EMPRESA DE VIVIENDA DE ANTIOQUIA – VIVA

TABLA DE CONTENIDO

1. INTRODUCCION.

La empresa de Vivienda de Antioquia - VIVA como entidad del orden público se encuentra expuesta a una serie de factores de tipo externo e interno que pueden poner en riesgo el cumplimiento de su misión y objetivos institucionales, así como el desarrollo eficiente y efectivo de sus procesos; por ende se hace necesario realizar el análisis del contexto e implementar una guía metodológica que permita identificar, analizar, valorar y el tratamiento encaminado al manejo de los impactos generados.

Es importante así mismo el cumplimiento de requisitos de orden normativo contemplados a través del Decreto 1537 de 2001 en donde se establece la identificación y el análisis de riesgos como un proceso permanente e interactivo entre las oficinas de control interno y la administración, y deja a la vista la responsabilidad que deben adquirir los encargados de los procesos en la aplicación de las políticas de tratamiento definidas. En este sentido, el Decreto 1599 de 2005 adopta el Modelo Estándar de Control Interno – MECI para todas las entidades del Estado, en donde se contempla a la administración del riesgo dentro del Subsistema de Control Estratégico. Valiéndose de elementos como la misión, la visión, los objetivos, los valores y las estrategias para promover el compromiso de la dirección e involucrarse en todos los procesos de la entidad. Este modelo fue actualizado a través de los decretos 943 de 2014 y 1499 de 2017.

Por otra parte, una vez la entidad estructure su sistema de administración de riesgos, éste: contribuye al logro de los objetivos institucionales y al mejoramiento del desempeño organizacional a través de la generación de una cultura del riesgo, define una base confiable para la planeación y la toma de decisiones, involucra a todos los procesos y el talento humano de la entidad y promueve el mejoramiento continuo a partir del seguimiento, la revisión y el establecimiento de metas de desempeño institucional, dirigidas a mejorar la calidad de los servicios ofertados y la eficacia de las operaciones realizadas.

A continuación, se describen las etapas para la identificación, análisis, evaluación y tratamiento de los riesgos vinculados con los procesos del Sistema de Gestión de VIVA y aquellos que por disposición de la Ley 1474 de 2011 son denominados riesgos de corrupción.

2. OBJETIVO.

Establecer los lineamientos metodológicos para llevar a cabo la identificación, análisis, valoración y tratamiento de riesgos por procesos con miras a generar y gestionar el Mapa de Riesgos de VIVA. Reducir los casos eventuales que pueden, volver los riesgos en oportunidades y con enfoque de futuro.

3. ALCANCE.

La administración del riesgo aplica para todos los procesos del Sistema de Gestión (estratégicos, misionales, de apoyo y de evaluación independiente) que integrados al mapa de procesos de VIVA. Inicia con la evaluación análisis del contexto (externo e interno) de una forma actualizada

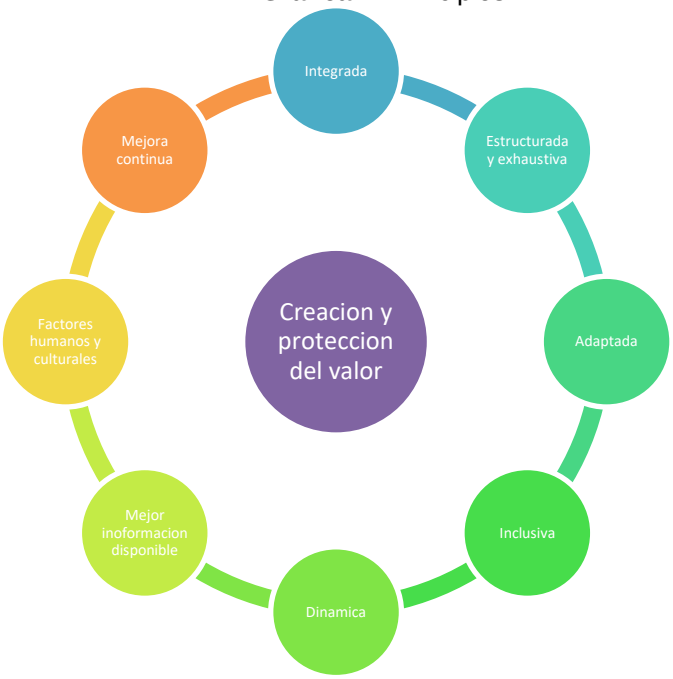
el contexto se convierte en una fuente primaria para la adecuada gestión del riesgo de los riesgos y termina con su monitoreo y seguimiento, con el fin de evidenciar el cumplimiento de las acciones planteadas.

4. PRINCIPIOS.

El propósito de la gestión del riesgo es la creación y la protección del valor, mejorar el desempeño, fomentar la innovación y contribuye al logro de objetivos de VIVA.

Los principios proporcionan orientación sobre las características de una gestión del riesgo eficaz y eficiente, comunicando su valor y explicando su intención y propósito. Son el fundamento de la gestión del riesgo y se deberían considerar cuando se establece el marco de referencia en los procesos de la gestión del riesgo de la organización. Estos principios habilitan a la entidad para gestionar los efectos de la incertidumbre sobre sus objetivos institucionales.

Gráfica 1: Principios.



Fuente: NTC ISO 31000: 2018 - Gestión del riesgo. Directrices.

La gestión del riesgo eficaz requiere los elementos de la gráfica 1 y puede explicarse como sigue:

Integrada: La gestión del riesgo es parte integral y transversal a todas las actividades de la organización.
Estructurada y exhaustiva: Un enfoque estructurado y exhaustivo hacia la gestión del riesgo contribuye a resultados coherentes y comparables.

Adaptada: El marco de referencia de la 31000 y el proceso de la gestión del riesgo se adaptan y son proporcionales a los contextos externo e interno de la organización relacionados con sus objetivos.
Inclusiva: La participación apropiada y oportuna de las partes interesadas permite que se consideren su conocimiento, puntos de vista y percepciones. Esto resulta en una mayor toma de conciencia y una gestión del riesgo informada.
Dinámica: Los riesgos pueden aparecer, cambiar o desaparecer con los cambios de los contextos externo e interno de la organización. La gestión del riesgo anticipa, detecta, reconoce y responde a esos cambios y eventos de una manera apropiada y oportuna.
Mejor información disponible: Las entradas a la gestión del riesgo se basan en información histórica y actualizada, así como en expectativas futuras. La gestión del riesgo tiene en cuenta explícitamente cualquier limitación e incertidumbre asociada con tal información y expectativas. La información debería ser oportuna, clara y disponible para las partes interesadas pertinentes.
Factores humanos y culturales: El comportamiento humano y la cultura influyen considerablemente en todos los aspectos de la gestión del riesgo en todos los niveles y etapas.
Mejora continua: La gestión del riesgo mejora continuamente mediante aprendizaje y experiencia.

La segunda línea de defensa liderada por la Dirección de planeación conjuntamente con el apoyo del proceso de Gestión Organizacional evaluará como mínimo una vez al año y se presentará a la línea Estratégica (Alta Dirección) informe sobre la apropiación de estos principios verificando y midiendo la creación y la protección del valor, el mejoramiento del desempeño y el fomento de la innovación para el logro de objetivos institucionales en el **Formato PLE-FO-17 Aplicación principios gestión de riesgos** y que a su vez permitirá evaluar el nivel de madurez de la gestión de los riesgos de VIVA.

5. MARCO LEGAL Y/O NORMATIVO.

- 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.

- 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.

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

- Directiva Presidencial 09 de 1999. Lineamientos para la implementación de la política de lucha contra la corrupción.

- NTC ISO 31000:2018. Gestión del riesgo - Directrices

- NTC ISO 9001:2015. Sistemas de Gestión de la Calidad – Requisitos.

- NTC ISO 27000:2017. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información (SGSI). Visión general y vocabulario.

- NTC ISO 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.

- NTC 137 de 2011: Equivalente a la guía 73

- Plan Anticorrupción y de Atención al Ciudadano VIVA.

- Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas-DAFP versión 6 de noviembre del 2022.

