EMPRESA DE VIVIENDA DE ANTIOQUIA – VIVA

POLÍTICA DE ADMINISTRACIÓN DE RIESGOS ORGANIZACIONALES.

2024

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 GENERAL.

Establecer de manera precisa y efectiva los lineamientos y criterios metodológicos destinados a la identificación, análisis, valoración, monitoreo y tratamiento de los riesgos que la entidad Vivienda de Antioquia - VIVA pueda enfrentar. Este enfoque abarca los procesos, planes y proyectos, resguardando el logro de los objetivos institucionales, el cual busca activamente la disminución de la materialización de riesgos, permitiendo una identificación más precisa de las oportunidades de mejora e innovación. Estas acciones están intrínsecamente orientadas a fortalecer la relación esencial entre el ciudadano y el Estado, reafirmando el compromiso de la entidad con la excelencia y la satisfacción de los grupos de valor.

2.1 Objetivos específicos.

- **Control Integral:** Supervisar de manera exhaustiva todo el proceso vinculado al manejo de riesgos, materializándolo a través del Mapa de Riesgos, con especial énfasis en la eficiencia del Sistema de Gestión.
- **Directrices Estratégicas:** Facilitar orientaciones concretas para la administración de riesgos inherentes a los procesos de la entidad. Esto busca contribuir de manera efectiva a la adecuada identificación, análisis, valoración (tanto de riesgos como de controles) y tratamiento de estos.
- **Integración Multidimensional:** Integrar de manera coherente el manejo de riesgos relacionados con la gestión, corrupción y seguridad de la información. Este enfoque global abarca los diversos procesos que conforman el Sistema de Gestión.
- **Responsabilidad y Roles Claros**: Establecer con precisión las responsabilidades de los líderes de los procesos en VIVA, así como definir de manera clara el papel de las diferentes áreas dentro de la entidad.
- **Cumplimiento Legal:** Asegurar el cumplimiento de los requisitos legales aplicables al manejo de riesgos de gestión, garantizando una operación acorde con el marco normativo vigente.
- **Probabilidad de Éxito Aumentada:** Incrementar significativamente la probabilidad de alcanzar los objetivos institucionales, proporcionando a la entidad un nivel de aseguramiento razonable respecto al logro de estos.
- **Aprendizaje Organizacional:** Fomentar el aprendizaje continuo y la flexibilidad organizacional, promoviendo la adaptabilidad y la capacidad de respuesta frente a cambios y desafíos.
- **Desarrollo Profesional y Conciencia de Riesgos:** Fortalecer el comportamiento tanto profesional como personal de los funcionarios de la Empresa de Vivienda VIVA. Esto se logrará mediante la generación de una profunda conciencia sobre el pensamiento basado en riesgos, impulsando una cultura organizacional comprometida con la gestión eficaz de riesgos.
- **Fomentar la innovación continua en la Gestión de Riesgos**: Impulsar una cultura organizacional innovadora para mejorar constantemente los procesos de administración de riesgos. Incorporar prácticas y tecnologías innovadoras para fortalecer la capacidad de anticipación a desafíos, adaptarse a cambios y mejorar la eficiencia en la gestión de riesgos, contribuyendo a la mejora continua de la política de riesgos institucionales de VIVA.

3. ALCANCE.

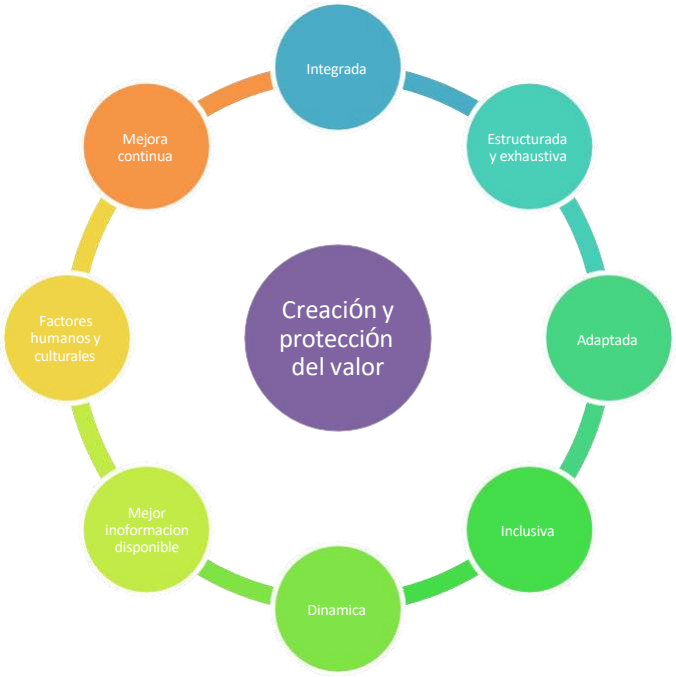
La presente Política abarca la gestión integral de riesgos, incluyendo aquellos relacionados con la corrupción, en todos los procesos de la entidad. Desde la definición de lineamientos hasta la evaluación y mejora continua, la política busca establecer un marco integral que fortalezca la resiliencia organizacional de VIVA, promoviendo prácticas éticas, eficiencia operativa y seguridad digital en todas sus dimensiones.

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: 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:

- **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. 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.

