INFORME DE VERIFICACIÓN AL ESTADO DE LOS RIESGOS DE LOS PROCESOS DE LA EMPRESA PARA LA SEGURIDAD Y SOLUCIONES URBANAS – ESU – TERCER CUATRIMESTRE 2022 Y SEGUIMIENTO A LA POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

Presentado a:

EDWIN MUÑOZ ARISTIZABAL

Gerente General ESU

Preparado por:

Equipo de Auditoría Interna ESU

Elaborado por:

Equipo de Auditoría Interna

Medellín, diciembre de 2022

INFORME DE VERIFICACIÓN AL ESTADO DE LOS RIESGOS DE LOS PROCESOS DE LA EMPRESA PARA LA SEGURIDAD Y SOLUCIONES URBANAS – ESU – PRIMER CUATRIMESTRE 2022 Y SEGUIMIENTO A LA POLITICA DE ADMINISTRACIÓN DEL RIESGO

Tabla de contenido

INTRODUCCIÓN ***3***

OBJETIVO ***3***

ALCANCE ***4***

1. Metodología **4**

Tabla de Criterios para definir la frecuencia de la actividad ***5***

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 gestión 2022 9

5. MATRIZ DE RIESGOS DE CORRUPCIÓN **10**

5.1 Matriz de riesgos inherente 10

5.2 Matriz de riesgos residual 10

5.3 tipificación de acciones y controles para mitigación del riesgo de corrupción 2022 11

6. MATRIZ DE RIESGOS DE SEGURIDAD DIGITAL **13**

6.1 Matriz de riesgo inherente 13

6.2 Matriz de riesgos residual 13

7. EFECTIVIDAD DE LOS CONTROLES **14**

8. MATERIALIZACIÓN DEL RIESGO **16**

9. RECOMENDACIONES **16**

10. CONCLUSIONES **17**

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 V, establecida por la Función Pública en diciembre de 2020.

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 tercer cuatrimestre de 2022 (Septiembre 1 – 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 tercer cuatrimestre de 2022, de acuerdocon 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.

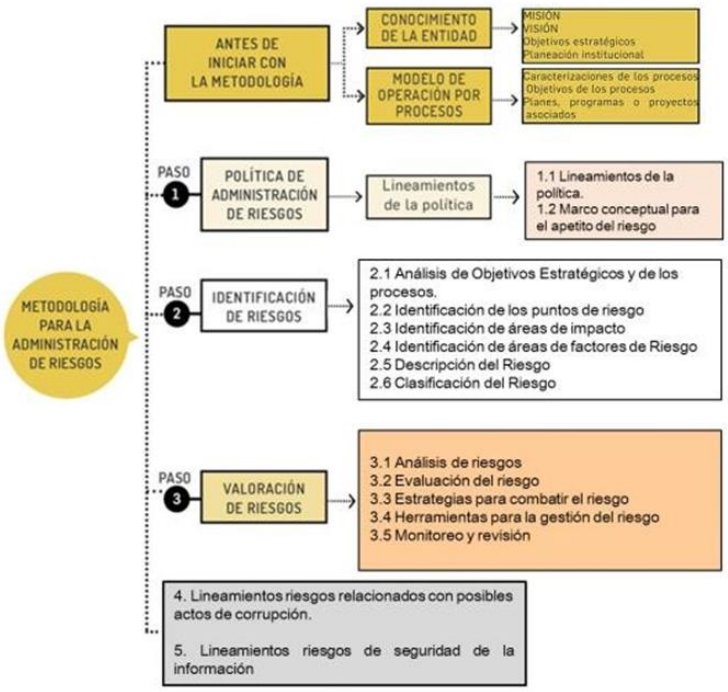
ALCANCE

Verificación de los riesgos de cada uno de los procesos de la entidad en el periodo comprendido septiembre 1 al 31 de diciembre de 2022.

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, 2020)

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 a los riesgos de procesos se tuvo en cuenta 12 riesgos, para corrupción 11 riesgos y, finalmente para seguridad de la información se determina la existencia de 5 riesgos. Es importante precisar que la información anterior se apoya en 16 procesos organizacionales.

