OBJETIVO

Establecer los lineamientos generales e instrumentos requeridos para la administración y control de los riesgos que puedan afectar el logro de los objetivos institucionales, con el propósito de Identificar, valorar y clasificar las posibles desviaciones y efectos no favorables para la entidad tomando las acciones correctivas adecuadas y oportunas.

ALCANCE

Los lineamientos de esta política de administración de riesgos, deben aplicarse por parte de los responsables de acuerdo con su rol definido en las líneas de defensa de manera transversal, a los objetivos estratégicos, procesos, planes, programas y proyectos de la Entidad, desde la identificación del contexto del riesgo hasta el seguimiento, tratamiento y comunicación de la información resultante de la administración de este; desarrollado mediante la guía de Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP.

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.
- **Capacidad de riesgo**: Es el máximo valor del nivel de riesgo que una Entidad puede soportar a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.
- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo
- **Causa Inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo
- **Causa Raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.
- **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.
- **Control:** Medida que permite reducir o mitigar un riesgo.
- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.
- **DAFP:** Departamento Administrativo de la Función Pública.
- **Factores de riesgo:** Son las fuentes generadoras de riesgos.
- **Integridad:** Propiedad de exactitud y completitud.
- **Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **MIPG:** Modelo Integrado de Planeación y Gestión.
- **Nivel de riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que

este evento traería sobre la capacidad institucional de alcanzar los objetivos. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto.

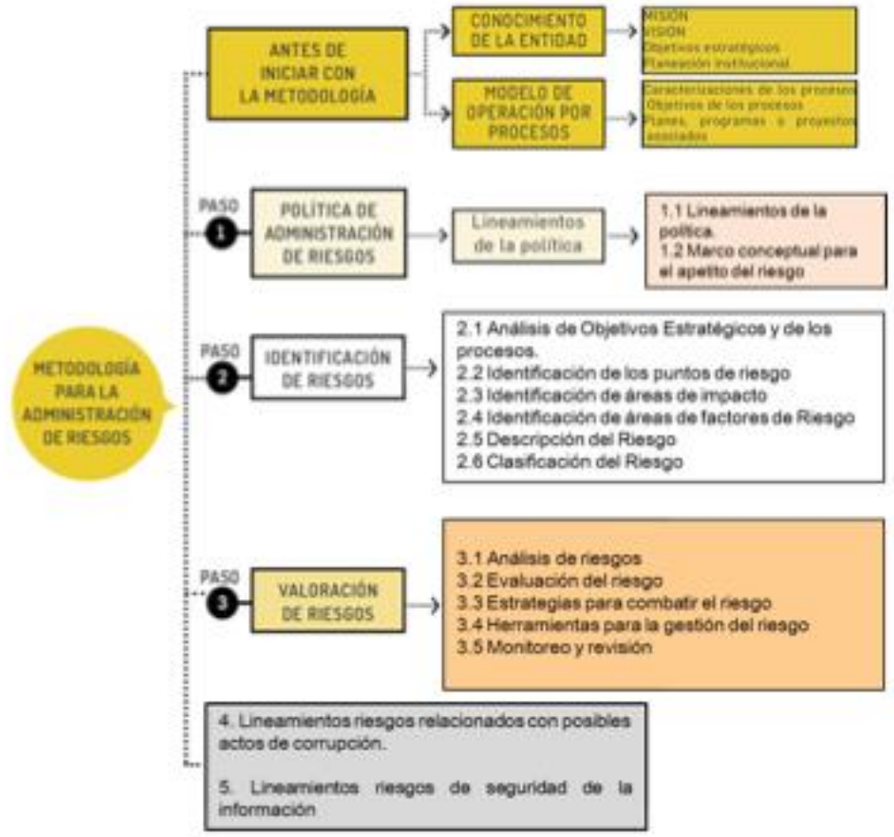
- **Probabilidad:** Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.
- **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.
- **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).
- **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.
- **Tolerancia del riesgo:** Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.
- **Vulnerabilidad:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

ESTRUCTURA PARA LA ADMINISTRACIÓN DE RIESGOS

1. Metodología a utilizar

Comprende, los lineamientos de la política de administración de riesgos, el marco conceptual para el apetito del riesgo, la identificación del riesgo y la valoración del riesgo. El desarrollo de las diferentes etapas que se presentan a continuación se describe de “Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, DAFP.*”.*

Ilustración 1. Metodología para la administración de riesgos



Fuente: DAFP, 2022. Guía para la Administración del Riesgo y diseño de controles en entidades públicas V06

2. Herramientas para la Gestión del Riesgo

La Empresa Municipal de Servicios Públicos Domiciliarios de Piedecuesta E.S.P. Piedecuestana de Servicios Públicos, cuenta con un *"Mapa de Riesgos", GPI-OPI.PAR-210.POL7. F01, como* herramienta asociada. En este se gestionan los riesgos, desde la identificación de los factores de riesgos hasta el respectivo seguimiento de acuerdo con la periodicidad establecida.

