INFORME DE VERIFICACIÓN AL ESTADO DE LOS RIESGOS DE PROCESOS, CORRUPCIÓN Y SISTEMA DE INFORMACIÓN DE LA EMPRESA PARA LA SEGURIDAD Y SOLUCIONES URBANAS – ESU –SEGUNDO SEMESTRE 2023 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, marzo de 2024

INFORME DE VERIFICACIÓN AL ESTADO DE LOS RIESGOS DE PROCESOS, CORRUPCIÓN Y SISTEMA DE INFORMACIÓN DE LA EMPRESA PARA LA SEGURIDAD Y SOLUCIONES URBANAS – ESU – SEGUNDO SEMESTRE 2023 Y SEGUIMIENTO A LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

Tabla de contenido

INTRODUCCIÓN

La evaluación de la gestión del riesgo ha sido contemplada como uno de los componentes del Sistema de Control interno dentro del Modelo Integrado de Planeación y Control (MIPG) entre los que se contempla para auditoría interna, la verificación de aquellos eventos, tanto internos como externos que puedan afectar o impedir el logro de los objetivos estratégicos, eventos que permitan identificar oportunidades para un mejor cumplimiento de su función; los cuales se desarrollan en la ley 87 de 1993 y en los Decretos 648 y 1499 de 2017.

Es preciso resaltar que el seguimiento de este Mapa de Riesgos por parte de la Dirección de Auditoría Interna (tercera línea de defensa), consiste en la verificación de las acciones realizadas frente al riesgo identificado; sin embargo, se deja constancia que cada líder de proceso realizará de forma periódica el análisis de la valoración de sus riesgos aplicando la Guía metodológica para la administración del riesgo versión VI, establecida por la Función Pública en diciembre de 2022.

Dicha guía trae una nueva calificación en cuanto al nivel de probabilidad e impacto del riesgo, esto para verificar que efectivamente los controles establecidos cumplen con el objetivo de reducir el riesgo y prevenir su materialización, actividad que deberá realizarse en conjunto con la Oficina Estratégica de la ESU y de la profesional encargada de Planeación estratégica (Segunda Línea de Defensa).

Por tanto, este informe tiene como finalidad hacer la verificación a la gestión del riesgo, realizada por la entidad en el segundo semestre de 2023 (Julio 01 – Diciembre 31), evaluando la matriz de riesgos identificados por los diferentes líderes de procesos y sus comités operativos (Primera Línea de Defensa), y las acciones diseñadas para su mitigación, registradas por cada una de las áreas, evidenciando el estado de los riesgos y su grado de mitigación; o en su defecto la identificación de nuevos riesgos y controles; Igualmente se hará seguimiento, a la política de gestión del riesgo de la entidad.

OBJETIVO

Realizar la verificación a los riesgos estratégicos para el segundo semestre de 2023, 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.

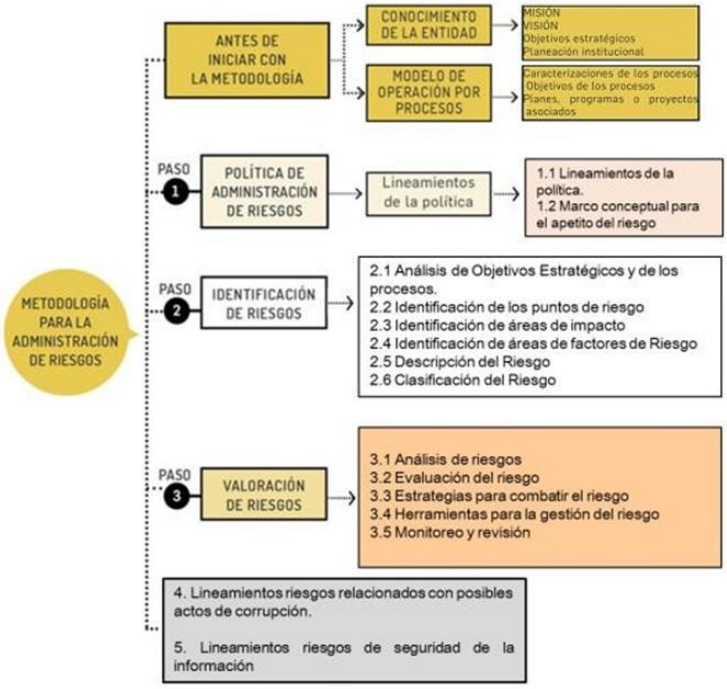
ALCANCE

Verificación de los riesgos de cada uno de los procesos de la entidad en el periodo comprendido entre julio 01 a diciembre 31 de 2023.

