Dirección
Planeación

POLÍTICA
DE OPERACIÓN DEL RIESGO

TABLA DE CONTENIDO

1 RESPONSABLE DEL DOCUMENTO

Dirección de Planeación

2 OBJETIVOS

2.1 GENERAL

Establecer una orientación metodológica que facilite la comprensión y operación del riesgo de gestión, corrupción, fiscal y de seguridad de la información con el fin de asegurar el cumplimiento de la misión institucional, los compromisos del Plan de Desarrollo Departamental PDD, los objetivos del Plan Estratégico - PE y de los procesos institucionales mediante la identificación, valoración y control del riesgo que incluye el análisis, evaluación, monitoreo y revisión con el propósito de contar con herramientas que permitan anticiparse a posibles situaciones que afecten el cumplimiento de la misión y objetivos estratégicos de la empresa.

2.2 ESPECÍFICOS

- Proteger los activos de la entidad, asegurándolos contra la materialización de los riesgos y amenazas identificadas.
- Implementar procesos y controles que permitan realizar una adecuada administración del riesgo, evitando en lo posible su materialización.
- Ofrecer herramientas para identificar, analizar, evaluar los riesgos y determinar roles y responsabilidades de cada uno de los actores de la entidad (esquema de las líneas de defensa) en los riesgos.
- Establecer, mediante una adecuada administración del riesgo, una base confiable para la toma de decisiones y para la planeación institucional.

3 ALCANCE

Aplica a todos los procesos, programas, proyectos y productos, conforme al modelo de operación por procesos de Empresas Públicas de Cundinamarca S.A E.S.P., incluidos los controles para mitigar el daño al patrimonio público, conforme a cada tipo y clasificación de riesgos, bajo la responsabilidad de los líderes de procesos y líneas de defensa.

4 NORMATIVIDAD APLICABLE

- 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.
- Directiva presidencial 09 de 1999, Lineamientos para la implementación de la política de lucha contra la corrupción.
- Decreto 1599 de 2005, Por el cual se adopta el Modelo Estándar de Control Interno para el Estado colombiano y se presenta el anexo técnico del MECI 1000:2005. 1.3 Componentes de administración del riesgo.
- Ley 1474 de 2011. Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
- Decreto 403 de 2020. Por el cual se dictan normas para la correcta implementación del Acto Legislativo 04 de 2019 y el fortalecimiento del control fiscal.
- Guía para la Administración del Riesgo y el Diseño de Controles en entidades Públicas Versión 6 - DAFP 2022

5 DEFINICIONES

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.

Administración del riesgo: Conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.

Amenaza: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Análisis del riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel del riesgo.

Apetito de riesgo: Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

Bien público: Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales, definidos así:

- **Bien de uso público:** Aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. Ejemplos: Las calles, plazas, puentes, vías, parques etc.
- **Bienes fiscales:** Aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades. Ejemplos: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.

Calificación del riesgo: estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.

Capacidad de riesgo: Es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos 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 impacta en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Control: Medida que permite reducir o mitigar un riesgo.

Control fiscal Interno (CFI): Primer nivel para la vigilancia fiscal de los recursos públicos y para la prevención de riesgos fiscales y defensa del patrimonio público. El Control Fiscal Interno, hace parte del Sistema de Control Interno y es

responsabilidad de todos los servidores públicos y de los particulares que administran recursos, bienes, e intereses patrimoniales de naturaleza pública y de las líneas de defensa, en lo que corresponde a cada una de ellas. El Control Fiscal Interno es evaluado por la Contraloría respectiva, siendo dicha evaluación determinante para el fenecimiento de la cuenta.

Control fiscal Multinivel: Es la articulación entre el sistema de control interno (primer nivel de control) y el control externo (segundo nivel de control), con la participación activa del control social.

Descripción del Riesgo: Redacción que facilite el entendimiento el entendimiento del riesgo tanto para el líder del proceso como para personas ajenas al proceso, es importante dar respuesta al ¿Qué?, ¿Cómo? Y ¿Por qué?

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

Efecto: es el daño que se generaría sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, en caso de ocurrir el evento potencial.

Evaluación del riesgo: Análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto determinando la zona de riesgo.

Evento Potencial: Hechos inciertos o incertidumbres, refiriéndonos a riesgo fiscal, se relaciona con una potencial acción u omisión que podría generar daño sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública. En esta guía, el evento potencial es equivalente a la causa raíz.

Factores de Riesgo: Son las fuentes generadoras de riesgos.

Gestión de riesgos: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Gestor Fiscal: Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes.

Identificación del riesgo: Proceso que posibilita conocer los eventos potenciales, que estén o no bajo el control de la organización, para ello se debe tener en cuenta

el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también, el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

Impacto: Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Integridad: Propiedad de exactitud y completitud.

Matriz de riesgos: herramienta de registro del análisis de riesgos, que sirve para evaluar la probabilidad y la gravedad del riesgo. Incluye la calificación del impacto de cada riesgo, las cuales ayudan a determinar la prioridad de tratamiento, determinar los controles y definir las acciones para abordarlos y gestionarlos de manera efectiva.

Mitigación: Son todas las medidas que se llevan a cabo para limitar o reducir la materialización de un riesgo.

Monitorear: observar, analizar, verificar y evaluar los riesgos identificados, determinando el adecuado desarrollo de cada una de las etapas de administración y el nivel de cumplimiento y efectividad de los controles y acciones definidas.

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.

Patrimonio público: se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C- 340-07).

Programa de Transparencia y Ética Pública: Programa de cumplimiento que las entidades públicas deben implementar para promover una cultura de legalidad, transparencia y rendición de cuentas. El PTEP busca identificar, medir, controlar y monitorear los riesgos de corrupción y otros riesgos para la integridad en el ejercicio de la función pública.

Política de Administración del Riesgo: Declaración de la Dirección y las intenciones generales de una organización con respecto a la gestión del riesgo, (NTC ISO31000 Numeral 2.4). La gestión o Administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.

Probabilidad: Se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

Riesgos 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 gestión: Posibilidad de que suceda algún evento que tendrá un efecto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

Riesgo de seguridad de la información o digital: 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 Fiscal: Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

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 escala de severidad.

Riesgo Residual: El resultado de aplicar la efectividad de los controles al riesgo inherente.

