POLÍTICA INSTITUCIONAL DE ADMINISTRACIÓN DEL RIESGO

Versión 2.0.
Febrero 2022

CIÉNAGA AVANZA
De la Mano con el Pueblo

INTRODUCCIÓN

El concepto de Administración del Riesgo se introduce en las entidades públicas debido a que todas las organizaciones, independientemente de su naturaleza, tamaño y objeto misional están expuestas a diversos eventos que pueden poner en peligro su existencia, metas, objetivos y hasta la oportunidad y eficacia de los servicios y bienes que ofrece.

Desde el enfoque de la Norma Técnica **NTC-ISO 31000** e **ISO 9001 - 2015** se considera que los sistemas de gestión se deben trabajar con un enfoque basado en riesgos que permita identificarlos y actuar con suficiente anticipación para evitar que sucedan o aminorar sus efectos. La administración de riesgos es la base para la planificación que debe contribuir al logro de los objetivos institucionales; además, permite identificar, analizar y abordar los hechos que se presenten para adoptar estrategias o actividades que garanticen cumplir con la misión, la visión y la entrega de bienes y servicios con calidad por parte de la entidad. **Administrar riesgos es anticiparse a las dificultades, deficiencias o adversidades** internas o externas que pueden impedir que logremos nuestros propósitos, o que no cumplamos nuestras responsabilidades.

Con el propósito de contar con una política de administración de riesgos para la gestión de riesgos de gestión y de corrupción actualizada con los últimos lineamientos y metodologías, a través de este documento la Alcaldía de Ciénaga, estandariza las herramientas y la metodología general y adiciona la de gestión de **riesgos residuales** haciendo más sencillo el uso de las herramientas que diseñamos para esos propósitos, además de evitar discrepancias o duplicidades en la gestión de riesgos en nuestros procesos.

Esta política está articulada con las orientaciones de las Norma ISO 31000 (Gestión de Riesgos), 27001 (Gestión en la seguridad de la información), y los de la Función Pública colombiana, tanto en aceptación de los riesgos, como en actividades asociadas al tratamiento de los mismos y el diseño de controles; y, en especial, con la versión 5.0 de la Guía para la Implementación del Riesgo y el Diseño de Controles en Entidades Públicas de diciembre del 2020.

En la Alcaldía de Ciénaga la administración del riesgo es direccionada por la Oficina Asesora de Planeación y por el Comité Institucional de Gestión y Desempeño, y ejecutada por los responsables de los quince (15) procesos institucionales con los que cuenta la entidad.

Para el éxito de esta política es indispensable la participación y compromiso de todos los funcionarios y colaboradores de la alcaldía, de tal forma que todos cumplan los lineamientos de este documento para la identificación, análisis, valoración y tratamiento de los riesgos que puedan afectar la misión y el cumplimiento de los objetivos institucionales, mediante:

- La identificación de riesgos de gestión, de corrupción y de seguridad digital en cada proceso de la entidad,
- El diseño de acciones o controles preventivos para administrar los riesgos y,
- La actuación correctiva y oportuna ante una eventual materialización de los riesgos.

Para administrar adecuadamente los riesgos de gestión, corrupción y de seguridad digital, la entidad utilizará tres (3) herramientas ofimáticas, en hojas de cálculo, debidamente parametrizados con los lineamientos de la presente política, cuya elaboración contó con el apoyo decidido del personal de la Fundación Tecnológica de la Región del Caribe Colombiano "**Fundcarcol"** como auxiliar de la administración.

Para garantizar el éxito en la implementación de la gestión del riesgo, proponemos desarrollar el sistema de líneas de defensa, en el que se asignan roles estratégicos, ejecución de controles y administración del riesgo, y monitoreos y seguimientos que conducen a un examen, constante y en tiempo real, sobre la eficacia de los controles, de modo que la gestión del riesgo sea una acción coordinada de actores que aseguren el cumplimiento de sus propósitos.

Esperamos que este documento sirva de orientación y de guía para los funcionarios, colaboradores y contratistas en la prevención de los riesgos en general, que mejoremos los indicadores de gestión y de resultados de nuestra administración, y que ello redunde en mejorar la calidad de vida de nuestros habitantes.

1. OBJETIVOS DE LA POLÍTICA

La Alcaldía de Ciénaga asume la administración del riesgo como un elemento esencial de carácter estratégico, **con un enfoque preventivo en torno a los riesgos** que representan amenazas para el cumplimiento de nuestros objetivos. La gestión del riesgo **debe ser cumplida en todos los procesos**, y en todos los proyectos, programas y acciones de la entidad.

La administración del riesgo en la Alcaldía de Ciénaga tiene los siguientes objetivos:

- Identificar técnicamente los riesgos en general que puedan afectar nuestros objetivos.
- Formular acciones de prevención y de control oportuna de los riesgos.
- Contar con una metodología y con herramientas de gestión adecuadas para el análisis y evaluación de riesgo, la asignación de roles y establecimiento de controles e indicadores de seguimiento.
- Utilizar un enfoque de prevención de riesgos, que permita anticiparnos a los hechos o situaciones que representan un obstáculo o desviación para el cumplimiento de nuestras metas y objetivos.

2. GLOSARIO DE TERMINOS.

En este capítulo detallamos en orden alfabético las definiciones de conceptos técnicos utilizados en este documento, para facilitar su comprensión:

Análisis de Riesgos: corresponde a la determinación del impacto en función de la consecuencia o efecto y de la probabilidad de ocurrencia del riesgo.