6. GLOSARIO.

- **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.
- **Amenaza:** situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.
- **Análisis del riesgo**: proceso para comprender la naturaleza del riesgo y determinar el nivel del riesgo
- **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.
- **Causas:** 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.
- **Capacidad de riesgo**: (tercer nivel del 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 institucionales de la entidad.
- **Control:** medida que permite reducir, mitigar u optimizar para convertir en una oportunidad un riesgo.
- **Confidencialidad:** propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

- **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.
- **Contexto estratégico**: conjunto de circunstancias internas y externas que puedan generar eventos que originen oportunidades o afecten el cumplimiento de su función, misión y objetivos institucionales
- **Criterios de riesgos:** términos de referencia sobre los cuales se evalúa la importancia de un riesgo (Probabilidad e impacto). Estos criterios se definen con base en los objetivos de la organización y en el contexto interno y externo.
- **Disponibilidad:** propiedad de ser accesible y utilizable a demanda por una entidad.
- **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.
- **Evaluación del riesgo**: proceso de la identificación, análisis y de los riesgos, para determinar si están dentro del apetito al riesgo.
- **Factores de riesgo:** son las fuentes generadoras de riesgos.
- **Gestión de riesgos:** 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.
- **Identificación del riesgo**: proceso que posibilita conocer los eventos potenciales, que estén o no bajo el control de la organización, para ello se debe tener en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.
- **Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo
- **Integridad:** propiedad de exactitud y completitud.
- **Incidente:** evento o serie de eventos de seguridad digital no deseados o inesperados, que tienen probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Mapa de riesgos:** documento con la información resultante de la evaluación de los riesgos y tratamientos de la gestión del riesgo.
- **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.
- **Política de administración de riesgos**: declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo. La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.
- **Probabilidad:** se entiende como la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. (Hace referencia a datos para determinar el escenario probabilístico) desde el concepto matemático basado en riesgo. Posibilidad con alta carga de incertidumbre**.**

- **Proceso:** conjunto de actividades mutuamente relacionadas o que interactúan, que utilizan las entradas para proporcionar un resultado previsto.
- **Propietario del riesgo:** persona o entidad con responsabilidad y autoridad para gestionar un riesgo.
- **Riesgo:** efecto de incertidumbre sobre los objetivos institucionales.
- **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. Nivel de riesgo que queda después de la aplicación de los controles
- **Valoración del riesgo**: es la tercera fase de la evaluación) es el resultado del análisis de los valores asignados a cada riesgo a partir de los criterios de probabilidad e impacto, universidad de Valencia.
- **Vulnerabilidad:** representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

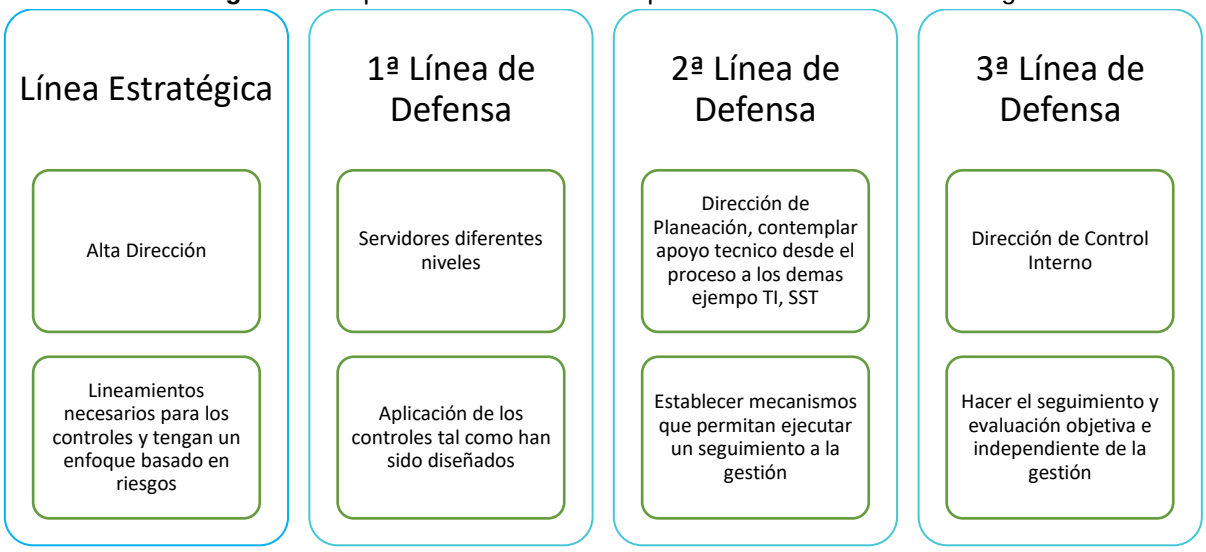
7. DISPOSICIONES GENERALES.

Considerando que la gestión del riesgo es un proceso efectuado por la alta dirección de la VIVA y por todo el personal con el propósito de proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos, los principales beneficios para la entidad son los siguientes:

- Apoyo a la toma de decisiones de la Alta Dirección.
- Garantiza la operación normal de la organización y la búsqueda permanente de la mejora continua.
- Minimiza la probabilidad e impacto de los riesgos de los diferentes procesos.
- Mejoramiento en la calidad de procesos y sus servidores (calidad va de la mano con riesgos).
- Fortalecimiento de la cultura de control de VIVA.
- Incrementa la capacidad de la entidad para alcanzar sus objetivos.
- Dota a la entidad de herramientas y controles para hacer una administración más eficaz y eficiente

El modelo integrado de planeación y gestión (MIPG) define para su operación articulada la creación en todas las entidades del Comité Institucional de Gestión y Desempeño, regulado por el Decreto 1499 de 2017 y el Comité Institucional de Coordinación de Control Interno, reglamentado a través del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017 y a nivel de Institución- VIVA estableció la resolución 137 del 7 de septiembre de 2022 en donde define roles, responsabilidad y autoridad frente al Modelo de Operación por Procesos, en este marco general, para una adecuada gestión del riesgo, dicha institucionalidad entra a funcionar de la siguiente forma:

Diagrama 1: Operatividad institucional para la administración del riesgo.



Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, DAFP - 2020.

Una vez determinados estos lineamientos básicos, es preciso analizar el contexto estratégico VIVA para establecer su complejidad, procesos y planeación institucional, entre otros aspectos. Esto permite conocer y entender la entidad y su entorno, lo que determinará la gestión y la aplicación de la metodología en general.

Grafica 2: Conocimiento y análisis de entidad.

Fuente: construcción propia a partir de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, DAFP - 2020

8. RESPONSABILIDAD Y AUTORIDAD.

Todos los líderes de los procesos definidos en el Sistema de Gestión de VIVA, con su equipo de trabajo, serán responsables de la aplicación de esta metodología, la implementación de los controles definidos y su seguimiento, con el apoyo permanente del proceso Gestión Organizacional.

La responsabilidad en la implementación y ejecución de los controles y acciones asociadas a la gestión del riesgo, estará definida a partir de roles y no definir nombres específicos de los colaboradores.

a. **Primera línea de defensa:** La primera línea de defensa desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.
   - Son responsables de participar activamente en el desarrollo de la Administración de Riesgo a través del monitoreo permanente de los asuntos de su competencia en cada uno de los componentes, tomando las decisiones que procuren su mejoramiento y disponiendo de los recursos requeridos para su desarrollo; frente a la administración del riesgo les corresponde:

- Realizar seguimiento al cumplimiento de los controles y las acciones de tratamiento de los riesgos, para garantizar que se desarrollen con la oportunidad y calidad requeridas.
- Orientar el desarrollo e implementación de política y procedimientos internos y asegurar que sean compatibles con las metas, y objetivos de la entidad y emprender las acciones de mejoramiento para su logro.
- Evitar y/o minimizar los riesgos asociados al grupo de valor de VIVA que impacta la operación de sus procesos, satisfaciendo sus necesidades y sus expectativas.

b. **Segunda Línea de Defensa:** La segunda línea de defensa asegura que los controles y los procesos de gestión de riesgo implementados por la primera línea de defensa estén diseñados apropiadamente y funcionen como se pretende. Está a cargo de la Dirección de Planeación responsable de apoyar a la Gerencia y que tienen responsabilidades directas en el monitoreo y evaluación de los controles y la gestión del riesgo. Actores involucrados en la Segunda línea de defensa: proceso Gestión Organizacional.

c. **Tercera Línea de Defensa:** Proporciona información sobre la efectividad del Sistema de Gestión a través de un enfoque basado en riesgo incluida la operación de la primera y segunda línea de defensa, verificará el cumplimiento e implementación de esta guía en los procesos definidos por la entidad y la medición de la eficacia de las acciones y controles que permitan contrarrestar la materialización de los riesgos identificados y estará a cargo de la Oficina de Control Interno.

Para el establecimiento e implementación de la gestión de Riesgos es necesario contar con el compromiso y la definición de responsabilidades desde la Gerencia hacia todos los niveles de la entidad por este motivo se presentarán en el Comité Institucional de Gestión y Desempeño los resultados de los seguimientos y monitoreo realizados al mapa de riesgos.

