



POLÍTICA DE GESTIÓN DEL RIESGO, EMPRESAS PÚBLICAS MUNICIPALES DE CANDELARIA

Agosto de 2019

Carrera 11 No 10 – 55 Esquina
Villagorgona (Candelaria)
Teléfono: (+57 2) 260 6496
Celular: 318 706 8540
www.emcandelaria.gov.co
gerencia@emcandelaria.gov.co
Valle del Cauca - Colombia



INTRODUCCIÓN

La Política de Administración del riesgo de Empresas Públicas Municipales de Candelaria EMCANDELARIA, manifiesta el compromiso de la gerente y su equipo directivo, ante a la identificación, tratamiento y control de los riesgos y oportunidades, que intervienen con los resultados de la gestión y permiten el cumplimiento de las metas establecidas en el Plan Estratégico 2016 - 2019.

La presente política involucra, a todos los servidores de la entidad mediante tres líneas de defensa, soportándose en los mecanismos de comunicación disponibles, y cubriendo todas las responsabilidades institucionales, las de cada proceso y las propias de cada servidor.

De igual manera se tienen comprendidos los niveles de aceptación de riesgo, los niveles de calificación, la identificación de riesgos estratégicos, operacionales, de corrupción, los riesgos informáticos y demás eventos que afecten el cumplimiento de los objetivos de la organización.

La política pretende direccionar e influenciar la cultura organizacional, en función del pensamiento basado en riesgos. Cabe resaltar que, en su diseño contempla la administración de otras tipologías de riesgos correspondientes a los sistemas de gestión implementados en EMCANDELARIA como son: Seguridad de la Información, Gestión de Seguridad y Salud en el Trabajo, entre otros.

La política del riesgo se define tomando como referente los parámetros del Modelo Integrado de Planeación y Gestión – MIPG en los procesos, así como los del Modelo Estándar de Control Interno – MECI, en lo referente a las líneas de defensa, los lineamientos de la Guía para la administración del riesgo de la Función Pública 2018¹.

Todos los procesos deben establecer los lineamientos que permitan la identificación, el análisis, la valoración y el tratamiento de los riesgos que pudieran afectar la misión y el cumplimiento de los objetivos institucionales en el marco de los programas, proyectos, planes y procesos de las Empresas Públicas Municipales de Candelaria, mediante:

a) La identificación y documentación de riesgos de gestión (financieros, contractuales, jurídicos, entre otros), corrupción y de seguridad digital en los programas.

¹ Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital – Versión 4 – DAFP – octubre 2018

b) El establecimiento de acciones de control, de detección y prevención para los riesgos identificados.

c) La actuación correctiva y oportuna ante la materialización de los riesgos identificados.

OBJETIVOS

OBJETIVO GENERAL:

Establecer los parámetros para la gestión integral de los riesgos de las Empresas Públicas Municipales de Candelaria, a través de la presentación de los criterios para la identificación, análisis, evaluación, tratamiento, monitoreo, revisión, comunicación y consulta de los riesgos, que pueden afectar el cumplimiento de la misión y objetivos institucionales, orientando la entidad hacia un nivel de aseguramiento razonable.

OBJETIVOS ESPECÍFICOS.

- Generar confianza institucional a través del establecimiento de estrategias que permitan detectar, prevenir, minimizar y controlar los riesgos.
- Orientar las actividades de identificación y documentación de los riesgos.
- Definir las actividades de seguimiento y evaluación a la gestión de los riesgos.
- Orientar la toma de decisiones oportunas y minimizar efectos adversos al interior de la Entidad, con el fin de garantizar la continuidad a la gestión institucional y el logro de los objetivos estratégicos.

ALCANCE

La Política de administración de riesgos en las Empresas Públicas Municipales de Candelaria, es aplicable al direccionamiento estratégico de la Entidad, a todos los procesos del modelo de operación por procesos, a los programas y proyectos; y a las acciones ejecutadas por los servidores durante el ejercicio de sus funciones; dándoles el tratamiento necesario, con base en la metodología definida, para cada tipología de riesgo existente.

NORMATIVIDAD

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. (Modificada parcialmente por la Ley 1474 de 2011). Artículo 2 Objetivos del Control Interno: Literal a). Proteger los recursos de la organización, buscando adecuada administración ante posibles riesgos que los afectan. Literal f). Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.