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 31073:2022 – Gestión del riesgo – vocabulario
- 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 calor:** Plano en el que se presentan simultáneamente las escalas de medición de impacto y de probabilidad, y que, como producto de su combinación, mediante colorimetría representa la importancia (nivel de severidad o criticidad) del riesgo.
- **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.
- **Riesgo de corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Riesgo de gestión**: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- **Riesgo de Seguridad de la Información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias (ISO/IEC 27000).
- **Riesgos de auditoria:** Se refiere tanto a los riesgos del proceso de auditoria para alcanzar sus objetivos, como al riesgo potencial de la auditoria para interferir con las actividades y

procesos del auditado (GTC ISO 19011)

- **Riesgo de tratamiento de datos personales:** Información personal que ha sido registrada, procesada y no ha sido salvaguardada por la entidad
- **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.
  (Fuente: NTC 31073:2022 – Gestión del riesgo – vocabulario).

7. ROLES Y RESPONSABILIDAD DE ACUERDO CON LAS LINEAS DE DEFENSA.

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 definición de nombres específicos de los colaboradores.

Línea de defensa	**Responsables**	**Roles y responsabilidad**
		a. Roles y responsabilidad
		1. Definir y aprobar el marco general para la gestión del riesgo. 2. Analizar los resultados de los riesgos, amenazas, vulnerabilidad y escenarios de pérdidas que puedan afectar el cumplimiento de los objetivos, planes, metas, compromiso y capacidad para prestar servicios.
		b. Actividades a realizar

Línea estratégica (Instancia decisoria)	Alta Dirección – Equipo Directivo	1. Aprobar y recomendar actualizaciones a la política de administración del riesgo. 2. Definir los niveles de aceptación del riesgo. 3. Establecer la periodicidad del monitoreo y seguimiento.
	Comité Institucional de Gestión y Desempeño. Comité Institucional de Coordinación de Control Interno.	1. Supervisar el cumplimiento de cada una de las etapas de la administración del riesgo. 2. Revisar los cambios en el Direccionamiento Estratégico y en el entorno y en como estos pueden generar nuevos riesgos o modificar los existentes. 3. Revisar los planes de acción establecidos en los riesgos materializados a fin de que se tomen medidas oportunas y eficaces para evitar su posible repetición. 4. Evaluar la forma como funciona el esquema de líneas de defensa. 5. Realizar la evaluación de la política de administración del riesgo, considerando su aplicación, cambios en el entorno, dificultades para su desarrollo y riesgos emergentes. 6. Realizar revisiones periódicas de los escenarios de riesgo, considerando variaciones en el entorno mediante el análisis de contexto interno y externo de la entidad, como lo son avances tecnológicos, cambios legislativos, condiciones económicas y otros factores relevantes. Ajustar el mapa de riesgos y las estrategias de mitigación según sea necesario.
		c. Comunicación y divulgación.
		1. Corresponde al Comité Institucional de Coordinación de Control Interno y al Comité Institucional de Gestión y Desempeño asegurarse de que la política de administración de riesgos se dé a conocer en todos los niveles de la entidad, que se conozca claramente los niveles de responsabilidad que posee cada una de las tres líneas de defensa frente a la gestión del riesgo.

		2. Buscar crear conciencia en todos los servidores de la entidad, sobre la importancia de la gestión preventiva y el autocontrol en la gestión de sus actividades. 3. Divulgar y socializar la política, metodología y mapa de riesgo incluyendo su publicación en la página web.
		d. Accionar frente a la materialización del riesgo
		1. Revisar los planes de acción definidos en los riesgos materializados, a fin de que se tomen medidas oportunas y eficaces para evitar la posible repetición del evento. 2. Si es riesgo materializado es de corrupción realizar la denuncia ante las instancias de control correspondiente. 3. Ante la materialización de riesgos de gestión, continuidad del negocio, seguridad digital proceder de manera inmediata a aplicar el plan de contingencia que permita el restablecimiento del servicio.
Primera línea de defensa	Lideres de proceso	Esta línea está bajo la responsabilidad, principalmente, de los líderes de programas, procesos y proyectos y de sus equipos de trabajo (en general servidores públicos en todos los niveles de la entidad); su rol principal es el mantenimiento efectivo de controles internos, la ejecución de gestión de riesgos y controles en el día a día. Para ello, identifica, evalúa, controla y mitiga los riesgos a través del “Autocontrol”. Los aspectos clave para el Sistema de Control Interno SCI para tener en cuenta por parte de la 1ª Línea: 1. El conocimiento y apropiación de las políticas, procedimientos, manuales, protocolos y otras herramientas que permitan tomar acciones para el autocontrol en sus puestos de trabajo. 2. La identificación de riesgos y el establecimiento de controles, así como su seguimiento, acorde con el diseño de dichos controles, evitando la materialización de los riesgos. 3. El seguimiento a los indicadores de gestión de los procesos e institucionales, según corresponda.

		4. La formulación de planes de mejoramiento, su aplicación y seguimiento para resolver los hallazgos presentados. 5. La coordinación con sus equipos de trabajo, de las acciones establecidas en la planeación institucional a fin de contar con información clave para el seguimiento o autoevaluación aplicada por parte de la 2ª línea de defensa. 6. Identificar, analizar y valorar los riesgos que pueden afectar el cumplimiento de los objetivos y actualizarlos cuando sea requerido. 7. Definir y aplicar los controles establecidos para mitigar los riesgos identificados, alinearlos con los objetivos institucionales y proponer mejoras a la gestión del riesgo en los procesos. 8. Supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión de los procesos, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar. 9. Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles. 10. Reportar los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado. 11. Revisar que las actividades de control de los procesos se encuentren documentadas y actualizadas en los procedimientos. 12. Revisar el cumplimiento de los objetivos de los procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando. 13. Revisar los eventos de riesgos que se han materializado, incluyendo los riesgos de corrupción, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos.

