POLITICAS DE ADMINISTRACIÓN DEL RIESGO DE METROLINEA S.A

Tabla de Contenido

1. INTRODUCCIÓN

La estructuración del presente documento para METROLINEA S.A. está basada en la guía para la administración del riesgo vigente y el diseño de controles en entidades públicas y se establece para asegurar el cumplimiento de la misión institucional y los objetivos estratégicos y de proceso.
La política está compuesta por el objetivo, alcance, niveles de aceptación al riesgo, niveles para calificar el impacto, el tratamiento de riesgos, el seguimiento periódico según nivel de riesgo residual y responsabilidad de gestión para cada línea de defensa.

METROLINEA S.A., establece su política de administración del riesgo tomando como referente los lineamientos establecidos por el Modelo Integrado de Planeación y Gestión – MIPG, el Modelo Estándar de Control Interno en lo pertinente al modelo de las líneas de defensa, los referentes de la Guía para la administración del riesgo y el diseño de controles en entidades públicas emitida por el Departamento Administrativo de la Función Pública y demás lineamientos expedidos por los entes rectores en el tema.

Su compromiso está direccionado al cumplimiento del marco legal, la satisfacción de los usuarios, los objetivos de los procesos, asegurar los activos de la información, el manejo transparente de los recursos público y garantizar un ambiente de trabajo seguro y saludable; a través de la identificación, valoración y seguimiento de todos los riesgos para que la Entidad evalúe e intervenga aquellos eventos, tanto internos como externos, que puedan afectar de manera positiva o negativa el logro de objetivos Institucionales.

2. MARCO NORMATIVO

- Ley 1712 de 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".

- Ley 1474 de 2011 "Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública".

- Ley 87 de 1993 "Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones".

- Decreto 1499 de 2017. "Por medio del cual se modifica el Decreto 1083 de 2015, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015"

- Decreto 1081 de 2015 "Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República".

- Decreto 124 del 26 de enero de 2016 "Por el cual se sustituye el Título IV de la Parte 1 del Libro 2 del Decreto 1081 de 2015, relativo al "Plan Anticorrupción y de Atención al Ciudadano".

- Decreto 648 de 2017 "Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública".

3. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS

La política de administración de riesgos de Metrolínea, tiene un carácter estratégico y está fundamentada en *el modelo integrado de planeación y gestión*, la *guía de administración del riesgo* y el diseño de controles en entidades públicas, con un enfoque preventivo de evaluación permanente de la gestión y el control, el mejoramiento continuo y con la participación de todos los servidores de la entidad.

Aplica para todos los niveles, áreas y procesos de Metrolínea e involucra el contexto, la identificación, valoración, tratamiento, monitoreo, revisión, comunicación, consulta y el análisis de los siguientes riesgos:

- Los riesgos de gestión de proceso que pueda afectar el cumplimiento de la misión y objetivos institucionales.
- Los riesgos de posibles actos de corrupción a través de la prevención de la ocurrencia de eventos en los que se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- Los riesgos de seguridad digital que puedan afectar la confidencialidad, integridad y disponibilidad de la información de los procesos de la entidad.
- Los riesgos de continuidad de negocio que impiden la prestación normal de los servicios institucionales debido a eventos calificados como crisis.

El periodo de revisión e identificación de los riesgos institucionales se debe realizar cada vigencia, atendiendo la metodología vigente, una vez se defina el plan de acción anual, asegurando la articulación de éstos con los compromisos de cada proceso.

La Gerencia, se compromete a gestionar los riesgos identificados de gestión, corrupción, seguridad de la información y seguridad y salud en el trabajo, mediante la aplicación de controles y acciones que permitan el desarrollo de una gestión pública efectiva y el cumplimiento de los objetivos estratégicos, respondiendo a las necesidades y expectativas de sus partes interesadas.

4. OBJETIVOS DE LA ADMINISTRACIÓN DE RIESGOS

Alcanzar un nivel aceptable de riesgos residuales en todos los procesos, a través de la gestión de acciones de control, con el fin de asegurar el cumplimiento de la misión institucional, los compromisos, los objetivos estratégicos y de procesos vigentes.

Como objetivos específicos se presentan los siguientes:

- Definir los roles y responsabilidades frente a la gestión de los riesgos en la Entidad.
- Comunicar la política de administración de riesgos en todos los niveles de la Entidad.
- Brindar una herramienta metodológica para la gestión de los diferentes tipos de riesgos en todos los procesos de la Entidad.
- Generar mecanismos y medidas para disminuir la materialización de los riesgos de corrupción en Metrolínea.
- Generar mecanismos para mitigar las amenazas y tratar las vulnerabilidades que enfrentan los activos de información y tecnológicos, con el fin de asegurar la confidencialidad, integridad y disponibilidad de la información de la Entidad.
- Identificar peligros y valorar los riesgos para intervenirlos y propiciar un ambiente de trabajo seguro y saludable.