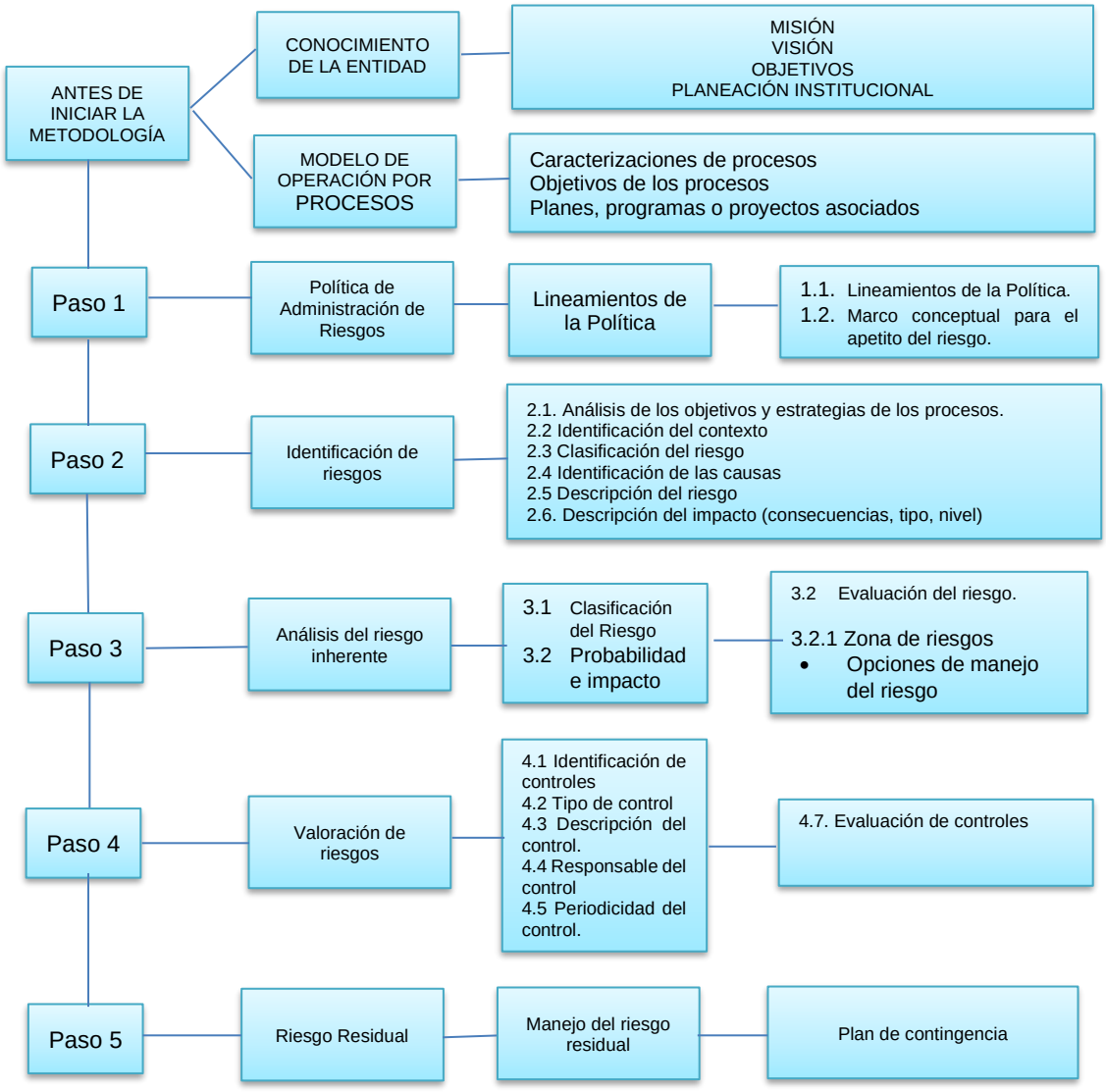
Para esto, la alta dirección designa a un representante de la alta dirección, en este caso la Dirección de Planeación según lo establece la Resolución 137 de 2022, para apoyar a los líderes de procesos y demás servidores quienes son en última instancia los encargados de identificar y actualizar de manera permanente los riesgos asociados a los diferentes procesos.

Cuando se requiera la actualización del contenido de esta política, se realizará bajos los parámetros establecidos por el Proceso Gestión Organizacional y si las hubiere seguir las recomendaciones de los diferentes líderes de procesos.
Será responsabilidad del proceso de Planeación Estratégica realizar el acompañamiento y los seguimiento a los riesgos de gestión y a la oficina de Control Interno le corresponde verificar la eficacia a los controles establecidos tanto para los riesgos de gestión como para los de corrupción, en todo caso esta guía se articulara con la responsabilidad y autoridad establecida en el Plan Anticorrupción y Atención al Ciudadano – PAAC vigente a la fecha.

9. METODOLOGÍA PARA LA ADMINISTRACIÓN Y GESTIÓN DEL RIESGOS.

La metodología para la administración del riesgo requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en la entidad, además del conocimiento de esta desde un punto de vista estratégico de la aplicación de los tres (5) pasos básicos para su desarrollo y, finalmente, de la definición e implantación de estrategias de comunicación transversales a toda la entidad para que su efectividad pueda ser evidenciada. A continuación se puede observar la estructura completa con sus desarrollos básicos:

Diagrama 2: Metodología para la administración y gestión de riesgos.



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, DAFP - 2020.

10. POLÍTICA DE ADMINISTRACIÓN Y GESTIÓN DE RIESGOS.

"Los procesos de la Empresa De Vivienda De Antioquia - VIVA, durante su accionar pueden presentar situaciones o eventos que generen desviaciones en la consecución de sus objetivos. Para ello, a través de su esquema de líneas de defensa establece y aplica herramientas de gestión de riesgos mediante la identificación, análisis, valoración y tratamiento, con el fin de reducir la probabilidad de ocurrencia y/o mitigación del impacto de la materialización de los mismos. Para lograrlo, establece actividades de prevención, sensibilización y control para el tratamiento de los riesgos que puedan afectar los objetivos y metas institucionales, aumentando la capacidad para lograr los resultados previstos, previniendo, reduciendo o eliminando los efectos indeseados".

10.1 Objetivos de la política.

- Controlar a través del Mapa de Riesgos todo el proceso relacionado con el manejo de los riesgos asociados al Sistema de Gestión.
- Proporcionar directrices para la administración de los riesgos asociados a los procesos de la entidad, con el propósito de contribuir a la adecuada identificación, análisis, valoración (riesgos y controles) y tratamiento de los mismos.
- Integrar el manejo de los riesgos de gestión, corrupción, ambientales, seguridad de la información, Seguridad y Salud en el Trabajo asociados a los diferentes procesos que integran el Sistema de Gestión.
- Establecer la responsabilidad de los diferentes líderes de los procesos de. VIVA
- Establecer el rol de las diferentes áreas de VIVA.
- Dar cumplimiento a los requerimientos legales que apliquen al manejo de riesgos de gestión, corrupción, ambientales, seguridad de la información, Seguridad y Salud en el Trabajo.
- Fortalecer el comportamiento profesional y personal de los funcionarios de VIVA, generando toma de conciencia frente al pensamiento basado en riesgos.

10.2 Determinación de la capacidad de riesgo.

El Comité Institucional de Gestión y Desempeño con la participación y aprobación de la alta dirección y en el marco del Comité Institucional de Coordinación de Control Interno debe realizar el análisis de eventos y riesgos críticos que tienen un nivel de severidad muy alto frente a los cuales se deben tomar decisiones, teniendo en cuenta los siguientes valores:

- Valor máximo de la escala que resulta de combinar la probabilidad y el impacto.

- Valor máximo del nivel de riesgo que la entidad puede soportar y a partir del cual se considera por la alta dirección que no sería posible el logro de los objetivos de la entidad que corresponde a la “capacidad de riesgo”.

10.3 Determinación del apetito de riesgo.

Se debe así mismo, determinar el “apetito de riesgo”, equivalente al nivel de riesgo que la entidad puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la alta dirección en condiciones normales de operación del Modelo Integrado de Planeación y Gestión en la entidad.

El apetito de riesgo puede ser diferente para los distintos tipos de riesgos de la entidad, se debe tener en cuenta que los riesgos de corrupción son inaceptables.

10.4 Tolerancia de riesgo.

El límite o valor de la tolerancia de riesgo es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado. Se debe definir un valor que es igual o superior al apetito de riesgo y menor o igual a la capacidad, el cual es definido por la alta dirección y aprobado por el órgano de gobierno respectivo.

