INVIAS
INSTITUTO NACIONAL DE VIAS

Política Institucional de Administración del Riesgo

INVIAS

"EL PEOR RIESGO ES CREER QUE TODO ESTA BAJO CONTROL"

PROPUESTA DE ACTUALIZACIÓN
MARZO DE 2021

OFICINA ASESORA DE PLANEACIÓN.

Grupo de Planeamiento Institucional.

Contenido

1 GLOSARIO

APETITO AL RIESGO: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección 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.

ÁREAS DE IMPACTO: consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional

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.

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 el riesgo.

CONSECUENCIA: 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.

CONTROL: Medida que permite reducir o mitigar un riesgo. Los responsables de implementar y monitorear los controles son los líderes de proceso.

ESTRATEGIA PARA COMBATIR EL RIESGO (tratamiento): Decisión que se toma frente a un determinado nivel de riesgo. Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos , se procede a partir del riesgo inherente y puede ser:

- **Reducir**: Después de realizar un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante transferencia o mitigación del mismo.
    - **Transferir:** Después de realizar un análisis, se considera que la mejor estrategia es tercerizar el proceso o trasladar el riesgo a través de seguros o pólizas. La responsabilidad económica recae sobre el tercero, pero no se transfiere la responsabilidad sobre el tema reputacional.
    - **Mitigar:** Después de realizar un análisis y considerar los niveles de riesgo se implementan controles que mitiguen el nivel de riesgo. Mo necesariamente es un control adicional.
- **Aceptar**: Después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo conociendo los efectos de su posible materialización.
- **Evitar**: Después de realizar un análisis y considerar que el nivel de riesgo es demasiado alto, se determina NO asumir la actividad que genera este riesgo.

EVENTO: Riesgo materializado. Los eventos de riesgo son aquellos incidentes que generan o podrían generar pérdidas a la entidad.

FACTORES DE RIESGO: Son las fuentes generadoras de riesgos. Pueden ser: Procesos, Talento Humano, Tecnología, Infraestructura y Eventos externos (Terceros).

INDICADORES CLAVE DE RIESGO (Un indicador de riesgos clave, también conocido como KRI de sus siglas en inglés Key Risk Indicators): Es una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados riesgos.

IMPACTO: Las consecuencias que puede ocasionar a la organización la materialización del riesgo.

GESTIÓN DEL RIESGO: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos. La gestión de riesgos no es estática, se integra en el desarrollo de la estrategia, la formulación de los objetivos de la entidad y la implementación de esos objetivos a través de la toma de decisiones cotidiana.

GESTIÓN DEL RIESGO DE DESASTRES: Es el proceso social de planeación, ejecución, seguimiento y evaluación de políticas y acciones permanentes para el conocimiento del riesgo y promoción de una mayor conciencia del mismo, impedir o evitar que se genere, reducirlo o controlarlo cuando ya existe para prepararse y manejar las situaciones de desastre, así como para la posterior recuperación, entiéndase: rehabilitación y reconstrucción. Estas acciones tienen el propósito explícito de contribuir a la seguridad, el bienestar y la calidad de vida de las personas y al desarrollo sostenible.

MAPA DE RIESGOS: Documento con la información resultante de la gestión del riesgo, administrado por la Oficina Asesora de Planeación.

MODELO DE TRES LÍNEAS DE DEFENSA (3LD): Realza el entendimiento del manejo de riesgos y controles mediante la asignación o clarificación de roles y responsabilidades a través de toda la organización.

- Línea Estratégica Este nivel analiza los riesgos y amenazas institucionales al cumplimiento de los planes estratégicos, tendrá la responsabilidad de definir el marco general para la gestión del riesgo (política de administración del riesgo) y garantiza el cumplimiento de los planes de la entidad.
- 1ª Línea de Defensa: La gestión operacional se encarga del mantenimiento efectivo de controles internos, ejecutar procedimientos de riesgo y el control sobre una base del día a día.
- La gestión operacional identifica, evalúa, controla y mitiga los riesgos.
- 2ª Línea de Defensa: Asegura que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente, supervisan la implementación de prácticas de gestión de riesgo eficaces.
- Consolidan y analizan información sobre temas clave para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos.
- 3ª Línea de Defensa: ejercida por la Oficina de Control interno.