Vulnerabilidad: Representa la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

6 CONDICIONES GENERALES

En Colombia a través del Decreto 1083 de 2015 el Estado refiere con relevancia la necesidad de que las entidades oficiales cuenten con una política de administración del riesgo, que establezca los parámetros para el control de los mismos, con el

propósito de tener el control pertinente para el logro eficiente de los objetivos institucionales y contar con estrategias para enfrentar cualquier contingencia que se pueda presentar. Por lo tanto, en EPC se define el presente documento con el fin de establecer los mecanismos para el adecuado manejo y control de los riesgos tanto negativos, como positivos (oportunidades)

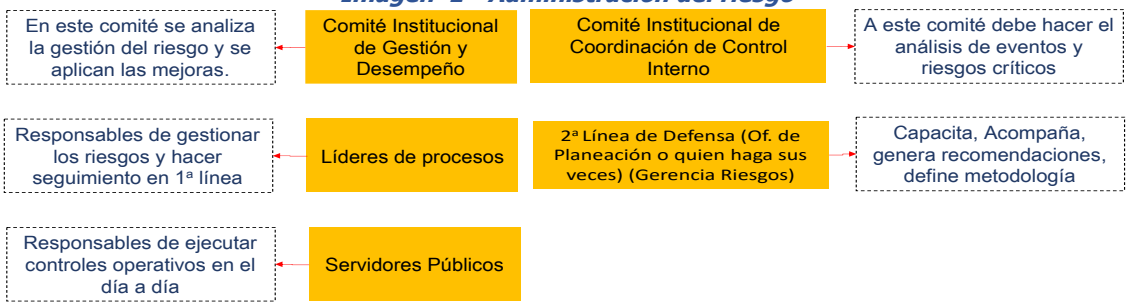
La administración de riesgos requiere establecer un proceso sistemático para identificar, analizar, evaluar y controlar los riesgos que pueden afectar la operación o las estrategias de la Empresa, para minimizar las pérdidas y maximizar las oportunidades, asegurando que los objetivos se alcancen de manera efectiva; por lo tanto, debe ser iterativo para que genere una cultura de autocontrol y autoevaluación.

6.1 INSTITUCIONALIDAD PARA LA ADMINISTRACIÓN DEL RIESGO

Considerando que la gestión del riesgo es un proceso efectuado por la alta dirección y por todos los servidores públicos y contratistas de Empresas Públicas de Cundinamarca S.A. E.S.P., con el propósito de proporcionar en el desarrollo de su gestión, un aseguramiento razonable con respecto al logro de los objetivos, se debe tener en cuenta los siguientes beneficios:

- Apoyo a la toma de decisiones
- Fortalecimiento en la operación organizacional
- Minimizar la probabilidad e impacto de los riesgos
- Mejoramiento en la calidad de procesos (la calidad va de la mano con la gestión del riesgo)
- Fortalecimiento de la cultura de control
- Controla fuga de capital intelectual de la empresa
- Incrementa la capacidad de la empresa para alcanzar sus objetivos
- Dota a la empresa de herramientas y controles para hacer una administración más eficaz y eficiente.

Imagen 1 - Administración del riesgo



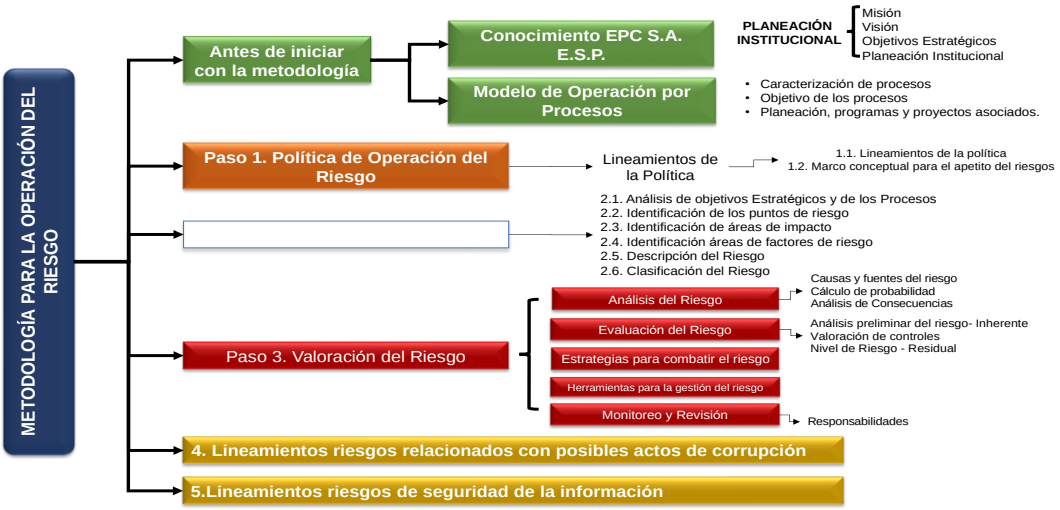
Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

6.2 METODOLOGÍA PARA LA GESTIÓN DEL RIESGO

Empresas Públicas de Cundinamarca S.A. E.S.P. establece la metodología para la gestión del riesgo previo al análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión, además del conocimiento de la metodología desde un punto de vista estratégico, de la aplicación de tres (3) pasos básicos para su desarrollo y finalmente, de la definición e implantación de estrategias de comunicación transversales a toda la administración para que su efectividad pueda ser evidenciada.

6.1 Estructura con su desarrollo básico

Imagen 2 - Estructura de la metodología para la gestión del riesgo



6.3 LINEAMIENTOS DE LA POLÍTICA DE OPERACIÓN DE RIESGOS

Para Empresas Públicas de Cundinamarca S.A ESP, la Política de Operación de Riesgos se define según los parámetros del Modelo Integrado de Planeación y Gestión-MIPG Dimensión de Direccionamiento Estratégico - adoptado mediante decisión empresarial 028 de 2018 y 025 de 2021, el cual esta articulado con los requisitos de las Normas Técnicas ISO 9001:2015, ISO 14001:2015 e ISO 45001:2018, para lo cual toma como referente la estructura de alto nivel y por consiguiente las líneas de defensa para la operación frente a los riesgos de gestión, fiscales, corrupción y de seguridad de la información.

La presente política involucra todos los procesos y dependencias, quienes 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 del Plan Estratégico, mediante:

- El establecimiento de acciones de control detectivas y preventivas para los riesgos identificados conforme al modelo de operación por procesos y en especial con tendencias a riesgos con trazabilidad de la información y a la identificación de riesgos jurídicos.
- La actuación correctiva y oportuna ante la materialización de los riesgos identificados.

Para operar adecuadamente los riesgos Empresas Públicas de Cundinamarca S.A ESP, determina las acciones para asumir, reducir y mitigar el riesgo al igual que establece acciones de contingencia en caso de que se presente la materialización de estos.

De igual forma, la presente guía de operación de riesgos involucra acciones frente riesgos relacionados con la fuga de capital intelectual de la entidad y llevar a cabo acciones para evitar la pérdida de conocimiento.

6.3.1 Aplicabilidad de la política de operación de riesgos

La política de riesgos es aplicable a todos los procesos, proyectos, productos y/o servicios de Empresas Públicas de Cundinamarca S.A E.S.P., y a las acciones ejecutadas por los servidores públicos durante el desarrollo de sus funciones en cumplimiento de los objetivos institucionales.

6.3.2 Determinación de la capacidad de riesgo

Empresas Públicas de Cundinamarca S.A E.S.P., aplica los valores de probabilidad e impacto sugeridos mediante metodología suministrada por el Departamento Administrativo de la Función Pública (DAFP), contenidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas, la cual tiene como base la NTC ISO 31000:2018 con lo cual determina, bajo la participación y aprobación de la alta dirección en el marco del comité institucional de coordinación de control interno, teniendo en cuenta los siguientes valores:

- Valor máximo de la escala que resulta de combinar la probabilidad y el impacto.
- Valor máximo que, según el buen criterio de la alta dirección y bajo los requisitos del marco legal aplicable a la misión de Empresas Públicas de Cundinamarca S.A E.S.P., puede ser resistido antes de perder total o parcialmente la capacidad de cumplir con sus objetivos. Este valor se denomina "capacidad de riesgo".