3. ADMINISTRACIÓN DEL RIESGO

Matriz de Riesgo Integrado de Gestión de Procesos

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

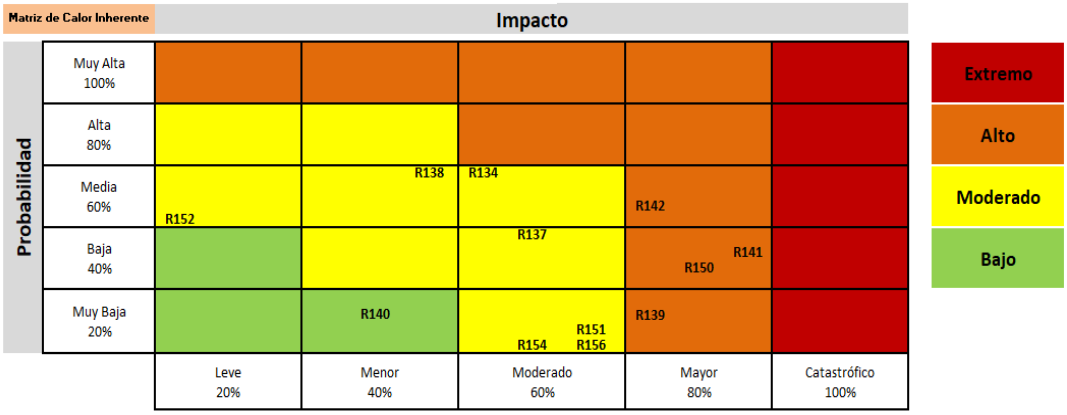
4. MATRIZ DE RIESGOS DE PROCESOS

4.1 Matriz de riesgos inherente

Después de realizada la identificación, análisis y evaluación de los 12 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.

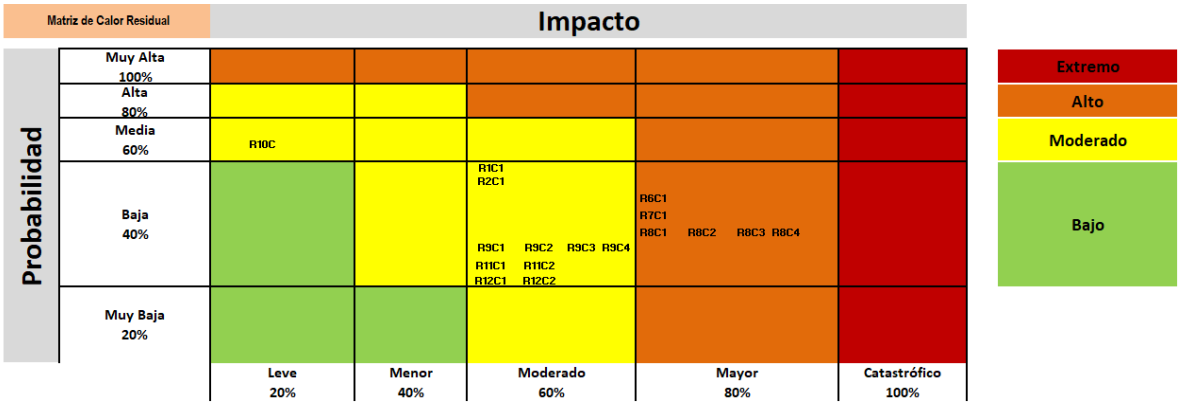
De acuerdo con esta matriz de riesgos inherente se encuentran:

- 4 nivel Alto
- 7 nivel moderado
- 1 nivel 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 implantadas las acciones para el manejo de los riesgos se obtiene la matriz de riesgos residual:



Con los controles implantados, la matriz residual ubica:

- 6 riesgos nivel Alto
- 11 riesgos nivel moderado

De acuerdo a lo anterior, se tienen diseñados y establecidos 17 controles, ya que para cada uno de los riesgos en su mayoría se gestiona el mismo con la construcción de más de un control. Así mismo, se verifica detalladamente y se evidencia que para el 80% aproximadamente de ellos no se encuentra documentado su procedimiento.

Así mismo, la mayoría de las implementaciones de estos controles son manuales lo cual presenta un factor a mejorar y a fortalecer en la eficacia de este proceso. Para esto, se sugiere el diseño de un plan y cronograma que complemente la construcción de la documentación del procedimiento de los controles diseñados.