		14. Revisar los planes de contingencia establecidos para los riesgos materializados, con el fin de tomar medidas oportunas y eficaces para evitar en lo posible la repetición del evento. 15. Revisar y hacer seguimiento al cumplimiento de las actividades y planes de tratamiento con relación a la gestión de riesgos. 16. Reportar a la segunda línea de defensa el resultado de la gestión de riesgos del proceso, para su inclusión en la Matriz de Riesgos Institucionales e incluidos los riesgos de corrupción. 17. Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos generan nuevos riesgos o modifican los identificados en cada uno de los procesos, para la actualización de la Matriz de Riesgos.
Segunda línea de defensa	Dirección de Planeación a través del proceso Gestión Organizacional	1. Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, valoración y evaluación del riesgo. 2. Supervisar en coordinación con los demás responsables de la segunda línea de defensa que se hayan establecido en otras instancias, que la primera línea identifique, analice, valore, evalúe y realice el tratamiento de los riesgos, que se adopten los controles para la mitigación de los riesgos identificados y se apliquen las acciones pertinentes para reducir la probabilidad o impacto de los riesgos. 3. Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos. 4. Evaluar que la gestión de los riesgos este acorde con la presente política de la entidad y que sean monitoreados por la primera línea de defensa. 5. Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados.

		6. Actualizar, según se requiera, los escenarios de riesgo y la documentación asociada bajo su responsabilidad. 7. Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos generan nuevos riesgos o modifican los identificados en cada uno de los procesos, para la actualización de la Matriz de Riesgos. Los aspectos clave para el Sistema de Control Interno SCI a tener en cuenta por parte de la 2ª Línea son: • Aseguramiento de 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. • Consolidación y análisis de información sobre temas claves para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos. • Realizar el seguimiento al mapa de riesgos de su proceso. • Proponer las acciones de mejora a que haya lugar posterior al análisis, valoración, evaluación o tratamiento del riesgo. • Actualizar, según se requiera, los escenarios de riesgo y la documentación asociada a su responsabilidad. • Supervisar la implementación de las acciones de mejora o la adopción de buenas prácticas de gestión del riesgo asociado a su responsabilidad. • Comunicar al equipo de trabajo a su cargo la responsabilidad y resultados de la gestión del riesgo. • Trabajo coordinado con las oficinas de control interno o quien haga sus veces, en el fortalecimiento del Sistema de Control Interno.

		• Establecimiento de los mecanismos para la autoevaluación requerida (auditoría interna a sistemas de gestión, seguimientos a través de herramientas objetivas, informes con información de contraste que genere acciones para la mejora).
Tercera línea de defensa	Dirección de Control Interno	1. Dar orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Dirección de Planeación. 2. Monitoreo a la exposición de la entidad al riesgo y realizar recomendaciones con alcance preventivo. 3. Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos. 4. Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa. 5. Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos (gestión, corrupción y seguridad digital) de conformidad con el Plan Anual de Auditoria y reportar los resultados

		al Comité Institucional de Coordinación de Control Interno. 6. Recomendar mejoras a la política de administración del riesgo. 7. Revisión de la definición y alineación de los objetivos de los procesos con los objetivos institucionales, sobre los cuales se identificaron los riesgos y realizar las recomendaciones a que haya lugar. 8. Revisar que se hayan identificado los riesgos que afecten directamente el cumplimiento de los objetivos de los procesos y que se hayan incluido los riesgos de corrupción. 9. Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos. 10. Revisar el perfil de riesgo inherente y residual por cada proceso consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas. 11. Para mitigar los riesgos de los procesos, revisar que se encuentren documentados y actualizados los procedimientos y planes de mejora establecidos como resultado de las auditorías efectuadas, además, que se lleven a cabo de manera oportuna, se establezcan las causas raíz del problema y se evite, en lo posible, la repetición de hallazgos y la materialización de los riesgos. 12. Capacitación continua en temas relacionados con la gestión de riesgos, con el fin de fortalecer el rol de evaluador independiente.

8. MANIFIESTO 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, monitoreo 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".

9. 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 entidad 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.
- Optimización de Recursos Financieros.
- Al tener riesgos identificados, tratados y bajo seguimiento, se podría lograr una evaluación más favorable al asegurar la entidad.

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.

Gráfica: Conocimiento y análisis de entidad.