Ley 1474 de 2011: Estatuto Anticorrupción Artículo 73. “Plan Anticorrupción y de Atención al Ciudadano” que deben elaborar anualmente en todas las entidades, incluyendo el mapa de riesgos de corrupción, las medidas concretas para mitigar esos riesgos, las estrategias anti-trámites y los mecanismos para mejorar la atención al ciudadano

Decreto 1083 de 2015: Por el cual se actualiza el Modelo Estándar de Control Interno (MECI).

Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. “Riesgos de Gestión, Corrupción y Seguridad Digital”: Función Pública octubre 2018

Estrategias para la construcción del Plan Anticorrupción y Atención al Ciudadano versión 2. Presidencia de la Republica 2015

ISO 31000:2009 Norma Técnica Internacional Administración del Riesgo - Principios y orientaciones.

DEFINICIONES

- **Administración del Riesgo:** un proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la entidad un aseguramiento razonable con respecto al logro de los objetivos. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de planeación.
- **Activo de Información:** toda aquella información que reside en medio electrónico o físico, que tiene un significado y valor para las Empresas Públicas Municipales de Candelaria y, por ende, necesita ser protegida.
- **Amenaza:** causa potencial de un incidente no deseado que puede resultar en perjuicio de un sistema o la organización.
- **Autocontrol:** la capacidad que tiene cada servidor público para detectar las desviaciones en su trabajo y realizar los correctivos necesarios; en tal virtud, la

autoevaluación, como herramienta complementaria al autocontrol se convierte en un instrumento básico para la mejora continua de las entidades.

- **Autoevaluación:** comprende el monitoreo que se le debe realizar a la operación de la entidad a través de la medición de los resultados generados en cada proceso, procedimiento, proyecto, plan y/o programa, teniendo en cuenta los indicadores de gestión, el manejo de los riesgos, los planes de mejoramiento, entre otros.
- **Causa:** medios, circunstancias, situaciones o agentes generadores del riesgo.
- **Ciclo de vida del proyecto:** la serie de fases que atraviesa un proyecto desde su inicio hasta su cierre.
- **Confidencialidad:** principio de la Seguridad de la Información que busca asegurar que la información de las Empresas Públicas Municipales de Candelaria sea accedida únicamente por personal autorizado (tanto interno como externo al municipio) supliendo una necesidad legítima para la realización de sus funciones, con el fin de prevenir el uso o divulgación de esta en forma no autorizada.
- **Consecuencia:** efectos generados por la ocurrencia de un riesgo que afecta los objetivos o un proceso de la entidad. Pueden ser entre otros, una pérdida, un daño, un perjuicio, un detrimento.
- **Contenedor de la Información:** cualquier plataforma tecnológica o lugar físico que almacena, procesa, transmite un Activo de Información por cualquier termino de tiempo o propósito.
- **Contexto Externo:** Ambiente externo en el cual la organización busca alcanzar sus objetivos.
- **Control:** medida que modifica el riesgo. Controles incluyen cualquier proceso, política, estrategia, mecanismo, práctica y otras acciones que modifican el riesgo.
- **Control Preventivo:** está diseñado para evitar un evento no deseado en el momento en que se produce.
- **Control Detectivo:** está diseñado para identificar un evento o resultado no previsto después de que se haya producido. Busca detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes.
- **Disponibilidad:** principio de la Seguridad de la Información que busca asegurar que la información esté disponible cuando sea requerido por los procesos, servicios, ciudadanos y demás entidades que interactúan con la administración municipal.
- **Dueño del Proceso:** funcionario responsable del adecuado cumplimiento de las actividades que conforman un proceso, y que están encaminadas a satisfacer una demanda tanto interna como externa a las Empresas Públicas Municipales de Candelaria.
- **Evento:** ocurrencia o cambio de un particular conjunto de circunstancias. Un evento puede tener una o más consecuencias, o puede tener diferentes causas; puede consistir en algo no ocurrido, y puede ser referido algunas veces como un “incidente” o “accidente”.