Finalmente, Se concluye que un control es de tipo correctivo, y 16, son de tipo preventivo. En concordancia con lo expuesto anteriormente, se recomienda seguir trabajando activamente en el fortalecimiento para la identificación de posibles nuevos riesgos y continuar con la concientización de la importancia de estos en orientación al cumplimiento de objetivos y metas organizacionales.

4.3 Tipificación de acciones y controles para mitigación del riesgo de gestión 2022

En la matriz de riesgos de gestión de procesos en el periodo evaluado se cuenta 17 controles, de acuerdo con los resultados se encuentran 6 de ellos en una zona de riesgo residual nivel ALTO y los 11 controles restantes están en un nivel de zona residual nivel MODERADO.

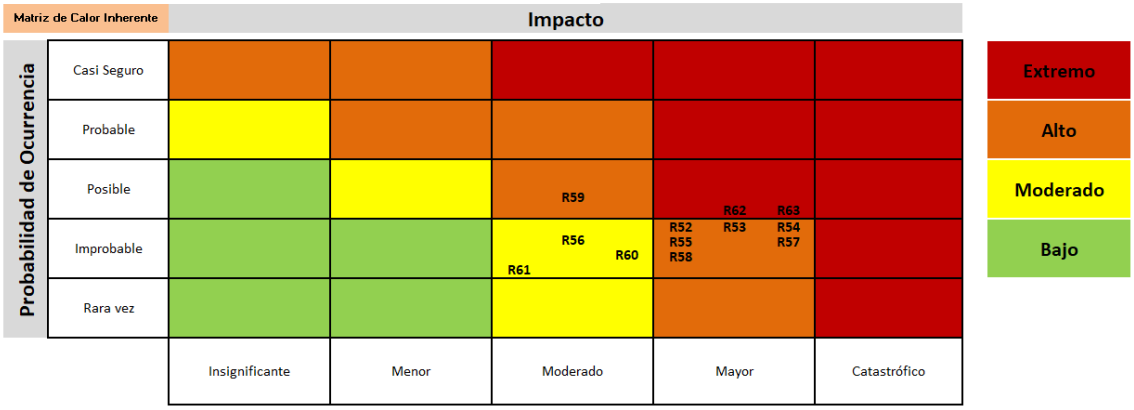
ITEM	CONTROL	RESPONSABLE
1	Política de seguridad y privacidad de la información. ID 134	- Profesional Universitario G2 - Oficina Estratégica (TI)
2	El Profesional Universitario y Técnico de Gestión Humana, realizan calendario de liquidación de nómina, prestaciones sociales, seguridad social y parafiscales. ID 137	- Líder de programa gestión talento humano
3	Revisión mensual de la construcción y envío oportuno de información a los entes reguladores. ID 141	- Profesional Universitario G2 - Oficina Estratégica (TI)
4	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. ID142	- Profesional Universitario G2 - Oficina Estratégica (TI)
5	Establecer en común acuerdo el plazo y condiciones para cumplir requisitos de la firma y legalización del contrato. ID150	-Profesional Universitario G1 - Unidad de Mercadeo y Ventas (1)
6	Comunicación constante con el cliente. ID150	-Profesional Universitario G1 - Unidad de Mercadeo y Ventas (1)
7	Disponibilidad de personal a cargo para la revisión de la plataforma Secop II constantemente. ID150	-Profesional Universitario G1 - Unidad de Mercadeo y Ventas (1)
8	Gestionar solicitud de firmas vía correo electrónico. ID150	-Profesional Universitario G1 - Unidad de Mercadeo y Ventas (1)
9	Realizar un análisis a los planes de adquisición y los planes de desarrollo a los clientes actuales y potenciales para verificar las necesidades de contratación. ID151	-Profesional Universitario G1 - Unidad de Mercadeo y Ventas (1)
10	Cumplimiento del cronograma de visitas, jornadas de socialización del portafolio de servicios con potenciales clientes. ID151	-Profesional Universitario G1 - Unidad de Mercadeo y Ventas (1)
11	Inventario de clientes actuales y del año inmediatamente anterior. ID151	-Profesional Universitario G1 - Unidad de Compras y contratación (1)
12	Plan de mercadeo anual. ID151	-Profesional Universitario G1 - Unidad de Mercadeo y Ventas (1)
13	Activar al proveedor para que este realice el análisis de las posibles causas del daño con el fin de tomar decisiones para la prevención de estos daños. ID152	-Profesional Universitario - Unidad de Bienes y Servicios
14	El director de Auditoría Interna elabora un cronograma de planeación anual de informes de ley y delega entre su equipo de trabajo la responsabilidad de proyección de cada uno de ellos. ID154	-Profesional Universitario - Unidad de Bienes y Servicios
15	De acuerdo con la planeación anual de informes de Ley, el	-Director Auditoría Interna

