
	EMPRESAS PÚBLICAS DEL QUINDIO EPQ SA ESP			
	POLITICA PARA LA GESTIÓN DE RIESGOS			
Código: DE-D-05	Versión: 06	Fecha emisión: 02/05/2023	Página: 1 de 17	DOCUMENTO CONTROLADO

"Empresas Públicas del Quindío, EPQ S.A. E.S.P., establece su compromiso para gestionar todos aquellos riesgos que representen una amenaza para la organización, a través del fortalecimiento de la cultura de autocontrol y la adopción de metodologías y herramientas prácticas y de fácil comprensión que permitan ser certeros en su tratamiento, contribuyendo efectivamente al logro de las metas institucionales".

1- Objetivos

- Establecer una adecuada gestión de los riesgos con la efectiva utilización de las Líneas de Defensa, a través de la identificación de acciones de control, respuestas oportunas y estrategias Institucionales ante las situaciones que puedan afectar el cumplimiento de la misionalidad y el logro de objetivos institucionales, disminuyendo las potenciales consecuencias negativas, reduciendo las vulnerabilidades ante las amenazas internas y externas o mejorando las capacidades institucionales de respuesta a eventos identificados o inesperados que afecten al talento humano, la infraestructura tecnológica o los servicios esenciales de los que depende la Entidad.
- Aumentar la probabilidad de alcanzar los objetivos y metas institucionales y proporcionar a la entidad un aseguramiento razonable con respecto al logro de los mismos.
- Ser conscientes de la necesidad de identificar y tratar los riesgos en todos los niveles de la organización.
- Involucrar y comprometer a todos los funcionarios y/o contratistas de Empresas Públicas del Quindío, E.P.Q S. A E.S.P, en la búsqueda de acciones encaminadas a prevenir y administrar los riesgos.
- Cumplir con los requisitos legales y reglamentarios pertinentes aplicables.
- Establecer una base confiable para la toma de decisiones y la planificación.
- Asignar y usar eficazmente los recursos para el tratamiento del riesgo.
- Mejorar la eficacia y eficiencia operativa.
- Mejorar el aprendizaje y la flexibilidad organizacional.



	EMPRESAS PÚBLICAS DEL QUINDIO EPQ SA ESP			
	POLITICA PARA LA GESTIÓN DE RIESGOS			
Código: DE-D-05	Versión: 06	Fecha emisión: 02/05/2023	Página: 2 de 17	DOCUMENTO CONTROLADO

2- Alcance.

La administración de los riesgos es aplicable para todos los procesos de Empresas Públicas del Quindío, E.P.Q S.A E.S.P, los cuales dan respuesta al direccionamiento estratégico y requisitos legales establecidos en el documento "Procedimiento para la administración del riesgo".

3-Responsables.

- La alta dirección de la entidad deberá liderar el proceso de administración de riesgos acorde con la legislación vigente aplicable y la normatividad interna.
- el comité de gestión y desempeño aprobará los procedimientos generales de administración de riesgos para tratar los más importantes de cada proceso.
- Los líderes de procesos con sus respectivos equipos de trabajo, serán los responsables de la identificación, valoración, tratamiento y seguimiento a las acciones y controles de los riesgos definidos, así como de velar por la eficacia de éstos en las tareas a su cargo.
- La Oficina de Planeación y los que hagan sus veces como segunda línea de defensa, les corresponde establecer mecanismos de seguimiento o autoevaluación orientando y generando alertas a las primeras líneas de defensa, sugiriendo correctivos que ayuden al mejoramiento de los procesos y a la implementación de prácticas de gestión eficaces.
- El Comité de Gestión y Desempeño es el instrumento para socializar periódicamente los riesgos y las modificaciones a estos.
- Es la segunda línea de defensa acorde con la normatividad vigente y sus competencias, la que efectuará el seguimiento y monitoreo a los mapas de riesgo, para asegurar que las acciones se están llevando a cabo por parte de los líderes de los procesos y evaluar la eficacia de su implementación. La finalidad principal de la oficina de control interno será la de sugerir los correctivos y ajustes necesarios a los líderes de los procesos para asegurar un efectivo manejo de los mismos.
- La Oficina de Control interno de gestión realiza valoración y evaluación independiente de los riesgos