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. En general la fórmula del Nivel del Riesgo es Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto**.**

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.

POLÍTICA DE ADMINISTRACIÓN DEL RIESGO: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo (NTC ISO31000 Numeral 2.4). La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos

POLÍTICA DE PREVENCIÓN DEL DAÑO ANTIJURÍDICO: Solución de los problemas administrativos que generan litigiosidad e implica el uso de recursos públicos para reducir los eventos generadores del daño antijurídico

PROBABILIDAD: Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

PUNTOS DE RIESGO: Son actividades dentro del flujo del proceso donde existe evidencia o se tiene indicios que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

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

RIESGO DE SEGURIDAD DE LA INFORMACIÒN: 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. (ISO/IEC 27000).

RIESGO INHERENTE: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

RIESGO RESIDUAL: El resultado de aplicar la efectividad de los controles al riesgo inherente.

SEVERIDAD: Nivel de un riesgo, dado por una probabilidad y un impacto. En cada nivel se define el tratamiento y los niveles de responsabilidad.

TOLERANCIA DEL 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.

2 NORMATIVIDAD

AÑO	NORMA	NOVEDAD
1991	Constitución Política	Adopta los principios de la función administrativa y elimina el control fiscal previo y obligatoriedad para todas las entidades estatales de contar con el control interno.
1993	Ley 87	Crea el Sistema Institucional de Control Interno y dota a la administración de un marco para el control de las actividades estatales, directamente por las mismas autoridades.
1998	Ley 489	Fortalece el Control Interno, con la creación del Sistema Nacional de Control Interno
2001	Decreto 1537	Provee elementos técnicos y administrativos para fortalecer el Sistema de Control Interno (SCI) Establece la administración del Riesgo se contempla como parte integral del fortalecimiento de los SCI
2005	Decreto 1599	Adopta un marco general para el ejercicio del Control Interno, a través del Modelo Estándar de Control Interno –MECI y dota al Estado colombiano de una estructura única.
2012	Decreto 1599	Integra en un solo sistema todas aquellas herramientas de gestión, presenta a las entidades el Modelo Integrado de Planeación y Gestión, el cual recoge el Sistema de Desarrollo Administrativo en cinco políticas MECI se configura como la herramienta de seguimiento y control del Modelo.
2012	Ley 1523	Adopta la política nacional de gestión del riesgo de desastres y se establece el Sistema Nacional de Gestión del Riesgo de Desastres
2014	Decreto 943	Actualiza el MECI a una versión más moderna y de fácil comprensión por parte de las entidades.
2014	Decreto 1443	implementación del sistema de seguridad y salud en el trabajo (SG-SST).
2015	Ley 1753	Iintegra en un solo Sistema de Gestión, los Sistemas de Gestión de la Calidad (Ley 872 de 2003) y de Desarrollo Administrativo (Ley 489 de 1998) articulado con los Sistemas Nacional e Institucional de Control Interno (Ley 87 de 1993 y en los artículos 27 al 29 de la Ley 489 de 1998)

2017	Decreto 602	Adiciona la Parte 4 del Libro 2 del Decreto 1079 de 2015 y se reglamentan los artículos 84 de la Ley 1523 de 2012 y 12 y 63 de la Ley 1682 de 2013, en relación con la gestión del riesgo de desastres en el Sector Transporte
2017	Decreto 1499	Articula el Sistema de Gestión en el marco del Modelo Integrado de Planeación y Gestión – MIPG, a través de los mecanismos de control y verificación que permiten el cumplimiento de los objetivos y el logro de resultados de las entidades Actualiza el Modelo Estándar de Control Interno para el Estado Colombiano – MECI a través del Manual Operativo del Modelo Integrado de Planeación y Gestión – MIPG (correspondiendo a la 7° Dimensión de MIPG)
2017	Decreto 2157	Adopta directrices generales del Plan de Gestión de Riesgo de Desastres de la Entidades Públicas y Privadas en el marco del artículo 42 de la Ley 1523 de 2012
2018	Guía	Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 - Octubre de 2018, disponible en: https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2IjUBdeu/view_file/34316499
2019	Manual	Manual Operativo del Modelo Integrado de Planeación y Gestión Consejo para la Gestión y Desempeño Institucional Versión 3 - Diciembre 2019, disponible en https://www.funcionpublica.gov.co/documents/28587410/34112007/Manual+Operativo+MIPG.pdf/ce5461b4-97b7-be3b-b243-781bbd1575f3
2020	Guía	Guía de auditoría interna basada en riesgos para entidades públicas - Versión 4 - Julio de 2020, disponible en: https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2IjUBdeu/view_file/37060226 Guía para la gestión por procesos en el marco del modelo integrado de planeación y gestión (Mipg) - Versión 1 - Julio de 2020, disponible en https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2IjUBdeu/view_file/36963907
2020	Guía	Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 Diciembre de 2020. https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2IjUBdeu/view_file/34316499