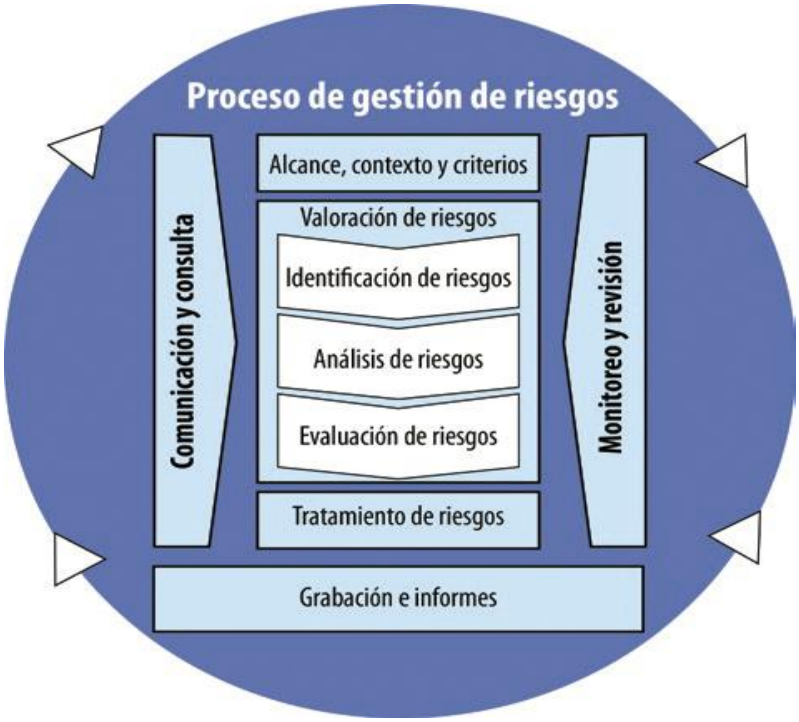
La determinación de la tolerancia de riesgo es optativa para la entidad y su uso está limitado a determinar el tipo de acciones para abordar los riesgos, dado que las acciones que se desprendan a partir del análisis de riesgos deben ser proporcionadas y razonables, lo cual se puede determinar en función del valor del nivel de riesgo residual obtenido y su comparación con el apetito y tolerancia de riesgo.

11. ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO.

Para el desarrollo del elemento de Administración de Riesgo en VIVA se debe contar con una serie de pasos lógicos y ordenados que permita a los colaboradores responsables de su ejecución desarrollar las actividades pertinentes para construir herramientas de decisión Gerencial que encaminen a la entidad en un proceso de mejoramiento continuo. Los pasos establecidos para el desarrollo de esta metodología se clasifican en:

- Definición del contexto
- Identificación de Riesgos
- Análisis de riesgos
- Valoración de Riesgos
- Establecimiento de opciones de tratamiento de los riesgos
- Seguimiento y revisión
- Registros e informes

Imagen 1: Proceso



Fuente: NTC ISO 31000: 21018 - Gestión del riesgo. Directrices.

11.1 Análisis de objetivos estratégicos y de los procesos.

Los líderes de los diferentes procesos revisaran de manera periódica si el objetivo establecido para el proceso requiere actualización.

Los riesgos identificados deben tener impacto en el cumplimiento de objetivos estratégicos, estar alineados con la misión y la visión institucional, así como, su desdoble hacia los objetivos de los procesos.
Para su adecuada formulación, deben contener unos atributos mínimos, para lo cual se puede hacer uso de las características SMART:

S - **Específico:** Resuelve cuestiones como qué, cuándo, cómo, dónde, con qué, quién considerando el orden y los necesarios para el cumplimiento de la misión.

M - **Medible:** Involucra algunos números en su definición. Ejemplo: porcentajes o cantidades cuando aplique

A - **Alcanzable:** Realizar un análisis de los que se ha hecho y logrado hasta el momento para determinar si lo que se propone es posible o cómo resultaría mejor.

R - **Relevante:** Considera recursos, factores externos e información de actividades previas

T- **Temporal:** Establecer un tiempo al objetivo ayudará a saber si lo que se está haciendo es lo óptimo para llegar a la meta, así mismo permite determinar el cumplimiento y las mediciones

finales.

De acuerdo a lo anterior, se debe tener en cuenta que los indicadores del Sistema de Gestión, permiten medir el cumplimiento del objetivo de cada proceso, alineados con la plataforma estratégica del SIG (Objetivos, política, misión y visión) y de la misma manera los riesgos se identifican a partir de los factores de riesgo que puedan afectar el cumplimiento del objetivo de cada proceso.

11.2 Contexto del riesgo.

Definir las condiciones internas y del entorno que puedan influir negativamente en los procesos y de esta manera tener el panorama general a partir del cual se identifiquen los riesgos. Las situaciones del entorno o externas pueden ser de carácter social, cultural, económico, tecnológico, político y legal, etc, bien sean internacionales, nacionales o regionales.

Las situaciones internas están relacionadas con la estructura, cultura organizacional, el modelo de operación por procesos, el cumplimiento de los planes y programas, los sistemas de información, procesos, procedimientos, recursos humanos y económicos con los que cuenta la Entidad.

11.3 Método para generar el contexto del riesgo.

El proceso de Planeación Estratégica debe realizar y/o actualizar el contexto organizacional por lo menos una vez al año, en el que se incluya un análisis de las debilidades, oportunidades, fortalezas y amenazas de la entidad que a partir de unas condiciones internas o del entorno puedan afectar los elementos de la plataforma estratégica. Es recomendable, en primera instancia que en reunión interna de los diferentes procesos se realice un análisis individual utilizando la caracterización de estos y haciendo un consolidado completo para identificar riesgos que puedan afectar de manera negativa su objetivo. Para ello, se debe revisar en particular aquellas debilidades y amenazas que representen la existencia de un riesgo desde el proceso objeto de análisis.

Luego de identificar los riesgos de gestión de los procesos, se deben incorporar en la matriz **PLE-MT-12 Mapa de Riesgos** y en la matriz **PLE-MT-13**, para los riesgos de corrupción.

Diagrama 3: DOFA

ANALISIS DOFA	**FORTALEZAS**	**DEBILIDADES**
	F1	D1
	F2	D2
	Fn	Dn
OPORTUNIDADES	ESTRATEGIAS (FO)	ESTRATEGIAS (DO)
O1	FO11	DO11
O2	FO12	DO12
On	FOnn	DOnn

AMENAZAS	ESTRATEGIA (FA)	ESTRATEGIA (DA)
A1	FA11	DA11
A2	FA12	DA12
An	FAnn	DAnn

Fuente: Elaboración propia.

A partir de esta herramienta, la cual corresponde a la matriz DOFA se pueden identificar posibles riesgos del proceso, partiendo principalmente de las amenazas y debilidades, ya que estos dos aspectos permiten identificar el riesgo en alguno de sus elementos: Evento, fuente del riesgo, causa, área de impacto y/o consecuencia.

Siga el hipervínculo establecido en la **matriz PLE-MT-12 Mapa de Riesgos y en la matriz PLE-MT-13,** para los riesgos de corrupción, y seleccione una de las opciones que se le presentan, caso de identificar otra opción solicite al Proceso de Gestión Organizacional la inclusión del mismo con su respectiva justificación.

Imagen 2: Contexto estratégico

CONTEXTO ESTRATÉGICO	
FACTORES EXTERNOS	**FACTORES INTERNOS**
Económicos: disponibilidad de capital, emisión de deuda o no pago de la misma, liquidez, mercados financieros, desempleo, competencia.	**Infraestructura:** disponibilidad de activos, capacidad de los activos, acceso al capital.
Medioambientales: emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.	**Personal:** capacidad del personal, salud, seguridad.
Políticos: cambios de gobierno, legislación, políticas públicas, regulación.	**Procesos:** capacidad, diseño, ejecución, proveedores, entradas, salidas, conocimiento.
Sociales: demografía, responsabilidad social, terrorismo.	**Tecnología:** integridad de datos datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento.
Tecnológicos: interrupciones, comercio desarrollo, producción, mantenimiento electrónico, datos externos, tecnología emergente.	

Fuente: Mapa de riesgos organizacionales – VIVA, elaboración propia.

11.4 Clasificación del riesgo.

Representa las clases de riesgos que pueden presentarse, vale aclarar que la clasificación debe ser solo una, la más representativa por cada uno de los riesgos que se identifiquen en este mapa de riesgos.

Siga el hipervínculo establecido en la **matriz PLE-MT-12 Mapa de Riesgos y en la matriz PLE-MT-13,** para los riesgos de corrupción para conocer las características de los riesgos: estratégico, de imagen, Operativo, Financiero, de cumplimiento, de tecnología, de conocimiento, ambientales y de salud ocupacional; y seleccione solo una clasificación de la lista desplegable, por cada uno de los riesgos identificados.

Imagen 3: Clasificación de los riesgos.