- **Establecimiento del contexto:** definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo.
- **Factor de riesgo:** toda característica proveniente del contexto cuya presencia o comportamiento incide en una mayor o menor probabilidad de materialización de una o varias causas asociadas a uno o varios riesgos.
- **Fuentes de riesgo externas:** son eventos asociados a la fuerza de la naturaleza u ocasionados por terceros, que escapan en cuanto a su causa y origen al control de la entidad.
- **Gestión del Riesgo:** actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Identificación del Riesgo:** etapa en la cual se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias.
- **Impacto:** consecuencias o efectos que pueden ocasionar a la organización la materialización del riesgo.
- **Integridad:** principio de Seguridad de la Información que busca asegurar que la información esté protegida contra modificaciones no autorizadas para garantizar su consistencia, exactitud y completitud. Se debe garantizar la trazabilidad de la información.
- **Líder o responsable del proceso:** persona con la responsabilidad y autoridad para gestionar un riesgo.
- **Matriz de Riesgo:** representación final de la probabilidad e impacto de uno o más riesgos frente a un proceso, proyecto o programa.
- **Parte involucrada:** persona u organización que puede afectar o verse afectada o percibirse a sí misma como afectada por una decisión o una actividad.
- **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de frecuencia o factibilidad.
- **Proceso:** grupo de actividades relacionadas de manera lógica que, cuando se llevan a cabo, utilizan los recursos de las Empresas Públicas Municipales de Candelaria para lograr resultados definitivos o transformar elementos de entrada, a través de una serie de actividades, en un producto o servicio.
- **Propietario del Activo (o de la Información):** funcionario encargado de identificar y establecer el alcance y valor o criticidad de un Activo de Información, los requerimientos de seguridad de este y la comunicación de éstos a los custodios del Activo de Información.
- **Riesgo:** 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 Corrupción:** la posibilidad de que, por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular
- **Riesgos de Cumplimiento:** se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

- **Riesgo Estratégico:** se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
- **Riesgos Financieros:** se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.
- **Riesgos de Imagen:** están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.
- **Riesgo Inherente:** es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
- **Riesgos Operativos:** comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad, de la articulación entre dependencias.
- **Riesgo Residual:** nivel de riesgo que permanece luego de tomar medidas de tratamiento del riesgo.
- **Riesgos de Tecnología:** están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.
- **Riesgos de Seguridad Digital:** 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 personas.
- **Seguridad de la Información:** Preservación de la Confidencialidad, Integridad y Disponibilidad de la información, en adición también de otras propiedades como autenticación, autorización, registro de actividad, no repudio y confiabilidad pueden ser también consideradas.
- **Tolerancia al riesgo:** son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. **Para el riesgo de corrupción la tolerancia es inaceptable.**
- **Valoración del Riesgo:** Establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (riesgo inherente).
- **Vulnerabilidad:** debilidad asociada al Contenedor de un Activo de Información y que puede ser explotada para materializar un Riesgo, causando incidentes no deseados que pueden dar lugar a la pérdida de Confidencialidad, Integridad o Disponibilidad de los Activos de Información.

RESPONSABILIDAD EN LA GESTIÓN DEL RIESGO

Para realizar un análisis y valoración del riesgo que permita mitigar efectivamente los riesgos identificados, la entidad tiene en cuenta los siguientes roles y responsabilidades:

Responsabilidades de la primera línea, direccionamiento estratégico

- Establecer y aprobar la Política de administración del riesgo la cual incluye los niveles de responsabilidad y autoridad.
- Definir y hacer seguimiento a los niveles de aceptación de los riesgos.
- Analizar los cambios en el entorno (interno y externo) que puedan tener un impacto significativo en la operación de los procesos de la entidad y que puedan generar cambios no previstos.
- Realizar seguimiento y análisis continuo a los riesgos identificados.
- Evaluar el estado del sistema de control interno y aprobar las modificaciones, actualizaciones y acciones de fortalecimiento de este.

Responsabilidades de la primera línea (líderes de proceso)

- Identificar y valorar los riesgos que pueden afectar los programas, proyectos, y procesos a su cargo y actualizarlos cuando se requiera.
- Establecer, aplicar y monitorear los controles para mitigar los riesgos identificados alineado con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo en su proceso.
- El responsable del proceso debe supervisar el cumplimiento a la aplicación de los controles en su equipo de trabajo en el desarrollo de las actividades y detectar las deficiencias en los controles y determinar las acciones de mejora que se requieran.
- Monitorear los controles para establecer su eficiencia, eficacia y efectividad.
- Informar al Departamento administrativo de Planeación e informática (segunda línea) sobre los riesgos materializados en los programas, proyectos y/o procesos a su cargo.
- Reportar en el Sistema de Gestión de Calidad los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado.

Responsabilidades de la Segunda Línea

- Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo.
- Consolidar el Mapa de riesgos institucional y presentarlo para análisis y seguimiento ante el Comité de Gestión y Desempeño Institucional.
- Presentar al Comité institucional de control interno el seguimiento a la eficacia de los controles en las áreas identificadas en los diferentes niveles de operación de la entidad.
- Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis y valoración del riesgo.
- Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos.
- Supervisar en coordinación con los demás responsables de esta segunda línea de defensa que la primera línea identifique, evalúe y gestione los riesgos y controles para que se generen acciones.
- Evaluar que los riesgos sean consistentes con la presente política de la entidad y que sean monitoreados por la primera línea de defensa.
- Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles.
- Identificar cambios en el impacto del riesgo en la entidad, especialmente en aquellos riesgos ubicados en zona baja y presentarlo para aprobación del comité institucional de coordinación de control interno.

