Radicado:20250000079

INFORME DE VERIFICACIÓN AL ESTADO DE LOS RIESGOS DE PROCESOS, CORRUPCIÓN, SISTEMA DE INFORMACIÓN Y FISCAL DE LA EMPRESA PARA LA SEGURIDAD Y SOLUCIONES URBANAS – ESU – SEGUNDO SEMESTRE 2024 Y SEGUIMIENTO A LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

Presentado a:

CAMILO ZAPATA WILLS

Gerente General ESU

Preparado por:

JORGE HERNÁN LOPERA TABORDA

Director Auditoría Interna ESU

Elaborado por:

Equipo de Auditoría Interna

Medellín, enero 09 de 2025

INFORME DE VERIFICACIÓN AL ESTADO DE LOS RIESGOS DE PROCESOS, CORRUPCIÓN, SISTEMA DE INFORMACIÓN Y FISCAL DE LA EMPRESA PARA LA SEGURIDAD Y SOLUCIONES URBANAS – ESU – SEGUNDO SEMESTRE 2024 Y SEGUIMIENTO A LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

Tabla de contenido

INTRODUCCIÓN 3

OBJETIVO 4

ALCANCE 4

1. Metodología 4

2. CAMBIOS QUE AFECTARON LA MATRIZ DE RIESGOS DE PROCESOS, DE CORRUPCIÓN Y DE SEGURIDAD DE LA INFORMACIÓN 6

3. ADMINISTRACIÓN DEL RIESGO 6

4. MATRIZ DE RIESGOS DE PROCESOS 7

4.1 Matriz de riesgos inherente 7

4.2 Matriz de riesgos residual 7

4.3 Tipificación de acciones y controles para mitigación del riesgo de procesos. 8

5. MATRIZ DE RIESGOS DE CORRUPCIÓN 9

5.1 Matriz de riesgos inherente 9

5.2 Matriz de riesgos residual. 9

5.3 Tipificación de acciones y controles para mitigación del riesgo de procesos. 10

6. MATRIZ DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 13

6.1 Matriz de riesgo inherente 13

6.2 Matriz de riesgos residual. 14

6.3 Tipificación de acciones y controles para mitigación de los riesgos de seguridad y privacidad de la información. 15

7. MATRIZ DE RIESGO FISCAL 16

8. EFECTIVIDAD DE LOS CONTROLES. 18

9. MATERIALIZACIÓN DEL RIESGO. 19

10. RECOMENDACIONES 19

11. CONCLUSIONES 24

INTRODUCCIÓN

La evaluación de la gestión del riesgo se establece como un componente fundamental del Sistema de Control Interno dentro del Modelo Integrado de Planeación y Control (MIPG). Este proceso incluye, entre otros aspectos, la auditoría interna, en la verificación de eventos internos y externos que puedan afectar o impedir el logro de los objetivos estratégicos. Asimismo, permite identificar oportunidades para un mejor cumplimiento de las funciones organizacionales, en concordancia con lo dispuesto en la Ley 87 de 1993 y los Decretos 648 y 1499 de 2017.

Es importante destacar que el seguimiento del mapa de riesgos, liderado por la Dirección de Auditoría Interna (tercera línea de defensa), consiste en verificar las acciones implementadas frente a los riesgos identificados. Sin embargo, se enfatiza que cada líder de proceso es responsable de realizar periódicamente el análisis y valoración de los riesgos asociados a sus áreas, utilizando la "Guía Metodológica para la Administración del Riesgo" (versión VI), publicada por la Función Pública en noviembre de 2022.

Esta guía conserva la estructura conceptual para la administración del riesgo, incorporando como novedad un capítulo específico sobre riesgo fiscal. Dicho capítulo se complementa con un anexo denominado "Catálogo Indicativo y enunciativo de Puntos de Riesgo Fiscal", diseñado para facilitar el análisis dentro del modelo de operación por procesos.

El presente informe tiene como propósito verificar la gestión del riesgo realizada por la entidad durante el segundo semestre de 2024 (01 de julio – 31 de diciembre). Para ello, se evaluará la matriz de riesgos identificados por los líderes de proceso y sus comités operativos (primera línea de defensa), así como las acciones diseñadas para mitigar dichos riesgos. Además, se documentará el estado actual de los riesgos, su nivel de mitigación, y se identificarán nuevos riesgos y controles, en caso de ser necesario. Finalmente, se realizará un seguimiento a la política de gestión del riesgo de la entidad.

OBJETIVO

Realizar la verificación a los riesgos de la entidad para el segundo semestre de 2024, de acuerdo con la aplicación de la guía metodológica para la administración del riesgo versión VI, establecida por la Función Pública en noviembre de 2022, evidenciando los riesgos que se mantienen iguales, se mitigaron o se aumentaron; o en su defecto la identificación de nuevos riesgos y controles, y el seguimiento realizado por las diferentes áreas de gestión a los mismos. Así como también a la política de administración de riesgos de la Empresa para la Seguridad y Soluciones Urbanas ESU.