CLASIFICACIÓN DEL RIESGO	
ESTRATÉGICOS	Son aquellos que se asocian con toda posibilidad de que suceda algo relacionado con el cumplimiento de los objetivos estratégicos y la misión institucional, la sostenibilidad y subsistencia de la entidad en el corto, mediano y largo plazo.
IMAGEN	Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la entidad, tiene que ver con conocimiento de prácticas corruptas, manejo desacertado de los medios de comunicación, insatisfacción ciudadana por el mal servicio, incumplimiento de planes, programas y proyectos.
OPERATIVO	El riesgo operacional es el riesgo de sufrir pérdidas debido a la inadecuación o fallas en los procesos, personal y sistemas internos o bien por eventos externos. Lo que NO incluye a los riesgos reputacionales, estratégicos y sistémicos
FINANCIERO	Son los relacionados con la Gestión Financiera de la entidad, los cuales pueden estar relacionados con transferencias, ejecución presupuestal, pagos, tesorería, ineficiencias en el manejo de bienes, pérdidas económicas.
REPUTACIONAL	Es aquel que provoca una pérdida potencial de capital financiero, capital social y / o participación de mercado debido a daños relacionados con la reputación de la entidad.
INFRAESTRUCTURA	Son las fallas en los proyectos, liquidez o flujo de caja y cambios regulatorios son los principales factores de riesgo de la infraestructura en Colombia. Elementos que constituyen variables decisivas para la apropiada ejecución y financiación de los prometedores proyectos venideros.
CUMPLIMIENTO	Son todos los relacionados con la capacidad de la entidad para cumplir con los requisitos, aca están inmersos los requisitos regulativos, legales, contractuales, políticas internas, solicitudes de información, ética, calidad, entre otros.
TECNOLOGÍA	Son los relacionados con la capacidad de la entidad, para que la tecnología disponible y proyectada satisfaga las necesidades actuales, futuras y de soporte de la entidad. Esto tiene que ver con Software (compatibilidad, configuración), Hardware (capacidades, desempeños, obsolescencia), Sistemas (Diseños, especificidades, complejidad)
CONOCIMIENTO	Son aquellos que se relacionan con el daño generado por la pérdida de conocimiento e información vital para el desarrollo de las actividades de la entidad. En esta clasificación se encuentran los riesgos en los activos y la seguridad de la información.
LEGAL	Es la posibilidad de incurrir en pérdidas, debido al incumplimiento (o imperfección) de la legislación que afecta a los contratos, o la imposibilidad de exigir el cumplimiento del contrato legalmente.
CORRUPCIÓN	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.
PROCESO	Resultado de la deficiencia de los procesos internos ya utilizados por la organización, como indicadores de desempeño inadecuados, controles ineficaces, modelado inexacto e incluso violación de la ley.
ASOCIADOS A NATURALEZA	Un riesgo natural se puede definir como la probabilidad de que un territorio y la sociedad que habita en él, se vean afectados por episodios naturales de rango extraordinario. En otras palabras, la vulnerabilidad de una población o región a una amenaza o peligro natural.
SEGURIDAD Y SALUD EN EL TRABAJO	Son aquellos generados por la exposición a factores internos y externos que afectan el medio ambiente de la entidad (la contaminación, ambientes poco saludables, malos hábitos) inherentes a las actividades que desarrolla en cada proceso.
CONFLICTO DE INTERES	Cuando el servidor público o contratista actúan movidos por su interés particular en provecho propio, y no se declaran impedidos, este se convierte en un hecho de corrupción
FRAUDE INTERNO	Podemos encontrar distintos tipos de fraude interno en las empresas. Entre ellos destacan los siguientes: **Fraude documental:** Este fraude se produce cuando el empleado presenta una factura o un ticket que no cumple las condiciones para considerarse válido. **Fraude de tipo cronológico**: Se trata de un tipo de fraude interno en el que los, gastos presentados por el empleado a través de una nota de pago no se ajustan a los límites marcados por las políticas de viaje de la empresa. Es decir, que exceden la máxima cuantía autorizada. **Compra de artículos "no compliance":** En estos casos la infracción se comente cuando el empleado adquiere un producto sin autorización de la empresa. Puede ir desde un cargador de móvil hasta equipos de mayor valor económico. **Presentación del gasto fuera de plazo:** Se trata de un fraude porque el empleado presenta sus notas de gastos o facturas fuera del plazo establecido por la empresa. **Manipulación de capital social y patrimonio:** Generalmente es realizado por administradores de recursos y con abuso de cargos de confianza. **Fuga de información intencional:** Esta fuga puede ser sobre la tecnología usada por la compañía, sobre sus transacciones, servicios y productos, etc. **Apropiación Ilícita:** Puede ser de dinero, vienes o valores.

Fuente: Mapa de riesgos organizacionales – VIVA, elaboración propia.

11.5 Identificación del riesgo.

La identificación de los riesgos comprende el establecimiento de los siguientes aspectos fundamentales:

11.5.1 RIESGO:

Es la posibilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso, escriba de forma general el riesgo identificado.

- El riesgo identificado debe tener relación directa con las causas.
- Se recomienda que al momento de redactar los riesgos se utilicen palabras como: Inadecuado.., ausencia de.., Pérdida de.., Inexistencia de.., Deterioro de.., Desorganización.., Falta de.., Inoportunidad.., Inefectividad..., Desequilibrio..., Indebida...,

Desconocimiento de..., Incumplimiento de..., Carencia de..., desactualización de.., Deficiencias en..., Violación de.., Registro inoportuno de.., retraso en..., extemporaneidad en.., Desatención frente a.., Des financiación de... No realización de seguimiento a .., Inconsistencias en .., Volcamiento de.., Insuficiencias de..., Deserción de ..... entre otros.

- Es importante tener en cuenta que no todos los riesgos que puedan llegar a existir en el proceso, se deben plasmar en el mapa de riesgos, la escogencia o definición de estos riesgos, depende de lo que al interior del proceso se considere qué son los eventos (riesgos) MAS IMPORTANTES que de llegar a materializarse, podrían truncar, obstaculizar, retrasar o afectar de alguna manera, el cumplimiento de los objetivos del proceso y por ende los institucionales.

Para la identificación de los riesgos de corrupción se deben tener en cuenta algunas actividades susceptibles de riesgos de corrupción identificadas en la Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas del DAFP, principalmente:

11.5.2 Direccionamiento estratégico (alta dirección).

● Concentración de autoridad o exceso de poder.
● Extralimitación de funciones.
● Ausencia de canales de comunicación.
● Amiguismo y clientelismo.

11.5.3 Financiero (está relacionado con las Direcciones de Planeación y Administrativa y Financiera).

● Inclusión de gastos no autorizados.
● Inversiones de dineros públicos en entidades de dudosa solidez financiera, a cambio de beneficios indebidos para servidores públicos encargados de su administración.
● Inexistencia de registros auxiliares que permitan identificar y controlar los rubros de inversión.
● Inexistencia de archivos contables.
● Afectar rubros que no corresponden con el objeto del gasto en beneficio propio o a cambio de una retribución económica.

11.5.4 De contratación (proceso o bienes y servicios).

● Estudios previos o de factibilidad deficientes.
● Estudios previos o de factibilidad manipulados por personal interesado en el futuro proceso de contratación. (Estableciendo necesidades inexistentes o aspectos que benefician a una firma en particular).
● Disposiciones establecidas en los pliegos de condiciones que dirigen los procesos hacia un grupo en particular. (Ej. media geométrica).
● Visitas obligatorias establecidas en el pliego de condiciones que restringen la participación.
● Adendas que cambian condiciones generales del proceso para favorecer a grupos determinados.
● Urgencia manifiesta inexistente.

● Otorgar labores de supervisión a personal sin conocimiento para ello.
● Concentrar las labores de supervisión en poco personal.
● Contratar con compañías de papel que no cuentan con experiencia.

11.5.5 De información y documentación.

● Ausencia o debilidad de medidas o políticas de conflictos de interés.
● Concentración de información de determinadas actividades o procesos en una persona.
● Ausencia de sistemas de información.
● Ocultar la información considerada pública para los usuarios.
● Ausencia o debilidad de canales de comunicación
● Incumplimiento de la Ley 1712 de 2014.

11.5.6 De investigación y sanción.

● Ausencia o debilidad de canales de comunicación.
● Dilatar el proceso para lograr el vencimiento de términos o la prescripción del mismo.
● Desconocimiento de la ley, mediante interpretaciones subjetivas de las normas vigentes para evitar o postergar su aplicación.
● Exceder las facultades legales en los fallos.

11.5.7 De trámites o servicios internos y externos.

● Cobros asociados al trámite.
● Influencia de tramitadores
● Tráfico de influencias: (amiguismo, persona influyente).
● Demorar su realización. De reconocimiento de un derecho (expedición de licencias o permisos)
● Falta de procedimientos claros para el trámite.
● Imposibilitar el otorgamiento de una licencia o permiso.
● Ofrecer beneficios económicos para aligerar la expedición o para amañar la misma.
● Tráfico de influencias: (amiguismo, persona influyente). Los riesgos de seguridad digital se basan en la afectación de tres criterios en un activo o un grupo de activos dentro del proceso.

11.5.8 Descripción del riesgo.

Describa el riesgo identificado. Esta descripción se refiere a las características generales o las formas en que se observa o manifiesta el riesgo identificado.

11.5.9 Causas.

Son los medios, las circunstancias y/o agentes que generan o propician riesgos. Estas causas deben estar relacionadas con lo identificado en el contexto estratégico, es esencial que las causas tengan relación directa con el riesgo identificado.

Se puede combinar celdas para asociar varias causas a un factor interno o externo del contexto estratégico.