De esta manera, la capacidad institucional de riesgo, para el tipo de riesgo en análisis, es el máximo valor del nivel de riesgo que EPC S.A. E.S.P. puede soportar y a partir del cual se considera por la alta dirección que no sería posible el logro de los objetivos institucionales.

6.3.3 Determinación del apetito de riesgo

El valor máximo deseable del nivel de riesgo que podría permitir el logro de los objetivos institucionales en condiciones normales de operación del Modelo Integrado de Planeación y Gestión se denomina "apetito de riesgo", dado que equivale al nivel de riesgo que EPC S.A. E.S.P., puede aceptar, relacionado con sus objetivos, el marco legal y las disposiciones de la alta dirección, es así, como en EPC determinó que los riesgos de corrupción y aquellos riesgos en zonas extrema, alta y moderada no son aceptadas y deben tratarse, por su parte, los riesgos en zona baja serán aceptados.

6.3.4 Tolerancia del riesgo

La tolerancia de riesgo es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por EPC S.A. E.S.P.

Para determinar la tolerancia de riesgo, se debe definir un valor que es igual o superior al apetito de riesgo y menor o igual a la capacidad de riesgo.

El límite o valor de la tolerancia de riesgo es definido por la alta dirección y no puede ser superior al valor de la capacidad de riesgo.

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

La política de gestión de riesgos de Empresas Públicas de Cundinamarca S.A. E.S.P., genera un entorno permanente de lucha y cero tolerancias contra la corrupción, integrando sus procesos con enfoque a la prevención y detección de hechos asociados a este fenómeno, tomando las medidas necesarias para combatirlo mediante la aplicación de los requisitos de la presente política de gestión de riesgos la cual cuenta con un carácter estratégico y está fundamentada en el Modelo Integrado de Planeación y Gestión MIPG, con un enfoque preventivo de evaluación

permanente sobre la gestión y el control, el mejoramiento continuo y con la participación de todos los servidores públicos y contratistas y el análisis de los siguientes riesgos:

- Riesgos de gestión de proceso bajo el efecto que se causa sobre los objetivos de EPC S.A. E.S.P., debido a eventos potenciales.
- Los riesgos de posibles actos de corrupción a través de la prevención de la ocurrencia de eventos en los por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- Los riesgos de seguridad de la información como la 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 27001).
- Los Riesgos de Contratación CCE como los eventos que pueden afectar la realización de la ejecución contractual y cuya ocurrencia no puede ser predicha de manera exacta por las partes involucradas en el proceso de contratación.
- Riesgo Fiscal con el efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

6.4 LAS LÍNEAS DE DEFENSA

La presente política involucra la gestión de los servidores públicos y contratistas Empresas Públicas de Cundinamarca S.A. E.S.P., permitiendo la identificación, el análisis, la valoración, el tratamiento, el registro y el seguimiento de las acciones con el fin de mitigar los riesgos que pudieran afectar el logro de los objetivos por proceso y por ende los institucionales.

6.4.1 Línea estratégica

La Alta Dirección, representada en el Comité Institucional de Coordinación de Control Interno y en el Comité de Gestión y Desempeño como línea estratégica, define el marco general para la gestión del riesgo y supervisa su cumplimiento.

6.4.2 Primera Línea de defensa

A cargo de: gerente, subgerentes y directores, líderes de los procesos, programas y proyectos de la Empresa, cuyo **rol principal** es diseñar, implementar y monitorear los controles y gestionar de manera directa en el día a día los riesgos de Empresa; así mismo, debe orientar el desarrollo e implementación de: políticas y procedimientos internos, asegurar que éstos sean compatibles con las metas y objetivos de la Empresa y emprender las acciones de mejoramiento para su logro.

6.4.3 Segunda línea de defensa

A cargo de los servidores públicos que tienen responsabilidades directas en el monitoreo y evaluación de los controles y la gestión del riesgo.

Responsables: Líder de Planeación, supervisores e interventores de contratos o proyectos, responsables de otros sistemas de gestión de la Empresa, comités de riesgos (donde existan), comités de contratación, entre otros.

El **rol principal** de esta línea es: Soportar y guiar la línea estrategia y la primera línea de defensa en la gestión adecuada de los riesgos a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos, y lleva a cabo un monitoreo independiente al cumplimiento de las etapas de la operación de riesgos.

6.4.4 Tercera línea de defensa

A cargo de la Dirección de Control Interno; tiene como **rol principal**: proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primera y segunda línea de defensa cumplan con sus responsabilidades en la operación de riesgos.

El alcance de este aseguramiento, a través de la auditoría interna cubre todos los componentes del Sistema de Control Interno.

7. IDENTIFICACIÓN DEL RIESGO

En esta etapa Empresas Públicas de Cundinamarca S.A. E.S.P., identifica los riesgos que estén o no bajo el control, para ello se debe tener en cuenta el contexto estratégico en el que opera la empresa, 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.

7.1 Análisis de objetivos Estratégicos

Empresas Públicas de Cundinamarca S.A. E.S.P., debe analizar los objetivos estratégicos e identificar los posibles riesgos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso.

Es necesario revisar que los objetivos estratégicos se encuentren alineados con la misión y la visión institucional, así como, analizar su adecuada formulación, es decir, que contengan las siguientes características mínimas:

- Específico
- Medible
- Alcanzable
- Relevante
- Proyectado en el tiempo

7.2 Análisis de objetivos de los procesos

Los objetivos por proceso deben ser analizados con base en las características mínimas explicadas en los objetivos estratégicos, además, se debe revisar que los mismos estén alineados con la Misión y la Visión, es decir, asegurar que los objetivos de proceso contribuyan a los objetivos estratégicos.

7.3 Identificación de los puntos de riesgo

Dentro de la gestión por procesos que desarrolla Empresas Públicas de Cundinamarca S.A. E.S.P., se verifica si existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo y que estos deban mantenerse bajo control para asegurar que el o los procesos cumplan con su objetivo.

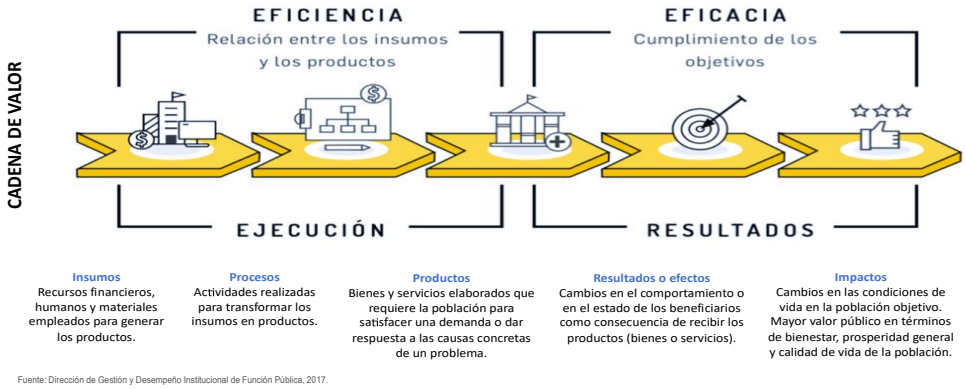


Imagen 3 - Cadena de valor en la identificación de puntos de control

7.4 IDENTIFICACIÓN DE ÁREAS DE IMPACTO

El área de impacto es la consecuencia económica o reputacional a la cual se ve expuesta Empresas Públicas de Cundinamarca S.A. E.S.P., en caso de materializarse

un riesgo. Los impactos que aplican son afectación económica (o presupuestal) y reputacional.