	Director de Auditoría interna comunica vía correo electrónico a Planeación, con un mes de anticipación (min) los informes que deben ser publicados, con el fin de gestionar la información correspondiente para su elaboración. ID154	-Profesional Universitario – Auditoría Interna (1) -Profesional Universitario – Auditoría Interna (2) -Profesional Universitario – Auditoría Interna (3)
16	Cumplimiento de requisitos legales asociados a normas de riesgos laborales. ID156	-Profesional Universitario G1- Unidad de Gestión del Talento Humano
17	Evaluación de estándares mínimos. ID156	- Profesional Universitario G1- Unidad de Gestión del Talento Humano

5. MATRIZ DE RIESGOS DE CORRUPCIÓN

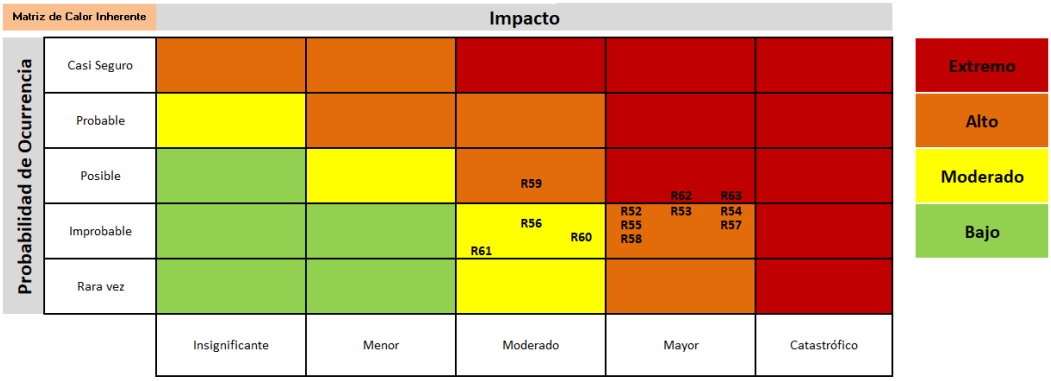
5.1 Matriz de riesgos inherente

Una vez realizada la evaluación del Riesgo Inherente se obtuvo 1 riesgo en nivel extremo, 7 riesgos en nivel Alto, 3 en nivel moderado y 0 en nivel 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 implantadas las acciones para el manejo de los riesgos se obtiene la matriz de riesgos residual:



Con los controles implantados, la matriz residual ubica:

- 3 riesgos nivel Alto
- 8 riesgos nivel moderado

5.3 tipificación de acciones y controles para mitigación del riesgo de corrupción 2022

En la matriz de riesgos de corrupción en el periodo evaluado se identificaron 65 controles, de los cuales, dos se ubicaron en una calificación moderada y los demás (63), en una calificación fuerte.

ITEM	CONTROL	RESPONSABLE
1	Informes de supervisión.	- Harley Castrillón Palacios
2	Seguimiento a la supervisión de contratos.	- Harley Castrillón Palacios
3	Sensibilización para la prevención y control de riesgos de corrupción.	- Harley Castrillón Palacios
4	Aprobación del subgerente administrativo y financiero y acto administrativo por medio de traslado firmado por el gerente.	-Sandra Zapata Grisales
5	Procedimientos del proceso: ejecución y seguimiento del presupuesto. Procedimiento modificaciones presupuestales.	-Sandra Zapata Grisales
6	Parametrización del Software Financiero.	-Sandra Zapata Grisales
7	Procedimientos y políticas de gestión contable.	-María Nidia Marín Giraldo
8	Desagregación de los procesos contables en diferentes personas del área.	-María Nidia Marín Giraldo
9	Comité financiero.	-María Nidia Marín Giraldo
10	Conciliación entre contabilidad y los demás módulos que transfieren información a contabilidad.	-María Nidia Marín Giraldo
11	Presentación de estados financieros al comité financiero y de gerencia.	- María Nidia Marín Giraldo
12	Modelo de selección bancario.	-Yarlys Mosquera Caro
13	Comité financiero.	-Yarlys Mosquera Caro
14	Manual de inversiones.	-Yarlys Mosquera Caro
15	Políticas de tesorería: Políticas de seguridad en las operaciones de tesorería - Política Pago de Obligaciones.	-Yarlys Mosquera Caro
16	Matriz de pares.	-Yarlys Mosquera Caro
17	Lista de chequeo de contrato interadministrativo.	-Sandra Cecilia Morales Camacho