11.5.10 Impacto.

Son las consecuencias potenciales que genera el hecho que se llegue a materializar el riesgo; este impacto se da generalmente sobre las personas, bienes materiales e inmateriales, daños físicos, sanciones, investigaciones, pérdidas económicas, de información, de bienes, afectación de la imagen, de la credibilidad y de la confianza, interrupción de servicios, daños ambientales, entre otros.

Este ítem lo integran dos elementos:

11.5.11 Consecuencias potenciales:
En donde se describen de forma general, cual(es) son las consecuencias potenciales que generaría la materialización del riesgo.

11.5.12 Tipo
Relaciona cada una de la(s) consecuencia(s) potencial(es) generada(s) por la posible materialización del riesgo, con uno (1) de los cuatro (4) tipos de impacto posibles, que se presentan a continuación:

1. **Confidencialidad en la información**: El impacto de confidencialidad de la información se refiere a la pérdida o revelación de la misma. Cuando se habla de Información reservada institucional se hace alusión a aquella que por la razón de ser de la entidad solo puede ser conocida y difundida al interior de la misma; así mismo, la sensibilidad de la información depende de la importancia que esta tenga para el desarrollo de la misión de la entidad.

2. **Credibilidad o imagen**: El impacto de credibilidad se refiere a la pérdida de la misma frente a diferentes actores sociales o dentro de la entidad.

3. **Legal**: El impacto legal se relaciona con las consecuencias legales para una entidad, determinadas por los riesgos relacionados con el incumplimiento en su función administrativa, ejecución presupuestal y normatividad aplicable.

4. **Operativo**: El impacto operativo aplica en la mayoría de las entidades para los procesos clasificados como de apoyo, ya que sus riesgos pueden afectar el normal desarrollo de otros procesos.

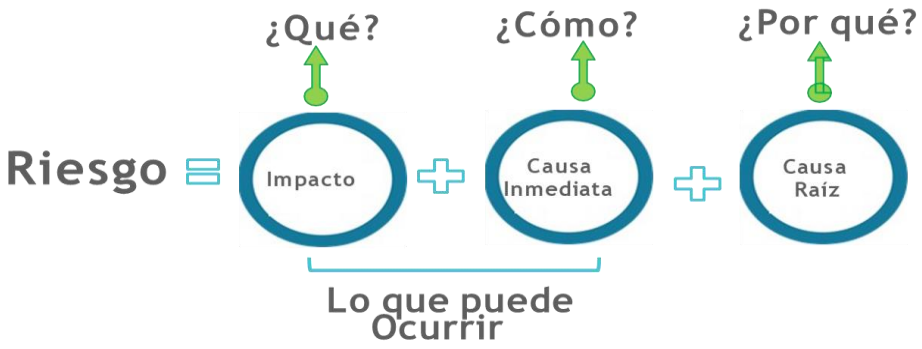
En la matriz **PLE-MT-12 Mapa de Riesgos** y en la **matriz PLE-MT-13**, para los riesgos de corrupción siga el Hipervínculo para conocer las características de cada uno de los cuatro (4) Tipos de impacto identificados en esta matriz y elija de la lista desplegable una de las opciones.

a. **Nivel:** Siga el Hipervínculo de matriz **PLE-MT-12 Mapa de Riesgos** y en la **matriz PLE-MT-13**, para los riesgos de corrupción y elija de la lista desplegable, uno (1) de

los cinco (5) niveles disponibles, teniendo en cuenta la descripción que se tiene para los impactos que se presentarían si el riesgo se llega a materializar.

1. INSIGNIFICANTE
2. MENOR
3. MODERADO
4. MAYOR
5. CATASTRÓFICO

Imagen 3: Clasificación de los riesgos.



Fuente: elaboración propia.

11.6 Análisis del riesgo inherente.

El Análisis del riesgo Inherente es el elemento de control que permite establecer la probabilidad de ocurrencia de los riesgos y el impacto de su materialización, calificándolos y evaluándolos a fin de determinar la capacidad de la entidad, para su aceptación y manejo.

Se denomina riesgo inherente ya que es el riesgo inicial al que se expone o enfrenta el proceso o la entidad, en ausencia de controles que permitan modificar su probabilidad e impacto.

Este ítem tiene los siguientes componentes:

11.6.1 Calificación del Riesgo

Se logra a través de la estimación de la probabilidad de su ocurrencia y del impacto que puede generar la materialización del riesgo.

11.6.2 Probabilidad

Es la medida para estimar la ocurrencia del riesgo y se mide con criterios de frecuencia, si se ha materializado cierto número de veces en un tiempo determinado) o de factibilidad; teniendo en cuenta la presencia de factores internos y externos, que pueden propiciar el riesgo, aunque este no se haya materializado.

Consulte el hipervínculo dispuesto en esta celda de la matriz **PLE-MT-12 Mapa de Riesgos** y en la **matriz PLE-MT-13** para los riesgos de corrupción, para conocer los criterios establecidos en relación con la probabilidad y luego seleccione de FORMA MANUAL una opción de la lista desplegable.

Imagen 4: Tabla de probabilidad

TABLA DE PROBABILIDAD			
NIVEL	DESCRIPTOR	DESCRIPCIÓN (FACTIBILIDAD)	FRECUENCIA
1	RARO	El evento puede ocurrir solo en circunstancias excepcionales	No se ha presentado en los últimos 5 años.
2	IMPROBABLE	El evento puede ocurrir en algún momento.	Al menos de 1 vez en los últimos 5 años.
3	POSIBLE	El evento podría ocurrir en algún momento.	Al menos de 1 vez en los últimos 2 años.
4	PROBABLE	El evento probablemente ocurrirá en la mayoría de las circunstancias.	Al menos de 1 vez en el último año.
5	CASI SEGURO	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.

Fuente: elaboración propia.

11.6.3 Impacto

Son las consecuencias que puede generar la materialización del riesgo, al proceso y por ende a la entidad.

La calificación del impacto del riesgo inherente se obtiene AUTOMÁTICAMENTE del promedio simple de las calificaciones de cada consecuencia potencial descrita en la identificación del riesgo, dado que esas consecuencias potenciales pueden ser de cuatro (4) tipos: Confidencialidad en la información, Credibilidad o imagen, Operativo y Legal, el impacto promediado que aquí se obtiene, se ubicará en una (1) de las siguientes cinco (5) categorías generales:

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. **CATASTRÓFICO**: Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

11.6.4 Evaluación del Riesgo

permite comparar los resultados de la calificación del riesgo, con los criterios definidos para establecer el grado de exposición de la entidad al mismo; de esta forma es posible distinguir entre los riesgos bajos, moderados, altos y extremos y poder fijar las prioridades de las medidas a tomar, requeridas para su manejo.

Imagen 5: Tabla de impacto

CONCEPTO	IMPACTO				
PROBABILIDAD	INSIGNIFICANTE (1)	MENOR (2)	MODERADO (3)	MAYOR (4)	CATASTRÓFICO (5)
RARO (1)	11	12	13	14	15
IMPROBABLE (2)	21	22	23	24	25
POSIBLE (3)	31	32	33	34	35
PROBABLE (4)	41	42	43	44	45
CASI SEGURO (5)	51	52	53	54	55

ZONA DE RIESGO BAJA
ZONA DE RIESGO MODERADA
ZONA DE RIESGO ALTA
ZONA DE RIESGO EXTREMA

Fuente: elaboración propia.

El mapa de calor permite visualizar los riesgos en las zonas definidas (bajo, moderado, alto y extremo) permitiendo identificar y priorizar los riesgos asociados a su gestión que requieren mayor atención, así como los que está dispuesta a aceptar (apetito del riesgo) en función del impacto de estos en la Entidad.

Frente a las zonas de riesgo se define el siguiente tratamiento:

- **Zona de riesgo Baja**: Asumir el riesgo.
- **Zona de riesgo Moderada**: Asumir el riesgo, reducir el riesgo.
- **Zona de riesgo Alta:** Reducir el riesgo, evitar, compartir o transferir.
- **Zona de riesgo Extrema:** Reducir el riesgo, evitar, compartir o transferir.

Los riesgos que se encuentren en zona baja se aceptan y se continúa el monitoreo. Los riesgos de corrupción no admiten la aceptación del riesgo, siempre deben conducir a un tratamiento.

Los riesgos que se encuentran en las zonas más altas o de mayor gravedad son los que se priorizan disminuyéndose para estos el nivel de aceptación, determinando en el plan de contingencia las actividades de control (correctivas) que ataquen las causas del riesgo, cuando éste se llegue a materializar.

Esto ayuda a la Entidad a mejorar su administración de riesgos, priorizando los esfuerzos y acciones sobre los riesgos potencialmente de mayor impacto.