"La responsabilidad frente a la Gestión de Riesgos, está definida mediante las líneas de defensa, estipuladas en el Nuevo Modelo de Planeación y Gestión (MIPG)". Y en la entidad se acogen Según el siguiente cuadro:





EMPRESAS PÚBLICAS DEL QUINDIO EPQ SA ESP

POLITICA PARA LA GESTIÓN DE RIESGOS

Código: DE-D-05	Versión: 06	Fecha emisión: 02/05/2023	Página: 3 de 17	DOCUMENTO CONTROLADO
--------------------	----------------	------------------------------	--------------------	---------------------------------

Líneas de Defensa Responsable	Responsable	Responsabilidad frente al riesgo
Línea Estratégica	Comité Directivo y comité de gestión y desempeño institucional	<p>Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.</p> <p>Definir el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control.</p> <p>Recomendaciones de mejoras a la política de operación para la administración del riesgo.</p>
		<p>Desde la Línea Estratégica (Alta Dirección) Gerente General de EPQ, se define y somete a aprobación la Política de Administración del Riesgo, en el marco del Comité Institucional de Coordinación de Control Interno. La cual se encuentra previamente actualizada por parte del proceso de planeación, corporativa como segunda línea de defensa en la entidad; la cual realiza la compilación y seguimiento de los riesgos, frente a la gestión del riesgo institucional y la prevención y detección de fraude y mala conducta.</p> <p>Revisar la política de administración del riesgo por lo menos una vez al año para su actualización y validar su eficacia a la gestión del riesgo institucional.</p> <p>Se deberá hacer especial énfasis en la prevención y detección de fraude y mala conducta.</p> <p>Aprobar el marco general para la gestión del riesgo, la gestión de la continuidad del negocio y el control.</p> <p>Analizar los riesgos, vulnerabilidades, amenazas y escenarios de pérdida de continuidad de negocio institucionales que pongan en peligro el cumplimiento de los objetivos estratégicos, planes institucionales, metas, compromisos de la entidad y capacidades para prestar servicios.</p> <p>Garantizar el cumplimiento de los planes de la entidad.</p>
Primera Línea	Líderes de Procesos	Identificar, valorar, evaluar los riesgos que pueden





EMPRESAS PÚBLICAS DEL QUINDIO EPQ SA ESP

POLITICA PARA LA GESTIÓN DE RIESGOS

Código: DE-D-05	Versión: 06	Fecha emisión: 02/05/2023	Página: 4 de 17	DOCUMENTO CONTROLADO
--------------------	----------------	------------------------------	--------------------	---------------------------------

		<p>afectar los programas, proyectos, planes y procesos a su cargo, actualizando cuando se requiera, con énfasis en la prevención del daño antijurídico.</p> <p>Definir, adoptar, aplicar y hacer seguimiento a los controles para mitigar los riesgos identificados alineado con las metas y objetivos de la entidad y proponer mejoras a la gestión del riesgo en su proceso delegar, por parte del líder del proceso, el (los) profesionales que se encargaran de la identificación, monitoreo, reporte y socialización de los riesgos.</p> <p>Informar a la –OAP- los cambios de responsables de reporte en caso de ausentismo laboral supervisar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar.</p> <p>Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles</p> <p>Informar a la Subgerencia de planeación (segunda línea) sobre los riesgos materializados en los objetivos, programas, proyectos y planes de los procesos a cargo.</p> <p>Reportar a la Subgerencia de Planeación por medio del formato Excel (normalizado) los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado, dentro de los plazos establecidos.</p>
Segunda Línea	Subgerencia de Planeación *secretaria general, Líderes de procesos de Contratación, Área Financiera, Talento Humano, Área Administrativa, Sistemas de	Asesorar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo Presentar al CCCI el seguimiento a la eficacia de los controles para el tratamiento de los riesgos en las áreas identificadas en los diferentes niveles de operación de la entidad