5. ALCANCE

Aplica a todos los procesos, proyectos, servicios y planes de la entidad, conforme a cada tipo y clasificación de riesgo, bajo la responsabilidad de los líderes de proceso y líneas de defensa en el marco de la implementación del Modelo Integrado de Planeación y Gestión.

6. TÉRMINOS Y DEFINICIONES

Activo de Información: En el contexto de seguridad digital, son activos elementos tales como: Aplicaciones de la organización, Servicios web, Redes, Información física o digital, Tecnologías de información TI, Tecnologías de operación TO que utiliza la organización para funcionar, en el entorno digital.

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

Apetito al Riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Gerencia.

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

Comité Institucional de Coordinación de Control Interno (CICCI): Es un órgano de asesoría y decisión en los asuntos de control interno de Metrolínea. En su rol de responsable y facilitador, hace parte de las instancias de articulación para el funcionamiento del Sistema de Control Interno.

Comité Institucional de Gestión y Desempeño (CIGD): Es la instancia encargada de orientar, articular y ejecutar las acciones y estrategias para la correcta implementación, operación, desarrollo, evaluación y seguimiento del Modelo Integrado de Planeación y **Gestión** – MIPG, en Metrolínea S.A.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

Consecuencias: Son los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

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

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

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

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

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

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

Controles Preventivos: Medida que permite eliminar las causas del riesgo, para prevenir su ocurrencia o materialización.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una Entidad.

Evaluación del Riesgo: Proceso para determinar el nivel de riesgo asociado al nivel de probabilidad de que dicho riesgo se concrete y al nivel de severidad de las consecuencias de esa concreción.

Fraude Externo: Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).

Fraude Interno: Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.

Gestión del Riesgo: Actividades coordinadas para dirigir y controlar una Entidad con respecto al riesgo y proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Impacto: Consecuencias que puede ocasionar a la Entidad la materialización del riesgo.

Integridad: Propiedad de exactitud y completitud.

Mapa de Riesgos: Herramienta metodológica que permite hacer un inventario de los riesgos ordenada y sistemáticamente, haciendo la descripción de cada uno de estos y las posibles consecuencias y sus acciones preventivas o correctivas.

Mapa de Riesgos Institucional: Contiene los riesgos de mayor criticidad (zona residual extrema y alta) frente al logro de los objetivos institucionales e integra los riesgos de Gestión, Corrupción y Seguridad de la Información

Plan Anticorrupción y de Atención al Ciudadano: contempla la estrategia para la lucha contra la corrupción que debe ser implementado por todas las entidades del orden nacional, departamental y municipal.

Probabilidad: Se entiende por la posibilidad de ocurrencia del riesgo, que se debe medir a través de la relación entre los hechos ocurridos realmente y la cantidad de eventos que pudieron ocurrir.

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos

potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos

Riesgo de Corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgo de Gestión: Es la posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos; los cuales pueden ser:

- **Riesgos Estratégicos**: Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la Entidad.
- **Riesgos Gerenciales**: Posibilidad de ocurrencia de eventos que afecten los Procesos gerenciales y/o la alta dirección.

- **Riesgos Operativos**: Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la Entidad.
- **Riesgos Financieros**: Posibilidad de ocurrencia de eventos que afecten los Estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.
- **Riesgos Tecnológicos**: Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una Entidad.
- **Riesgos de Cumplimiento**: Posibilidad de ocurrencia de eventos que afecten la situación jurídica y contractual de la Entidad, debido a su incumplimiento o desacato a la normatividad legal o las obligaciones contractuales.
- **Riesgo de Imagen o de Reputación**: Posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus usuarios, partes interesadas y comunidad en general
- **Riesgo Inherente:** El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
- **Riesgo Materializado:** Son aquellos incidentes que generan o podrían generar pérdidas a la entidad.
- **Riesgo Residual:** Es el resultado de aplicar la efectividad de los controles al riesgo inherente.
- **Riesgo de Seguridad de la Información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- **Riesgo de Seguridad y Salud en el Trabajo:** Combinación de la probabilidad de que ocurran eventos o exposiciones peligrosos relacionados con el trabajo y la severidad de la lesión y deterioro de la salud que pueden causar los eventos o exposiciones.
- **Seguridad Informática:** se refiere a la protección del sistema informático, tratando de asegurar la integridad y la privacidad de la información que contiene.
- **Servicio Tercerizado**: corresponde a los servicios y productos suministrados externamente, teniendo en cuenta: a) los servicios y productos suministrados por un tercero que están destinados a incorporarse dentro de los propios servicios y productos de la entidad; b) los servicios y productos proporcionados directamente a las partes interesadas en nombre de la entidad; c) un proceso o parte del proceso proporcionado por un tercero como un resultado de una decisión de la entidad.