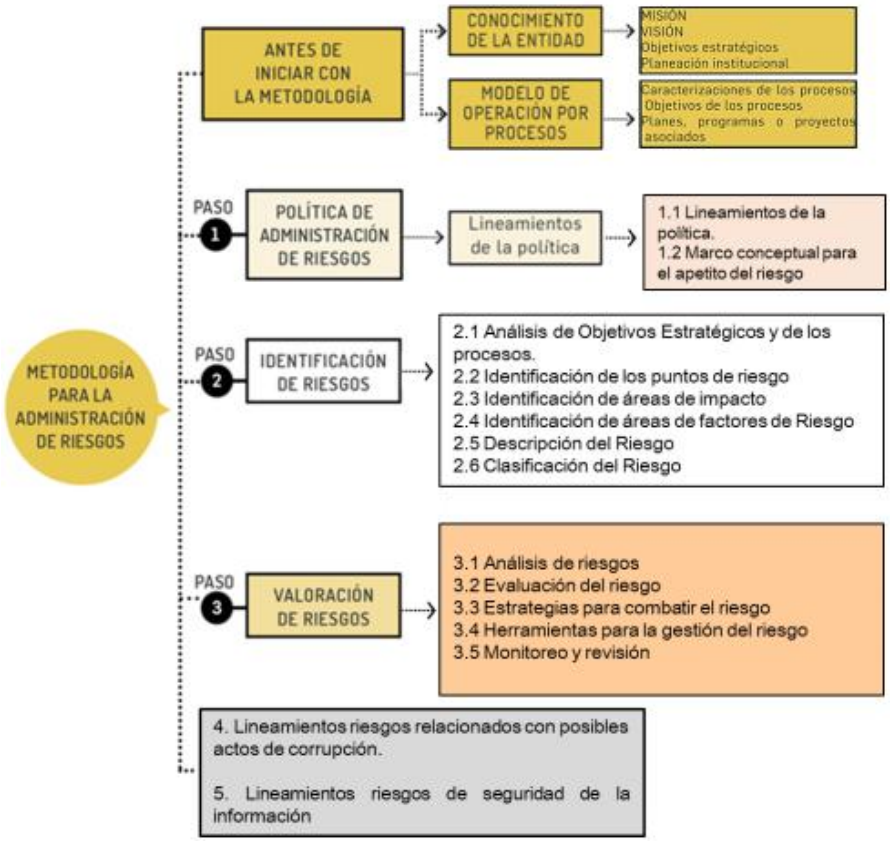
ALCANCE

Verificación de los riesgos de cada uno de los procesos de la entidad en el periodo comprendido entre julio 01 a diciembre 31 de 2024.

1. Metodología

Para la administración y verificación del riesgo se utiliza la metodología planteada por la Guía de la administración del riesgo y el diseño de controles Versión 6; la cual dice lo siguiente:

“La metodología para la administración del riesgo requiere de un análisis inicial relacionado con el estado actual de la estructura de riesgos y su gestión en la entidad, además del conocimiento de esta desde un punto de vista estratégico de la aplicación de los tres (3) pasos básicos para su desarrollo y, finalmente de la definición e implementación de estrategias de comunicación transversales a toda la entidad para que su efectividad pueda ser evidenciada. A continuación, se puede observar la estructura completa con sus desarrollos básicos:”



Fuente: Guía de la administración del riesgo y el diseño de controles Versión 6

Tabla de Criterios para definir la frecuencia de la actividad

Tabla 4 Criterios para definir el nivel de probabilidad

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

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

Tabla 5 Criterios para definir el nivel de impacto

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

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

2. CAMBIOS QUE AFECTARON LA MATRIZ DE RIESGOS DE PROCESOS, DE CORRUPCIÓN Y DE SEGURIDAD DE LA INFORMACIÓN

Todos los riesgos se evaluaron con la Versión 6 del DAFP, lo cual disminuye la subjetividad y aumenta el grado de eficiencia en este proceso.

En relación con los riesgos de procesos se tuvo en cuenta 60 riesgos, para corrupción 19 y, finalmente para seguridad y privacidad de la información se determina la existencia de 6 riesgos. Es importante precisar que la información anterior se apoya en 14 procesos organizacionales.

3. ADMINISTRACIÓN DEL RIESGO

Matriz de Riesgo Integrado de Gestión de Procesos

- I + ID (riesgo): Riesgo Inherente
- R + ID (riesgo): Riesgo Residual

4. MATRIZ DE RIESGOS DE PROCESOS

4.1 Matriz de riesgos inherente

Después de realizada la identificación, análisis y evaluación de 60 riesgos, se obtiene la matriz de riesgos inherente, la cual representa el riesgo sin haberse aplicado un control para ello; es decir, es el nivel inicial en el cual se identifica el riesgo sin control asociado.

De acuerdo con esta matriz de riesgos inherente se encuentran:

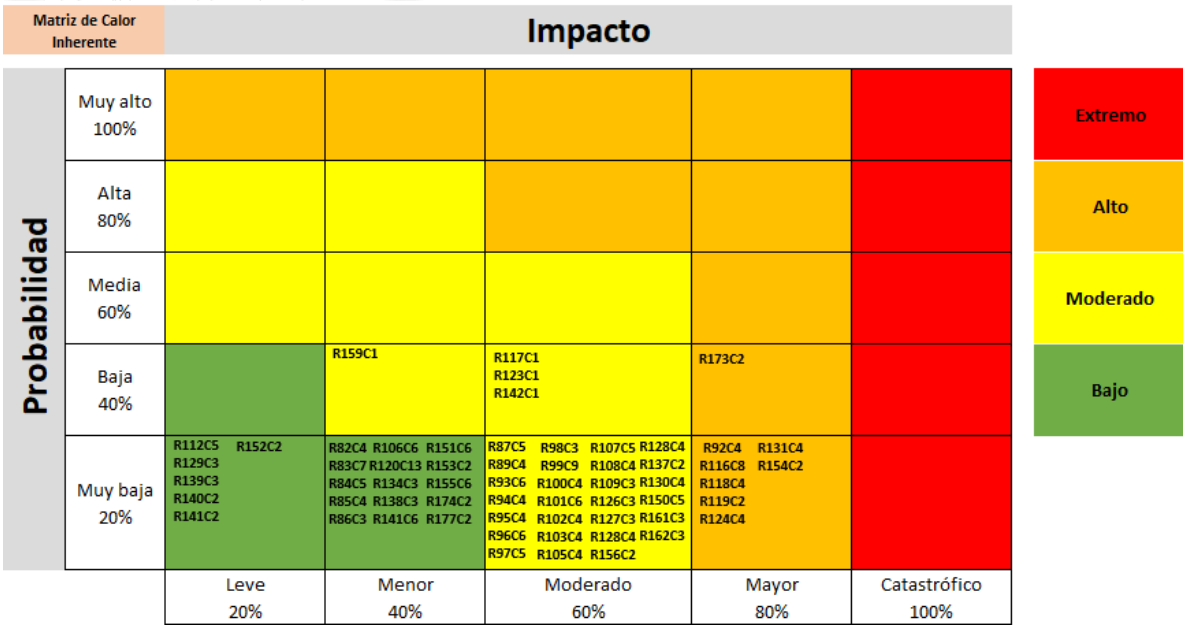
- 9 nivel alto.
- 42 nivel moderado.
- 9 nivel bajo.