Consecuencias: son los efectos que resultan de la ocurrencia o la materialización de un riesgo.

Causas: son los hechos, circunstancias, situaciones generadoras del evento.

Control: son las acciones que propone la entidad para reducir la probabilidad de ocurrencia o el impacto que pueda generar su materialización.

Evento o riesgo: es el hecho que se afecta el logro del objetivo del mismo, tiene relación directa con las actividades críticas de los planes operativos, las actividades de ruta crítica de los Proyectos de Inversión y las actividades críticas de control de los procesos.

Frecuencia: es la periodicidad con que ha ocurrido un evento.

Gestión del riesgo: Es un proceso que involucra a todos los funcionarios y que lidera la alta dirección para garantizar la prestación adecuada de bienes y servicios, y para asegurar el cumplimiento del objeto misional.

Gestor del Riesgo: Funcionario líder de una dependencia, secretaria u oficina, quien apoya al responsable del riesgo.

Identificación del Riesgo: Descripción de la situación, hecho o evento riesgoso.

Impacto: es la magnitud de las consecuencias que pueden ocasionar a la entidad la materialización del riesgo.

Matriz de gestión del riesgo: Es una herramienta de gestión parametrizada de los riesgos, para la identificación, análisis, valoración y administración de los riesgos.

Las matrices de gestión del riesgo son tres: de riesgos de gestión, corrupción y seguridad digital.

Mapa de riesgos: Es el documento con la información resultante de la gestión del riesgo consolidado.

Políticas de manejo del Riesgo: Son los criterios que orientan la toma de decisiones para tratar, y en lo posible minimizar, los riesgos en la entidad, en función de su evaluación.

Probabilidad: Medida para determinar la posibilidad de que ocurra un evento.

Responsable del riesgo: Es el responsable del proceso encargado de identificar, valorar y definir el plan de contingencia, el manejo y monitoreo de cada uno de los riesgos.

Riesgo de gestión: Es la posibilidad de que suceda algún evento que afecte negativamente el cumplimiento de los objetivos

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

Riesgo de seguridad digital: Es la combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las persona.

Riesgo residual: Es aquel que resulta después de aplicar controles existentes para mitigar el riesgo.

Riesgo Inherente: Es el riesgo puro, al cual no se han aplicado controles, para controlarlo y buscar evitar su materialización.

Tratamiento: Opciones que determinan el tipo de acciones a implementar para administrar el riesgo.

Valoración: Grado de exposición al riesgo con la clasificación de probabilidad e impacto aplicando los controles existentes.

3. CONTEXTUALIZACION.

Para entender los términos de esta política, es necesario identificar el contexto general de la Alcaldía de Ciénaga, para conocer sus características, generalidades, entorno, funciones, procesos; y en general, todo lo relacionado con sus elementos esenciales:

La **MISIÓN Y VISIÓN** expresan los principales fines de la entidad, su rumbo y aspiraciones o proyección a media plazo.

LOS **OBJETIVOS ESTRATÉGICOS** contienen el fin en el que deben dirigirse los recursos y esfuerzos de la entidad. Se plasman en el Plan de Desarrollo y en los instrumentos de planeación institucional.

El **MAPA DE PROCESO** es la representación gráfica de los procesos estratégicos, misionales, de apoyo, de evaluación de la entidad, y su interacción, de acuerdo con el Modelo de Operación por Procesos MOP.

La **CARACTERIZACIÓN DE LOS PROCESOS** es el documento que detalla los objetivos específicos, las características, proveedores, acciones, productos, clientes, indicadores, procedimientos y formatos más relevantes de cada proceso de la organización, desarrollando el ciclo PHVA (Planear, Hacer, Verificar, Actuar).

4. ASPECTO METODOLOGICO PARA LA GESTIÓN DEL RIESGO

4.1 MODELO DE LÍNEAS DE DEFENSA.

El modelo de Líneas de Defensa es un sistema en el que se distribuyen los roles y responsabilidades en los funcionarios de las organizaciones, en relación con la administración de los riesgos; ayudando a asegurar el éxito en la gestión del riesgo apoyado en la estructura orgánica y en el modelo de operación por procesos de la Alcaldía de Ciénaga y en el ciclo de gestión PHVA.

El Modelo contiene **cuatro (4) líneas de defensa** así:

4.1.1. Línea de defensa estratégica

Esta línea de defensa es la que define el marco general para la gestión del riesgo y el control y además, supervisa su cumplimiento. Está a cargo de la Alta dirección y el Comité institucional de coordinación de control interno "**CCCI**".

Funcionarios de esta línea de defensa: Alcalde municipal y Comité Coordinador de Control Interno Institucional "**CCCI"**.

Responsabilidades:

Los funcionarios que pertenecen a esta línea de defensa tienen los siguientes roles:

- Diseñar la **Política institucional de Administración del Riesgo**.
- **Formular y socializar** la metodología para la identificación, análisis, valoración, monitoreo y seguimiento de los riesgos, así como las oportunidades que contribuyan a aumentar los efectos deseables para el cumplimiento de los objetivos del plan de acción institucional y de los procesos.
- **Establecer objetivos institucionales** articulados con la visión, misión y el plan de desarrollo, con las metas y estrategias de la entidad.
- Asegurarse **que el sistema de control interno funcione**; identificar y evaluar los cambios que lo puedan impactar.
- **Revisar los cambios en el "Direccionamiento estratégico**" y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados.
- Verificar que los **objetivos** de los procesos **sean coherentes** con los objetivos institucionales.
- **Hacer seguimiento,** en el seno del Comité Institucional y de coordinador de Control Interno, **a la gestión del riesgo** y a los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna.
- **Revisar el cumplimiento de los objetivos institucionales** y de los procesos a través de indicadores, y detectar los riesgos que se estén materializando.
- **Revisar**, al menos trimestralmente, **los informes sobre los riesgos** que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que los ocasionaron.