- **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. Para el riesgo de corrupción la tolerancia es inaceptable.
- **Vulnerabilidad:** Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

7. RESPONSABILIDADES

Con la entrada en vigencia del Modelo Integrado de Planeación y Gestión - MIPG, que integra los sistemas de gestión de la calidad y de desarrollo administrativo; se crea un único sistema de gestión articulado con el sistema de control interno, el cual se actualiza y alinea con el modelo de las tres líneas de defensa. Este modelo de líneas de defensa, proporciona una manera simple y efectiva para mejorar las comunicaciones en la gestión de riesgos y control mediante la aclaración de las funciones y deberes esenciales relacionados.

A continuación, se describen las responsabilidades frente a la gestión de los riesgos por línea estratégica y líneas de defensa:

Línea Estratégica

Responsables: Está a cargo de la Alta Gerencia y el Comité Institucional de Coordinación de Control Interno*;* dentro de esta línea en la Entidad se encuentra:

- Alta dirección: conformado por la gerente y directores de área.
- El Comité Institucional de Coordinación de Control Interno, órgano de asesoría y decisión en los asuntos de control interno de Metrolínea. En su rol de responsable y facilitador, hace parte de las instancias de articulación para el funcionamiento armónico del Sistema de Control Interno; responsable de someter a aprobación de la Gerente de Metrolínea la política de administración del riesgo y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta.

Responsabilidad frente al riesgo:

- Definir el marco general para la gestión del riesgo y el control y supervisar su cumplimiento.
- Establecer y aprobar la política de administración del riesgo, incluyendo los niveles de responsabilidad y autoridad.
- Definir y hacer seguimiento a los niveles de aceptación del riesgo.
- Analizar los cambios en el entorno que puedan tener un impacto significativo en la operación de la Entidad y que puedan generar cambios en la estructura de riesgos y controles.
- Realizar seguimiento y análisis periódico a los riesgos institucionales.

- Evaluar el estado del sistema de control interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento del mismo.

Primera línea de defensa

Responsables: Está conformada por los directores de área y líderes de los procesos, programas y proyectos y servidores en general de Metrolínea S.A.

Responsabilidad frente al riesgo:

- Desarrollar e implementar procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.
- Identificar y valorar los riesgos que pueden afectar los programas, proyectos, planes y procesos a su cargo y actualizarlo cuando se requiera.
- Actualizar los riesgos de corrupción y/o reporte de la materialización de los riesgos cuando se genere una alerta sobre presuntos hechos de corrupción.
- Actualizar los riesgos y/o controles asociados cuando la Oficina de Control Interno genere una alerta sobre la materialización de los riesgos.
- Definir, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados alineado con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo en su proceso.
- Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar.
- Implementar el procedimiento transversal de activos de información para identificación de los riesgos de seguridad de la información.

Segunda línea de defensa

Responsables: Dirección de Planeación, Jefes de Área, CIGD, TICs, SGSST, Calidad Gestión del Riesgo, Contabilidad, Tesorería, Presupuesto, Talento Humano y Atención al Ciudadano.

Responsabilidad frente al riesgo:

Por parte de la Dirección de Planeación:

- Elaborar e impartir lineamientos en materia de los Sistemas de Gestión y Control Integrados, y verificar su cumplimiento.

- Elaborar e impartir lineamientos sobre la metodología de administración de riesgos de gestión y corrupción

- Diseñar instrumentos para el mejoramiento continuo de los Sistemas de Gestión y Control Integrados.

- Asesorar a la línea estratégica en el análisis del contexto, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo.
- Consolidar el Mapa de riesgos institucional (riesgos de mayor criticidad frente al logro de los objetivos) y presentarlo para análisis y seguimiento ante el Comité Institucional de Coordinación de Control Interno.
- Presentar al Comité Institucional de Coordinación de Control Interno el seguimiento a la eficacia de los controles en las áreas identificadas en los diferentes niveles de operación de la entidad.
- Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis y valoración del riesgo.
- Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos.
- Supervisar en coordinación con los demás responsables de esta segunda línea de defensa que la primera línea identifique, evalúe y gestione los riesgos y controles para que se generen acciones.
- Evaluar que los riesgos sean consistentes con la presente política de la entidad y que sean monitoreados por la primera línea de defensa.
- Identificar cambios en el apetito del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlo para aprobación del Comité Institucional de Coordinación de Control Interno.

Por parte de los profesionales del SGSST:

- Administrar los riesgos relacionados con el Sistema de Gestión de Seguridad y Salud en el Trabajo en Metrolínea S.A. y actuar como representante del empleador en los comités relacionados.
- Realizar la identificación de peligros y evaluación y valoración de los riesgos para intervenirlos de acuerdo a su priorización.
- Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos.
- Realizar seguimiento al Plan de Trabajo del Sistema de Seguridad y Salud en el trabajo.

Por parte de Gestión Documental:

- Elaborar e impartir lineamientos respecto al manejo del inventario y registro de activos de información.