Matriz de Calor Inherente		Impacto				
Probabilidad	Muy alto 100%					
	Alta 80%			I100	I118	
	Media 60%	I112	I106 I120 I134	I87 I117 I89 I123 I93 I128 I94 I161 I99 I162	I119 I173	
	Baja 40%	I129 I139 I140 I141	I84 I155 I85 I159 I86 I174 I138 I177	I83 I103 I137 I96 I108 I142 I98 I109 I150 I101 I126 I102 I127	I116 I124 I154	
	Muy baja 20%	I152	I82 I151 I153 I157	I95 I130 I97 I156 I105 I160 I107	I92 I131	
		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%

Extremo
Alto
Moderado
Bajo

4.2 Matriz de riesgos residual

Una vez se evalúan los riesgos, se procede a realizar la valoración, definiendo los controles que se tienen para la mitigación de estos. Después de implementadas las acciones para el manejo de los riesgos se obtiene la matriz de riesgos residual:



En la anterior matriz se ubicaron los últimos controles implementados para cada riesgo. De acuerdo con lo anterior, se tienen diseñados y establecidos 218 controles para los 60 riesgos, 215 son de tipo preventivo y 3 detectivo, en su implementación 206 son manuales y 12 automáticos, factor que se puede mejorar con el fin de aumentar la eficiencia de los controles, disminuyendo el riesgo residual.

Con los controles implantados, la matriz residual ubica:

- 8 riesgo nivel alto.
- 31 riesgos nivel moderado.
- 21 riesgos nivel bajo.

4.3 Tipificación de acciones y controles para mitigación del riesgo de procesos.

En el siguiente archivo se relacionan los 218 controles de los 60 riesgos de procesos:

Controles riesgos de procesos.xlsx

5. MATRIZ DE RIESGOS DE CORRUPCIÓN

5.1 Matriz de riesgos inherente

Después de realizada la identificación, análisis y evaluación de los 19 riesgos, se obtiene la matriz de riesgos inherente, la cual representa el riesgo sin haberse aplicado un control para ello; es decir, es el nivel inicial en el cual se identifica el riesgo sin control asociado.
De acuerdo con esta matriz de riesgos inherentes se encuentran:

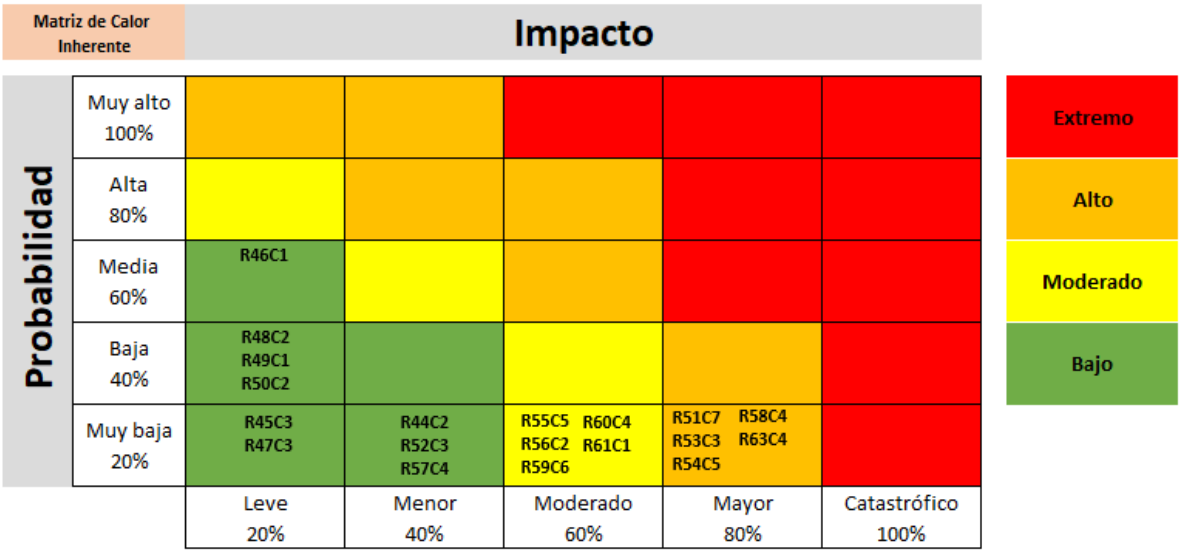
- 9 nivel alto
- 9 nivel moderado
- 1 nivel bajo

Matriz de Calor Inherente		Impacto				
Probabilidad	Muy alto 100%					
	Alta 80%					
	Media 60%			I46 I55		
	Baja 40%			I47 I50 I60 I48 I56 I61 I49 I59	I51 I57 I63 I53 I58 I54	
	Muy baja 20%		I44	I45	I52	
		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%

Extremo
Alto
Moderado
Bajo

5.2 Matriz de riesgos residual.

Una vez se evalúan los riesgos, se procede a realizar la valoración, definiendo los controles que se tienen para la mitigación de estos. Después de implementadas las acciones para el manejo de los riesgos se obtiene la matriz de riesgos residual:



Con los controles implantados, la matriz residual ubica:

- 5 riesgos nivel alto.
- 5 riesgos nivel moderado.
- 9 riesgos nivel bajo.

En la anterior matriz se ubicaron los últimos controles implementados para cada riesgo. De acuerdo con lo anterior, se tienen diseñados y establecidos 63 controles para los 19 riesgos, 50 preventivos y 13 correctivos.