3 CONTEXTO

Contribuyendo a la implementación del Modelo Integrado de Planeación y Gestión (MIPG), la Oficina Asesora de Planeación formuló para la vigencia 2020 un plan de trabajo que incluye la revisión participativa de la Plataforma Estratégica y el modelo de operación de la entidad.

Es así, que mediante MEMORANDO CIRCULAR No OAP 18573 del 01/04/2020, se socializó el esquema virtual del acompañamiento, vinculando a los Líderes de Proceso y Facilitadores del MIPG.

En desarrollo de la "***Fase I: Revisión Plataforma Estratégica***", se identificaron aspectos de mejora en la MISIÓN, VISIÓN y OBJETIVOS ESTRATÉGICOS y durante la "***Fase II: Revisión Modelo de Operación (gestión por procesos)***" se recolectó información para actualizar el diagnóstico de capacidades y entornos y se documentaron las necesidades y expectativas de los grupos de valor; dando inicio a la "**Fase III: Actualización /documentación de las caracterizaciones de *proceso***".

Teniendo en cuenta, que el Departamento Administrativo Función Pública realizó el lanzamiento de la nueva "***Guía para la gestión por procesos en el marco del modelo integrado de planeación y gestión (MIPG)***" -acorde con el esquema de trabajo de la Oficina Asesora de Planeación- y socializó la nueva versión de las "***Guía para la administración del riesgo y el diseño de controles en entidades públicas***", se hace necesario actualizar la actual política de administración de riesgos, incorporando mejoras a la existente.

En virtud de lo anterior, la presente política contiene lineamientos para la administración de los **riesgos de gestión, corrupción y seguridad digital.** En cuanto a los demás riesgos aplicables a la entidad se considerará los siguiente:

- Los Riesgos relacionados con la **seguridad y salud en el trabajo,** se intervendrán de acuerdo con la Metodología GTC 45 Versión 2012 y la matriz de peligros y riesgos de conformidad con el documento ATALHU-FR- 64, Matriz de identificación de peligros, evaluación y valoración de riesgos, los cuales están disponibles en el sistema de gestión del INVIAS
- Para la gestión de los **riesgos de contratación** se tendrá en cuenta el Documento Conpes 3714 de 2011 y los lineamientos de Colombia Compra Eficiente.
- Los **riesgos defensa jurídica** serán administrados bajo la metodología de prevención del daño antijurídico de la Agencia Nacional de Defensa Jurídica del Estado donde el Comité de Conciliación anualmente aprobará la Política de Prevención del Daño Antijurídico, el representante legal de la Entidad expedirá el documento mediante el cual se adopte la Política de Prevención del Daño Antijurídico e impartirá las directrices para su divulgación y el Secretario Técnico del Comité de Conciliación junto con su grupo de apoyo, brindará la información y prestará la colaboración necesaria para realizar el respectivo seguimiento y evaluación.
- La gestión de **riesgos de desastres *(naturales y antrópicos)*** se desarrollará de acuerdo con lo estipulado en el Decreto 2157 de 2017 "*por medio del cual se adoptan directrices generales para la elaboración del plan de gestión del riesgo de desastres de las entidades públicas y privadas en el marco del artículo 42 de la ley 1523 de 2012*" o normas que la actualicen o sustituyan. Anualmente, el Director General liderará la formulación y actualización del *PLAN DE GESTIÓN DEL RIESGO DE DESASTRES DE LAS ENTIDADES PÚBLICAS Y PRIVADAS* y los órganos de control del Estado ejercerán procesos de monitoreo, evaluación y control y, la sociedad, a través de los mecanismos de veeduría ciudadana, al plan de gestión del Riesgo de la Entidad.