- Elaborar e impartir lineamientos para la conservación, preservación y el uso adecuado del patrimonio documental del Municipio de Santiago de Cali, y verificar su cumplimiento.
- Promover y verificar el cumplimiento de las normas en materia de Transparencia y Acceso a la Información.
- Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis y valoración de riesgos de seguridad de la información.
- Revisar y dar copia de su visto bueno a la Subdirección de Gestión Organizacional en caso de presentarse solicitudes de actualización del mapa de riesgos respecto a riesgos de seguridad de la información.

Por parte del P.U. de las Tics:

- Impartir lineamientos en materia de tecnología digital para el intercambio, pertinencia, calidad, oportunidad y seguridad de la información.
- Gestionar la seguridad informática en cada uno de los componentes de tecnología para garantizar la integridad, disponibilidad y confidencialidad de la información.
- Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis y valoración de riesgos de seguridad informática en lo que respecta a los activos secundarios.

Por parte de líderes de procesos transversales:

- Monitorear los riesgos identificados y controles establecidos por la primera línea de defensa acorde con la estructura de los temas a su cargo.
- Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, y valoración del riesgo y definición de controles en los temas a su cargo y con enfoque en la prevención del daño antijurídico.
- Supervisar que la primera línea de defensa identifique, evalúe y gestione los riesgos en los temas de su competencia.

Tercera línea de defensa:

Responsables: Oficina de Control Interno.

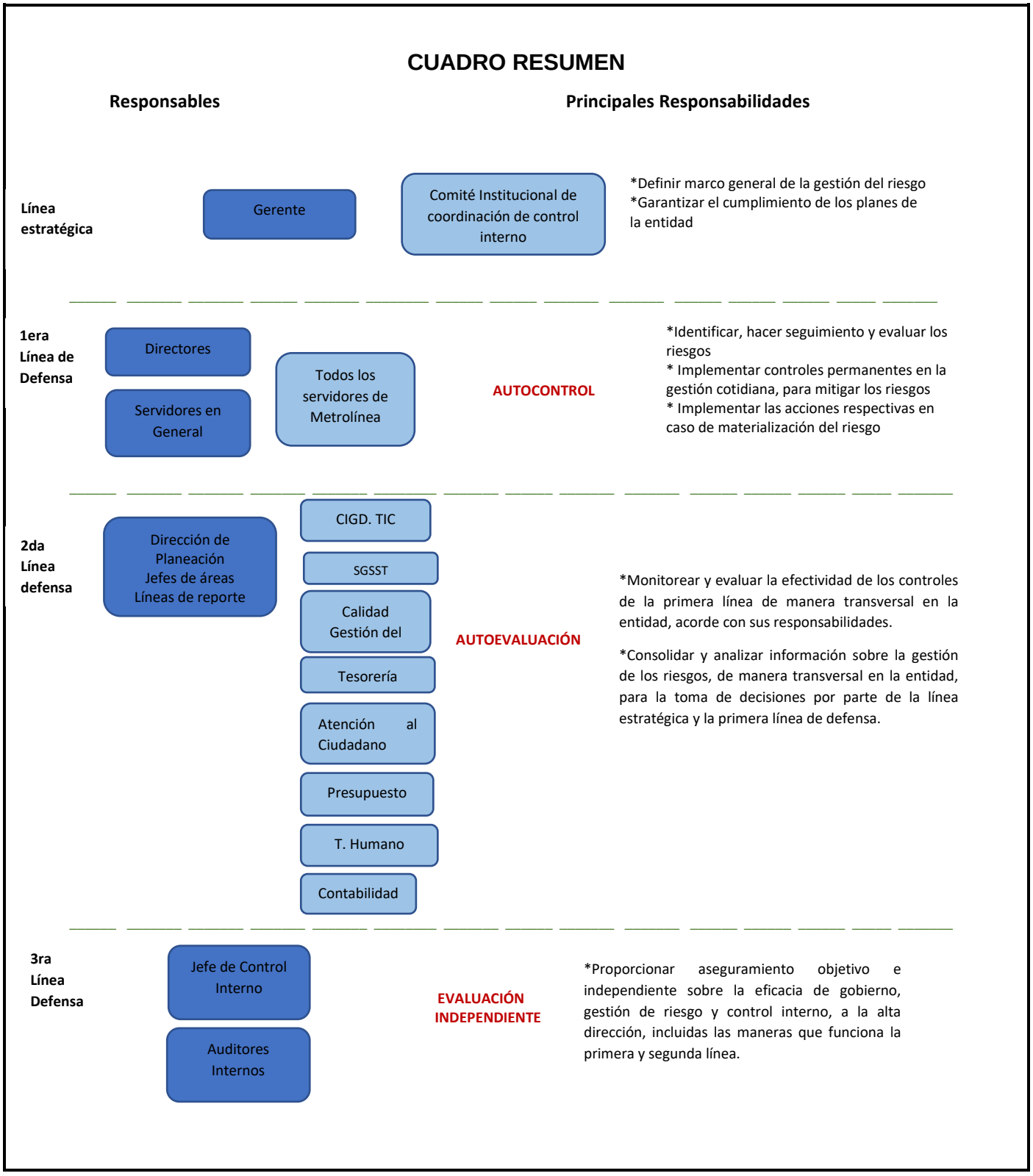
Responsabilidad frente al riesgo:

- Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos.