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
(Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2022)

Tabla de Criterios para definir la frecuencia de la actividad

	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.

	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

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 tuvieron en cuenta 16, para corrupción 19 y, finalmente para seguridad y privacidad de la información se determina la existencia de 5 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 los 16 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:

- 2 nivel alto.
- 8 nivel moderado.
- 6 nivel bajo.

Matriz de Calor Inherente		Impacto				
Probabilidad	Muy alto 100%					
	Alta 80%					
	Media 60%		I134			
	Baja 40%	I140 I141 I152	I138 I155 I159	I137 I150	I142	
	Muy baja 20%		I139 I151 I157	I156 I160	I154	
		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:

Matriz de Calor Inherente		Impacto				
Probabilidad	Muy alto 100%					
	Alta 80%					
	Media 60%					
	Baja 40%		R159C1		R142C1	
	Muy baja 20%	R140C2 R141C2 R152C2	R134C3 R138C3 R139C3 R151C4 R155C6 R157C1	R137C2 R150C4 R156C2 R160C1	R154C2	
		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%

Extremo
Alto
Moderado
Bajo

Con los controles implantados, la matriz residual ubica:

- 2 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 a lo anterior, se tienen diseñados y establecidos 39 controles para los 16 riesgos, todos son de tipo preventivo, pero en su implementación 35 son manuales y 4 automáticos, factor que se puede mejorar con el fin de aumentar la eficiencia de los controles, disminuyendo el riesgo residual.

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

A continuación, se relacionan los 39 controles de los 16 riesgos de procesos:

ID	Nombre	Responsable de ejecución
134-C1	Política de seguridad y privacidad de la información	- Profesional Universitario G2 - Oficina Estrategia (TI)
134-C2	Check list revisión de infraestructura	- Profesional Universitario G2 - Oficina Estrategia (TI)
134-C3	Control de Data Center	- Profesional Universitario G2 - Oficina Estrategia (TI)
137-C1	El Profesional Universitario y/o Técnico de Gestión Humana, realizan calendario de liquidación de nómina, prestaciones sociales, seguridad social y parafiscales	- Profesional Universitario G1- Unidad de Gestión Talento Humano (Nom)
137-C2	Procedimiento actualizado y/o pago parametrizado	- Profesional Universitario G1- Unidad de Gestión Talento Humano (Nom)

ID	Nombre	Responsable de ejecución
138-C1	Mantenimiento preventivo	- Profesional Universitario - Unidad de Bienes y Servicios
138-C2	Control de requerimientos internos	- Profesional Universitario - Unidad de Bienes y Servicios
138-C3	Campañas de sensibilización sobre el cuidado de los bienes de la entidad	- Profesional Universitario - Unidad de Bienes y Servicios
139-C1	Aplicar procedimiento de recepcion	- Tecnico Administrativo G2- Unidad de Gestión Documental (3)
139-C2	Revisión de documentos recibidos electrónica y físicamente	- Tecnico Administrativo G2- Unidad de Gestión Documental (3)
139-C3	Comparar la relación de las facturas recibidas contra las radicadas	- Tecnico Administrativo G2- Unidad de Gestión Documental (3)
140-C1	Revision de los funcionarios asociados a las diferentes rutas de los flujos documentales	- Tecnico Administrativo G2- Unidad de Gestión Documental (3)
140-C2	Reception de los permisos solicitados a cada funcionario con el fin de tener acceso a la información según el perfil del funcionario	- Tecnico Administrativo G2- Unidad de Gestión Documental (3)
141-C1	Consolidación y gestión de publicación de la información	- Profesional Especializado - Oficina Estrategica - Director Auditoria Interna - Profesional Universitario - Oficina Estrategia (Comunicaciones)
141-C2	Envio de información correspondiente	- Profesional Especializado - Oficina Estrategica
142-C1	Los Profesionales del área contable, elaboran cada vigencia la lista de chequeo sobre la información a presentar, de acuerdo con cronograma, normatividad y realizan seguimiento a su cumplimiento.	- Lider De Programa - Unidad de Contabilidad y Costos
150-C1	Establecer en comun acuerdo el plazo y condiciones para cumplir requisitos de la firma y legalización del contrato.	- Profesional Universitario G1 - Unidad de Mercadeo y Ventas (1)
150-C2	Comunicación constante con el cliente	- Profesional Universitario G1 - Unidad de Mercadeo y Ventas (1)
150-C3	Disponibilidad de personal a cargo para la revisión de la plataforma Secop II constantemente.	- Profesional Universitario G1 - Unidad de Mercadeo y Ventas (1)
150-C4	Gestionar solicitud de firmas vía correo electronico.	- Profesional Universitario G1 - Unidad de Mercadeo y Ventas (1)
151-C1	Realizar un analisis a los planes de adquisicion y los planes de desarrollo a los clientes actuales y potenciales para verificar las necesidades de contratación.	- Profesional Universitario G1 - Unidad de Mercadeo y Ventas (1)
151-C2	Cumplimiento con la atención del servicio al cliente	- Profesional Universitario G1 - Unidad de Mercadeo y Ventas (1)
151-C3	Inventario de clientes actuales y del año inmediatamente anterior.	- Profesional Universitario G1 - Unidad Compras y Contratación (1)
151-C4	Plan de mercadeo anual.	- Profesional Universitario G1 - Unidad de Mercadeo y Ventas (1)