4 OBJETIVO

Contribuir a la seguridad razonable frente al cumplimiento de la misión y al logro de los objetivos institucionales, mediante la asignación de roles y responsabilidades de cada uno de los servidores y contratistas de prestación de servicios de la Entidad (Esquema de las Líneas de Defensa) y adopción de lineamientos para el tratamiento, manejo y seguimiento a los riesgos de *gestión, corrupción, y seguridad digital,* para la administración de riesgos de la entidad.

5 ALCANCE

La Política Institucional de Administración del Riesgo es aplicable a todos los procesos del modelo de operación por procesos, a los planes institucionales, a los programas, a los proyectos y a las acciones ejecutadas por los servidores públicos y contratistas de prestación de servicios del Instituto Nacional de Vías, durante el ejercicio de sus funciones y obligaciones, respectivamente, tanto en Planta Central como las Direcciones Territoriales.

Incluye lineamientos para el tratamiento, manejo y seguimiento a los riesgos de: *gestión, corrupción, y seguridad digital.*

6 ROLES (Niveles de Autoridad y Responsabilidad)

Los roles serán acordes con el **modelo de líneas de defensa:**

6.1 LÍNEA ESTRATÉGICA:

El Director General y la alta dirección:
Definirán los lineamientos para la administración del riesgo de la entidad; el equipo directivo determinará el apetito, tolerancia y capacidad de los riesgos, identificará aquellos riesgos que impidan el logro de su propósito fundamental y las metas estratégicas.

La alta dirección:
Analizará los cambios en el entorno (contexto interno y externo), que puedan tener un impacto significativo en la operación de la entidad y generen cambios en la estructura de riesgos y controles. Para ello, durante la formulación del Plan Estratégico Institucional (o antes, cuando las circunstancias lo ameriten) la Oficina Asesora de Planeación coordinará la revisión de la Plataforma Estratégica y la elaboración del Diagnóstico de Capacidades y del Entorno bajo la metodología DOFA, con el fin de documentar el contexto general de la entidad y asesorar a la línea estratégica en la decisión y/o actualización de la Política Institucional de Administración del Riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo.

Comité Institucional de Coordinación de Control Interno:

- Asegurará de la permeabilización en todos los niveles de la organización pública de la presente política institucional, de tal forma que cada una de las tres líneas de defensa conozcan claramente los niveles de responsabilidad y autoridad que posee frente a la gestión del riesgo.
- Evaluará y dará línea sobre la administración de los riesgos en la Entidad.
- Evaluará el estado del Sistema de Control Interno y aprobará las modificaciones, actualizaciones y acciones de fortalecimiento del mismo.
- Realizará seguimiento a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por la Oficina de Control Interno.
- Analizará eventos y riesgos críticos.

Comité Institucional de Gestión y Desempeño:

- Aprobará el Mapa de riesgos de corrupción que hace parte del Plan Anticorrupción y de Atención al Ciudadano y las actualizaciones del mismo.
- Analizará gestión del riesgo y aplica mejoras.

6.2 PRIMERA LÍNEA DE DEFENSA – Gerentes públicos, líderes de proceso y sus equipos de trabajo

Desarrollarán e implementarán procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora, para ello se diseñan, implementan y monitorean los controles y gestionaran de manera directa en el día a día los riesgos de la entidad, por lo tanto:

- Identificarán y valorarán los riesgos, que pueden afectar los procesos a su cargo y los actualizarán cuando se requiera, bajo la metodología vigente, informando de la novedad a la Oficina Asesora de Planeación.
- Definirán, diseñarán, aplicarán y realizarán seguimiento a los controles para mitigar los riesgos y propondrán mejoras a la gestión del riesgo en su proceso.