Responsabilidades de la Segunda Línea

En esta línea de defensa están incluidos los siguientes actores: líderes de procesos de contratación, financiera, talento humano, gestión y defensa jurídica, TIC, servicio al ciudadano, comunicaciones, gestión del conocimiento y gestión documental y los supervisores de contrato de la Entidad entre otros.

- Monitorear los riesgos identificados y controles establecidos por la primera línea de defensa acorde con la estructura de los temas a su cargo.

- Reportar al Departamento administrativo de Planeación e informática a través del SGC – módulo de riesgos, el seguimiento efectuado al mapa de riesgos a su cargo y proponer las acciones de mejora a que haya lugar.
- Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis, y valoración del riesgo y definición de controles en los temas a su cargo y con enfoque en la prevención del daño antijurídico.
- Supervisar que la primera línea de defensa identifique, evalúe y gestione los riesgos en los temas de su competencia.

Responsabilidades de la Tercera Línea (Jefe de control interno)

- 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.
- Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa.
- Asesorar de forma coordinada con la gerencia, a la primera línea de defensa en la identificación de los riesgos institucionales y diseño de controles.
- Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos de conformidad con el Plan Anual de Auditoría y reportar los resultados al comité institucional de control interno.
- Recomendar mejoras a la política de administración del riesgo.

ESTRUCTURA PARA LA ADMINISTRACIÓN Y GESTIÓN DE RIESGOS

En las Empresas Públicas Municipales de Candelaria, para la gestión del riesgo se siguen las etapas de identificación y valoración de los riesgos, teniendo como referencia la **Guía para la Administración del riesgo y el diseño de controles en entidades públicas V4** del Departamento Administrativo de la Función Pública (DAFP) y la Guía para la Gestión del Riesgo de Corrupción de la Secretaría de Transparencia de la Presidencia de la República.

Tabla 1. Criterios y responsabilidades en el desarrollo de las fases de gestión del riesgo en las Empresas Públicas Municipales de Candelaria.

FASE		RESPONSABLE	CRITERIOS
1	Lineamientos de la Política de Administración de Riesgos	Gerencia y jefe de control interno.	Definición de política, roles, responsabilidades y criterios para la gestión integral del riesgo.
2	Establecimiento del contexto para la gestión del riesgo.	Jefe de Control interno.	Definición de características o aspectos del entorno externo e interno, así como los aspectos esenciales de los procesos de la Empresas Públicas Municipales de Candelaria.
2.1	Identificación del riesgo	Estratégicos: Gerencia y Jefe de control interno. Operativos: Líderes de Procesos Seguridad de la Información: Jefe de control interno	Identificación de fuentes o factores de riesgo, eventos, causas y consecuencias, teniendo en cuenta los eventos con base en el análisis del contexto estratégico (interno, externo, del proceso y/o factores generadores de corrupción). Puede abarcar datos históricos, análisis teóricos, opiniones informadas y expertas, y las necesidades de las partes involucradas. Así mismo, se deben realizar las siguientes preguntas para la etapa de identificación: qué, cómo y cuándo puede suceder, y qué consecuencias tendría su materialización. De ser posible, para este análisis se deben tener en cuenta datos históricos, incidentes de Seguridad de la Información, conocimiento sobre la entidad y los procesos de las personas involucradas, y opiniones de expertos.
3	Análisis del riesgo	Responsables de proceso.	Valoración de probabilidad de ocurrencia y de impacto.
3.1	Evaluación del riesgo	Gerencia y la Jefe de control interno.	Determinación del nivel de riesgo inherente según niveles de mapa de riesgo. Identificación de controles asociados a las causas del riesgo, valoración de controles y del grupo de controles. Determinación de riesgo residual, en función de la valoración del grupo de controles. Determinación de la opción de tratamiento de acuerdo con los criterios de Opciones de tratamiento