Dentro del contexto de riesgo fiscal, el área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público, a la cual se vería expuesta EPC S.A. E.S.P., en caso de materializarse el riesgo.

Es importante, tener en cuenta que no todos los efectos económicos corresponden a riesgos fiscales, pero todos los riesgos fiscales (efecto dañoso sobre bienes o recursos o intereses patrimoniales de naturaleza publica) representan un efecto económico.

Son ejemplo de efectos económicos que no son riesgos fiscales, los siguientes:

- (i) Los riesgos de daño antijurídico, riesgo de pago de condenas y conciliaciones.
- (ii) Los efectos económicos generados por causas exógenas, es decir, no relacionadas con acción u omisión de los gestores públicos, como son hechos de fuerza mayor, caso fortuito o hecho de un tercero (es decir, de alguien que no tenga la calidad de gestor público).
- Otro aspecto, que es fundamental para definir de manera correcta el impacto al momento de identificar y redactar riesgos fiscales, es tener claro el concepto de patrimonio público, así como el de las tres expresiones de patrimonio público que se derivan del artículo 6 de la Ley 610 de 2000: (i) bienes públicos; (ii) recursos públicos o (iii) intereses patrimoniales de naturaleza pública.

7.5 CLASIFICACIÓN DE RIESGOS

Ejecución y administración de procesos: Pérdidas derivadas de errores en la ejecución y administración de procesos. - **Factor de Riesgo: Proceso**

Fraude externo: Pérdidas derivada de actos de fraude por personas ajenas a la organización (no participa personal de EPC S.A. E.S.P.). - **Factor de Riesgo: Evento externo**

Fraude Interno: Pérdidas debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de EPC S.A. E.S.P., en las cuales está involucrado por lo menos 1 participante interno de EPC S.A. E.S.P., son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros. - **Factor de Riesgo: Evento externo.**

Fallas tecnológicas: Errores en hardware, software, telecomunicaciones, interrupción de servicios básicos. - **Factor de Riesgo: Tecnológico.**

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. - **Factor de Riesgo: Varios factores.**

Usuarios, productos y prácticas: Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos. - **Factor de Riesgo: Varios factores.**

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. - **Factor de Riesgo: Infraestructura – Evento Externo.**

Relación ente factores de riesgo y clasificación del riesgo

Tabla 1 - Relación ente factores de riesgo y clases del riesgo

Clasificación	Factores de Riesgo
Ejecución y administración de procesos	Procesos
Fraude externo	Eventos externos
Fraude Interno	Talento humano
Fallas tecnológicas	Tecnología
Relaciones laborales	Pueden asociarse a varios factores
Usuarios, productos y prácticas	
Daños a activos fijos	Infraestructura
	Eventos externos

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas V.6

7.5.1 RIESGO FISCAL

Para la identificación del **riesgo fiscal** es necesario establecer los puntos de riesgo y las circunstancias inmediatas.
Los puntos de riesgos: Son situaciones en las que potencialmente se genera riesgo fiscal, es decir, son aquellas actividades de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos, así como a la recaudación, manejo e inversión de sus rentas.

En conclusión, los puntos de riesgo fiscal son todas las actividades que representen gestión fiscal, así mismo, se deben tener en cuenta aquellas actividades en las cuales se han generado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal.

Las circunstancias inmediatas: se trata de aquella situación o actividad bajo la cual se presenta el riesgo, pero no constituyen la causa principal o básica - causa raíz - para que se presente el riesgo; es necesario resaltar que, por cada punto de riesgo fiscal, existen múltiples circunstancias inmediatas.

Tabla 2 - Pautas para identificación de riesgos fiscales

SIRVE PARA IDENTIFICAR	PREGUNTAS Y RESPUESTAS PARA LA IDENTIFICACIÓN
Puntos de riesgo fiscal	¿En qué procesos de la entidad se realiza gestión fiscal? (ver capítulo inicial la definición de gestión fiscal).
Puntos de riesgo fiscal y circunstancias inmediatas	Clasifique por procesos (según mapa de procesos de la empresa), los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal y/o los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector y/o las advertencias de la Contraloría General de la República y/o las alertas reportadas en el Sistema de Alertas de Control Interno.
	Nota 1: Para este efecto se recomienda consultar los hallazgos con presunta incidencia fiscal y los fallos con responsabilidad fiscal de los últimos 5 años.
	Nota 2: Los hallazgos fiscales de los últimos años y las advertencias que se hayan emitido en relación con la gestión fiscal de la entidad, se obtienen de la matriz de plan de mejoramiento institucional y de los históricos, información con la que cuenta la Oficina de Control Interno o quien haga sus veces.
	Nota 3: Los fallos con responsabilidad fiscal en firme son información pública, a la cual se puede acceder mediante solicitud de información y documentos (derecho de petición) ante el o los entes de control fiscal que vigilen a la entidad respectiva o al sector que esta pertenece. Estos precedentes son muy importantes para conocer las causas raíz (hechos generadores) por los que se ha fallado con responsabilidad en los últimos años y así implementar los controles adecuados para

SIRVE PARA IDENTIFICAR	PREGUNTAS Y RESPUESTAS PARA LA IDENTIFICACIÓN
	atacar de forma preventiva esas causas y evitar efectos dañosos sobre los recursos, bienes o intereses patrimoniales del Estado.
	Nota 4: La organización y agrupación por procesos (según el mapa de procesos de la entidad) de los hallazgos con presunta incidencia fiscal identificados por el ente de control fiscal, los fallos con responsabilidad fiscal en firme relacionados con hechos de la entidad o del sector, las advertencias de la Contraloría General de la República y las alertas reportadas en el Sistema de Alertas de Control Interno -SACI-, es una labor de la segunda línea de defensa, específicamente de la Oficinas de Planeación o quien haga sus veces, con la asesoría de la Oficina de Control Interno o quien haga sus veces.
Circunstancias inmediatas	En un ejercicio autocritico, realista y objetivo, ¿Cuáles son las causas de los hallazgos fiscales identificados por el ente de control fiscal y/o de los fallos con responsabilidad fiscal relacionados con hechos de la entidad o del sector y/o las advertencias de la oficina de control interno, en los últimos 3 años?
	Nota: Se recomienda no copiar las causas escritas por el órgano de control en el hallazgo, salvo que luego del análisis propio la entidad concluya que la causa del hallazgo es la identificada por el órgano de control.
Puntos de riesgo fiscal y circunstancias inmediatas	¿Qué puntos de riesgo fiscal y circunstancias inmediatas del "¿Catálogo Indicativo y Enunciativo de Puntos de riesgo fiscal y Circunstancias Inmediatas" (anexo1), son aplicables a la entidad?