EMPRESAS PÚBLICAS DEL QUINDIO EPQ SA ESP

POLITICA PARA LA GESTIÓN DE RIESGOS

Código: DE-D-05	Versión: 06	Fecha emisión: 02/05/2023	Página: 5 de 17	DOCUMENTO CONTROLADO
--------------------	----------------	------------------------------	--------------------	---------------------------------

	<p>Información, Gestión de Recursos, Gestión Documental y los Supervisores de contrato de la Entidad entre otros.</p>	<p>Los riesgos presentados desde la primera línea de defensa para cambio o actualización serán presentados por la segunda línea de defensa al comité institucional de gestión y desempeño para su aprobación.</p> <p>Capacitar al grupo de trabajo de cada dependencia en la herramienta para la gestión del riesgo como líder de la política de Gestión y desempeño.</p> <p>Revisar el adecuado diseño de los controles para la Mitigación de los riesgos que sea establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimientos para el fortalecimiento de estos.</p> <p>Verificar que las acciones de control se diseñen conforme a los requerimientos de la metodología.</p> <p>Revisar el perfil de riesgo inherente y riesgo residual por cada proceso y pronunciarse sobre cualquier riesgo que este por fuera del perfil del riesgo residual aceptado por la entidad.</p> <p>Hacer seguimiento al plan de acción establecido para la mitigación de los riesgos de los procesos registrados.</p> <p>Revisar que el cargue de información este acorde con lo aprobado por el líder del proceso.</p> <p>Revisar los mapas de riesgos institucionales para identificar los más críticos frente al logro de los objetivos y presentarlo para análisis al Comité de gestión y desempeño.</p> <p>Se presenta al comité institucional de gestión y desempeño el resultado de la medición del nivel de eficacia de los controles para el tratamiento de los riesgos identificados en los procesos.</p> <p>Revisar las acciones y planes de mejoramiento establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas</p>
--	---	---





EMPRESAS PÚBLICAS DEL QUINDIO EPQ SA ESP


POLITICA PARA LA GESTIÓN DE RIESGOS

Código: DE-D-05	Versión: 06	Fecha emisión: 02/05/2023	Página: 6 de 17	DOCUMENTO CONTROLADO
--------------------	----------------	------------------------------	--------------------	---------------------------------

		<p>oportunas y eficaces para evitar en lo posible que se vuelvan a materializar.</p> <p>Informar al comité de gestión y desempeño los riesgos materializados no identificados que envían la primera línea de defensa para que sea incluidos y seguir siendo medidos.</p> <p>Monitorear los controles establecidos por la primera línea de defensa acorde con la información suministrada por los líderes de los procesos.</p> <p>Evaluar que la gestión de los riesgos este acorde a la presente política de la entidad y que sean gestionados por la primera línea de defensa</p> <p>Promover ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles seleccionados para el tratamiento de los riesgos identificados.</p>
Tercera Línea	Oficina de Control interno De Gestión	<p>Proporcionar aseguramiento objetivo sobre la eficacia de la gestión del riesgo y control, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos.</p> <p>Proporcionar aseguramiento objetivo en las áreas identificadas no cubiertas por la segunda línea de defensa.</p> <p>Asesorar de forma coordinada con la Oficina de Planeación, a la primera línea de defensa en la identificación de los riesgos institucionales y diseño de controles.</p> <p>Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos de conformidad con el Plan Anual de Auditoria y reportar los resultados al CCCI.</p> <p>Recomendar mejoras a la política de administración del riesgo.</p>

Niveles de autoridad y responsabilidad



	EMPRESAS PÚBLICAS DEL QUINDIO EPQ SA ESP			
	POLITICA PARA LA GESTIÓN DE RIESGOS			
Código: DE-D-05	Versión: 06	Fecha emisión: 02/05/2023	Página: 7 de 17	DOCUMENTO CONTROLADO

A través de la matriz niveles de responsabilidad y autoridad se definen los cargos que pueden identificar, valorar, definir controles y acciones, validar y reportar los riesgos institucionales a la Subgerencia de Planeación y Mejoramiento Institucional y a la Oficina de Control Interno De Gestión.

4- Marco Legal.