ID	Nombre	Responsable de ejecución
152-C1	Realizar capacitaciones sobre el buen uso de los bienes	- Profesional Universitario - Unidad de Bienes y Servicios
152-C2	Informe de análisis de posibles causas del daño	- Profesional Universitario - Unidad de Bienes y Servicios
154-C1	Planeación anual de informes de ley	- Director Auditoria Interna
154-C2	Comunicación asertiva con planeación institucional	- Director Auditoria Interna - Profesional Universitario - Auditoria Interna (1) - Profesional Universitario - Auditoria Interna (2) - Profesional Universitario - Auditoria Interna (3)
155-C1	Políticas del proceso de gestión del talento humano	- Profesional Universitario G1- Unidad de Gestión Talento Humano (Nom)
155-C2	Plan de bienestar institucional	- Profesional Universitario G1- Unidad de Gestión Talento Humano (Nom)
155-C3	Plan de capacitación	- Profesional Universitario G1- Unidad de Gestión Talento Humano (Nom)
155-C4	Pago oportuno de nomina	- Profesional Universitario G1- Unidad de Gestión Talento Humano (Nom)
155-C5	Infraestructura y puestos de trabajo adecuados	- Profesional Universitario G1- Unidad de Gestión Talento Humano (Nom)
155-C6	Gestionar el ambiente laboral y el riesgo psicosocial	- Lider De Programa - Unidad de Gestión Talento Humano
156-C1	Cumplimiento de requisitos legales asociados a normas de riesgos laborales.	- Profesional Universitario G1- Unidad de Gestión Talento Humano (Nom)
156-C2	Evaluación de estándares mínimos	- Profesional Universitario G1- Unidad de Gestión Talento Humano (Nom)
157-C1	Planeación anual de informes de ley	- Director Auditoria Interna
159-C1	Capacitaciones periódicas	- Director Auditoria Interna
160-C1	Solicitar mensualmente al SENA el paz y salvo	- Profesional Universitario G1- Unidad de Gestión Talento Humano (Nom)

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		
Baja 40%			I47 I50 I60 I48 I56 I61 I149 I59	I51 I55 I63 I53 I57 I54 I58	
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:

Matriz de Calor Inherente	Impacto				
Probabilidad					
Muy alto 100%					
Alta 80%					
Media 60%	R46C1				
Baja 40%	R48C2 R49C1 R50C2				
Muy baja 20%	R45C3 R47C3	R44C2 R52C3 R57C4	R56C2 R61C1 R59C6 R60C4	R51C7 R55C5 R53C3 R58C4 R54C5 R63C4	
	Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%

Extremo
Alto
Moderado
Bajo

Con los controles implantados, la matriz residual ubica:

- 6 riesgos nivel alto.
- 4 riesgos nivel moderado.
- 9 riesgos nivel bajo.