- **Revisar los planes de acción frente a los riesgos** que hayan ocurrido, para asegurarse que tomen medidas oportunas y eficaces para evitar que se repitan.

4.1.2. Primera Línea de Defensa

Los funcionarios de esta línea de defensa son los encargados de desarrollar e implementar los procesos de control y gestión de riesgos, por medio de la identificación, análisis, valoración, aplicación, monitoreo y el diseño y cumplimiento de las acciones de mejora.

Funcionarios de esta línea de defensa: Líderes de los Procesos Institucionales (Secretarios de despacho, jefes de oficina y, asesores líderes de procesos)

Responsabilidades:

Los funcionarios que pertenecen a esta línea de defensa tienen los siguientes roles:

- **Identificar y valorar los riesgos** que pueden afectar el logro de los objetivos institucionales.
- **Definir y diseñar los controles** a los riesgos.
- **Establecer sistemas de gestión de riesgos** y las responsabilidades para controlarlos, bajo la supervisión de la alta dirección.
- Diseñar los riesgos por procesos.
- **Identificar y gestionar los riesgos asociados a posibles actos de corrupción**.
- **Identificar y detectar fraudes**, y revisar con el auditor o control interno de la organización, la exposición de la entidad al fraude.
- Verificar los **cambios en el Direccionamiento Estratégico** o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de sus procesos.

- Verificar que el **diseño y ejecución** de los controles para la mitigación de los riesgos sea adecuado y eficaz

- Verificar que las **actividades de control** de sus procesos se encuentren documentadas y actualizadas en los procedimientos.

- Monitorear el cumplimiento de los objetivos de sus procesos a través de sus **indicadores de desempeño**, e identificar en caso de que no se estén cumpliendo, los riesgos que están ocurriendo.

- **Revisar y reportar a Planeación** los riesgos que se han materializado en la entidad, incluyendo los de corrupción, así como las causas que los originaron.

- **Revisar los planes de acción** establecidos para cada uno **de los riesgos materializados**, con el fin de verificar que contemplen medidas oportunas y eficaces para evitar la repetición del evento y lograr el cumplimiento a los objetivos.

- Revisar y **hacer seguimiento al cumplimiento de las actividades** y planes de acción acordados con la línea estratégica, segunda y tercera línea de defensa con relación a la gestión de riesgos.

4.1.3. Segunda Línea de Defensa

Los funcionarios que pertenecen a esta línea de defensa apoyan y guían la línea estratégica y la primera línea de defensa en la gestión adecuada de los riesgos que pueden afectar el cumplimiento de los objetivos institucionales y sus procesos. Lleva un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos.

Funcionarios de esta línea de defensa: Oficina Asesora de Planeación, responsables de monitoreo y evaluación de controles, supervisores y miembros de comités que existan en la entidad.

Responsabilidades:

Los funcionarios que pertenecen a esta línea de defensa tienen los siguientes roles:

- **Monitorear** el cumplimiento de **las acciones de control o de ejecución de controles** a través de indicadores de los planes de acción de los procesos.

- **Revisar los cambios en el direccionamiento estratégico** o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de **actualizar los controles** de los riesgos.

- **Revisar el diseño de los controles** que establece la primera línea de defensa **y formular recomendaciones** para su fortalecimiento.

- Asegurarse que se documenten las actividades de control para la mitigación de los riesgos.

- **Revisar los planes de acción para los riesgos materializados**, con el fin de que contemplen medidas oportunas y eficaces para evitar que vuelva a ocurrir.

- Contar con **un esquema de monitoreo** en cada uno de los procesos, sobre la ejecución de los controles.

- **Elaborar informes** consolidados para las partes interesadas sobre las actividades de monitoreo realizadas.

- **Hacer seguimiento a los resultados** de las acciones de mitigación de los riesgos, cuando haya lugar a ello.

- Los **supervisores e interventores de contratos** deben **hacer seguimiento a los riesgos de estos** y generar las alertas respectivas.

4.1.4. Tercera Línea de Defensa

Los funcionarios que pertenecen a esta línea de defensa realizan la evaluación independiente y objetiva sobre la efectividad del sistema de gestión de riesgos, **verificando que la línea estratégica, la primera y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos**.

Responsable: Proceso de Evaluación y Seguimiento (Asesor con funciones de control interno).

Responsabilidades:

Los funcionarios que pertenecen a esta línea de defensa tienen los siguientes roles:

- **Evaluar la eficacia de la gestión del riesgo y del control** con énfasis en el diseño e idoneidad de los controles establecidos en los procesos.
- Hacer **seguimiento objetivo a las áreas no cubiertas por la segunda línea de defensa**.
- **Asesorar**, en coordinación con la Oficina Asesora de Planeación, **sobre la identificación de los riesgos** institucionales y el diseño de controles.
- Llevar a cabo el **seguimiento a los riesgos consolidados** en los mapas de riesgos de conformidad con el Plan Anual de Auditoria y reportar los resultados al "CCCI".
- **Recomendar mejoras** a la política de administración del riesgo.
- **Identificar y evaluar cambios que podrían tener un impacto significativo en el Sistema de Control Interno**, durante las evaluaciones periódicas de riesgos y en el curso de las auditorías internas.
- **Revisar la efectividad y la aplicación de controles, planes de contingencia y actividades de monitoreo** vinculadas a riesgos claves de la entidad.
- **Alertar** sobre la probabilidad de riesgo de fraude o corrupción en las áreas auditadas.
- **Revisar los cambios en el "Direccionamiento estratégico"** o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados, con el fin de que se formulen ajustes o mejoras.

