.

# MANUAL DE RIESGOS INTEGRADOS INVEST IN BOGOTÁ

**Noviembre, 2021**

**CONTENIDO**

1. INTRODUCCIÓN....3
2. OBJETIVOS....3
2.1 Objetivo general....3
2.2 Objetivos específicos....3
3. ALCANCE....3
4. DEFINICIONES....4
5. POLÍTICAS....6
5.1 Políticas de Administración del Riesgo....6
5.2 Políticas Específicas....6
6. RESPONSABILIDAD FRENTE A LA GESTIÓN DEL RIESGO DE ACUERDO CON EL ESQUEMA DE LÍNEAS DE DEFENSA....7
7. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO....9
7.1 Contexto de la Organización....9
7.2 Metodología para el Análisis del Contexto....10
7.3 Frecuencia y Responsabilidad Frente al Análisis del Contexto....12
8. IDENTIFICACIÓN DEL RIESGO....13
8.1 Identificación de riesgos por proceso....13
9. CLASIFICACIÓN DEL RIESGO....13
10. Identificación de los Riesgos de Corrupción....16
12. ANÁLISIS DEL RIESGO....21
14.APROBACIÓN....25

## 1. INTRODUCCIÓN

El presente manual establece las directrices y metodologías del Sistema de Administración de Riesgos de la Corporación para el Desarrollo y la Productividad de Bogotá Región Dinámica Invest in Bogotá, para el cual se ha tomado como referencia, los 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.
Para la Corporación la Administración de los riesgos es el conjunto de objetivos, políticas, procedimientos, herramientas y acciones que se implementan para identificar, analizar, evaluar, tratar, monitorear y revelar los riesgos a que se encuentre expuesta en el desarrollo de sus operaciones.
El Manual Integral de Administración del Riesgo de IIB tiene como propósito establecer la metodología de aplicación, reconocimiento y gestión de los riesgos que puede impedir o dificultar el logro de sus objetivos estratégicos y de sus procesos, los riesgos de corrupción, seguridad de la información, seguridad y salud en el trabajo (SGSST) y gestión ambiental (PIGA). En concordancia con la ISO 9001 versión 2018 se pretende que la gestión de riesgos se involucre con el direccionamiento estratégico, la gestión de los procesos y el desarrollo de auditorías internas. Se busca que cada uno de los colaboradores de la Corporación conozca sus riesgos, sea participe en la identificación y en la propuesta de acciones preventivas y en su seguimiento.

## 2. OBJETIVOS

### 2.1 Objetivo general

El objetivo del presente manual es establecer y formalizar la metodología que será aplicada en Invest In Bogotá para la administración de los riesgos de gestión, corrupción y seguridad de la información en todas las etapas apartir del análisis y monitoreo del contexto de la Corporación. La metodología desarrollada enel manual define los detalles para llevar a cabo las actividades de identificación,análisis, evaluación, tratamiento, monitoreo y reporte de los riesgos.

### 2.2 Objetivos específicos

- Establecer una metodología integral para la administración de riesgos, de acuerdo con el marco normativo vigente que tenga en cuenta los riesgos de gestión, de corrupción, de seguridad digital, ambiental y de seguridad y salud en el trabajo.
- Dar a conocer el marco general de actuación para la gestión de los riesgos, mediante lineamientos metodológicos para identificar, analizar, valorar, establecer controles, determinar los responsables y formular planes de tratamiento de los riesgos de gestión.
- Comunicar a todos los niveles de la Corporación los lineamientos sobre la gestión del riesgo para generar cultura y compromiso en la aplicación de la metodología propuesta en el presente manual.
- Asignar responsabilidades a las líneas de defensa para la identificación, formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos, así como su seguimiento y reporte de estos.
- Establecer lineamientos para el monitoreo y evaluación de los controles propuestos para la mitigación de los riesgos.

## 3. ALCANCE

Las directrices establecidas en el presente manual son de obligatoria aplicación para todos los riesgos que aborda la Corporación en todos los procesos y en todos los niveles, desde el análisis del contexto interno, externo y de proceso. hasta la identificación, evaluación, tratamiento, monitoreo y reporte del seguimiento a la matriz de riesgos. Así mismo esta

metodología, para la administración de los riesgos en el sistema de gestión de calidad, sistema de gestión de seguridad y salud en el trabajo, seguridad de la información, riesgos ambientales y los riesgos de la gestión documental.

## 4. DEFINICIONES

Para el sistema de administración del riesgo de la Corporación se tendrán en cuenta los siguientes términos:

*Tabla 1 Definiciones*

| TÉRMINO | DEFINICIÓN |
|---|---|
| ***ACTIVO*** | En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital. |
| ***ADMINISTRACIÓN DE RIESGOS*** | Conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos. |
| ***AMENAZA*** | Situación externa que no controla la entidad y que puede afectar su operación. |
| ***APETITO DE RIESGO*** | Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar. |
| ***CALIFICACIÓN DEL RIESGO*** | Estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización. |
| ***CAPACIDAD DE RIESGO*** | Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad. |
| ***CAUSA*** | Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo Medios, circunstancias y/o agentes que generan riesgos |
| ***CAUSA INMEDIATA*** | Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo. |
| ***CAUSA RAÍZ*** | Causa principal o básica, corresponde a las razones por la cuales se puede presentar |
| ***CONFIDENCIALIDAD*** | Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados |
| ***ANÁLISIS DEL RIESGO INHERENTE*** | Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo, sin considerar los controles existentes. |
| ***ANÁLISIS DEL RIESGO RESIDUAL*** | Corresponde al nivel de riesgo que permanece después de haber identificado y evaluado la eficacia de los controles para mitigar los riesgos. |
| ***CONTEXTO*** | Factores externos e internos que pueden afectar la capacidad de la Entidad para alcanzar los objetivos y metas. |
| ***CONTEXTO EXTERNO*** | Factores externos a la entidad sobre los cuales no tiene control directo pero que pueden afectar positiva o negativamente su capacidad para alcanzar los objetivos y metas |
| ***CONTEXTO INTERNO*** | Factores internos a la entidad sobre los cuales tiene control directo ypueden afectar positiva o negativamente su capacidad para alcanzar los objetivos y metas. |
| ***CONTROL*** | Medida o mecanismo que busca disminuir o mitigar el nivel de riesgo, actuandosobre las causas sobre las consecuencias |