En la anterior matriz se ubicaron los últimos controles implementados para cada riesgo. De acuerdo a 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 39 controles de los 16 riesgos de riesgos de corrupción:

ID	Nombre	Responsable de ejecución
44-C1	Seguimiento a los planes en comité del sistema integrado de gestión	Jefe de Oficina Estrategica
44-C2	Seguimiento realizado por el proceso de Auditoría Interna	Jefe de Oficina Estrategica
45-C1	Aprobación y cierre en el software por parte del Profesional especializado de la oficina estratégica	Jefe de Oficina Estrategica
45-C2	Comité del sistema integrado de gestión o comité de gestión y desempeño	Jefe de Oficina Estrategica
45-C3	Seguimiento por parte del proceso de Auditoría Interna	Jefe de Oficina Estrategica
46-C1	Politicas de comunicación corporativa ESU	Profesional Universitario - Oficina Estrategia (Comunicaciones)
46-C2	Plan de medios, espacios y formas de comunicación internos y externos	Profesional Universitario - Oficina Estrategia (Comunicaciones)
47-C1	Capacitación y campañas sobre riesgos de corrupción y sus consecuencias.	Subgerente Comercial y De Mercadeo
47-C2	Documentación del proceso de contratación y realización de auditorías	Subgerente Comercial y De Mercadeo
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-C1	Documentación del proceso y realización de auditorias.	Subgerente Comercial y De Mercadeo
48-C2	Capacitación y campañas sobre riesgos de corrupción y sus consecuencias	Subgerente Comercial y De Mercadeo
49-C1	Inducción sobre riesgos de corrupción y sus consecuencias.	Profesional Universitario - Oficina Estrategia (Comunicaciones)
50-C1	Capacitación y campañas sobre riesgos de corrupción y sus consecuencias.	Gerente General
50-C2	Documentación del proceso y realización de auditorías.	Gerente General
51-C1	Comité asesor de contratación	Lider De Programa - Unidad de compras y contratación

ID	Nombre	Responsable de ejecución
51-C2	Formato informe de evaluación	Lider De Programa - Unidad de compras y contratación
51-C3	Revisión jurídica de pliegos y/o estudios previos antes de su publicación	Lider De Programa - Unidad de compras y contratación
51-C4	Aprobación de la adenda por el o los subgerente(s) del área	Lider De Programa - Unidad de compras y contratación
51-C5	Estudios previos y/o referenciamiento de precios mínimo con dos posibles proponentes	Lider De Programa - Unidad de compras y contratación
51-C6	Redacción interdisciplinaria de Pliegos de condiciones	Lider De Programa - Unidad de compras y contratación
51-C7	Sensibilización para la prevención y control de riesgos de corrupción	Lider De Programa - Unidad de compras y contratación
52-C1	Informes de supervisión	Lider De Programa - Unidad de Logística
52-C2	Seguimiento a la supervisión de contratos	Lider De Programa - Unidad de Logística
52-C3	Sensibilización para la prevención y control de riesgos de corrupción	Lider De Programa - Unidad de Logística
53-C1	Aprobación del subgerente administrativo y financiero y acto administrativo por medio de traslado firmado por el gerente	Lider De Programa - Unidad de Presupuesto
53-C2	Procedimientos del proceso: ejecución y seguimiento del presupuesto. Procedimiento modificaciones presupuestales	Lider De Programa - Unidad de Presupuesto
53-C3	Parametrización del Software Financiero	Lider De Programa - Unidad de Presupuesto
54-C1	Procedimientos y políticas de gestión contable	Lider De Programa - Unidad de Contabilidad y Costos
54-C2	Desagregación de los procesos contables en diferentes personas del área	Lider De Programa - Unidad de Contabilidad y Costos
54-C3	Comité financiero	Lider De Programa - Unidad de Contabilidad y Costos
54-C4	Conciliación entre contabilidad y los demás módulos que transfieren información a contabilidad	Lider De Programa - Unidad de Contabilidad y Costos
54-C5	Presentación de estados financieros al comité financiero y de gerencia	Lider De Programa - Unidad de Contabilidad y Costos
55-C1	Modelo de selección bancario	Tesorero General
55-C2	Comité financiero	Tesorero General
55-C3	Manual de inversiones	Tesorero General
55-C4	Políticas de tesorería: Políticas de seguridad en las operaciones de tesorería - Política Pago de Obligaciones	Tesorero General
55-C5	Matriz de pares	Tesorero General
56-C1	Lista de chequeo de contrato interadministrativo	Profesional Universitario - Unidad de Liquidación de Convenios (1)