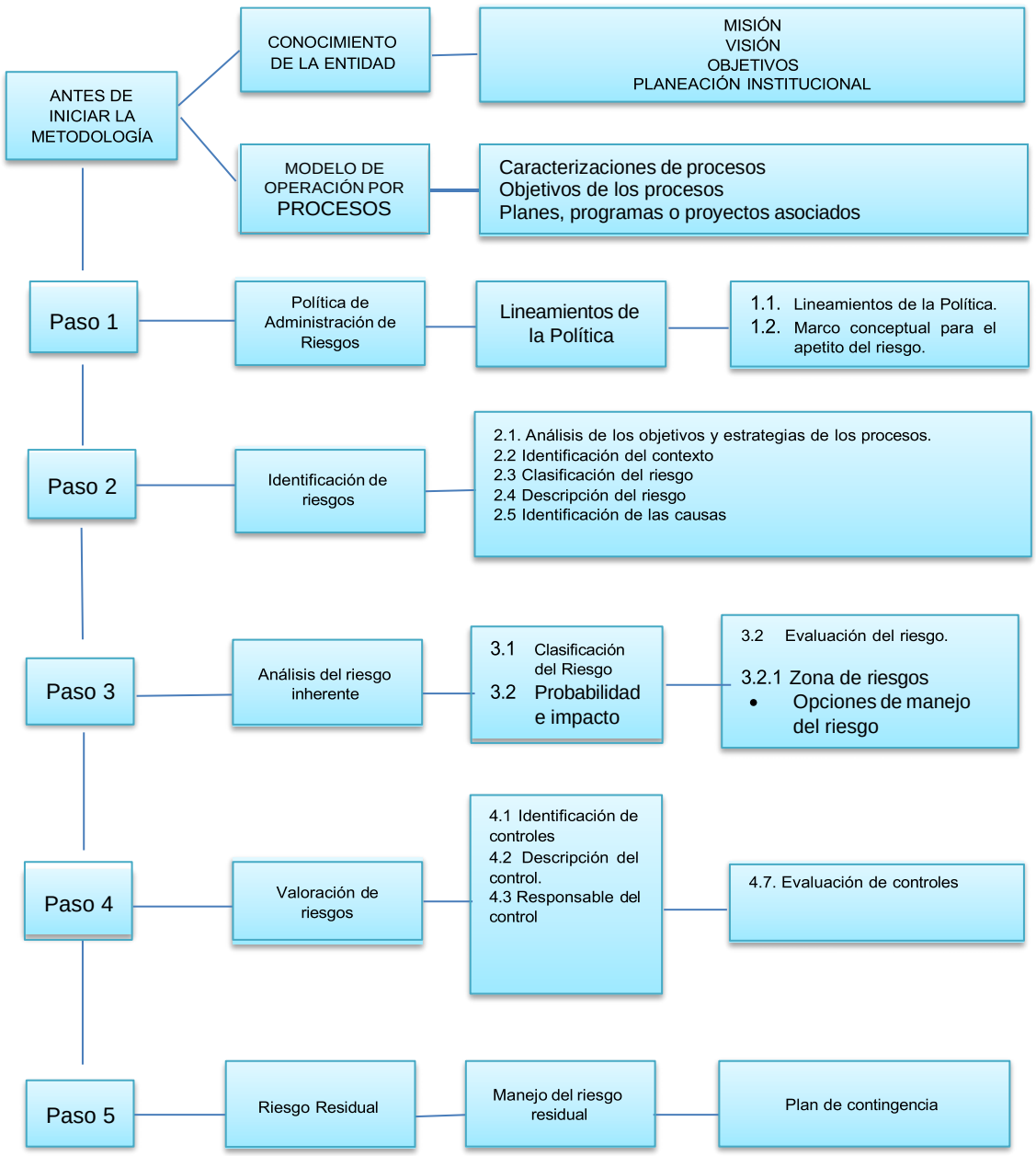
Fuente: construcción propia a partir de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, DAFP - 2022

10. 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 cinco (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: Metodología para la administración y gestión de riesgos.



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, DAFP – 2022

10.1 Determinación de la capacidad de riesgo.

Se 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 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”.

10.2 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.

10.3 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.

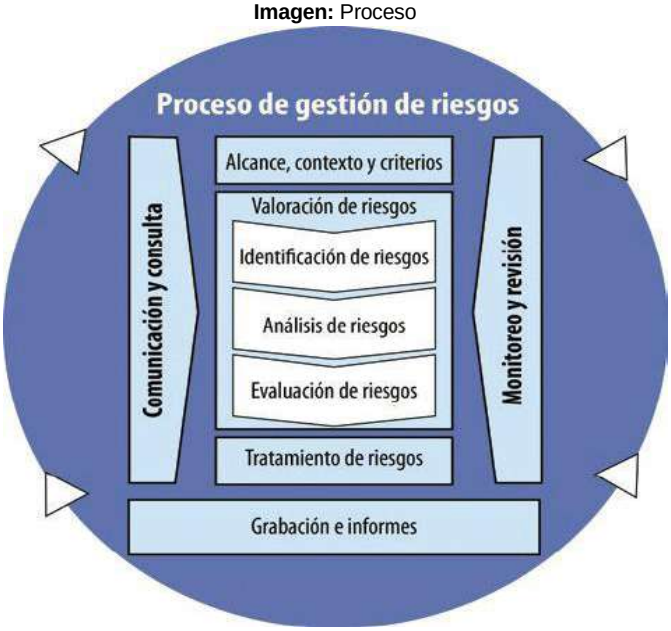
11. ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO.

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: 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 el Modelo de Gestión Organizacional, 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 reputacional, 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 Gestión Organizacional 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 las matrices **Mapa de Riesgos** que se tienen definidas en el Modelo de Gestión Organizacional.

Diagrama: DOFA

	FORTALEZAS	**DEBILIDADES**
ANALISIS DOFA	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 el **Mapa de Riesgos** y seleccione una de las opciones que se le presentan, caso de identificar otra opción solicite al Proceso de Gestión Organizacional la inclusión de este con su respectiva justificación.

Imagen: 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.	
Reputacionales: Cualquier evento o circunstancia externa que podría dañar la reputación de una organización pública. Esto puede incluir la percepción pública negativa, críticas de los medios de comunicación, protestas sociales, fallas en el cumplimiento de normas éticas, y cualquier otro evento que pueda afectar cómo la entidad es vista por el público, partes interesadas, y otros organismos.	

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 Mapa de Riesgos, para** conocer las características de los riesgos: Fallas tecnológicas, relaciones laborales, usuarios, productos y prácticas, daños a activos fijos/eventos externos; y seleccione solo una clasificación de la lista desplegable, por cada uno de los riesgos identificados.

Imagen: Clasificación de los riesgos.