5.3 Tipificación de acciones y controles para mitigación del riesgo de procesos.

A continuación, se relacionan los 63 controles de los 19 riesgos de riesgos de corrupción:

ID Riesgo	ID Control	Orden Control	Nombre	Responsable de ejecución
44	144	44-C1	Seguimiento a los planes en comité del sistema integrado de gestión	Jefe de Oficina Estratégica
44	598	44-C2	Seguimiento realizado por el proceso de Auditoría Interna	Jefe de Oficina Estratégica
45	127	45-C1	Aprobación y cierre en el software por parte del Profesional especializado de la oficina estratégica	Jefe de Oficina Estratégica
45	128	45-C2	Comité del sistema integrado de gestión o comité de gestión y desempeño	Jefe de Oficina Estratégica
45	599	45-C3	Seguimiento por parte del proceso de Auditoría Interna	Jefe de Oficina Estratégica

ID Riesgo	ID Control	Orden Control	Nombre	Responsable de ejecución
46	129	46-C1	Políticas de comunicación corporativa ESU	Profesional Universitario - Oficina Estrategia (Comunicaciones)
46	130	46-C2	Plan de medios, espacios y formas de comunicación internos y externos	Profesional Universitario - Oficina Estrategia (Comunicaciones)
47	131	47-C1	Capacitación y campañas sobre riesgos de corrupción y sus consecuencias.	Subgerente Comercial y De Mercadeo
47	132	47-C2	Documentación del proceso de contratación y realización de auditorías	Subgerente Comercial y De Mercadeo
47	201	47-C3	Seguimiento periódico a la ejecución de los planes de ventas y de mercadeo según la caracterización del proceso.	Subgerente Comercial y De Mercadeo
48	133	48-C1	Documentación del proceso y realización de auditorías.	Subgerente Comercial y De Mercadeo
48	134	48-C2	Capacitación y campañas sobre riesgos de corrupción y sus consecuencias	Subgerente Comercial y De Mercadeo
49	203	49-C1	Inducción sobre riesgos de corrupción y sus consecuencias.	Profesional Universitario - Oficina Estrategia (Comunicaciones)
50	136	50-C1	Capacitación y campañas sobre riesgos de corrupción y sus consecuencias.	Gerente General
50	137	50-C2	Documentación del proceso y realización de auditorías.	Gerente General
51	138	51-C1	Comité asesor de contratación	Líder De Programa - Unidad de compras y contratación
51	139	51-C2	Formato informe de evaluación	Líder De Programa - Unidad de compras y contratación
51	140	51-C3	Revisión jurídica de pliegos y/o estudios previos antes de su publicación	Líder De Programa - Unidad de compras y contratación
51	141	51-C4	Aprobación de la adenda por el o los subgerentes(s) del área	Líder De Programa - Unidad de compras y contratación
51	169	51-C5	Estudios previos y/o referenciamiento de precios mínimo con dos posibles proponentes	Líder De Programa - Unidad de compras y contratación
51	170	51-C6	Redacción interdisciplinaria de Pliegos de condiciones	Líder De Programa - Unidad de compras y contratación
51	173	51-C7	Sensibilización para la prevención y control de riesgos de corrupción	Líder De Programa - Unidad de compras y contratación
52	145	52-C1	Informes de supervisión	Líder De Programa - Unidad de Logística
52	171	52-C2	Seguimiento a la supervisión de contratos	Líder De Programa - Unidad de Logística
52	172	52-C3	Sensibilización para la prevención y control de riesgos de corrupción	Líder De Programa - Unidad de Logística
53	146	53-C1	Aprobación del subgerente administrativo y financiero y acto administrativo por medio de traslado firmado por el gerente	Líder De Programa - Unidad de Presupuesto

ID Riesgo	ID Control	Orden Control	Nombre	Responsable de ejecución
53	147	53-C2	Procedimientos del proceso: ejecución y seguimiento del presupuesto. Procedimiento modificaciones presupuestales	Líder De Programa - Unidad de Presupuesto
53	148	53-C3	Parametrización del Software Financiero	Líder De Programa - Unidad de Presupuesto
54	149	54-C1	Procedimientos y políticas de gestión contable	Líder De Programa - Unidad de Contabilidad y Costos
54	178	54-C2	Desagregación de los procesos contables en diferentes personas del área	Líder De Programa - Unidad de Contabilidad y Costos
54	179	54-C3	Comité financiero	Líder De Programa - Unidad de Contabilidad y Costos
54	180	54-C4	Conciliación entre contabilidad y los demás módulos que transfieren información a contabilidad	Líder De Programa - Unidad de Contabilidad y Costos
54	181	54-C5	Presentación de estados financieros al comité financiero y de gerencia	Líder De Programa - Unidad de Contabilidad y Costos
55	151	55-C1	Modelo de selección bancario	Tesorero General
55	152	55-C2	Comité financiero	Tesorero General
55	153	55-C3	Manual de inversiones	Tesorero General
55	154	55-C4	Políticas de tesorería: Políticas de seguridad en las operaciones de tesorería - Política Pago de Obligaciones	Tesorero General
55	216	55-C5	Matriz de pares	Tesorero General
56	199	56-C1	Lista de chequeo de contrato interadministrativo	Profesional Universitario - Unidad de Liquidación de Convenios (1)
56	200	56-C2	Verificación por parte de tesorería que el titular de la cuenta sea la entidad pública firmante del acta	Profesional Universitario - Unidad de Liquidación de Convenios (1)
57	138	57-C1	Comité asesor de contratación	Líder De Programa - Unidad de Logística
57	139	57-C2	Formato informe de evaluación	Líder De Programa - Unidad de Logística
57	140	57-C3	Revisión jurídica de pliegos y/o estudios previos antes de su publicación	Líder De Programa - Unidad de Logística
57	145	57-C4	Informes de supervisión	Líder De Programa - Unidad de Logística
58	156	58-C1	Acceso restringido al sistema de gestión documental	Profesional Universitario G1 - Gestión documental
58	157	58-C2	Políticas de gestión documental donde se limita el préstamo de documentos físicos	Profesional Universitario G1 - Gestión documental
58	158	58-C3	Proceso de inducción obligatoria a todo el personal nuevo que ingresa a la empresa.	Profesional Universitario G1 - Gestión documental
58	159	58-C4	Procedimiento PR-MG-DOC-03 para consulta de los documentos en la Unidad de Gestión Documental.	Profesional Universitario G1 - Gestión documental
59	158	59-C1	Proceso de inducción obligatoria a todo el personal nuevo que ingresa a la empresa.	Profesional Universitario G1 - Gestión documental