ID	Nombre	Responsable de ejecución
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-C1	Comité asesor de contratación	Lider De Programa - Unidad de Logística
57-C2	Formato informe de evaluación	Lider De Programa - Unidad de Logística
57-C3	Revisión jurídica de pliegos y/o estudios previos antes de su publicación	Lider De Programa - Unidad de Logística
57-C4	Informes de supervisión	Lider De Programa - Unidad de Logística
58-C1	Acceso restringido al sistema de gestión documental	Profesional Universitario G1 - Gestión documental
58-C2	Políticas de gestión documental donde se limita el préstamo de documentos físicos	Profesional Universitario G1 - Gestión documental
58-C3	Proceso de inducción obligatoria a todo el personal nuevo que ingresa a la empresa.	Profesional Universitario G1 - Gestión documental
58-C4	Procedimiento PR-MG-DOC-03 para consulta de los documentos en la Unidad de Gestión Documental.	Profesional Universitario G1 - Gestión documental
59-C1	Proceso de inducción obligatoria a todo el personal nuevo que ingresa a la empresa.	Profesional Universitario G1 - Gestión documental
59-C2	Procedimiento PR-M6-DOC-02 para recepción de correspondencia	Profesional Universitario G1 - Gestión documental
59-C3	Procedimiento PR-M6-DOC-05 para recepción de propuestas	Profesional Universitario G1 - Gestión documental
59-C4	Cámaras de video con grabación de video y registro de hora.	Profesional Universitario G1 - Gestión documental
59-C5	Relojes en la recepción y en el archivo.	Profesional Universitario G1 - Gestión documental
59-C6	Aplicación de la circular 14 y circular 06 de 2019	Profesional Universitario G1 - Gestión documental
60-C1	Parametrización del sistema de liquidación y cruce con contabilidad y tesorería para que se valide las acreencias laborales.	Tecnico Administrativo G1- Unidad de Contabilidad y Costos (3)
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.	Tecnico Administrativo G1- Unidad de Contabilidad y Costos (3)
60-C3	Informe del sistema sobre las diferencias entre lo liquidado y pagado.	Tecnico Administrativo G1- Unidad de Contabilidad y Costos (3)
60-C4	Existencia de los soportes que autoricen el reconocimiento y pago de los beneficios	Tecnico Administrativo G1- Unidad de Contabilidad y Costos (3)
61-C1	Procedimiento reclutamiento, selección y vinculación de personal	Tecnico Administrativo G1- Unidad de Contabilidad y Costos (3)
63-C1	Aplicación Politica de seguridad y privacidad de la información	Profesional Universitario G2 - Oficina Estrategia (TI)

ID	Nombre	Responsable de ejecución
63-C2	Configuración de los perfiles de usuarios y permisos de acceso a los sistemas	Profesional Universitario G2 - Oficina Estrategia (TI)
63-C3	Oportunidad en el reporte de novedades de personal (retiros/vacaciones)	Profesional Universitario G2 - Oficina Estrategia (TI)
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 5 riesgos, se obtiene la matriz de riesgos 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.
- 1 nivel moderado.
- 3 nivel bajo.

Matriz de Calor Inherente		Impacto				
Probabilidad	Muy alto 100%					
	Alta 80%					
	Media 60%					
	Baja 40%					
	Muy baja 20%		I144 I145 I146	I81	I143	
		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%

Extremo
Alto
Moderado
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:

Matriz de Calor Inherente		Impacto				
Probabilidad	Muy alto 100%					
	Alta 80%					
	Media 60%					
	Baja 40%					
	Muy baja 20%		R144C3 R145C5 R146C2	R81C3	R143C2	
		Leve 20%	Menor 40%	Moderado 60%	Mayor 80%	Catastrófico 100%

Extremo
Alto
Moderado
Bajo

Con los controles implantados, la matriz residual ubica:

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

En la anterior matriz se ubicaron los últimos controles implementados para cada riesgo. De acuerdo a lo anterior, se tienen diseñados y establecido 15 controles para los 5 riesgos, todos son preventivos; pero en su implementación 12 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 15 controles de los 5 riesgos de riesgos de seguridad y privacidad de la información:

