INFORME MONITOREO DE SEGUNDA LÍNEA DE DEFENSA A LOS MAPAS DE RIESGOS DE GESTIÓN, CORRUPCIÓN Y DE SEGURIDAD DE LA INFORMACIÓN DE LA SECRETARÍA DISTRITAL DE PLANEACIÓN

CORTE A 30 DE ABRIL DE 2024
SECRETARÍA DISTRITAL DE PLANEACIÓN
SUBSECRETARÍA DE GESTIÓN INSTITUCIONAL
DIRECCION DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
DIRECCIÓN DE PLANEACIÓN INSTITUCIONAL
22 DE MAYO DE 2024

BOGOTÁ
Secretaría de Planeación

TABLA DE CONTENIDO

1 INTRODUCCIÓN

Para una adecuada "Gestión del Riesgo", la Secretaría Distrital de Planeación, atiende las directrices de la Ley 1474 de 2011 «Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública» y el Decreto Distrital 189 de 2020 "Por el cual se expiden lineamientos generales sobre transparencia, integridad y medidas anticorrupción en las entidades y organismos del orden distrital y se dictan otras disposiciones"

Así mismo, implementa los lineamientos del Modelo Integrado de Planeación y Gestión-MIPG, el cual es el marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar las actividades de las entidades y organismos públicos. Este Modelo tiene como finalidad generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos con integridad y calidad en el servicio.

El MIPG opera a través de 7 dimensiones que agrupan las políticas de gestión y desempeño institucional. La gestión del riesgo hace parte de la Dimensión de Direccionamiento Estratégico de la entidad y de Control Interno y es un proceso efectuado por la alta dirección de la entidad y por todo el personal con el propósito de proporcionar a la administración un aseguramiento razonable con respecto al logro de la misión, visión, objetivos, metas, programas, proyectos y planes de la entidad.

La gestión del riesgo es el proceso que implica la aplicación sistemática de políticas, procedimientos y prácticas a las acciones de comunicación, consulta, establecimiento del contexto y evaluación, tratamiento, seguimiento, revisión, registro e informe del riesgo[1].

El Sistema de Gestión de Calidad de la Secretaría Distrital de Planeación, certificada bajo la NTC ISO 9001:2015, incorpora, entre otros, el pensamiento basado en riesgos. Esta norma internacional, exige planificar e implementar acciones para abordar los riesgos y las oportunidades. En particular, el numeral 6.1 menciona que la organización debe determinar las cuestiones externas e internas que son pertinentes para su propósito y dirección estratégica y que afectan su capacidad para lograr los resultados previstos del sistema de gestión de la calidad, es decir, que como insumo para la gestión de riesgos se requiere contar con la planeación estratégica institucional, la cual fue adoptada en la entidad mediante la Resolución 1666 del 11 de octubre de 2021.

El 03 de agosto de 2022 se actualizó la Política de Administración del Riesgos con código interno E-LE-030 en su versión 18. El monitoreo a los mapas de riesgos de gestión y de corrupción fueron realizados por la Dirección de Planeación Institucional y el monitoreo a los riesgos de seguridad de la información, fueron realizados por la Dirección de Tecnologías de la Información y las Comunicaciones. De acuerdo con lo anterior, a continuación, se presentan las principales recomendaciones de segunda línea de defensa, a los riesgos de los procesos de la entidad.

[1] ICONTEC, Curso virtual Sistema de Gestión Antisoborno, Noviembre de 2023.

2 PROCESOS ESTRATÉGICOS

2.1 DIRECCIONAMIENTO ESTRATÉGICO

2.1.1 E-LE-047 MAPA DE RIESGOS DE GESTIÓN DEL PROCESO DIRECCIONAMIENTO ESTRATÉGICO VERSIÓN 7 ACTA DE MEJORAMIENTO 88 DE FEBRERO 12 DE 2024

Riesgos de Gestión

1. Posibilidad de afectación económica y reputacional por la definición, orientación y coordinación de la planeación institucional desarticulada de los lineamientos distritales y nacionales, debido a bajo nivel de apropiación de las metodologías e instrumentos para la planeación estratégica, operativa y del sistema de gestión de la entidad, dificultad en la interacción de los procesos y debilidad en la cultura de planeación.

2. Posibilidad de afectación económica y reputacional por desempeño de los procesos y resultados de los proyectos en un nivel inferior al esperado, debido a incumplimiento de la planeación estratégica y plan de desarrollo, debilidad en la articulación de los instrumentos de planeación interna (plan de contratación, plan de acción, POA, plan estratégico, planes de mejoramiento, mapa de riesgos), deficiencias en la calidad y oportunidad en la información reportada por los procesos y dificultad en la interacción de los mismos.

2.1.1.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias***.

   Se evidencia por parte de la segunda línea de defensa que el contexto estratégico del proceso no se modifica, esto teniendo en cuenta que los riesgos identificados responden a lo establecido en el Plan Estratégico 2020-2024 de la SDP y adicionalmente se encuentran recientemente formulados bajo la nueva metodología de administración del riesgo en la vigencia 2022. Sin embargo, se deja claridad, que durante el segundo semestre de la vigencia se realizará la nueva plataforma estratégica de la entidad, por lo que se verificará el contexto estratégico del mismo. Adicionalmente, se evidencia por parte de la segunda línea de defensa que en el formato establecido para el monitoreo de riesgos, se cuenta con la identificación del contexto del proceso, donde se evidencia la correlación entre los riesgos de gestión formulados y el objetivo del proceso, lo que permitió que la identificación y actualización de los riesgos realizada se encuentre en coherencia con el objetivo del proceso, así como con las causas y consecuencias identificadas.

2. ***Autoevaluación de la efectividad de los controles***.

   De acuerdo con la información suministrada por parte de la primera línea de defensa se evidencia que las acciones adelantadas por el proceso en el marco de los controles de los riesgos de gestión identificados, están siendo correctamente ejecutadas y se cuenta con la respectiva evidencia de las mismas, de tal manera que la materialización del riesgo no se ha efectuado. Así mismo, es importante destacar que con corte al mes de abril no se cuenta con hallazgos de auditoría asociados a los controles identificados en el mapa de riesgos del proceso.

3. ***Autoevaluación de la eficacia de las acciones:***

   Teniendo en cuenta la información suministrada por la primera línea de defensa, las acciones establecidas en el marco de los controles formulados, se encuentran directamente relacionadas con las causas que originan los riesgos, razón por la cual a la fecha el riesgo no se ha materializado pues las acciones de tipo preventivo y detectivo han permitido contrarrestar y mitigar la materialización de los mismos, lo que indica que las acciones han sido efectivas a la fecha. De igual modo es importante mencionar que durante el periodo del monitoreo de segunda línea de defensa con corte a abril de 2024 no se han materializado ninguno de los riesgos identificados para el proceso, así como tampoco se ha determinado como hallazgo de algún tipo de auditoría.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

   Según el reporte realizado por parte de la primera línea de defensa, se observa que el cumplimiento de los objetivos y compromisos del proceso se han podido llevar a cabo a través de la ejecución de las diferentes herramientas de planeación operativa destinadas para ello, lo que demuestra la efectividad de los controles, dado que a la fecha no se han materializado ninguno de los riesgos de gestión identificados por el proceso y que son objeto de este monitoreo.

5. ***Actualización de Riesgos****:*

   Teniendo en cuenta lo reportado por parte de la primera línea de defensa, y tomando como referencia que el proceso de actualización y revisión de los riesgos con la nueva metodología dispuesta para ello y que producto de los cambios externos de la entidad y de las retroalimentaciones de partes interesadas tales como, auditorías tanto internas como externas, no se ha evidenciado hasta el momento la necesidad de modificar, actualizar o crear nuevos riesgos de gestión asociados al proceso.

2.1.1.2 ALERTAS:

No se evidencian alertas relacionadas con la posible materialización de los riesgos de gestión identificados para el proceso de Direccionamiento Estratégico, pues la efectividad en la administración de los riesgos a través de la ejecución de los adecuados controles, ha permitido consolidar en términos de eficacia el sistema de riesgos asociados al proceso.

2.1.1.3 RECOMENDACIONES:

Se recomienda dar continuidad a la aplicación de los controles y así mismo una vez se realicé la plataforma estratégica 2024-2027, se deberá evaluar el contexto estratégico del proceso, así como las causas y consecuencias de los riesgos identificados y validar la necesidad de asociar o documentar nuevos riesgos para el proceso.

2.1.2 E-LE-104 MAPA DE RIESGOS DE CORRUPCIÓN DEL PROCESO DIRECCIONAMIENTO ESTRATÉGICO VERSIÓN 2 ACTA DE MEJORAMIENTO 2 DE ENERO 29 DE 2024

Riesgo de Corrupción
1. Posibilidad de manipulación de la información relacionada con la planeación, inversión, resultados y metas para favorecer a terceros.
2. Posibilidad de desviación de la gestión en la asignación, programación y ejecución presupuestal con destinación diferente al cumplimiento de las metas y programas institucionales para favorecimiento de terceros.

2.1.2.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias.***

Los riesgos para el proceso fueron identificados y actualizados al principio de la vigencia por lo que su alineación con el plan estratégico de la entidad es coherente y se mantiene. Sin embargo, se aclara que la plataforma estratégica 2024-2027 se encuentra programada a realizar durante el segundo semestre de la vigencia y en ella se realizará la respectiva validación del contexto estratégico del proceso. Se puede apreciar en el formato establecido para el monitoreo de riesgos la identificación del contexto del proceso, donde se establece la correlación entre los riesgos de corrupción formulados y el objetivo del proceso, lo que permitió que la identificación y actualización de los riesgos realizada se encuentre en coherencia con el objetivo del proceso.

Tanto las causas como las consecuencias identificadas en el mapa de riesgos de corrupción del proceso se deben mantener, pues a la fecha el riesgo continúa, es latente y sus consecuencias e impacto son catastróficos, razón por la cual al no materializarse se evidencia que los controles identificados responden a la naturaleza de las causas y el nivel de impacto identificado en las consecuencias de los riesgos.

2. ***Autoevaluación de la efectividad de los controles.***

De acuerdo con la información suministrada por la primera línea de defensa se evidencia la presencia de registros y soportes correspondientes a los controles establecidos para mitigar la materialización de los riesgos de corrupción identificados para el proceso. Así mismo, se pueden observar las actividades desarrolladas por parte del proceso para llevar a cabo los controles identificados y de esta manera a través de la publicación constante en la página web de la entidad, garantizar espacios de transparencia en la gestión que eviten de manera directa escenarios de manipulación de los resultados de la gestión institucional. Así como la información registrada de manera permanente en el SEGPLAN, garantiza la trazabilidad del cumplimiento de los proyectos de inversión del sector planeación, información que se encuentra debidamente registrada y disponible en cualquier momento para ser consultada por cualquier grupo de interés, grupo de valor o parte interesada. La trazabilidad de las actividades y los controles realizados por el proceso en sus herramientas de seguimiento a la gestión institucional, garantizan la confiabilidad de la información, la cual es objeto de constante verificación por parte de la tercera línea de defensa y por parte de organismos de control. Es importante destacar que con corte al mes de abril no se cuenta con hallazgos de auditoría asociados a los controles identificados en el mapa de riesgos del proceso.

3. ***Autoevaluación de la eficacia de las acciones:***

Teniendo en cuenta la información suministrada por la primera línea de defensa, las acciones establecidas en el marco de los controles formulados, se encuentran directamente relacionadas con las causas que originan los riesgos, razón por la cual a la fecha, el riesgo no se ha materializado pues las acciones de tipo preventivo y detectivo han permitido contrarrestar y mitigar la materialización de los mismos, lo que indica que las acciones han sido efectivas hasta el momento. Durante el periodo del monitoreo de segunda línea de defensa con corte a abril de 2024 no se han materializado ninguno de los riesgos identificados para el proceso, así como tampoco se ha determinado como hallazgo de algún tipo de auditoría.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

Según el reporte realizado por parte de la primera línea de defensa, se observa que el cumplimiento de los objetivos y compromisos del proceso se han podido llevar a cabo a través del monitoreo de las diferentes herramientas de planeación operativa destinadas para ello, lo que demuestra la efectividad de los controles, dado que a la fecha no se han materializado ninguno de los riesgos de corrupción identificados por el proceso y que objeto de este monitoreo.

5. ***Actualización de Riesgos****:*

Teniendo en cuenta lo reportado por parte de la primera línea de defensa, y tomando como referencia que el proceso de actualización y revisión de los riesgos con la nueva metodología dispuesta para ello, fue llevado a cabo en la vigencia anterior y que producto de los cambios externos de la entidad y de las retroalimentaciones de partes interesadas tales como, auditorías, no se ha evidenciado hasta el momento la necesidad de modificar, actualizar o crear nuevos riesgos de corrupción asociados al proceso.

2.1.2.2 ALERTAS:

No se evidencian alertas relacionadas con la posible materialización de los riesgos de corrupción identificados para el proceso de Direccionamiento Estratégico, pues la efectividad en la administración de los riesgos de corrupción a través de la ejecución de los adecuados controles, ha permitido consolidar en términos de eficacia el sistema de riesgos asociados al proceso.

2.1.2.3 RECOMENDACIONES:

Se recomienda dar continuidad a la aplicación de los controles y así mismo una vez se realicé la plataforma estratégica 2024-2027, se deberá evaluar el contexto estratégico del proceso, así como las causas y consecuencias de los riesgos identificados y validar la necesidad de asociar o documentar nuevos riesgos de corrupción para el proceso.

2.1.3 E-LE-103 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DEL PROCESO DIRECCIONAMIENTO ESTRATÉGICO VERSIÓN 2 ACTA DE MEJORAMIENTO 15 DE FEBRERO 15 DE 2024

Riesgo de Seguridad de la Información
1. Posibilidad de Pérdida de Disponibilidad por fallas humanas relacionadas a las Resoluciones y/o Actas de Mejoramiento anteriores al año 2012 debido a manejo manual de la información.
2. Posibilidad de Pérdida de integridad por fallas humanas, falsificación de derechos de acceso relacionadas con la información. reportada de los resultados de la gestión institucional, debido a la ausencia de validación de autenticación y deficiencia en la autorización de permisos de la información.

2.1.3.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias***.

El contexto estratégico del proceso se mantiene, teniendo en cuenta que los riesgos identificados responden a lo establecido en el Plan Estratégico 2020-2024 de la SDP. Es importante destacar que el líder del proceso está tomando medidas proactivas para analizar el contexto considerando los cambios en el entorno de la SDP derivados del Plan Estratégico 2024-2027 que será formulado en el segundo semestre de la vigencia, los cuales podrían afectar la probabilidad o el impacto del riesgo.

Los riesgos identificados para el proceso se encuentran directamente relacionados con los objetivos estratégicos identificados en el Plan Estratégico 2020-2024 de la SDP. De acuerdo con lo informado por el líder de proceso, el Plan Estratégico 2024-2027 será formulado en el segundo semestre de la vigencia, por lo que se deberá evaluar nuevamente la coherencia del riesgo con el objetivo estratégico en ese momento. Es importante que la definición del riesgo se mantenga alineada con los objetivos estratégicos de la entidad para que las acciones de mitigación sean efectivas.

La matriz de riesgos y el informe de seguimiento de riesgos del primer cuatrimestre de 2024 confirman que los riesgos identificados para el proceso de Direccionamiento Estratégico se encuentran alineados con el objetivo del mismo. De acuerdo con lo informado por el líder de proceso es importante tener en cuenta que el Plan Estratégico 2024-2027 será formulado en el segundo semestre de la vigencia, por lo que se deberá evaluar nuevamente la coherencia del riesgo con el objetivo estratégico y del proceso en ese momento. Es importante que la definición del riesgo se mantenga alineada con los objetivos estratégicos de la entidad para que las acciones de mitigación sean efectivas.

Si bien es importante realizar un seguimiento continuo de las causas de los riesgos, la información disponible en este momento no permite concluir que haya habido cambios significativos en las causas inicialmente identificadas para los riesgos del proceso de Direccionamiento Estratégico por lo tanto las causas identificadas inicialmente para los riesgos del proceso de Direccionamiento Estratégico se mantienen.

Al igual que con las causas, con base en el análisis realizado y la evidencia disponible, se puede afirmar que las consecuencias identificadas inicialmente para los riesgos del proceso de Direccionamiento Estratégico se mantienen.

2. ***Autoevaluación de la efectividad de los controles****.*

La evidencia presentada demuestra que el control para el registro y control de acceso a los activos de información del proceso de Direccionamiento Estratégico se está utilizando de manera efectiva. Se han implementado diferentes mecanismos para garantizar que los activos de información estén protegidos y que solo las personas autorizadas tengan acceso a ellos.

Los controles adoptados permiten minimizar la materialización de los riesgos identificados para el proceso. Respecto de esta afirmación y de forma general se destacan los siguientes puntos:

- La clasificación de la información permite identificar los activos de información que son más críticos para el proceso y que, por lo tanto, requieren un mayor nivel de protección.

- El mantenimiento de áreas seguras para el almacenamiento de la información física ayuda a proteger los activos de información contra el acceso no autorizado, el robo y otros daños.

- Las directrices de la Dirección en seguridad de la información establecen normas y procedimientos para la protección de los activos de información, lo que ayuda a prevenir la pérdida o el uso indebido de la información.

- El control efectivo de acceso a los sistemas de información de reporte de avances de la gestión institucional susceptible de riesgo limita el acceso a la información solo a las personas autorizadas, lo que reduce el riesgo de filtraciones o accesos no autorizados.

Con base en la evidencia disponible, se puede concluir que los controles implementados para el proceso de Direccionamiento Estratégico son efectivos en la prevención o mitigación de los riesgos identificados. La utilización de los controles, su capacidad para prevenir riesgos y la ausencia de hallazgos de auditoría negativos demuestran la efectividad del sistema de control interno del proceso.

3. ***Autoevaluación de la eficacia de las acciones:***

Las acciones establecidas en el marco de los controles formulados, se encuentran directamente relacionadas con las causas que originan los riesgos, razón por la cual a la fecha el riesgo no se ha materializado. Las acciones de tipo preventivo (4), correctivo (1) y detectivos (1), han permitido contrarrestar y mitigar la materialización de los riesgos.

Las acciones frente a los controles implementados para dar tratamiento al riesgo vienen siendo implementadas de manera eficaz de tal manera que ninguno de los riesgos identificados se ha visto materializado, así como tampoco se ha determinado como hallazgo de algún tipo de auditoría lo que ha permitido que el proceso cumpla con los objetivos y compromisos a cargo a través de las acciones plasmadas en las herramientas de planeación operativa, propendiendo por la mejora continua del proceso.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

De acuerdo con la evidencia disponible, la gestión del riesgo hace parte de las acciones que adelanta el proceso para el cumplimiento de los objetivos del proceso de Direccionamiento Estratégico. Al identificar, evaluar y tratar los riesgos de manera

proactiva, el líder del proceso ha podido prevenir eventos negativos y garantizar el cumplimiento de los compromisos establecidos. La ausencia de materializaciones, el cumplimiento de objetivos y la mejora continua son indicadores claros de la efectividad de la gestión del riesgo en este proceso.

5. ***Actualización de Riesgos**:*

Teniendo en cuenta que los riesgos de seguridad de la información para el proceso de Direccionamiento Estratégico son recientes, adecuadamente definidos y alineados con las necesidades del proceso, y no se han presentado cambios relevantes en el contexto, se considera que no es necesario modificarlos o actualizarlos en este momento. Sin embargo, se debe estar atento a cualquier cambio que pueda requerir una actualización como por ejemplo la entrada en vigor de nuevo mapa de procesos.

Si bien es importante estar atentos a la aparición de nuevos riesgos, la información disponible en este momento no sugiere la necesidad de documentar y gestionar nuevos riesgos. El monitoreo continuo del proceso y su entorno permitirá identificar oportunamente cualquier nuevo desafío o amenaza que pueda surgir y tomar las medidas necesarias para mitigarlos.

2.1.3.2 ALERTAS:

De acuerdo con el monitoreo de primera línea de defensa referente a los riesgos identificados de seguridad de la información del proceso de Direccionamiento estratégico, no se reportan alertas que indiquen que los riesgos se han materializado.

2.1.3.3 RECOMENDACIONES:

El líder del proceso indica que el contexto estratégico se mantiene. Sin embargo, se recomienda realizar un análisis proactivo considerando los cambios que se pueden presentar en aplicación del Decreto 432 de 2022.

Realizar jornadas de capacitación para evitar fallas humanas relacionadas con el manejo manual de las Resoluciones y/o Actas de Mejoramiento anteriores al año 2012 y generar estrategias para digitalizar la información histórica.

Se recomienda realizar un seguimiento a las actividades de los usuarios con acceso a información confidencial.

Se recomienda continuar con la implementación y ejecución de los controles definidos en el plan de tratamiento de riesgos de seguridad de la Información.

Se recomienda asistir a las jornadas de capacitación y sensibilización que adelanta la Dirección de Tecnologías de la información y las comunicaciones.

2.2 PARTICIPACIÓN Y COMUNICACIÓN

2.2.1 E-LE-048 MAPA DE RIESGOS DE GESTIÓN DEL PROCESO DE PARTICIPACIÓN Y COMUNICACIÓN VERSIÓN 8 ACTA DE MEJORAMIENTO 148 DE MARZO 12 DE 2024

Riesgos de Gestión

1. Posibilidad de afectación económica y reputacional por incumplimiento de los lineamientos contenidos en el modelo colaborativo de participación que se sustenta en los pilares de gobierno abierto (transparencia, rendición de cuentas, participación y colaboración), debido a inadecuado diseño y/o implementación, seguimiento y evaluación de las estrategias de participación para la formulación de los instrumentos de planeación.

2. Posibilidad de afectación reputacional por entrega de información incompleta, errónea, inoportuna o confusa, debido a la desarticulación de las áreas de la SDP con la Oficina Asesora de Comunicaciones, la variación de los tiempos para la generación de información por factores exógenos, la divulgación de información a los medios de comunicación por parte de funcionarios públicos y contratistas sin autorización.

2.2.1.1 OBSERVACIONES:

El proceso ECA-003 Participación y Comunicación, mediante radicado en SIPA 3-2024-16830 del 8 de mayo de 2024 remite a la Dirección de Planeación Institucional el monitoreo de primera línea de defensa a los riesgos de gestión, con corte 30/04/2024. Con la implementación de la nueva herramienta tecnológica, Gestiónate: Isolución, se hará efectiva la puesta en operación del nuevo mapa de procesos de la SDP, lo cual implicará la separación de los procesos: "Articulación del diálogo con el ciudadano" y "Comunicación estratégica", cada uno los cuales iniciará la implementación de su respectiva caracterización de proceso, y a la luz de una nueva planeación estratégica 2024-2027.

1. ***Definición del riesgo, sus causas y consecuencias***.

El riesgo es coherente con el objetivo del proceso, debido a que es relevante en términos de los sucesos que se pueden producir a nivel de la entidad y las consecuencias que puedan tener sobre los objetivos de ésta, teniendo en cuenta la incertidumbre, la posibilidad de sucesos futuros y los efectos que se generan sobre el objetivo planificado.

Las causas se mantienen dado que el riesgo se identificó con base en las causas internas y externas según lo definido en el contexto estratégico. Las consecuencias identificadas para el riesgo se mantienen, debido a que éste, no se ha materializado. Tanto las causas, como las consecuencias, se deben revisar a la luz de los nuevos procesos: "Articulación del diálogo con el ciudadano" y "Comunicación estratégica", cada uno los cuales iniciará la implementación de su respectiva caracterización de proceso.

2. ***Autoevaluación de la efectividad de los controles***.

La efectividad de los controles se puede evidenciar a partir del desarrollo de las acciones que se enuncian a continuación:

<u>Para el Riesgo 1:</u>

Se formuló el Plan Institucional de Participación Ciudadana -PIPC- de la vigencia 2024, el cual fue presentado al Comité Institucional de Gestión y Desempeño para su aprobación. Se cuenta con archivo digital denominado Matriz Agenda Plan Institucional de Participación 2024, instrumento que permite realizar seguimiento y monitoreo permanente, disponiendo de las evidencias respectivas.

El líder del Proceso de Participación y Comunicación verifica, cada vez que se implementa una estrategia de participación para un instrumento de planeación, que dicha estrategia se encuentre alineada con los criterios de contenido y estructura definidos en el procedimiento E-PD-020 Diseño e implementación de las estrategias de participación ciudadana en los instrumentos de planeación de la SDP. Se elaboró el documento Lineamientos estrategias de participación OPDC de estrategias de participación para la formulación de instrumentos de planeación, el cual da los lineamientos para la construcción de las estrategias para la vigencia 2024.

Para el riesgo No 2:

En el primer cuatrimestre de 2024, la Jefatura de la Oficina Asesora de Comunicaciones socializó los *"Lineamientos para gestión de las comunicaciones internas"* - Circular 015 del 23 de abril de 2024. Se cuenta con la ejecución de los procedimientos E-PD-015 GESTION PARA LA CONCEPTUALIZACIÓN Y ELABORACIÓN DE LOS PRODUCTOS DE COMUNICACIÓN y E-PD-027 PUBLICACIÓN Y O ACTUALIZACIÓN DE LA INFORMACIÓN EN LOS CANALES INTERNOS Y O EXTERNOS DE LA SDP, Se puede verificar en el Excel la relación de radicados del último año, en el cual se evidencia la solicitud de productos a la Oficina de Comunicaciones. Se cuenta con la verificación de los requisitos de los productos de la oficina, estos establecidos en la matriz E-LE-066_OAC Matriz de Productos Las evidencias de la aplicación de los procedimientos se encuentran en correos electrónicos o equipos de los funcionarios de la oficina. Es importante al acceso a las evidencias para verificar trazabilidad.