- Analizar el comportamiento de los riesgos consolidados en el mapa de riesgos de conformidad con el Programa Anual de Auditoría Interna y reportar los resultados al Comité Institucional de Coordinación de Control Interno.
- Recomendar mejoras a la política de administración del riesgo.
- Generar a través de su rol de asesoría una orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Dirección de Planeación.
- Evaluar el análisis al monitoreo de la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo.
- Brindar un nivel de asesoría proactiva y estratégica, frente a la segunda y primera línea de defensa.
- Informar los hallazgos y proporcionar recomendaciones de forma independiente.
- Generar un reporte cuatrimestral al Comité Institucional de Coordinación de Control Interno acerca del cumplimiento de las metas y los objetivos en relación a la gestión integral del riesgo, que puede ser en el informe cuatrimestral de control interno sobre el seguimiento al Plan Anticorrupción y de Atención al Ciudadano y al Mapa de riesgos.

Seguidamente, se presenta un cuadro resumen de las diferentes líneas de defensa, en cada una de sus responsabilidades de AUTOCONTROL, AUTOEVALUACION Y EVALUACION INDEPENDIENTE

CUADRO RESUMEN



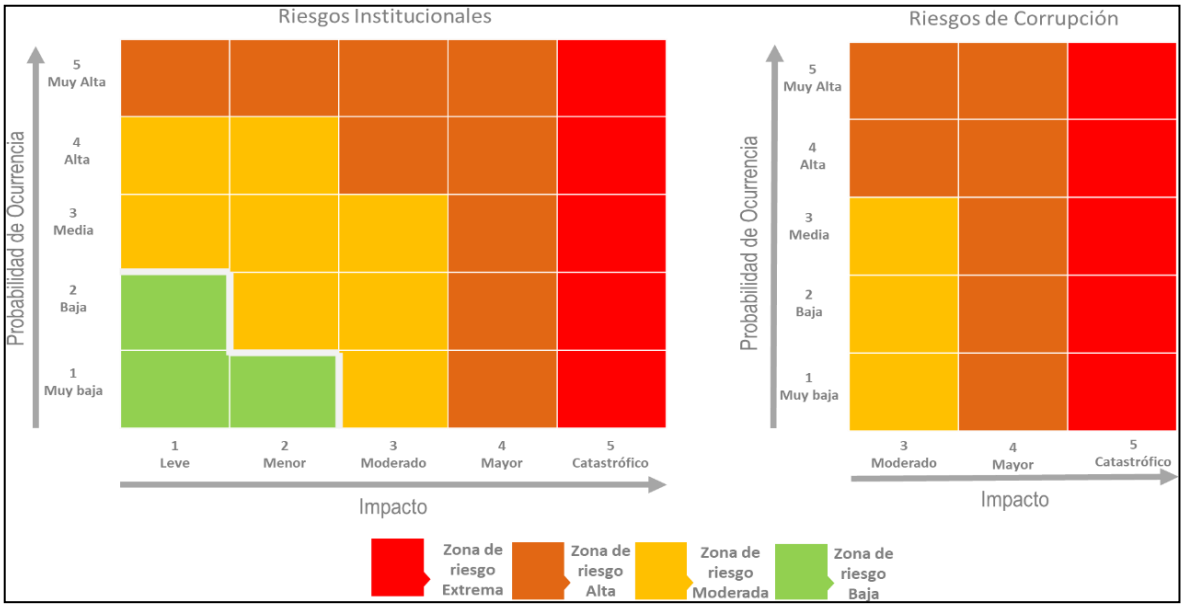
8. LINEAMIENTOS GENERALES PARA LA ADMINISTRACIÓN DE RIESGOS

a. Nivel de aceptación o tolerancia al riesgo

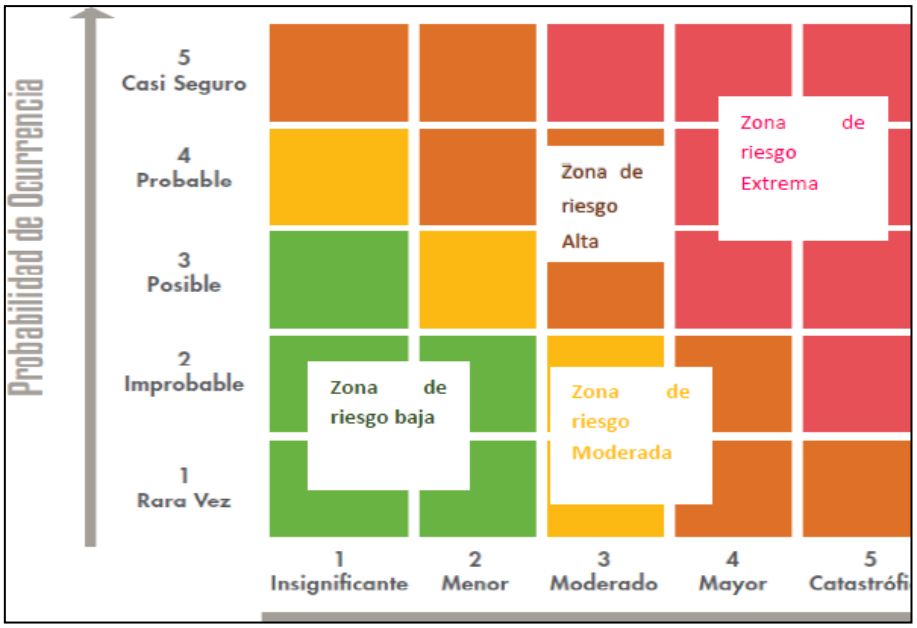
Para los riesgos de corrupción, la Entidad no es flexible en la aceptación de conductas o hechos de corrupción, por lo tanto, **no hay aceptación del riesgo**, siempre deben conducir a formular acciones de fortalecimiento.
En los demás riesgos, acorde con los riesgos residuales aprobados por los líderes de procesos y socializados en el correspondiente Comité Institucional, Metrolínea S.A., aceptará el riesgo residual que se encuentran en zona baja y moderada. Si llegase a quedar en un nivel superior, debe justificarse por qué la dificultad de mitigar este riesgo. Igualmente, se debe realizar un seguimiento cuatrimestral a la estrategia de tratamiento a los riesgos residuales aceptados.

b. Niveles para calificar el impacto del riesgo

Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor tal como se visualiza en el siguiente cuadro.



Niveles para calificar el impacto del riesgo (riesgo de gestión)



Niveles para calificar el impacto del riesgo (riesgo de corrupción)

Probabilidad	Nivel	Zonas de Riesgo de Corrupción		
Casi seguro	5	Moderada	Alta	Extrema
Probable	4	Moderada	Alta	Extrema
Posible	3	Moderada	Alta	Extrema
Improbable	2	Baja	Moderada	Alta
Rara vez	1	Baja	Baja	Moderada
Impacto		3	4	5

Criterios para calificarel impacto - Riesgos de Gestión

NIVEL	IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
CATASTRÓFICO	- Impacto que afecte la ejecución presupuestal en un valor ≥50%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de información crítica para la entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