3. Identificación del riesgo

Esta etapa tiene como objetivo identificar los riesgos 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.

- **Análisis de objetivos estratégicos y de los procesos:** Todos los riesgos que se identifiquen deben tener impacto en el cumplimiento del objetivo estratégico o del proceso.
- **Identificación de los puntos de riesgo:** Actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

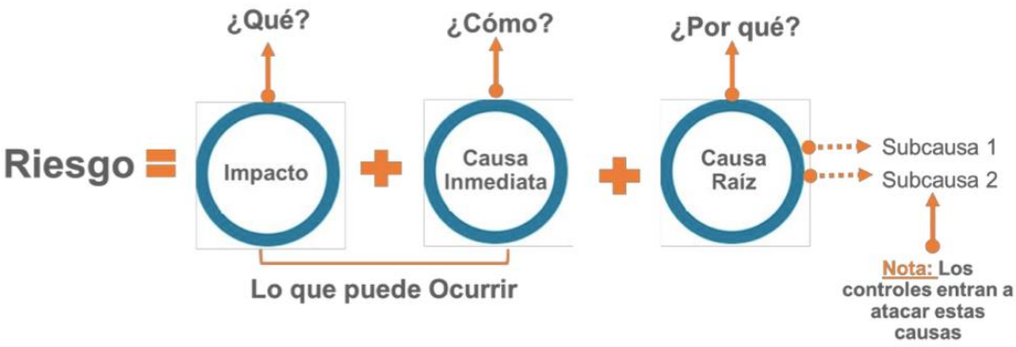
Cra. 8 #12-28, La Candelaria, Piedecuesta
Tel. (607) 6 55 0058
www.piedecuestanaesp.gov.co

- **Identificación de áreas de impacto:** El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta la organización en caso de materializarse un riesgo.

4. Descripción del riesgo:

La descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. Se propone una estructura que facilita su redacción y claridad que inicia con POSIBILIDAD DE y se analizan los siguientes aspectos:

Ilustración 2: Descripción del riesgo



Fuente: DAFP, 2022. Guía para la Administración del Riesgo y diseño de controles en entidades públicas V06

5. Clasificación del riesgo

Una vez descrito el riesgo, se debe seleccionar la clasificación del riesgo según los criterios descritos a continuación:

- **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 estos.
- **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.
- **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.
- **Seguridad de la información:** Posibilidad de que se exploten las vulnerabilidades de los sistemas de información de la organización.
- **Riesgo fiscal:** Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

6. Análisis de Riesgos

En el análisis de riesgos se establece la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (Riesgo Inherente).

6.1. Determinar la probabilidad

Por probabilidad se entiende la posibilidad de ocurrencia del riesgo, 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.

La exposición al riesgo estará asociada a la frecuencia de ejecución de la actividad generadora del riesgo que se esté analizando, es decir, al número de veces que se ejecuta la actividad, y por ende que se pasa por el punto de riesgo en el periodo de 1 año; en la tabla 1 se establecen los criterios para definir el nivel de probabilidad de los riesgos de gestión.

Tabla 1. Criterios para definir el nivel de probabilidad

	Frecuencia de La Actividad	Probabilidad
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces al año.	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces al año.	40%
Media	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces al año.	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 501 veces al año y máximo 5000 veces al año.	80%
Muy alta	La actividad que conlleva el riesgo se ejecuta más de 5001 veces al año.	100%

Fuente: Adaptado de DAFP, 2022. Guía para la Administración del Riesgo y diseño de controles en entidades públicas. V06

6.1.1 Análisis de la probabilidad (Riesgo de corrupción)

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, donde frecuencia implica analizar el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; factibilidad implica analizar 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 es posible que suceda.