El conjunto de actividades o medidas adoptadas en cada uno de los controles previstos mitiga los riesgos derivados del trabajo realizado por el Proceso en cuanto la Posibilidad de manipulación de los instrumentos de planeación en los procesos de participación ciudadana con el fin de obtener el beneficio propio o de un tercero.

3. ***Autoevaluación de la eficacia de las acciones:***

Con relación al criterio *Autoevaluación de la eficacia de las acciones,* teniendo en cuenta que los riesgos se encuentran en zona de riesgo residual "Moderada" y su opción de tratamiento está asociada a "Reducir (mitigar)", no se encuentran acciones descritas dado que comprende la aplicación adecuada de los controles[2], por tal razón, se evidencia que han sido eficaces los controles para apuntar a la mitigación del riesgo.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

Conforme al seguimiento de la primera línea de defensa se concluye que la gestión de riesgo ha sido útil para evitar situaciones que afecten los objetivos del proceso. Es importante contar con registros que evidencien la gestión del ciclo completo, desde la elaboración, la implementación,

[2] De acuerdo con el instrumento establecido en el numeral 6.3.2.4 de la Política de Administración de Riesgos (E-LE-030 Versión 18 del 03/08/2022).

hasta el seguimiento de las estrategias de participación y comunicación, con destino a los usuarios internos y externos de la SDP. los cuales son descritos explícitamente en el riesgo.

5. ***Actualización de Riesgos**:*

Para el segundo semestre de 2024, se realizará la revisión integral del riesgo, evaluando la necesidad de modificar los riesgos actuales o crear nuevos riesgos, dada la implementación de la nueva herramienta tecnológica: Gestiónate (Isolución), y la puesta en operación del nuevo mapa de procesos de la SDP, lo cual implicará la separación de los procesos: "Articulación del diálogo con el ciudadano" y "Comunicación estratégica", cada uno los cuales iniciará la implementación de su respectiva caracterización de proceso, a la luz de una nueva planeación estratégica 2024-2027.

2.2.1.2 ALERTAS:

No aplica por cuanto el riesgo no se ha materializado.

2.2.1.3 RECOMENDACIONES:

Es importante que en el repositorio no existan restricciones acceso para la verificación de evidencias.

Con la implementación de la nueva herramienta tecnológica, Isolución, se hará efectiva la puesta en operación del nuevo mapa de procesos de la SDP, lo cual implicará la separación de los procesos: "Articulación del diálogo con el ciudadano" y "Comunicación estratégica", cada uno los cuales iniciará la implementación de su respectiva caracterización de proceso, a la luz de una nueva planeación estratégica 2024-2027, por lo cual los riesgos van a ser impactados y se recomienda revisarlos.

2.2.2 E-LE-106 MAPA DE RIESGOS DE CORRUPCIÓN DEL PROCESO DE PARTICIPACIÓN Y COMUNICACIÓN VERSIÓN 2 ACTA DE MEJORAMIENTO 59 DE ENERO 31 DE 2024

Riesgo de Corrupción
1. Posibilidad de manipulación de los instrumentos de planeación en los procesos de participación ciudadana con el fin de obtener el beneficio propio o de un tercero.

2.2.2.1 OBSERVACIONES:

El proceso ECA-003 Participación y Comunicación, mediante radicado en SIPA 3-2024-16286 del 6 de mayo de 2024 remite a la Dirección de Planeación Institucional el monitoreo de primera línea de defensa a los riesgos de corrupción, con corte 30/04/2024.

1. ***Definición del riesgo, sus causas y consecuencias.***

El riesgo es coherente con el objetivo del proceso, debido a que es relevante en términos de los sucesos que se pueden producir a nivel de la entidad y las consecuencias que puedan tener sobre los objetivos de ésta, teniendo en cuenta la incertidumbre, la posibilidad de sucesos futuros y los efectos que se generan sobre el objetivo planificado. Se debe revisar a la luz de una nueva caracterización (E-CA-008 Articulación del diálogo con el ciudadano) y una nueva planeación estratégica para la entidad.

Las causas se mantienen dado que el riesgo se identificó con base en las causas internas y externas según lo definido en el contexto estratégico. Con la implementación de la nueva herramienta tecnológica, Gestiónate (Isolución), se hará efectiva la puesta en operación del nuevo mapa de procesos de la SDP, lo cual, junto con una nueva planeación estratégica determinará si se modifican las causas. Las consecuencias identificadas para el riesgo se mantienen, debido a que éste, no se ha materializado. Se debe revisar a la luz de una nueva caracterización (E-CA-008 Articulación del diálogo con el ciudadano) y una nueva planeación estratégica para la entidad.

2. ***Autoevaluación de la efectividad de los controles.***

Conforme a lo descrito en la revisión realizada por la primera línea de defensa se evidencia el desarrollo de acciones orientadas a mitigar el riesgo, Control 1: En el documento aportado, se puede evidenciar el lineamiento que se tuvo en cuenta al momento de formular una estrategia de participación.

Control 2: En el documento aportado, se puede tener evidencia de las reuniones de equipo realizadas, en las cuales se tratan los temas sobre el manejo de evidencias y disponibilidad de la información, que soporte los procesos de participación ciudadana.

Control 3: Según lo informado por la primera línea de defensa, durante los meses de junio y julio se realizará una capacitación a los servidores públicos y demás colaboradores del área, en Código General Disciplinario y Código de Ética, según el caso. Está acción será verificada en el monitoreo a realizar en el mes de agosto de 2024.

El conjunto de actividades o medidas adoptadas en cada uno de los controles previstos mitiga los riesgos derivados del trabajo realizado por el Proceso en cuanto la Posibilidad de manipulación de los

instrumentos de planeación en los procesos de participación ciudadana con el fin de obtener el beneficio propio o de un tercero.

3. ***Autoevaluación de la eficacia de las acciones:***

Las acciones formuladas para dar tratamiento al riesgo, están orientadas a contrarrestar las causas identificadas. Las acciones que se tienen programadas para la vigencia 2024 son las siguientes: "Sensibilizar permanentemente a los servidores y colaboradores de la dependencia en el manejo de evidencias y disponibilidad de la información que soporte los procesos de participación ciudadana" y "Socializar a los servidores públicos y demás colaboradores de la dependencia, en temas relacionados con Código General Disciplinario, Código de Ética y gestión de los riesgos asociados al proceso". Se realizan reuniones periódicas en las que se presenta el estado de las evidencias y se resalta la importancia de mantener actualizadas las mismas. Se tiene previsto realizar sensibilización en Código General Disciplinario y Código de Ética, según el caso, en los meses de junio y julio de 2024.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

Conforme al seguimiento de la primera línea de defensa se concluye que la gestión de riesgo ha sido útil para evitar situaciones que afecten los objetivos del proceso.

5. ***Actualización de Riesgos****:*

Para el segundo semestre de 2024, se realizará la revisión integral del riesgo, dada la implementación de la nueva herramienta tecnológica: Gestiónate (Isolución), y la puesta en operación del nuevo mapa de procesos de la SDP, lo cual implicará la separación de los procesos: "Articulación del diálogo con el ciudadano" y "Comunicación estratégica", cada uno los cuales iniciará la implementación de su respectiva caracterización de proceso, a la luz de una nueva planeación estratégica 2024-2028.

2.2.2.2 ALERTAS:

No se generan alertas al proceso teniendo en cuenta que las acciones establecidas en el marco de los controles formulados de tipo preventivo y detectivo, se encuentran directamente relacionadas con las causas que originan los riesgos y han permitido contrarrestar y mitigar la materialización de los riesgos.

2.2.2.3 RECOMENDACIONES:

Con la implementación de la nueva herramienta tecnológica, Isolución, se hará efectiva la puesta en operación del nuevo mapa de procesos de la SDP, lo cual implicará la separación de los procesos: "Articulación del diálogo con el ciudadano" y "Comunicación estratégica", cada uno los cuales iniciará la implementación de su respectiva caracterización de proceso, a la luz de una nueva planeación estratégica 2024-2027, por lo cual los riesgos van a ser impactados y se recomienda revisarlos.

2.2.3 E-LE-105 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DEL PROCESO DE PARTICIPACIÓN Y COMUNICACIÓN VERSIÓN 2 ACTA DE MEJORAMIENTO 172 DE MARZO 14 DE 2024

Riesgo de Seguridad de la Información
1. Posibilidad de Pérdida de Disponibilidad por fallas humanas, de bases de datos, evidencias de los procesos de participación y comunicación, insumos para la divulgación de información y documentos de gestión administrativa y misional, debido a desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información, ausencia de copias de respaldo o backups de la información.
2. Posibilidad de Pérdida de Confidencialidad por fallas humanas, de bases de datos, evidencias de los procesos de participación y comunicación, insumos para la divulgación de información y documentos de gestión administrativa y misional, debido a desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información, deficiencia en la autorización de permisos de la información.

2.2.3.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias***.

   El contexto estratégico identificado por el proceso se mantiene, con algunas salvedades. Se ha realizado una actualización del mapa de riesgos de seguridad de la información del proceso Participación y Comunicación, a la versión 2, según Acta de Mejoramiento 172 de marzo 14 de 2024. Sin embargo, se hace necesario revisar el contexto estratégico identificado a fin de alinearlo con el ejercicio de planeación estratégica 2024-2027 en el marco del nuevo Plan de Desarrollo Distrital (PDD). Además, con la entrada en operación del nuevo mapa de procesos, será necesario revisar el contexto estratégico para alinearlo con los nuevos procesos: Comunicación Estratégica y Articulación del Diálogo con el Ciudadano.

   El riesgo identificado es coherente con el objetivo estratégico al cual le aporta el proceso, Sin embargo, es necesario alinear los riesgos con la nueva plataforma estratégica que defina la entidad en el marco del nuevo Plan de desarrollo Distrital. Con la separación del proceso Participación y Comunicación en dos nuevos procesos (Comunicación Estratégica y Articulación del Diálogo con el Ciudadano), será necesario revisar la coherencia de los riesgos con los nuevos objetivos estratégicos.

   El riesgo identificado es coherente con el objetivo del proceso E-CA-003 Participación y Comunicación, sin embargo, de acuerdo con lo reportado por el líder del proceso en el seguimiento de primera línea de defensa, con la entrada en operación del nuevo mapa de procesos, será necesario revisar los riesgos para alinearlos y ajustarlos con los nuevos procesos: Comunicación Estratégica y Articulación del Diálogo con el Ciudadano.

   Las causas identificadas inicialmente para los riesgos se mantienen en gran medida. En este sentido, el líder del proceso informó que se hará una revisión de una parte de las causas atendiendo el ejercicio de planeación estratégica y de acuerdo con la nueva operación por procesos, será necesario revisar las causas para alinearlas con los nuevos procesos de Comunicación Estratégica y Articulación del Diálogo con el Ciudadano.

Las consecuencias identificadas inicialmente para el Riesgo 1: Posibilidad de Pérdida de Disponibilidad (Afectación de la imagen de la entidad a nivel municipal, Pérdida de acceso a la información y los sistemas de la entidad, Interrupción de los procesos de participación y comunicación, Perjuicios económicos por la imposibilidad de realizar actividades, se mantienen.

De igual forma, las causas identificadas en el Riesgo 2: Posibilidad de Pérdida de Confidencialidad (Fuga de información confidencial, Daño a la reputación de la entidad, Perjuicios económicos por la pérdida de información confidencial, Sanciones legales por el incumplimiento de las normas de protección de datos, siguen siendo relevantes y se mantienen.
Sin embargo, también se hará revisión de frente al ejercicio de planeación estratégica y los dos nuevos procesos: Comunicación Estratégica y Articulación del diálogo con el ciudadano.

2. ***Autoevaluación de la efectividad de los controles****.*

De acuerdo con la respuesta del líder del proceso, existe evidencia de que los controles están siendo utilizados. El proceso de Participación y Comunicación indicó que no ha presentado pérdidas de disponibilidad y confidencialidad de la información, la gestión de la información se realiza atendiendo las políticas establecidas institucionalmente, se registran las respectivas incidencias para la gestión de roles y permisos en las diferentes aplicaciones, bases de datos y repositorios de información utilizados, se realizan las respectivas socializaciones de las políticas de seguridad de la información y en las reuniones de equipo de la oficina de participación y diálogo de ciudad, se realiza sensibilización permanente sobre el manejo de evidencias y disponibilidad de la información que soporte los procesos de participación ciudadana. Desde el proceso se aportó evidencia reunión https://drive.google.com/file/d/1VKHo5Aj3E7CZCqKq3-ilLaaPk27LkGPB/view?usp=sharing en la cual se puede observar que en los temas tratados se incluyó el registro de incidencias para la gestión de roles y permisos y la existencia de actas de las reuniones de equipo donde se ha realizado sensibilización sobre el manejo de la información.

Los controles establecidos han permitido prevenir la materialización de los riesgos de pérdida de disponibilidad y confidencialidad de la información, no se han presentado hallazgos de auditoría asociados a los controles.

No se han presentado hallazgos de auditoría relacionados con la efectividad de los controles establecidos en el proceso E-CA-003 PARTICIPACIÓN Y COMUNICACIÓN.

3. ***Autoevaluación de la eficacia de las acciones:***

De acuerdo con la respuesta del líder del proceso, la aplicación de controles guarda coherencia con los riesgos identificados. Las actividades para el cumplimiento del control se han diseñado para prevenir o mitigar las causas de los riesgos.

No se formularon planes de acción. Se recomienda para los próximos seguimientos, publicar las evidencias que permita soportar lo reportado en el monitoreo de primera línea de defensa.

Las acciones formuladas en los controles para dar tratamiento al riesgo se vienen implementando de acuerdo con lo planeado sin que se identifiquen problemas significativos en su ejecución.

De conformidad con la respuesta del líder del proceso, los riesgos identificados no se han materializado y tampoco se han determinado como hallazgo de auditoría interna o externa.

El riesgo no se ha materializado, por lo que no ha sido necesario formular correcciones o acciones correctivas.

4. ***Evaluación de la efectividad de la gestión de los riesgos**:*

   La gestión integral de los riesgos de seguridad de la información ha demostrado ser un componente esencial para el éxito del proceso Participación y Comunicación. Al prevenir incidentes, garantizar el cumplimiento de objetivos y fomentar la satisfacción de los usuarios, la gestión de riesgos ha contribuido significativamente al logro de los compromisos establecidos.

   Se recomienda continuar fortaleciendo la gestión de riesgos, mejorando la comunicación y promoviendo una cultura de seguridad en toda la entidad.

5. ***Actualización de Riesgos**:*

   Desde el proceso se identifica la necesidad de modificar y/o actualizar el riesgo establecido actualmente con ocasión de la entrada en vigor de la nueva operación por procesos de la SDP. Esto implica la división del proceso Participación y Comunicación en dos nuevos procesos: Comunicación Estratégica y Articulación del Diálogo con el Ciudadano. Adicionalmente, la definición de la nueva plataforma estratégica 2024-2027 podría generar nuevos riesgos o modificar la probabilidad e impacto de los riesgos existentes.

   Teniendo como base que desde el proceso se identifica la necesidad de modificar y/o actualizar el riesgo establecido actualmente, se prevé la necesidad de documentar y gestionar nuevos riesgos alineados a la nueva operación por procesos de la SDP y la plataforma estratégica 2024-2027.

2.2.3.2 ALERTAS:

De acuerdo con el monitoreo de primera línea de defensa referente a los riesgos identificados de seguridad de la información del proceso de Participación y comunicación, no se reportan alertas que indiquen que los riesgos se han materializado.

2.2.3.3 RECOMENDACIONES:

Se recomienda validar que el personal responsable de las bases de datos, evidencias de los procesos de participación y comunicación, insumos para la divulgación de información y documentos de gestión administrativa y misional comprendan su rol y responsabilidades.

Es posible que las acciones formuladas para dar tratamiento al riesgo estén orientadas a contrarrestar sus causas. Sin embargo, se recomienda realizar actividades de análisis para confirmar la eficacia de las acciones y verificar que están orientadas a contrarrestar las causas del riesgo de manera adecuada.

Es posible que no se hayan formulado correcciones ni acciones correctivas debido a que el riesgo no se ha materializado. Sin embargo, se recomienda realizar un seguimiento continuo del riesgo para confirmar que no se materialice en el futuro y, en caso de que se materialice, se formulen las

correcciones y/o acciones correctivas necesarias.

Se recomienda continuar con la implementación y ejecución de los controles definidos en el plan de tratamiento de riesgos. Se debe liderar desde el proceso de Participación y comunicación las acciones de depuración de usuarios a sus repositorios, sistemas de información, además de verificar si las copias de respaldo que la DTIC realiza sobre su información pueden ser recuperadas y en qué condiciones.

Se recomienda asistir a las jornadas de capacitación y sensibilización en temas de seguridad y privacidad de la información programadas por la entidad.

3 PROCESOS MISIONALES

3.1 PLANEACIÓN TERRITORIAL Y GESTIÓN DE SUS INSTRUMENTOS

3.1.1 M-LE-132 MAPA DE RIESGOS DE GESTIÓN DEL PROCESO PLANEACIÓN TERRITORIAL Y GESTIÓN DE SUS INSTRUMENTOS VERSIÓN 9 ACTA DE MEJORAMIENTO 482 DE NOVIEMBRE 30 DE 2023

Riesgos de Gestión

1. Posibilidad de afectación económica y reputacional por decisiones jurídicas en contra de las acciones relacionadas con el ordenamiento territorial, debido a seguimiento y evaluación inadecuadas frente a la implementación del plan de ordenamiento territorial – POT vigente antes de la adopción del nuevo POT; insuficiencia y falta de acceso a datos, información y estudios poblacionales y del territorio para un adecuado diagnóstico del modelo de ordenamiento territorial; documentos del POT sin los contenidos mínimos establecidos en las normas vigentes; incumplimiento en las etapas de planificación territorial definidas por la ley y fallas en el proceso de formulación del POT con las partes interesadas (concertación, consulta, aprobación y adopción).

2. Posibilidad de afectación económica y reputacional por entrega de los productos y/o servicios del proceso sin los requisitos de calidad establecidos como: claridad, publicidad, oportunidad y legalidad, debido a inconsistencias en la documentación técnica de soporte de los actos administrativos; desarticulación de los procesos de la Secretaría Distrital de Planeación en la generación de instrumentos de planeación territorial; falla de coordinación interinstitucional de las entidades que inciden en la planeación territorial; desconocimiento de los requerimientos de las partes interesadas en el proceso; desconocimiento previo del territorio para la proyección de los actos administrativos; desconocimiento por parte de la comunidad en el proceso de participación sobre la dinámica del mismo y la integralidad del proyecto; publicación y desactualización de la información de la Base de Datos Geográfica Corporativa – BDGC.

3.1.1.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias***.

   Mediante radicado en SIPA 3-2024-16827 del 9 de mayo de 2024 el proceso Planeación Territorial y Gestión de sus Instrumentos remitió a la Dirección de Planeación Institucional el monitoreo de primera línea de defensa a los riesgos de gestión asociados al mismo.

   La actualización más reciente del mapa de riesgos de gestión (versión 9) se realizó en noviembre de la vigencia 2023, mediante acta de mejoramiento 482 del sistema SIPA, en la cual fueron revisados los controles en cuenta a su estructura según la guía del DAFP y clasificación.

   Teniendo en cuenta que el Riesgo Nº1 está orientado a las decisiones jurídicas en contra de las acciones relacionadas con el ordenamiento territorial y el Riesgo Nº2 está enfocado a la entrega de los productos y/o servicios del proceso sin los requisitos de calidad establecidos como: claridad, publicidad, oportunidad y legalidad, se evidencia que están directamente relacionados con el objetivo

estratégico "Definir y promover un modelo colectivo de ciudad en el largo plazo, mediante la reglamentación y viabilización del territorio, a través de los instrumentos de planeación buscando el bienestar de la ciudadanía".

Los dos riesgos de gestión guardan coherencia con el objetivo del proceso, toda vez que se orientan a las decisiones jurídicas en contra de las acciones relacionadas con el ordenamiento territorial y a la entrega de los productos y/o servicios del proceso sin los requisitos de calidad establecidos como: claridad, publicidad, oportunidad y legalidad, aspectos claves dentro del propósito del proceso que es la generación de condiciones normativas mediante Decisiones Urbanísticas, Actuaciones Administrativas y Formulación de Proyectos Distritales para el beneficio social.

Para el periodo de monitoreo, la primera línea de defensa manifiesta que las causas y consecuencias identificadas inicialmente se mantienen, razón por la cual se infiere que durante la normal operación del proceso no se han evidenciado alertas de nuevas causas y/o consecuencias que puedan incidir en la definición de los riesgos de gestión.

2. ***Autoevaluación de la efectividad de los controles****.*

Para el Riesgo Nº 1 la primera línea de defensa reporta evidencias que dan cuenta de la aplicación de los seis (6) controles definidos para el riesgo. Es así como a través de las acciones y resultados asociados al Decreto 555 de 2021, se evidencia la aplicación de dichos controles, así: 1. Seguimiento y evaluación del POT vigente y el diagnóstico del estado actual del territorio, 2. Programación de las etapas definidas para su formulación, 3. Documentos para la concertación ambiental en cumplimiento de los contenidos mínimos establecidos en las normas vigentes, 4. Documentos necesarios para la consulta ante el Consejo Territorial de Planeación Distrital (CTPD) y Consejo Consultivo de Ordenamiento Territorial, 5. Documentos para la presentación ante el Concejo de Bogotá en cumplimiento de los contenidos mínimos.6. Verificación de implicaciones de decisiones judiciales que afecten el POT.

En cuanto al Riesgo Nº 2 los diferentes actos administrativos que se expidieron surtieron los controles definidos, en lo relacionado con el estudio técnico, socialización, revisión, adopción y publicación. Para el caso de los actos administrativos aprobados mediante resolución adicionalmente se surte el proceso de notificación. Los registros de los controles se encuentran incorporados a los expedientes de los respectivos trámites. El proceso atendió la recomendación de registrar en su monitoreo de primera línea la evidencia de la aplicación de cada uno de los controles asociados a este riesgo, así como el registro en el repositorio definido por la entidad, con el fin de identificar más puntualmente la aplicación de los controles definidos así: 1. Verificar mediante lista de chequeo que los documentos para el inicio del trámite estén completos 2. Verificar que los documentos para el inicio de los trámites estén acordes con los requerimientos 3. Revisar que el contenido jurídico y técnico cumpla con la normatividad vigente (visto bueno y/o firma en el documento físico o electrónico) 4. Verificar que se haya socializado a las partes interesadas. 5. Verificación en SIPG de ejecución de las metas y actividades POA . 6. Verificación de trazabilidad de publicación de actos administrativos.

Es importante mencionar dentro del monitoreo de segunda línea de defensa las

manifestaciones de interés de las partes interesadas reportadas por el proceso en los primeros mese del presente año y que corresponden al segundo semestre de 2023, asociadas principalmente a aspectos legales como aclaraciones a proyectos de resolución de planes de regularización, delimitaciones, adopción de planes de implantación, modificaciones de reglamentación, adopción de plan director, aspectos contenidos en el POT, observaciones frente al Documento Técnico de Soporte - DTS que acompaña a los documentos normativos que expide la SDP, entre otras; las cuales fueron respondidas por la entidad mediante comunicaciones radicadas por SIPA y a través de la plataforma Legal Bog.

Por su parte, la salida no conforme que se presentó en la Dirección de Trámites Administrativos (reportada en los primeros meses del presente año y que corresponde al segundo semestre de la vigencia 2023) relacionada con el trámite de recursos por las decisiones que se adoptan frente al trámite de estaciones radioeléctricas, han sido documentadas en el formato definido por la SDP dejando la trazabilidad de las acciones de mejora adoptadas.

Para el periodo de monitoreo la primera línea de defensa reporta no tener hallazgos de auditoría asociados a los controles de los dos (2) riesgos de gestión del proceso.

3. ***Autoevaluación de la eficacia de las acciones:***

   Teniendo en cuenta que los riesgos se encuentran en zona residual moderada, no fue necesario formular plan de acción como herramienta para el tratamiento del riesgo, toda vez que con los controles es suficiente para mitigar la ocurrencia de estos.

   No se evidencia materialización de riesgos en el periodo objeto de monitoreo.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

   La información reportada por la primera línea de defensa y las evidencias de la aplicación efectiva de los controles formulados para los riesgos, permiten concluir que la gestión del riesgo ha sido adecuada y útil para evitar situaciones indeseables que afecten el cumplimiento de los objetivos y compromisos a cargo del proceso.

5. ***Actualización de Riesgos****:*

   Para el periodo del monitoreo, no se identificó la necesidad de modificar o actualizar los riesgos de gestión, ni tampoco la necesidad de documentar o gestionar nuevos riesgos de este tipo. Sin embargo, para el segundo cuatrimestre del año, desde la Dirección de Planeación Institucional se agendarán jornadas virtuales con los procesos para la revisión de indicadores y mapas de riesgos de conformidad con el nuevo mapa de procesos de la entidad e implementación del nuevo software para el Sistema de Gestión.