| TÉRMINO | DEFINICIÓN |
|---|---|
| ***CONSECUENCIA O IMPACTO*** | Efecto negativo generado por la materialización de un riesgo yque puede afectar los resultados previstos. |
| ***CORRUPCIÓN*** | Uso del poder, por acción o por omisión, para desviar la gestión de lo público hacia el beneficio particular |
| ***DISPONIBILIDAD DE LA INFORMACIÓN*** | Acceso y utilización de la información y los sistemasde tratamiento de esta por parte de los individuos, entidades o procesos autorizadoscuando lo requieran. |
| ***EVALUACIÓN DEL RIESGO*** | Proceso de comparación de los resultados del análisis del riesgocon los criterios del riesgo para determinar si el riesgo se asume o se trata a través de una acción preventiva. |
| ***FACTOR DEL CONTEXTO*** | Subcategoría del contexto sobre la que se analizan los aspectos específicos que dificultan o facilitan el logro de los objetivos de la Entidad. |
| ***FUENTE GENERADORA DE RIESGOS:*** | Elemento del factor del contexto que solo en combinación tiene el potencial intrínseco de originar un riesgo o una oportunidad. |
| ***IDENTIFICACIÓN DEL RIESGO*** | Proceso sistemático para encontrar, reconocer y describir losriesgos surgidos del contexto que pueden dificultar u obstaculizar el logro de losresultados previstos. |
| ***IDENTIFICACIÓN DE LA OPORTUNIDAD*** | Proceso sistemático para encontrar, reconocer y describir las oportunidades surgidas del contexto que pueden facilitar o potenciar el logrode los resultados previstos. |
| ***INTEGRIDAD DE LA INFORMACIÓN*** | Mantenimiento de la exactitud y completitud de lainformación y los métodos de proceso. |
| ***GESTIÓN DEL RIESGO DE CORRUPCIÓN*** | Conjunto de actividades coordinadas para dirigir y controlar la Entidad en lo relacionado al riesgo de corrupción |
| ***MATRIZ DE RIESGOS*** | Herramienta que permite visualizar cuáles son los riesgos y oportunidades que han sido identificados por la Entidad y su estado de gestión |
| ***MODELO INTEGRADO DE PLANEACIÓN Y DE GESTIÓN*** | Marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las Entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad ycalidad en el servicio, de acuerdo con el Decreto1499 de 2017. |
| ***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 |
| ***NIVEL DE TOLERANCIA AL RIESGO*** | Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad. |
| ***CAPACIDAD DE RIESGO*** | Es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad. |
| ***PLAN ANTICORRUPCIÓN Y DE ATENCIÓN AL CIUDADANO*** | Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las Entidades del orden nacional, departamental y municipal. |
| ***PRIVACIDAD*** | Derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayanentregado o esté en poder de la entidad en el marco de las funciones que a ella le compete y que tiene obligación de proteger dicha información en observancia del marcolegal vigente |
| ***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*** | Efecto de la incertidumbre sobre los objetivos, entendido como la posibilidad deque suceda algún evento que tendrá un impacto negativo sobre los objetivos de la entidad, de un subsistema o de un proceso. |

| TÉRMINO | DEFINICIÓN |
|---|---|
| | |
| ***RIESGO INHERENTE*** | Es aquel al que se enfrenta una entidad en ausencia de acciones dela dirección para modificar su probabilidad o impacto. |
| ***RIESGO RESIDUAL*** | Nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento. |
| ***TRATAMIENTO DEL RIESGO*** | acciones que define la Entidad, tendientes a establecer o fortalecer un control que permita evitar, reducir o transferir un riesgo |

## 5. POLÍTICAS

### 5.1 Políticas de Administración del Riesgo

La Corporación se compromete a estructurar, implementar y mantener el Sistema de Administración de Riesgos con el propósito de identificar, analizar, evaluar, tratar y hacer seguimiento de los riesgos de gestión de los procesos, riesgos de corrupción, seguridad de la información, seguridad y salud en el trabajo y riesgos ambientales a los que está expuesta y que puedan generar un detrimento de su imagen, afectar la integridad de sus empleados. Mediante el diseño de controles efectivos aplicando una metodología propia y adecuada para el cumplimiento de los objetivos estratégicos.

### 5.2 Políticas Específicas

- Los responsables de procesos de la Corporación deben promover la cultura de prevención y gestión de riesgos a través de la aplicación de la metodología de administración de riesgos definida, la formulación y cumplimiento de los mecanismos de control de estos, con relación al manejo de información, y las actividades que se desarrollan en cumplimiento de su misión y de las exigencias de los entes de inspección, vigilancia y control.
- Todos los empleados de la Corporación deben participar en la administración de los riesgos de procesos a su cargo con criterios técnicos, de cumplimiento y evidenciados en el correcto desarrollo de sus actividades acordes con el modelo operativo por procesos implementado y dando cumplimiento a las políticas de operación y otros lineamientos adoptados para el desarrollo de estas.
- Con el propósito de impulsar la cultura de control de riesgos, todos los empleados de la Corporación deben informar al Asesor de calidad y Asesor de Control Interno los riesgos que se materialicen en desarrollo de las actividades para implementar las acciones a que haya lugar.

Para la Corporación, de acuerdo con su contexto, su misionalidad y la naturaleza de los procesos que desarrolla ha definido el nivel de aceptación del riesgo de acuerdo conlos siguientes criterios:

*Tabla 2 Nivel de aceptación del riesgo*

| NIVEL DE RIESGO INHERENTE | CRITERIOS DE DECISIÓN DEACEPTACIÓN DEL RIESGO | MÉTRICA | FRECUENCIA DE MONITOREO |
|---|---|---|---|
| **Inaceptable** | El riesgo en este nivel no se acepta. Deben establecerse medidas de intervención inmediatas para disminuir su calificación<br>Se debe tratar con cada gerencia y validar con la Dirección Ejecutiva, requiere la definición de planes de tratamiento para mitigar los riesgos. Se exceptúa la aplicación de estas acciones cuando son riesgos no controlables por la organización. | 80-100%<br>Probabilidad muy alta (5) | Bimestral |
| **Importante** | El riesgo en este nivel no se acepta. Es necesario que la entidad desarrolle acciones prioritarias a corto plazo para su mitigación, debido al alto impacto que tendría su materialización sobre el logro de losobjetivos | 51-79%<br>Probabilidad alta (4) | Trimestral |
| **Tolerable** | El riesgo en este nivel no se acepta. Es necesario desarrollar medidas de intervención sobre el riesgo con prioridad de segundo nivel para disminuir su calificación a una zona asumible | 50%<br>Probabilidad moderada (3) | Semestral |
| **Aceptable** | El riesgo en este nivel se acepta. El riesgo no presenta una gravedad significativa, por lo que no amerita la aplicación de acciones adicionales. El riesgo se debe gestionar mediantemonitoreo periódico.Ningún riesgo de corrupción puede aceptarse | 20-49%<br>Probabilidad baja (2)<br>0-19%<br>Probabilidad muy baja (1) | Semestral |