- **Revisar que se hayan identificado los riesgos que afectan en el cumplimiento de los objetivos** de los procesos, además de incluir los riesgos de corrupción.

- **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 su fortalecimiento.

- Revisar **que las acciones orientadas a mitigar los riesgos de los procesos se encuentren documentadas** y actualizadas en los procedimientos y los planes de mejora, además, que se lleven a cabo de manera oportuna, se establezcan las causas y se evite, en lo posible, la repetición de hallazgos y la materialización de los riesgos.

- Formular recomendaciones sobre cantidad y contenido de identificación de riesgos, causas, controles, períodos de ejecución, indicadores.

4.2. IDENTIFICACIÓN DEL RIESGO.

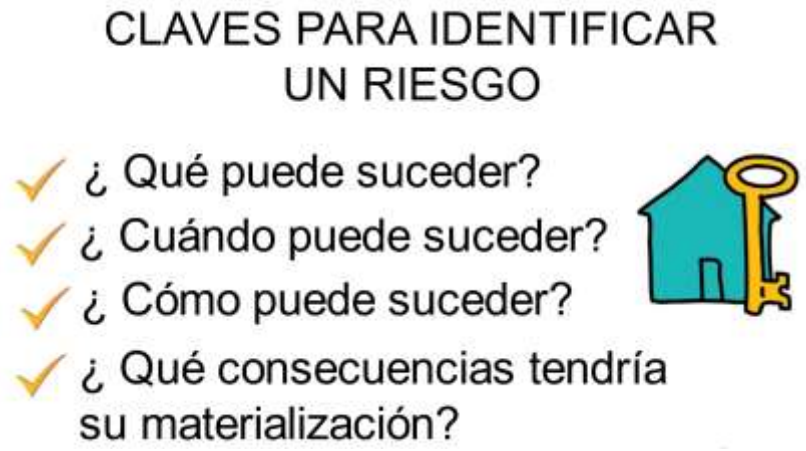
La identificación del riesgo **le corresponde a la primera línea de defensa**. En esta primera fase se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas (NTC ISO31000, Numeral 2.15).

Teniendo en cuenta que la metodología para la gestión del riesgo se enfoca en tres (3) tipos de riesgos: **de gestión, corrupción y de seguridad digital**; en adelante, se especificarán los lineamientos para cada uno de estos de manera separada.

La identificación del riesgo se realiza a partir de la descripción de los eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del proceso con base en el contexto interno y externo. Se debe hacer una breve descripción del riesgo refiriéndose a sus características o las formas en que se manifiesta.

Para la identificación de los riesgos es recomendable concentrarse en los riesgos más significativos para los procesos, relacionados con sus objetivos y el cumplimiento de metas.

Para identificar un riesgo, sus causas y consecuencias, se sugiere formular las siguientes preguntas:



Para la identificación del **riesgo de corrupción** se deben describir las situaciones que sugieren la ocurrencia de un hecho que **implique el uso del poder para desviar la gestión de lo público** con el propósito de **obtener un beneficio particular**, de tal modo que deberán concurrir los siguientes elementos:

NOTA: Es importante recordar que el "Uso de Poder" y "Beneficio privado" **son característicos del Riesgo de Corrupción**, por lo que debe asegurarse que en la formulación de este tipo de riesgos se incluyan esos elementos.

El beneficio privado corresponde a la intensión de generar un lucro o beneficio a un tercero o para el mismo servidor público.

El uso del poder corresponde a la circunstancia de que un servidor público o particular en ejercicio de funciones públicas, haga uso de su cargo o de sus funciones para generar el hecho de corrupción.

Para la identificación de **riesgos de seguridad digital** se deben identificar los activos en cada proceso, esta labor debe ser realizada por la Primera Línea de Defensa – Líderes de Proceso, en cada uno donde aplique la gestión del riesgo de

seguridad digital, siendo debidamente orientados por el responsable de seguridad digital o de seguridad de la información de la Alcaldía de Ciénaga.

Un **activo** es cualquier elemento que tiene valor para la organización, sin embargo, en el contexto de seguridad digital, **son activos que utiliza la organización para funcionar en el entorno digital**: aplicaciones de la organización, servicios web, redes, información física o digital, tecnologías de información -TI, tecnologías de operación -TO.

Se busca proteger los activos para garantizar tanto su funcionamiento interno como el funcionamiento de la entidad de cara al ciudadano, aumentando su confianza en el uso del entorno digital.

Para identificar los activos, se deben seguir los siguientes pasos:

El resultado de este ejercicio es la consolidación del inventario de activos.

4.3 IDENTIFICACION DE CAUSAS Y CONSECUENCIAS.

Causas: Cuando se identifican y describen los riesgos, se deben identificar las causas generadoras de estos; es decir, todos aquellos **factores tanto de carácter interno como externos** que, solos o en combinación con otros, posibilitan la materialización de un riesgo.