   Es importante mencionar que el Departamento Administrativo de la Función Pública - DAFP publicó en noviembre de 2022 la versión 6 de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, la cual contiene un nuevo capítulo para el análisis de riesgos fiscales cuya finalidad es prevenir el daño al patrimonio público, representando en el menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos o a los intereses patrimoniales del Estado. Por tal razón, la Dirección de Planeación Institucional se

encuentra adelantando lo pertinente para definir la hoja de ruta que permita su incorporación a los actuales mapas de riesgos de la entidad, con el acompañamiento de las dependencias correspondientes dada la naturaleza de este tipo de riesgos.

3.1.1.2 ALERTAS:

Para el periodo de monitoreo no se generan alertas para el proceso.

3.1.1.3 RECOMENDACIONES:

Para el segundo cuatrimestre de la presente vigencia, revisar los riesgos de gestión, de conformidad con el nuevo mapa de procesos de la entidad e implementación de la nueva herramienta tecnológica para el Sistema de Gestión denominada Gestiónate – Isolucion.

3.1.2 M-LE-225 MAPA DE RIESGOS DE CORRUPCIÓN DEL PROCESO PLANEACIÓN TERRITORIAL Y GESTIÓN DE SUS INSTRUMENTOS VERSIÓN 3 ACTA DE MEJORAMIENTO 32 DE ENERO 29 DE 2024

Riesgos de Corrupción
1. Posibilidad de generación de condiciones normativas en los instrumentos de planeación sin el lleno de requisitos para favorecer a un tercero.
2. Posibilidad de expedición de conceptos relacionados con la planeación territorial para favorecimiento indebido a un tercero

3.1.2.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias***.

   Mediante radicado en SIPA 3-2024-16274 del 6 de mayo de 2024 el proceso Planeación Territorial y Gestión de sus Instrumentos remitió a la Dirección de Planeación Institucional el monitoreo de primera línea de defensa a los riesgos asociados al mismo.

   El proceso realizó la actualización del mapa de riesgos de corrupción (versión 3) el 29 de enero de 2024 mediante acta de mejoramiento Nº32, en la cual se realizó el ajuste en la redacción de dos controle y de algunos aspectos del contexto como los procedimientos asociados, áreas que participan en el proceso, trámites, Opas y Consultas de información, líder del proceso y enlaces del SG.

   Por su parte, a partir de los talleres virtuales realizados con la Dirección de Planeamiento Local, Subdirección de Renovación Urbana y Desarrollo y Subdirección de Mejoramiento Integral (con la Subdirección de Planes Maestros se realizará en mayo de 2024) para la identificación de posibles riesgos de corrupción en trámites y OPAs, se realizará una nueva actualización del mapa de riesgos de corrupción en el segundo semestre de la presente vigencia.

   Los dos riesgos de corrupción guardan coherencia con el objetivo estratégico "Definir y promover un modelo colectivo de ciudad en el largo plazo, mediante la reglamentación y viabilización del territorio, a través de los instrumentos de planeación buscando el bienestar de la ciudadanía", toda vez que están orientados a la posibilidad de generación de condiciones normativas en los instrumentos de planeación sin el lleno de requisitos para favorecer a un tercero (riesgo Nº1) y a la posibilidad de expedición de conceptos relacionados con la planeación territorial para favorecimiento indebido a un tercero (riesgo Nº2).

   Teniendo en cuenta que el propósito del proceso contempla aspectos clave como la generación de condiciones normativas mediante Decisiones Urbanísticas, Actuaciones Administrativas y Formulación de Proyectos Distritales para el beneficio social, los dos riesgos de corrupción formulados por el proceso son coherentes con dicho objetivo al estar enmarcados en estos aspectos clave del proceso.

La primera línea de defensa manifiesta que para el periodo de monitoreo, las causas y consecuencias identificadas inicialmente se mantienen, razón por la cual se infiere que durante la normal operación del proceso no se han evidenciado alertas de nuevas causas y/o consecuencias que puedan incidir en el análisis del riesgo de corrupción.

2. ***Autoevaluación de la efectividad de los controles****.*

Para el presente monitoreo se observa que el proceso atendió la recomendación efectuada por la segunda línea de defensa relacionada con la profundización en el análisis de los controles y las evidencias que dan cuenta de su aplicación.

El Riesgo Nº1 cuenta con tres controles definidos:

** El primer control asociado a la revisión en la expedición de los actos administrativos, se aplica en las etapas que surten los diferentes actos expedidos por el proceso. Las evidencias aportadas por la primera línea de defensa corresponden a la trazabilidad de los actos en el sistema SIPA.*

** El segundo control se ejecuta a través del M-FO-017 Solicitud de determinantes para la formulación del plan parcial con sello de radicación de la SDP, así como por medio de oficios radicados formalmente en la entidad, en el marco de la solicitud de los trámites por parte de los usuarios.*

** Para el tercer control, la dependencia del proceso diligencia una matriz de actos administrativos con la información de la publicación en Gaceta de Urbanismo y Construcción, la página Web de la SDP y la BDGC. Igualmente, el proceso reporta como evidencia los correos emitidos por la Dirección Administrativa con el listado de las publicaciones. La evidencia SDP-2024-3755 contiene dos links de acceso, por tanto, se recomienda cargar un solo archivo cada vez que se diligencie el formulario para evitar errores o confusiones al momento de la consulta de la misma.*

El Riesgo Nº2 cuenta con dos controles:

** Se evidencia la aplicación del primer control relacionado con la revisión del contenido jurídico y técnico en la emisión de conceptos solicitados por la ciudadanía sobre normatividad urbanística, los cuales son proyectados por el profesional designado para revisión y firma del Directivo de la respectiva dependencia. Las evidencias que aporta el proceso corresponden a la trazabilidad de las revisiones en SIPA así como los oficios de respuesta con la información de quien elaboró, revisó y firmó los conceptos técnicos emitidos.*

** Para el segundo control, asociado a la matriz de actos administrativos con la información de la publicación en la Gaceta de Urbanismo y Construcción, la página web de la SDP y el cargue en la BDGC., las evidencias son las mismas que se referenciaron en el control 3 del riesgo 1.*

Por lo anteriormente expuesto, los cinco (5) controles revisados, previenen o mitigan los dos (2) riesgos de corrupción, razón por la cual estos se mantienen para tal fin.

3. ***Autoevaluación de la eficacia de las acciones:***

La acción formulada por el proceso en el plan de tratamiento del riesgo asociada a la realización de una capacitación en coordinación con la Oficina de Control

Disciplinario Interno sobre las implicaciones de tipo disciplinario que tiene para los servidores públicos los actos de corrupción, se viene ejecutando con normalidad. Las evidencias aportadas por el proceso reflejan la temática abordada en la capacitación, así como los datos básicos de los asistentes a la misma.

En el periodo objeto del monitoreo no hay indicios de la materialización de riesgos de corrupción ni hallazgos en las auditorías internas o externas relacionados con estos riesgos.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

   La información reportada por la primera línea de defensa y las evidencias de la aplicación efectiva de los dos controles formulados para los riesgos de corrupción, permiten concluir que su gestión ha sido adecuada y útil para evitar situaciones indeseables que afecten el cumplimiento de los objetivos y compromisos a cargo del proceso.

5. ***Actualización de Riesgos****:*

   Mediante memorando 3-2024-13355 del 8 de abril de 2024 la Dirección de Planeación Institucional informó a directivos y enlaces a cerca de la realización de talleres virtuales para la identificación de posibles riesgos de corrupción en trámites y OPAs. Así las cosas, se realizaron las sesiones correspondientes con la Dirección de Planeamiento Local, Subdirección de Renovación Urbana y Desarrollo y Subdirección de Mejoramiento Integral. El taller con la Subdirección de Planes Maestros se encuentra programado para mayo del presente año.

   Por lo anterior, se observa que es necesario modificar y/o actualizar los riesgos de corrupción.

3.1.2.2 ALERTAS:

Para el periodo de monitoreo no se generan alertas para el proceso.

3.1.2.3 RECOMENDACIONES:

Para el segundo cuatrimestre de la presente vigencia, revisar los riesgos de corrupción, de conformidad con el nuevo mapa de procesos de la entidad e implementación de la nueva herramienta tecnológica para el Sistema de Gestión denominada Gestiónate – Isolucion.

3.1.3 M-LE-224 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DEL PROCESO PLANEACIÓN TERRITORIAL Y GESTIÓN DE SUS INSTRUMENTOS VERSIÓN 2 ACTA DE MEJORAMIENTO 93 DE FEBRERO 14 DE 2024

Riesgo de Seguridad de la Información

1. Posibilidad de Perdida de Disponibilidad por fallas humanas; error en el uso o abuso de derechos y privilegios y destrucción de la Información que conforma la producción documental oficial del proceso de planeación territorial y gestión de sus instrumentos (decretos, resoluciones, cartografía, actas de concertación ambiental), debido a manejo manual de la información, insuficiente entrenamiento y capacitación sobre las políticas de seguridad y privacidad de la información, deficiencia en la autorización de permisos de la información y ausencia de copias de respaldo o backups de la información.

3.1.3.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias***.

   Se verificó la documentación proporcionada por Primera Línea y se confirma que el contexto estratégico identificado por el proceso se mantiene vigente. La actualización del mapa de riesgos M-LE-224 y en particular los controles establecidos para el riesgo identificado demuestran el compromiso del proceso con la gestión de riesgos de seguridad de la información.

   Se recomienda realizar un análisis con respecto a la formalización de la nueva plataforma estratégica de la SDP y la formalización de los nuevos mapas de procesos proyectada para mediados de la vigencia actual.

Se revisó la relación entre el riesgo identificado y el objetivo estratégico del proceso ("Definir y promover un modelo colectivo de ciudad en el largo plazo, mediante la reglamentación y viabilización del territorio, a través de los instrumentos de planeación buscando el bienestar de la ciudadanía"), concluyendo que el riesgo identificado es coherente con el objetivo estratégico, ya que la pérdida de disponibilidad de la información podría afectar significativamente la capacidad del proceso para cumplir con su objetivo.

En la revisión de la relación entre el riesgo identificado y el objetivo del proceso ("Generar condiciones normativas mediante Decisiones Urbanísticas, Actuaciones Administrativas y Formulación de Proyectos Distritales, que permitan viabilizar la estrategia de ordenamiento territorial y facilitar el desarrollo urbano y rural en términos de equilibrio y equidad territorial para el beneficio social"), se concluyó que el riesgo identificado es coherente con el objetivo del proceso, ya que la pérdida de disponibilidad de la información podría impedir la generación de condiciones normativas y la formulación de proyectos distritales.

En el monitoreo de Segunda Línea de Defensa, se revisaron las causas identificadas para el riesgo en el mapa de riesgos actualizado y se confirma que siguen siendo válidas.

Las causas incluyen:

- Manejo manual de la información.
- Insuficiente entrenamiento y capacitación sobre las políticas de

seguridad y privacidad de la información.
- Deficiencia en la autorización de permisos de la información.
- Ausencia de copias de respaldo o Backup de la información.

Estas causas siguen siendo relevantes en el contexto actual y podrían generar la pérdida de disponibilidad de la información.

Así mismo, se revisaron las consecuencias identificadas para el riesgo en el mapa de riesgos actualizado y se confirma que siguen siendo válidas. Las consecuencias incluyen:

- Afectación de la imagen de la entidad
- Pérdidas económicas.
- Retrasos en la ejecución de proyectos.
- Dificultad para el acceso a la información por parte de los ciudadanos.

Estas consecuencias siguen siendo relevantes en el contexto actual y podrían tener un impacto significativo en el proceso y en la entidad.

2. ***Autoevaluación de la efectividad de los controles****.*

Revisada la evidencia proporcionada por Primera Línea, se confirma que los cuatro controles establecidos para mitigar el riesgo "Posibilidad de Pérdida de Disponibilidad por fallas humanas, error en el uso o abuso de derechos y privilegios y destrucción de la Información" están siendo utilizados. La existencia de registros como videos de sesiones de talleres, formatos diligenciados para la entrega de puesto de trabajo, bitácoras de copias de respaldo, entre otros, demuestra la implementación y aplicación de los controles.

Como resultado del análisis para determinar la relación entre los controles establecidos y el riesgo, se concluye que los controles son adecuados para prevenir o mitigar el riesgo.

A continuación, se detalla la contribución por cada control:

Control 1. Capacitación en seguridad de la información: Esta capacitación ayuda a sensibilizar al personal sobre las buenas prácticas para proteger la información confidencial, lo que puede contribuir a reducir la probabilidad de errores o abusos por parte de los usuarios.

Control 2. Entrega formal de activos de información y transferencia de conocimiento: Al realizar una entrega formal de activos de información y una transferencia de conocimiento, se asegura que el personal que asume nuevas responsabilidades esté al tanto de los procedimientos de seguridad y la importancia de proteger la información.

Control 3. Verificación de usuarios: La revisión de los usuarios en la base de datos del directorio activo ayuda a garantizar que solo las personas autorizadas tengan acceso a la información.

Control 4. Copias de seguridad periódicas: Las copias de seguridad regulares permiten restaurar la información en caso de pérdida o corrupción accidental, lo que reduce el impacto potencial del riesgo.

Teniendo como base la información y evidencias suministradas por el líder del proceso, se infiere que no existen hallazgos de auditoría asociados a los controles establecidos para mitigar el riesgo identificado en el proceso. Esto

indica que los controles están siendo implementados de manera efectiva y cumplen con su propósito.

3. ***Autoevaluación de la eficacia de las acciones:***

   Si bien la valoración inicial del riesgo lo ubicó en una zona de riesgo bajo, es importante considerar que la materialización del riesgo podría tener un impacto significativo en el proceso y en la entidad. Adicionalmente, aunque el riesgo se ubicó como bajo, en el tratamiento del riesgo, el proceso optó por reducirlo /mitigarlo. Es de recordar que de conformidad con el instructivo del formato en lo que respecta a los planes de acción establece que: "*Esta casilla dependerá del tratamiento establecido, si es Aceptar no se requieren acciones adicionales, en caso de escoger Reducir (mitigar) se deben diligenciar las acciones que se adelantarán como complemento a los controles establecidos, no necesariamente son controles adicionales. Para Reducir (compartir), es viable diligenciar la acción que deriva de esta (ejemplo póliza seguros, tercerización), indicando información relevante*. ", en resumen, se recomienda revisar el tratamiento seleccionado y en el caso que se mantenga, es obligatorio la formulación de un plan de acción.

   No se formularon acciones para dar tratamiento al riesgo debido a su baja valoración inicial. Sin embargo, como se mencionó antes, se debe revisar si la opción de tratamiento es mitigar / reducir o es necesario formular un plan de acción o una corrección en la valoración.

   Resultado del análisis de la información suministrada por el proceso, hasta la fecha del reporte, no se evidencia que el riesgo se haya materializado ni que se haya identificado como hallazgo en auditorías internas o externas.

   Dado que el riesgo no se ha materializado, no se han formulado correcciones y/o acciones correctivas para darle tratamiento.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

   Se confirma que la gestión del riesgo ha sido útil para evitar situaciones o hechos que puedan afectar el cumplimiento de los objetivos y compromisos del proceso. La aplicación de los controles establecidos ha permitido:

   - Proteger la información contra accesos no autorizados, modificaciones o eliminación accidental o intencional.
   - Garantizar la continuidad de las operaciones del proceso.
   - Minimizar las pérdidas económicas y el impacto reputacional que podrían derivarse de la materialización del riesgo.

5. ***Actualización de Riesgos****:*

   Se confirma que, en este momento no existe la necesidad de modificar o actualizar el riesgo. La información proporcionada por Primera Línea, incluyendo la actualización del mapa de riesgos y del plan de tratamiento de riesgos, demuestra que el riesgo está siendo adecuadamente gestionado.

   Se recomienda validar este análisis frente a los cambios en el contexto estratégico que pueden suscitarse con la formalización de la nueva plataforma estratégica de la SDP y la puesta en marcha de los nuevos mapas de procesos que estará aplicando la entidad a mediados de la vigencia 2024 según lo proyectado.

Se ha realizado un análisis del contexto actual del proceso, considerando los cambios estratégicos, los resultados de auditorías internas y externas, y otros aspectos relevantes. En este momento, no se identifican nuevos riesgos que deban ser documentados y gestionados. Sin embargo, se recomienda mantener una vigilancia constante del entorno del proceso para identificar oportunamente cualquier nuevo riesgo que pueda surgir.

3.1.3.2 ALERTAS:

De acuerdo con el monitoreo de primera línea de defensa referente a los riesgos identificados de seguridad de la información del proceso de Planeación Territorial y Gestión de sus instrumentos, no se reportan alertas que indiquen que los riesgos se han materializado.

3.1.3.3 RECOMENDACIONES:

Se observa que el líder del proceso ha presentado evidencia que soporta la utilización de los controles, se recomienda establecer mecanismos para preservar la evidencia que permita confirmar que el control está siendo utilizado de manera efectiva, suficiencia y confiabilidad.

Liderar desde el proceso de Planeación Territorial las acciones de depuración de usuarios a sus repositorios, sistemas de información.

Realizar un seguimiento continuo de la revisión de los usuarios del directorio activo para verificar que se elimina el acceso de los usuarios que ya no lo necesitan.

Realizar un seguimiento continuo y verificar si las copias de respaldo que la DTIC realiza sobre su información verificar que las copias de respaldo se realizan de manera regular, se almacenan en un lugar seguro y se pueden ser recuperadas y en qué condiciones.

Se recomienda asistir a las sesiones de capacitación e inducción programadas por la entidad con el objeto de apropiar los conocimientos necesarios para conservar la confidencialidad, integridad y disponibilidad de la información.

3.2 COORDINACIÓN DE LAS POLÍTICAS PÚBLICAS Y DE LOS INSTRUMENTOS DE PLANEACIÓN

3.2.1 M-LE-137 MAPA DE RIESGOS DE GESTIÓN DEL PROCESO COORDINACIÓN DE LAS POLÍTICAS PÚBLICAS Y DE LOS INSTRUMENTOS DE PLANEACIÓN VERSIÓN 9 ACTA DE MEJORAMIENTO 68 DE ENERO 31 DE 2024

Riesgos de Gestión

1. Posibilidad de afectación económica y reputacional por desacierto en el seguimiento de política pública, debido a la a inexistencia y/o desactualización de los sistemas de información y/o de los instrumentos de seguimiento de políticas públicas y a la ausencia de oportunidad y calidad en la presentación de los informes de seguimiento a los planes de acción de las políticas públicas por parte de algunos sectores rectores de política.

2. Posibilidad de afectación reputacional por debilidad en el proceso de formulación e implementación de políticas públicas e instrumentos de planeación, debido a modificación de lineamientos técnicos de acuerdo con los cambios en la administración de grupos de valor, invisibilización de los grupos poblacionales en algunos espacios de la agenda pública e incumplimiento por parte de las entidades distritales de los lineamientos y/o circulares establecidos por la SDP.

3. Posibilidad de afectación reputacional por emisión de conceptos de traslado presupuestal a los Fondos de Desarrollo Local sin cumplimiento de requisitos de los conceptos de gasto, debido a la carencia de un repositorio que concentre el conocimiento funcional del equipo ejecutor del proceso y de buenas prácticas y lecciones aprendidas pese a la consolidación de procesos, procedimientos, guías metodológicas, formatos a nivel institucional como herramientas reconocidas.

3.2.1.1 OBSERVACIONES:

El proceso M-CA-002 Coordinación de las Políticas Públicas y de los Instrumentos de Planeación, mediante radicado en SIPA 3-2024-16640 del 8 de mayo de 2024, remite a la Dirección de Planeación Institucional el monitoreo de primera línea de defensa a los riesgos de gestión con corte 30/04/2024. Con la implementación de la nueva herramienta tecnológica Gestiónate (Isolución), se hará efectiva la puesta en operación del nuevo mapa de procesos de la SDP, lo cual implicará la separación de los procesos: "Políticas Públicas", "Plan Distrital de Desarrollo" y "Articulación del Diálogo Supradistrital", cada uno los cuales iniciará la implementación de su respectiva caracterización de proceso, a la luz de una nueva planeación estratégica 2024-2027.

1. ***Definición del riesgo, sus causas y consecuencias***.

El riesgo es coherente con los objetivos estratégicos a los cual le aporta el proceso debido a que el riesgo hace referencia a la Posibilidad de uso del poder en el proceso de política pública en el desarrollo de todo el ciclo de las políticas públicas. Las causas se mantienen dado que el riesgo se identificó con base en las causas internas y externas según lo definido en el contexto estratégico. Para el corte de abril de 2024, se verifica la

publicación del procedimiento M-PD-206, donde se evidencia el refuerzo a los controles. Con la implementación de la nueva herramienta tecnológica, Gestiónate-Isolución, se hará efectiva la puesta en operación del nuevo mapa de procesos de la SDP y se determinará si se modifican las causas para cada riesgo asociado a los tres nuevos procesos.

Las consecuencias identificadas para el riesgo se mantienen, debido a que éste, no se ha materializado. Con la implementación del nuevo mapa de procesos y a partir del análisis de nuevos riesgos y nuevas causas, se determinará cómo se modifican las consecuencias.

2. ***Autoevaluación de la efectividad de los controles****.*

Al revisar de la información aportada por la primera línea de defensa, se puede concluir lo siguiente respecto a cada riesgo:

Riesgo 1: se evidencia un acta de reunión con el nombre: Revisión de reportes y alcances de la política de Actividades Sexuales Pagadas con corte a diciembre 2023. En dicha acta, no existe forma de verificar que el control se aplique con periodicidad trimestral para la información cualitativa y cuantitativa de cada indicador. Control 2: valida los criterios definidos para el reporte cualitativo y cuantitativo, de acuerdo con la cadena de valor del producto y resultado y con la información que se debe asociar a los enfoques definidos, valor de meta programado, línea base y tipo de anualización.

Se verifica en el consecutivo 4276, el cual dirige al Drive Q4 Gráficas finales, en el cual reposa el Excel donde se realiza seguimiento a las PP a cargo de los diferentes sectores. Si bien el archivo remite al Plan de acción para realizar el seguimiento de la PP, no es clara la forma en que se validan los criterios para el reporte, conforme a lo definido en la redacción del control.

Riesgo 2: Debilidad en el proceso de formulación e implementación de Políticas públicas y los instrumentos de Planeación. Conforme a la información suministrada por la primera línea de defensa, no aplica la aplicación de controles en la medida que al corte 30/04/2024, no se han formulado PP.

Riesgo 3: Emisión de conceptos de traslado presupuestal a los fondos de desarrollo sin cumplimiento de requisitos Control 1: valida cada vez que se requiera que la solicitud de concepto de traslado y sus soportes adjuntos, sustenten el cumplimiento de lineamientos del CONFIS Distrital, el manual de presupuesto (de Hacienda) y los Criterios de Elegibilidad y Viabilidad Técnica y de incorporación de enfoques poblacionales (de los sectores lideres de los conceptos del gasto afectados). La evidencia cargada en el repositorio con código 4283, denominada: "Consolidado gestión para emisión y documentos conceptos Ene-Abril 2024" da cuenta de la relación de conceptos y soportes adjuntos conforme a los criterios definidos.

3. ***Autoevaluación de la eficacia de las acciones:***

No aplica, conforme a lo establecido en la política de riesgos, al quedar el riesgo residual en zona "moderado", no se deben formular acciones de tratamiento de riesgos.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

Si bien se evidencia la aplicación de los controles, es importante que los registros que son aportados para el cumplimiento de los controles, guarden relación con la forma como está redactado el riesgo.

5. ***Actualización de Riesgos****:*

Para el proceso M-CA-002 Coordinación de las Políticas Públicas y de los Instrumentos de Planeación se identifica la necesidad de gestionar modificar o actualizar los riesgos, esto, a partir de la implementación de la nueva herramienta tecnológica Gestiónate (Isolución), con la que se hará efectiva la puesta en operación del nuevo mapa de procesos de la SDP, lo cual implicará la separación de los procesos: "Políticas Públicas", "Plan Distrital de Desarrollo" y "Articulación del Diálogo Supradistrital", cada uno los cuales iniciará la implementación de su respectiva caracterización de proceso, a la luz de una nueva planeación estratégica 2024-2027.

3.2.1.2 ALERTAS:

No se generan alertas al proceso teniendo en cuenta que las acciones establecidas en el marco de los controles formulados de tipo preventivo y detectivo, se encuentran directamente relacionadas con las causas que originan los riesgos y han permitido contrarrestar y mitigar la materialización de los riesgos.

3.2.1.3 RECOMENDACIONES:

En general los riesgos se deben revisar a la luz del nuevo mapa de procesos y una vez se formule la nueva planeación estratégica para la entidad 2024-2027.

Se sugiere que para el próximo monitoreo se detalle en el campo de observaciones, el sustento mediante el cual se identifica que la gestión de la dependencia ha sido útil para evitar situaciones o hechos que puedan afectar el cumplimiento de los objetivos y compromisos a su cargo, dado que no se relacionaron argumentos para el análisis de los tres riesgos de gestión. Si bien las evidencias constituyen elementos fundamentales en la gestión de una parte del ciclo de las Políticas Públicas, para prevenir la materialización de los riesgos, es importante contar con registros que evidencien la gestión del ciclo completo, y sobre todo en los aspectos de planificación, ordenamiento y renovación urbana, los cuales son descritos explícitamente en el riesgo.

3.2.2 M-LE-222 MAPA DE RIESGOS DE CORRUPCIÓN DEL PROCESO COORDINACIÓN DE LAS POLÍTICAS PÚBLICAS Y DE LOS INSTRUMENTOS DE PLANEACIÓN VERSIÓN 2 ACTA DE MEJORAMIENTO 67 DE ENERO 31 DE 2024

Riesgos de Corrupción
1. Posibilidad de uso del poder en el proceso de política pública por el rol de la SDP en el liderazgo y coordinación del ciclo de políticas públicas, por el creciente interés de diferentes actores en los temas de planificación, ordenamiento y renovación urbana.