ID Riesgo	ID Control	Orden Control	Nombre	Responsable de ejecución
59	160	59-C2	Procedimiento PR-M6-DOC-02 para recepción de correspondencia	Profesional Universitario G1 - Gestión documental
59	161	59-C3	Procedimiento PR-M6-DOC-05 para recepción de propuestas	Profesional Universitario G1 - Gestión documental
59	191	59-C4	Cámaras de video con grabación de video y registro de hora.	Profesional Universitario G1 - Gestión documental
59	192	59-C5	Relojes en la recepción y en el archivo.	Profesional Universitario G1 - Gestión documental
59	220	59-C6	Aplicación de la circular 14 y circular 06 de 2019	Profesional Universitario G1 - Gestión documental
60	162	60-C1	Parametrización del sistema de liquidación y cruce con contabilidad y tesorería para que se valide las acreencias laborales.	Técnico Administrativo G1- Unidad de Contabilidad y Costos (3)
60	163	60-C2	Capacitación en la herramienta, así como control en los cambios y ajustes a la herramienta, previa autorización del Líder de Programa de la Unidad de Gestión Humana y/o Subgerente Administrativo y financiero.	Técnico Administrativo G1- Unidad de Contabilidad y Costos (3)
60	164	60-C3	Informe del sistema sobre las diferencias entre lo liquidado y pagado.	Técnico Administrativo G1- Unidad de Contabilidad y Costos (3)
60	196	60-C4	Existencia de los soportes que autoricen el reconocimiento y pago de los beneficios	Técnico Administrativo G1- Unidad de Contabilidad y Costos (3)
61	165	61-C1	Procedimiento reclutamiento, selección y vinculación de personal	Técnico Administrativo G1- Unidad de Contabilidad y Costos (3)
63	166	63-C1	Aplicación Política de seguridad y privacidad de la información	Profesional Universitario G2 - Oficina Estrategia (TI)
63	183	63-C2	Configuración de los perfiles de usuarios y permisos de acceso a los sistemas	Profesional Universitario G2 - Oficina Estrategia (TI)
63	184	63-C3	Oportunidad en el reporte de novedades de personal (retiros/vacaciones)	Profesional Universitario G2 - Oficina Estrategia (TI)
63	185	63-C4	Control de la configuración de dispositivos de seguridad perimetral	Profesional Universitario G2 - Oficina Estrategia (TI)

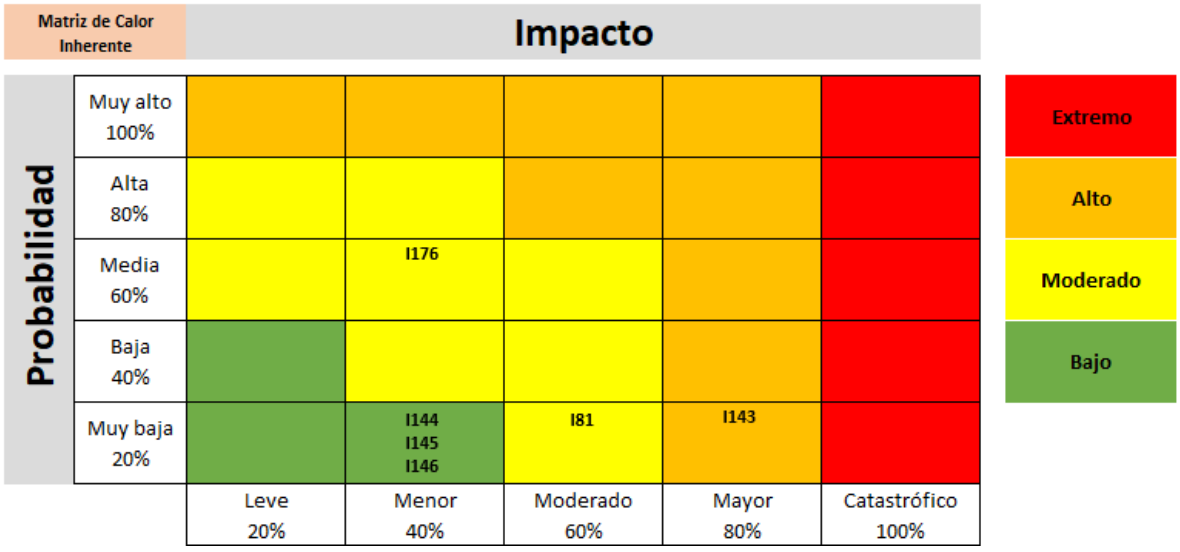
6. MATRIZ DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

6.1 Matriz de riesgo inherente

Después de realizada la identificación, análisis y evaluación de los 6 riesgos, se obtiene la matriz deriesgos inherentes, la cual representa el riesgo sin haberse aplicado un control para ello; es decir es el nivel inicial en el cual se identifica el riesgo sin control asociado.

