientes niveles:

Tabla 1. Nivel de apetito al riesgo

Nivel de apetito al riesgo	
BAJO	La Corporación evita riesgos innecesarios y se enfoca en proyectos con bajo perfil de riesgo.
MODERADO	La Corporación está dispuesta a asumir algunos riesgos calculados para alcanzar sus objetivos.
ALTO	La Corporación busca activamente oportunidades de alto riesgo y alta recompensa.

Nivel bajo:

Características:

- Prioriza la estabilidad y la predictibilidad.
- Evita inversiones especulativas o innovaciones radicales.
- Se enfoca en proteger los activos existentes.
- Los proyectos deben tener un alto grado de certeza en cuanto a sus resultados.

Consideraciones adicionales:

- Puede ser percibida como una organización poco innovadora.
- Puede perder oportunidades de crecimiento a largo plazo.

Nivel moderado:

Características:

- Balancea la búsqueda de oportunidades con la gestión del riesgo.
- Está dispuesta a asumir riesgos calculados para alcanzar objetivos estratégicos.
- Realiza análisis de costo-beneficio detallados antes de tomar decisiones.
- Implementa medidas de control de riesgos para mitigar posibles pérdidas.

Consideraciones adicionales:

- Fomenta una cultura de innovación controlada.
- Requiere una gestión de riesgos sólida.

Nivel alto:

Características:

- Busca activamente oportunidades de alto crecimiento, aunque impliquen mayor incertidumbre.
- Está dispuesta a invertir en proyectos innovadores y disruptivos.
- Tiene una alta tolerancia a la ambigüedad y al fracaso.
- Prioriza la velocidad y la agilidad en la toma de decisiones.

Consideraciones adicionales:

- Requiere una alta capacidad de adaptación y aprendizaje.
- Puede experimentar mayores pérdidas en caso de fracaso.

De acuerdo con el nivel de apetito de riesgo seleccionado, se define la capacidad y tolerancia de La Corporación, que se verá reflejada en los indicadores determinados y creados para cada uno de los riesgos identificados.

Es importante destacar que el apetito de riesgo no es estático y puede cambiar con el tiempo. Factores internos y externos, como cambios en el mercado, la competencia o la situación económica, pueden afectar la disposición de La Corporación a asumir riesgo. Algunas preguntas a considerar que pueden ser guía para definir el apetito al riesgo de La Corporación:

Tolerancia al fracaso: ¿Cuál es la reacción de La Corporación ante resultados negativos?
Cultura organizacional: ¿Fomenta la toma de riesgos o la aversión al riesgo?
Estructura financiera: ¿Existe un "colchón" financiero para absorber posibles pérdidas?
Liderazgo: ¿Los líderes están dispuestos a asumir riesgos y empoderar a sus equipos?
Complejidad del entorno: ¿El entorno de negocios es estable o volátil?