## 6. RESPONSABILIDAD FRENTE A LA GESTIÓN DEL RIESGO DE ACUERDO CON EL ESQUEMA DE LÍNEAS DE DEFENSA

El Modelo Integrado de Planeación y Gestión (MIPG) a través del Modelo Estándar de Control Interno (MECI) establece una estructura de control que determina los parámetros necesarios para la autogestión, la autorregulación y el autocontrol. Uno de los elementos fundamentales de esta estructura es el esquema de responsabilidades integrado por cuatro líneas de defensa el cual proporciona una manera efectiva para mejorar las comunicaciones en la gestión de los riesgos y los controles mediante la aclaración de las funciones y deberes relacionados. En la siguiente tabla se explica la aplicación de los roles y responsabilidades del esquema de líneas de defensa para IIB:

*Tabla 3 Roles y responsabilidades líneas de defensa IIB*

| LINEA DE DEFENSA | RESPONSABLE | RESPONSABILIDAD FRENTE A LA GESTIÓN DEL RIESGO |
|---|---|---|
| **LÍNEA ESTRATÉGICA** | La Alta Dirección de IIB (Dirección Ejecutiva)<br>El Comité Directivo | Analizar los riesgos y amenazas institucionales<br>Definir, aprobar y evaluar la Política de Administración del Riesgo de la Entidad<br>Implementar el Comité Institucional de Coordinación de Control Interno incrementando la periodicidad de las reuniones<br>Definir las líneas de reporte en temas claves para la toma de decisiones. |
| **PRIMERA LÍNEA DE DEFENSA** | Lideres de áreas y equipos<br>(Gerentes y equipos) | Identificar, evaluar, controlar y mitigar los riesgos através del autocontrol.<br>Mantener efectivamente los controles internos y loscontroles del día a día.<br>Conocer y apropiar las políticas, procedimientos,manuales, protocolos entre otras herramientas para el<br>autocontrol en los puestos de trabajo.<br>Informar a calidad y control interno sobre los riesgos sean identificados en los procesos |
| **SEGUNDALÍNEA DEDEFENSA** | Asesor Calidad<br>Comité de calidad<br>Oficial de Tecnología de la Información | Asegurar que los controles y procesos de gestión del<br>riesgo de la primera línea de defensa sean apropiados funcionen correctamente<br>Supervisar la implementación de prácticas eficaces para la gestión de los riesgos y para el diseño e implementación de controles<br>Evaluar y efectuar seguimiento a los controlesaplicados por la 1ª línea de defensa.<br>Realizar asesoría a la 1ª línea de defensa en la identificación de riesgos, el establecimiento de controles efectivos y la implementación de planes de tratamiento a los riesgos<br>Establecer los mecanismos para la autoevaluación sobre la gestión de los riesgos (seguimiento a través de herramientas objetivas, consolidación de informes<br>de gestión). |
| **TERCERALÍNEA DEDEFENSA** | Control Interno | Monitorear y revisar de manera independiente y<br>objetiva el cumplimiento de los objetivos institucionales y de procesos, a través de la adecuadagestión de riesgos<br>A través de su rol de asesoría, realizar orientación técnica y recomendaciones frente a la administracióndel riesgo en coordinación con Asesor deCalidad.<br>Realizar monitoreo a la exposición de la organizacióndel riesgo y realizar recomendaciones con alcance preventivo<br>Realizar asesoría proactiva y estratégica a la Alta Dirección y a los líderes de proceso, en materia decontrol interno y sobre las responsabilidades en materia de riesgos.<br>Formar a la alta dirección y a todos los niveles de laentidad sobre las responsabilidades en materia de riesgos.<br>Informar los hallazgos sobre la gestión de riesgo y proporcionar recomendaciones de forma independiente.1 |

Control interno debe llevar a cabo las siguientes acciones:

- Socializar anualmente la metodología de riesgos.
- Capacitar al grupo de trabajo de cada gerencia en la herramienta SIG para la gestión del riesgo.
- Liderar las mesas de trabajo de identificación del riesgo.
- Socializar y publicar el mapa de riesgos de gestión y de corrupción.

Los líderes de proceso tienen la responsabilidad de asegurar al interior de su grupo de trabajo el reconocimiento del concepto de "administración del riesgo", la política y la metodología definida, los actores y el entorno del proceso aprobados por la primera línea de defensa

Delegar, por parte del líder del proceso, el (los) profesionales que se encargarán del monitoreo, reporte y socialización del riesgo asociado.

## 7. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO

La Corporación ha definido su ciclo básico de gestión del riesgo en 5 etapas:

1. Establecimiento del contexto en el marco de administración de riesgos
2. Identificación del riesgo
3. Análisis, valoración, gestión del riesgo, monitoreo y revisión
4. Riesgos relacionados con posibles actos de corrupción
5. Riesgos de seguridad de la información

Teniendo en cuenta las etapas anteriores, se tendrán en cuenta parcialmente los lineamientos de la Guía para la Administración del riesgo y el diseño de controles en entidades públicas versión 5.

Para llevar a cabo la administración de los riesgos en la Corporación, se debe contar con una serie de pasos lógicos y ordenados que permitan su ejecución, realizar las actividades pertinentes para la construcción de herramientas de decisión gerencial que encaminen a la organización al proceso de mejoramiento continuo.
La metodología anterior se aplica para la administración de los riesgos de gestión, riesgos de corrupción, riesgos de seguridad digital, riesgos ambientales, riesgos de seguridad y salud en el trabajo y riesgos de seguridad y privacidad de la información. Para lograr esta integración de todos los riesgos en la misma metodología, este manual es un modelo de evaluación de riesgos que tiene en cuenta las particularidades de cada forma de calificación de acuerdo con lineamientos de cada tipo de riesgo.

Los numerales siguientes presentan cada una de las etapas a desarrollar durante la administración del riesgo. En la descripción de cada etapa se desplegarán 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.

### 7.1 Contexto de la Organización

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 de la misión y objetivos de la Corporación La definición del contexto estratégico contribuye al control de la organización frente a la exposición al riesgo porque permite conocer las situaciones generadoras de riesgos que facilita la formulación de controles que impidan el cumplimiento de los objetivos institucionales.