18	Verificación por parte de tesorería que el titular de la cuenta sea la entidad pública firmante del acta.	-Sandra Cecilia Morales Camacho
19	Comité asesor de contratación.	-Emiro Valdés López
20	Formato informe de evaluación.	-Emiro Valdés López
21	Revisión jurídica de pliegos y/o estudios previos antes de su publicación.	-Emiro Valdés López
22	Informes de supervisión.	-Emiro Valdés López
23	Acceso restringido al sistema de gestión documental Mercurio.	-Jorge Iván Zapata Henao
24	Políticas de gestión documental donde se limita el préstamo de documentos físicos.	-Jorge Iván Zapata Henao
25	Proceso de inducción obligatoria a todo el personal nuevo que ingresa a la empresa.	-Jorge Iván Zapata Henao
26	Procedimiento PR-MG-DOC-03 para consulta de los documentos en la Unidad de Gestión Documental.	-Jorge Iván Zapata Henao
27	Proceso de inducción obligatoria a todo el personal nuevo que ingresa a la empresa.	-Jorge Iván Zapata Henao
28	Procedimiento PR-M6-DOC-02 para recepción de correspondencia.	-Jorge Iván Zapata Henao
29	Procedimiento PR-M6-DOC-05 para recepción de propuestas.	-Jorge Iván Zapata Henao
30	Cámaras de video con grabación de video y registro de hora.	-Jorge Iván Zapata Henao
31	Relojes en la recepción y en el archivo.	-Jorge Iván Zapata Henao
32	Aplicación de la circular 14 y circular 06 de 2019.	-Jorge Iván Zapata Henao
33	Parametrización del sistema de liquidación y cruce con contabilidad y tesorería para que se valide las acreencias laborales.	-Ana Cecilia Valencia Aguirre
34	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.	-Ana Cecilia Valencia Aguirre
35	Informe del sistema sobre las diferencias entre lo liquidado y pagado.	-Ana Cecilia Valencia Aguirre
36	Existencia de los soportes que autoricen el reconocimiento y pago de los beneficios.	-Ana Cecilia Valencia Aguirre
37	Procedimiento reclutamiento, selección y vinculación de personal.	-Ana Cecilia Valencia Aguirre
38	Comité asesor de contratación.	-Paula Andrea Villa Rodríguez
39	Formato informe de evaluación.	-Paula Andrea Villa Rodríguez
40	Revisión jurídica de pliegos y/o estudios previos antes de su publicación.	-Paula Andrea Villa Rodríguez
41	Aprobación de la adenda por el o los subgerente(s) del área.	-Paula Andrea Villa Rodríguez
42	Política de seguridad y privacidad de la información.	-Daniel Esteban Montaño López
43	Adecuada perfilación de usuarios y permisos de acceso a los sistemas.	-Daniel Esteban Montaño López
44	Oportunidad en el reporte de novedades de personal (retiros/vacaciones).	-Daniel Esteban Montaño López