Tabla 2. Criterios para calificar la probabilidad (Riesgos de corrupción)

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
5	**Casi seguro**	Se espera que el evento ocurra en la mayoría de las circunstancias.	Más de 1 vez al año.
4	**Probable**	Es viable que el evento ocurra en la mayoría de las circunstancias.	Al menos 1 vez en el último año.
3	**Posible**	El evento podrá ocurrir en algún momento.	Al menos 1 vez en los últimos 2 años.
2	**Improbable**	El evento puede ocurrir en algún momento.	Al menos 1 vez en los últimos 5 años.
1	**Rara vez**	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales).	No se ha presentado en los últimos 5 años.

Fuente: DAFP, 2022. Guía para la Administración del Riesgo y diseño de controles en entidades públicas V06.

6.1.2. Determinar la probabilidad riesgos de seguridad digital

Para esta etapa se asociarán las tablas de probabilidad e impacto definidas para los riesgos de gestión.

6.2. Calificación del Impacto

Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales. En la tabla 3 se establecen los criterios para definir el nivel de impacto.

Tabla 3. Criterios para definir el nivel de impacto

	Afectación económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV.	El riesgo afecta la imagen de algún área de la organización.
Menor 40%	Entre 11 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 51 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 101 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 501 SMLMV.	El riesgo afecta la imagen de la entidad a nivel nacional con efecto publicitario sostenido a nivel país.

Fuente: Adaptado de DAFP, 2022. Guía para la Administración del Riesgo y diseño de controles en entidades públicas, V06

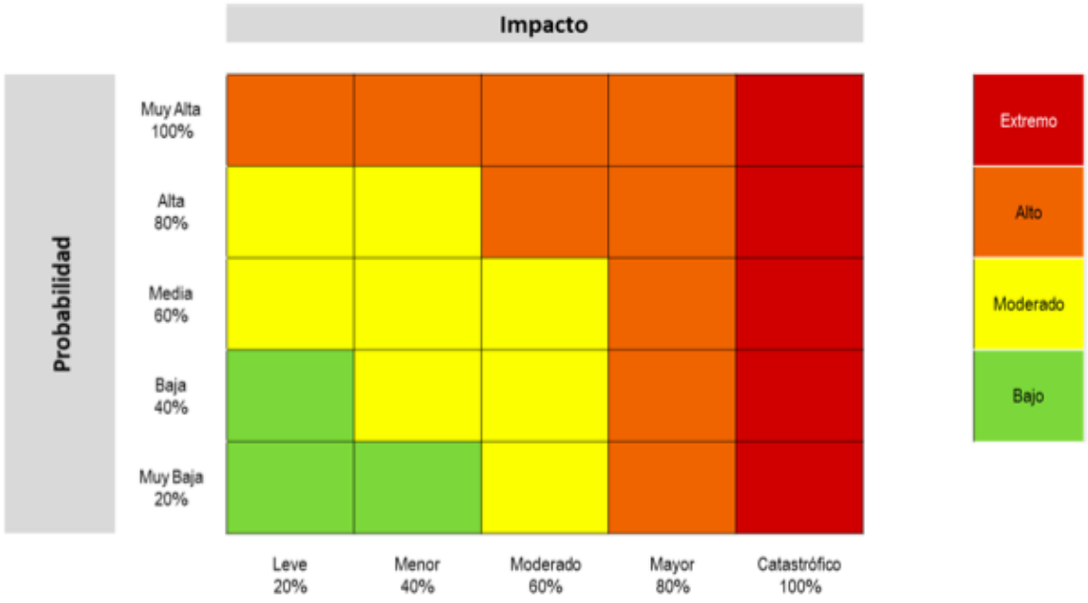
7. Evaluación del riesgo

Se calcula a partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, con esto se determina la zona de riesgo inicial, denominada riesgo inherente.

El riesgo inherente es el 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.

Se definen cuatro zonas de severidad en la matriz de calor, Ver ilustración 3: Mapa de calor para calcular el riesgo inherente. Las zonas de severidad son: Extremo, alto. Moderado y bajo.

Ilustración 3. Mapa de calor para calcular el riesgo inherente



Fuente: Adaptado de DAFP, 2022. Guía para la Administración del Riesgo y diseño de controles en entidades públicas, V06

8. Valoración de controles

Medidas que permiten reducir o mitigar el riesgo, para esto se debe tener en cuenta la identificación de los controles que se deben realizar, los responsables de realizarlo y el tiempo en el que se ejecutarán los controles, para esto, se deben tener en cuenta los siguientes atributos:

8.1. Atributos de eficiencia:

Son medibles, los cuales tienen asignados los siguientes porcentajes:

8.1.1. Tipo de control:

- **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. Al seleccionarlo se obtiene un valor de 25%.
- **Control detectivo:** Control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos. Al seleccionarlo se obtiene un valor de 15%.
- **Control correctivo:** Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos. Al seleccionarlo se obtiene un valor de 10%.