Frente al análisis de probabilidad e impacto no se utiliza criterio experto, esto quiere decir que el líder del proceso, como conocedor de su quehacer, define cuántas veces desarrolla la actividad, esto para el nivel de probabilidad, y es a través de la tabla establecida que se ubica en el nivel correspondiente, dicha situación se repite para el impacto, ya que no se trata de un análisis subjetivo. Se debe señalar que el criterio experto, es decir el conocimiento y experticia del líder del proceso, se utiliza para definir aspectos como: número de veces que se ejecuta la actividad, cadena de valor del proceso, factores generadores y para la definición de los controles.

11.6.5 Zona de riesgo.

Representa la zona en la que se encuentra el riesgo, a la que se enfrenta inicialmente un proceso o la entidad, en ausencia de controles.

El resultado en esta casilla de la matriz **PLE-MT-12 Mapa de Riesgos** y en la **matriz PLE-MT-13**, para los riesgos de corrupción se da de forma automática. En la eventualidad que el riesgo inherente se ubique en la zona de riesgo BAJA, es importante que se revise al interior del proceso, ya que muy posiblemente este no sea un riesgo importante que amerite que se le aplique todo la gestión de la administración del riego.

11.6.6 Opciones de manejo del riesgo.

Las opciones de manejo del riesgo, representan las posibilidades que se tienen para administrar el riesgo, a través de controles, luego de determinar la probabilidad e impacto del riesgo inherente.

Diagrama 4: Opciones de manejo del riesgo

Opciones de manejo del riesgo		Zona de riesgo
Asumir el riesgo	Implica que se ACEPTAN las consecuencias o efectos de la materialización del riesgo; en este caso no es necesario tomar medidas para seguir disminuyendo la probabilidad e impacto del riesgo. Nota: Si el riesgo inherente se ubica en la zona baja, se debe revisar si éste riesgo amerita o no, que se incluya en el mapa de riesgos, para su administración.	Baja
Reducir el riesgo	Implica tomar medidas encaminadas a DISMINUIR tanto la PROBABILIDAD, como el IMPACTO. 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 mejora u optimización de los procedimientos, la implementación de acertados controles y acciones de manejo complementarias. Se implementan controles y sus acciones de manejo del riesgo orientadas a disminuir la probabilidad de materialización del riesgo Y/O controles y sus acciones de manejo del riesgo, orientadas a disminuir el impacto de la materialización del riesgo. Lo anterior con el propósito de llevar el riesgo a la zona baja.	Moderado
Evitar el riesgo	Implica tomar medidas encaminadas a PREVENIR que el riesgo se materialice, evitar la materialización del riesgo es la primera alternativa a considerar, y esto se logra cuando al interior del proceso se generan CAMBIOS SUSTANCIALES, tales como: mejoramiento a raíz de ajustes drásticos, rediseños o eliminaciones realizadas en procedimientos u otros controles establecidos. Por ejemplo: el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc. Se implementan controles y sus acciones de manejo del riesgo, orientadas a disminuir o evitar la materialización del riesgo Y/O controles y sus acciones de manejo del riesgo orientadas a disminuir o evitar el impacto de la materialización del riesgo. Lo anterior con el propósito de llevar el riesgo a zona moderada. En lo relacionado con compartir o transferir el riesgo, se podría establecer el mantenimiento de pólizas (contratos de seguros), tercerización, entre otras; como controles o acciones de manejo del riesgo enfocadas a la protección. Esta opción de manejo se deberá tener en cuenta, con base en la capacidad del proceso y/o la entidad, para asumir las consecuencias del impacto producido por la materialización del riesgo.	Alta

Compartir o transferir el riesgo	Implica tomar medidas que REDUZCAN EL IMPACTO de la materialización del riesgo, a través del COMPARTIR O TRASPASO de las pérdidas potenciales a otras organizaciones o entidades, como en el caso de los contratos de seguros (Pólizas) 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, tercerización (Outsourcing), 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. Se implementan controles y sus acciones de manejo del riesgo, orientadas a disminuir o evitar la materialización del riesgo Y/O controles y sus acciones de manejo del riesgo orientadas a disminuir o evitar el impacto de la materialización del riesgo. En lo relacionado con Compartir o transferir el riesgo, teniendo en cuenta que en esta zona de riesgo se pueden producir pérdidas considerables para el proceso y/o la entidad, se hace necesario que se implementen controles de protección y sus acciones de manejo del riesgo, en los cuales se involucren pólizas, tercerizaciones, entre otras medidas que protejan el proceso y/o la entidad.	Extrema

Fuente: Elaboración propia.

11.7 VALORACIÓN DEL RIESGO.

11.7.1 Identificación de controles.

En este ítem el proceso deberá tener en cuenta los siguientes elementos y de esta manera tener una adecuada gestión de los riesgos. Recuerde que los controles deben estar dirigidos a atacar las causas identificadas.

11.7.2 Tipos de control.

Revise la información del Hipervínculo de la matriz **PLE-MT-12 Mapa de Riesgos** y en la **matriz PLE-MT-13**, para los riesgos de corrupción donde encontrará ejemplos de controles operativos, de gestión y legales, con el propósito de clasificar el o los controles definidos para mitigar el o los riesgos identificados en el proceso.

11.7.3 Descripción del control.

Describe de forma clara y general cuales son los controles que actualmente realiza el proceso para mitigar el riesgo inherente, tenga en cuenta la información que se encuentra descrita en los tipos de control, seleccione uno o varios según sea pertinente.

11.7.4 Responsable del control.

En este componente mencione quien será el responsable (Nombre y cargo) del control de los riesgos dentro del proceso.

11.7.5 Periodicidad.

Seleccione de la lista de desplegable de la matriz **PLE-MT-12 Mapa de Riesgos** y en la **matriz PLE-MT-13** para los riesgos de corrupción la periodicidad para evaluar los controles establecidos.

Cada proceso deberá evaluar los controles en el **documento PLE-FO-18 Formato evaluación de controles riesgos asociados al proceso** seleccionando si cada control está dirigido a minimizar la probabilidad, el impacto o ambos y se envía firmado como soporte vía correo electrónico institucional al equipo de Gestión Organizacional, con un informe finalizando cada trimestre (marzo, junio, septiembre y diciembre) en el **formato GEO-FO-04 Informe de Gestión** o el instrumento **GEO-FO-02 Formato Acta,** describiendo la gestión y el control realizado por el proceso para reducir, asumir, evitar los diferentes riesgos asociados al proceso, se deberá entregar los soportes y evidencias de los controles implementados en la matriz **PLE-MT-12 Mapa de Riesgos** y en la **matriz PLE-MT-13**, para los riesgos de corrupción**.**

Los líderes de procesos son responsables como primera línea de defensa de garantizar la gestión adecuada para evitar la materialización de los riesgos.

11.8 Evaluación de controles.

La evaluación de los controles se define en la matriz **PLE-MT-12 Mapa de Riesgos** y en la **matriz PLE-MT-13** para los riesgos de corrupción con preguntas claves ya establecidas que le permiten a los procesos identificar si los controles establecidos apuntan a disminuir la probabilidad, el impacto o ambos.

Elija una (1) de las dos (2) opciones (probabilidad o impacto), de la lista desplegable, teniendo en cuenta si el control es preventivo o correctivo.

Dependiendo de lo que se elija (probabilidad o impacto), se realizará un desplazamiento del riesgo en la matriz de calificación y evaluación, la cual se reflejará en el análisis de riesgo residual.

De la siguiente manera se realiza el desplazamiento anteriormente mencionado, desplazamiento del riesgo en la matriz de calificación y evaluación, en relación con la probabilidad y el impacto que pasará a ser riesgo residual.

La evaluación del control, en relación con la efectividad del mismo, representa la autoevaluación que se hace al interior de cada proceso como primera línea de defensa para determinar si los controles que se tienen actualmente documentados y aplicados, si están sirviendo para contrarrestar la probabilidad de materialización del riesgo o el impacto de su materialización.

Será responsabilidad del proceso de Planeación Estratégica como segunda línea de defensa realizar el seguimiento preliminar a la eficacia de los controles en la periodicidad establecida por los diferentes procesos en la matriz **PLE-MT-12 Mapa de Riesgos** y en la **matriz PLE-MT-13** para los riesgos de corrupción y deberá notificar mediante informe de la eficacia de los controles establecidos por el proceso a la Oficina de Control Interno como tercera línea de defensa.

Cuando se requiera actualizar los riesgos asociados a los procesos, se deberá solicitar vía correo electrónico institucional al equipo de Gestión Organizacional a través del instrumento **PLE-FO-19 Formato solicitud actualización de riesgos**, en donde se especificará los cambios que se requieran y se deberán diligenciar todas las casillas en su totalidad.

11.8.1 Riesgo residual.

Es responsabilidad del proceso de Planeación Estratégica como segunda línea de defensa realizar la evaluación del riesgo residual. El riesgo residual, representa el riesgo que PERMANECE, después de evaluar los controles establecidos en el proceso para mitigar el riesgo inherente.