			<p>de riesgos de acuerdo con la Zona de Riesgo.</p> <p>Definición de las acciones de tratamiento y asociación con procesos responsables.</p> <p>Ubicación en el mapa de riesgos.</p>
3.2	Monitoreo y revisión	<p>Responsables de proceso.</p> <p>La gerencia realiza el monitoreo y revisión de riesgos y acciones para tratamiento. Estas acciones se realizan con una periodicidad cuatrimestral para riesgos de corrupción y semestral para riesgos importantes e inaceptables.</p> <p>La gerencia: lleva a cabo la revisión de riesgos que sean escalados por el jefe de control interno.</p> <p>La jefe de control interno: realiza revisión mediante las auditorías, seguimientos y evaluaciones.</p>	<p>Monitoreo periódico de riesgos y eventos de materialización</p> <p>Monitoreo y revisión de riesgos y acciones para tratamiento:</p> <p>El seguimiento de riesgos será semestral para riesgos de gestión, cuatrimestral para riesgos de corrupción y de seguridad de la información de conformidad con lo establecido por la ley.</p> <p>Revisión por la Dirección</p> <p>Evaluación por la jefe de Control Interno, según plan de auditoría.</p>
3.3	Seguimiento	Jefe de Control Interno	<p>Reportes semestrales de riesgos a la Gerencia. Publicación de matrices y mapa de riesgos, campañas de promoción de cultura de gestión del riesgo y de avances y resultados en la gestión.</p>

Establecimiento del Contexto Estratégico

El contexto estratégico define los parámetros internos y externos que se deben tomar en consideración para la administración del riesgo. Teniendo en cuenta que las organizaciones son dinámicas, es necesario analizar los datos históricos, teóricos, opiniones informadas y las necesidades de cada proceso.

Para ello es necesario que los líderes de proceso identifiquen la información relacionada con el contexto y la identificación de las partes interesadas que pueden afectar los procesos, para lo cual se analizan las siguientes temáticas:

Contexto Externo (aplica para los riesgos de gestión y corrupción): se determinan las características o aspectos esenciales del entorno en el cual opera la Entidad. Se pueden considerar los siguientes factores:

CONTEXTO	FACTORES	DESCRIPCIÓN
EXTERNO	Económicos	Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia
	Políticos	Cambios de Gerencia, legislación, políticas públicas, regulación

	Sociales	Demografía, responsabilidad social, orden público.
	Tecnológicos	Avances en tecnología, acceso a los sistemas de información externos, gobierno digital.
	Medio ambientales	Emisiones y residuos, energía, catástrofes naturales, desarrollo sostenible.
	Comunicación Externa	Mecanismos utilizados para entrar en contacto con los usuarios o ciudadanos, canales establecidos para que el mismo se comunique con la entidad.

Así como aquellos impulsores claves y tendencias que tengan impacto a la organización, relaciones con las partes involucradas, sus percepciones y valores.

Contexto Interno (aplica para los riesgos de gestión y corrupción): se determinan las características o aspectos esenciales del ambiente en la cual la organización busca alcanzar sus objetivos. Se pueden considerar los siguientes factores:

CONTEXTO	FACTORES	DESCRIPCIÓN
INTERNO	Financieros	Presupuesto de funcionamiento y de inversión, infraestructura, capacidad instalada.
	Personal	Competencia de personal, estructura organizacional, funciones, responsabilidades, rotación, disponibilidad de personal, seguridad y salud, ocupaciones, cultura organizacional.
	Tecnología	Integridad, confiabilidad, sistemas de información y seguridad de información, flujos de información y proceso para la toma de decisiones, desarrollo, mantenimientos de los sistemas de producción.
	Estratégicos	Direccionamiento Estratégico, planeación institucional, liderazgo, trabajo en equipo, políticas y objetivos estratégicos.

Contexto del Proceso (aplica para los riesgos de gestión): se determinan las características o aspectos esenciales del proceso y sus interrelaciones. Se pueden considerar factores como:

CONTEXTO	FACTORES	DESCRIPCIÓN
PROCESO	Diseño del Proceso	Claridad en la descripción del objetivo y alcance del proceso
	Interacción con otros Procesos	Relación con otros procesos en cuanto a insumo, proveedores, productos, usuarios y clientes.
	Transversalidad	Proceso que determinan lineamientos necesarios para el desarrollo de todos los procesos.
	Procedimientos Asociados	La pertinencia de los procesos que se desarrollan.
	Responsable del Proceso	Grado de responsabilidad de los funcionarios frente al proceso.
	Comunicaciones entre los Procesos	Efectividad de los flujos de información determinado en la interacción de los procesos.

Determinar los factores generadores de riesgos de corrupción (aplica para los riesgos de corrupción): ocasionados entre otras cosas por la misión, por las funciones que desarrolla y el sector al que pertenece la entidad.

A partir, de la identificación del contexto se construyen los riesgos de gestión y de corrupción, respectivamente, de acuerdo con los lineamientos y pasos definidos en las Guías de la Función Pública y de la Secretaría de Transparencia.