- Ley 1474 de 2011
- Decreto 1499 de 2017. Modelo Integrado de Planeación y Gestión.
- NTC GP 1000:2009. Norma Técnica de Calidad de la Gestión Pública.
- NTC ISO 9001:2015. Sistema Gestión de Calidad. (Requisitos)
- NTC 31000. Gestión del Riesgo.
- Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6 noviembre de 2022.

5- Definiciones.

Política para la gestión del riesgo.

Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.

Mapa de Riesgos: Documento que resume los resultados de las actividades de gestión de riesgos, incluye una representación gráfica en modo de mapa de calor de los resultados de la evaluación de 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. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

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


Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

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.

Contingencia: Posible evento futuro, condición o eventualidad.

Continuidad: Capacidad de una organización para continuar la entrega de productos o servicios a niveles aceptables después de una crisis.



	EMPRESAS PÚBLICAS DEL QUINDIO EPQ SA ESP			
	POLITICA PARA LA GESTIÓN DE RIESGOS			
Código: DE-D-05	Versión: 06	Fecha emisión: 02/05/2023	Página: 8 de 17	DOCUMENTO CONTROLADO

Crisis (Emergencia): Ocurrencia o evento repentino, urgente, generalmente inesperado que requiere acción inmediata.

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

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.

Control: Medida que permite reducir o mitigar 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.

Factores de Riesgo: Son las fuentes generadoras de riesgos.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

Integridad: Propiedad de exactitud y completitud.

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


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

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.

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.



	EMPRESAS PÚBLICAS DEL QUINDIO EPQ SA ESP			
	POLITICA PARA LA GESTIÓN DE RIESGOS			
Código: DE-D-05	Versión: 06	Fecha emisión: 02/05/2023	Página: 9 de 17	DOCUMENTO CONTROLADO

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.

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.

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.

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.

Gestión del riesgo.

Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Riesgo de Corrupción.

Se entiende como la posibilidad de que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.

Riesgo Estratégico.


Se asocia con la forma en que se administra la entidad. El manejo del riesgo estratégico se enfoca en asuntos globales relacionados con el Plan Estratégico Institucional y su direccionamiento estratégico (Misión, Visión, Política y Objetivos de Calidad), el diseño y conceptualización de la entidad por parte de sus directivos.

Riesgos Operativos. Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información, de la definición de los procesos, de la estructura de la entidad y la articulación e interacción entre procesos.

Riesgos Financieros.

Se relacionan con el manejo de los recursos de la entidad que incluyen: La ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.



	EMPRESAS PÚBLICAS DEL QUINDIO EPQ SA ESP			
	POLITICA PARA LA GESTIÓN DE RIESGOS			
Código: DE-D-05	Versión: 06	Fecha emisión: 02/05/2023	Página: 10 de 17	DOCUMENTO CONTROLADO

Riesgos de Cumplimiento.

Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

Riesgos de Tecnología.

Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

Riesgos de Imagen.

Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la organización.

Definición y elementos del riesgo fiscal: Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

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.

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.

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 potencial². (ver conceptos de recursos públicos, bien público e Intereses patrimoniales de naturaleza pública).


Gestión del Riesgo Fiscal: son las actividades que debe desarrollar cada Entidad y todos los gestores públicos (ver concepto de gestor público) para identificar, valorar, prevenir y mitigar los riesgos fiscales (probabilidad de efecto dañoso sobre los bienes, recursos y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial).

Lo anterior se puede resumir de la siguiente manera:

Riesgo Fiscal = Evento Potencial (Potencial Conducta) + Efecto dañoso

IMPORTANTE: Se debe tener especial cuidado en no confundir el riesgo fiscal, con el daño fiscal; por lo tanto, la definición debe estar orientada hacia el efecto de un evento potencial (potencial acción u omisión) sobre los recursos públicos y/o los bienes o intereses patrimoniales de naturaleza pública.



	EMPRESAS PÚBLICAS DEL QUINDIO EPQ SA ESP			
	POLITICA PARA LA GESTIÓN DE RIESGOS			
Código: DE-D-05	Versión: 06	Fecha emisión: 02/05/2023	Página: 11 de 17	DOCUMENTO CONTROLADO

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).