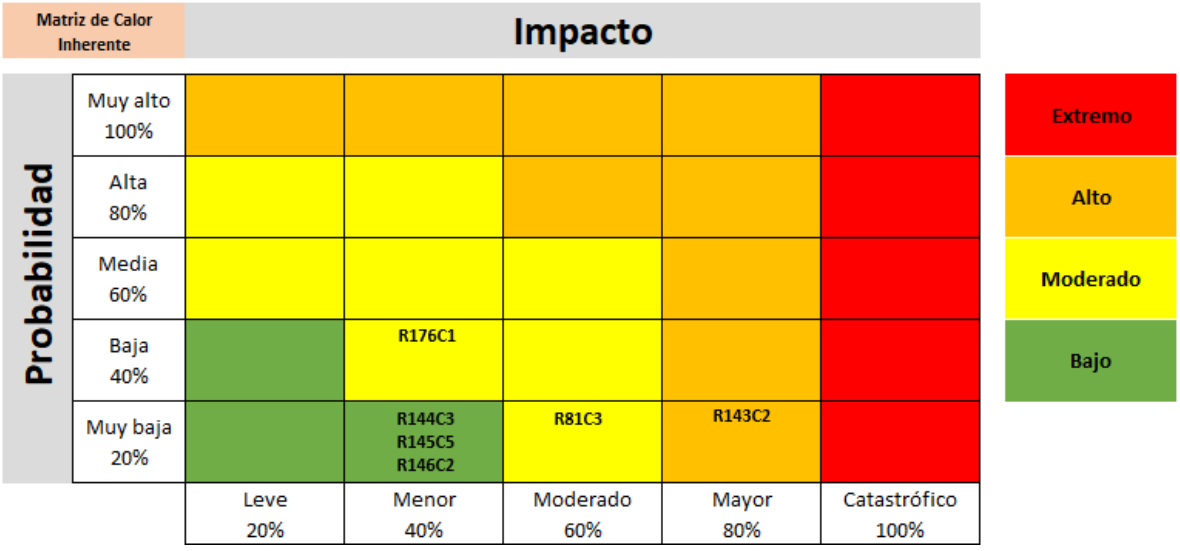
De acuerdo con esta matriz de riesgos inherentes se encuentran:

- 1 nivel Alto.
- 2 nivel moderado.
- 3 nivel bajo.



6.2 Matriz de riesgos residual.

Una vez se evalúan los riesgos, se procede a realizar la valoración, definiendo los controles que se tienen para la mitigación de estos. Después de implementadas las acciones para el manejo de los riesgos se obtiene la matriz de riesgos residual:



Con los controles implantados, la matriz residual ubica:

- 1 riesgo nivel alto.
- 2 riesgo nivel moderado.
- 3 riesgos nivel bajo.

En la anterior matriz se ubicaron los últimos controles implementados para cada riesgo. De acuerdo con lo anterior, se tienen diseñados y establecido 16 controles para los 6 riesgos, todos son preventivos; pero en su implementación 13 son manuales y 3 automáticos, factor que se puede mejorar con el fin de aumentar la eficacia de los controles, disminuyendo el riesgo residual.

6.3 Tipificación de acciones y controles para mitigación de los riesgos de seguridad y privacidad de la información.

A continuación, se relacionan los 16 controles de los 6 riesgos de riesgos de seguridad y privacidad de la información:

ID Riesgo	ID Control	Orden Control	Nombre	Responsable de ejecución
81	508	81-C1	Capacitar en política de seguridad de la información	Profesional Universitario G2 - Oficina Estrategia (TI)
81	529	81-C2	Inducción nuevos funcionarios y contratistas	Profesional Universitario G2 - Oficina Estrategia (TI)
81	530	81-C3	Documento de clasificación de información Publica Reservada	Profesional Universitario G2 - Oficina Estrategia (TI)
143	509	143-C1	Capacitar en política de seguridad de la información	Profesional Universitario G2 - Oficina Estrategia (TI)
143	531	143-C2	Control documento de clasificación de información Pública Reservada	Profesional Universitario G2 - Oficina Estrategia (TI)
144	510	144-C1	Aplicar procedimientos de seguridad de la información	Profesional Universitario G2 - Oficina Estrategia (TI)
144	532	144-C2	Control documento de clasificación de información Publica Reservado	Profesional Universitario G2 - Oficina Estrategia (TI)
144	533	144-C3	Check List revisión de infraestructura	Profesional Universitario G2 - Oficina Estrategia (TI)

ID Riesgo	ID Control	Orden Control	Nombre	Responsable de ejecución
145	511	145-C1	Realizar copias de seguridad	Profesional Universitario G2 - Oficina Estrategia (TI)
145	534	145-C2	Control documento de clasificación de información Publica Reservado	Profesional Universitario G2 - Oficina Estrategia (TI)
145	535	145-C3	Check List revisión de infraestructura	Profesional Universitario G2 - Oficina Estrategia (TI)
145	536	145-C4	Control de acceso limitado de acuerdo con las funciones	Profesional Universitario G2 - Oficina Estrategia (TI)
145	537	145-C5	Bloqueo de medios físicos	Profesional Universitario G2 - Oficina Estrategia (TI)
146	512	146-C1	Aplicar el control de permisos por usuario	Profesional Universitario G2 - Oficina Estrategia (TI)
146	538	146-C2	Acuerdo de confidencialidad de la información	Profesional Universitario G2 - Oficina Estrategia (TI)
176	653	176-C1	Blindar los datos solo a partes interesadas, en procesos de información reservada	Profesional Universitario G2 - Oficina Estrategia (TI)

7. MATRIZ DE RIESGO FISCAL

La guía de administración del riesgo versión 6 incorpora los riesgos fiscales, de acuerdo al análisis de investigaciones previas realizado por el Departamento Administrativo de la Función Pública, donde se estudiaron los fallos de responsabilidad fiscal de una muestra de 10 de las contralorías mejor calificadas en el 2022; también se tomó una muestra aleatoria de fallos de responsabilidad fiscal, en firme, emitidos por la Contraloría General de la República entre el 2020 y 2022; y se consideró un listado de hallazgos fiscales por temáticas, consolidado por la Auditoría General de la República en el 2021.

La definición del riesgo fiscal está contenida en el numeral 4.2 de la guía de administración del riesgo:

4.2 Definición y elementos del riesgo fiscal: Teniendo en cuenta la estructura y elementos de la definición de riesgos que tiene la presente guía, la cual es armónica con la norma ISO 31000, se define riesgo fiscal, así:

> ***Efecto dañoso sobre recursos públicos o bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.***

A continuación, se describen los elementos que componen la definición de riesgo fiscal:

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.

Lo anterior se puede resumir de la siguiente manera:

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

¿Qué?	¿Cómo?	¿Por qué?
Posibilidad de efectos dañoso sobre **bienes públicos**	por pérdida, extravío o hurto de bienes muebles de la entidad.	a causa de la omisión en la aplicación del procedimiento para el ingreso y salida de bienes del almacén

Para la identificación de los riesgos se recomienda revisar los puntos de riesgo fiscal (¿En qué procesos de la entidad se realiza gestión fiscal?) y consultar los hallazgos con presunta incidencia fiscal y los fallos de responsabilidad fiscal de los últimos 5 años. Para lo anterior se sugiere revisar el Anexo_1.docx de la guía de administración del riesgo.