- Supervisarán la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectando las deficiencias de los controles y determinando las acciones de mejora a que haya lugar.
- Revisarán el cumplimiento de los objetivos de sus procesos e identificarán en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.
- Revisará y realizará seguimiento al cumplimiento de las actividades y planes de acción acordados con la línea estratégica, segunda y tercera línea de defensa con relación a la gestión de riesgos.
- Revisarán los planes de acción o de contingencia establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento y lograr el cumplimiento a los objetivos.
- Orientará el desarrollo e implementación de políticas y procedimientos internos.
- Asegurará que sean compatibles con las metas y objetivos de la entidad, y cuando sea el caso emprenderá acciones de mejoramiento para su logro.
- Reportará a la Oficina Asesora de Planeación:
    - Los eventos (riesgos materializados) e incidentes que generan o podrían generar pérdidas a la entidad, junto con el tratamiento correspondiente.
    - El "*Desempeño del control= # eventos / frecuencia del riesgo (# veces que se hace la actividad)*" e indicadores calves de los riesgos, para evaluar la tendencia la eficacia de los controles que se disponen para mitigarlos.
    - Monitoreo y evaluación permanente a la gestión de riesgos

6.3 SEGUNDA LÍNEA DE DEFENSA

Para determinar quienes pertenecen a la segunda línea de defensa es necesario dar respuesta a las siguientes preguntas:

- ¿Pertenece a la media o alta gerencia de la entidad?
- ¿Responde ante la alta dirección por un tema transversal de la entidad?
- ¿Realiza actividades de seguimiento y evaluación a los controles de la primera línea de defensa?

En este orden de ideas la **Oficina Asesora de Planeación,** pertenece a la segunda línea de defensa, no obstante, esto no quiere decir que sea la única que pertenezca a dicha línea, ya que todas aquellas dependencias que cumplan los criterios antes enunciados también harán parte de la segunda línea.

La Oficina Asesora de Planeación se encargará de asistir y guiar a la línea estratégica y la primera línea de defensa en la gestión adecuada de los Riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos (a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos) y monitoreará la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo de la siguiente forma:

- Revisará los cambios en el Direccionamiento Estratégico o en el entorno y cómo éstos pueden generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de apoyar a sus líderes de proceso en la actualización del mapa de riesgos.
- Asesorará a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo.

- Difundirá la presente metodología y acompañará, orientará y entrenará a los líderes de procesos en la identificación, análisis y valoración del riesgo.
- Revisará la adecuada definición de los objetivos de los procesos y su alineación con los objetivos institucionales y realizará las recomendaciones a que haya lugar.
- Revisará el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizará recomendaciones para el fortalecimiento de los mismos.
- Diseñará y pondrá en marcha mecanismos para que los funcionarios, contratistas de prestación de servicios, la ciudadanía y los interesados externos (Interventores, Contratistas de obra, entre otros) conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del Mapa de Riesgos de Corrupción.
- Consolidará el Mapa de riesgos de Corrupción y lo presentará para revisión y aprobación del Comité Institucional de Gestión y Desempeño. Una vez sea aprobado, lo publicará en la página web de la entidad, como anexo al Plan Anticorrupción y de Atención al Ciudadano, a más tardar el 31 de enero de cada vigencia.
- Consolidará el Mapa de riesgos institucional y lo presentará para análisis y seguimiento ante el Comité Institucional de Coordinación de Control Interno.
- Supervisará en coordinación con los demás responsables de esta segunda línea de defensa, que la primera línea identifique, evalué y gestione los riesgos y controles para que se generen acciones.
- Evaluará que los riesgos sean consistentes con la presente política y que sean monitoreados por la primera línea de defensa.
- Identificará cambios en el apetito del riesgo en la Entidad, especialmente en aquellos riesgos ubicados en zona baja y los presentará para aprobación del Comité Institucional de Coordinación de Control Interno.
- Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos y realizará seguimiento mensual a los resultados de las acciones emprendidas para mitigar los riesgos.
- Consolidará los seguimientos a los mapas de riesgo y elaborará informes trimestrales para el Comité de Coordinación del Sistema de Control Interno.
- Administrará la una Base Histórica de Eventos con los incidentes que generan o podrían generar pérdidas a la entidad, reportadas por la 1° y 3° línea de defensa.
- Asegurará que los controles y procesos de gestión del riesgo de la 1ª línea de Defensa sean apropiados y funcionen correctamente (supervisión de la implementación de prácticas de gestión de riesgo eficaces)