CLASIFICACIÓN DEL RIESGO (Muestra las clases de riesgos que se pueden presentar)	
EJECUCIÓN Y ADMINISTRACIÓN DE PROCESOS	Pérdidas derivadas de errores en la ejecución y administración de procesos
FRAUDE EXTERNO	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
FRAUDE INTERNO	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos, abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
FALLAS TECNOLÓGICAS	Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos.
RELACIONES LABORALES	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
USUARIOS, PRODUCTOS Y PRÁCTICAS	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
DAÑOS A ACTIVOS FIJOS/EVENTOS EXTERNOS	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

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 Descripción del riesgo:

Consolida o resume los análisis sobre riesgo+ causa inmediata + causa raíz, permitiendo contar con una redacción clara y concreta del riesgo identificado. Tenga en cuenta la estructura de alto nivel establecida en la guía, inicia con POSIBILIDAD DE + Impacto para la entidad (Qué) + Causa Inmediata (Cómo) + Causa Raíz (Por qué).

- 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:

- **Direccionamiento estratégico (alta dirección).**
  - Concentración de autoridad o exceso de poder.
  - Extralimitación de funciones.
  - Ausencia de canales de comunicación.
  - Amiguismo y clientelismo.

- **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.

- **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.

- **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.

- **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.

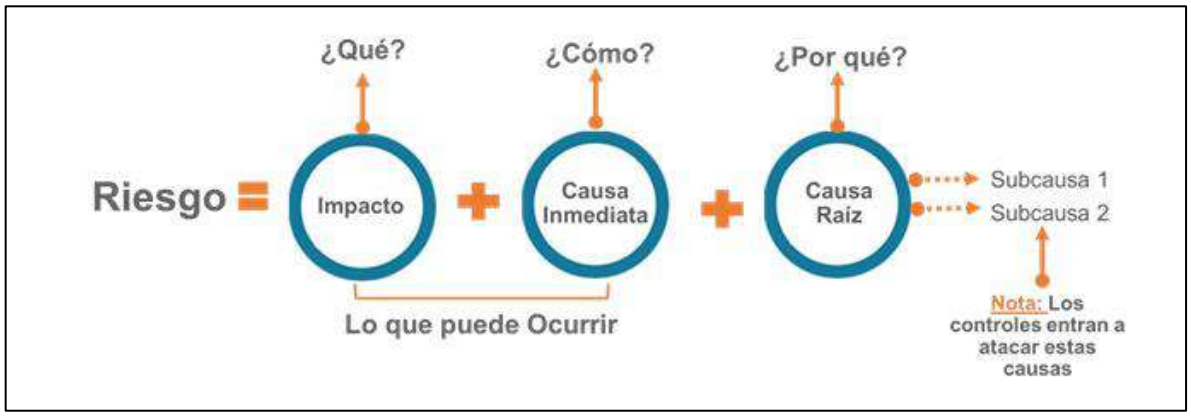
- **De trámites o servicios internos y externos.**
- Cobros asociados al trámite.
- Influencia de tramitadores
- Tráfico de influencias: (amiguismo, persona influyente).
- Demorar su realización. De reconocimiento de un derecho (expedición de licencias o permisos)
- Falta de procedimientos claros para 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.

11.5.2 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, para esto debes establecer:

- **Causa inmediata**: Circunstancias bajo las cuales se presenta el riesgo, es la situación más evidente frente al riesgo, redacte de la forma más concreta posible.
- **Causa raíz**: Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo, redacte de la forma más concreta posible.

Imagen: Clasificación de los riesgos.



Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6

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.
En este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto.

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.

Se entiende como la posibilidad de ocurrencia del riesgo. Para efectos de este análisis, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo**, la probabilidad inherente será el número de veces que se**

pasa por el punto de riesgo en el periodo de 1 año.

Bajo este esquema, la subjetividad que usualmente afecta este tipo de análisis se elimina, ya que se puede determinar con claridad la frecuencia con la que se lleva a cabo una actividad, en vez de considerar los posibles eventos que pudiesen haberse dado en el pasado.

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

Imagen: Tabla de probabilidad

TABLA DE PROBABILIDAD		
NIVEL	**FRECUENCIA DE LA ACTIVIDAD**	**PROBABILIDAD**
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año.	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año.	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año.	100%

Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6

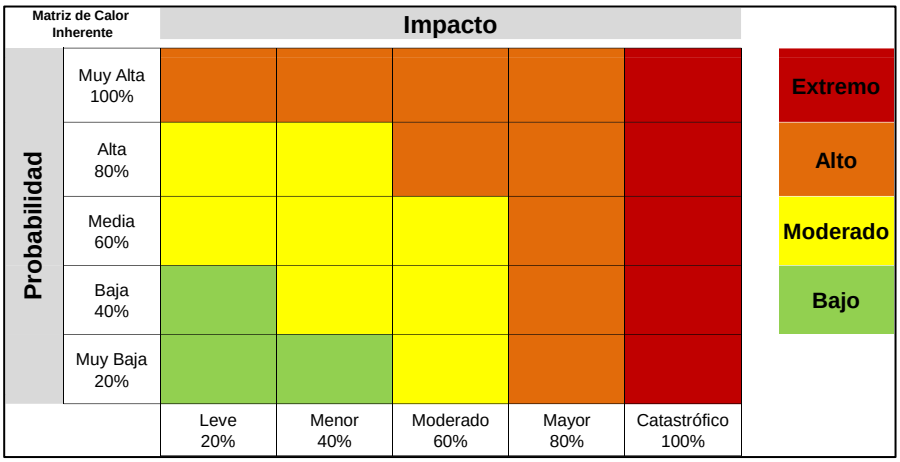
11.6.3 Impacto.

Son las consecuencias que puede generar la materialización del riesgo, al proceso y por ende a la entidad.
Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales. Cabe señalar que en la versión 2018 de la Guía de administración del riesgo se contemplaban afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal; así como afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio, todos estos temas se agrupan en impacto económico y reputacional en la versión 2020.

11.6.4 Evaluación del Riesgo.

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

Imagen: Tabla de impacto



Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6

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 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 inherente.