El proceso M-CA-002 Coordinación de las Políticas Públicas y de los Instrumentos de Planeación, mediante radicado en SIPA 3-2024-16290 del 6 de mayo de 2024 remite a la Dirección de Planeación Institucional el monitoreo de primera línea de defensa a los riesgos con corte 30/04/2024. Con la implementación de la nueva herramienta tecnológica Gestiónate (Isolución), se hará efectiva la puesta en operación del nuevo mapa de procesos de la SDP, lo cual implicará la separación de los procesos: "Políticas Públicas", "Plan Distrital de Desarrollo" y "Articulación del Diálogo Supradistrital", cada uno los cuales iniciará la implementación de su respectiva caracterización de proceso, a la luz de una nueva planeación estratégica 2024-2027.

3.2.2.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias.***

El riesgo es coherente con el objetivo del proceso: "Orientar y coordinar la formulación, seguimiento y evaluación de las políticas públicas e instrumentos de planeación mediante la definición de lineamientos, directrices y la asistencia técnica, para facilitar la acertada toma de decisiones en la gestión pública", debido a que es relevante en términos de los sucesos que se pueden producir a nivel de la entidad y las consecuencias que puedan tener sobre los objetivos de ésta, teniendo en cuenta la incertidumbre, la posibilidad de sucesos futuros y los efectos que se generan sobre el objetivo planificado. El riesgo se debe revisar a la luz del nuevo mapa de procesos de la entidad, y una vez se formule la nueva planeación estratégica para la entidad 2024-2027.

Las causas se mantienen dado que el riesgo se identificó con base en las causas internas y externas según lo definido en el contexto estratégico. Con la implementación de la nueva herramienta tecnológica, Gestiónate-Isolución, se hará efectiva la puesta en operación del nuevo mapa de procesos de la SDP y se determinará si se modifican las causas. Las consecuencias identificadas para el riesgo se mantienen, debido a que éste, no se ha materializado.

2. ***Autoevaluación de la efectividad de los controles.***

Según la información aportada por la primera línea de defensa, se concluye que, no aplica la realización de: Control 1: verificación del cumplimiento de la guía de formulación e implementación de política pública y la caja de herramientas, a través de la realización de mesas o talleres de trabajo Control 2: revisión del concepto técnico unificado de la SDP sobre la propuesta de estructuración de la política pública, en la medida en que no se ha realizado la formulación de ninguna PP, en el corte abril 2024.

3. ***Autoevaluación de la eficacia de las acciones:***

La acción que se tiene prevista en el Plan de tratamiento es la siguiente: Realizar jornadas de capacitación en temas de riesgos de corrupción, normativa asociada y

consecuencias, al equipo de la dirección de formulación y seguimiento de políticas públicas que emite los conceptos de viabilidad de en el proceso de formulación de las políticas públicas..", dicha acción está orientada a contrarrestar las causas identificadas, sin embargo, no se evidencia registro al seguimiento del plan de tratamiento para la vigencia 2024 (columnas BM BN y BO del mapa de corrupción). Conforme a la información aportada por la primera línea de defensa, se argumenta que las acciones se encuentran sin iniciar.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

Según se realice el reporte para el corte de agosto de 2024, se revisará este aspecto por parte de la segunda línea de defensa.

5. ***Actualización de Riesgos****:*

Para el segundo semestre 2024, se realizará la revisión integral del riesgo, dada la implementación de la nueva herramienta tecnológica: Gestiónate (Isolución), y la puesta en operación del nuevo mapa de procesos de la SDP, lo cual implicará la separación de los procesos: "Políticas Públicas", "Plan Distrital de Desarrollo" y "Articulación del Diálogo Supradistrital", cada uno los cuales iniciará la implementación de su respectiva caracterización de proceso, a la luz de una nueva planeación estratégica 2024-2028. Específicamente en el proceso Políticas Públicas, se deben revisar los riesgos asociados a la formulación, el seguimiento, la evaluación y la asistencia técnica del ciclo de la política pública.

3.2.2.2 ALERTAS:

No se generan alertas al proceso teniendo en cuenta que las acciones establecidas en el marco de los controles formulados de tipo preventivo y detectivo, se encuentran directamente relacionadas con las causas que originan los riesgos y han permitido contrarrestar y mitigar la materialización de los riesgos.

3.2.2.3 RECOMENDACIONES:

No aplica, ya que no se ha ejecutado la actividad que genera el riesgo no ha existido la necesidad de aplicar los controles para mitigar o evitar que se presente la materialización del riesgo.

3.2.3 M-LE-223 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DEL PROCESO COORDINACIÓN DE LAS POLÍTICAS PÚBLICAS Y DE LOS INSTRUMENTOS DE PLANEACIÓN VERSIÓN 2 ACTA DE MEJORAMIENTO 178 DE ABRIL 16 DE 2024

Riesgo de Seguridad de la Información

1. Posibilidad de Perdida de Integridad por fallas humanas; de conceptos técnicos, debido a insuficiente entrenamiento y capacitación sobre políticas las de seguridad y privacidad de la información

Posibilidad de Perdida de Disponibilidad por fallas humanas; de activos de información, debido a manejo manual de la información, ausencia de copias de respaldo o Backup de la información.

3.2.3.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias***.

El líder del proceso observó que, en el marco de la llegada de la nueva administración, se han identificado necesidades de ajuste y mejora en el proceso. De manera particular para Políticas Públicas, se establece un nuevo proceso que afectará los riesgos de seguridad de la información identificados anteriormente. En razón a esta afirmación, es importante considerar que una vez formalizado el cambio en el contexto estratégico puede tener un impacto significativo en los riesgos identificados para el proceso haciendo necesario evaluar si los riesgos actuales siguen siendo relevantes y si es necesario realizar una actualización del mapa de riesgos.

Por ahora, hasta tanto se adelante la actualización del Mapa de Procesos acorde al rediseño institucional, el riesgo es coherente con el objetivo estratégico, es importante recordar que el contexto estratégico y del proceso van a cambiar lo que hace necesario verificar una vez formalizados los cambios, el riesgo sigue siendo coherente con los nuevos objetivos estratégicos y del proceso.

Los riesgos identificados son acordes al proceso de Coordinación de Políticas Públicas y de los Instrumentos de Planeación. La respuesta de la primera línea es adecuada, ya que reconoce que los riesgos identificados son relevantes para el proceso actual y que el proceso está en proceso de rediseño lo cual evidencia que los riesgos deben ser actualizados.

La respuesta de la primera línea reconoce que el cambio en el proceso puede afectar las causas de los riesgos por ello algunas causas se deben ajustar teniendo en cuenta los lineamientos y el nuevo contexto que defina el proceso. No obstante, en el análisis se concluye que el insuficiente entrenamiento y capacitación sobre políticas las de seguridad y privacidad de la información, el manejo manual de la información y la ausencia de copias de respaldo o backups de la información son causas que deben ser revisadas y actualizadas con el fin de alinearlas a contexto estratégico formulado en el rediseño institucional.

Aunque se debe evaluar las consecuencias de los riesgos en detalle y determinar si es necesario realizar ajustes dado la implementación de nueva plataforma estratégica, por ahora en el marco del contexto actual, se mantiene hasta tanto no se haga efectiva la actualización al nuevo modelo organizacional de la entidad.

2. ***Autoevaluación de la efectividad de los controles.***

El líder del proceso en el monitoreo reportó que:

- Se guardan registros, en los repositorios oficiales, de acuerdo con lo establecido en materia de seguridad de la información y e integridad de esta.

- La Directora de DFSPP utiliza la herramienta oficial SIPA para verificar los documentos. Allì se guarda la trazabilidad y por tanto, evidencia del control.

- La DFSPP revisa y valida los documentos emitidos por su dependencia a través de Sipa, por lo que no se tiene registro ya que la trazabilidad queda en el Sipa.

- Así mismo, los funcionarios aplican las políticas de seguridad de la información y la conservación de la misma a través del repositorio donde se alojan los documentos elaborados por la dirección según las tablas de retención documental.

La respuesta de la primera línea indica que existen registros que evidencian la utilización del control. Sin embargo, es importante verificar la calidad y completitud de estos registros dado que verificadas la evidencia ID SDP-2024-4278 / ID SDP-2024-4279 no se encontró muestras de los registros para asegurarse de que sean suficientes para demostrar que el control se está utilizando de manera efectiva.

Los controles establecidos en el Riesgo 1: Posibilidad de Pérdida de Integridad por fallas humanas; de conceptos técnicos, debido a insuficiente entrenamiento y capacitación sobre políticas las de seguridad y privacidad de la información aportan a prevenir o mitigar los riesgos de la siguiente manera:

Control 1: Revisión y validación de conceptos por directivos del proceso. Este control mitiga el riesgo de pérdida de integridad de la información al garantizar que los conceptos técnicos sean revisados y validados por personal calificado antes de su emisión final. Esto ayuda a detectar y corregir errores o inconsistencias que podrían afectar la integridad de la información.

Control 2: Velar por el conocimiento y cumplimiento de procedimientos por parte del Líder del proceso. Este control mitiga el riesgo al asegurar que todos los colaboradores del proceso conozcan y apliquen los procedimientos establecidos para la gestión de la información. El control ayuda a minimizar la posibilidad de errores humanos que puedan comprometer la integridad de la información.
En el caso del Riesgo 2: Posibilidad de Pérdida de Disponibilidad por fallas humanas; de activos de información, debido a manejo manual de la información, ausencia de copias de respaldo o Backup de la información. Los controles coadyuvan a la seguridad y privacidad de la información así:

Control 1: Conocimiento y aplicación de lineamientos de seguridad de la información por parte de los colaboradores. Este control mitiga el riesgo al garantizar que los colaboradores del proceso conozcan y apliquen las políticas de seguridad de la información, lo que ayuda a proteger los activos de información contra accesos no autorizados, modificaciones no autorizadas y pérdida accidental o intencional.

Control 2: Conocimiento y aplicación de procedimientos y directrices de conservación de registros por parte de los colaboradores. Este control mitiga el riesgo al asegurar que los colaboradores del proceso conozcan y apliquen los procedimientos y directrices para

la conservación de registros, lo que garantiza que la información se almacena, protege y elimina de acuerdo con las normas y políticas establecidas.

No se han identificado hallazgos de auditoría asociados a los controles durante el período evaluado.

3. ***Autoevaluación de la eficacia de las acciones:***

La Primera Línea de Defensa no ha formulado acciones para tratar los riesgos identificados, por lo tanto, no se posible examinar si están orientadas a contrarrestar las causas.

No obstante, las acciones definidas en los controles para cada riesgo contrarrestan las causas de la siguiente forma:

En el caso del Riesgo 1. Posibilidad de Pérdida de Integridad de conceptos técnicos, las acciones que contrarrestan las causas por cada control son:

Control 1: La revisión y validación de conceptos por directivos del proceso, permite detectar con mayor precisión errores o inconsistencias en los conceptos técnicos, lo que reduce la probabilidad de que estos sean emitidos con información comprometida.

Control 2: Velar por el conocimiento y cumplimiento de procedimientos y políticas como la de seguridad y privacidad de la información por parte del Líder del proceso, permite identificar desviaciones o incumplimientos en el cumplimiento de los procedimientos, lo que facilita la toma de medidas correctivas oportunas para prevenir la pérdida de integridad de la información y a la vez fomenta una cultura de cumplimiento, crea un entorno en el que el cumplimiento de los procedimientos es valorado y exigido, lo que reduce la probabilidad de que se produzcan errores o fallas por negligencia o falta de conocimiento.

Para el riesgo 2. Posibilidad de Perdida de Disponibilidad de activos de información, se identifican las acciones por cada control así:

Control 1. El conocimiento y aplicación de lineamientos de seguridad de la información por parte de los colaboradores, permite que los estén en mejores condiciones para proteger los activos de información de la organización, reduciendo la probabilidad de errores humanos que puedan ocasionar la pérdida de disponibilidad de la información.

Control 2. El conocimiento y aplicación de procedimientos y directrices de conservación de registros por parte de los colaboradores, les permite gestionar la información de manera adecuada y prevenir su pérdida o alteración.

Considerando que no se formularon planes de acción, no se han implementado acciones complementarias a los controles.

De otra parte, en este momento, no es posible evaluar si las acciones en cada control propuestas para contrarrestar los riesgos en el proceso M-CA-002 se están implementando adecuadamente, debido a que desde el proceso no se presentaron evidencias sobre la implementación de las acciones en los controles definidos en el proceso.

La Primera Línea de Defensa indica que el riesgo no se ha materializado hasta el momento. Revisada la información suministrada no se encuentra evidencia que alguno de los riesgos se haya materializado.
No se formularon correcciones ni acciones correctivas dado que los dos riesgos identificados no se han materializado.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

La identificación y evaluación de los riesgos asociados a la información ha permitido

implementar medidas de control adecuadas para proteger la disponibilidad, confidencialidad e integridad de la información, como la capacitación en seguridad de la información, la implementación de procedimientos para la gestión de registros y la realización de copias de seguridad. Esto ha contribuido a prevenir incidentes de seguridad que podrían haber afectado el cumplimiento de los objetivos del proceso y la confianza de las partes interesadas.

La gestión de riesgos ha ayudado a la entidad a cumplir con las normas y regulaciones aplicables a la protección de la información, lo que ha evitado sanciones legales y multas. Esto ha contribuido a la imagen y reputación de la entidad.

Desde el proceso se ha fomentado una cultura de gestión de riesgos en la entidad, donde los colaboradores son conscientes de la importancia de identificar, evaluar y tratar los riesgos de manera adecuada, se conocen y aplican los lineamientos establecidos en la política A LE 429 Políticas de seguridad y privacidad de la información y se aplican los procedimientos documentados así como las directrices de conservación de los registros productos de los mismos, contribuyendo a la creación de un entorno más seguro y controlado para el desarrollo de las actividades del proceso.

5. ***Actualización de Riesgos****:*

La Primera Línea de Defensa debe realizar una actualización completa de la identificación de riesgos del proceso M-CA-002, considerando los cambios en el contexto estratégico, los resultados de informes de auditoría internos y externos, y otros aspectos relevantes. La actualización debe incluir la revisión de los riesgos existentes, la identificación de nuevos riesgos y la evaluación de la probabilidad e impacto de todos los riesgos.

La implementación de la nueva plataforma tecnológica y los mapas de procesos en 2024 puede generar nuevos riesgos o modificar la probabilidad o el impacto de los riesgos existentes generando la necesidad de documentar y gestionar nuevos riesgos. Es importante que la Primera Línea de Defensa realice una evaluación de riesgos actualizada en el marco de la implementación de la nueva plataforma y los mapas de procesos

3.2.3.2 ALERTAS:

De acuerdo con el monitoreo de primera línea de defensa referente a los riesgos identificados de seguridad de la información del proceso de Planeación Territorial y Gestión de sus instrumentos, no se reportan alertas que indiquen que los riesgos se han materializado**.**

3.2.3.3 RECOMENDACIONES:

Se recomienda que para el próximo monitoreo se presente evidencia que soporte la utilización de los controles, y establecer mecanismos para preservar la evidencia que permita confirmar que el control está siendo utilizado de manera efectiva, suficiencia y confiabilidad.

Realizar un seguimiento continuo de la revisión de los usuarios del directorio activo para verificar que se elimina el acceso de los usuarios que ya no lo necesitan.

Se recomienda adelantar lo necesario para estar listos a la formalización de la nueva plataforma estratégica de la entidad.

Se recomienda asistir a las sesiones de capacitación e inducción programadas por la entidad con el objeto de apropiar los conocimientos necesarios para conservar la confidencialidad, integridad y disponibilidad de la información.

.

3.3 PRODUCCIÓN, ANÁLISIS Y DIVULGACIÓN DE LA INFORMACIÓN

3.3.1 M-LE-164 MAPA DE RIESGOS DE GESTIÓN DEL PROCESO PRODUCCIÓN, ANÁLISIS Y DIVULGACIÓN DE LA INFORMACIÓN VERSIÓN 4 ACTA DE MEJORAMIENTO 86 DE FEBRERO 09 DE 2024

Riesgos de Gestión

1. Posibilidad de afectación económica y reputacional por deficiencia en la recolección, digitación y cargue de la información, debido a diseños metodológicos internos y externos inapropiados y/o desactualizados, recursos insuficientes tanto para la actualización de tecnologías como para la capacitación en la recolección de información y deficiencia en la apropiación y aplicación de los instructivos o protocolos frente a la información recibida.

2. Posibilidad de afectación reputacional por reclamaciones o quejas de las partes interesadas, que podrían implicar actuaciones judiciales y disciplinarias, debido a la inexactitud en la entrega y divulgación de la información gráfica y alfanumérica a través de los diferentes canales de atención.

3.3.1.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias.***

Mediante radicado en SIPA 3-2024-16713 en SIPA del 08 de mayo de 2024 el proceso remitió a la Dirección de Planeación Institucional el monitoreo de primera línea de defensa a los riesgos de gestión y seguridad de la información con corte a 30 de abril de 2024.

La primera línea de defensa reporta que el contexto estratégico no cuenta con cambios significativos, de igual manera, que se mantienen sus causas y consecuencias de los riesgos de gestión identificados. Sin embargo, se evidenció que no estaba mencionado el trámite de Certificación de Estratificación Socioeconómica, el cual sigue vigente en el inventario de trámites y OPA en la entidad.

Dichos riesgos son coherentes con el objetivo estratégico relacionado con "*Fortalecer la generación, procesamiento y disponibilidad de la información estratégica de Bogotá Región*", dado que tiene como principal objeto verificar que la información producida por la entidad con el ánimo de garantizar que sea de calidad, oportuna y divulgada al usuario final.

De igual manera son coherentes con el objetivo del proceso, específicamente en lo mencionado " *(...) con el fin de realizar el suministro de información para la toma de decisiones de la ciudadanía, administración distrital y partes interesadas, a través de los diferentes canales de atención*" dicha información debe cumplir con criterios de claridad, objetividad y transparencia para los diferentes grupos de valor e interés.

2. ***Autoevaluación de la efectividad de los controles.***

Para el **Riesgo N°1** la primera línea de defensa reporta evidencias de los ocho (8) controles establecidos, sin embargo, se presentaron dificultades en la revisión de los controles 3, 4, 5 y 6, si bien se relaciona un link de Drive que orienta a las evidencias de la aplicación de los controles en los procedimientos de la DIES, se recomienda para próximos monitoreos que se pueda indicar cada control en que procedimiento específico se

encuentra, para facilitar la revisión de la segunda y tercera línea de defensa.

En cuanto al **Riesgo N°2** cuenta con cinco (5) controles, de los cuales, no se encontró evidencia para los controles 2 y 3 a cargo de la Dirección de Servicio a la Ciudadanía.

Si bien la formulación de los controles está directamente relacionada con los riesgos, tras no contar con la totalidad de la aplicación de los controles por parte de proceso en sus dos riesgos, para la segunda línea de defensa no se cuenta con los argumentos suficientes para indicar si previene o mitiga el riesgo.

3. ***Autoevaluación de la eficacia de las acciones:***

Teniendo en cuenta que los riesgos se encuentran en zona residual baja, sin embargo, el proceso estableció la acción "*3 jornadas de socialización de los procedimientos del proceso realizadas por cada una de las Direcciones de la Subsecretaría",* pero en el seguimiento efectuado por la segunda línea no se cuenta con evidencias para demostrar su eficacia.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

En la revisión integral de la aplicabilidad de los controles y acciones establecidas para el riesgo, se evidencia que ha sido útil para evitar situaciones o hechos que puedan afectar el cumplimiento de las actividades del proceso.

5. ***Actualización de Riesgos****:*

Si bien para el momento del presente reporte no se tiene establecida una fecha concreta para la implementación de la nueva herramienta del sistema de gestión "Gestiónate", es importante que el proceso tenga presente que es necesario contar con una nueva actualización del mapa de riesgos de gestión, de conformidad con el ajuste del mapa de procesos.

3.3.1.2 ALERTAS:

- Remitir evidencias de todos los controles descritos para cada uno de los riesgos de gestión identificados por el proceso.
- Remitir evidencias del cumplimiento de la acción planteada para reducir el riesgo de gestión N°1.

3.3.1.3 RECOMENDACIONES:

- Fortalecer el reporte de los controles, se evidencia que, hay casos como los controles 1 y 2 del riesgo N°1 que están debidamente sustentados, mientras otros controles no brindan suficiente información como fue el caso de los controles 3, 4, 5 que no se especifica en que parte encontrar la evidencia clara de la aplicación.
- En términos de la redacción del reporte para el caso del ítem "*Efectividad de la gestión de riesgos*", es importante que el proceso fortalezca la argumentación para dar cuenta del cumplimiento de este ítem.
- Revisar que la información del contexto estratégico esté completa.

3.3.2 M-LE-221 MAPA DE RIESGOS DE CORRUPCIÓN DEL PROCESO PRODUCCIÓN, ANÁLISIS Y DIVULGACIÓN DE LA INFORMACIÓN VERSIÓN 2 ACTA DE MEJORAMIENTO 51 DE ENERO 31 DE 2024

Riesgos de Corrupción
1. Posibilidad de adulteración y /o manipulación por acción u omisión de la información oficial para beneficio privado.

3.3.2.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias***.

Mediante radicado en SIPA 3-2024-16305 en SIPA del 06 de mayo de 2024 el proceso remitió a la Dirección de Planeación Institucional el monitoreo de primera línea de defensa a los riesgos de corrupción con corte a 30 de abril de 2024.

La primera línea de defensa reporta que el contexto estratégico no cuenta con cambios significativos, de igual manera, que se mantienen sus causas y consecuencias de los riesgos de gestión identificados. Sin embargo, se evidenció que no estaba mencionado el trámite de Certificación de Estratificación Socioeconómica, el cual sigue vigente en el inventario de trámites y OPA en la entidad.

El riesgo definido para el proceso frente a la posibilidad de: "*Adulteración y /o manipulación por acción u omisión de la información oficial para beneficio privado*" es coherente con el objetivo estratégico relacionado con "*Fortalecer la generación, procesamiento y disponibilidad de la información estratégica de Bogotá Región*", dado que tiene como principal objeto verificar que la información producida por la entidad sea objetiva y estratégica para el usuario que lo solicita.

De igual manera es coherente con el objetivo del proceso, frente a la posibilidad de: "*Adulteración y /o manipulación por acción u omisión de la información oficial para beneficio privado*" es coherente con el objetivo del proceso, específicamente en lo mencionado *" (...) con el fin de realizar el suministro de información para la toma de decisiones de la ciudadanía, administración distrital y partes interesadas, a través de los diferentes canales de atención*" dicha información debe cumplir con criterios de claridad, objetividad y transparencia para los diferentes grupos de valor e interés.

2. ***Autoevaluación de la efectividad de los controles***.

La primera línea de defensa reporta evidencias de cinco (5) de los seis (6) controles establecidos, faltando evidencia o explicación alguna para el caso del control "*El profesional de la Dirección de Información y Estadísticas revisa semestralmente las causas relacionadas con la posible ocurrencia del riesgo, identificadas en la matriz de riegos de corrupción, de las causas establecidas en el riesgo, para identicar su posible materialización, para verificar su cumplimiento y garantizar que haya eficiencia en la recolección y cargue de la información con el fin de generar las alertas respectivas al servidor competente para la aplicación de correctivos*".

Desde la segunda línea de defensa se evidencia que los controles están asociados con el riesgo y su correcta aplicación dan cuenta de la mitigación del riesgo. Cabe aclarar que es importante que el proceso revise que todos sus controles estén debidamente documentados para dar cuenta de su aplicabilidad

3. ***Autoevaluación de la eficacia de las acciones:***

La acción "*3 jornadas de socialización de los procedimientos del proceso realizadas por cada una de las Direcciones de la Subsecretaría*" actualmente se encuentra en proceso de ejecución y de acuerdo con la información suministrada por la primera línea de defensa, se informa que la Dirección de Información y Estadísticas reporta el desarrollo de una jornada de socialización. Sin embargo, es necesario que para el próximo seguimiento se remitan las evidencias que den cuenta de los aspectos mencionados por la primera línea que busca tratar en cada una de las jornadas.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

En la revisión integral de la aplicabilidad de los controles y acciones establecidas para el riesgo, se evidencia que ha sido útil para evitar situaciones o hechos que puedan afectar el cumplimiento de las actividades del proceso. Se recomienda que el monitoreo de primera línea se recoja de manera integral los aportes de las dependencias, si bien estas son un insumo, la invitación es que el líder del proceso realice esta evaluación.

5. ***Actualización de Riesgos****:*

Teniendo en cuenta que mediante memorando 3-2024-08374 del 27 de febrero de 2024 la Oficina de Control Interno efectuó el llamado para revisar los riesgos de corrupción asociados a trámites y OPA es necesario que el proceso adelante una actualización de su mapa de riesgos en el entendido que cuenta con trámites asociados, este ajuste debe tenerse en cuenta para documentar y gestionar nuevos riesgos asociados a este tema. Con este fin, desde la Dirección de Planeación Institucional se expidió el memorando 3-2024-13355 del 08 de abril indicando la realización de talleres para la identificación y análisis de posibles factores que conlleven a riesgos de corrupción. Para el caso del proceso de PADI se programaron para los días 7 y 9 de mayo de 2024.