Para la definición del contexto estratégico, es fundamental tener claridad de la misión institucional: *"Facilitar la inversión internacional relevante, así como atraer reuniones y eventos de clase mundial que contribuyan al desarrollo socioeconómico, la competitividad y la calidad de vida de Bogotá-Región, posicionándola como el destino preferido para hacer negocios en América Latina"* y sus objetivos:

- Obj1: Atraer inversión extranjera para proyectos nuevos y proyectos de ciudad
- Obj2: Identificar y acompañar las oportunidades de reinversión de empresas extranjeras en Bogotá-Región
- Obj3: Articular el ecosistema de emprendimiento dinámico de Bogotá-Región y conectar capitales extranjeros con emprendimientos locales.
- Obj4: Promover a Bogotá - Región como destino para la inversión extranjera, el emprendimiento y la realización de eventos de negocios en América Latina.
- Obj5: Identificar y gestionar iniciativas y oportunidades de mejora del entorno de negocios en Bogotá Región
- Obj6: Atracción de congresos, viajes de incentivos y convenciones internacionales y articulación empresarios de la industria.

**7.2 Metodología para el Análisis del Contexto**

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

1. El análisis del contexto externo
2. El análisis del contexto interno
3. El análisis del contexto por proceso

*Tabla 4 Análisis del contexto*

| DIMENSIÓN | FACTOR | DESCRIPCIÓN |
|---|---|---|
| CONTEXTO EXTERNO | Políticos | Cambios de gobierno, legislación, políticas públicas, regulación. |
| | Económicos y financieros | Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia. |
| | Sociales y culturales | Demografía, responsabilidad social, orden público. |
| | Ambientales | Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible. |
| | Tecnológicos | Avances en tecnología, acceso a sistemas de informaciónexternos, gobierno en línea. |
| | Legales y reglamentarios | Normatividad externa (leyes, decretos, ordenanzas yacuerdos). |
| CONTEXTO INTERNO | Financieros | Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada. |
| | Personal | Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional. |
| | Procesos | Capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento. |
| | Tecnología | Integridad de datos, disponibilidad de datos y sistemas,desarrollo, producción, mantenimiento de sistemas de información. |
| | Estratégicos | Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo. |
| | Comunicación interna | Canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones. |
| | Activos de información | Información, aplicaciones, hardware entre otros, que se debenproteger para garantizar el funcionamiento interno de los procesos. |
| | Cultura organizacional | Es el conjunto de percepciones, sentimientos, actitudes, hábitos, creencias, valores, tradiciones y formas de interacción dentro y entre los grupos existentes en todas las organizaciones |
| | Objetivos estratégicos | Son los fines o metas desarrollados a nivel estratégico que una organización pretende alcanzar a mediano y largo plazo. |
| CONTEXTO DEL PROCESO | Diseño del proceso | Claridad en la descripción del alcance y objetivo del proceso. |
| | Interacciones con otros procesos | Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes. |
| | Transversalidad | Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad. |
| | Procedimientos asociados | Son aquellos que describen el proceso. |
| | Responsables del proceso | Son aquellos que lideran los procesos. |
| | Comunicación entre los procesos | Comunicación interna entre los procesos. |

| | | |
|---|---|---|
| **CONTEXTO DEL PROCESO** | Diseño del proceso | Claridad en la descripción del alcance y objetivo del proceso. |
| | Interacciones con otros procesos | Relación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes. |
| | Transversalidad | Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad. |
| | Procedimientos asociados | Pertinencia en los procedimientos que desarrollan los procesos. |
| | Responsables del proceso | Grado de autoridad y responsabilidad de los funcionarios frente al proceso. |
| | Comunicación entre los procesos | Efectividad en los flujos de información determinados en la interacción de los procesos. |

La Corporación a través de los procesos realizará el análisis de los factores anteriormente descritos periódicamente o cada vez se presente un cambio relevante en el contexto para establecer cuáles de ellos podrían afectar el logro de los objetivos estratégicos, de los procesos o de los planes, programas y proyectos.

Para lo anterior se debe realizar una clasificación **DOFA** para cada uno de los factores de contexto y de cómo se presenta el mismo frente a la entidad o frente al proceso analizado

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

- **Debilidad:** Factor interno que es controlado por la entidad, pero por sus característicaspuede generar un riesgo para la entidad.
- **Fortaleza**: Factor interno que es controlado por la entidad y que por sus características puede generar una oportunidad para la entidad o para sus procesos.
- **Amenaza**: Factor externo que es no está bajo el control de la entidad y que por sus características puede generar un riesgo para la entidad o para sus procesos. Para los riesgos de Seguridad de la información el concepto amenaza se asocia al concepto de Amenaza para los activos de la información.
- **Oportunidad:** Factor externo que no está bajo el control de la entidad y que por sus características puede generar una oportunidad para la entidad o para sus procesos.

**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 del contexto interno se pueden identificar Fortalezas y Debilidades, del análisis del contexto externo se identifican Oportunidades y Amenazas. Las Debilidades y Amenazas son fuentes generadoras de riesgos frente a los objetivos y Las Oportunidades y Fortalezas con fuentes generadoras de oportunidades frente al logro de los objetivos.

### 7.3 Frecuencia y Responsabilidad Frente al Análisis del Contexto

El análisis de contexto se debe realizar con frecuencia anual o en el momento en el que se presente un cambio o situación que pueda afectar el logro de los objetivos dela entidad.

Es responsabilidad de la Alta Dirección (línea estratégica) realizar el análisis de contexto de la entidad y dejar evidencia de este.

Es de responsabilidad del Dueño del Proceso (primera línea de defensa) en conjunto con su equipo de trabajo realizar el análisis de contexto de su proceso ydejar evidencia de este.

## 8. IDENTIFICACIÓN DEL RIESGO

La etapa de identificación de riesgos tiene varios componentes que se señalan a continuación:

### 8.1 Identificación de riesgos por proceso

- En la etapa de identificación de riesgos estratégicos, riesgos operativos, riesgos de corrupción, riesgos de imagen, riesgos de cumplimiento, riesgos financieros, riesgos tecnológicos, riesgos ambientales y riesgos de seguridad y salud en el trabajo será importante revisar los objetivos de los procesos y/o los compromisos establecidos en la planeación de la Corporación con el fin de determinar los eventos que potencialmente puedan afectar el cumplimiento de los objetivos institucionales.
- Dentro de la etapa de identificación de riesgos es importante aclarar que para los riesgos de seguridad digital y riesgos ambientales y de seguridad y salud en el trabajo se tendrán en cuenta criterios adicionales.
- La identificación de los riesgos de gestión se realiza con base en el resultado del análisisde los elementos del contexto interno y externo que pueden tener impacto en el logro de los objetivos de la Corporación, a partir de este análisis se determinan los posibles eventos que pueden afectar negativa o positivamente los objetivos, se establecen sus causas y sus consecuencias potenciales.
- El área de Calidad y control interno realizará el acompañamiento metodológico en los ejercicios de identificación de los riesgos de gestión en todos los niveles.
- Es responsabilidad del equipo directivo (línea estratégica) revisar los objetivos estratégicos e identificar los riesgos y oportunidades que pueden afectar esos objetivos.
- El ejercicio de identificación de los riesgos de gestión para los procesos se realiza por parte de los responsables de los procesos y sus equipos (primera línea de defensa) con base en la posible afectación a los objetivos de cada proceso.