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 **Mapa de Riesgos** 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 toda 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: Opciones de manejo del riesgo

TIPO DE RIESGO	ZONA DE RIESGO	NIVEL DE ACEPTACIÓN
RIESGOS DE GESTIÓN	BAJA	Se ASUMIRÁ el riesgo y se administra por medio de las actividades propias del proyecto o proceso asociado y se realiza en el reporte mensual de su desempeño.
	MODERADA	Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo, se hace seguimiento y se registra sus avances.
	ALTA-EXTREMA	Se establecen acciones de Control Preventivas y/o correctivas que permitan MITIGAR la materialización del riesgo. Se monitorea y se registra.
RIESGOS DE CORRUPCIÓN	BAJA	Ningún riesgo de corrupción podrá ser aceptado. Realizar seguimiento para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos.
	MODERADA	Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo. Realizar seguimiento para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos y se registra su avance.
	ALTA-EXTREMA	Se adoptan medidas para: REDUCIR la probabilidad o el impacto del riesgo,o ambos; por lo general conlleva a la implementación de controles. EVITAR Se abandonan las actividades que dan ugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo. TRANSFERIR O COMPARTIR una parte del riesgo para reducir la probabilidad o el impacto del mismo. Realizar seguimiento para evitar a toda costa su materialización por parte de los procesos a cargode los mismos y se registra su avance.

Fuente: Elaboración propia.

11.7 Valoración del riesgo.

11.7.1 Identificación de controles.

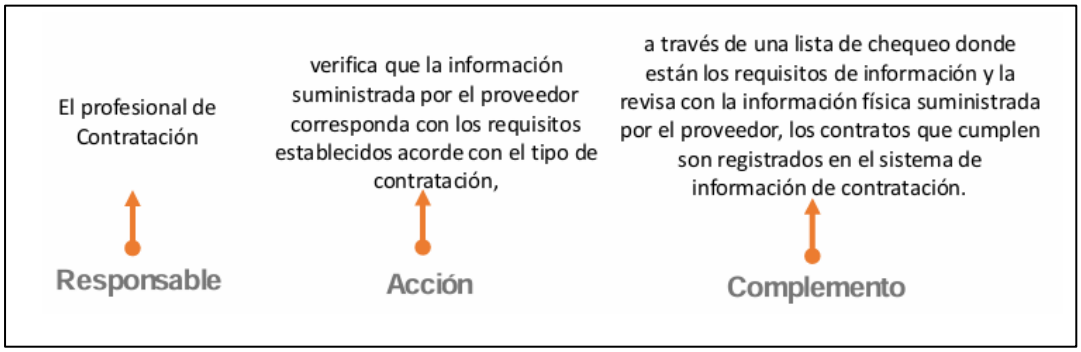
En este ítem el proceso deberá tener en cuenta los siguientes elementos y de esta manera tener una adecuada gestión de los riesgos. Recuerde que los controles deben estar dirigidos a atacar las causas identificadas.

11.7.2 Descripción del control.

Describe de forma clara y general cuales son los controles que actualmente realiza el proceso para mitigar el riesgo inherente, seleccione uno o varios según sea pertinente, todos los controles que se establezcan se tienen que evidenciar cuando se monitoree su cumplimiento.

Cada proceso deberá diligenciar la forma en que evalúa sus controles en el documento **Formato evaluación de controles riesgos asociados al proceso** seleccionando si cada control está dirigido a minimizar la probabilidad, el impacto o ambos, una única vez en cada vigencia, dado el caso de identificar o tener cambio en alguno de los riesgos se diligenciará nuevamente. A su vez, en el informe finalizando cada trimestre (marzo, junio, septiembre y diciembre) en el formato **Seguimiento al desempeño de los procesos,** deberá describir la gestión y el control realizado por el proceso para reducir, asumir, evitar los diferentes riesgos asociados al proceso, y el proceso deberá contar con los soportes y evidencias de los controles implementados en la matriz **Mapa de Riesgos,** los cuales reposarán en sus archivos de gestión**,** también es su responsabilidad evaluar la pertinencia de la eficacia del control y en caso de considerar que se deben actualizar se solicita a Gestión Organizacional el respectivo ajuste.

Imagen: Estructura control del riesgo



Fuente: Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6

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

11.7.3 Responsable del control.

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

11.8 Evaluación de controles.

Es responsabilidad del proceso de Gestión Organizacional como segunda línea de defensa evaluar la eficacia de los controles establecidos una vez en la vigencia, y realizar seguimiento a través de lo informes trimestrales en el formato **Seguimiento al desempeño de los procesos.**

La evaluación de los controles se define en la matriz **Mapa de Riesgos** 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.

La evaluación del control, en relación con la efectividad de este, 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.

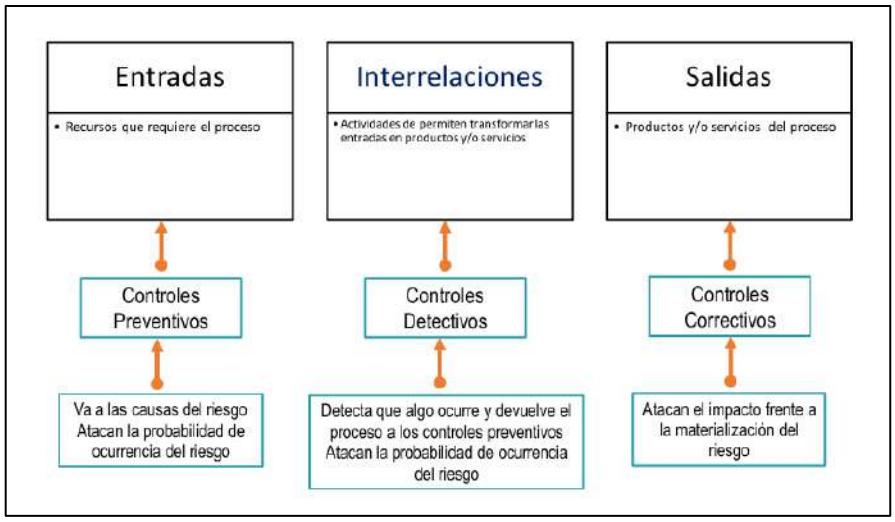
Será responsabilidad de la dirección de Planeación a través del proceso Gestión Organizacional como segunda línea de defensa realizar el seguimiento preliminar a la eficacia de los controles en la periodicidad establecida por los diferentes procesos en la matriz **Mapa de Riesgos.**