3.3.2.2 ALERTAS:

- Remitir evidencias de <u>todos</u> los controles descritos para cada uno de los riesgos de gestión identificados por el proceso.
- Tener presente la inclusión de los resultados de los talleres adelantados con la Dirección de Planeación Institucional frente a los riesgos de corrupción asociados a trámites y OPA.

3.3.2.3 RECOMENDACIONES:

- En términos de la redacción del reporte para el caso del ítem "*Efectividad de la gestión de riesgos*", es importante que el proceso fortalezca la argumentación para dar cuenta del cumplimiento de este ítem.
- Revisar que la información del contexto estratégico esté completa.
- Fortalecer el reporte de cumplimiento de la acción establecida para reducir el riesgo de corrupción.

3.3.3 M-LE-220 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DEL PROCESO PRODUCCIÓN, ANÁLISIS Y DIVULGACIÓN DE LA INFORMACIÓN VERSIÓN 2 ACTA DE MEJORAMIENTO 108 DE FEBRERO 22 DE 2024

Riesgo de Seguridad de la Información
1. Posibilidad de pérdida de confidencialidad de la "Información Sisbén" registrada en Oracle por accesos abusivos al sistema informático si no hay mecanismos de identificación y autenticación adecuados que eviten el acceso de personas no autorizadas en el sistema que consulten usen o sustraigan la información de las encuestas; igualmente, se puede presentar una pérdida de la confidencialidad si la información de Oracle es hurtada debido a fallas en la configuración correcta de los parámetros de seguridad del sistema contra software maliciosos o descargas ilegales de la base de datos por ejemplo. 2. Posibilidad de pérdida de la disponibilidad de la información en el Aplicativo de Consulta Sisbén a causa de una saturación del sistema imprevista al ser un software inmaduro, igualmente, se puede presentar un mal funcionamiento del software por fallas en el mismo al no hacer pruebas suficientes de software o que la información sea destruida y se pierda por no generar copias de respaldo suficientes y oportunas 3. Posibilidad de pérdida de integridad de la información por la denegación de servicios informáticos por parte del Departamento Nacional de Planeación -DNP si los equipos donde se instala el aplicativo no se configuran correctamente de acuerdo a los parámetros técnicos y de seguridad requeridos. Igualmente, se pueden presentar perdidas en la integridad de la información por no hacer el mantenimiento adecuado del sistema conforme a las versiones de actualización que establezca el DNP. 4. Posibilidad de pérdida de confidencialidad de la información registrada en el aplicativo por copias fraudulentas que se hagan a las bases de datos que alimentan el sistema debido a una configuración incorrecta de los parámetros de seguridad que permitan éstas y otras acciones no autorizadas; igualmente es posible que se pierda la confidencialidad si terceros no autorizados logran falsificar sus derechos de acceso porque los controles de identificación y autenticación de usuarios no operan correctamente.

3.3.3.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias.***

La respuesta del líder del proceso indica que se ha revisado el contexto estratégico identificado para el proceso y ha determinado que sigue siendo relevante. Esto significa que los factores externos e internos que pueden afectar al proceso no han cambiado significativamente. sin embargo, se debe evaluar cambios en la misión, visión y valores de la organización, la estructura organizacional y los sistemas de información con ocasión de la formalización de la nueva plataforma estratégica y los nuevos mapas de procesos prevista para mediados de 2024.

Los riesgos identificados están relacionados con la confidencialidad, integridad y disponibilidad de la información por debilidades en la gestión de los sistemas de información, la denegación de servicios informáticos por parte del Departamento Nacional de Planeación -DNP y copias fraudulentas que se hagan a las bases de datos. En el caso de su materialización puede afectar el logro del objetivo estratégico de fortalecer la generación, procesamiento y disponibilidad de la información estratégica

para la Región de Bogotá. Por ejemplo, si se pierde información confidencial, se puede afectar la reputación de la entidad, si la información se modifica o corrompe, puede provocar errores en la toma de decisiones y si la información no está disponible, puede obstaculizar la prestación de servicios y el logro de los objetivos de la entidad.

Se confirma que los riesgos identificados son coherentes con el objetivo del proceso. En el caso de que se materialice alguno de estos, puede afectar el logro del objetivo del proceso de capturar, recolectar, administrar, actualizar, analizar y producir información estratégica del Distrito Capital y la región de la siguiente manera:

- Si se pierde información confidencial, se puede afectar la capacidad del proceso para cumplir con su objetivo de proporcionar información confiable a las partes interesadas.

- Si la información se modifica o corrompe, se puede afectar la capacidad del proceso para producir información precisa y útil.

- Si la información no está disponible, se puede afectar la capacidad del proceso para cumplir con su objetivo de proporcionar información a las partes interesadas de manera oportuna.

Producto del análisis integral de los riesgos y de acuerdo con la respuesta del líder del proceso, las causas se mantienen.

Para el caso del Riesgo 1: Posibilidad de pérdida de confidencialidad de la "Información Sisbén" registrada en Oracle por accesos abusivos al sistema informático, las causas con respecto a las vulnerabilidades en los sistemas de información definidos por el proceso incluyen controles de acceso inadecuados, Software desactualizado, Fallas de configuración. En este sentido, se debe prestar atención a amenazas como: Hackers, funcionarios malintencionados, Spyware, Malware, entre otros y a eventos tales como errores humanos y desastres naturales.

En el Riesgo 2: Posibilidad de pérdida de la disponibilidad de la información en el Aplicativo de Consulta Sisbén a causa de una saturación del sistema imprevista al ser un software inmaduro también se puede entre ver que existen causas relacionadas con vulnerabilidades en los sistemas de información como software inmaduro, capacidad de procesamiento insuficiente y errores de diseño. Se recomienda evaluar eventos relacionados con el aumento inesperado del tráfico de usuarios, fallas de hardware, fallas en la conectividad y Desastres naturales.

En el Riesgo 3: Posibilidad de pérdida de integridad de la información por la denegación de servicios informáticos por parte del Departamento Nacional de Planeación -DNP si los equipos donde se instala el aplicativo no se configuran correctamente de acuerdo con los parámetros técnicos y de seguridad requeridos. el proceso identificó causas relacionadas con vulnerabilidades en los sistemas de información como lo son la configuración incorrecta del software, Falta de actualizaciones de seguridad y Hardware insuficiente. Se recomienda revisar eventos como fallas de comunicación con el DNP, ataques cibernéticos y desastres naturales.

Por último el proceso definió el Riesgo 4 como la posibilidad de pérdida de confidencialidad de la información registrada en el aplicativo por copias fraudulentas que se hagan a las bases de datos que alimentan el sistema debido a una configuración incorrecta de los parámetros de seguridad que permitan éstas y otras acciones no autorizadas; igualmente es posible que se pierda la confidencialidad si terceros no autorizados logran falsificar sus derechos de acceso porque los controles de

identificación y autenticación de usuarios no operan correctamente. Así mismo identificó causas en las vulnerabilidades en los sistemas de información relacionadas con controles de acceso inadecuados, software desactualizado y fallas de configuración.

Desde el proceso se identificó que las consecuencias del riesgo siguen siendo relevantes. Esto significa que los factores que pueden desencadenar el riesgo siguen existiendo.

Dentro de las consecuencias identificadas están las siguientes:

Pérdidas financieras:

- Costo de la recuperación de datos
- Pago de un rescate a los ciberdelincuentes
- Pérdida de ingresos por la interrupción del servicio

Daños a la reputación:

- Pérdida de confianza de los clientes o usuarios
- Daño a la imagen de la organización
- Dificultad para atraer y retener talento

Afectación al servicio:

- Interrupción del acceso a la información
- Disminución de la productividad
- Insatisfacción de los clientes o usuarios.

2. ***Autoevaluación de la efectividad de los controles****.*

De acuerdo con la respuesta de líder del proceso en el monitoreo de primera línea de defensa existe evidencia de que el control está siendo utilizado al realizar actividades relacionadas con: Solicitud de usuarios a través de la mesa de ayuda, Mejoras al aplicativo Oracle, Respaldos de información, Compromiso de uso de recursos informáticos.

Al revisar las evidencias SDP-2024-4316, SDP-2024-4317, SDP-2024-4318, SDP-2024-4319, no se encontraron registros que indiquen que el control está siendo implementado de manera efectiva. Se recomienda disponer para los próximos monitoreos las evidencias en Drive de tal forma que se pueda corroborar y mantener el soporte de lo reportado en el monitoreo.

Con base en la respuesta del líder de proceso se puede deducir que:

En los controles establecidos para el Riesgo 1 se están realizando verificaciones de los mecanismos de identificación y autenticación y la revisión de la configuración de los parámetros de seguridad del sistema y el servicio que Oracle presta internamente, lo que ayuda a prevenir el acceso no autorizado al sistema y la pérdida de confidencialidad de la información.

Para el caso del Riesgo 2 se realiza copias de seguridad de la información de forma regular, lo que ayuda a proteger la información en caso de pérdida o corrupción.

En la aplicación de los controles para el Riesgo 3, se están realizando mejoras periódicas al aplicativo, lo que ayuda a reducir la posibilidad de fallas del sistema y la pérdida de disponibilidad de la información.

En el caso del Riesgo 4, se están controlando los accesos al sistema, lo que ayuda a prevenir la pérdida de confidencialidad de la información por accesos no autorizados o por un mal uso de los recursos.

De acuerdo con la información suministrada por el proceso y dado que no se evidenció informes de auditoría asociadas a los controles, no hay hallazgos de auditoría.

Se destaca la efectividad de los controles implementados, la falta de hallazgos de auditoría y su contribución a la mitigación de

los riesgos identificados en el proceso de producción, análisis y divulgación de la información.

3. ***Autoevaluación de la eficacia de las acciones:***

El proceso no formuló un plan de acción, sin embargo las acciones establecidas para operacionalizar los controles son adecuadas para reducir la probabilidad de ocurrencia o el impacto del riesgo y permiten prevenir el acceso no autorizado al sistema, la pérdida de confidencialidad de la información, identificar y corregir errores que podrían causar fallas del sistema y la pérdida de disponibilidad de la información, proteger la información en caso de pérdida o corrupción y ayuda a prevenir la pérdida de confidencialidad de la información por accesos no autorizados o por un mal uso de los recursos.

Las acciones identificadas en el proceso comprenden la verificación periódica de los mecanismos de identificación y autenticación, pruebas periódicas al aplicativo y corrección de errores identificados, copias de seguridad de la información de forma regular y la implementación de los accesos al sistema las cuales se vienen efectuando adecuadamente de acuerdo con el reporte presentado por el proceso.

La Segunda Línea de Defensa concluye que, hasta la fecha, ninguno de los cuatro riesgos identificados en el proceso M-CA-003 PRODUCCIÓN, ANÁLISIS Y DIVULGACIÓN DE LA INFORMACIÓN se ha materializado ni se ha determinado como hallazgo de auditoría interna o externa.

Dado que no ha habido materialización de los riesgos, no es pertinente evaluar la existencia de acciones correctivas.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

Con base a la evidencia disponible, se concluye que la gestión del riesgo en el proceso M-CA-003 PRODUCCIÓN, ANÁLISIS Y DIVULGACIÓN DE LA INFORMACIÓN ha sido efectiva en la prevención de eventos adversos que podrían haber impactado negativamente los objetivos y compromisos del proceso, ha sido útil en la mitigación de los riesgos y en reducir la probabilidad de ocurrencia o su impacto en caso de que se materialicen y ha contribuido a evitar situaciones o hechos que podrían haber afectado el cumplimiento de los objetivos y compromisos.

5. ***Actualización de Riesgos****:*

La Segunda Línea de Defensa coincide con la respuesta de Primera Línea en que, en este momento no hay evidencia que sugiera la necesidad de modificar y/o actualizar los riesgos establecidos en el proceso M-CA-003 o de documentar y gestionar nuevos riesgos. Sin embargo, es importante resaltar que la gestión de riesgos es un proceso continuo que debe adaptarse a los cambios en el entorno.

La Segunda Línea se concluye que, en este momento, no hay evidencia que sugiera la necesidad de documentar y gestionar nuevos riesgos. Sin embargo, se recomienda continuar monitoreando el contexto estratégico, los resultados de las auditorías y otros aspectos relevantes para la gestión de riesgos, y realizar evaluaciones periódicas de la necesidad de actualizar los riesgos.

3.3.3.2 ALERTAS:

De acuerdo con el monitoreo de primera línea de defensa referente a los riesgos identificados de seguridad de la información del Proceso Producción, Análisis y Divulgación de la Información, no se reportan alertas que indiquen que los riesgos se han materializado

3.3.3.3 RECOMENDACIONES:

Se recomienda continuar monitoreando el contexto estratégico, los resultados de las auditorías y otros aspectos relevantes para la gestión de riesgos.

Realizar evaluaciones periódicas de los riesgos para identificar cualquier cambio en su probabilidad o impacto.

Si bien durante el ejercicio de identificación y gestión de riesgos de seguridad de la información no se establecieron acciones complementarias a los controles ya existentes, es necesario continuar con el mejoramiento continuo del diseño y aplicación de los controles para gestionar los riesgos de seguridad de la información. Es preciso recomendar que en el próximo monitoreo el proceso aporte observaciones pertinentes que evidencien la ejecución de los controles o el seguimiento a los mismos.

Se recomienda revisar los cambios derivados de la entrada en vigor del Decreto 432 de 2022 y realizar un análisis del contexto estratégico, la coherencia entre el riesgo y los objetivos, las causas y las consecuencias del riesgo para verificar que la definición del riesgo es adecuada al contexto actual de la entidad.

Por último, aunque todos los riesgos definidos por el proceso están enfocados al tipo de activos Software, es necesario que se evalué si se requiere una identificación de riesgos asociados a los demás activos; además de incorporar controles de seguimiento, revisión y depuración por parte del proceso.

Se recomienda asistir a las sesiones de capacitación, socialización y sensibilización sobre temas de seguridad privacidad de la información y privacidad de la información programadas por la entidad.

4 PROCESOS DE APOYO

4.1 ADMINISTRACIÓN DEL TALENTO HUMANO

4.1.1 A-LE-306 MAPA DE RIESGOS DE GESTIÓN DEL PROCESO ADMINISTRACIÓN DEL TALENTO HUMANO VERSIÓN 10 ACTA DE MEJORAMIENTO 78 DE FEBRERO 07 DE 2024

Riesgos de Gestión

1. Posibilidad de afectación económica y reputacional por incumplimiento de la ejecución de los programas de bienestar, capacitación, seguridad y salud en el trabajo, debido a inadecuada identificación de las necesidades de los planes y programas por parte de los procesos, fuga de conocimiento por movimientos de personal, cambios en la normatividad, falta de participación en las actividades y/o situaciones fortuitas (eventos socio naturales), que no permitan realizar una adecuada gestión del talento humano.

2. Posibilidad de afectación económica y reputacional por errores e inconsistencias en la liquidación de la nómina, debido a parametrización del sistema para la liquidación de la nómina, flexibilización en los tiempos establecidos para radicar las novedades del mes, recepción de novedades por canales diferentes al establecido (SIPA) y cultura institucional para atender y cumplir las circulares emitidas por la Dirección de Talento Humano.

3. Posibilidad de afectación reputacional por pérdida o extravío de las historias laborales o de los documentos que reposan en las mismas, debido a insuficiencia de recursos tecnológicos apropiados para el adecuado desarrollo de las actividades archivísticas, inadecuada aplicación de las normas, procesos y procedimientos que generan demandas o investigaciones y recursos económicos limitados para desarrollar los planes a cargo del proceso.

4.1.1.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias***.

   Mediante radicado en SIPA 3-2024-16251 del 6 de mayo de 2024 el proceso Administración del Talento Humano remitió a la Dirección de Planeación Institucional el monitoreo de primera línea de defensa a los riesgos de gestión asociados al mismo.

   El proceso realizó la actualización del mapa de riesgos de gestión (versión 10 el 7 de febrero de 2024 mediante acta de mejoramiento Nº78, en la cual se realizó el ajuste en la redacción de controles y de algunos aspectos del contexto como los procedimientos asociados.

   Por su parte, el contexto estratégico se mantiene desde la implementación del rediseño en la vigencia 2022.

   Los riesgos de gestión guardan coherencia con los dos objetivos estratégicos a los cuales le aporta el proceso "Fortalecer la estructura y la cultura institucional para contribuir a una gestión pública efectiva, mediante el desarrollo de habilidades para el talento humano, simplificación de procesos, mecanismos eficientes para la toma de decisiones y mejora continua" y "Desarrollar e implementar una estrategia

de gestión del conocimiento e innovación interna que permita retener experiencias y fomentar nuevas formas de trabajo y soluciones innovadoras en la entidad además, de apoyar la formulación de la política de CTi en el Distrito", teniendo en cuenta que los riesgos están orientados a la ejecución de los programas de bienestar, capacitación, Seguridad y Salud en el Trabajo, liquidación de nómina y gestión de las historias laborales.

Teniendo en cuenta que el propósito del proceso se asocia a la administración del Talento Humano en el marco del ingreso, desarrollo y retiro de los servidores en la entidad, se observa que los riesgos de gestión son coherentes con este objetivo, toda vez que están definidos para aquellas actividades que enmarcan la gestión del talento humano.

De acuerdo con el análisis efectuado por la primera línea de defensa, se puede concluir que las causas y consecuencias identificadas inicialmente para los riesgos se mantienen.

La segunda línea de defensa recomienda para el segundo cuatrimestre de la presente vigencia, considerar la inclusión de riesgos asociados a Gestión del Conocimiento y la Innovación, en conjunto con la Dirección de Planeación Institucional, Oficina de Laboratorio de Ciudad y Dirección de Tecnologías de la Información y las Comunicaciones .

2. ***Autoevaluación de la efectividad de los controles****.*

La segunda línea de defensa reitera la recomendación de realizar el monitoreo de primera línea de defensa relacionado con la efectividad de los controles de forma más precisa para cada uno de ellos, así como para cada uno de los riesgos, indicando las evidencias que den cuenta de la aplicación de dichos controles y de la forma como estos han aportado a la mitigación de los riesgos.

Lo anterior, fortalecerá la gestión del riesgo realizada por el proceso y, a su vez, facilitará el ejercicio de la segunda y tercera línea de defensa para corroborar la efectividad de los controles.

En atención a lo aportado por la primera línea de defensa, se infiere que los controles previenen o mitigan los riesgos de gestión, razón por la cual estos se mantienen para fortalecer la adecuada administración del talento humano de la entidad.

No se encuentra información correspondiente a hallazgos de auditorías o evidencias resultantes de auditorías de que el proceso no esté cumpliendo con los controles establecidos o no se estén implementando de acuerdo con lo planificado.

La segunda línea de defensa recomienda tener en cuenta las situaciones de mejora consignadas en el Informe de Seguimiento a la austeridad del gasto del cuarto trimestre de 2023 elaborado por la OCI con radicado 3-2024-12272 del 27 de marzo de 2024, en el cual quedó consignada una situación de mejora compartida con la Dirección Administrativa relacionadas con las debilidades en los reportes de control que soportan los pagos de horas extras.

3. ***Autoevaluación de la eficacia de las acciones:***

Teniendo en cuenta que los riesgos se encuentran en zona residual moderada, no fue necesario formular plan de acción como herramienta para el tratamiento del riesgo, toda vez que con los controles es

suficiente para mitigar la ocurrencia de los mismos.

No se evidencia materialización de riesgos en el periodo objeto de monitoreo.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

   La información reportada por la primera línea de defensa y las evidencias de la aplicación efectiva de los controles formulados para los riesgos, permiten concluir que la gestión del riesgo ha sido adecuada y útil para evitar situaciones indeseables que afecten el cumplimiento de los objetivos y compromisos a cargo del proceso.

5. ***Actualización de Riesgos****:*

   Para el periodo del monitoreo, no se identificó la necesidad de modificar o actualizar los riesgos de gestión, ni tampoco la necesidad de documentar o gestionar nuevos riesgos de este tipo. Sin embargo, para el segundo cuatrimestre del año, desde la Dirección de Planeación Institucional se agendarán jornadas virtuales con los procesos para la revisión de indicadores y mapas de riesgos de conformidad con el nuevo mapa de procesos de la entidad e implementación del nuevo software para el Sistema de Gestión.

   Es importante mencionar que el Departamento Administrativo de la Función Pública - DAFP publicó en noviembre de 2022 la versión 6 de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, la cual contiene un nuevo capítulo para el análisis de riesgos fiscales cuya finalidad es prevenir el daño al patrimonio público, representando en el menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos o a los intereses patrimoniales del Estado. Por tal razón, la Dirección de Planeación Institucional se encuentra adelantando lo pertinente para definir la hoja de ruta que permita su incorporación a los actuales mapas de riesgos de la entidad, con el acompañamiento de las dependencias correspondientes dada la naturaleza de este tipo de riesgos.

4.1.1.2 ALERTAS:

Para el periodo de monitoreo no se generan alertas para el proceso.

4.1.1.3 RECOMENDACIONES:

La segunda línea de defensa reitera la recomendación de realizar el monitoreo de primera línea de forma más precisa para cada uno de los controles de cada riesgo identificado, con el fin de verificar su efectividad, indicando las evidencias que den cuenta de la aplicación de dichos controles y de la forma como estos han aportado a la mitigación de los riesgos.

Lo anterior, fortalecerá la gestión del riesgo realizada por el proceso y, a su vez, facilitará el ejercicio de la segunda y tercera línea de defensa para corroborar la efectividad de los controles.

Para el segundo cuatrimestre de la presente vigencia, revisar los riesgos de gestión, de conformidad con el nuevo mapa de procesos de la entidad e implementación de la nueva herramienta tecnológica para el Sistema de Gestión denominada Gestiónate – Isolucion.

Igualmente, la segunda línea de defensa recomienda para el segundo cuatrimestre de la presente vigencia, considerar la inclusión de riesgos asociados a Gestión del Conocimiento y la Innovación, en conjunto con la Dirección de Planeación

Institucional, Oficina de Laboratorio de Ciudad y Dirección de Tecnologías de la Información y las Comunicaciones .

4.1.2 A-LE-519 MAPA DE RIESGOS DE CORRUPCIÓN DEL PROCESO ADMINISTRACIÓN DEL TALENTO HUMANO VERSIÓN 3 ACTA DE MEJORAMIENTO 71 DE ENERO 31 DE 2024

Riesgos de Corrupción
1. Manipulación dolosa de los registros y/o documentos de los procedimientos a cargo de la Dirección de Talento Humano para favorecer los intereses propios o de terceros.

4.1.2.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias***.

   Mediante radicado en SIPA 3-2024-16251 del 6 de mayo de 2024 el proceso Administración del Talento Humano remitió a la Dirección de Planeación Institucional el monitoreo de primera línea de defensa a los riesgos de corrupción asociados al mismo.

   El proceso realizó la actualización del mapa de riesgos de corrupción (versión 3) el 31 de enero de 2024 mediante acta de mejoramiento Nº71, en la cual se realizó el ajuste en la redacción de controles y de algunos aspectos del contexto como los procedimientos asociados.

   El riesgo de corrupción guarda coherencia con los dos objetivos estratégicos a los cuales le aporta el proceso "Fortalecer la estructura y la cultura institucional para contribuir a una gestión pública efectiva, mediante el desarrollo de habilidades para el talento humano, simplificación de procesos, mecanismos eficientes para la toma de decisiones y mejora continua" y "Desarrollar e implementar una estrategia de gestión del conocimiento e innovación interna que permita retener experiencias y fomentar nuevas formas de trabajo y soluciones innovadoras en la entidad además, de apoyar la formulación de la política de CTi en el Distrito", teniendo en cuenta que el riesgo está orientado al uso inadecuado de los documentos del proceso.

   Por su parte, el contexto estratégico se mantiene desde la implementación del rediseño en la vigencia 2022.

   Teniendo en cuenta que el propósito del proceso se dirige a la administración del Talento Humano en el marco del ingreso, desarrollo y retiro de los servidores en la entidad, se observa que el riesgo de corrupción es coherente con este objetivo, teniendo en cuenta el manejo especial que se otorga a las historias laborales y al manejo y control de los demás documentos del proceso.

   El análisis efectuado por la primera línea de defensa permite concluir que las causas y consecuencias identificadas inicialmente para el riesgo se mantienen.

   Durante la normal operación del proceso no se han evidenciado alertas de nuevas causas y/o consecuencias que puedan incidir en el análisis del riesgo de corrupción.

2. ***Autoevaluación de la efectividad de los controles***.

   Como segunda línea de defensa se reitera la recomendación de realizar el análisis de la efectividad de los controles de forma más detallada, indicado las evidencias de su cumplimiento para cada uno de los 6 controles y la forma como estos han aportado a la mitigación del riesgo.

   Lo anterior, fortalecerá la gestión del riesgo realizada por el proceso y, a su vez, facilitará el ejercicio de la segunda y

tercera línea de defensa para corroborar la efectividad de los controles.

En atención a lo aportado por la primera línea de defensa, se infiere que los siete (7) controles previenen o mitigan el riesgo de corrupción, razón por la cual estos se mantienen para prevenir la manipulación dolosa de los documentos para beneficio propio o de terceros.

No se encuentra información correspondiente a hallazgos de auditorías o evidencias resultantes de auditorías de que el proceso no esté cumpliendo con los controles establecidos o no se estén implementando de acuerdo con lo planificado.

3. ***Autoevaluación de la eficacia de las acciones:***

   Las acciones formuladas por el proceso en el plan de tratamiento del riesgo asociadas a la pérdida de información, expedientes y otros documentos del proceso, derogatoria de nombramientos aún no se han implementado por cuanto estas situaciones no se presentaron en el periodo objeto de monitoreo.