6.4 TERCERA LÍNEA DE DEFENSA- Oficina de Control Interno

Proporcionará un aseguramiento, a través de la auditoría interna, sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primer línea y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, basado en el más alto nivel de independencia y objetividad sobre la efectividad del Sistema de Control Interno (SCI), para lo cual:

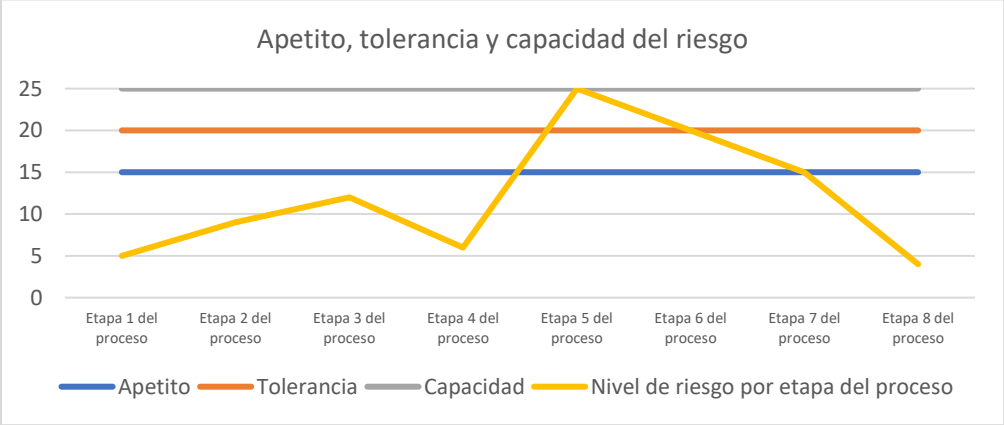
- Identificará y evaluará cambios que podrían tener un impacto significativo en el Sistema de Control Interno (SCI) y/o evaluación de los riesgos, durante las evaluaciones periódicas de

riesgos y en el curso del trabajo de auditoría interna y lo reportará al Comité de Coordinación del Sistema de Control Interno.

- Proporcionará un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del SCI.
- Revisará la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos de la entidad.
- Alertará a la línea estratégica sobre la probabilidad de riesgo de corrupción en las áreas auditadas.
- Asesorará de forma coordinada con la Oficina Asesora de Planeación, a la primera línea de defensa en la identificación de los riesgos institucionales y diseño de controles.
- Recomendará mejoras a la política de administración del riesgo.
- Revisará la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo vinculadas a riesgos de la entidad.
- Adelantará seguimiento a la gestión de riesgos de corrupción, verificando la publicación del Mapa de Riesgos de Corrupción en la página web de la entidad y la efectividad de los controles. Y publicará los resultados en la página web de la Entidad dentro de los diez (10) primeros días de los meses de **mayo** (con corte a 30 de abril), **septiembre** (corte 31 de agosto) y **enero** (corte 31 de diciembre).
- Proporcionará un aseguramiento objetivo e independiente sobre la eficacia de gobierno, gestión de riesgos y control interno a la Alta Dirección de la entidad, incluidas las maneras en que funciona la primera y segunda línea de defensa.

7 METODOLOGÍA

El apetito, tolerancia y capacidad del riesgo será la misma para los riesgos de gestión, corrupción y seguridad digital y se calculó de la siguiente forma:



- El apetito del riesgo corresponde a 15, valor máximo deseable del nivel de riesgo que podría permitir el logro de los objetivos institucionales en condiciones normales de operación del modelo integrado de planeación y gestión en la entidad.
- La tolerancia es 20, valor que es superior al apetito de riesgo y menor a la capacidad de riesgo.
- La capacidad del riesgo es 25, teniendo en cuenta qué es el valor máximo al combinar la escala de probabilidad e impacto.

La identificación de riesgos tiene como objetivo establecer cuáles son los riesgos asociados a la operación de la entidad, lo que permitirá determinar cuáles están identificados, controlados y cuales no. Para ello se debe tener en cuenta el contexto estratégico en el que opera la Entidad, objetivos estratégicos y de procesos, puntos de riesgo operativo, áreas de impacto y factores de riesgo.