Consecuencias: Es necesario identificar las consecuencias; es decir, los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, los grupos de valor y demás partes interesadas.

A continuación, se ilustran ejemplos y esquemas para la identificación de riesgos, causas y consecuencias para cada uno de los tipos de riesgos tratados en la presente política.

RIESGOS DE GESTION			
#	Descripción del Riesgo	Causas	Consecuencias
1	Desactualización de los funcionarios sobre las normas que regulan los procesos de la entidad.	Ausencia de un Plan Institucional de Capacitación	Productos y servicios deficientes, bajos estándares de calidad, demandas, denuncias, investigaciones disciplinarias, afectación del clima laboral, improductividad laboral
		Indebido análisis y priorización de temáticas en los procesos de capacitación.	
		Ausencia de procedimientos para formular el plan de capacitación institucional.	

RIESGOS DE CORRUPCION			
#	Descripción del Riesgo	Causas	Consecuencias
1	Ocultar en los informes de evaluación y seguimiento irregularidades o deficiencias o conceptualizar favorablemente, contrario a las evidencias, con el fin de conseguir algún beneficio particular para sí o para terceros.	Amiguismo	Investigaciones disciplinarias, baja calidad de productos, incumplimiento de los objetivos del proceso y los institucionales; impunidad, deterioro de la confianza y de la autoridad.
		Ausencia de valores éticos	
		Tráfico de influencias	

RIESGOS DE SEGURIDAD DIGITAL				
#	Activo	Descripción del Riesgo	Causas	Consecuencias
1	SOFTWARE FINANCIERO	Pérdida de la confidencialidad	Ausencia de una política de restricción de acceso no autorizado al programa	Pérdida de la información, inoperatividad del sistema, afectación de procesos laborales, retrasos en la producción laboral
		Pérdida de la integridad	Manipulación de la información	
		Pérdida de disponibilidad	Ataques cibernéticos	

4.3. VALORACIÓN DEL RIESGO.

Consiste en analizar el riesgo para establecer su probabilidad de ocurrencia y el impacto o consecuencias que genera, con el fin de **estimar la zona de riesgo inicial** (**RIESGO INHERENTE**); y posteriormente evaluarlo, para confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (**RIESGO RESIDUAL**).

En la valoración del riesgo, para establecimiento de la zona del riesgo inherente se desarrollan las siguientes actividades:

4.3.1. Probabilidad e impacto.

Por **PROBABILIDAD** se entiende el grado de ocurrencia de un riesgo, éste puede ser medido con criterios de Frecuencia o Factibilidad. Bajo el criterio de **FRECUENCIA** se analizan el número de eventos en un periodo determinado, se trata de hechos que han ocurrido; y bajo el criterio de **FACTABILIDAD** se analiza la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero que puede ocurrir.

Para determinación de la probabilidad en los tres (3) tipos de riesgos se utiliza la tabla de probabilidad:

Como referente, a continuación, se muestra una tabla de actividades típicas relacionadas con la gestión de una entidad pública, bajo las cuales se definen las escalas de probabilidad:

Actividad	Frecuencia de la Actividad	Probabilidad frente al Riesgo
Planeación estratégica	1 vez al año	Muy baja
Actividades de talento humano, jurídica, administrativa	Mensual	Media
Contabilidad, cartera	Semanal	Alta
*Tecnología (incluye disponibilidad de aplicativos), tesorería *Nota: En materia de tecnología se tiene en cuenta 1 hora funcionamiento = 1 vez. Ej.: Aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia su frecuencia se calcularía 60 días * 24 horas= 1440 horas.	Diaria	Muy alta

Criterios para definir el nivel de probabilidad

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 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%

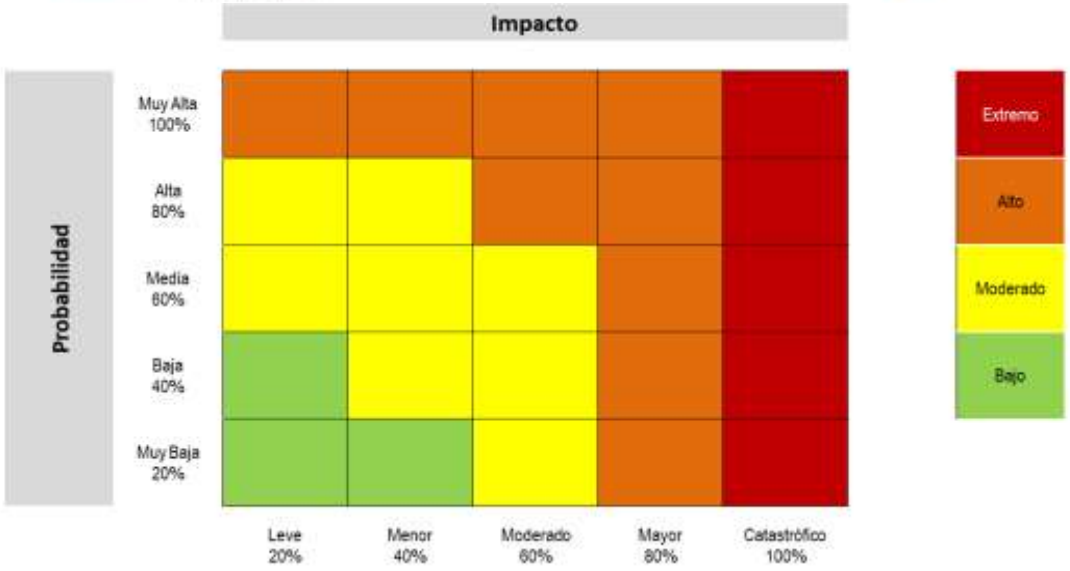
Por **IMPACTO** se entienden las consecuencias que genera la ocurrencia del riesgo. Para su determinación de acuerdo con el tipo de riesgo, se utilizan los siguientes criterios:

Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales. Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto, así por ejemplo: para un riesgo identificado se define un impacto económico en nivel

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país

Evaluación de riesgos

Análisis preliminar (**riesgo inherente**): se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor.