   Por su parte, la acción asociada con informar al personal retirado a cerca de la resolución de prestaciones, no cuenta con la evidencia en el repositorio. Se recomienda para el siguiente monitoreo, subir la evidencia y registrar el código de esta en el campo de avance de la sección "tratamiento del riesgo "en el mapa de riesgos y en esta sección del monitoreo.

   Lo anterior, se encuentra consignado en el mapa de riesgos del proceso- sección tratamiento del riesgo, el cual hace parte integral del monitoreo.

   En el periodo objeto del monitoreo no hay indicios de la materialización de riesgos de corrupción ni hallazgos en las auditorías internas o externas relacionados con estos riesgos.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

   La información reportada por la primera línea de defensa y las evidencias de la aplicación efectiva de los controles formulados para el riesgo de corrupción, permiten concluir que su gestión ha sido adecuada y útil para evitar situaciones indeseables que afecten el cumplimiento de los objetivos y compromisos a cargo del proceso.

   Desde la segunda línea de defensa se recomienda reforzar la gestión del riesgo con la realización de jornadas de sensibilización a los servidores del proceso en aspectos como transparencia, ética e integridad en la gestión pública.

5. ***Actualización de Riesgos****:*

   En el periodo de monitoreo, no se identificó la necesidad de modificar y/o actualizar el riesgo actual o documentar nuevos riesgos, teniendo en cuenta que no se evidencian cambios sustanciales en el contexto estratégico ni resultados de auditorías que lo ameriten.

4.1.2.2 ALERTAS:

Para el periodo de monitoreo no se generan alertas para el proceso.

4.1.2.3 RECOMENDACIONES:

La segunda línea de defensa reitera la recomendación de realizar el monitoreo de primera línea de forma más precisa para cada uno de los controles de cada

riesgo identificado, con el fin de verificar su efectividad, indicando las evidencias que den cuenta de la aplicación de dichos controles y de la forma como estos han aportado a la mitigación de los riesgos.

Lo anterior, fortalecerá la gestión del riesgo realizada por el proceso y, a su vez, facilitará el ejercicio de la segunda y tercera línea de defensa para corroborar la efectividad de los controles.

Para el segundo cuatrimestre de la presente vigencia, revisar los riesgos de gestión, de conformidad con el nuevo mapa de procesos de la entidad e implementación de la nueva herramienta tecnológica para el Sistema de Gestión denominada Gestiónate – Isolucion.

4.1.3 A-LE-518 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DEL PROCESO ADMINISTRACIÓN DEL TALENTO HUMANO VERSIÓN 2 ACTA DE MEJORAMIENTO 109 DE FEBRERO 26 DE 2024

Riesgo de Seguridad de la Información

1. Posibilidad de Pérdida de Confidencialidad por fallas humanas, divulgación ilegal de la información de las historias laborales debido a manejo manual de la información y copias no controladas

2. Posibilidad de Pérdida de Disponibilidad por mal funcionamiento del software, fallas del equipo, fallas humanas, error en el uso o abuso de derechos y privilegios, falsificación de derechos de acceso; de los registros que se generan o se ingresan con ocasión de las actividades(Nómina, Seguridad Social, Capacitación, Bienestar, Seguridad y Salud en el Trabajo, EDL) a cargo de la Dirección, debido a retraso en la salida de información de los sistemas, desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información o errores u omisiones en el registro de los datos e información que se gestiona diariamente.
.

4.1.3.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias***.

La Segunda Línea de Defensa coincide con la respuesta de Primera Línea en que el contexto estratégico identificado por el proceso se mantiene. La Dirección de Talento Humano sigue siendo la responsable de la administración de la información del talento humano de la SDP, y el riesgo definido sigue teniendo relación con las acciones que desarrolla el área para cumplir con el objetivo misional establecido. Sin embargo, es importante considerar que a mediados de 2024 la entidad estará formalizando la nueva plataforma tecnológica y los mapas de procesos. Este cambio podría afectar el contexto estratégico del proceso y, por lo tanto, la definición del riesgo, sus causas y consecuencias.

La Segunda Línea de Defensa determinó que los riesgos identificados siguen siendo coherente con los objetivos estratégicos. La Dirección de Talento Humano, como responsable de la información para liquidar y ordenar el pago de la nómina, la información de los planes, programas y proyectos para el desarrollo personal, así como de la administración de las historias laborales de los servidores de la SDP, debe velar por la seguridad de la información para la adecuada toma de decisiones por parte de la alta dirección. Los riesgos definidos se relacionan precisamente con la pérdida de la confidencialidad de la información y la perdida de disponibilidad del software aplicaciones que utiliza para cumplir con este objetivo.

De acuerdo con la información disponible, la Segunda Línea de Defensa concluyó que el riesgo identificado sigue siendo coherente con el objetivo del proceso. Las actividades que desarrolla el área en cumplimiento del POA se encuentran enmarcadas en los planes y documentos de todas las situaciones administrativas en que se ve incurso un servidor público durante su permanencia en el cargo. Los riesgos definidos se relacionan con el cumplimiento del objetivo del proceso, ya que el uso inadecuado del software o la falta de control en las historias laborales podrían afectar la toma de decisiones oportunas y el cumplimiento del objetivo misional.

El uso inadecuado del software y la falta de controles en las historias laborales siguen siendo factores que pueden afectar a la entidad. La información de los servidores podría ser filtrada y utilizada en su contra, lo que afectaría el cumplimiento del objetivo misional. Además, si las historias laborales no se actualizan adecuadamente, no se podrían tomar decisiones oportunas, por lo tanto, las causas identificadas se mantienen.

En general, se puede afirmar que las consecuencias identificadas inicialmente para el riesgo se mantienen, pero han sido mitigadas en cierta medida gracias a la implementación de controles y las acciones definidas en los planes de acción. Sin embargo, es importante mantener una vigilancia constante y actualizar las medidas de prevención y protección en función de los cambios en el entorno.

El impacto en la reputación de la entidad por pérdida de confidencialidad o disponibilidad de información sensible sigue siendo significativo. No obstante, la implementación de las medidas de control como la obligación que tiene todos los servidores y servidoras que se vinculen al proceso de asistir y participar activamente en las capacitaciones que sean programadas por la entidad y el diligenciamiento de los formatos A-FO-205 (Inducción en el puesto de trabajo) y el formato de asistencia (A-FO 183), ha contribuido a mitigar los riesgos, reduciendo la probabilidad de ocurrencia y la severidad del impacto.

Las posibles sanciones económicas por incumplimiento de normativas de protección de datos o por fallas en los sistemas de información podrían generar un impacto financiero considerable. La implementación de controles como la realización de copias de seguridad y la capacitación del personal ha contribuido a reducir la probabilidad de este tipo de eventos.

Las demandas por parte de personas afectadas por la pérdida o divulgación indebida de su información personal podrían generar costos legales significativos. La implementación de medidas como el control de acceso a la información y la sensibilización del personal en materia de protección de datos han sido fundamentales para reducir la probabilidad de este tipo de demandas.

Las interrupciones en el servicio debido a fallas en los sistemas de información podrían afectar la productividad y generar costos adicionales. La implementación de controles como la solicitud de restauración de la copia de respaldo del mes anterior para procesar la nómina del mes siguiente, contribuye de manera importante a reducir la probabilidad y el impacto de este tipo de eventos.

2. ***Autoevaluación de la efectividad de los controles****.*

Se evidencia controles en el proceso de vinculación de los servidores que hacen parte del proceso mediante el diligenciamiento del Formato A_FO 205 (Inducción en el puesto de trabajo) y el formato de asistencia (A-FO 183). Así mismo, existen controles como lo son los siguientes:

Los servidores que forman parte del proceso están en la obligación de guardar y verificar la información que gestiona diariamente en carpetas compartida y registra en la hoja de control (A-FO 258 Bitácora Solicitud Cuentas de Usuario), no está autorizado realizar copias no contraladas en diferentes medios removibles, el formato A-FO-227, para la solicitud o eliminación en los accesos a los sistemas de información mediante el diligenciamiento del formato A-FO-010 y para los retirados reporta en el A-FO-128. La efectividad del control se sustenta en el hecho que estos formatos permiten un mejor seguimiento y control de las historias laborales, minimizando el riesgo de pérdida o extravío.

De acuerdo con lo anterior, la Segunda Línea de Defensa verificó que existe evidencia de que el control está siendo utilizado. La Dirección de Talento Humano lleva registros de las actividades que desarrolla, hace seguimiento a las novedades en la liquidación de la nómina, solicita copias de seguridad, diligencia formatos para requerimientos, actualiza la información en las historias laborales y publica información de actos administrativos en la página web de la entidad. Sin embargo, es importante analizar la calidad y la suficiencia de los registros disponibles dado que como evidencia se aporta la descripción de la actividad de "MANTENER EN 2024 EN 93.88 % LA PERCEPCIÓN POSITIVA DE LOS SERVIDORES DE LA SDP CON LOS PROGRAMAS Y PLANES QUE DESARROLLA LA DTH A PARTIR DE LA LINEA BASE OBTENIDA EN LA ENCUESTA DE PERCEPCIÓN DEL 2023 Actos Administrativos" pero no se aporta registros. Se recomienda verificar que los registros sean completos, precisos y confiables, y que permitan demostrar efectivamente la aplicación del control.

En el monitoreo de Segunda Línea de Defensa, se realizó la revisión de los controles establecidos en la matriz de riesgos así:

Para el Riesgo 1: Posibilidad de Pérdida de Confidencialidad por fallas humanas, divulgación ilegal de la información de las historias laborales debido a manejo manual de la información y copias no controladas, se establecieron dos controles:

Control 1: Capacitación a los servidores sobre el manejo de la información confidencial y la importancia de seguir los procedimientos establecidos para la gestión de las historias laborales, mediante el cual se reduce la probabilidad de que los servidores cometan errores que puedan comprometer la confidencialidad de la información. En aplicación del control se mitiga el riesgo dado que en caso de que se produzca un error, la capacitación puede ayudar a que el servidor tome medidas oportunas para minimizar el impacto de este.

Control 2: Verificar la información que gestiona diariamente en la carpeta compartida que la Dirección de Tecnologías de la Información y las Comunicaciones habilitó para tal fin, restringiendo el acceso solo al personal autorizado. Este control previene y reduce la probabilidad de divulgación no autorizada al limitar el número de personas que pueden acceder a la información sensible. Así mismo, en caso de que un usuario no autorizado acceda a la información, el sistema de control de acceso puede facilitar su identificación y la toma de medidas correctivas.

En el caso del Riesgo 2: “Posibilidad de Pérdida de Disponibilidad por mal funcionamiento del software, fallas del equipo, fallas humanas, error en el uso o abuso de derechos y privilegios, falsificación de derechos de acceso; de los registros que se generan o se ingresan con ocasión de las actividades(Nómina, Seguridad Social, Capacitación, Bienestar, Seguridad y Salud en el Trabajo, EDL) a cargo de la Dirección, debido a retraso en la salida de información de los sistemas, desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información o errores u omisiones en el registro de los datos e información que se gestiona diariamente.”, se formuló seis controles:

Control 1: Realización de copias de seguridad periódicas. ayuda a prevenir la pérdida de datos en caso de un mal funcionamiento del software o fallas del equipo. Por medio de este control se propende porque la información esté disponible incluso en caso de que se produzca un fallo en el sistema o un error humano mitigando el impacto al permitir restaurar la información en caso de que se pierda o se corrompa.

Para el fortaleciendo de los controles se formularon dos planes de trabajo:

- Programar una actividad semestral de sensibilización para el manejo de la información y participar activamente en las capacitaciones que sobre el tema programe la DRF y GD pag. 23 tabla 6 política. (No se evidencia el avance del plan)

- Coordinar la programación y participación semestralmente de una Actividad de sensibilización para el control de la información que reposa en la carpeta compartida desde seguridad de la información (No se evidencia el avance del plan)

Control 2: Registro de proyectos de actos administrativos en SIPA. El registro de proyectos de actos administrativos en SIPA ayudará a garantizar que los documentos definitivos queden registrados en el repositorio de SIPA.

Control 3: Control del desarrollo de aplicaciones o módulos para registrar información de actividades. El control del desarrollo de aplicaciones o módulos para registrar información de actividades ayudará a garantizar que las aplicaciones sean seguras y confiables.

Control 4: Control de accesos a los sistemas de información. El control de accesos a los sistemas de información previene el ingreso de ingreso de personal no autorizado mitigando el resigo por error en el uso o abuso de derechos y privilegios y la confidencialidad de la información.

Control 5: Control de accesos a los sistemas de información de acceso privilegiado. Con la implementación de este control se busca que solo personal autorizado tenga privilegios para hacer actualizaciones o modificaciones sobre las configuraciones del software.

Control 6: Actualización de las políticas de seguridad y privacidad de la información ayuda a prevenir el acceso no autorizado a los datos y a garantizar que los empleados estén informados sobre las últimas prácticas de seguridad.

Para el fortaleciendo de los controles se formuló un plan de trabajo:

Solicitar restauración de la copia de respaldo del mes anterior para procesar la nómina del mes siguiente; se almacena la información en Excel mientras la Dirección de Tecnologías de la Información y las Comunicaciones hace el desarrollo y lo pone en producción; se debe validar la restricción de acceso no autorizado con Dirección Administrativa y de Tecnologías de la Información y las Comunicaciones; modificar A IN 019; para control de los actos administrativos que se remiten para firma de la SGI, crear un drive donde los servidores que proyectan resoluciones registren los campos de número de radicado en SIPA, Epígrafe, nombre de quien proyectó, número de resolución y la fecha de emisión, el cual se controlará semanalmente por parte de la persona asignada por la Dirección de Talento Humano para su control; en la evaluación del desempeño se requiere cumplimiento de los términos establecidos, en caso de fallas solicitar copia del registro manual como soporte al posterior registro; para la información de los certificados para bono pensional contemplar la posibilidad de escanear las historias laborales de exservidores.

Se recomienda hacer un análisis del plan dado que en la formulación se incluyeron actividades en una actividad de control, se sugiere dividir los tema en diferentes actividades de control cómo, por ejemplo:

Solicitar restauración de la copia de respaldo del mes anterior:

Se contactará a la Dirección de Tecnologías de la Información y las Comunicaciones para solicitar la restauración de la copia de seguridad del mes anterior.

Validar la restricción de acceso no autorizado: Se coordinará con la Dirección Administrativa y la Dirección de Tecnologías de la Información y las Comunicaciones para verificar la restricción de acceso no autorizado al sistema de nómina.

Modificar A IN 019: Se realizarán las modificaciones necesarias al formulario A IN 019 para adaptarlo a la nueva solución de nómina.

Control de actos administrativos: Se creará un Drive compartido donde los servidores que proyectan resoluciones registrarán la información y La información será revisada semanalmente por la persona asignada por la Dirección de Talento Humano.

Evaluación del desempeño: Se considerará el cumplimiento de los términos establecidos para el registro de la información en la evaluación del desempeño.
En caso de fallas, se solicitará una copia del registro manual como soporte para el posterior registro.

Certificados para bono pensional: Se evaluará la posibilidad de escanear las historias laborales de exservidores para obtener la información necesaria para los certificados de bono pensional.
De acuerdo con el análisis anterior, al aplicar los controles sobre las acciones desarrolladas, la Dirección de Talento Humano (DTH) puede identificar situaciones que podrían generar riesgos y tomar decisiones oportunas para prevenirlos o mitigarlos.

La Segunda Línea de Defensa de acuerdo con la respuesta de la Primera línea de defensa y con la información reportada en la matriz de riesgos deduce que no se identificó hallazgos de auditoría asociados al control por parte de la Oficina de Control Interno (OCI) ni auditorías externas.

Las acciones formuladas en los planes son coherentes con los riesgos identificados y tienen un enfoque hacia la mitigación de los dos riesgos identificados.

3. ***Autoevaluación de la eficacia de las acciones:***

Las acciones formuladas para dar tratamiento al riesgo están parcialmente orientadas a contrarrestar sus causas según el análisis realizado en la Segunda línea de Defensa:

En las acciones formuladas para el tratamiento para el Riesgo 1, se identificó que el mal manejo de la información por parte de los funcionarios puede deberse a diferentes factores, como la falta de conocimiento sobre las políticas de seguridad de la información, la negligencia o la falta de recursos para implementar medidas de control adecuadas, en este sentido, una vez revisado el plan de acción para el Riesgo 1. se observó que las dos actividades propuestas en el plan de acción (sensibilización y control de la información en la carpeta compartida) se enfocan en dos de las posibles causas raíz del riesgo: la falta de conocimiento y la necesidad de mejorar los controles sobre la información confidencial. Sin embargo, el plan de acción no aborda otras causas potenciales, como la negligencia o la falta de recursos ni establece los mecanismos de seguimiento específicos por cada actividad. Se recomienda realizar un análisis más profundo de las causas raíz del riesgo para identificar si se requieren acciones adicionales y definir cómo se realizará el seguimiento.

De otra parte, las acciones establecidas en el tratamiento para el Riesgo 2 relacionadas con el riesgo de pérdida de disponibilidad por mal funcionamiento del software, fallas del

equipo, errores humanos, etc. se origina en una combinación de factores técnicos como:

Problemas con el software, hardware o infraestructura del sistema de información, factores humanos relacionados con errores o negligencia por parte de los usuarios o administradores del sistema, factores organizacionales por falta de políticas y procedimientos adecuados para la gestión de la información, y falta de capacitación del personal o deficiencias en los controles de seguridad. En el análisis del plan de acción se identificó que aborda algunas de las causas raíz del riesgo, como la restauración de copias de seguridad, el control de acceso no autorizado y la mejora del control de los actos administrativos. Sin embargo, el plan de acción no profundiza en el análisis de las causas técnicas y organizacionales del riesgo. Se recomienda realizar un análisis más detallado de estas causas para identificar acciones preventivas más efectivas.

Si bien la Primera Línea de Defensa indica que las acciones se han implementado adecuadamente, la Segunda Línea de Defensa recomienda realizar una evaluación más profunda del proceso de implementación, considerando el siguiente aspecto:

En los planes de acción se identifican responsables claros (Las actividades se asignan al Director - Profesional responsable del tema de la DTH, con la colaboración de la Dirección Administrativa y la Dirección de Tecnologías de la Información y las Comunicaciones (DTIC)), fecha de seguimiento y reporte periódico del estado. Además, se menciona la inclusión de las actividades en el POA. No obstante, no se identifican indicadores claros para el seguimiento.

Teniendo en cuenta la declaración en el contexto del proceso y en el monitoreo de Primera línea de defensa realizado por el líder del proceso sobre la ausencia de hallazgos de auditoría, no se han presentado eventos relevantes en el contexto del proceso que puedan indicar la materialización de los Riesgos.

Basando en la afirmación del líder del proceso en el sentido que, no se han materializado los riesgos identificados, se concluye que desde el proceso no se requiere formular acciones correctivas para dar tratamiento al riesgo.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

Si bien la información proporcionada por la Primera Línea de Defensa indica que la gestión de riesgos ha permitido mantener un control con los monitoreos y advertir en caso de que sea necesario establecer medidas de contingencia, no se dispone de evidencia concluyente que demuestre de manera fehaciente que la gestión del riesgo haya evitado de forma concreta situaciones o hechos que afecten el cumplimiento de los objetivos y compromisos del proceso A-CA-005 "ADMINISTRACIÓN DEL TALENTO HUMANO".

De acuerdo con lo informado desde el proceso, si se materializa el Riesgo 1: Posibilidad de Pérdida de Confidencialidad, podría afectar el cumplimiento de objetivos como la retención del talento humano, la reputación de la entidad y el cumplimiento de las normas legales y regulatorias. La gestión de este riesgo, a través de la implementación de controles como capacitaciones y control de accesos, contribuye a mitigar estas potenciales afectaciones y facilita el cumplimiento de los compromisos de la Dirección de Talento Humano - DTH.

Así mismo, si se materializa Riesgo 2: Posibilidad de Pérdida de Disponibilidad, podría afectar el cumplimiento de objetivos como la oportuna prestación de servicios a los servidores y servidoras de la entidad, la eficiencia de los procesos administrativos y la

continuidad del negocio. La gestión de este riesgo, a través de la implementación de controles como copias de seguridad, Control de actos administrativos, verificación del cumplimiento de los términos establecidos para el registro de la información en la evaluación del desempeño, la evaluación de la posibilidad de escanear las historias laborales de exservidores, contribuye a mitigar estas potenciales afectaciones y facilita el cumplimiento de los compromisos de la DTH.

5. ***Actualización de Riesgos**:*

Con base a la información disponible, la Segunda Línea de Defensa considera que no es necesario modificar ni actualizar los riesgos identificados en el proceso A-CA-005 en este momento lo cual se fundamenta en lo siguiente:

- El análisis realizado por la Primera Línea de Defensa para cada riesgo sigue siendo válido en el contexto actual. Se ha identificado la causa raíz de los riesgos y se han considerado los factores que podrían afectar su probabilidad de ocurrencia o impacto potencial.

- La valoración de los riesgos realizada por la Primera Línea de Defensa es coherente con el análisis realizado y sigue siendo válida en el contexto actual. Se ha considerado la efectividad de los controles implementados para mitigar cada riesgo, y se ha ubicado cada riesgo en la zona de riesgo correspondiente.

- Las acciones definidas por la Primera Línea de Defensa para tratar cada riesgo son pertinentes, y siguen siendo válidas en el contexto actual. Se han considerado las diferentes opciones de tratamiento (evitar, transferir, mitigar o aceptar el riesgo) y se han seleccionado las más adecuadas en cada caso.

- La entidad se encuentra en proceso de formalizar una nueva plataforma tecnológica y los mapas de procesos. Sin embargo, esta nueva plataforma aún no se ha implementado, por lo que es prematuro evaluar su impacto en los riesgos identificados.

Teniendo en cuenta lo anterior y que no se evidencia auditorías internas y externas que hayan tenido como resultado hallazgos relacionados con los riesgos identificados y su tratamiento, se mantiene lo reportado desde el proceso, en el sentido de no modificar ni actualizar los riesgos.

Dado que no se han identificado nuevos riesgos en el contexto actual, que los riesgos identificados son controlables con los controles existentes y que no se han identificado nuevos riesgos, no se requiere documentar y gestionar riesgos adicionales.

4.1.3.2 ALERTAS:

De acuerdo con el monitoreo de primera línea de defensa referente a los riesgos identificados de seguridad de la información del Proceso ADMINISTRACIÓN DEL TALENTO HUMANO, no se reportan alertas que indiquen que los riesgos puedan materializarse o se hayan materializado.

4.1.3.3 RECOMENDACIONES:

Se recomienda que la Primera Línea de Defensa revise y actualice la información del Mapa de Riesgos una vez que se formalice la nueva plataforma tecnológica y los mapas de procesos.

Se recomienda analizar la calidad y la suficiencia de los registros disponibles. Se

recomienda verificar que los registros sean completos, precisos y confiables, y que permitan demostrar efectivamente la aplicación del control.

Las acciones de tratamiento propuestas en el plan de acción para el primer riesgo identificado son pertinentes y adecuadas, sin embargo, se recomienda implementar mecanismos de control para verificar la correcta gestión de la información y la prevención de copias no controladas.

La acción de tratamiento propuestas en el plan de acción para el segundo riesgo identificado es pertinente y adecuada. Se recomienda incluir en la socialización semestral al interior de la Dirección de Talento Humano las actividades relacionadas y verificar su cumplimiento, detallar las temáticas específicas a abordar e incluir indicadores o métricas para medir la efectividad y establecer un plan de seguimiento para evaluar el impacto de las capacitaciones con el fin de realizar ajustes si es necesario.

Continuar con la implementación, ejecución y seguimiento de los controles y el plan de tratamiento de riesgos.

Asistir a las sesiones de capacitación y sensibilización en temas de seguridad y privacidad de la información programadas por la entidad.

4.2 GESTIÓN DE RECURSOS FINANCIEROS

4.2.1 A-LE-305 MAPA DE RIESGOS DE GESTIÓN DE RECURSOS FINANCIEROS VERSIÓN 9 ACTA DE MEJORAMIENTO 44 DE ENERO 30 DE 2024

Riesgos de Gestión

1. Posibilidad de afectación económica y reputacional por hallazgos administrativos, disciplinarios y penales y sanciones por entes de control, debido a estados financieros con salvedades, interpretación errónea de la normatividad contable y falta de oportunidad, utilidad y confiabilidad en la información entregada por los proveedores de la misma.

2. Posibilidad de afectación económica y reputacional por hallazgos administrativos, disciplinarios y penales y sanciones por entes de control, debido a inexactitud en los movimientos presupuestales (modificaciones, certificados de disponibilidad presupuestal, registros presupuestales, anulaciones).

4.2.1.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias***.

La Dirección Financiera remitió a la Dirección de Planeación Institucional el monitoreo de primera línea de defensa a los riesgos asociados al mismo, mediante radicado en 3-2024-16273 del 6 de mayo, el cual es el insumo para el presente monitoreo de la segunda línea de defensa.

Para el periodo de monitoreo, no se han identificado situaciones o aspectos en el ámbito interno o externo que represente cambios en el contexto estratégico del proceso.

Se observa coherencia entre los riesgos de gestión identificados y el objetivo estratégico asociado al proceso "Fortalecer la estructura y la cultura institucional para contribuir a una gestión pública efectiva, mediante el desarrollo de habilidades para el talento humano, simplificación de procesos, mecanismos eficientes para la toma de decisiones y mejora continua". Así mismo, los riesgos de gestión identificados guardan coherencia con el objetivo del proceso.