Cuando se requiera actualizar los riesgos asociados a los procesos, se deberá solicitar al proceso de Gestión Organizacional a través de correo electrónico o en los espacios de seguimiento, en donde se especificará los cambios que se requieran.

11.8.1 Tipología de Controles.

A través del ciclo de los procesos es posible establecer cuándo se activa un control y, por lo tanto, establecer su tipología con mayor precisión. Para comprender esta estructura conceptual, en la figura siguiente se consideran 3 fases globales del ciclo de un proceso así:

Imagen: Ciclo del proceso y las tipologías de controles



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

Acorde con lo mencionado anteriormente:

- **Control preventivo**: control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.

- **Control Detectivo**: control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.

- **Control correctivo:** control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos.

Así mismo, de acuerdo con la forma como se ejecutan tenemos:

- **Control manual:** controles que son ejecutados por personas.

- **Control automático:** son ejecutados por un sistema.

Se analizan los atributos para el diseño de controles, teniendo en cuenta características relacionadas con la eficiencia y la formalización. En la siguiente tabla se puede observar la descripción y peso asociados a cada uno así:

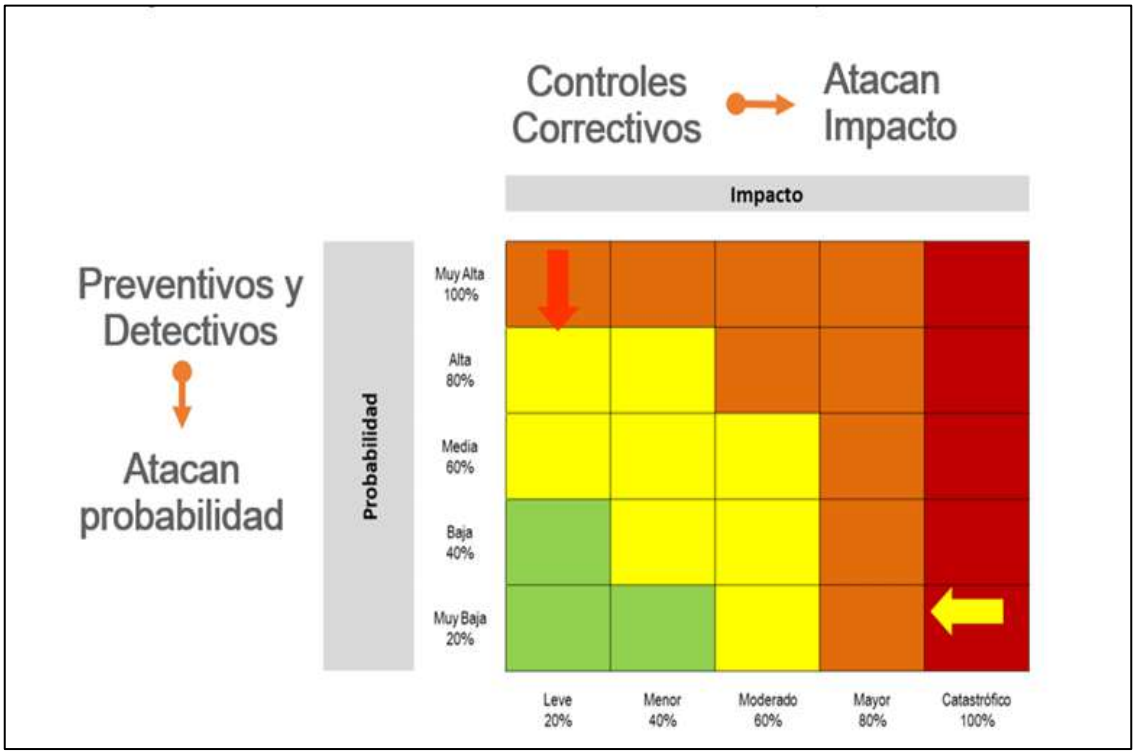
Imagen: Ciclo del proceso y las tipologías de controles

Tabla Atributos de para el diseño del control				
Características			**Descripción**	**Peso**
Atributos de Eficiencia	**Tipo**	**Preventivo**	Va hacia las causas del riesgo, aseguran el resultado final esperado.	**25%**
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	**15%**
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	**10%**
	Implementación	**Automático**	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	**25%**
		Manual	Controles que son ejecutados por una persona., tiene implícito el error humano.	**15%**
***Atributos de Formalización**	**Documentación**	**Documentado**	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin Documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso	-
	Frecuencia	**Continua**	Este atributo identifica a los controles que se ejecutan siempre que se realiza la actividad originadora del riesgo.	-
		Aleatoria	Este atributo identifica a los controles que no siempre se ejecutan cuando se realiza la actividad originadora del riesgo	-
	Evidencia	**Con Registro**	El control deja un registro que permite evidenciar la ejecución del control	-
		Sin Registro	El control no deja registro de la ejecución del control	-
***Nota 1:** Los atributos de formalización se recogerán de manera informativa, con el fin de conocer el entorno del control y complementar el análisis con elementos cualitativos; éstos no tienen una incidencia directa en su efectividad.				