7.5.2 RIESGO DE GESTIÓN

Para la identificación del **riesgo de gestion** es necesario establecer los puntos de riesgo y las circunstancias inmediatas, para la cual debe tener en cuenta lo siguiente.

7.5.2.1 Identificación de áreas de factores de riesgo

Son las fuentes generadoras de riesgos y de las cuales se debe tener en cuenta la siguiente clasificación:

Tabla 3 - Factores de riesgo

FACTOR	DEFINICIÓN	DESCRIPCIÓN
Procesos	Eventos relacionados con errores en las actividades que deben realizar los servidores públicos.	Falta de procedimientos
		Errores de grabación, autorización
		Errores en cálculos para pagos internos y externo.
		Falta de capacitación, temas relacionados con el personal
Talento humano	Incluye seguridad y salud en el trabajo. Se analiza posible dolo e intención frente a la corrupción.	Hurto activos
		Posibles comportamientos no éticos de los empleados
		Fraude interno (corrupción, soborno)

FACTOR	DEFINICIÓN	DESCRIPCIÓN
Tecnología	Eventos relacionados con la infraestructura tecnológica	Diseño de equipos
		Caída de aplicaciones
		Caída de Redes
		Errores en programas
Infraestructura	Eventos relacionados con la infraestructura física	Incendios
		Inundaciones
		Daños a activos fijos
Eventos Externos	Situaciones externas que externo afectan a EPC S.A. E.S.P.	Suplantación de identidad
		Asalto a la oficina
		Atentados, vandalismo, orden público

7.5.3 RIESGO DE SEGURIDAD DE LA INFORMACIÓN

Para el caso de los **RIESGOS DE SEGURIDAD DE LA INFORMACIÓN** debe tener en cuenta que estos están articulados con el modelo de seguridad y privacidad de la información (MSPI), el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital.

Para realizar la identificación del riesgo primero debe realizar la identificación de los activos de seguridad de la información.

Tabla 4 - Identificación de riesgos de seguridad de la información

¿Qué son Activos de seguridad de la información?	¿Por qué Identificarlos?
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 cada entidad y sus procesos 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 digital.

Una vez se haya realizado la identificación de los activos de información se puede proceder a realizar la identificación del riesgo, tenga en cuenta que se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad de la información:

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

Para cada riesgo se deben asociar el grupo de activos o activos específicos del proceso, y conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización. Para este efecto, es necesario consultar el "Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas".

A continuación, se presenta un ejemplo de la identificación del riesgo sobre un activo de información.

Tabla 5 - Ejemplo identificación riesgo de seguridad de la información

RIESGO	ACTIVO	DESCRIPCIÓN DEL RIESGO	AMENAZA	TIPO	CAUSAS/ VULNERA-BILIDADES	CONSECUENCIAS
Base de datos de nómina	Pérdida de la integridad	La falta de políticas de seguridad digital, ausencia de políti-cas de control de acceso, contraseñas sin protección y mecanismos de autenticación débil, pueden facilitar una modificación no autorizada, lo cual causaría la pérdida de la integridad de la base de datos de nómina.	Modificación no autorizada	Seguridad digital	Falta de políticas de seguridad digital	Posibles consecuencias que pueda enfrentar la entidad o el proceso a causa de la materialización del riesgo(legales, económicas, sociales, reputacionales, confianza en el ciudadano). Ej.: posible retraso en el pago de nómina.
					Ausencia de políticas de control de acceso	
					Contraseñas sin protección	
					Autenticación débil	

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas V.6

7.6 IDENTIFICACIÓN DE LA CAUSA RAÍZ O POTENCIAL HECHO GENERADOR

La causa raíz sería cualquier evento potencial (acción u omisión) que de presentarse provocaría un menoscabo, disminución, perjuicio, detrimento, pérdida o deterioro.

La causa raíz o potencial hecho generador y el efecto dañoso (daño) guardan entre sí una relación de causa/efecto. En este sentido, la determinación de la causa raíz o

potencial hecho generador se logra estableciendo la acción u omisión o acto lesivo del patrimonio de EPC S.A. E.S.P.

Para Empresas Públicas de Cundinamarca S.A. E.S.P., una adecuada gestión de riesgos exige que la identificación de causas sea especialmente objetiva y rigurosa, ya que los controles que se diseñen e implementen deben apuntarle a atacar dichas causas, para así lograr prevenir la ocurrencia de daños.

Siendo la causa raíz un elemento tan relevante para la eficaz gestión de riesgos, es importante tener claridad al respecto de qué es y qué no es una causa raíz o potencial hecho generador.

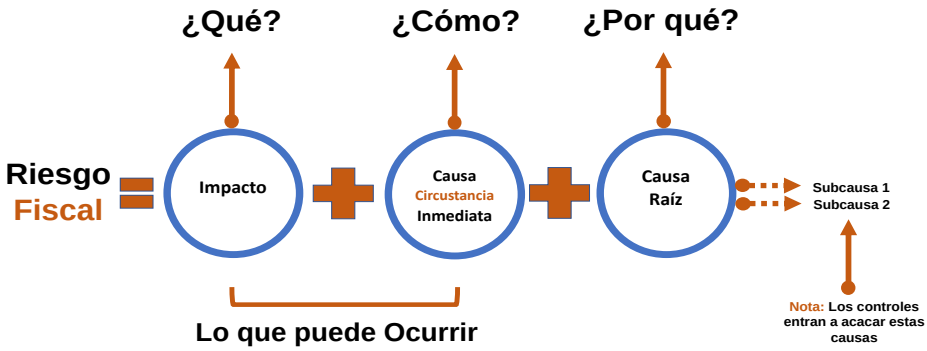
Es fundamental, entonces, tener claro que debe deslindarse el hecho que ocasiona el daño (hecho generador-causa raíz o causa adecuada), del daño propiamente dicho. En otras palabras, uno es el hecho generador -causa-, y otro es el daño -efecto-. Ver Tabla 1 - Pautas para identificación de riesgos.

7.8 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 la frase POSIBILIDAD DE y se analizan los siguientes aspectos:

Tabla 6 - Estructura propuesta para la redacción del riesgo



POSIBILIDAD DE… + Impacto para la entidad (Qué) + Causa Inmediata (Cómo) + Causa Raíz (Por qué)

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas V.6

Para redactar un riesgo se debe tener en cuenta:

- Iniciar con la oración: Posibilidad de, debido a que nos estamos refiriendo al evento potencial.
- Impacto: Corresponde al **¿qué?:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- Circunstancia inmediata: Corresponde al **¿cómo?:** Se refiere a aquella situación por la que se presenta el riesgo; pero no constituye la causa principal o básica - causa raíz- para que se presente el riesgo.
- Causa Raíz: Corresponde al **¿por qué?:** que es el evento (acción u omisión) que de presentarse es causante, es decir, generador directo, causa eficiente o adecuada. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera.