## 9. 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 5 Clasificación del riesgo*

| Tipo de Riesgo | Descripción |
|---|---|
| **Riesgo Estratégico** | Posibilidad de ocurrencia de eventos que afecten los objetivos y políticas estratégicas de la Corporación. |
| **Riesgo Reputacional o imagen** | Posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de la Corporación ante sus clientes o partes interesadas |
| **Riesgo Corrupción** | posibilidad de que, por acción u omisión, se use el poderpara desviar la gestión de lo público hacia un beneficio privado. |
| **Riesgos Financieros y Contables** | Posibilidad de ocurrencia de eventos que afecten los recursos de la entidad y todos aquellos temas relacionados con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, ejecución presupuestal, estados financieros, pagos, manejos de excedentes de tesorería y manejo de los bienes |
| **Riesgo Operativo** | Posibilidad de ocurrencia de eventos que afecten los procesosmisionales de la IIB. |
| **Riesgo Tecnológico** | Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de IIB |
| **Riesgos de cumplimiento** | Posibilidad de ocurrencia de eventos que afecten la situación jurídica ocontractual de IIB debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales. |
| **Riesgo Ambiental** | Cambios en los impactos ambientales adversos obeneficiosos para la entidad.<br>Situaciones de emergencias<br>Cambios climáticos<br>Contaminación<br>Gestión de residuos<br>Cambios normativos y de aplicabilidad institucional |
| **Riesgo Seguridad y Salud en el Trabajo** | Condiciones de trabajo producto de las emociones de los integrantes de un equipo o de toda la Entidad; contempla aspectos físicos y emocionales y de manera directa en la motivación de los empleados.<br>• Espacio físico, instalaciones, temperatura<br>• Conflictos en los equipos de trabajo<br>• Debilidad en las relaciones interpersonales<br>• Estabilidad laboral<br>• Remuneración laboral<br>• Política de ascenso<br>• Bajo nivel de participación de los servidores en procesos de formación y capacitación<br>• Organización inadecuada del trabajo<br>• Planeación inadecuada del tiempo de trabajo<br>• Carga mental elevada<br>• Resistencia al cambio<br>• Desinterés de los servidores o equipos de trabajo<br>• Acoso laboral<br>• Pandemias |
| **Riesgo Seguridad de la Información** | Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos ysociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas. |

| | |
|---|---|
| **Riesgo gerencial** | Posibilidad de ocurrencia de eventos que afecten los procesosgerenciales y/o la alta dirección |
| **Riesgo seguridad física** | Situaciones externas que afectan la entidad |

Al realizar la identificación de los riesgos se debe obtener la siguiente información:

- **Riesgo:** Evento que puede afectar el cumplimiento del objetivo estratégico o del proceso según sea el caso.
- **Causas:** Se establecen los factores que pueden generar la materialización del riesgo. Es importante tener en cuenta que las causas deben ser gestionables a partirdel establecimiento de actividades de controles.
- **Consecuencias:** Se determinan los posibles efectos por la materialización del riesgo. Es importante tener en cuenta que frente a estas consecuencias se determinará posteriormente el nivel de impacto.

Para realizar una mejor identificación de los riesgos, el ejercicio puede apoyarse en las siguientes herramientas técnicas y estadísticas que facilitan el análisis de la informacióndisponible:

- **Lluvia de ideas**: Técnica usada para estimular y fomentar el flujo libre de laconversación entre un grupo de personas con conocimiento. Entre sus múltiples aplicaciones es útil para identificar los riesgos de un proceso o los criterios para las

decisiones y/o las opciones de tratamiento. La lluvia de ideas implica tratar de garantizar la estimulación de la imaginación de las personas mediante los pensamientos y las declaraciones de los otros participantes.

- **Técnica Delphi**: Es una técnica para obtener un consenso confiable de la opinión de ungrupo de personas expertas en un tema específico, aunque se asocia a la lluvia de ideas, una característica de esta técnica es que los expertos expresan sus opiniones individualmente y de manera anónima al tiempo que tiene acceso a los puntos de vista de otros expertos a medida que el proceso avanza.
- **Análisis de escenarios:** En este esquema también se busca que un grupo de personas asociadas al proceso determinen situaciones potenciales que pueden llegar a presentarse y con base en estas posibilidades, se determina qué puede llegara suceder y las consecuencias de la afectación.
- **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 deuna discusión en un grupo no es el adecuado para las situaciones o las personas implicadas. Estas se pueden aplicar en cualquier etapa la gestión del riesgo. Se creaun conjunto de preguntas pertinentes para guiar al entrevistador, siempre que sea posible las preguntas deberían ser abiertas, sencillas, tener un lenguaje adecuado para los entrevistados y abarcar solamente un aspecto. También se elaboran posibles preguntas de seguimiento para buscar aclaraciones. Se recomienda precaución para no "guiar" al entrevistado. Las respuestas se deberían tomar en consideración con algún grado de flexibilidad con el fin de brindar la oportunidad de explorar las áreas hacia las cuales el entrevistado puede querer dirigirse.
- **Técnica ¿qué pasa sí?:** La técnica es un estudio sistemático, basado en el trabajo de equipo, que utiliza un conjunto de palabras o frases de "indicación" que el facilitador utiliza frente a un taller para estimular a los participantes a que identifiquenlos riesgos. 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 deriesgos de gestión de la entidad. A continuación, se presenta un ejemplo de identificación de un riesgo de gestión:

*Tabla 6 Ejemplo identificación de riesgo*

| EJEMPLO DE RIESGO DE GESTIÓN | | | | |
|---|---|---|---|---|
| **DESCRIPCIÓN DELRIESGO** | | **TIPO** | **CAUSAS** | **EFECTOS O CONSECUENCIAS** |
| Inoportunidad en la adquisición de los bienes y servicios requeridos por laCorporación | La combinación de factores como insu-eficiente capacitación del personal de contratos, cambios en la regulación contractual, políticas desactualizadas, carencia de controles el Procedimiento de compras y contrataciones pueden ocasionar inoportunidad en la adquisición de los bienes y serviciosrequeridos por la entidad yen consecuencia, afectar la continuidad de su operación. | Riesgo de Gestión / Operativo | Carencia de controles en el procedimiento de contratación<br><br>Insuficiente capacita- ción del personal de contratos<br><br>Desconocimiento de los cambios en la re-gulación contractual Inadecuadas políticasde operación | Parálisis en los Procesos<br><br>Incumplimiento en la entrega de bienes y servicios a los grupos de valor<br><br>Demandas y demás accionesjurídicas<br><br>Detrimento de laimagen de laentidad ante susgrupos de valor<br><br>Investigacionesdisciplinarias |

## 10. Identificación de los Riesgos de Corrupción

La identificación de los riesgos de corrupción se realiza de la misma manera que para los riesgos de gestión. Para la identificación de los riesgos de corrupción, esnecesario 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 7 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.*

***Nota:*** *La descripción de los riesgos de corrupción debe concurrir con los componentes de su definición: Acción u omisión + uso del poder+ desviación de la gestión de público+ beneficio privado*

*Tabla 8 Análisis del impacto de los riesgos de corrupción*

| FORMATO PARA DETERMINAR EL IMPACTO | | |
|---|---|---|
| **Riesgo** | **Utilización indebida de información privilegiada, en provecho propio o de un tercero** | |
| **RC 1** | | |
| **No** | | **Respuesta** |

| | Pregunta<br>Si el riesgo se materializa podría? | SI | NO |
|---|---|---|---|
| 1 | ¿Afectar al grupo de funcionarios del proceso? | 0 | 1 |
| 2 | ¿Afectar el cumplimiento de metas y objetivos de la dependencia? | 1 | 0 |
| 3 | ¿Afectar el cumplimiento de misión de la Entidad? | 1 | 0 |
| 4 | ¿Afectar el cumplimiento de la misión del sector al que pertenece la Entidad? | 1 | 0 |
| 5 | ¿Generar pérdida de confianza de la Entidad, afectando su reputación? | 1 | 0 |
| 6 | ¿Generar pérdida de recursos económicos? | 0 | 1 |
| 7 | ¿Afectar la generación de los productos o la prestación de servicios? | 0 | 1 |
| 8 | ¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos? | 0 | 1 |
| 9 | ¿Generar pérdida de información de la Entidad? | 1 | 1 |
| 10 | ¿Generar intervención de los órganos de control, de la Fiscalía, u otro ente? | 0 | 1 |
| 11 | ¿Dar lugar a procesos sancionatorios? | 0 | 1 |
| 12 | ¿Dar lugar a procesos disciplinarios? | 0 | 1 |
| 13 | ¿Dar lugar a procesos fiscales? | 0 | 1 |
| 14 | ¿Dar lugar a procesos penales? | 0 | 1 |
| 15 | ¿Generar pérdida de credibilidad del sector? | 0 | 1 |
| 16 | ¿Ocasionar lesiones físicas o pérdida de vidas humanas? | 0 | 1 |
| 17 | ¿Afectar la imagen regional? | 0 | 1 |
| 18 | ¿Afectar la imagen nacional? | 0 | 1 |
| | | | |
| | **Total, preguntas afirmativas:** | 5 | |
| | **Total preguntas negativas:** | | 14 |
| | **CALIFICACIÓN DEL RIESGO** | **MODERADO** | |

**Ejemplo Esquema de Validación de Riesgos de Corrupción**

| EJEMPLO DE RIESGO DE CORRUPCIÓN | | | | |
|---|---|---|---|---|
| **RIESGO** | **DESCRIPCION** | **TIPO** | **CAUSAS** | **CONSECUENCIAS** |
| Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceroscon el fin celebrar un contrato. | Situaciones como: debilidades en la etapade la planeación delcontrato, la excesiva discrecionalidad, las presiones indebidas, la carencia de controles, lafalta de conocimiento y/o experiencia, sumados ala falta de integridadpueden generar un riesgo de corrupción enla contratación, comopor ejemplo "exigenciasde condiciones en losprocesos de selecciónque solo cumple undeterminado proponente". | Riesgo de Corrupción | Debilidades en la etapa de planeación, que faciliten la inclusión en los estudios previos, y/o en los pliegos de condiciones de requisitos orientados a favorecer a un proponente.<br><br>Presiones indebidas.<br><br>Carencia de controles en el procedimiento de contratación.<br><br>Falta de conocimiento y/o experiencia delpersonal que manejala contratación<br><br>Excesiva discrecionalidad.<br><br>Adendas que modifican las condiciones generales del proceso de contratación para favorecer a un proponente. | Pérdida de la imagen institucional.<br><br>Demandas contrael Estado.<br><br>Pérdida de confianza en lo público.<br><br>Investigaciones penales, disciplinarias y fiscales.<br><br>Detrimento patrimonial.<br><br>Obras inconclusas.<br><br>Mala calidad de las obras.<br><br>Enriquecimiento ilícito de contratistas y/o servidores públicos. |

## 11. Identificación de los Riesgos de Seguridad de la Información

### 11.1 Identificación y Valoración de Activos de Información

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 organización, sin embargo, en el contexto de seguridad digital, son activos elementos que utiliza la organización para funcionar en el entorno digital tales como: aplicaciones de la organización, servicios web, redes, información física o digital, tecnologías de información -TI, tecnologías de operación -TO. Para identificar estos activos, la entidad debe cumplir con los siguientes pasos:

1. Hacer un listado de los activos por de información por cada proceso (Inventario activos de información)
2. Identificar los dueños de los activos
3. Calificar los activos
4. Clasificar la información
5. Determinar la criticidad del activo

***Anexo1.*** *matriz de inventario activos de información*

Después se procederá a valorar el activo determinando la importancia de estosen el logro de los objetivos de los procesos y de la entidad y bajo este criterio establecer su criticidad y se establecen los controles adecuados para su protección.