Conforme al monitoreo de la primera línea de defensa, las causas y consecuencias del riesgo se mantienen. No se reportan situaciones u otros aspectos, que evidencien otras causas o consecuencias de los riesgos identificados.

2. ***Autoevaluación de la efectividad de los controles***.

De acuerdo al monitoreo a riesgos gestión por parte de la primera línea de defensa, se han utilizado los controles establecidos y los controles examinados previenen y mitigan los riesgos, sin embargo; no es posible consultar las evidencias y soportes que se encuentran en cada aplicativo (Bogdata, Sicapital), ni tampoco las que mencionan se ubican en las tablas de retención documental organizadas digitalmente por la Dirección Financiera, donde solo tienen acceso algunos funcionarios de la Dirección. 8carpeta: f///R:/Privada/Dir.Gestion_Financiera/2024).
De acuerdo a lo reportado en el monitoreo de la primera línea de defensa con corte al 30 de abril/2024 y los resultados de las auditorías internas y externa adelantadas en el primer cuatrimestre, no se evidencian hallazgos asociados a los controles establecidos.

3. ***Autoevaluación de la eficacia de las acciones:***

No se requieren acciones en el marco del Plan para tratamiento a riesgos, debido al resultado en el nivel del riesgo residual, en zona del riesgo final Moderado. El proceso indica en el monitoreo a riesgos de la primera línea de defensa la ejecución de acciones que dan cuenta de la aplicación de los controles con evidencias (f///R:/Privada/Dir.Gestion_Financiera/2024/ Repositorio de evidencias ID ID SDP-2024-4207 / ID SDP-2024-4250 https://www.sdp.gov.co/transparencia/planeacion-presupuesto-informes) tal como se indicó en la sección Autoevaluación de la efectividad de los controles.
En consecuencia, los riesgos de gestión identificados no se han materializado, ni tampoco se han determinado como hallazgo de auditoria interna o externa

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

De acuerdo al monitoreo de primera línea de defensa han revisado los controles confirmando que son adecuados, y no han tenido hallazgos para la formulación de planes de mejoramiento. De igual forma, el proceso responde que la gestión del riesgo llevada a cabo le ha sido útil para evitar situaciones o hechos que puedan afectar el cumplimiento de los objetivos. Por lo anterior, se observa la necesidad de fortalecer los argumentos incluidos de tal forma que se dé cuenta del interrogante del numeral 4.1.

Durante el periodo Enero - Abril de 2024 no se han materializado los riesgos de gestión y no se refleja afectación en el cumplimiento de los objetivos del proceso, asociando estos hechos a la efectividad de la gestión del riesgo.

5. ***Actualización de Riesgos****:*

Conforme al reporte del monitoreo con corte al 30 de abril, la primera de defensa no identificó la necesidad de modificar o actualizar los riesgos de corrupción, ni tampoco la necesidad de documentar o gestionar nuevos riesgos, teniendo en cuenta que no se ha materializado el riesgo y que los controles son adecuados, soportado con el hecho de no presentarse planes de mejoramiento. Tomando como referencia el proceso de revisión y actualización llevado a cabo bajo la metodología de DAFP adoptada por la entidad y los informes de auditoría internas y externas no se ha identificado la necesidad de modificar, actualizar, documentar o gestionar nuevos riesgos.

4.2.1.2 ALERTAS:

No se generan alertas al proceso. La ejecución de las acciones asociadas a los controles establecidos, han permitido contrarrestar y mitigar la materialización de los riesgos.

4.2.1.3 RECOMENDACIONES:

Continuar con la gestión de los riesgos de gestión por parte de la primera línea de defensa, reforzando el monitoreo (los argumentos que responden a cada uno de los criterios, así como la presentación de las evidencias) conforme a los lineamientos establecidos, los informes de auditorías, la revisión del resultado del monitoreo de segunda línea de defensa y las sensibilizaciones al riesgo llevadas a cabo en la SDP, con el propósito de optimizar los resultados del seguimiento que contribuyan a la mejora en la gestión del riesgo. Revisar y validar los riesgos una vez se implemente la plataforma estratégica 2024-2027, y actualizar el contexto estratégico del proceso.

4.2.2 A-LE-515 MAPA DE RIESGOS DE CORRUPCIÓN DEL PROCESO GESTIÓN DE RECURSOS FINANCIEROS VERSIÓN 2 ACTA DE MEJORAMIENTO 47 DE ENERO 30 DE 2024

Riesgos de Corrupción
1. Posibilidad de aplicación incorrecta de la normatividad tributaria en el proceso de revisión y liquidación de pagos para favorecer a terceros.

4.2.2.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias.***

La Dirección Financiera remitió a la Dirección de Planeación Institucional el monitoreo de primera línea de defensa a los riesgos asociados al mismo, mediante radicado en 3-2024-16273 del 6 de mayo.

Para el periodo de monitoreo, no se han identificado situaciones o aspectos en el ámbito interno o externo que represente cambios en el contexto estratégico del proceso.

Se observa coherencia entre el riesgo identificado "Posibilidad de aplicación incorrecta de la normatividad tributaria en el proceso de revisión y liquidación de pagos para favorecer a terceros" y el objetivo estratégico asociado al proceso "Fortalecer la estructura y la cultura institucional para contribuir a una gestión pública efectiva, mediante el desarrollo de habilidades para el talento humano, simplificación de procesos, mecanismos eficientes para la toma de decisiones y mejora continua".

El riesgo identificado guarda coherencia con el objetivo del proceso.

Conforme al monitoreo de la primera línea de defensa, las causas y consecuencias del riesgo se mantienen. No se reportan situaciones u otros aspectos, que evidencien otras causas o consecuencias del riesgo identificado.

2. ***Autoevaluación de la efectividad de los controles.***

El proceso manifiesta que se han aplicado los controles establecidos y que el control examinado previene y mitiga los riesgos, sin embargo; no es posible consultar las evidencias que referencia en carpetas a las que no se tiene acceso (R:\Privada\Dir.Gestion_Financiera\2024).
En cuanto a las evidencias ID SDP-2024-4252 / ID SDP-2024-4253, se asocian a la ejecución del control No.2. En el reporte (observaciones) del numeral 2.1 se registró información y evidencia de avance de las actividades formuladas en el plan de acción - tratamiento del riesgo, la cual corresponde al campo observaciones del numeral 3.2. Evidencia ID SDP-2024-4251. En consecuencia, se evidencia la utilización del control No. 2, no obstante, al contar con información parcial, no es posible determinar la efectividad de los controles (3). Por lo anterior, es necesario que para el próximo monitoreo se incluya la información de los argumentos frente a la utilización de los controles establecidos de forma individual y específica, de tal forma que se identifique claramente las evidencias que se asocian a cada uno de los 3 controles. Así mismo, que todas las evidencias que aporten en el repositorio dispuesto, puedan ser consultadas por la segunda y tercera línea de defensa y recordar que deben ser accesibles *por los entes de control, en el caso que se requieran.*
No se evidencian hallazgos asociados a los controles establecidos.

3. ***Autoevaluación de la eficacia de las acciones:***

De conformidad con lo indicado en el monitoreo a riesgos de la primera línea de defensa y las evidencias adjuntas (ID SDP-2024-4251) está implementando de forma adecuada las acciones formuladas para dar tratamiento al riesgo, y se orientan a contrarrestar sus causas. Dichas acciones consisten en: mesas de trabajo con el equipo gestión de cuentas para unificar criterios relacionados con descuentos tributarios y capacitaciones a los enlaces de contratación y contratistas de la entidad en relación con la presentación correcta de los documentos para tramitar los pagos, las cuales. de acuerdo a las actas y soportes de reunión, se han desarrollado en febrero de 2024.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

El proceso considera que la gestión el riesgo le ha sido útil para evitar situaciones o hechos que puedan afectar el cumplimiento de los objetivos. En el primer cuatrimestre 2024 no se ha materializado el riesgo de corrupción y no se visto afectado el cumplimiento de los objetivos del proceso, asociando estos hechos a la efectividad de la gestión del riesgo.

5. ***Actualización de Riesgos****:*

Conforme al reporte del monitoreo con corte al 30 de abril, la primera de defensa no identificó la necesidad de modificar o actualizar el actual riesgo de corrupción, ni tampoco la necesidad de documentar o gestionar nuevos riesgos, teniendo en cuenta que no se ha materializado el riesgo y que los controles son adecuados. Tomando como referencia el proceso de revisión y actualización llevado a cabo bajo la metodología de DAFP adoptada por la entidad y los informes de auditoría internas y externas no se ha identificado la necesidad de modificar, actualizar, documentar o gestionar nuevos riesgos.

4.2.2.2 ALERTAS:

No se generan alertas al proceso. La ejecución de las acciones asociadas a los controles establecidos, han permitido contrarrestar y mitigar la materialización de los riesgos.

4.2.2.3 RECOMENDACIONES:

Fortalecer los argumentos que responden a cada uno de los criterios, así como la presentación de las evidencias, con el propósito de optimizar los resultados del seguimiento que contribuyan a la mejora en la gestión del riesgo.

Revisar y validar los riesgos una vez se implemente la plataforma estratégica 2024-2027, y actualizar el contexto estratégico del proceso.

4.2.3 A-LE-516 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DEL PROCESO GESTIÓN DE RECURSOS FINANCIEROS VERSIÓN 2 ACTA DE MEJORAMIENTO 46 DE ENERO 30 DE 2024

Riesgo de Seguridad de la Información

1. 1. Posibilidad de pérdida de integridad por fallas humanas; de instrumentos de apoyo no oficiales, para el cumplimiento de los objetivos del proceso, almacenados en los repositorios oficiales de la entidad, debido a desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información, manejo manual de la información.

4.2.3.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias***.

El contexto estratégico se mantiene vigente, Sin embargo, es necesario realizar un análisis de manera proactiva con ocasión del rediseño institucional realizado por la entidad mediante el Decreto 432 de 2022, es posible que el objetivo no siga siendo relevante en el nuevo marco institucional. Adicionalmente, el mapa de procesos que se defina a mediados de 2024 podría afectar el contexto actual.

El riesgo de Pérdida de Integridad sigue siendo relevante para el logro del objetivo estratégico de fortalecer la estructura y la cultura institucional, ya que podría afectar la confianza en la entidad, incluso en el contexto del nuevo rediseño institucional. También es importante considerar que el nuevo mapa de procesos, que se hará oficial a mediados de la vigencia 2024, puede introducir nuevos riesgos de seguridad de la información.

El proceso de gestión de recursos financieros implica el manejo de información sensible, como datos financieros de la entidad, información de usuarios y personal de planta, contratistas y pasantes, y datos de proyectos estratégicos. La confidencialidad de esta información es fundamental para proteger los intereses de la entidad y cumplir con las regulaciones aplicables, en razón a ésta afirmación, se recomienda realizar un análisis para determinar si existen riesgos de confidencialidad que pueden afectar al proceso de gestión de recursos financieros como lo son: la divulgación no autorizada de información, pérdida o destrucción de información, uso indebido de la información confidencial, no cumplimiento de las regulaciones de protección de datos y las normas de la Superintendencia Financiera de Colombia, entre otros.

El riesgo de Pérdida de Integridad también es coherente con el objetivo del proceso de GESTIÓN DE RECURSOS FINANCIEROS, ya que podría afectar la eficiencia y oportunidad en la gestión de los recursos financieros, incluso en el marco del nuevo diseño institucional.

Las causas identificadas inicialmente para el riesgo, como el desconocimiento o la no aplicación de las políticas de seguridad y privacidad, el manejo manual de los archivos y la deficiencia en la autorización de permisos de la información, siguen siendo relevantes. Se sugiere revisar la redacción de las causas evitando usar la palabra *desconocimiento* en la formulación dado que la entidad realiza jornadas de capacitación a la cual debe asistir todos los funcionarios, contratistas y pasantes vinculados.

Las consecuencias identificadas inicialmente para el riesgo, como el impacto reputacional por afectación de la imagen de algún área de la organización, siguen siendo posibles si no se toman las medidas adecuadas para mitigar el riesgo.

2. ***Autoevaluación de la efectividad de los controles.***

Se evidencia que la Dirección Financiera ha socializado las actualizaciones recibidas por parte de la Dirección de Tecnología con todo el personal. Existe un registro de la socialización realizada sobre datos abiertos, como la Evidencia ID SDP-2024-4248. Sin embargo, se recomienda socializar las políticas de seguridad y privacidad de la información las cuales son actualizadas anualmente por la Dirección de TIC y publicadas en el sistema de gestión de la entidad.

En la revisión de las evidencias también se observó que se ha diligenciado el Formato A-FO-010 para la gestión de usuarios, como la Evidencia ID SDP-2024-4249 solicitud gestión cuentas de usuario diligenciado solicitando creación cuenta el 01 de abril de 2024 para la señora DUBIANA CAICEDO ZULOAGA.

En conclusión, La Dirección Financiera ha reportado a la Dirección de Tecnología las novedades en la gestión de usuarios. Así mismo, se han socializado las comunicaciones recibidas por parte de la Dirección de Tecnología. La existencia de registros como el Formato A-FO-010 y las comunicaciones entre la Dirección Financiera y la Dirección de Tecnología demuestran que los controles implementados están siendo utilizados de manera efectiva.

La implementación de los controles 1 (definición, revisión, actualización y socialización de las políticas de seguridad de la información) y 2 (diligenciamiento del A-FO-010 para gestión de cuentas de usuarios) contribuye a prevenir o mitigar el riesgo de Pérdida de Integridad por fallas humanas y error en el uso o abuso de derechos y privilegios de la información, de la siguiente manera:

- La definición, revisión y actualización periódicas de las políticas de seguridad de la información garantizan que estas se encuentren alineadas con las mejores prácticas y los riesgos actuales de la entidad.

- La socialización de estas políticas a todo el personal de la Dirección Financiera permite que todos los colaboradores conozcan sus responsabilidades en materia de seguridad de la información y cómo deben manejarla de manera adecuada. Esto ayuda a prevenir errores humanos y el uso o abuso de derechos y privilegios, ya que los colaboradores estarán informados sobre las normas que deben seguir y las consecuencias de su incumplimiento. (control 5.1 de ISO27001:2013)

- El diligenciamiento del Formato A-FO-010 para la gestión de cuentas de usuarios como por ejemplo cambio de usuario en los sistemas de información permite controlar de manera efectiva los accesos a la información. Al registrar cada ingreso o retiro de un usuario, se puede verificar que solo las personas autorizadas tengan acceso a los datos y sistemas que necesitan para realizar su trabajo. Esto ayuda a prevenir accesos no autorizados, que podrían poner en riesgo la confidencialidad, integridad y disponibilidad de la información. (control 9.4 de ISO27001:2023)

De acuerdo con la respuesta del proceso, la Dirección Financiera no tiene hallazgos de auditoría interna o externa relacionados con los controles (definición, revisión, actualización y socialización de las políticas de seguridad de la información) y

(diligenciamiento del A-FO-010 para la gestión de cuentas de usuarios).

La ausencia de hallazgos de auditoría asociados a estos controles es un indicador positivo de que están siendo implementados de manera efectiva y que cumplen con su propósito de prevenir o mitigar el riesgo de Pérdida de Integridad.

3. ***Autoevaluación de la eficacia de las acciones:***

Las acciones son adecuadas para contrarrestar las causas del riesgo. La socialización de las políticas de seguridad de la información (control 1) permite establecer claramente las normas y procedimientos que deben seguir los servidores públicos, contratistas y pasantes en materia de seguridad de la información y ayuda a crear una cultura de seguridad de la información en la entidad. Por otro lado, el diligenciamiento del Formato A-FO-010 para la gestión de cuentas de usuarios (control 2) permite controlar de manera efectiva los accesos a la información, lo que reduce el riesgo de que personas no autorizadas accedan a datos confidenciales.

las acciones formuladas para dar tratamiento al riesgo de Pérdida de Integridad por fallas humanas y error en el uso o abuso de derechos y privilegios de la información se están implementando adecuadamente. La socialización de las actualizaciones recibidas por parte de la Dirección de Tecnología y el diligenciamiento del Formato A-FO-010 para cambios de usuarios son evidencias de que los controles están siendo implementados de manera efectiva.

De acuerdo con lo reportado por el proceso, el riesgo de Pérdida de Integridad por fallas humanas y error en el uso o abuso de derechos y privilegios de la información no se ha materializado hasta la fecha, y no ha sido identificado como hallazgo en ninguna auditoría interna o externa. La ausencia de hallazgos de auditoría asociados a este riesgo es un indicador positivo de que los controles están siendo implementados de manera efectiva y que están cumpliendo con su propósito de prevenir la materialización del riesgo.

Dado que, el riesgo no se ha materializado, no es necesario formular correcciones o acciones correctivas, Sin embargo, es importante continuar con el monitoreo y la revisión de los controles para garantizar su efectividad en la prevención del riesgo.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

La gestión del riesgo de Pérdida de Integridad por fallas humanas y error en el uso o abuso de derechos y privilegios de la información ha sido útil para evitar situaciones o hechos que puedan afectar el cumplimiento de los objetivos y compromisos del proceso como por ejemplo: La fuga de información confidencial puede dañar la reputación de la organización, afectar la confianza de los usuarios, y generar pérdidas financieras significativas, los ataques cibernéticos pueden interrumpir las operaciones de la organización, afectar la disponibilidad de la información, el incumplimiento de las regulaciones de protección de datos o las regulaciones financieras que pueden conllevar a sanciones importantes para la entidad y los errores humanos, como el envío accidental de información confidencial a la persona incorrecta o la eliminación accidental de archivos importantes, pueden tener un impacto negativo en el cumplimiento de los objetivos y compromisos de la organización.

La ausencia de planes de mejora en la presente vigencia y la falta de hallazgos en las auditorías internas y externas son indicadores positivos de que la gestión del riesgo ha sido efectiva en la prevención de las situaciones mencionadas anteriormente.

5. ***Actualización de Riesgos****:*

La respuesta del líder del proceso, en la que indica que no es necesario modificar el riesgo debido a la falta de planes de mejora y hallazgos en auditorías, es parcialmente válida. Si bien estos indicadores son positivos, no son suficientes para determinar definitivamente que el riesgo no necesita ser actualizado. Existen factores como el rediseño de la entidad, la implementación de nuevos sistemas o la contratación de nuevo personal pueden afectar el riesgo de Pérdida de Integridad. Se sugiere soportar la respuesta considerando estos factores en el caso que apliquen.

De acuerdo con la respuesta del proceso, no se identifica la necesidad de modificar y/o actualizar los riesgos, sin embargo, Si bien la gestión del riesgo de Pérdida de Integridad por fallas humanas y error en el uso o abuso de derechos y privilegios de la información ha sido efectiva hasta la fecha, es importante realizar una evaluación proactiva de nuevos riesgos para considerar los cambios en el contexto estratégico de la organización, específicamente el nuevo rediseño institucional. Estas acciones ayudarán a garantizar que el proceso de GESTIÓN DE RECURSOS FINANCIEROS siga siendo seguro y confiable en el futuro.

4.2.3.2 ALERTAS:

De acuerdo con el monitoreo de primera línea de defensa referente a los riesgos identificados de seguridad de la información del Proceso de Gestión de Recursos Financieros, no se reportan alertas que indiquen que los riesgos se han materializado.

4.2.3.3 RECOMENDACIONES:

Se recomienda realizar un análisis del contexto estratégico a la luz del Decreto 432 de 2022, los resultados de las auditorías y otros aspectos relevantes para verificar que no hay cambios que puedan afectar la definición del riesgo o que no hay nuevos riesgos que puedan afectar el proceso.

Se recomienda validar si existen riesgos relacionados con la confidencialidad de la información realizando un análisis proactivo frente a la publicación a mediados de la vigencia 2024 de los nuevos mapas de procesos.

Se recomienda continuar con la implementación y ejecución de los controles definidos en el plan de tratamiento de riesgos como se encuentra mencionado en el mapa final de riesgos de seguridad de la información del proceso.

4.3 ADMINISTRACIÓN DE RECURSOS FÍSICOS Y SERVICIOS GENERALES

4.3.1 A-LE-311 MAPA DE RIESGOS DE GESTIÓN DEL PROCESO DE ADMINISTRACIÓN DE RECURSOS FÍSICOS Y DE SERVICIOS GENERALES VERSIÓN 11 ACTA DE MEJORAMIENTO 41 DE ENERO 30 DE 2024

Riesgos de Gestión

1. Posibilidad de afectación económica y reputacional por desmejoramiento de las buenas prácticas ambientales en la entidad y preservación del ambiente, debido a incumplimiento de requisitos legales y ambientales, baja apropiación en la implementación de hábitos sostenibles por parte de los servidores y colaboradores para contribuir con la reducción en los impactos negativos al ambiente, generados por las actividades inherentes al funcionamiento de la entidad.

2. Posibilidad de afectación económica y reputacional por disminución de la capacidad técnica y operativa de la Secretaría Distrital de Planeación en la prestación de servicios de mantenimiento locativo y parque automotor, debido a incremento en el nivel de deterioro de la infraestructura física y parque automotor, solicitudes de mantenimiento locativo y transporte realizadas fuera de tiempo y sin los requisitos establecidos.

3. Posibilidad de afectación económica por multas y sanciones de los entes reguladores, debido a inconvenientes con la supervisión en la ejecución de los contratos de apoyo logístico, bajo nivel de apropiación de los lineamientos del manual de supervisión y de la normatividad legal vigente aplicable.

4.3.1.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias.***

   Los riesgos identificados abarcan la posibilidad de afectación económica y reputacional debido a diversas causas. En primer lugar, el desmejoramiento de las buenas prácticas ambientales puede resultar en sanciones y pérdida de credibilidad. En segundo lugar, la disminución de la capacidad técnica y operativa en la prestación de servicios de mantenimiento locativo y del parque automotor puede conllevar costos adicionales y deteriorar la reputación institucional. Finalmente, inconvenientes en la supervisión de contratos de apoyo logístico, junto con una baja apropiación de los lineamientos del Manual de Supervisión y la normatividad vigente, pueden derivar en multas y sanciones regulatorias, incrementando los gastos financieros. En conjunto, estos riesgos subrayan la importancia de fortalecer la supervisión, la formación en prácticas sostenibles y la capacidad operativa para mitigar las posibles consecuencias económicas y reputacionales.

   El contexto estratégico se debe ajustar debido a la fusión con el proceso de gestión documental, lo que implica ajustes en la identificación y gestión de riesgos. Aunque el riesgo identificado se encuentra alineado con los objetivos estratégicos, se requiere una revisión para garantizar su coherencia con el nuevo proceso unificado. A pesar de los cambios, las

causas subyacentes del riesgo se mantienen, destacando la necesidad de una atención continua de mejoramiento continuo.

Producto de la verificación se identificaron las siguientes observaciones:

- ✓ Se debe ajustar el contexto estratégico dado que este proceso se unifica con el proceso de gestión documental, lo anterior conforme al rediseño, con el fin de que el riesgo identificado sea coherente con el objetivo del proceso.

2. ***Autoevaluación de la efectividad de los controles****.*

Los controles definidos para los riesgos son preventivos ya que se trata de verificaciones previas, adicional a lo anterior, no se evidencia hallazgos a la fecha, asociados al control.

La implementación de los controles no ha sido completamente efectiva, ya que para el riesgo denominado "Posibilidad de afectación económica y reputacional por disminución de la capacidad técnica y operativa de la secretaría distrital de planeación en la prestación de servicios de mantenimiento locativo y parque automotor, debido a incremento en el nivel de deterioro de la infraestructura física y parque automotor, solicitudes de mantenimiento locativo y transporte realizadas fuera de tiempo y sin los requisitos establecidos ", no se evidencia soportes de la verificación semanal de las necesidades de mantenimiento preventivo de la infraestructura física y vehículos a través del Plan de Mantenimiento Preventivo, así como tampoco se pudo observar si se han encontrado retrasos, y de presentarse si se ajustan la programación y/o adelantan las acciones a que haya lugar según cada caso en particular, lo anterior de acuerdo a lo establecido en los controles.

Del mismo modo, ocurre para el riesgo de "Posibilidad de afectación económica por multas y sanciones de los entes reguladores, debido a inconvenientes con la supervisión en la ejecución de los contratos de apoyo logístico, bajo nivel de apropiación de lineamientos del manual de supervisión y de la normatividad legal vigente aplicable", en el cual no se evidenciaron soportes del cumplimiento del control.

3. ***Autoevaluación de la eficacia de las acciones:***

Las acciones formuladas en el plan de acción de los riesgos están orientadas a contrarrestar sus causas, no se ha reportado la materialización del riesgo ni se ha identificado hallazgos en auditorías internas o externas asociados a los riesgos hasta la fecha, según lo informado por la Dirección Administrativa.

En la primera actividad, se destaca la importancia de especificar las planillas de seguimiento de actividades y los cuadros de Excel que se utilizarán para verificar mensualmente la ejecución del Plan Institucional de Gestión Ambiental (PIGA) a través del Plan Institucional de Residuos (PAI), el Plan de Gestión de Residuos Peligrosos (PGIRS) y el Plan Institucional de Movilidad Sostenible (PIMS). Esto aseguraría una gestión más efectiva al tener claridad sobre los instrumentos concretos que se emplearán para monitorear las actividades. En cuanto a la segunda actividad, se observa una falta de evidencia que demuestre el progreso de los planes de mantenimiento locativo y automotor. Sería necesario implementar mecanismos de seguimiento y reporte que permitan verificar el avance de estos planes y generar alertas de atención de servicio cuando sea necesario, tanto para los profesionales responsables como para la Dirección del área, lo que mejorarían la eficiencia en la gestión de mantenimiento.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

Los riesgos se encuentran relacionados directamente con los objetivos estratégicos, las metas y las funciones de la dirección administrativa, por lo tanto, contribuye para evitar situaciones o hechos que puedan afectar el cumplimiento del proceso.