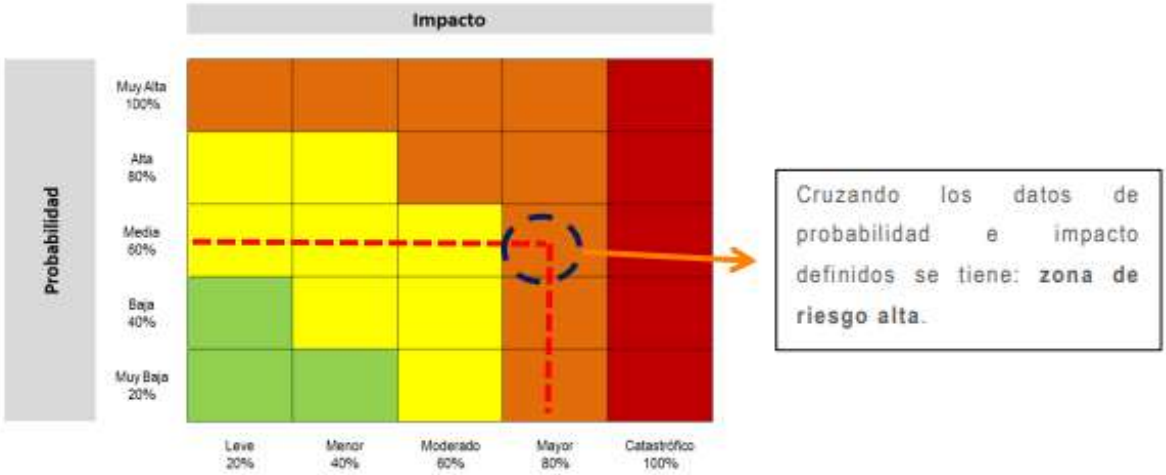
EJEMPLO:

Proceso de Gestión Administrativa: Adquirir con oportunidad y calidad técnica los bienes y servicios requeridos por la entidad para su continua operación.

Riesgo identificado: Afectación económica por multa y sanción del ente regulador debido a la adquisición de bienes y servicios sin el cumplimiento de los requisitos normativos.

Probabilidad Inherente= moderada 60%
Impacto Inherente: mayor 80%

Aplicando la matriz de calor, tenemos:



Criterios para calificar el IMPACTO en los RIESGOS DE CORRUPCIÓN

No	PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA…	RESPUESTA SI	RESPUESTA NO
1	¿Afectar al grupo de funcionarios del proceso?		
2	¿Afectar el cumplimiento de metas y objetivos de la dependencia?		
3	¿Afectar el cumplimiento de misión de la entidad?		
4	¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos		
9	¿Generar pérdida de información de la entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía u otro ente?		
11	¿Dar lugar a procesos sancionatorios?		
12	¿Dar lugar a procesos disciplinarios?		
13	¿Dar lugar a procesos fiscales?		
14	¿Dar lugar a procesos penales?		
15	¿Generar pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		

NIVELES DE IMPACTO

CRITERIO	IMPACTO	CONSECUENCIA
Responder afirmativamente de UNA a CINCO preguntas(s)	**MODERADO**	Genera medianas consecuencias sobre la entidad
Responder afirmativamente de SEIS a ONCE preguntas	**MAYOR**	Genera altas consecuencias sobre la entidad.
Responder afirmativamente de DOCE a DIECINUEVE preguntas	**CATASTRÓFICO**	Genera consecuencias desastrosas para la entidad

4.4. EVALUACIÓN DEL RIESGO.

La evaluación del riesgo está dirigida a confrontar los resultados del Riesgo inicial (**RIESGO INHERENTE**) frente a los controles establecidos con el fin de determinar la zona de riesgo final (**RIESGO RESIDUAL**).

En ese sentido, se busca identificar controles dirigidos a la administración del riesgo y valorarlos. Se deben seguir las siguientes acciones:

- Identificar los riesgos inherentes que pueden afectar el cumplimiento de los objetivos estratégicos y de proceso.
- Identificar las causas o fallas que pueden materializar el riesgo.
- Para cada causa se debe asignar un control.
- Evaluar si los controles están dirigidos a evitar o mitigar el riesgo.
- Las causas se deben trabajar de manera separada (**no se deben combinar en una misma columna o renglón**).
- Un control puede ser tan eficiente que me ayude a mitigar varias causas, en estos casos se repite el control, asociado de manera independiente a la causa específica.

Al momento de definir las actividades de control por parte de la primera línea de defensa, es importante considerar que los controles estén bien diseñados; es decir, que efectivamente estos mitigan las causas que hacen que el riesgo se materialice.