Para redactar un riesgo fiscal se debe tener en cuenta la siguiente estructura:

POSIBILIDAD DE + Impacto para la entidad (Qué) efecto dañoso sobre bienes públicos + Causa Inmediata (Cómo) por pérdida de bienes muebles de EPC S.A. E.S.P. + Causa Raíz (Por qué) a causa de la omisión en la aplicación del procedimiento para el ingreso y salida de bienes conforme a controles del proceso de gestión de recursos físicos.

8. VALORACIÓN DEL RIESGO

Imagen 4 - Valoración de riesgos

Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2018.

8.1 Análisis del riesgo

Para efectos de este análisis, la probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo,

la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Tabla 7 - Actividades relacionadas con la gestión del riesgo en entidades públicas

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 y Cartera	Semanal	Alta
*Tecnología (incluye disponibilidad de aplicativos) **Nota:** En materia de tecnología se tiene en cuenta 1 hora funcionamiento= 1 vez. Ej.: El aplicativo FURAG está disponible durante 2 meses las 24 horas, en consecuencia su frecuencia se calcula 60 días * 24 horas= 1440 horas.	Diaria	Alta

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas V.6

8.2 Determinar la probabilidad

Teniendo en cuenta lo explicado en el punto anterior sobre el nivel de probabilidad, la exposición al riesgo estará asociada al proceso o actividad que se esté analizando, es decir, al número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

8.2.1 Nivel de calificación de probabilidad

Tabla 8 - Calificación de la probabilidad

NIVEL	PROBABILIDAD	DESCRIPCIÓN
20%	Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año – 20%año.
40%	Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año – 40%año.
60%	Media	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año – 60%
80%	Alta	La actividad que conlleva el riesgo se ejecuta mínimo 501 veces al año y máximo 5000 veces por año – 80%
100%	Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año – 100% año.

8.3 Determinar el impacto

Para la construcción de la tabla de criterios se definen los impactos económicos y reputaciones como las variables principales. (afectaciones a la ejecución presupuestal, pagos por sanciones económicas, indemnizaciones a terceros, sanciones por incumplimientos de tipo legal; así como afectación a la imagen institucional por vulneraciones a la información o por fallas en la prestación del servicio).

Nota: *Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferente niveles se debe tomar el nivel más alto, así por ejemplo: para un riesgo identificado se define un impacto económico en nivel insignificante e impacto reputacional en nivel moderado, se tomará el más alto, en este caso sería el nivel moderado.*

8.3.1 Niveles de calificación del impacto

Tabla 9 - Impacto

Nivel	Impacto	Descripción Económica o Presupuestal	Descripción Reputacional
20%	Leve	Pérdida económica menor a 10 SMLMV	Solo de conocimiento de algunos funcionarios.
40%	Menor	Pérdida económica Entre 11 y 50 SMLMV	De conocimiento general de la entidad a nivel interno, Gerencia y Comités
60%	Moderado	Pérdida económica Entre 51 y 100 SMLMV	Deterioro de imagen con algunos usuarios de relevancia frente a cumplimiento de objetivos. Deterioro de imagen con algunos usuarios de relevancia frente a cumplimiento de objetivos.
80%	Mayor	Pérdida económica Entre 101 y 500 SMLMV	Deterioro de imagen con efecto publicitario sostenido a nivel Territorial.
100%	Catastrófico	Pérdida económica Mayor a 500 SMLMV	Deterioro de imagen a nivel Nacional con efecto publicitario sostenido a nivel Nacional

La calificación del impacto para los riesgos de **corrupción** se realiza aplicando la siguiente tabla de valoración establecida por Secretaria de Transparencia de la Presidencia de la Republica. Cada riesgo identificado es valorado de acuerdo con las preguntas, la tabla y la calificación obtenida se compara con la tabla de medición de impacto de riesgo de corrupción para obtener el nivel de impacto del riesgo.

Tabla 10 - Calificación de impacto para los riesgos de corrupción

DETERMINACIÓN DEL IMPACTO		R1	
Nº	PREGUNTA Si el riesgo de corrupción se materializa podría…	RESPUESTA	
		AFIRMATIVAS	NEGATIVAS
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 pérdidas de confianza en 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 deterioro de calidad de vida de la comunidad por la pérdida del bien o servicios o los 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?		
TOTAL			
PUNTAJE			

Nº	DESCRIPCIÓN	RESPUESTAS AFIRMATIVAS	
1	Genera un impacto moderado sobre EPC S.A. E.S.P.	1 a 5	
2	Genera un impacto mayor EPC S.A. E.S.P.	6 a 11	
3	Genera un impacto catastrófico para EPC S.A. E.S.P.	12 a 19	
MODERADO	Genera medianas consecuencias sobre EPC S.A. E.S.P.		
MAYOR	Genera altas consecuencias sobre EPC S.A. E.S.P.		

Fuente: *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6 - Dirección de Gestión y Desempeño Institucional Noviembre 2022*

9. EVALUACIÓN DE RIESGOS

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

9.1 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

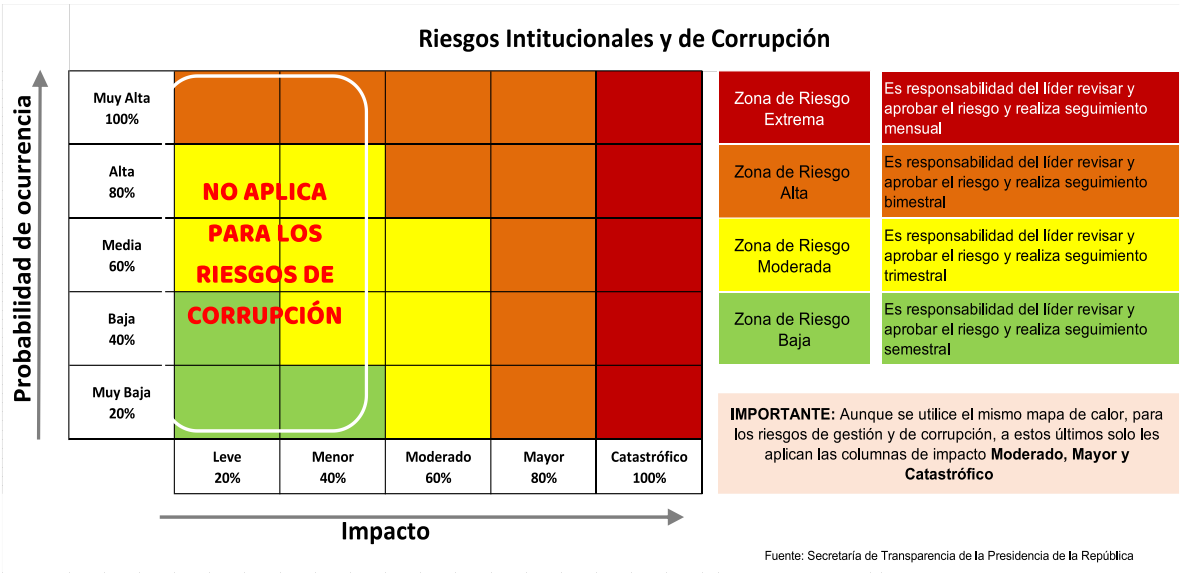
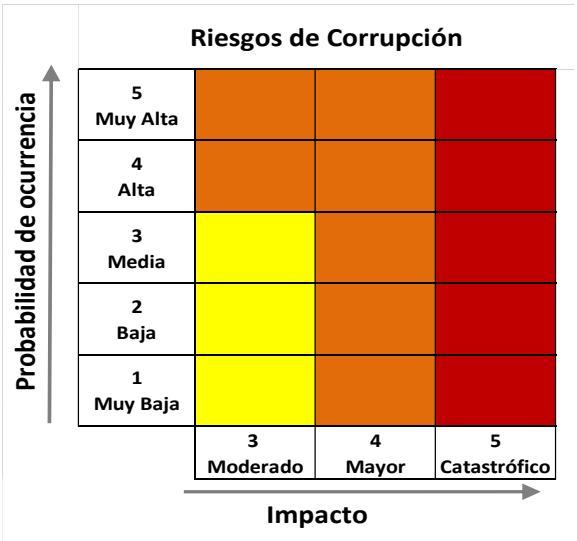