La periodicidad para evaluar el riesgo residual a los procesos se realizará semestralmente en los meses de junio y diciembre, se tendrán en cuenta los respectivos informes entregados por los procesos y los soportes de verificación que evidencien que el control fue efectivo para el tratamiento de las diferentes causas identificadas, en el riesgo inherente.

La Calificación del Riesgo se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede generar la materialización del riesgo.

11.8.2 Calificación del riesgo residual.

Si el promedio de la sumatoria de los puntajes (%) en la columna PUNTAJE FINAL de todos los controles preventivos que contrarrestan la PROBABILIDAD de materialización del riesgo se ubica en el rango (0-50), No se disminuyen casillas, si se ubica en el rango (51-75), se disminuye una (1) casilla, si se ubica en el rango (76-100), se disminuyen dos (2) casillas.

Si el promedio de la sumatoria de los puntajes (%) de todos los controles correctivos que contrarrestan el IMPACTO de la materialización del riesgo se ubica en el rango (0-50), No se disminuyen casillas, si se ubica en el rango (51-75), se disminuye una (1) casilla, si se ubica en el rango (76-100), se disminuyen dos (2) casillas.

11.8.3 Evaluación del riesgo residual.

La evaluación del Riesgo permite comparar los resultados de la calificación del riesgo, con los criterios definidos para establecer el grado de exposición de la entidad al mismo; de esta forma es posible distinguir entre los riesgos bajos, moderados, altos y extremos y poder fijar las prioridades de las medidas a tomar, requeridas para su manejo.

11.8.4 Zona de riesgos residual.

Representa la nueva zona de riesgo, después de evaluar los controles establecidos por los procesos para mitigar el riesgo inherente.

11.8.5 Opciones de manejo del riesgo residual.

Esta nueva opción de manejo del riesgo, representa las posibilidades que se tienen para administrar el riesgo residual, a través de acciones de manejo del riesgo.

Estas acciones de manejo del riesgo son las que se deben describir en la siguiente sección (MANEJO DEL RIESGO RESIDUAL).

11.9 Manejo del riesgo residual.

Representan acciones adicionales y diferentes a los controles existentes identificados y aplicados.

11.9.1 Descripción general de la acción.

Describa la acción a implementar, esta es la acción que se documentará en la matriz **PLE-MT-12 Mapa de Riesgos** y en la **matriz PLE-MT-13** para los riesgos de corrupción el proceso de Gestión Organizacional será el responsable de realizar el acompañamiento al proceso siguiendo los lineamientos establecidos en el procedimiento **GEO-PR-01 PROCEDIMIENTO ACCIONES CORRECTIVAS, PREVENTIVAS Y MEJORA,** y deberá ser garante que se realice el análisis de causa al riesgo en el **formato GEO-FO-05 Formato Análisis de causa, GEO-FO-08 Plan de mejoramiento Institucional.**

Nota: Debido a que estas acciones refuerzan o suplen la falta de establecimiento de controles en los procesos, se hace necesario, que una vez estas acciones se ejecuten se vuelva a realizar la evaluación de controles y así determinar nuevas zonas de riesgo.

11.10 Plan de contingencia.

El plan de contingencia describe las posibles acciones inmediatas a realizar SOLO cuando el riesgo se materialice, para corregir los efectos o consecuencias inmediatas de la materialización (correcciones) y las acciones correctivas para evitar su recurrencia.".
Nota: Es importante tener en cuenta, que las correcciones y acciones correctivas descritas en el plan de contingencia, solo se activan una vez el riesgo se materialice, situación DIFERENTE a los controles y a las acciones de manejo del riesgo residual; que operan sin que el riesgo se haya materializado.
De acuerdo a lo anterior, el hecho de que el riesgo de materialice, exhorta al responsable del proceso y a su grupo de trabajo, a que revisen las causas o identifiquen otras nuevas, a que revisen y evalúen nuevamente sus controles, que los modifiquen, rediseñen o eliminen y creen nuevos si es necesario, estas son ejemplos de acciones correctivas que se pueden dejar proyectadas en el plan de contingencia, las cuales se deberán informar al Comité Institucional de Gestión y Desempeño de VIVA, en donde se tomaran las decisiones pertinentes al caso y se

dejará acta como constancia de las decisiones tomadas.

11.11 Monitoreo y revisión.

El monitoreo y revisión tiene como propósito valorar la efectividad de los controles establecidos por la entidad, el nivel de ejecución de los planes de manejo o tratamiento de los riesgos que permiten asegurar los resultados de la gestión, así como detectar las desviaciones y tendencias para generar recomendaciones sobre el mejoramiento de los procesos, y determinar si existen cambios en el contexto interno o externo, incluyendo los cambios en los criterios de riesgo y en el propio riesgo.

11.12 Divulgación de la política de administración de riesgos.

La divulgación de la política de Administración de Riesgos estará bajo la responsabilidad de la Dirección de Planeación, con el acompañamiento de Comunicaciones y el proceso de Gestión Organizacional con el fin de asegurar la disponibilidad y consulta de todos los funcionarios de la Entidad, se publicará en la intranet, pagina web, vía correo electrónico y otros mecanismos que se disponga para que esté disponible para las partes interesadas y grupo de valor.

Se realizaran eventos de socialización y divulgación de la política de Administración de Riesgos, para complementar lo anterior se realizaran mesas de trabajo en las diferentes Direcciones y Jefaturas de la entidad.

11.13 Responsabilidad de los procesos.

El monitoreo y revisión de la gestión de riesgos, está alineada con la dimensión de “Control Interno”, del Modelo Integrado de Planeación y Gestión – MIPG, que se desarrolla con el MECI a través de un esquema de asignación de responsabilidades y roles, el cual se distribuye en diversos servidores de la entidad en el marco de las líneas de defensa así (Fuente: Manual MIPG).

11.13.1 LÍNEA ESTRATÉGICA

Define el marco general para la gestión del riesgo y el control, mediante el establecimiento de la política de administración del riesgo y está a cargo de la Junta Directiva y la Alta Dirección, siendo el máximo órgano en esta estructura a la que se le debe dar a conocer los riesgos estratégicos, los de mayor magnitud y planes de tratamiento de los mismos. La Junta Directiva estará encargada de velar por el adecuado funcionamiento de la política de Administración de Riesgos.

11.13.2 PRIMERA LÍNEA DE DEFENSA

La gestión operacional se encarga de: Desarrollar e implementar procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.

A cargo de los Directores, Jefaturas y líderes de los procesos, programas y proyectos de la entidad. Tiene como rol principal: diseñar, implementar y monitorearlos controles y gestionar de manera directa en el día a día los riesgos de la entidad.

Así mismo, orientar el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la entidad y emprender las acciones de mejoramiento para su logro.

De acuerdo a lo anterior, cada líder de proceso debe mantener la traza o documentación respectiva de todas las actividades realizadas que garanticen de forma razonable que dichos riesgos no se materializarán y por ende que los objetivos del proceso se cumplan.

11.13.3 SEGUNDA LÍNEA DE DEFENSA.

A cargo de la Dirección de Planeación.
Asegura que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende.

A cargo de los servidores que tienen responsabilidades directas en el monitoreo y evaluación de los controles y la gestión del riesgo: Jefes de planeación, supervisores e interventores de contratos o proyectos, coordinadores de otros sistemas de gestión de la entidad, comités de riesgos (donde existan), comités de contratación, entre otros.
El rol principal es monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo, así como, el aseguramiento sobre el diseño apropiado de los controles.

11.13.4 TERCERA LÍNEA DE DEFENSA.

A cargo de la Oficina de Control Interno.
El rol principal es proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del Sistema de Control Interno. El alcance de este aseguramiento, se realiza a través de la auditoría interna y de seguimiento y cubre todos los componentes del Sistema de Control Interno.

Adicionalmente, tiene como roles el liderazgo estratégico, enfoque hacia la prevención, evaluación de la gestión del riesgo, relación con entes externos de control y el de evaluación y seguimiento.

12. Anexos.

PLE-MT-12 Mapa de Riesgos.
PLE-MT-13 Matriz riesgos de corrupción
PLE-FO-17 Formato aplicación principios gestión de riesgos.
PLE-FO-18 Formato evaluación de controles riesgos asociados al proceso
PLE-FO-19 Formato solicitud actualización de riesgos
GEO-PR-01 Procedimiento acciones correctivas, preventivas y mejora
GEO-FO-02 Formato acta
GEO-FO-04 Informe de gestión

GEO-FO-05 Formato Análisis de causa
GEO-FO-08 Plan de mejoramiento Institucional.

13. Control de documento.

ELABORÓ	REVISÓ	APROBÓ
Gloria Estela Hernández Manrique - Líder Gestión Organizacional.	Alejandra Hoyos Correa – Dirección de Planeación Luis Fernando Quirós Henao - Dirección Jurídica Gustavo García Urán – Profesional Gestión Organizacional.	Junta Directiva Comité Institucional de Coordinación de Control Interno