Identificación de Activos

En esta etapa se deben identificar los contendores y Activos de Información que se podrían ver afectados por la materialización de los riesgos, tomando en cuenta la matriz de identificación de Activos, producto de la ejecución de lo establecido en la Metodología de Activos de Información las Empresas Públicas Municipales de Candelaria y el plan de tratamiento de riesgos de privacidad y seguridad de la información vigente.

La administración de riesgos en las Empresas Públicas Municipales de Candelaria tendrá un carácter prioritario y estratégico, en el marco del cumplimiento de los lineamientos establecidos por la gerencia.

Los tipos de riesgos a tener en cuenta son los siguientes:

Tabla 2. Descripción de los tipos de riesgos considerados en la gestión integral de riesgos en las Empresas Públicas Municipales de Candelaria.

TIPO DE RIESGO	DESCRIPCIÓN
Riesgos Estratégicos	Están relacionados con la planificación, diseño y conceptualización de la Entidad por parte de la gerencia, en relación con su marco estratégico: misión, visión, cumplimiento de los objetivos estratégicos y la definición de políticas
Riesgos de Imagen	Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la entidad, considerando el cumplimiento de requisitos legales
Riesgos de Corrupción	Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
Riesgos Financieros	Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.
Riesgos Operativos	Derivados del funcionamiento de los sistemas de gestión institucional, la definición y ejecución de los procesos, la operación de los sistemas de información y herramientas de apoyo a la gestión, de la estructura de la entidad y de los mecanismos de comunicación y articulación entre dependencias.
Riesgos de Tecnología	Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

Riesgo Ambiental*	Son los riesgos que están relacionados con la responsabilidad y compromiso de la entidad hacia el cuidado del ambiente
Riesgo de Seguridad y Salud en el Trabajo*	Son los riesgos que están relacionados con el compromiso de la entidad de preservar la salud y seguridad de los funcionarios y servidores
Riesgo de Seguridad de la Información	Son los riesgos asociados con la afectación a la confidencialidad, la integridad y la disponibilidad de información.

* Estos riesgos se llevarán de manera independiente a través del Proceso de Gestión del Talento Humano, por cuanto cuentan con metodología y tratamiento por parte del Proceso.

Análisis del Riesgo

De acuerdo con la guía de administración de riesgos del Departamento Administrativos de la Función Pública el análisis para la identificación del riesgo se realiza determinando las causas, con base en el contexto interno, externo y del proceso ya analizados para la entidad, y que pueden afectar el logro de los objetivos. Algunas causas externas no controlables por la entidad se podrán evidenciar en el análisis de contexto correspondiente, para ser tenidas en cuenta en el análisis y valoración del riesgo.

A partir de este levantamiento de causas se procederá a identificar el riesgo, el cual estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del proceso, es necesario referirse a sus características o las formas en que se observa o manifiesta. En este caso es posible hacer una corta descripción del riesgo dentro de la identificación de acuerdo con sus necesidades de ampliación o compresión del riesgo.

Una vez identificados los riesgos, es necesario Establecer la probabilidad de ocurrencia del riesgo y el nivel de consecuencias o impacto, con el fin de estimar la zona de riesgo inicial.

Este proceso se inicia con la revisión del mapa de procesos de la entidad, donde está contemplado todo el quehacer de la entidad. Los encargados de cada proceso realizan la identificación de los riesgos que sean de su competencia y estos serán diligenciados en el software destinado para este fin, donde no solo se relacionan los riesgos por cada proceso, sino que también se valoran, se establecen los controles y se plantean las acciones que la entidad desarrollara para impedir la materialización del riesgo.

Las Empresas Públicas Municipales de Candelaria ha adquirido el software INTRAFILE ©, que da soporte al sistema de gestión documental y, que cuenta con un módulo específico para la identificación de los riesgos de la entidad, este módulo permite que cada proceso realice la identificación de los riesgos, sistematizando las causas y efectos de los mismos. Adicionalmente de acuerdo con las calificaciones otorgadas y los controles existentes, calcula la valoración de los riesgos en cuanto

probabilidad e impacto. De igual manera, la plataforma INTRAFILE© tiene habilitada la opción de establecer los controles para cada uno de los riesgos y de definir las políticas institucionales, pormenorizando también las actividades que se requieren para llevar a cabo el control, los responsables de ejecutarlas y el tiempo en el que se efectuarán las mismas.