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

Posteriormente a la identificación de los riesgos de Seguridad de la Información paracada activo, se agrupan los activos por tipo de riesgo para realizar el análisis de las amenazas y vulnerabilidades que podrían causar su materialización.
La identificación y valoración de activos de información debe ser realizada por la Primera Línea de Defensa – Líderes de Proceso, en cada proceso donde aplique la gestión del riesgo de seguridad de la información, siendo un ejercicio orientado por el responsable de Gestión Documental, el responsable de seguridad de la información de la Corporación y con el acompañamiento del área de Calidad como segunda línea de defensa y Control interno como tercera línea de defensa para la gestión del riesgo.
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.

| 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 o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros. |
| **SOFTWARE** | Activo informático lógico como programas, herramientas ofimáticas osistemas 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 DERED** | Servicio brindado por parte de la entidad para el apoyo de las actividades delos 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 conexperiencia y capacitado para realizar una tarea específica en la ejecución de las actividades |
| **INFRAESTRUCTURA** | Espacio o área asignada para alojar y salvaguardar los datos consideradoscomo activos críticos para la entidad |
| **PROCESOS** | Procedimientos, buenas prácticas, directrices, políticas y lineamientos de laentidad para la realización o ejecución de sus funciones misionales |

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 naturaleso como efecto colateral de otro evento.

### 11.2 Identificación de Vulnerabilidades de Seguridad de la Información

Las vulnerabilidades se entienden como las debilidades en los activos de seguridad de la Información o en su administración lo que incrementa el grado de exposición ante las posibles amenazas facilitando de esta manera la materialización de los riesgos.
Para identificar la vulnerabilidad se puede tomar como base la tabla de vulnerabilidadescomunes definida en la ISO /IEC 27005: 2009.

*9 Ejemplo de Vulnerabilidades Vs Amenazas*

| TIPO DE ACTIVO | EJEMPLOS DE VULNERABILIDADES | EJEMPLOS DE AMENAZAS |
|---|---|---|
| **HARDWARE** | Almacenamiento de medios sin protección | Hurto de medios o documentos |
| **SOFTWARE** | Ausencia de parches de seguridad | Abuso de los derechos |
| **RED** | Líneas de comunicación sin protección | Escucha encubierta |
| **INFORMACIÓN** | Falta de controles de acceso físico | Hurto de información |
| **PERSONAL** | Falta de capacitación en las herramientas | Error en el uso |
| **ORGANIZACIÓN** | Ausencia de políticas de seguridad | Abuso de los derechos |

*Tabla 10 Ejemplo de Riesgo de Seguridad de la Información*

| ACTIVO | RIESGO | DESCRIPCIÓN | TIPO | CAUSAS | | CONSECUENCIAS |
|---|---|---|---|---|---|---|
| | | | | Amenazas | Vulnerabilidades | |
| Base de datos de nómina | Pérdida de la integridad | La falta de políticas de seguridad digital, ausencia de políticas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada, lo cual causaría la pérdida de la integridad de la base de datosde nómina. | Riesgo de Seguridad de la Información | Modificaciónno autorizada | Falta de Políticas de Seguridad digital<br>Ausencia de Políticas de Control deacceso<br>Contraseñas sin protección<br>Autenticación débil | Posibles consecuenciasque pueda enfrentar la entidad o el proceso a causa de la materializaciónde riesgos(legales, económicos, sociales, reputacionales, confianza en el ciudadano).<br>Ej. posible retraso en el pago de nómina. |

## 12. ANÁLISIS DEL RIESGO

Esta etapa consiste en comprender la naturaleza y el nivel del riesgo, Lo anterior permite conocer el perfil de riesgo de la SSF en términos de criticidad, así mismo permite establecer prioridades para intervenir los riesgos. Para tal fin es necesario determinar el nivel de riesgo el cual resulta de analizar el nivel de probabilidad de ocurrencia y el nivel de impacto o consecuencias de cada riesgo identificado, con el fin de estimar la zona de riesgo inicial o (RIESGO INHERENTE), lo cual indica que se trata del nivel de riesgo sin aplicación de controles. Para realizar el análisis de los riesgos se deben seguir los siguientes pasos:

***Nota**: La determinación de la Probabilidad aplica de la misma manera para los 3 tipos*
*Determinación del Nivel de Probabilidad del Riesgo*

Consiste en evaluar de la manera más objetiva posible que tan expuesta esta la Entidad frente al riesgo que se está analizando.

La probabilidad puede ser entendida también como la frecuencia con la que el riesgose puede materializarse en términos de frecuencia y factibilidad.

- **Frecuencia:** se analizan el número de eventos en un periodo determinado, en cuyo caso se analizan los históricos de eventos asociados al riesgo.
- **Factibilidad:** se analiza la presencia de factores internos y externos que puedenpropiciar el riesgo que no se ha materializado y que se pueda pronosticar su materialización.

Este ejercicio debe ser participativo e incluir el juicio experto de los colaboradores que más conocen el proceso en donde se está llevando a cabo este análisis. Una deficiente o subjetiva determinación de los niveles de probabilidad o de impacto deriva en una ineficaz gestión de los riesgos.

| Calificación probabilidad de ocurrencia | Descripción | Frecuencia | Frecuencia para actividades continuas | Frecuencia para actividades o eventos ocasionales | Frecuencia en función de la exposición | Escala en función de especialización requerida para que el riesgo ocurra |
|---|---|---|---|---|---|---|
| **1. MUY BAJA** | La eventualidad de ocurrencia es muy baja, casi nula. | Ocurre ente el 0 – 19% de los casos | El evento ocurre anualmente | El evento nunca ha ocurrido | La situación de exposición se presenta de manera eventual durante la jornada laboral | Se requieren recursos o habilidades extremadamente especializadas para explotar la vulnerabilidad |
| **2. BAJA** | El evento podría ocurrir sólo bajo circunstancias muy excepcionales. | Ocurre ente el 20 – 39% de los casos | El evento ocurre semestralmente | el evento ocurre una de cada 20 veces que se realiza la actividad | La situación de exposición se puede presentar alguna vez en un periodo de tiempo corto durante la jornada laboral | Se requieren recursos o habilidades de Administrador del Sistema o programador experimentado para explotar la vulnerabilidad |
| **3. MODERADA** | El evento podría ocurrir en algún momento. | Ocurre ente el 40 – 59% de los casos | El evento ocurre mensualmente | el evento ocurre una de cada 10 veces que se realiza la actividad | La situación de exposición se puede presentar alguna vez por un periodo de tiempo prolongado durante la jornada laboral | Se requieren recursos o habilidades básicas de usuario TI y conocimientos generales del negocio para explotar la vulnerabilidad |
| **4. ALTA** | El evento puede ocurrir algunas veces. | Ocurre entre el 60 – 79% de los casos | El evento ocurre semanalmente | el evento ocurre una de cada 5 veces que se realiza la actividad | La situación de exposición se puede presentar varias veces, por periodos de tiempo cortos durante la jornada laboral | Se requieren recursos o habilidades muy limitadas para explotar la vulnerabilidad |
| **5. MUY ALTA** | Se espera que el evento ocurra en la mayoría de las circunstancias. | Ocurre entre el 80 – 100% de los casos | El evento ocurre diariamente | El evento ocurre una de cada dos veces que se realiza la actividad | La situación de exposición se puede presentar varias veces por periodos de tiempo prolongados durante la jornada laboral | No se requiere ningún recurso o habilidad especial. para explotar la vulnerabilidad |