8.1.2. Implementación:

- **Control manual:** Controles que son ejecutados por personas. Al seleccionarlo se obtiene un valor de 15%.
- **Control automático:** Son ejecutados por un sistema. Al seleccionarlo se obtiene un valor de 25%.

8.2. Atributos informativos:

Se determinan para darle formalidad al control y su fin es conocer el entorno y complementar el análisis, sin embargo, al no tener valor porcentual no tienen una incidencia directa en su efectividad:

8.2.1. 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.

8.2.2. 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.

8.2.3. 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.

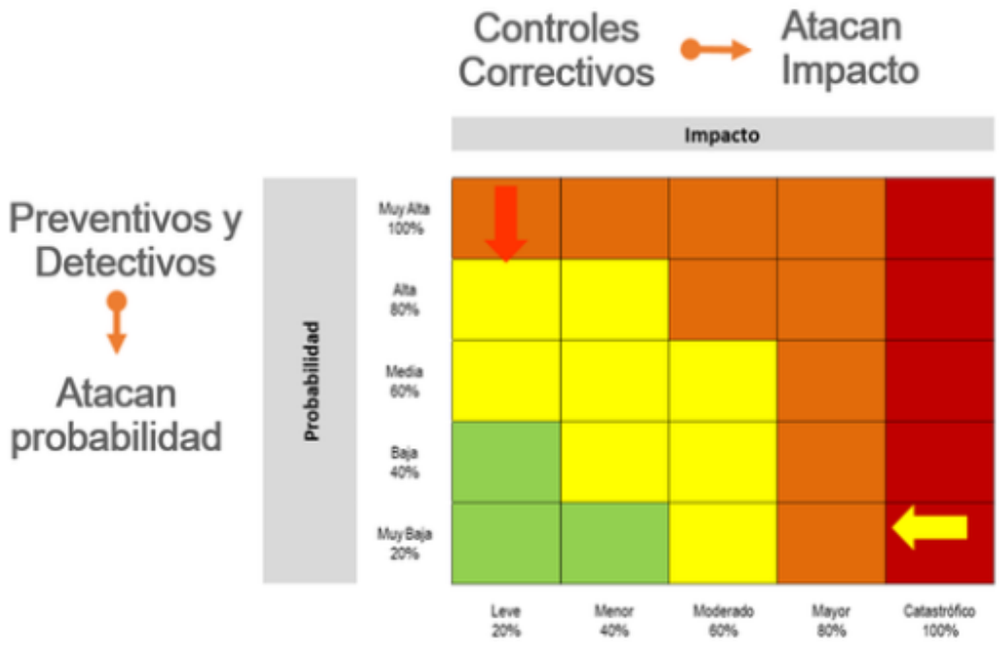
9. Cálculo del riesgo residual

Se analizan los atributos de controles teniendo en cuenta las características relacionadas anteriormente. Los controles mitigan el riesgo de forma acumulativa, por lo tanto, el valor que se aplica en uno de los controles impacta directamente con el riesgo residual.

El riesgo residual surge del resultado de aplicar la efectividad de los controles al riesgo inherente.

Cra. 8 #12-28, La Candelaria, Piedecuesta
Tel. (607) 6 55 0058
www.piedecuestanaesp.gov.co

Ilustración 4. Mapa de calor para calcular el riesgo residual



Fuente: Adaptado de DAFP, 2022. Guía para la Administración del Riesgo y diseño de controles en entidades públicas, V06

10. Medidas de Tratamiento de Riesgo

El objetivo de esta etapa es identificar las opciones para tratar los riesgos de acuerdo con el nivel de riesgo residual obtenido, esto para procesos en funcionamiento, pero cuando se trate de procesos nuevos se procede a partir del riesgo inherente.

Dentro de las actividades a desarrollar en esta etapa se encuentra la de identificar y formalizar las opciones de tratamiento adecuadas, dentro de las cuales se encuentran:

- **Reducir:** Después de realizar un análisis y considerar que el nivel de riesgo es alto, se determina tratarlo mediante un plan de acción.