En el aplicativo INTRAFILE©, se realiza la sistematización del análisis de los riesgos, a través de la estimación de la probabilidad de su ocurrencia y el impacto o consecuencias que puede causar su materialización, realizando la calificación y evaluación con el fin de estimar la zona de riesgo inicial, se definen los controles aplicables para evitarlo si el riesgo está en zona baja o para mitigarlo si está en zona alta.

Calificación de los Riesgos.

Se realiza a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del mismo. La probabilidad de ocurrencia representa el número de veces que el riesgo se ha presentado en un determinado tiempo o puede llegar a presentarse y el impacto hace referencia a la magnitud de sus efectos.

Niveles De Aceptación Del Riesgo

Tabla 3. Nivel de aceptación de riesgos en Las Empresas Públicas Municipales de Candelaria.

TIPO DE RIESGO	ZONA DE RIESGO	NIVEL DE ACEPTACIÓN
Riesgos de Corrupción	Moderada	Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo. Periodicidad MENSUAL de seguimiento para evitar a toda costa su materialización por parte de los procesos a cargo de estos y se registra su avance en el aplicativo INTRAFILE ©
	Alta y 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 lugar 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 de este. Periodicidad MENSUAL de seguimiento para evitar a toda costa su materialización por parte de los procesos a cargo de estos y se registra su avance en el aplicativo INTRAFILE ©

Riesgos de Gestión (Proceso, Producto y Proyecto)	Baja	Se incluyen en el Mapa de riesgos Institucional. Se ACEPTARÁ el riesgo y se administra por medio de las actividades propias del proyecto o proceso asociado y MENSUALMENTE se registra su avance en el aplicativo INTRAFILE ©
	Moderada	Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo, se hace seguimiento BIMESTRAL y se registran sus avances en el aplicativo INTRAFILE ©
	Alta y Extrema	Se debe incluir el riesgo tanto en el Mapa de riesgo del Proceso como en el Mapa de Riesgo Institucional y se establecen acciones de Control Preventivas que permitan MITIGAR la materialización del riesgo. Se monitorea MENSUAL y se registran sus avances en el aplicativo INTRAFILE ©
Riesgos de Seguridad de la Información	Baja	Se ACEPTARÁ el riesgo, pero se realizará seguimiento periódico CUATRIMESTRAL por parte del responsable y custodio del activo de información, este seguimiento debe quedar documentado.
	Moderada	Se establecerá plan de acción para control preventivo que permitirá MITIGAR la probabilidad de ocurrencia del riesgo. De acuerdo con la periodicidad establecida en las actividades de control, se realiza monitoreo por parte del responsable y custodio del activo de información. Adicional, se realizarán seguimientos de forma BIMESTRAL, y se registran sus avances en el aplicativo INTRAFILE ©
	Alta y Extrema	Se debe incluir el riesgo tanto en el Mapa de riesgo del Proceso, como en el Mapa de Riesgo Institucional y se establecen acciones de Control Preventivas, con el fin de MITIGAR, TRANSFERIR O EVITAR la materialización del riesgo. Se monitorea de forma MENSUAL, y el equipo de seguridad de la Información de la entidad realiza acompañamiento hasta que la calificación del riesgo sea menor, se registran sus avances en el aplicativo INTRAFILE ©

Tratamiento de los Riesgos

Las acciones para el tratamiento de los riesgos se encuentran definidas en el aplicativo INTRAFILE©, en el módulo de riesgos. Es en este software que Las Empresas Públicas Municipales de Candelaria define las acciones concretas para

el manejo o tratamiento de los riesgos. Se establece si es preventivo (afectan la probabilidad de ocurrencia) o correctivo (afectan el impacto de los riesgos).

Se define el cargo del responsable de ejecutar y/o controlar la acción definida para tal fin y se fijan las fechas para su implementación sin olvidar que también deben velar por el cumplimiento en el desarrollo e implementación de dichas tareas. Se establece la fecha de inicio y la fecha de terminación para la implementación de las acciones de control. Se especifican los indicadores para medir la eficacia de las acciones implementadas.

Metodología de Seguimiento y Registro de Eventos Materializados

Con el propósito de realizar una revisión objetiva de la valoración de los controles de los riesgos de gestión identificados, el aplicativo INTRAFILE ©, guardará el registro, conformando una base de datos sobre eventos de riesgos materializados, la cual permitirá contar con información de tendencias y causas de aquellos presentados, para controlar la ocurrencia futura de los mismos. Respecto de los riesgos de privacidad y seguridad de la información, el seguimiento será realizado por el jefe de control interno.