Plan Anticorrupción y de Atención al Ciudadano: Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

MIPG: Modelo Integrado de Planeación y Gestión.

CCCI: Comité de Coordinación de Control Interno.

CGDI: Comité de Gestión y Desempeño Institucional.

6- Metodología para la administración del riesgo:

Es básico como primera medida la identificación del riesgo, 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, alcance y el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.

Nivel de aceptación del riesgo

Acorde con los riesgos aprobados por el Comité institucional de gestión y desempeño, se deberá definir la periodicidad de seguimiento a los diferentes riesgos identificados por cada proceso de la Entidad.





EMPRESAS PÚBLICAS DEL QUINDIO EPQ SA ESP

POLITICA PARA LA GESTIÓN DE RIESGOS

Código:
DE-D-05

Versión:
06

Fecha emisión:
02/05/2023

Página:
12 de 17

**DOCUMENTO
CONTROLADO**

		Impacto								
		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%	Extremo	Alto	Moderado	Bajo
Probabilidad	Muy Alta 100%									
	Alta 80%									
	Media 60%									
	Baja 40%									
	Muy Baja 20%									


Empresas Públicas del Quindío E.P.Q S. A E.S.P., se basará en las orientaciones metodológicas que sobre la materia imparta el Departamento Administrativo de la Función Pública DAFP y en Normas Técnicas emitidas sobre el tema. Por lo anterior según La Guía para la Administración del Riesgo y el Diseño de Controles para las Entidades Públicas en su Versión 6 noviembre 2022, se utilizará como referente para su consulta y aplicación en las diferentes actualizaciones para la Gestión del Riesgo, y en sus tablas de probabilidad e Impacto, para las nuevas mediciones en las Entidades Públicas.

A continuación, miremos los puntos claves en la **Identificación De Áreas De Impacto**; que concurrieron a una nueva mirada del riesgo con ajustes realizados en esta nueva guía, ya que antes se identificaban los riesgos a los procesos y se miraban como procesos, ahora la mirada del impacto del riesgo no es el proceso, es la entidad y esto genera dos impactos

- una afectación económica
- una afectación reputacional


De otra parte, la **Identificación De Áreas De Factores De Riesgo** antes se reunían en factores internos y externos ahora se reúnen en 5 categorías como son:



	EMPRESAS PÚBLICAS DEL QUINDIO EPQ SA ESP			
	POLITICA PARA LA GESTIÓN DE RIESGOS			
Código: DE-D-05	Versión: 06	Fecha emisión: 02/05/2023	Página: 13 de 17	DOCUMENTO CONTROLADO

1. **PROCESOS** es todo lo que sucede dentro de un proceso los eventos relacionados con errores en las actividades que deben realizar los servidores de la entidad. por ej. falta de procedimientos, de capacitación.
 2. **TALENTO HUMANO:** incluye seguridad salud en el trabajo y toda la parte ética del talento humano. Habla de posibles comportamientos no éticos de los empleados, hurtos activos, fraude interno (corrupción, soborno).
 3. **TECNOLOGIA** eventos relacionados con la infraestructura tecnológica de la entidad. (daño de equipos, caída de aplicaciones, de redes, errores en programas)
 4. **INFRAESTRUCTURA:** eventos relacionados con la infraestructura física de la entidad. (derrumbes, incendios, inundaciones, daños a activos fijos).
 5. **EVENTOS EXTERNOS TERCEROS:** situaciones externas que afectan la entidad por ej. el covid y no lo teníamos identificado en ninguna entidad y puede el riesgo haberse materializado en algunas entidades, otros (suplantación de identidad, asalto a la oficina, atentados, vandalismo, orden público).
- ✓ En cuanto a la **PROBABILIDAD** del riesgo se califica de acuerdo a la exposición del riesgo es decir el número de veces que yo hago la actividad, es el que me marca el nivel de probabilidad de la exposición al riesgo.
 - ✓ Para el manejo de los mapas de riesgos Institucional y por Procesos, se contará con el procedimiento para la gestión del riesgo GCI-P-02 el cual define los pasos secuenciales para su gestión y la Matriz para la Gestión de Riesgos GCI-P-02-R-02 la cual facilita su tratamiento, control y seguimiento.
 - ✓ Los riesgos de **MENOR** probabilidad e impacto (**Zona de riesgo BAJA, MODERADA**) serán sujetos de seguimiento mínimo cada SEIS (6) meses por parte de los líderes de procesos. Deberá estar debidamente documentado su planteamiento, tratamiento y cada seguimiento en el registro diseñado para tal fin.
 - ✓ Los riesgos de **MAYOR** probabilidad e impacto (**Zona de riesgo ALTA, EXTREMA**) serán llevados al Mapa de Riesgos Institucional y serán sujetos de seguimiento mínimo cada CUATRO (4) meses por parte de la oficina de Control Interno. Deberá estar debidamente documentado su planteamiento, tratamiento y cada seguimiento en el registro correspondiente. Cabe anotar que para un efectivo control se hace necesario la aplicación de las Líneas de Defensa estipuladas en el Nuevo Modelo de Planeación y Gestión. Y