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

Teniendo en cuenta que es a partir de los controles que se dará el movimiento, en la matriz de calor que corresponde a la figura siguiente, se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

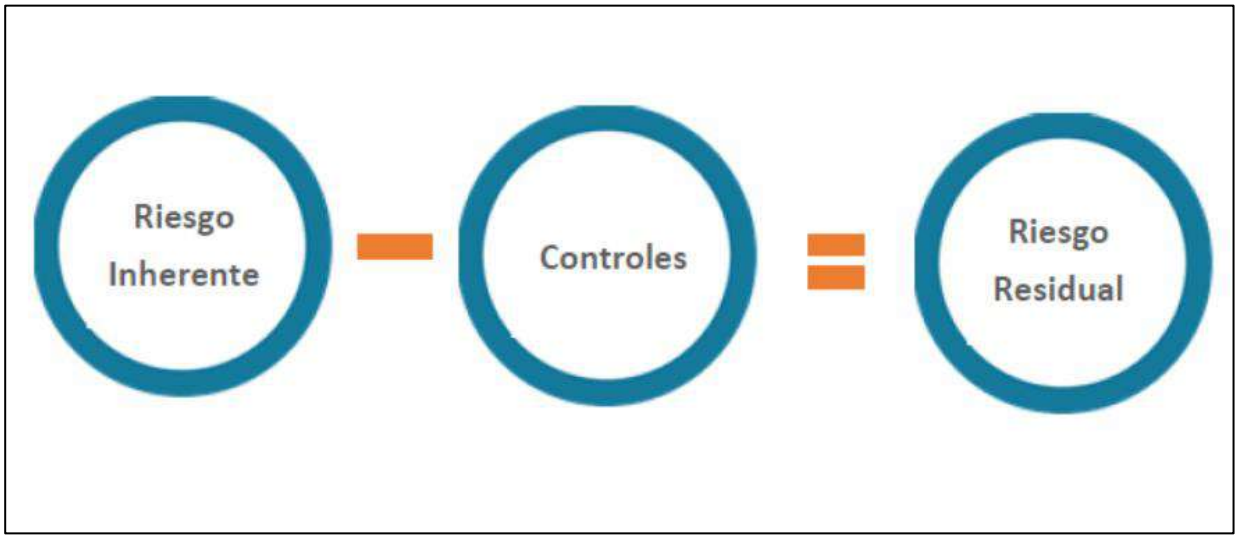
Imagen: Movimiento en la matriz de calor acorde con el tipo de control



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

11.8.2 Riesgo residual.

Imagen: Riesgo residual



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

El riesgo residual, representa el riesgo que PERMANECE, después de evaluar los controles establecidos en el proceso para mitigar el riesgo inherente.

Es responsabilidad del proceso de Gestión Organizacional como segunda línea de defensa realizar la evaluación del riesgo residual, previa validación de le efectividad de los controles.

La periodicidad para evaluar el riesgo residual a los procesos se realizará anualmente en el mes de enero y 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.

Cuando se identifique la materialización de un riesgo se deberá evaluar el riesgo residual y establecer el plan de mejoramiento para evitar repeticiones de la acción.

El proceso de Gestión Organizacional presenta al Comité Institucional de Gestión y Desempeño Interno los resultados de la evaluación del riesgo residual y el comportamiento de estos durante la vigencia, a través del informe de revisión por la alta dirección.

11.8.3 Calificación del riesgo residual.

R. Residual = R. Inherente – (R.I. * Control)

Para la aplicación de los controles se debe tener en cuenta que los estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

Opera una política de reducción máxima del 50% para los controles La metodología acumulativa busca reducir los niveles de probabilidad e impacto residual, teniendo en cuenta la eficiencia del control.

11.8.4 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.

11.8.5 Zona de riesgos residual.

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

11.8.6 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 las acciones tomadas por los procesos una vez se evalúa el riesgo residual

11.9.1 Descripción general de la acción.

Describa la acción a implementar, esta es la acción que se documentará en la matriz **Mapa de Riesgos,** el proceso será el responsable definir si luego de la evaluación del riesgo residual continúa o modifica tanto sus riesgos como sus controles, dependiendo la relevancia que estos tengan en su gestión.

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 con lo anterior, el hecho de que el riesgo se 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, las acciones correctivas que se dejen proyectadas en el plan de mejoramiento.

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 del Proceso de Gestión Organizacional, con el acompañamiento de Comunicaciones con el fin de asegurar la disponibilidad y consulta de todos los funcionarios de la Entidad, se publicará en la intranet y pagina web para que esté disponible para las partes interesadas y grupo de valor

11.13 Responsabilidad de los procesos.

El monitoreo y revisión de la gestión de riesgos, está alineada con la dimensión 7 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 (Fuente: Manual MIPG).

12. Anexos.

Mapa de Riesgos.
Formato aplicación principios gestión de riesgos.
Formato evaluación de controles riesgos asociados al proceso
Procedimiento acciones correctivas, preventivas y mejora
Informes procesos
Formato Análisis de causa
Plan de mejoramiento Institucional.

13. Control de documentos

ELABORÓ	REVISÓ	APROBÓ
Stefanía Acevedo Carvajal Tecnóloga de Apoyo Gestión Organizacional.	Tatiana Andrea Maya Gutiérrez Profesional Universitaria Gestión Organizacional	Susana Andrea Gómez Zapata Coordinadora Gestión Organizacional Junta Directiva – Acta junio 2023 Comité Institucional de Gestión y Desempeño