El reporte de los eventos de riesgos materializados será enviado mediante correo electrónico por el Jefe de control interno avalado por el Líder de Procesos a la gerencia, en el cuál debe informar la situación presentada (incluyendo el análisis de causas respectivo), fecha inicio y fin del suceso, fecha de reporte, riesgo al cual está asociado (opcionalmente), proceso en donde se identificó el suceso, impacto, acciones adelantadas y consecuencias. Este reporte debe realizarse cuando el evento de riesgo materializado se presente.

Partiendo del análisis de causas del evento materializado se debe formular un plan de mejora que indique la corrección o actividades que indiquen la acción de mitigación de este. Sólo para los casos en los cuales ya se tenga un plan de mejora formulado y las acciones correspondan directamente a la mitigación de las causas que motivaron a la materialización del riesgo, se homologará al ya existente y no requerirá formular un nuevo plan de mejora.

La gerencia, debe validar, consolidar y analizar los eventos de riesgos materializados reportados por los procesos, y presentar en los casos requeridos, ante el Comité Institucional de Coordinación de Control Interno aquellos que deban ser de su conocimiento y revisión.

Definición y Aprobación de Planes de Tratamiento de Riesgos de Gestión

Una vez concluidas las etapas de la administración y valoración de los riesgos de gestión de la Entidad, se deben clasificar aquellos riesgos cuya calificación residual se encuentren en Mayor y Catastrófico y por lo anterior queden en zona Alta o Extrema. En estos casos, los procesos en los cuales se obtenga dicha calificación residual deberán formular un plan de tratamiento de riesgos que contenga las acciones requeridas para mitigar de nuevo su ocurrencia e impacto dentro de la Entidad, y presentarlo para conocimiento y aprobación en el Comité Institucional de Coordinación de Control Interno.

Monitoreo y Revisión

El Monitoreo de Riesgos consiste en realizar el seguimiento periódico al comportamiento de los riesgos, los eventos de materialización, el cumplimiento de acciones de manejo determinadas y cuando corresponda al plan de acción asociado.

En ese orden de ideas, se tiene que se debe realizar:

- Consolidación y revisión periódica de la información generada en todas las etapas por parte de la gerencia y el jefe de control interno, como resultado del monitoreo periódico según la tabla 3 – Nivel de aceptación del riesgo.
- Autoevaluación del desempeño por parte de cada líder de proceso, en la cual se realiza la evaluación autónoma del cumplimiento de políticas para la gestión integral de riesgos, la gestión realizada sobre los riesgos que aplican en su dependencia, la identificación y reporte de eventos de materialización, el cumplimiento y eficacia de los controles y opciones de manejo definidos y el análisis de nuevas opciones de manejo que sean necesarias. Esta medición se llevará a cabo de manera mensual y será reportada a la Jefe de control interno.
- Retroalimentación a la Dirección. En el marco del proceso de Evaluación del Sistema de Control Interno, en el ejercicio de la revisión por parte de la gerencia, se presentan y analizan los resultados de la medición del desempeño y los logros en la gestión integral del riesgo. Esta información se consolida y presenta por parte del jefe de control interno, para que a partir de los análisis se tomen las decisiones y acciones necesarias para fortalecer la aplicación de la gestión integral de los riesgos de las Empresas Públicas Municipales de Candelaria.

Divulgación y Consulta.

El jefe de control interno coordinará las acciones necesarias para promover la comunicación de información que promueva la cultura de gestión integral de los riesgos en las Empresas Públicas Municipales de Candelaria.

De igual forma, coordinará la divulgación y publicación de la matriz integral de riesgos, considerando la posibilidad de presentar la matriz integral o vista específica de la misma, las cuales pueden ser por nivel de identificación, por tipo de riesgo, por nivel de severidad del riesgo, o por la clasificación que se considere pertinente, de acuerdo con las necesidades de divulgación y las partes interesadas a quienes se dirija la publicación, principalmente considerando: la página web de la entidad y la intranet, aplicativo INTRAFILE ©.

Productos para la Administración de Riesgos

Mapa institucional de riesgos

Contiene a nivel estratégico los mayores riesgos a los cuales está expuesta la entidad, se alimenta con los riesgos residuales Altos o Extremos de cada uno de los procesos que pueden afectar el cumplimiento de la misión institucional y objetivos de la entidad. En este mapa se deberán incluir los riesgos identificados como posibles actos de Corrupción, en cumplimiento del artículo 73 de la Ley 1474 de 2011 y los riesgos de Seguridad de la Información.

Mapa de riesgos por procesos

Recoge los riesgos identificados para cada uno de los procesos, los cuales pueden afectar el logro de sus objetivos.