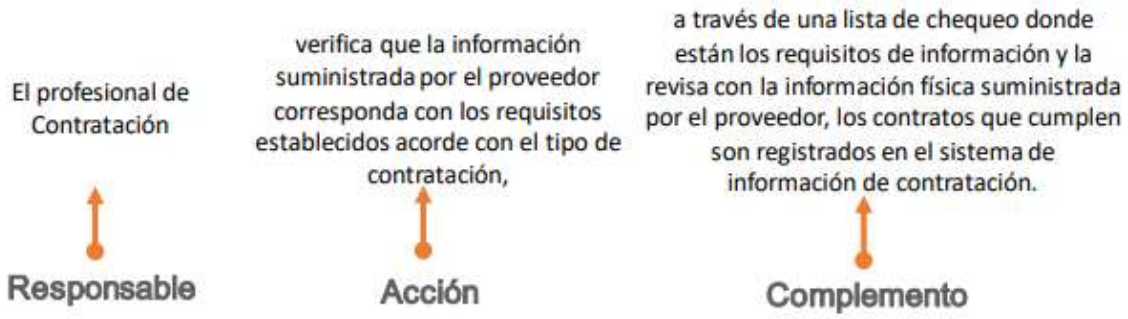
Para diseñar un control (*acciones preventivas o detectivas de los riesgos*) debemos utilizar la siguiente estructura de descripción del control:

Para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración.

La estructura es la siguiente:

- **Responsable de ejecutar el control:** identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad
- **Acción:** se determina mediante verbos que indican la acción que deben realizar como parte del control.
- **Complemento:** corresponde a los detalles que permiten identificar claramente el objeto del control.

Ejemplo:



4.4.1. TIPOLOGÍA DE CONTROLES

- **Control preventivo:** control accionado en la entrada del proceso y **antes de que se genere el 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.

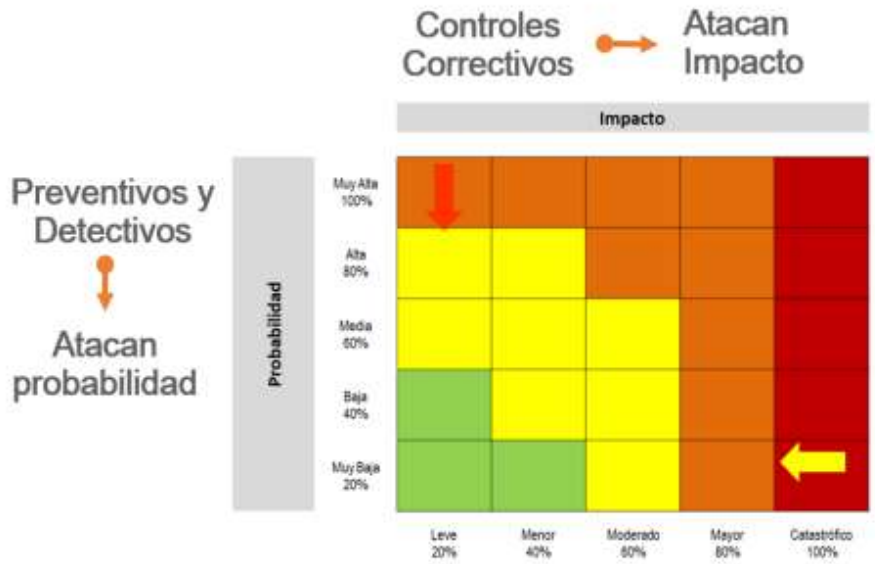
4.4.2. ANÁLISIS Y EVALUACIÓN DE LOS CONTROLES

Atributos de para el diseño del control

Características			Descripción	Peso
			intervención de personas para su realización.	
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
*Atributos informativos	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	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

Características			Descripción	Peso
			intervención de personas para su realización.	
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
*Atributos informativos	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	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

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



4.5. LINEAMIENTOS SOBRE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

4.5.1. Identificación de los activos de seguridad de la información:

Conceptualización de los activos de información.

¿Qué son los activos?	¿Por qué identificar los activos?
Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como: ☑ Aplicaciones de la organización ☑ Servicios web ☑ Redes ☑ Información física o digital ☑ Tecnologías de información TI ☑ Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital	Permite determinar qué es lo más importante que los Procesos de la entidad poseen (sean bases de datos, archivos, servidores web o aplicaciones clave para que la entidad pueda prestar sus servicios). La entidad puede saber qué es lo que debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, aumentando así su confianza en el uso del entorno digita

4.5.2. PASOS PARA LA IDENTIFICACIÓN DE ACTIVOS

- ☑ Listar los activos de cada proceso
- ☑ Identificar los dueños de los activos
- ☑ Clasificar los activos
- ☑ Clasificar la información

- Determinar la criticidad del activo
- Identificar si existe infraestructura crítica cibernética
- Establecer las amenazas
- Establecer el tipo de riesgo
- Establecer las causas o vulnerabilidades
- Identificar las consecuencias

Para la identificación del riesgo de seguridad de la información, se tendrán en cuenta los siguientes tipos de riesgos:

- Pérdida de la confidencialidad
- Pérdida de la integridad
- Pérdida de la disponibilidad

4.6. TRATAMIENTO DEL RIESGO.

Es tratamiento del riesgo es la respuesta establecida por **la primera línea de defensa** para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción.

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

- **Aceptar el Riesgo**: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.

NOTA: Ningún riesgo de corrupción podrá ser aceptado).

- **Reducir el Riesgo**: se adoptan medidas para **reducir la probabilidad o el impacto del riesgo**, o ambos; por lo general implica diseñar controles.