Los criterios para calificar el nivel de probabilidad de cada riesgo se muestran en la siguiente tabla

*11Criterios para Calificar Nivel de Probabilidad del Riesgo Inherente*

| Tabla de valoración de impacto de riesgo | | | | | |
|---|---|---|---|---|---|
| **CALIFICACION IMPACTO** | **1. MUY BAJO** | **2. BAJO** | **3. MODERADO** | **4. ALTO** | **5. MUY ALTO** |
| **Riesgos estratégicos** | Problemas menores con los objetivos estratégicos. Existe posibilidad de ajustar el plan de trabajo o esquema táctico. | Restricciones para lograr los objetivos estratégicos. | Incumplimiento de algunos aspectos de los objetivos estratégicos. | Incumplimiento parcial de los objetivos estratégicos o incumplimiento de algunos de ellos | Incumplimiento total de los objetivos estratégicos |
| **Riesgos de Imagen** | Ante el personal que ejecuta la actividad | Ante el personal del área que lidera el proceso. | Ante otras áreas de la Entidad | Ante las entidades con las que interactúa la entidad.<br>Incumplimiento de requisitos legales. Medidas por entes de control. Multas a la Entidad. Prórrogas | Ante el nivel nacional e internacional. Incumplimiento de requisitos legales que genera sanciones legales. Proceso disciplinario |
| **Riesgos de Corrupción** | No Aplica | No Aplica | Pérdidas o perjuicios en un área o dependencia de la entidad | Pérdidas o perjuicios que afectan a la entidad | Perjuicios a personas fuera de la entidad, detrimento patrimonial o deterioro significativo de la imagen de la entidad |
| **Riesgos operativos** | Sin consecuencia en procesos ni actividades | Incumplimiento de actividades que no generan reproceso. Existe posibilidad de reprogramar la actividad o ajustar el plan de trabajo. | Impacto en cumplimiento de actividades o en salidas de proceso, que pueden generar reprocesos | Impacto en el cumplimiento de procesos, productos IIB en indicadores de proceso, en planes de acción. | Impacto en cumplimiento de objetivos y metas institucionales |
| **Riesgos de Tecnología** | Interrupción de labores < medio día | Interrupción de actividades entre 5 horas y 1 día | Interrupción de actividades de más de un1 día a 1 semana | Interrupción de actividades entre 1-2 semanas | Interrupción de labores mayor a 2 semanas |
| **Riesgo Ambiental** | Cambios leves y reversibles en el entorno | Cambios leves pero irreversibles en el entorno | Cambios moderados en el entorno de carácter reversible | Cambios moderados en el entorno, pero irreversibles | Cambios considerables en el entorno |
| **Riesgo de Seguridad y Salud en el Trabajo** | Lesiones o enfermedades que no requieren incapacidad. | Lesiones o enfermedades con incapacidad menor a una semana. | Lesiones o enfermedades con incapacidad entre una semana y 29 días | Lesiones o enfermedades con incapacidad entre 30 días y 6 meses | Lesiones o enfermedades graves o irreparables (con incapacidad permanente o invalidez) |

| Tabla de valoración de impacto de riesgo | | | | | |
|---|---|---|---|---|---|
| **CALIFICACION IMPACTO** | **1. MUY BAJO** | **2. BAJO** | **3. MODERADO** | **4. ALTO** | **5. MUY ALTO** |
| | Daños puntuales o menores en instalaciones, reparables sin necesidad de suspensión de actividades | Daño parcial de instalaciones de una dependencia, reparables con afectación de actividades máx. 1 día | Daño parcial de instalaciones de algunas dependencias, reparables con afectación de actividades máx. 1 semana | Daños importantes en instalaciones afectando varias dependencias, cuya reparación comprometerá su uso máx.1 semana | Afectación total de instalaciones, de difícil reparación, que impedirán su uso por más de 15 días |
| **Seguridad de la información Integridad** | La pérdida de exactitud y completitud afecta a la persona que ejecuta el proceso y conlleva un impacto no significativo para la entidad o entes externos | La pérdida de exactitud y completitud afecta al personal interno del proceso y conlleva un impacto no significativo para la entidad o entes externos | La pérdida de exactitud y completitud afecta otras áreas, procesos o personas en la Entidad y puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen a funcionarios de la entidad | La pérdida de exactitud y completitud afecta una entidad con las que interactúa IIB y puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad | La pérdida de exactitud y completitud afecta dos o más entidades con las que interactúa en IIB y puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad |
| **Seguridad de la información Disponibilidad** | Afecta sólo a la persona que ejecuta el proceso. | Afecta al personal del área que lidera el proceso | Afecta otras áreas, procesos o personas en la Entidad | Afecta una entidad con las que interactúa IIB | Afecta dos o más entidades con las que interactúa IIB |
| | Afecta la disponibilidad 1 hora en el día laboral | Afecta la disponibilidad de la información en el horario laboral entre semana (5x8). | Afecta la disponibilidad de la información en el horario laboral entre semana, e incluyendo los sábados (6x10) | Afecta la disponibilidad de la información en el horario todos los días menos las primeras horas del día no laborales (7x20) | Afecta la disponibilidad de la información en tiempo completo, todos los días y todas las horas (7x24) |
| **Seguridad de la información Confidencialidad** | Afecta la información de pública de uso interno de la persona que ejecuta el proceso. | Afecta la información pública del área que lidera el proceso. | Afecta la información pública de otras áreas, procesos o personas en la Entidad | Afecta la información reservada y clasificada del área, procesos o personas en la Entidad | Afecta la información reservada y clasificada de las entidades con las que interactúa IIB |

## 13. 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.<br>• La metodología relacionada con los riesgos de la seguridad de la información<br>• Se ajustó la definición de términos relacionado con el riesgo de la planeación estratégica |
| Enero 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. |

## 14.APROBACIÓN

| Aprobación | Nombre | Cargo | Fecha de aprobación |
|---|---|---|---|
| Elaboró | Diana Paola Suárez | Asesor Calidad | Enero 27 de 2022 |
| Revisó y aprobó | María Ximena Obando | Gerente Administrativa y financiera | |

**(ORIGINAL FIRMADO)**