Imagen 5 - Calificación riesgos de corrupción



Nota: *Es necesario mencionar, que esta matriz de severidad está diseñada de acuerdo a estándares internacionales que permiten tener trazabilidad en los desplazamientos en cada zona, por lo que se recomienda no modificarla.*

Fuente: *Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6 - Dirección de Gestión y Desempeño Institucional Noviembre 2022*

9.2 Niveles de aceptación o de tolerancia al riesgo

Para riesgos de gestión y de seguridad digital, se consideran aceptables o tolerables los que se ubiquen en zonas de riesgo inherente o residual baja; para los cuales es optativo la definición de acciones para el tratamiento o abordaje de riesgos.

Son inaceptables o intolerables los riesgos de corrupción en cualquier zona de riesgo inherente o residual.

10. VALORACIÓN DE CONTROLES

En primer lugar, conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los lideres de procesos o servidores públicos expertos en su quehacer.
- Los responsables de implementar y monitorear los controles son los lideres de proceso con el apoyo de su equipo de trabajo.

10.1 Estructura para la descripción del control

Responsable de ejecutar el control: Identifica el cargo del servidor público 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.

10.2 Tipología de controles

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

Control defectivo: 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.

10.3 Análisis y evaluación de los controles – Atributos

Se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización. Es necesario tener en cuenta la descripción y peso asociados a cada uno, para lo cual se registra de la siguiente manera:

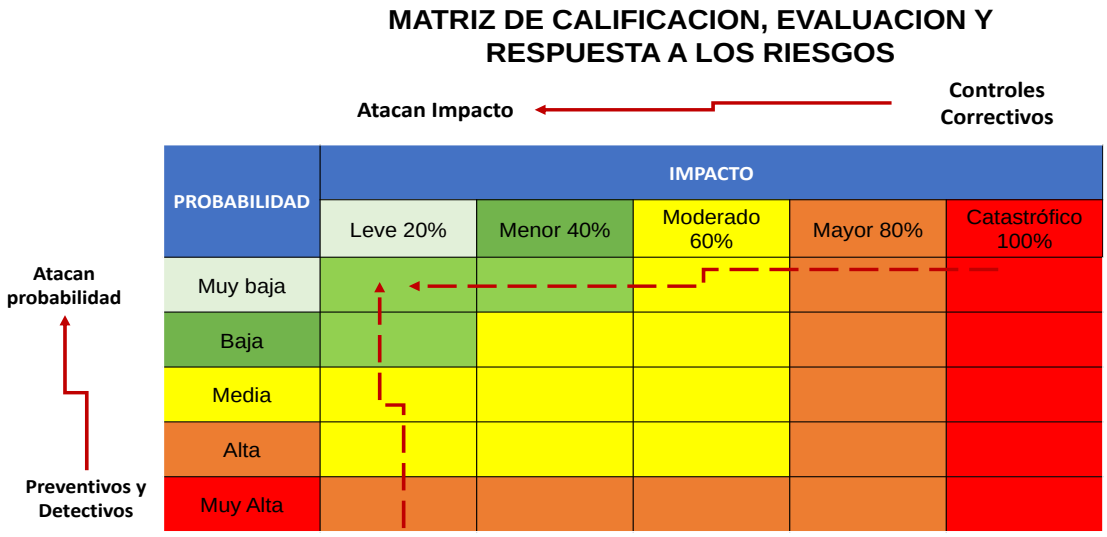
Imagen 6 – Atributos para el diseño del control

CARACTERÍSTICAS			DESCRIPCIÓN	PESO
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado.	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se pueden generar reprocesos.	15%
		Correctivo	Dado que permiten reducir el impacto de la materialización del riesgo, tienen un costo en su implementación.	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización.	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito 15% 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.	

Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

Teniendo en cuenta que es a partir de los controles que se dará el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

Imagen 7 - Calificación de riesgos



Para el caso de los **riesgos de seguridad de la información**, el nivel de probabilidad e impacto no se evalua después de controles

.

11. ROLES Y RESPONSABILIDADES

LÍNEA ESTRATÉGICA

- Establece y aprueba la Política de administración del riesgo la cual incluye los niveles de responsabilidad y autoridad con énfasis en la prevención del daño antijurídico.
- Analiza los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la gestión de EPC S.A. E.S.P., y que puedan generar cambios en la estructura de riesgos y sus controles.
- Realiza seguimiento y análisis periódico a los riesgos institucionales.
- Realimenta sobre los ajustes que se deban hacer frente a la gestión del riesgo.
- Evalúa el estado del sistema de control interno y aprueba las modificaciones, actualizaciones y acciones de fortalecimiento del mismo.

PRIMERA LÍNEA

Servidores en sus diferentes niveles, especialmente subgerente y directores líderes de los procesos, programas y proyectos de la empresa.

- Conocer y apropiar las políticas, procedimientos, manuales, protocolos y otras herramientas que permitan tomar acciones para el autocontrol en sus puestos de trabajo.
- Identifica riesgos y establece controles, asi como realiza su seguimiento, acorde con el diseño de dichos controles, evitando la materialización de los riesgos.
- Define, aplica y hace seguimiento a los controles para mitigar los riesgos identificados alineado con las metas y objetivos institucionales y propone mejoras a la gestión del riesgo en su proceso
- Reaiza seguimiento y control a la ejecución de los controles aplicados por los servidores públicos dentro de su gestión, identificando las deficiencias de los controles y determina las acciones de mejora a que haya lugar.
- Desarrolla acciones de autoevaluación enfocados a la eficiencia, eficacia y efectividad de los controles.
- Informa a la oficina de planeación (segunda línea) sobre los riesgos materializados en los programas, proyectos, planes y/o procesos a su cargo.
- Reporta los avances y evidencias de la gestión de los riesgos a cargo de los procesos asociados.

SEGUNDA LÍNEA

Director de planeación, subgerentes y directores quienes realizan labores de supervisión sobre temas transversales y rinden cuentas ante la Gerencia.