	EMPRESAS PÚBLICAS DEL QUINDIO EPQ SA ESP			
	POLITICA PARA LA GESTIÓN DE RIESGOS			
Código: DE-D-05	Versión: 06	Fecha emisión: 02/05/2023	Página: 14 de 17	DOCUMENTO CONTROLADO

detallada sus competencias en el cuadro superior de este documento, para la responsabilidad de la Gestión de Riesgos.

- **LINEA ESTRATEGICA:** Se toman decisiones y se dan los lineamientos de control de riesgos.
- **PRIMERA LINEA DE DEFENSA:** Primeros responsables de los riesgos de su proceso, los evalúa y diseña los controles y hace seguimiento, lo cual se convierte en un autocontrol.
- **SEGUNDA LINEA DE DEFENSA:** Consolida la información y hace acompañamiento.
- **TERCERA LINEA DE DEFENSA:** es la oficina de control interno de Gestión y hace una evaluación independiente.

RIESGOS DE CORRUPCIÓN, el riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos. Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, por tanto, se utiliza la matriz GCI-P-02-R-01 de definición de riesgo de corrupción diferente a la Matriz de Riesgo de Gestión.


- ✓ De otra parte, tal como está establecido en la normatividad aplicable emitida por el DAFP, los Riesgos de Corrupción serán llevados directamente al Mapa de Riesgos De Corrupción Institucional por su naturaleza de **ALTOS Y EXTREMOS**, y ningún riesgo de corrupción podrá ser aceptado, por lo tanto, se deben adoptar medidas para:

REDUCIR la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.

EVITAR Se abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo.

TRANSFERIR O COMPARTIR una parte del riesgo para reducir la probabilidad o el impacto del mismo, Deberán ser evaluados en los tiempos establecidos para los demás riesgos de la entidad, para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos. serán de **UNICO IMPACTO**, sin embargo, se tomará en consideración los tiempos previstos para la rendición de informes en la página web de la entidad, dispuesto por el Departamento Administrativo de la Función Pública DAFP tres (3) veces al año, esto es con corte a abril 30, agosto 31 y diciembre 31.



	EMPRESAS PÚBLICAS DEL QUINDIO EPQ SA ESP			
	POLITICA PARA LA GESTIÓN DE RIESGOS			
Código: DE-D-05	Versión: 06	Fecha emisión: 02/05/2023	Página: 15 de 17	DOCUMENTO CONTROLADO

- Dentro de los procesos susceptibles de corrupción en la entidad se pueden identificar: Gestión Financiera, contratación, Comercialización del servicio y atención a al ciudadano, Gestión de Recursos, Gestión sistemas de Información.
- *La gestión el riesgo se realizará según lo establecido en el Procedimiento para la gestión del riesgo GCI-P-02* adscrito a la oficina de Control Interno. Cada proceso deberá como mínimo realizar un ejercicio de actualización del Mapa de Riesgos una vez al año o cada vez que las circunstancias lo ameriten y revisar los registros de ocurrencia o materialización, para tomar las acciones correctivas pertinentes.
- La Política de Administración del Riesgo, deberá ser revisada para garantizar que sea adecuada al propósito de la organización, en la revisión gerencial que se realiza anualmente.
- En los procesos de auditoria interna que realiza la entidad, se deberá verificar que se cuente con políticas de administración del riesgo actualizadas, que se estén ejecutando y que se realicen revisiones periódicas a las mismas.
- La entidad deberá adelantar mecanismos de comunicación, actividades de capacitación y concientización a todos los servidores públicos sobre la importancia de tratar los riesgos de cada proceso.