Para la elaboración de la matriz de riesgo fiscal, se recomienda realizar un taller entre personal del nivel directivo, asesores y aquellos servidores que por su conocimiento, experiencia o formación puedan aportar especial valor, en el que, basados en las anteriores definiciones, identifiquen los puntos de riesgo fiscal (actividades de gestión fiscal en las que potencialmente se genera riesgo fiscal) y circunstancias Inmediatas (situación por la que se presenta el riesgo, pero no constituye la causa principal del riesgo fiscal). Cabe destacar que esta recomendación ya fue incluida en el Informe del estado de los riesgos correspondiente al primer semestre de 2024. Además, el 17 de diciembre se remitió un correo electrónico recordando este tema a la Oficina Estratégica. En su respuesta, la oficina indicó que habían identificado 20 riesgos fiscales, actualmente clasificados como riesgos de proceso, y que solicitaron al proveedor de la plataforma Kawak la migración de estos riesgos y sus controles a una nueva matriz de riesgos fiscales. Sin embargo, hasta el momento, dicha matriz no ha sido publicada.

8. EFECTIVIDAD DE LOS CONTROLES.

Durante el segundo semestre de 2024, la primera línea de defensa evaluó 20 controles de un total de 218, asociados a 60 riesgos de procesos. Sin embargo, no se ha evaluado ningún control relacionado con los riesgos de privacidad y seguridad de la información, ni con los de corrupción. Se recomienda avanzar con la evaluación de todos los controles, aplicando los criterios de calificación establecidos en la guía de administración del riesgo del DAFP.

9. MATERIALIZACIÓN DEL RIESGO.

Para el periodo evaluado no se han identificado riesgos materializados.

10. RECOMENDACIONES

- De un total de 85 riesgos identificados (60 correspondientes de procesos, 6 de seguridad y privacidad de la información, y 19 de corrupción), al cierre de diciembre de 2024, únicamente se han evaluado 8 relacionados con procesos. Se recomienda realizar la evaluación completa de todos los riesgos y sus respectivos controles, conforme a lo establecido en los puntos 10 (Monitoreo y Revisión) y 11 (Comunicación y Consulta) de la Política de Administración del Riesgo de la entidad.

- De acuerdo con el numeral 2.5 de la guía de administración del riesgo versión 6, se sugiere revisar la descripción del riesgo ID 87 (Perdida de negocios debido a fluctuaciones en el mercado competitivo, lo que podrá traducirse en que la competencia ofrezca servicios por menor valor en su administración y ejecución).

- El riesgo 112 tiene vinculado el control 635, cuyo nombre es "Posibilidad de afectación en el cumplimiento de solución de los requerimientos generados en las demás áreas". Sin embargo, este enunciado describe el riesgo en lugar de un control. Por lo tanto, se sugiere eliminar este control.

- El nombre del riesgo 94 hacen alusión a su descripción, se recomienda que esa información se ubique en el campo de la descripción de la matriz de riesgos y que en el nombre se mencione el riesgo de forma abreviada. En el informe del estado de los riesgos del primer semestre de 2024, también se recomendó revisar este riesgo.

- El 18 de junio de 2024 el riesgo 95 fue calificado con probabilidad muy baja y el 96 y 108, con probabilidad baja. Se sugiere revisar la valoración de los respectivos riesgos, considerando lo indicado en la página 37 de la guía de administración del riesgo versión 6 del DAFP: *"3.1.1 Determinar la probabilidad: se entiende como la posibilidad de ocurrencia 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 4 Criterios para definir el nivel de probabilidad

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

- Los nombres de los riesgos 97, 98 y 138 son idénticos a su descripción. Se recomienda modificar el campo correspondiente al nombre, empleando un texto más breve y eliminando la palabra "posibilidad", dado que esta forma parte de la descripción del riesgo.

- Los nombres de los riesgos 128, 129, 134 y 141 contienen la palabra “posibilidad”, se recomienda quitar esa palabra, utilizando un texto más conciso para el nombre.

- El riesgo 95 tiene asociado el control 405, que consiste en la revisión diaria, por parte del auxiliar de la Subgerencia de Servicios, del estado de la publicación en Gestión Transparente y SECOP, con el envío de correos en la mañana y la tarde informando sobre los contratos pendientes de publicación. Este control representa una mejora respecto al control 277, que establece un seguimiento mensual por parte del auxiliar administrativo de la Subgerencia de Servicios sobre la publicación en SECOP y Gestión Transparente. Para evitar la duplicidad de controles y no afectar el resultado del riesgo residual, se recomienda eliminar el control 277.

- El riesgo **ID152** (Daño de un bien de la entidad debido al mal uso de un funcionario) tiene cómo segundo control el Informe de análisis de posibles causas por parte del proveedor con el fin de tomar decisiones para la prevención de estos daños, se recomienda revisar este control, ya que un informe de análisis de las posibles causas de daño de un bien no es un control, ya que no está atacando la probabilidad de ocurrencia del riesgo (control preventivo), ni el impacto frente a la materialización del riesgo (control correctivo).

- Los controles 637 Ataque informático y 638 están duplicados, no son controles, además hacen referencia en su nombre y descripción al riesgo de seguridad y privacidad de la información ID143. Se sugiere eliminarlos. En el informe del estado de los riesgos del primer semestre de 2024, también se recomendó eliminar estos controles.

- El control 639 Pérdida, alteración o sustracción de Información en medio magnético o físico, no es un control, hace alusión en su nombre y descripción al riesgo de seguridad y privacidad de la información ID145. Se sugiere eliminar. En el informe del estado de los riesgos del primer semestre de 2024, también se recomendó eliminar este control.