Durante el análisis de los riesgos se establecerá la probabilidad de ocurrencia y sus consecuencias o impacto. Partirá del análisis preliminar (riesgo inherente) y tendrá en cuenta la valoración de los controles, para establecer el movimiento en la matriz de calor y determinar el nivel de riesgo residual; elementos considerados para definir el plan de acción (opción de tratamiento) acorde con las estrategias para combatir el riesgo.

El paso a paso para la identificación y valoración de los riesgos variará teniendo en cuenta las particularidades de los riesgos de gestión, corrupción y seguridad digital.

7.1 RIESGOS DE GESTIÓN

Las políticas de operación y el paso a paso se encuentran detallados en el ***Anexo 1: EDEPI-PR-9 ADMINISTRACIÓN DE RIESGOS DE GESTIÓN.***

7.2 RIESGOS DE CORRUPCIÓN

La metodología será acorde con el Decreto 124 de 2016 y la normatividad que la actualice la Secretaria de Transparencia del Departamento Administrativo de la Presidencia de República.

Las políticas de operación y el paso a paso se encuentran detallados en el ***anexo 2: EDEPI-PR-10 ADMINISTRACIÓN DE RIESGOS DE CORRUPCIÓN.***

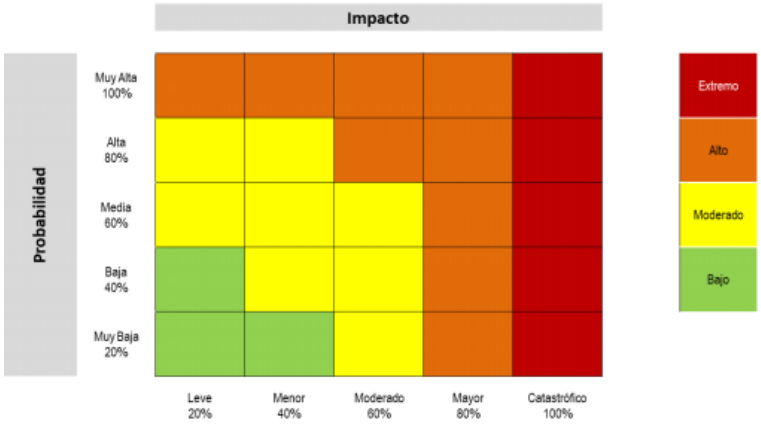
7.3 RIESGOS DE SEGURIDAD DIGITAL

La metodología será acorde con el Modelo de Privacidad y Seguridad de Información, el Marco de Transformación Digital y lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC.

Las políticas de operación y el paso a paso se encuentran detallados en el ***anexo 3: ETICOM-PR-19 ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD DIGITAL.***

8 NIVELES DE ACEPTACIÓN

Los niveles de aceptación de los riesgos de gestión y seguridad digital, variarán según la celda en la que se ubica el riesgo residual en la matriz de calor (niveles de severidad):



La matriz cuenta con 5 filas y 5 columnas, siendo las columnas las alternativas de impacto y las filas las opciones de probabilidad.

Los niveles aceptables de riesgos serán los siguientes:

	Descripción
Extremo	Los riesgos que se ubiquen en esta zona superan los niveles de riesgo aceptado, la Alta Dirección debe establecer el tratamiento e informar al Comité Institucional de Coordinación de Control Interno.
Alto	Los riesgos que se ubiquen en esta zona superan los niveles de riesgo aceptado, el líder del proceso debe establecer el tratamiento e informar al Comité Institucional de Gestión y Desempeño.
Moderado	Los riesgos que se ubiquen en esta zona superan los niveles de riesgo aceptado, el líder del proceso debe hacer seguimiento mediante procedimientos existentes.
Bajo	Los riesgos que se ubiquen en esta zona serán aceptados, el líder del proceso debe hacer seguimiento y llevar el registro correspondiente.