RIESGOS FISCALES: Para la identificación del riesgo fiscal es necesario establecer los puntos de riesgo fiscal 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.

Identificación de áreas de impacto en los riesgos fiscales:

Dentro de este contexto el área de impacto siempre corresponderá a una consecuencia económica sobre el patrimonio público, a la cual se vería expuesta la organización en caso de materializarse el riesgo.



	EMPRESAS PÚBLICAS DEL QUINDIO EPQ SA ESP			
	POLITICA PARA LA GESTIÓN DE RIESGOS			
Código: DE-D-05	Versión: 06	Fecha emisión: 02/05/2023	Página: 16 de 17	DOCUMENTO CONTROLADO

Control fiscal interno y prevención del riesgo fiscal: la construcción de este capítulo tiene como finalidad prevenir la constitución del elemento medular de la responsabilidad fiscal, que es el daño al patrimonio público, representando en el menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos, o a los intereses patrimoniales del Estado (Decreto 403, 2020, art.6).

Los cuáles serán incluidos en la matriz existente de riesgos de gestión con el código GCI-P-02-R-02.

RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

En primer lugar, se debe tener en cuenta que la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI)¹², 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: seguridad de la información, arquitectura, servicios ciudadanos digitales.

Identificación del riesgo: 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 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 Anexo 4 Modelo nacional de gestión de riesgos de seguridad de la información para entidades públicas.

Los cuáles serán incluidos en la matriz existente de riesgos de gestión con el código GCI-P-02-R-02.

8- ANEXOS

Para una mayor comprensión de la política de operación para la administración del riesgo, se define que los anexos son parte fundamental de este documento técnico, por tanto, se recomienda su consulta y conocimiento por parte de todos los servidores públicos de la Entidad.



	EMPRESAS PÚBLICAS DEL QUINDIO EPQ SA ESP			
	POLITICA PARA LA GESTIÓN DE RIESGOS			
Código: DE-D-05	Versión: 06	Fecha emisión: 02/05/2023	Página: 17 de 17	DOCUMENTO CONTROLADO

<https://www.funcionpublica.gov.co/web/mipg/como-opera-mipg>

Gestión del Riesgo

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

Nota: En esta guía, en el aparte *Anexos* en la página 107, encontrará la siguiente información:

- Formato matriz mapa de riesgo parametrizado
- Modelo Nacional Gestión Riesgos Seguridad de la información.
- Protocolo para la identificación riesgos de corrupción en trámites.
- Documentos buenos prácticas para el análisis de riesgos de fraude y corrupción.
- Matriz de seguimiento a riesgos de corrupción.
- Catalogo indicativo puntos riesgo fiscal.

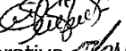

De otra parte, la consulta en el Micro sitio de MIPG

- Manual operativo MIPG
- Metodología de riesgos
- Guía para la Administración del riesgo de FP
- Matriz de autoridad y responsabilidad
- Manual del usuario – módulo de riesgos SGI
- Manual Metodología de gestión de riesgo

7- Recursos necesarios para la administración del riesgo.

La implementación de la Política de Administración de Riesgos, cuenta con el compromiso de la Alta Dirección de Empresas Públicas del Quindío EPQ S.A. E.S.P., para lo cual se dispone de los recursos físicos, económicos, tecnológicos y humanos necesarios.


JHON FABIO SUAREZ VALERO
GERENTE GENERAL

Proyectó: Martha Liliana Gómez Fajardo. P.u Planeación Corporativa 
Revisó: Victoria Eugenia Hurtado Palacio. Jefe de Planeación Corporativa 
Aprobó: Darnelly Toro Jiménez. Subgerente de Planeación y Mejoramiento Institucional 