- Los controles ID633 y 640 Alteración, divulgación o uso mal intencionado de información sensible para la Entidad, están duplicados, además hacen referencia en su nombre y descripción al riesgo de seguridad y privacidad de la información ID146. Se sugiere eliminarlos. En el informe del estado de los riesgos del primer semestre de 2024, también se recomendó eliminar estos controles.

- La guía para la administración del riesgo versión VI establecida por la Función Pública, indica en el numeral 5 los elementos para la descripción del riesgo de corrupción:

RIESGO DE CORRUPCIÓN

Definición de riesgo de corrupción:

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

"Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos" (Conpes N° 167 de 2013).

Es necesario que en la descripción del riesgo concurran los **componentes de su definición**, así:

ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO.

MATRIZ: DEFINICIÓN DEL RIESGO DE CORRUPCIÓN				
Descripción del riesgo	**Acción u omisión**	**Uso del poder**	**Desviar la gestión de lo público**	**Beneficio privado**
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

Fuente: Secretaría de Transparencia de la Presidencia de la República.

De acuerdo con lo anterior, se sugiere revisar la descripción de los siguientes riesgos (en el informe del estado de los riesgos del primer semestre de 2024, también se hizo la misma recomendación):

ID47: Riesgo de direccionamiento indebido del mercado y promoción de la venta de una Línea de negocio determinada para beneficio personal o de un tercero.

ID50: Situaciones como: Direccionar la investigación y desarrollo de nuevos productos que solo ofrezca determinado proveedor en aras de obtener un beneficio propio o para un tercero, por falta de integridad y ética, excesiva discrecionalidad y falta de controles al momento de revisar el proceso.

ID51: Se trata de recibir o solicitar cualquier dadiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato, y que pueden generar un riesgo de corrupción en la contratación de la empresa; como por ejemplo establecer requisitos o exigencias en los pliegos de condiciones para los procesos de selección, y que solo cumple un determinado proponente.

- La guía de administración del riesgo versión 6 indica referente al tratamiento de los riesgos de corrupción, que la respuesta será evitar, compartir o reducir el riesgo; pero no pueden ser aceptados o asumidos. De acuerdo con lo anterior, de los 19 riesgos de corrupción, el 51, 53, 54, 58 y 63 tienen cómo respuesta a la aceptación un “no”, se sugiere para los demás modificar la respuesta. Esta recomendación también se dio en el informe del estado de los riesgos del primer semestre de 2024.

- El control "Capacitación y campañas sobre riesgos de corrupción y sus consecuencias", asociado a los riesgos 47, 48 y 50, se ha implementado parcialmente mediante

inducciones dirigidas al personal que ingresa a la entidad. Sin embargo, en el plan anual de capacitaciones de 2024 no se incluyeron formaciones destinadas a todo el personal, ni se han llevado a cabo campañas. Por lo tanto, se recomienda incorporar estas actividades en el plan de 2025.

- Se recomienda cambiar el nombre del control 160 Procedimiento *PR-M6-DOC-02 para recepción de correspondencia*, este hace referencia al procedimiento *PR-M3-DOC-2, recepción, organización y distribución de la documentación*. También se sugiere modificar el nombre del control *161 Procedimiento PR-M6-DOC-05 para recepción de propuestas*, la codificación correcta del procedimiento es *PR-M3-5, recepción de propuestas para solicitud pública de oferta*. Esta recomendación también se dio en el informe del estado de los riesgos del primer semestre de 2024.

- El riesgo 61 Aceptar documentación adulterada y/o falsa de candidatos para procesos de vinculación, tiene asignado cómo responsable al técnico administrativo de la Unidad de Contabilidad y costos, el responsable es el técnico administrativo de la Unidad de Gestión Humana. Esta recomendación también se dio en el informe del estado de los riesgos del primer semestre de 2024.

- La guía de administración del riesgo versión 6 del DAFP establece que se debe publicar en la página web de la entidad, el mapa de riesgos de corrupción a más tardar el 31 de enero de cada año. Se sugiere proceder con la actualización del mapa de riesgos y su publicación.

- En la plataforma Kawak se encuentra la opción de registrar los seguimientos a la evaluación de los controles, pero sólo se tiene registro de los controles asociados a los riesgos de la Dirección de Auditoría Interna. Se recomienda emplear esta herramienta para facilitar la verificación de la gestión de los riesgos y el cumplimiento y eficiencia de los controles.

11. CONCLUSIONES

- Desde la oficina estratégica se está liderando la actualización de la matriz de riesgos, pero al 31 de diciembre sólo se han evaluado 8 riesgos de procesos de un total de 60 (13,33%), a esa fecha ningún riesgo de seguridad y privacidad de la información, ni de corrupción ha sido evaluado. Es importante efectuar los seguimientos periódicos y evaluaciones oportunas que permitan gestionar las causas o factores que puedan o pudieron provocar una situación de peligro o incertidumbre para la entidad.

- No se está registrando la ejecución de los controles en la plataforma Kawak, salvo en el caso de los riesgos asociados a la Dirección de Auditoría Interna. Este registro es fundamental para que la segunda y tercera línea de defensa puedan llevar a cabo de manera efectiva las actividades de monitoreo y revisión, ya que permite contar con evidencia del cumplimiento de los controles.

- De acuerdo con los lineamientos establecidos en la Guía de Administración del Riesgo (versión 6) para el análisis del riesgo fiscal, la entidad tiene la obligación de elaborar una matriz que identifique este tipo de riesgos, especificando los controles necesarios para mitigar tanto la probabilidad como el impacto de los efectos dañosos sobre los recursos públicos, bienes e intereses patrimoniales de naturaleza pública derivados de eventos potenciales. En el informe del estado de los riesgos correspondiente al primer semestre de 2024, se recomendó construir y publicar dicha matriz. La Oficina Estratégica indicó en el mes de diciembre que se han identificado 20 riesgos fiscales y que se escaló con el proveedor del kawak la construcción de la matriz en dicha plataforma, pero a la fecha no se ha procedido con su publicación.

Atentamente,

Jorge Hernán Lopera Taborda
Director Auditoría Interna

Proyectó: Diego Armando Botero Zuluaga **–** Auditor Contable.