- **Mitigar:** Después de realizar un análisis y considerar los niveles de riesgo se implementan acciones que mitiguen el nivel de riesgo. No necesariamente es un control adicional.

- **Aceptar:** Después de realizar un análisis y considerar los niveles de riesgo se determina asumir el mismo conociendo los efectos de su posible materialización.

- **Evitar:** Después de realizar un análisis y considerar que el nivel de riesgo es demasiado alto, se determina no asumir la actividad que genera este riesgo.

Nota 1: Para los riesgos de corrupción, la respuesta será evitar, compartir o mitigar el riesgo. Nunca se debe aceptar.

Nota 2: Cuando un riesgo de corrupción se encuentre en zona de riesgo (**Moderado:** 3, **Rara Vez:** 1), no aplicarán las opciones de tratamiento compartir o reducir el riesgo, ya que en este caso el riesgo se encontrará en su máxima disminución posible dentro del mapa de calor.

11. Periodicidad para el monitoreo, revisión, actualización y seguimiento de los riesgos

El monitoreo y revisión de los riesgos corresponde a la Primera Línea de Defensa como un seguimiento constante a la gestión del riesgo y a la efectividad de los controles establecidos. Por otra parte, el monitoreo y revisión realizado por los lideres de área se realizará de manera formal cuatrimestral, y la validación del avance de la ejecución de las acciones realizada por la Oficina de Control Interno se lleva a cabo en los siguientes cortes:

- **Primer monitoreo**: Con corte al 30 de abril, y corresponderá al seguimiento en el proceso de formulación y actualización cada año, si se requiere, de los mapas de riesgos de cada proceso. En esa medida, la publicación deberá surtirse una vez se realice la verificación y validación de los soportes aporta por los diferentes procesos. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.

- **Segundo monitoreo**: Con corte al 31 de agosto, la publicación deberá surtirse una vez se realice la verificación y validación de los soportes aportados por los diferentes procesos. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.

- **Tercer monitoreo:** Con corte al 31 de diciembre, la publicación deberá surtirse una vez se realice la verificación y validación de los soportes aportados por los diferentes procesos. Donde se realizará el cierre de la vigencia la publicación deberá surtirse una vez se realice la verificación y validación de los soportes aportados por los diferentes procesos en el mes de enero. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero del siguiente año.

El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano.

El mapa de riesgos será revisado anualmente con el fin de identificar posibles cambios, en caso de que se presenten modificaciones, estas serán revisadas y aprobadas por el Comité de Gestión y Desempeño para su actualización.

12. Líneas de Responsabilidad frente a la gestión del riesgo.

Las responsabilidades se definen mediante la línea estratégica y las tres líneas de defensa las cuales se encuentran definidas en la siguiente tabla:

Tabla 4. Responsabilidades

Líneas de Defensa	Responsables	Operatividad
Línea estratégica	Alta Dirección y Comité Institucional de Coordinación de Control Interno.	Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento.
		Analiza los riesgos y amenazas institucionales al cumplimiento de los planes estratégicos.
1ª. Línea de Defensa	Líderes de proceso, programas y proyectos y sus equipos (En general servidores públicos de todos los niveles de la organización).	Desarrollar e implementar procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora, reportando a la segunda línea sus avances o dificultades.
		Diseñar, implementar y monitorear los controles y gestionar de manera directa en el día a día los riesgos de la entidad.
		Asimismo, orientar el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la entidad, emprender las acciones de mejoramiento para su logro.
2ª. Línea de Defensa	A cargo de los servidores que tienen responsabilidades directas de monitoreo y revisión de los controles de la gestión del riesgo: Jefe de planeación, supervisores o interventores de proyectos, coordinadores de otros sistemas de gestión de la entidad, coordinadores de equipos de trabajo, comités institucionales, directores de área, entre otros que generen información para el Aseguramiento de la operación.	Monitorear la gestión de riesgos y control ejecutada por la primera línea de defensa complementando su trabajo.
		Asegurar 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 eficaces, de gestión de riesgo.
		Consolidan y analizan información sobre temas clave para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos.
		Asesorar a la 1ª línea de defensa en temas clave para el Sistema de Control Interno: i) riesgos y controles; ii) planes de mejoramiento; iii) indicadores de gestión; iv) procesos y procedimientos.