MAYOR	- Impacto que afecte la ejecución presupuestal en un valor ≥20%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad.	- Interrupción de las operaciones de la entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.

NIVEL	VALOR DEL IMPACTO	CRITERIOS DE IMPACTO PARA RIESGOS DE SEGURIDAD DIGITAL	
		IMPACTO (CONSECUENCIAS) CUANTITATIVO	IMPACTO (CONSECUENCIAS) CUALITATIVO
INSIGNIFICANTE	1	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. No hay afectación medioambiental.	Sin afectación de la integridad. Sin afectación de la disponibilidad. Sin afectación de la confidencialidad.
MENOR	2	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de ≥X días de recuperación.	Afectación leve de la integridad. Afectación leve de la disponibilidad. Afectación leve de la confidencialidad.
MODERADO	3	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación leve del medio ambiente requiere de ≥X semanas de recuperación.	Afectación moderada de la integridad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación moderada de la confidencialidad de la información debido al interés particular de los empleados y terceros.
MAYOR	4	Afectación ≥X% de la población. Afectación ≥X% del presupuesto anual de la entidad. Afectación importante del medio ambiente que requiere de ≥X meses de recuperación.	Afectación grave de la integridad de la información debido al interés particular de los empleados y terceros. Afectación grave de la disponibilidad de la información debido al interés particular de los empleados y terceros. Afectación grave de la confidencialidad de la información debido al interés particular de los empleados y terceros.

Criterios para calificar el impacto - Riesgos de gestión

Criterios para calificar el impacto -Riesgos de corrupción

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

Nivel de impacto MAYOR

c. Análisis del contexto interno y externo de Metrolínea S.A.

En esta etapa se debe identificar:

CONTEXTO EXTERNO	POLÍTICOS: Cambios de gobierno, legislación, políticas públicas, regulación
	ECONÓMICOS Y FINANCIEROS: Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia, transporte informal
	SOCIALES Y CULTURALES: Demografía, responsabilidad social, orden público.
	TECNOLÓGICOS: Avances en tecnología, acceso a sistemas de información externos, gobierno en línea
	AMBIENTALES: emisiones y residuos, energía, catástrofes naturales desarrollo sostenible
	LEGALES Y REGLAMENTARIOS: Normatividad externa (leyes, decretos, ordenanzas y acuerdos)
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
	PROCESOS LEGALES: Demandas contra Metrolínea S.A.
	COMUNICACIÓN INTERNA: canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones
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, usuario 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
	ACTIVIDADES DE SEGURIDAD DIGITAL DEL PROCESO: información, aplicaciones, hardware entre otros que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano.