En la siguiente tabla se encuentran las acciones a emprender ante los riesgos materializados:

Responsable	Acción
Líder de Proceso	Informar a la Secretaría General y a la Oficina Asesora de Planeación sobre el hecho encontrado y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado) realizar la denuncia ante la instancia de control correspondiente. Identificar las acciones correctivas necesarias y documentarlas en el Plan de Mejoramiento, efectuando análisis de causas y determinando acciones preventivas y de mejora. Coordinar con la Oficina Asesora de Planeación la actualización de lo pertinente en los mapas de riesgos de corrupción, del proceso e institucional.
Oficina de Control Interno	Informar al Líder del proceso, quien analizará la situación y definirá las acciones a que haya lugar y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado) realizará la denuncia ante la instancia de control correspondiente. Informar a la Secretaría General y a la Oficina Asesora de Planeación con el fin facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar lo pertinente en los mapas de riesgos de corrupción, del proceso e institucional.
Comité de Coordinación de Control Interno	Analizará las causas de los eventos (riesgos materializados) y definirá cursos de acción.

En el caso de los riesgos de corrupción, estos no pueden ser aceptados, en cumplimiento de la consigna tolerancia cero a los hechos de corrupción. De igual manera, el análisis de impacto se realizará teniendo en cuenta solamente los niveles *"moderado", "mayor"* y *"catastrófico"*, dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor.

9 MONITOREO Y REVISIÓN

Anualmente los **líderes de proceso con sus respectivos equipos de trabajo**, identifican y/o validan los riesgos de gestión, corrupción y seguridad digital asociados al logro de los objetivos de los procesos institucionales. Para ello, documentarán lo propio en las hojas de trabajo institucionales y podrán contar con el acompañamiento de la Oficina Asesora de Planeación.

Los riesgos de gestión, corrupción y seguridad digital que se encuentren en zona de riesgo BAJO, que soporten documentación de sus controles en procedimientos, se evidencie la implementación de sus controles existentes y no presenten materialización durante la vigencia, pueden ser considerados para su eliminación.

A continuación, se encuentra una tabla de resumen con la frecuencia y responsable de cada reporte:

RESPONSABLE	FRECUENCIA	REPORTE
COMITÉ INSTITUCIONAL DE COORDINACIÓN DE CONTROL INTERNO	Anual	Pronunciamiento sobre el perfil de riesgo inherente y residual de la entidad
	Semestral	Análisis de los riesgos institucionales
	Trimestral	Seguimiento sobre los riesgos ubicados en la zona de riesgos extremo
LÍDERES DE PROCESO	Acorde al nivel de Riesgo Residual: • MODERADO: Trimestral • ALTO: Bimensual • EXTREMO: Mensual	Seguimiento sobre los riesgos en formato estandarizado de reporte.
JEFE OFICINA ASESORA DE PLANEACIÓN	Mensual	Estado del arte de implementación de la política institucional de administración del riesgo, socializado mediante memorando circular
	Trimestral	• Seguimientos a los mapas de riesgo • Eventos de riesgos que se han materializado en la entidad
JEFE OFICINA DE CONTROL INTERNO	Cuatrimestral	Seguimiento a la gestión de riesgos de corrupción
	De conformidad con el Plan Anual de Auditoria	Seguimiento a los riesgos consolidados en los mapas de riesgos

10 ESTRATEGIAS DE COMUNICACIÓN TRANSVERSALES

Los mecanismos de comunicación utilizados para dar a conocer la política de riesgos en todos los niveles de la entidad serán acordes al Plan de Comunicaciones Institucional.

Con el fin de construir una relación de confianza entre la Entidad y la ciudadanía que derive en el fortalecimiento institucional, se vincularán en las distintas etapas de la gestión del riesgo para:

- Identificar puntos críticos sobre los procesos que permitan mejorar la presentación del servicio y satisfacer las necesidades de los ciudadanos.
- Realizar una valoración sobre la probabilidad e impacto de los riesgos para determinar el nivel de riesgo al que está expuesta la entidad.
- Diseñar y ejecutar controles que atiendan la(s) causa(les) que generan los riesgos.
- Realizar seguimiento a los controles.
- Facilitar la generación de alertas tempranas y oportuna toma de decisiones.

11 ANEXOS

Anexo 1: EDEPI-PR-9 ADMINISTRACIÓN DE RIESGOS DE GESTIÓN.

Anexo 2. EDEPI-PR-10 ADMINISTRACIÓN DE RIESGOS DE CORRUPCIÓN.

Anexo 3. ETICOM-PR-19 ADMINISTRACIÓN DE RIESGOS DE SEGURIDAD DIGITAL.