Código	Nombre	Responsable de ejecución
81-C1	Capacitar en política de seguridad de la información	Profesional Universitario G2 - Oficina Estrategia (TI)
81-C2	Inducción nuevos funcionarios y contratistas	Profesional Universitario G2 - Oficina Estrategia (TI)
81-C3	Documento de clasificación de información Publica Reservada	Profesional Universitario G2 - Oficina Estrategia (TI)
143-C1	Capacitar en política de seguridad de la información	Profesional Universitario G2 - Oficina Estrategia (TI)
143-C2	Control documento de clasificación de información Publica Reservadoá	Profesional Universitario G2 - Oficina Estrategia (TI)
144-C1	Aplicar procedimientos de seguridad de la información	Profesional Universitario G2 - Oficina Estrategia (TI)
144-C2	Control documento de clasificación de información Publica Reservado	Profesional Universitario G2 - Oficina Estrategia (TI)
144-C3	Check List revisión de infraestructura	Profesional Universitario G2 - Oficina Estrategia (TI)
145-C1	Realizar copias de seguridad	Profesional Universitario G2 - Oficina Estrategia (TI)
145-C2	Control documento de clasificación de información Publica Reservado	Profesional Universitario G2 - Oficina Estrategia (TI)
145-C3	Check List revisión de infraestructura	Profesional Universitario G2 - Oficina Estrategia (TI)
145-C4	control de acceso limitado de acuerdo con las funciones	Profesional Universitario G2 - Oficina Estrategia (TI)
145-C5	Bloqueo de medios físicosá	Profesional Universitario G2 - Oficina Estrategia (TI)
146-C1	Aplicar el control de permisos por usuario	Profesional Universitario G2 - Oficina Estrategia (TI)
146-C2	acuerdo de confidencialidad de la información	Profesional Universitario G2 - Oficina Estrategia (TI)

7. EFECTIVIDAD DE LOS CONTROLES

Para la evaluación de los controles en este periodo, se implementó la metodología actualizada por el DAFP, empleando los siguientes criterios de calificación.

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	25%

Características			Descripción	Peso
			intervención de personas para su realización.	
		Manual	Controles que son ejecutados por una persona, tiene implícito 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.	-

8. MATERIALIZACIÓN DEL RIESGO

Para el periodo evaluado se materializó el riesgo ID 157 (Incumplimiento del plan anual auditorías), originado por la causa 3 del respectivo riesgo: ausencia de líder responsable para la aprobación de dichos informes (origen: Interno, factor: Recurso humano).

9. RECOMENDACIONES

- Teniendo en cuenta cómo se describe el riesgo según la guía metodológica para la administración del riesgo versión VI establecida por la Función Pública, se sugiere revisar los siguientes riesgos, ya que sus nombres son iguales a sus descripciones:

  ID134: Posibilidad de afectación de los sistemas de información por pérdida de información debido a ataques cibernéticos, caída de aplicaciones, daño en equipos, caída de redes o errores en los programas.

  ID138: Posibilidad de pérdida reputacional por hallazgos, sanciones de entes de control o insatisfacción de los grupos de valor, debido al incumplimiento normativo en el desarrollo de actividades para la provisión de bienes y servicios.

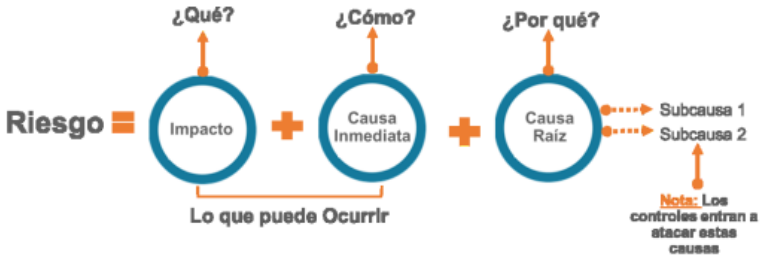
  ID139: Pérdida económica y reputacional por quejas, demandas o sanciones debido al inadecuado manejo del sistema de gestión documental y desconocimiento de los lineamientos de radicación.

  ID140: Afectación reputacional por perdida de confidencialidad debido a inadecuada configuración de roles y permisos en el sistema de gestión documental.