3ª. Línea de defensa	A cargo de la Oficina de Control Interno, Auditoría Interna o quién haga sus veces.	Proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del Sistema de Control Interno.
		El alcance de este aseguramiento, a través de la auditoría interna, cubre todos los componentes del Sistema de Control Interno.
		Genera a través de su rol de asesoría un orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Oficina Asesora de Planeación o quien haga sus veces.
		Monitorear la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo.
		Brinda un nivel de asesoría proactiva y estratégica, frente a la Alta Dirección y los líderes de proceso.

Fuente: Construcción propia 2022

13. Comunicación

Esta estrategia de comunicación busca socializar e interiorizar en todos los servidores públicos y terceros que presten sus servicios a la Empresa Municipal de Servicios Públicos Domiciliarios de Piedecuesta E.S.P. Piedecuestana de Servicios Públicos, de los distintos niveles de responsabilidad, sobre la importancia de la gestión del riesgo así:

- **Nivel institucional**: Se publicará en la página web de la Entidad. Así mismo, de acuerdo con los niveles de responsabilidad establecidos en las líneas de defensa, el monitoreo y revisión por parte de la primera y segunda línea de defensa y, seguimiento por parte de la tercera línea de defensa.
- **Nivel de procesos**: Teniendo en cuenta las responsabilidades sobre una base del día a día estará a cargo de los líderes de proceso y consiste en realizar la divulgación de los mapas de riesgos por proceso al interior de sus respectivos equipos de trabajo.

14. Materialización del riesgo

La materialización de un riesgo representa una amenaza real al cumplimiento de los objetivos institucionales, por lo que resulta fundamental contar con un lineamiento claro sobre las acciones que deben ejecutarse en estos casos. Una respuesta oportuna, organizada y basada en procedimientos previamente establecidos permite contener los impactos negativos, mitigar daños adicionales, identificar las causas que originaron el evento y fortalecer los controles existentes. Esta capacidad de reacción no solo protege los recursos y la reputación de la entidad, sino que también fortalece la cultura de gestión del riesgo y mejora la toma de decisiones futuras. A continuación, se presentan los pasos a seguir una vez se identifique la materialización del riesgo (ya sean del proceso o de

corrupción):

Tabla 5. Actividades de materialización del riesgo

Actividad	Responsable	Evidencia
Iniciar una notificación inmediata a las partes responsables	Líder del proceso, Oficina de Control Interno.	Correo electrónico
Realizar un análisis de los impactos reales (económicos, reputacionales, operativos) generados por la materialización del riesgo.	Líder del proceso y jefe o director del área.	Mapa de riesgos
Identificar la causa raíz del evento.	Líder del proceso y jefe o director del área.	Mapa de riesgos
Implementar medidas inmediatas para mitigar daños adicionales (por ejemplo: aislamiento de sistemas, suspensión de actividades, etc.).	Líder del proceso y jefe o director del área.	Mapa de riesgos
Monitorear el cumplimiento de las acciones correctivas.	Oficina control interno – Líder del proceso	Mapa de riesgos
Evaluar la efectividad de los controles actualizados.	Oficina control interno – Líder del proceso	Mapa de riesgos

15. Bibliografía

- DAFP. (2022). Guía para la administración del riesgo y el diseño de controles en entidades públicas Bogotá: Departamento Administrativo de la Función Pública. V06
- NTC-ISO 31000. (2018). Gestión del riesgo. Principios y directrices. Icontec Internacional.
- Decreto 2641 de 2012. Por el cual se reglamentan los artículos 73 y 76 de la Ley 1474 de 2011.
- Decreto 1499 de 2017 Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública
- Decreto 1122 de 2024: Programa de transparencia y ética pública.

COMPROMISO DE LA ALTA DIRECCION

La política de gestión de riesgos establecida por la Empresa Municipal de Servicios Públicos Domiciliarios de Piedecuesta E. S. P. refleja el nivel de compromiso hacia el logro de sus metas estratégicas y su plan de acción.

Esta política orienta los procesos hacia la adopción de un enfoque basado en riesgos, lo cual permite anticipar, reducir y mitigar el efecto de situaciones inesperadas.

Esta política se fundamenta en la "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas" versión 6, emitida por el Departamento Administrativo de la Función Pública y el Departamento Nacional de Planeación.

Fredy Johany Zambrano Becerra
Gerente
Mayo de 2025

Cra. 8 #12-28, La Candelaria, Piedecuesta
Tel. (607) 6 55 0058
www.piedecuestanaesp.gov.co