Fuente: Guía del DAFP (2018, pág. 20).

d. Identificación del riesgo

La identificación del riesgo se realiza determinando las causas y consecuencias potenciales, con base en los factores para los tipos de contexto interno, externo y/o proceso analizados para Metrolínea y que pueden afectar el logro de los objetivos.

La identificación del riesgo no se puede realizar de manera fragmentada, debe existir una relación total entre las causas identificadas, el riesgo y las consecuencias que podrían presentarse producto de la materialización, para evitar confusiones y definir articuladamente todos los componentes de la identificación del riesgo se deberá realizarse las siguientes preguntas:

- ¿QUE PUEDE SUCEDER?
- ¿COMO PUEDE SUCEDER?
- ¿CUÁNDO PUEDE SUCEDER?
- ¿QUE CONSECUENCIAS TENDRÍA SU MATERIALIZACIÓN?

Una vez identificado el riesgo (determinación del riesgo con las causas y consecuencias asociadas), se debe definir la incidencia de este frente a la prestación de servicios para el usuario externo, es decir el cumplimiento de la razón de ser Metrolínea S.A.

Posterior a realizar el análisis de la posible incidencia del riesgo frente al usuario externo, se debe responder la siguiente pregunta con "SI o NO", según corresponda:

¿El impacto generado por la materialización del riesgo, tiene incidencia directa en los servicios prestados al usuario externo, es decir tiene incidencia en el cumplimiento de la razón de ser de la entidad?

El anterior ejercicio se realiza con el fin de clasificar como riesgos institucionales aquellos que, en el caso de materializarse, tengan una incidencia en el usuario externo.

e. Análisis del riesgo

La etapa de análisis busca establecer la probabilidad de ocurrencia del riesgo y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información cuantitativa y cualitativa para establecer el nivel de riesgo y las acciones que se van a implementar. Este análisis del riesgo depende de la información obtenida en la fase de identificación de riesgos.

Determinar la Probabilidad

Se han establecido dos aspectos a tener en cuenta en el análisis de los riesgos identificados: La Probabilidad y el Impacto. Por la primera se entiende la posibilidad de ocurrencia del riesgo, esta puede ser medida a partir de la determinación de la frecuencia de ocurrencia del riesgo (si se ha materializado). Por Impacto, se entiende las consecuencias que puede ocasionar a la entidad la materialización del riesgo.

Para adelantar el análisis del riesgo se deben considerar la calificación del riesgo que se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo, para esto se debe tener en cuenta las siguientes tablas:

Criterios para definir el nivel de probabilidad

	Frecuencia de La Actividad	**Probabilidad**
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces al año.	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces al año.	40%
Media	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces al año.	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 501 veces al año y máximo 5000 veces al año.	80%
Muy alta	La actividad que conlleva el riesgo se ejecuta más de 5001 veces al año.	100%

Fuente: Adaptado de DAFP, 2020. Guía para la Administración del Riesgo y diseño de controles en entidades públicas.

Análisis de la probabilidad (Riesgo de corrupción)

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

Criterios para calificar la probabilidad (Riesgos de corrupción)

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

Fuente: DAFP, 2020. Guía para la Administración del Riesgo y diseño de controles en entidades públicas V05.

Tabla de impacto

NIVEL	DESCRIPTOR	DESCRIPCION
1	**Insignificante**	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad
2	**Menor**	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad
3	**Moderado**	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad
4	**Mayor**	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad
5	**Casi seguro**	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad

Para determinar el impacto se puede además de la anterior, usar las siguientes tablas que representan los temas en que suelen impactar la ocurrencia de riesgo.

Impacto Operativo

NIVEL	DESCRIPCIÓN
1	Ajustes a una actividad concreta
2	Cambios en los procedimientos
3	Cambios en la interacción de los procesos
4	Intermitencia en el servicio
5	Para total del proceso

Impacto Legal

NIVEL	DESCRIPCIÓN
1	Multas
2	Demandas
3	Investigaciones Disciplinarias
4	Investigación Fiscal
5	Intervención – Sanción

Determinar la probabilidad riesgos de seguridad digital

Para esta etapa se asociarán las tablas de probabilidad e impacto definidas para los riesgos de gestión.

f. Evaluación del riesgo

Esta fase permite comparar los resultados de la calificación, con los criterios definidos para establecer el grado de exposición al riesgo, de esta forma, se define la zona de ubicación del riesgo. Para ello, basta cruzar el resultado obtenido en la probabilidad y el impacto y ubicarlo en la zona correspondiente. Se utilizará una sola matriz para efectuar la calificación de los diferentes tipos de riesgo, buscando la simplificación de la metodología, pero sin perder en ningún momento lo estricto de la evaluación en cada caso.

g. Gestión del riesgo- Controles para el tratamiento del riesgo

El resultado del desplazamiento dentro de la matriz, determinará finalmente la selección de las opciones de tratamiento del riesgo, así:

Evitar el riesgo, tomar las medidas encaminadas a prevenir su materialización.

Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se genera cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. Por ejemplo: el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.

Reducir el riesgo, implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Por ejemplo: a través de la optimización de los procedimientos y la implementación de controles.

Compartir o transferir el riesgo, reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar, la tercerización.

Asumir un riesgo, luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso, el gerente del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

En caso de materialización del riesgo, se deben identificar para todos los riesgos, independiente de su evaluación residual o de los controles existentes, acciones enfocadas en las correcciones que se deben desarrollar de acuerdo con las consecuencias identificadas, analizando la causa raíz de lo sucedido, en donde se deberá definir el plan de acción a seguir.

h. Seguimiento del riesgo

Esta etapa dinamiza la gestión integral del riesgo, cada cuatro meses con cortes a abril, agosto y diciembre, los procesos deben realizar seguimiento al estado de sus riesgos garantizando que se analizaron entre otros los siguientes aspectos:

- Documentación – Modificaciones al proceso
- Estado de los controles - Aplicación y efectividad. Análisis detallado con evidencias de aplicación.
- Estado del riesgo – Vigencia
- Acciones de tratamiento
- Materialización del riesgo
- Revisión de informes externos y de entes de control

i. Mapa de riesgos.

El mapa se construye con aquellos riesgos que afectan de manera directa el cumplimiento de los objetivos o la misión institucional. Los riesgos institucionales, son producto del análisis de los riesgos por proceso y son denominados de este tipo cuando cumplen alguna de las siguientes características:

- Son clasificados como riesgos estratégicos
- Los riesgos que después de la evaluación residual se ubican en zona alta o extrema.
- Los riesgos que tengan incidencia en usuario o destinatario final externo.

El Mapa de Riesgos será la herramienta organizacional que facilite a los colaboradores de Metrolínea S.A. la visualización y entendimiento de los riesgos y la definición de una estrategia para su adecuada administración, de igual manera en el mapa de riesgos se establecerán los controles, evaluación de estos e indicadores de eficacia de las actividades de control y efectividad del plan de manejo establecido en cada riesgo.

j. Implementación de la política de administración del riesgo.

- Corresponde al Comité Institucional de Coordinación de Control Interno establecer y aprobar la Política y Metodología de Gestión de Riesgos y asegurarse de su permeabilización en todos los niveles de la organización, de tal forma que se conozcan claramente los niveles de responsabilidad y autoridad que posee cada una de las tres líneas de defensa frente a la gestión del riesgo.
- Corresponde a los jefes de área y/o grupo asegurarse de implementar esta metodología para mitigar los riesgos en la operación.
- Corresponde al área encargada de la gestión del riesgo, en este caso planeación interna, la difusión y asesoría de la presente metodología, así como de los planes de tratamiento de riesgo identificados en todos los niveles de Metrolínea S.A., de tal forma que se asegure su implementación.
- El levantamiento de la información sobre los riesgos se hará con un equipo de personas conocedoras del quehacer de cada proceso y la consolidación de la información será producto del consenso. Además, cada mapa será revisado y aprobado por los directores o Jefes de Área previo a la entrega a Planeación para su consolidación.
- Le corresponde a la Jefatura de Control Interno de Gestión, realizar evaluación independiente sobre la gestión del riesgo en Metrolínea S.A., catalogándola como una unidad auditable más dentro de su universo de auditoría.

CUADRO DE APROBACIÓN			
	CARGOS	**NOMBRE**	**FECHA**
ELABORADO POR:	P.E. Planes, Programas y Proyectos	Sandra Milena Gelves Ayala	23/08/2022
	Jefe de Oficina de Control Interno	David Rivera Ardila	23/08/2022
REVISADO POR:	Director de Planeación	Claudia Patricia García Burgos	23/08/2022
APROBADO POR:	Comité Institucional de Coordinación de Control Interno	Acta No. 2 del día 23 de agosto de 2022	23/08/2022

CONTROL DE CAMBIOS

VERSIÓN	FECHA DE REVISIÓN	SOLICITUD NO.	DESCRIPCIÓN DEL CAMBIO
00	25/08/2022	219	Emisión inicial. La estructuración del presente documento para Metrolínea S.A. esta basada en la guía para la administración del riesgo vigente y el diseño de controles en entidades publicas y se establece para asegurar el cumplimiento de la misión institucional y los objetivos estratégicos y de proceso. Solicitud realizada por: Sandra Milena Gelves Ayala-P.E. Planes, Programas y Proyectos