  ID142: Posibilidad de afectación económica y reputacional por procesos penales, fiscales, judiciales o disciplinarios y posibles incumplimientos contractuales, debido a Inexactitud e inoportunidad en la información legal y obligatoria (Suministro de información no confiable o extemporánea

2.5 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:

Figura 10 Estructura propuesta para la redacción del riesgo



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

- Los riesgos relacionados a continuación no tienen su respectiva descripción en la plataforma Kawak, se recomienda completarlos:

ID 55: Fraude en la gestión de tesorería:

FICHA TÉCNICA

INFORMACIÓN GENERAL

Id	55	Código	
Fecha identificación	2019-04-23		
Nombre	Fraude en la gestión de tesorería	Descripción	
Alcance	Organización	Responsable (Por cargos)	Tesorero General
Actividad relacionada			
Procesos	• Gestion de Tesoreria	Sedes	
¿Riesgo de seguridad de la información?	No		

ID 56: Traslado de recursos a cuentas que no corresponden con el titular en favorecimiento de un tercero:

INFORMACIÓN GENERAL

Id	56	Código	
Fecha identificación	2019-04-23		
Nombre	Traslado de recursos a cuentas que no corresponden con el titular en favorecimiento de un tercero	Descripción	
Alcance	Organización	Responsable (Por cargos)	Profesional Universitario - Unidad de Liquidación de Convenios (1)
Actividad relacionada			
Procesos	• Gestion de Liquidacion Convenios	Sedes	
¿Riesgo de seguridad de la información?	No		

- Para el riesgo **ID137** (Reprocesos por información de nómina errada) revisar en detalle la causa (Falencias en las competencias del recurso humano por falta de capacitación, inadecuada parametrización en el sistema y actualizaciones en la normatividad vigente), de la redacción presente se podrían inferir tres causas lo que daría como resultado proceder con la construcción y el diseño de controles para cada una de ellas.

- Se recomienda para el riesgo **ID141** (Posibilidad de afectación económica por multas o sanciones por un ente regulador) diseñar nuevos controles para la prevención de materialización de este riesgo. Por lo que sería de suma importancia, que abarque una capacitación o concientización de ello como control preventivo.

- El riesgo **ID150** (Posibilidad de afectación económica y/o reputacional por demoras en el proceso de legalización de contratos interadministrativos), contiene la siguiente descripción: *Posibilidad de que se presente retrasos en el proceso de firmas de los contratos lo cual se puede traducir en perdida de un cliente y afectación de la imagen corporativa*. Se recomienda revisar la descripción, ya que en esta no debe ir los posibles efectos de materialización del riesgo, sino las causas de acuerdo a lo definido por la guía metodológica para la administración del riesgo versión VI establecida por la Función Pública.

- 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, se

recomienda revisar este control, ya que un informe de análisis de las posibles causas de daño de un bien no sería un control efectivo.

- Se recomienda revisar los controles del riesgo **ID156** (Mala conformación del copasst)**:** en los controles propuestos para dicho riesgo se plantea el objetivo y no los medios como se desea alcanzar, por lo que es importante precisar la forma en cómo se aplica o se quiere aplicar este.

- Se recomienda ampliar las causas del riesgo **ID157** (Incumplimiento del plan anual auditorías), incluyendo la imposibilidad u obstáculos de recibir información de los responsables de los procesos.

- Se recomienda a la segunda línea de defensa (lideres de procesos) efectuar la evaluación de los riesgos y controles de forma oportuna, ya que desde agosto del 2023 no se ha realizado.

- En la plataforma Kawak se encuentra la opción de registrar los seguimientos a la evaluación de los controles, pero no se tiene ningún registro. Se recomienda emplear esta herramienta para facilitar la verificación de la gestión de los riesgos y el cumplimiento y eficiencia de los controles.

- Se recomienda analizar la posibilidad y pertinencia de rediseñar y reestructurar los controles para los riesgos en los que no se mitiga ni la probabilidad ni el impacto.

10. CONCLUSIONES

- Los riesgos se encuentran medidos a agosto del 2023 por parte de la segunda línea, lo que sugiere que se deben implementar 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.

- A pesar de los cambios realizados por la adopción de la guía versión 6 del DAFP, ninguno de los riesgos residuales asociados a la gestión estuvo en riesgo extremo; esto debido a que los

controles que se tienen actualmente para la entidad son satisfactorios para evitar un riesgo extremo (ver tabla de riesgo residual de la gestión de procesos y tabla de controles asociados).

Atentamente,

Jorge Hernán Lopera Taborda
Director Auditoría Interna

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