45	Control adecuado de la configuración de dispositivos de seguridad perimetral.	-Daniel Esteban Montaño López

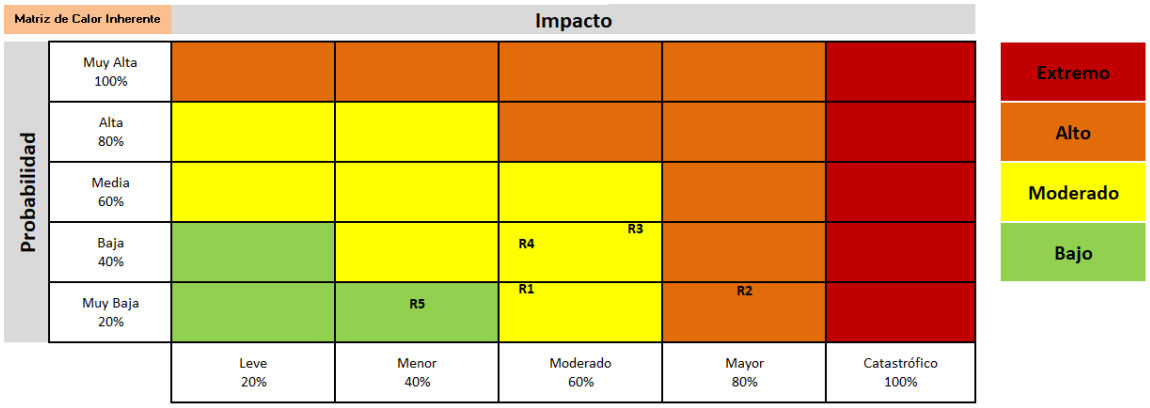
6. MATRIZ DE RIESGOS DE SEGURIDAD DIGITAL

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.

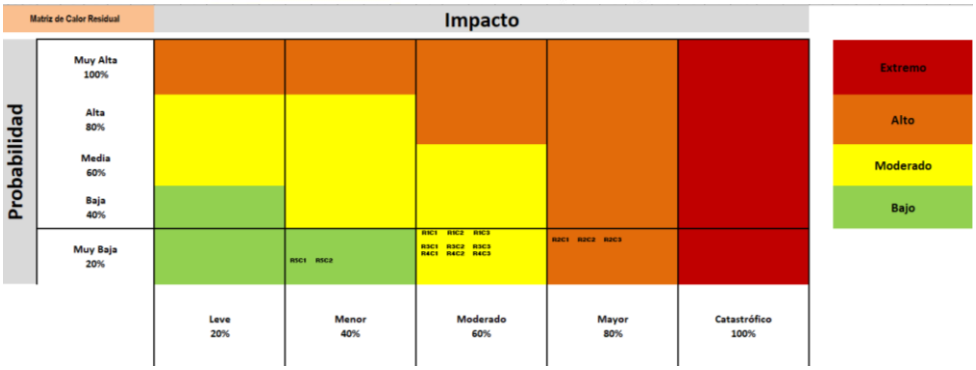
De acuerdo con esta matriz de riesgos inherentes se encuentran:

- 1 nivel Alto
- 3 nivel moderado
- 1 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 implantadas 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
- 3 riesgos nivel moderado
- 1 riesgo nivel bajo

Es importante mencionar que los controles diseñados disminuyen la probabilidad de ocurrencia de algunos riesgos. De la misma manera, es necesario rediseñar y estructurar nuevamente controles para los riesgos en los que no se mitiga ni la probabilidad ni el impacto.

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
			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.	-
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 no se han identificado riesgos materializados.

9. RECOMENDACIONES

- Se sugiere actualizar la información de la sede presente (Edificio Centro Empresarial Ciudad del Río) en el sistema de gestión, ya que este cumplimiento esta desactualizado.
- Se recomienda revisar la clasificación de tipos de control diseñados para la matriz de gestión de riesgos de procesos, ya que para algunos no está definido.

- Se propone identificar las personas responsables de procesos con el fin de actualizar el responsable a lo que ocupa el presenta.
- Se aconseja hacer revisión continua con el propósito de identificar la existencia de posibles nuevos riesgos.

- Se sugiere verificar la redacción y denominación del nombre del riesgo de acuerdo a la guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5, tanto para los riesgos de gestión de procesos como para los de corrupción.
- Se recomienda verificar los riesgos de corrupción ID57 y ID62 ya que se repiten.

10. CONCLUSIONES

- A pesar de los cambios realizados por la adopción de la guía versión 5 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 en la entidad **(Ver tabla de riesgo residual de la gestión de procesos y tabla de controles asociados)**.
- En general la entidad cumple con la Política de Administración de Riesgos, específicamente para el tratamiento, manejo, seguimiento y monitoreo de los riesgos de gestión de procesos, corrupción y sistemas digitales.

Proyectó y elaboró: Katherine Yépez Duque **–** Auditoría Interna