- **Evitar el Riesgo**: se abandonan las actividades que dan lugar al riesgo; es decir, se suprime la actividad, plan, programa, función o proyecto asociado al riesgo.

- **Compartir el Riesgo**: se reduce la probabilidad o el impacto del riesgo **transfiriendo o compartiendo una parte de este**. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad

4.7. MONITOREO Y REVISIÓN.

El monitoreo y revisión busca que las acciones de control de los mapas de riesgos se cumplan, para ello se evalúa la eficacia en su implementación, **verificando** las situaciones o factores que pueden influir en la aplicación de las acciones preventivas.

El monitoreo está a cargo de:

a. RESPONSABLES DE LOS PROCESOS Y DE LA OFICINA ASESORA DE PLANEACIÓN.

Son los funcionarios responsables de cumplir las **acciones asociadas a los controles** de cada riesgo. Debe hacerse en la periodicidad establecida en esta Política.

Al hacer los seguimientos cada líder de proceso debe conservar los soportes que evidencian su aplicación.

La Oficina Asesora de Planeación realizará actividades de monitoreo periódicas.

b. PROCESO DE EVALUACIÓN Y SEGUIMIENTO (Control Interno)

Es el proceso encargado de realizar el seguimiento a los riesgos consolidados. En sus procesos de auditoría interna se debe analizar el diseño e idoneidad de los controles, determinando:

- Si son o no adecuados para prevenir o mitigar los riesgos de los procesos,
- Si se aplicaron oportuna y adecuadamente,
- Si se dejaron evidencias de su aplicación y,
- Si se reportaron las desviaciones detectadas, haciendo uso de las técnicas relacionadas con pruebas de auditoría que permitan determinar la efectividad de los controles.

Los informes de control interno **deben incluir recomendaciones** que promuevan ajustes, mejoras o actividades para subsanar las desviaciones detectadas.

4.7.1. Lineamientos para los riesgos materializados

Si dentro del seguimiento realizado, bien sea por parte del proceso de control interno y calidad, la Secretaría de Planeación o por los líderes de los procesos, se detecta que ocurrido uno o más riesgos, se deben seguir las siguientes rutas:

a. POR PARTE DEL PROCESO DE EVALUACIÓN Y SEGUIMIENTO

<u>Cuando el riesgo sea de corrupción</u>

- Convocar al Comité Coordinador de Control Interno e informar sobre los hechos detectados, desde donde se tomarán las decisiones para iniciar la investigación de los hechos.

- Dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante el ente de control respectivo.

- Facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos y sus controles asociados.

- Verificar que se tomaron las acciones y se actualizó el mapa de riesgos.

Si el riesgo es de gestión o de seguridad digital y se encuentra en las ZONAS: EXTREMA, ALTA O MODERADA:

- Informar al líder del proceso sobre el hecho encontrado.

- Orientar al líder del proceso para que realice la revisión, análisis y acciones correspondientes para resolver el hecho.

- Verificar que se tomaron las acciones y que se actualizó el mapa de riesgos correspondiente.

- Convocar al Comité Coordinador de Control Interno e informar sobre la actualización realizada.

Si el riesgo es de gestión o de seguridad digital y se encuentra en las ZONA BAJA:

- Aplicar las orientaciones de la política de riesgos institucional. (Verificar los niveles de aceptación del riesgo).

b. POR PARTE DE LOS LÍDERES DE LOS PROCESO U OTROS FUNCIONARIOS QUE PARTICIPAN O INTERACTÚAN CON EL PROCESO.

<u>Cuando el riesgo sea de corrupción:</u>

- Informar a la Alta Dirección sobre el hecho encontrado.

- De considerarlo necesario, realizar la denuncia ante el ente de control respectivo.

- Iniciar con las acciones correctivas necesarias.

- Realizar el análisis de causas y determinar acciones preventivas y de mejora.

- Análisis y actualización del mapa de riesgos.

Si el riesgo es de gestión o de seguridad digital y se encuentra en las ZONAS: EXTREMA, ALTA O MODERADA.

- Promover las acciones correctivas necesarias, dependiendo del riesgo materializado.

- Identificar las causas y determinar acciones preventivas y de mejora.
- Analizar y actualizar el mapa de riesgos.
- Informar a la Alta Dirección sobre el hallazgo y las acciones tomadas.

Si el riesgo es de gestión o de seguridad digital y se encuentra en las ZONA BAJA

- Aplicar las orientaciones de la política de riesgos institucional. (*Verificar los niveles de aceptación del riesgo*).

De acuerdo con el seguimiento realizado es importante determinar**, al final de cada vigencia**, si los mapas de riesgos deben ser actualizados o si se mantienen bajo las mismas condiciones en cuanto a factores de riesgo, identificación, análisis y valoración del riesgo.

Para poder determinarlo se analizará si no se han presentado hechos significativos como:

- Riesgos materializados relacionados con posibles actos de corrupción.
- Riesgos de gestión materializados en cualquiera de los procesos.
- Observaciones o hallazgos por parte del proceso de Control Interno y Calidad o bien por parte de un ente de control, respecto de la idoneidad y efectividad de los controles.
- Cambios importantes en el entorno estratégico o normativo que puedan generar nuevos riesgos.
- Inclusión de nuevos riesgos o controles identificados por la entidad.

No obstante, los mapas de riesgos deben ser flexibles y permitir cambios cuando se requieran.