- Asesora 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.
- Asegura que los controles y procesos de gestión del riesgo sean apropiados y funcionen correctamente.
- Consolida el Mapa de riesgos institucional (riesgos de mayor criticidad frente al logro de los objetivos) y lo presenta para análisis y seguimiento ante el Comité de Gestión y Desempeño Institucional.
- Presenta 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 EPC S.A. E.S.P.
- Acompaña, orienta y capacita a los líderes de procesos en la identificación, análisis y valoración del riesgo.
- Monitorea los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de procesos.
- Supervisa en coordinación con los demás responsables de esta segunda línea de defensa que la primera línea identifique, evalué y gestione los riesgos y controles para que se generen acciones.
- Evalúa que los riesgos sean consistentes con la presente política de EPC S.A. E.S.P., promueve acciones de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles.
- Identifica cambios en la gestión del riesgo, especialmente en aquellos riesgos ubicados en zona baja y presenta para aprobación del comité institucional de Coordinación de Control Interno.
- Monitorea los riesgos identificados y controles establecidos por la primera línea de defensa acorde con la estructura de los temas a su cargo.
- Reporta a la Oficina de Planeación o quien haga sus veces, el seguimiento efectuado al mapa de riesgos a su cargo y propone las acciones de mejora a que haya lugar.
- Acompaña, orienta y capacita 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.
- Hace seguimiento a la identificación, evaluación y gestión de los riesgos en los temas de su competencia por parte de la primera línea de defensa.

TERCERA LÍNEA

Dirección de Control Interno o quien haga sus veces

- Apoya sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos.
- Evalúa de manera independiente y objetiva sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primera y segunda línea de defensa cumplan con sus responsabilidades en la operación de riesgos
- Proporciona aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa.
- Asesora de forma coordinada con el área de planeación o quien haga sus veces, a la primera línea de defensa en la identificación de los riesgos institucionales y diseño de controles.
- Hace el seguimiento a los riesgos consolidados en los mapas de riesgos de conformidad con el Plan Anual de Auditoria y reporta los resultados.

12. ACCIONES ANTE LOS RIESGOS MATERIALIZADOS

Tabla 11 – Actividades de contingencia ante la materialización de riesgos

TIPO DE RIESGO	RESPONSABLE	ACCIÓN DE CONTROL
Riesgos de Corrupción	Líder de proceso	Informar al Jefe de Control Interno sobre el hecho encontrado
		Una vez surtido el conducto regular establecido por EPC S.A. E.S.P., y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante la instancia de control correspondiente.
		Identificar las acciones correctivas necesarias y documentarlas en el Plan de mejoramiento
		Efectuar el análisis de causas y determinar acciones de mejora.
		Actualizar el mapa de riesgos.
	Oficina de control interno	Informar al Líder del proceso, quien analizará la situación y definirá las acciones a que haya lugar.
		Una vez surtido el conducto regular establecido por EPS S.A E.S.P., y dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante la instancia de control correspondiente.
		Informar a la segunda línea de defensa con el fin de facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar y de ser necesario actualizar el mapa de riesgos

TIPO DE RIESGO	RESPONSABLE	ACCIÓN DE CONTROL
Riesgos de Proceso/Proyecto/Producto (Zona Extrema, Alta y Moderada)	Líder de proceso	Implementar el plan de contingencia que permita la continuidad o prestación del servicio, documentar en el Plan de mejoramiento.
		Iniciar el análisis de causas y determinar acciones de mejora, documentar.
		Replantear los riesgos del proceso.
		Analizar y actualizar el mapa de riesgos.
		Informar a la línea Estratégica y primer línea de defensa, sobre el hallazgo y las acciones tomadas.
Riesgos de Proceso/Proyecto/Producto (Zona Baja)	Líder de proceso	Establecer acciones correctivas al interior de cada proceso, a cargo del líder respectivo y verificar la calificación y ubicación del riesgo para su inclusión en el mapa de riesgos.
Riesgos de Proceso/Proyecto/Producto (Zona Extrema, Alta y Moderada) **Riesgos de Proceso/Proyecto/Producto (Zona Baja)**	Oficina de control interno	Informar al lieder del proceso sobre el hecho encontrado.
		Informar a la segunda línea de defensa con el fin facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos.
		Acompañar al líder del proceso en la revisión, análisis y toma de acciones correspondientes para resolver el hecho.
		Verificar que se tomaron las acciones y se actualizó el mapa de riesgos correspondiente.

13. MONITOREO, SEGUIMIENTO Y CONTROL DE RIESGOS

ACOMPAÑAMIENTO DEL ÁREA DE PLANEACIÓN O QUIEN HAGA SUS VECES

- Reconocer la metodología, lineamientos del líder frente al riesgo y objetivo, alcance, planes del proceso.
- Participar de las mesas de trabajo para la identificación/validación de los riesgos del proceso.
- Registrar en la herramienta los pasos requeridos por la metodología para la identificación, calificación, valoración de los riesgos.
- Redactar y calificar las acciones de control para los riesgos conforme a los requerimientos de la metodología.
- Determinar los responsables de las acciones y las fechas de realización.
- Elaborar el mapa de riesgos de proceso con toda la información respectiva.
- Presentar la propuesta para aprobación del líder del proceso.
- Una vez aprobado, comuníquelo al interior del proceso para asegurar el compromiso de todos los responsables definidos.

SEGUIMIENTO A LAS ACCIONES DE CONTROL DEL RIESGO EN CADA PROCESO

Según la periodicidad definida para cada riesgo, verifique las acciones y registre el avance junto con la evidencia en el respectivo mapa de riesgos. Tenga en cuenta la fecha Inicio y fecha fin establecida para su implementación.

- Analice los resultados del seguimiento y establezca acciones inmediatas ante cualquier desviación.
- Comunique al líder del proceso las desviaciones del riesgo según el nivel de aceptación del riesgo.
- Documente las acciones de corrección o prevención en el plan de mejoramiento.
- Revise y actualice el mapa de riesgo cuando se modifique las acciones o ubicación del riesgo.

PERIODO DE REVISIÓN RIESGOS INSTITUCIONALES

Los riesgos asociados al logro de los objetivos de los procesos institucionales, se identifican y/o validan en cada vigencia a través de la metodología propia de Función Pública.

14. DOCUMENTOS ASOCIADOS

- PDE-F300 Mapa del Riesgos Institucionales
- PDE-F301 Gestión para la administración del riesgo
- PDE-F419 Mapa de Riesgos de Gestión y de Seguridad de la Información

CONTROL DE CAMBIOS DEL DOCUMENTO

CONTROL DE CAMBIOS				
VERSIÓN	**FECHA**	**DESCRIPCIÓN DEL CAMBIO**	**RESPONSABLE**	**CARGO**
1	03/06/2025	Versión inicial	Diego Ernesto Guevara	Director de Planeación

PROYECTÓ	REVISÓ	APROBÓ
Nombre: Luis Alfredo Mendoza	Nombre: Lida Santos Rojas	Nombre: Diego Ernesto Guevara
Cargo: Contratista Asesor Planeación	Cargo: Contratista coordinación SIGC	Cargo: Director Planeación
Subgerencia/Dirección: Planeación	Subgerencia/Dirección: Planeación	Subgerencia/Dirección: Planeación
Fecha: 23/04/2025	Fecha: 02/05/2025	Fecha: 03/06/2025