5. ***Actualización de Riesgos****:*

Basándose en el análisis previo, incluyendo cambios en el contexto estratégico, informes de auditoría interna y externa, y otros factores, se reconoce la necesidad de modificar y/o actualizar el riesgo establecido actualmente para alinearse con el nuevo mapa de procesos. Sin embargo, no se identifica la necesidad de documentar y gestionar nuevos riesgos en este momento.

4.3.1.2 ALERTAS:

- Alinear el mapa de riesgos al nuevo mapa de procesos y a la última versión de la caracterización del proceso.

4.3.1.3 RECOMENDACIONES:

- Adjuntar soportes que evidencien la ejecución del control en su totalidad.

4.3.2 A-LE-523 MAPA DE RIESGOS DE CORRUPCIÓN DEL PROCESO DE ADMINISTRACIÓN DE RECURSOS FÍSICOS Y DE SERVICIOS GENERALES VERSIÓN 1 ACTA DE MEJORAMIENTO 42 DE ENERO 30 DE 2023

Riesgos de Corrupción
1. Posibilidad de manejo indebido de la información relacionada con el proceso y/o abuso del poder, con el fin de interferir en la gestión para beneficio propio o de un tercero.

4.3.2.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias.***

   El riesgo identificado se centra en la posibilidad de un manejo indebido de la información y abuso de poder para interferir en la gestión en beneficio propio o de terceros. Sus causas principales incluyen el registro intencionalmente incorrecto en sistemas de información para ganancia personal o ajena, así como la omisión o incumplimiento de procedimientos para acelerar actividades dentro del proceso. Estas acciones aumentan la probabilidad de manipulación de datos y autorización indebida, generando vulnerabilidades que pueden comprometer la integridad y confidencialidad de la información.

   El contexto estratégico está experimentando ajustes debido a la unificación del proceso con la gestión documental como parte de un rediseño organizacional. A pesar de estos cambios, el riesgo identificado sigue siendo coherente tanto con el objetivo estratégico al que contribuye el proceso como con el objetivo específico del proceso objeto de seguimiento. Además, las causas y consecuencias del riesgo identificadas inicialmente se mantienen según la implementación del Mapa de Riesgos.

   Producto de la verificación se identificaron las siguientes observaciones:

   - ✓ Se debe ajustar el contexto estratégico dado que este proceso se unifica con el proceso de gestión documental, lo anterior conforme al rediseño, con el fin de que el riesgo identificado sea coherente con el objetivo del proceso.

2. ***Autoevaluación de la efectividad de los controles.***

   La evaluación de los controles muestra que, aunque se han establecido procedimientos, la evidencia proporcionada no concuerda con las actividades y los controles definidos, lo que indica una falta de coherencia en la implementación. Solo se adjunta evidencia de ejecución de un control específico relacionado con la gestión de bienes, mientras que no hay soporte para el control relacionado con la socialización interna de procedimientos y riesgos. Ambos controles se consideran preventivos, ya que implican verificaciones previas para mitigar riesgos. No se han encontrado hallazgos de auditoría asociados a estos controles hasta la fecha, según la revisión de la matriz de seguimiento del Sistema de Información y Planificación Administrativa (SIPA).

3. ***Autoevaluación de la eficacia de las acciones:***

   La evaluación de las acciones formuladas para tratar el riesgo muestra que están directamente orientadas a contrarrestar sus causas subyacentes. La actividad de

remitir mensualmente el informe de movimientos de bienes contrarresta el registro erróneo intencional en los sistemas de información, mientras que la socialización interna de procedimientos contrarresta la omisión o incumplimiento de estos. Sin embargo, solo se puede evidenciar la ejecución de la actividad relacionada con el Informe de Movimientos de Bienes de la Entidad. Hasta la fecha, según el reporte de la Dirección Administrativa, el riesgo identificado no se ha materializado ni ha sido determinado como hallazgo en auditorías internas o externas.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

   El análisis integral de la gestión del riesgo indica que ha sido útil para evitar situaciones o hechos que podrían afectar el cumplimiento de los objetivos y compromisos a cargo, según lo reportado por la Dirección Administrativa. Lo anterior indica, que las medidas implementadas en la gestión del riesgo han sido efectivas para salvaguardar los intereses y metas establecidas.

5. ***Actualización de Riesgos****:*

Basándose en el análisis previo, incluyendo cambios en el contexto estratégico, informes de auditoría interna y externa, y otros factores, se reconoce la necesidad de modificar y/o actualizar el riesgo establecido actualmente para alinearse con el nuevo mapa de procesos. Sin embargo, no se identifica la necesidad de documentar y gestionar nuevos riesgos en este momento.

4.3.2.2 ALERTAS:

- Alinear el mapa de riesgos al nuevo mapa de procesos y a la última versión de la caracterización del proceso.

4.3.2.3 RECOMENDACIONES:

- Adjuntar soportes que evidencien la ejecución del control y de las actividades en su totalidad.

4.3.3 A-LE-525 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DEL PROCESO ADMINISTRACIÓN DE RECURSOS FÍSICOS Y DE SERVICIOS GENERALES VERSIÓN 2 ACTA DE MEJORAMIENTO 112 DE FEBRERO 28 DE 2024

Riesgo de Seguridad de la Información
1. Posibilidad de Pérdida de Integridad por fuego, agua y fenómenos sísmicos, debido a ausencia de copias de respaldo o Backup de la información.

4.3.3.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias.***

El objetivo estratégico apalancado por el proceso sigue vigente y no se han identificado cambios relevantes en el entorno de la SDP que puedan afectar la posibilidad de pérdida de integridad de la información. Es importante estar atento y actualizar una vez la entidad defina contexto estratégico derivado de la implementación del Decreto 432 de 2022 y la publicación del mapa de procesos a mediados de la vigencia 2024 identificando cambios significativos que puedan afectar la definición del riesgo.

La pérdida de integridad de la información puede afectar negativamente la imagen de la SDP, lo que podría dificultar el logro del objetivo estratégico de fortalecer la estructura y la cultura institucional. Por lo tanto, el riesgo identificado está directamente relacionado con el objetivo estratégico.

Se recomienda verificar que la definición del riesgo esté alineada con los objetivos y que sea específica, es decir que en el mapa final de riesgos en la columna optimización de la descripción del riesgo se incluya la perdida de activos tipo datos e información (Planes, programas, historias, inventarios, entre otros). Adicionalmente se sugiere revisar si existen riesgos de confidencialidad que puedan afectar el proceso.

La pérdida de integridad de la información puede afectar la capacidad del proceso de ADMINISTRACIÓN DE RECURSOS FÍSICOS Y DE SERVICIOS GENERALES para cumplir con su objetivo de garantizar la continua operación de la entidad. Por lo tanto, el riesgo identificado está directamente relacionado con el objetivo del proceso.

Las causas del riesgo, como la ausencia de copias de respaldo o backup de la información, siguen siendo relevantes. Es importante continuar monitoreando estas causas para garantizar que se tomen las medidas necesarias para mitigar el riesgo. El líder del proceso indica que el contexto estratégico se mantiene. Sin embargo, se recomienda realizar un análisis frente a la entrada en vigor del Decreto 432 de 2022 para identificar posibles cambios que puedan afectar la probabilidad o el impacto del riesgo.

También se indica en el monitoreo de primera línea que, el riesgo identificado es coherente con el objetivo estratégico y del proceso, que las causas del riesgo se mantienen, en este último aspecto se recomienda realizar una evaluación periódica de las causas del riesgo para asegurar que siguen siendo válidas.

Así mismo, el líder del proceso indica que las consecuencias del riesgo se mantienen. Se recomienda realizar una evaluación periódica de las consecuencias del riesgo para asegurar que siguen siendo válidas.

Las consecuencias del riesgo, como el impacto reputacional, siguen siendo relevantes. Es importante continuar monitoreando las consecuencias del riesgo para garantizar que

se tomen las medidas necesarias para mitigar el impacto en caso de que se materialice.

2. ***Autoevaluación de la efectividad de los controles.***

El líder del proceso indica que los tres controles preventivos están siendo implementados y ejecutados. esta afirmación sugiere que tiene copias de seguridad, se aplican políticas de seguridad y que los equipos se encuentran en una ubicación adecuada y protegidos de las condiciones ambientales que los ponga en riesgo (fuego y agua), lo que indica el cumplimiento de las políticas de seguridad de la información y la integridad de los documentos. No se evidencian registros relacionados con los controles, se sugiere mantener registro que soporte los controles aplicados y si se formularan actividades adicionales en o planes de tratamiento. Es importante verificar que se estén generando registros que evidencien la utilización de los controles. Estos registros pueden incluir, por ejemplo, bitácoras de copias de seguridad, actas de capacitación en seguridad de la información y reportes de mantenimiento preventivo. La existencia de estos registros permite demostrar que los controles se están implementando de manera efectiva.

Los controles relacionados con copias de seguridad, ubicación de los equipos son relevantes para mitigar el riesgo de Pérdida de Integridad por fuego, agua y fenómenos sísmicos.

El monitoreo de primera línea de defensa manifiesta que no se han experimentado materializaciones del riesgo ni se han identificado como hallazgos en auditorías internas o externas. Esto destaca la efectividad de los controles implementados y la gestión proactiva del riesgo para evitar posibles consecuencias negativas. Se recomienda tener en cuenta que la identificación de oportunidades de mejora es un proceso continuo que debe realizarse independientemente de si el riesgo se ha materializado o no.

3. ***Autoevaluación de la eficacia de las acciones:***

La formulación de planes de acción dependerá del tratamiento establecido, si es Aceptar no se requieren acciones adicionales, en caso de escoger Reducir (mitigar) se deben diligenciar las acciones que se adelantarán como complemento a los controles establecidos, no necesariamente son controles adicionales.

De acuerdo con lo anterior y que el proceso estableció que como tratamiento la opción Reducir (mitigar), es fundamental que el proceso defina acciones concretas para mitigar el riesgo de Pérdida de Integridad por fuego, agua y fenómenos sísmicos. La ausencia de estas acciones aumenta la probabilidad de que el riesgo se materialice y genere las consecuencias negativas identificadas.

No es posible evaluar la existencia de correcciones o acciones correctivas dado que no se ha formulado un plan de acción.

En la Auditoría Interna realizada del 14 de agosto de 2023 al 22 de agosto de 2023, por la Asociación Internacional de Consultoría no se observó hallazgos relacionados con los riesgos identificados por el proceso, tampoco se evidencia que el riesgo haya sido objeto de otras auditorías internas o externas ni que el riesgo se haya materializado.

De acuerdo con lo reportado por el proceso, el riesgo no se ha materializado y por tanto no se formularon acciones correctivas para darle tratamiento.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

Los controles implementados ayudan a prevenir la pérdida de información crítica para el proceso, las disrupciones en la operación del proceso que puedan afectar el cumplimiento de los objetivos y compromisos del proceso e institucionales y los daños a la reputación de la entidad ocasionados por la pérdida o el acceso no autorizado a información sensible.

5. ***Actualización de Riesgos****:*

Si bien la respuesta del proceso indica que no es necesario modificar o actualizar el riesgo en este momento, es importante realizar un análisis cuidadoso de los factores que podrían afectar la validez de la evaluación actual del riesgo. Estos factores incluyen los Cambios en el contexto estratégico, avances tecnológicos, cambios en el entorno regulatorio o nuevos eventos de seguridad de la información.

No se identifica la necesidad de documentar nuevos riesgos, sin embargo, es importante estar atento a la aparición de nuevos riesgos que puedan afectar la seguridad de la información del proceso de ADMINISTRACIÓN DE RECURSOS FÍSICOS Y DE SERVICIOS GENERALES. Estos nuevos riesgos pueden surgir como resultado de cambios en el contexto, nuevas tecnologías, o nuevos eventos de seguridad de la información.

4.3.3.2 ALERTAS:

De acuerdo con el monitoreo de primera línea de defensa referente a los riesgos identificados de seguridad de la información del Proceso Recursos físicos y de Servicios Generales, no se reportan alertas que indiquen que los riesgos se han materializado.

4.3.3.3 RECOMENDACIONES:

El líder del proceso indica que el riesgo identificado es coherente con el objetivo estratégico. Se recomienda verificar que la definición del riesgo esté alineada con los objetivos y que sea específica, es decir que, por ejemplo, el riesgo se defina “Posibilidad de Pérdida de Integridad de los activos tipo datos e información, Planes, programas, historias, inventarios, entre otros, por fuego, agua y fenómenos sísmicos, debido a ausencia de copias de respaldo o backups de la información.

Se recomienda realizar un análisis para identificar posibles cambios que puedan afectar la probabilidad o el impacto del riesgo considerando los siguientes aspectos:

- Cambios en el entorno de la organización: ¿Se han presentado cambios en el entorno de la SDP que puedan afectar la probabilidad o el impacto del riesgo? En especial revisar los efectos después de entrada en vigor del Decreto 432 de 2022.

- Nuevos proyectos o iniciativas: ¿Se han implementado nuevos proyectos o iniciativas que puedan afectar la gestión del riesgo? en este aspecto validar la estrategia Camaleón, la implementación del Sistema de Gestión de Documentos Electrónicos de Archivo, entre otros.

Se recomienda evaluar la eficacia de los controles para determinar si están logrando el objetivo de reducir el riesgo a un nivel aceptable. Por ejemplo: evaluar el control de copias de seguridad para determinar si se está realizando de forma adecuada y si está logrando el objetivo de proteger la información.

Se recomienda implementar un plan de respuesta a incidentes y formular el plan de continuidad de las operaciones para mitigar los impactos de la materialización de un riesgo.

Por la naturaleza y criticidad de la información, se recomienda mantener evidencia como, por ejemplo: Informes de auditoría interna o externa que no encuentren hallazgos relacionados con el riesgo, casos documentados en los que la implementación de medidas de control haya evitado la materialización de un riesgo, Indicadores de riesgo que muestren una tendencia a la baja en la probabilidad o el impacto del riesgo y evidencias de la aplicación de los controles y el seguimiento.

Se recomienda realizar capacitaciones y entrenamiento continuo en gestión de riesgos dirigido a las personas que participan en la gestión de los activos de información como planes, programas, historias, inventarios para los integrantes de las áreas que hacen parte del proceso.

Ser recomienda a participación activamente en las capacitaciones sobre seguridad y privacidad de la información programadas por la entidad.
.

4.4 GESTIÓN DOCUMENTAL

4.4.1 A-LE-312 MAPA DE RIESGOS DE GESTIÓN DEL PROCESO GESTIÓN DOCUMENTAL VERSIÓN 9 ACTA DE MEJORAMIENTO 40 DE ENERO 30 DE 2024

Riesgos de Gestión

1. Posibilidad de afectación económica y reputacional por pérdida o deterior de los documentos de archivo, debido a falencias en el diseño, despliegue e implementación de políticas de gestión documental.

4.4.1.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias.***

   El riesgo identificado involucra la posibilidad de sufrir afectaciones económicas y de reputación debido a la pérdida o deterioro de documentos de archivo, ocasionadas por deficiencias en el diseño, despliegue e implementación de políticas de gestión documental. La causa raíz e inmediatas están estrechamente relacionadas, ya que las deficiencias en las políticas de gestión documental conducen directamente a la pérdida o deterioro de los documentos. El impacto de este riesgo se manifiesta tanto en pérdidas económicas como en daños a la reputación de la Secretaria de Planeación.

   La evaluación del contexto estratégico indica que no se mantiene, se observa coherencia del riesgo identificado con los objetivos estratégicos y del proceso en seguimiento. Además, tanto las causas como las consecuencias identificadas inicialmente para el riesgo permanecen según el mapa de riesgos. Lo anterior indica, que se debe ajustar la pertinencia del riesgo en relación con el entorno.

   Producto de la verificación se identificaron las siguientes observaciones:

   - ✓ Se debe ajustar el contexto estratégico dado que este proceso se unifica con el proceso de Administración de recursos físicos y de servicios generales, lo anterior conforme al rediseño, con el fin de que el riesgo identificado sea coherente con el objetivo del proceso.

2. ***Autoevaluación de la efectividad de los controles.***

   Se evidencia que los controles están siendo utilizados, como se demuestra mediante la presentación de registros específicos para cada control establecido. Estos controles están diseñados para prevenir riesgos, ya que implican verificaciones periódicas de integridad y distribución de comunicaciones, consulta documental y estado físico de unidades de almacenamiento de archivo. Además, no se han encontrado hallazgos de auditoría asociados a estos controles hasta la fecha.

3. ***Autoevaluación de la eficacia de las acciones:***

Las acciones formuladas para abordar el riesgo están directamente orientadas a contrarrestar sus causas, y se evidencia que están siendo implementadas según los registros proporcionados. Hasta la fecha, según el reporte de la Dirección Administrativa, el riesgo identificado no se ha

materializado ni ha sido determinado como hallazgo en auditorías internas o externas. Lo anterior indica, que las medidas implementadas están siendo efectivas para mitigar el riesgo y proteger los intereses de la Secretaria de Planeación.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

El análisis integral de la gestión del riesgo indica que ha sido útil para evitar situaciones o hechos que podrían afectar el cumplimiento de los objetivos y compromisos a cargo, según lo reportado por la Dirección Administrativa. Esto sugiere que las medidas implementadas en la gestión del riesgo han sido efectivas para salvaguardar los intereses y metas establecidas.

5. ***Actualización de Riesgos****:*

Basándose en el análisis previo, incluyendo cambios en el contexto estratégico, informes de auditoría interna y externa, y otros factores, se reconoce la necesidad de modificar y/o actualizar el riesgo establecido actualmente para alinearse con el nuevo mapa de procesos. Sin embargo, no se identifica la necesidad de documentar y gestionar nuevos riesgos en este momento.

4.4.1.2 ALERTAS:

- Alinear el mapa de riesgos al nuevo mapa de procesos y a la última versión de la caracterización del proceso.

4.4.1.3 RECOMENDACIONES:

4.4.2 A-LE-522 MAPA DE RIESGOS DE CORRUPCIÓN DEL PROCESO GESTIÓN DOCUMENTAL VERSIÓN 2 ACTA DE MEJORAMIENTO 39 DE ENERO 30 DE 2024

Riesgos de Corrupción

1. Posibilidad de adulteración o sustracción de la documentación custodiada por la Dirección Administrativa con participación de servidores y/o contratistas de la entidad.

4.4.2.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias***.

   El riesgo identificado implica la posibilidad de adulteración o sustracción de la documentación custodiada por la Dirección Administrativa, con participación de servidores y/o contratistas de la entidad. Este riesgo está asociado al trámite u OPA de consulta de documentación urbanística. Sus causas incluyen el no acatamiento de políticas y procedimientos de gestión documental, falta de conocimiento de los requisitos para ser usuario de los servicios documentales y documentación sin la completa intervención documental. Estas causas sugieren deficiencias en la implementación de políticas y procedimientos, así como la necesidad de fortalecer la conciencia y capacitación sobre la gestión documental para prevenir posibles incidentes de seguridad.

   En relación con el análisis del contexto estratégico se requiere ajustar debido a la unificación con el proceso Administración de recursos físicos y de servicios generales, conforme al rediseño. Sin embargo, el riesgo identificado sigue siendo coherente tanto con el objetivo estratégico como con el objetivo del proceso objeto del seguimiento. Además, las causas como las consecuencias identificadas inicialmente para el riesgo se mantienen según el mapa de riesgos implementado. Esto sugiere que el riesgo sigue siendo relevante y pertinente a pesar de los cambios en el contexto estratégico y de proceso.

2. ***Autoevaluación de la efectividad de los controles***.

   La evidencia proporcionada indica que el control no está siendo utilizado de manera adecuada, ya que los soportes presentados no son coherentes con las actividades y el control definido. Por ejemplo, se adjuntan registros de préstamo documental y reuniones de revisión de riesgos de corrupción, que no concuerdan con las actividades de sensibilización sobre el código de ética y el Código General Disciplinario. Aunque el control está diseñado para prevenir riesgos mediante la revisión permanente de la integridad de los expedientes consultados, se sugiere una mejora en la redacción para incluir los formatos utilizados en la ejecución del control. Además, no se han encontrado hallazgos de auditoría asociados a este control hasta la fecha, según la revisión de la matriz de seguimiento del Sistema de Información y Planificación Administrativa (SIPA).

3. ***Autoevaluación de la eficacia de las acciones:***

Las acciones formuladas para abordar el riesgo están dirigidas a contrarrestar una de las causas identificadas: el no acatamiento de las políticas, procedimientos y directrices de gestión documental por parte de los

funcionarios. Sin embargo, se recomienda revisar y formular acciones adicionales para abordar las causas restantes: la falta de conocimiento de los usuarios internos y externos sobre los requisitos para ser usuarios de los servicios documentales, así como la documentación sin la completa intervención documental. La implementación adecuada de estas acciones no se puede verificar debido a la falta de coherencia en los soportes proporcionados. Hasta la fecha, según el reporte de la Dirección Administrativa, el riesgo identificado no se ha materializado ni ha sido determinado como hallazgo en auditorías internas o externas.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

El análisis del riesgo indica que ha sido útil para evitar situaciones o hechos que podrían afectar el cumplimiento de los objetivos y compromisos a cargo, según lo reportado por la Dirección Administrativa. Esto sugiere que las medidas implementadas en la gestión del riesgo han sido efectivas para proteger los intereses y metas establecidas.

5. ***Actualización de Riesgos****:*

Basándose en el análisis previo, cambios en el contexto estratégico y resultados de informes de auditoría, se identifica la necesidad de modificar y/o actualizar el riesgo establecido actualmente para alinearlo con el nuevo mapa de procesos y asegurar que los controles estén adaptados a la realidad del proceso. Sin embargo, no se percibe la necesidad de documentar y gestionar nuevos riesgos en este momento.

4.4.2.2 ALERTAS:

- Alinear el mapa de riesgos al nuevo mapa de procesos y a la última versión de la caracterización del proceso.

4.4.2.3 RECOMENDACIONES:

- Adjuntar soportes que evidencien la ejecución del control y de las actividades en su totalidad.

4.4.3 A-LE-524 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DEL PROCESO GESTIÓN DOCUMENTAL VERSIÓN 2 ACTA DE MEJORAMIENTO 120 DE MARZO 04 DE 2024

Riesgo de Seguridad de la Información
1. Posibilidad de pérdida de disponibilidad por destrucción de la información, que se encuentra en diferentes medios removibles y que es identificada para preservar digitalmente, debido a copias insuficiente entrenamiento y capacitación sobre las políticas de seguridad y privacidad de la información, copias no controladas, información sensible sin cifrado, ausencia de copias de respaldo o backups de la información. 2. Posibilidad de pérdida de disponibilidad por mal funcionamiento del software; utilizado para la visualización de la información susceptible para preservar digitalmente (word, excel, ppt, tiff...), por mal funcionamiento del software y saturación del sistema de información, debido a ausencia de la gestión en el versionamiento de los sistemas de información, software nuevo o inmaduro o ausencia de mecanismos de identificación y autenticación en los sistemas de información. 3. Posibilidad de Perdida de Disponibilidad por mal funcionamiento del software que afecte la información almacenada en SGDEA o en el módulo de preservación digital, debido a software nuevo o inmaduro, configuración incorrecta de parámetros , ausencia de la gestión en el versionamiento de los sistemas de información, ausencia de control de cambios en sistemas de información además por Error en el uso o abuso de derechos y privilegios debido a la Gestión deficiente de las contraseñas - Contraseñas sin protección y por la Falsificación de derechos de acceso debido a la Ausencia de mecanismo de identificación y autenticación en los sistemas de información 4. Posibilidad de Perdida de Disponibilidad por mal funcionamiento del equipo de cómputo o servidores que almacenan la información a preservar digitalmente, debido a ausencia de esquemas de reemplazo periódico, por fallas del equipo debido a la obsolescencia tecnológica tipo hardware y por uso no autorizado del equipo por el Acceso al Hardware sin protección o protocolos de seguridad 5. Posibilidad de pérdida de disponibilidad, en lugar de almacenamiento de los equipos, medios removibles, o servidores donde se almacena la información a preservar digitalmente; por fenómenos climáticos, fuego, agua o fenómenos sísmicos; debido a ausencia de mecanismos de dispersión de humo y fuego, uso inadecuado de los controles de acceso físico a las edificaciones y áreas seguras, ubicación en un área susceptible de inundación, ausencia de protección física de la edificación, puertas y ventanas. 6. Posibilidad de Perdida de Disponibilidad por fallas humanas; de personas responsables de la producción, gestión, almacenamiento y custodia de la información a preservar digitalmente, debido a insuficiente entrenamiento y capacitación sobre las políticas de seguridad y privacidad de la información.

4.4.3.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias***.

El líder del proceso confirmó que el contexto estratégico se mantiene, lo que sugiere una continuidad en la relevancia y pertinencia de

los riesgos identificados en relación con los objetivos estratégicos de la organización. Esto indica que los riesgos identificados siguen siendo significativos para la dirección estratégica de la organización y refuerza la necesidad de mantener un enfoque proactivo en la gestión de riesgos para salvaguardar los activos y los intereses institucionales.

La respuesta afirmativa del líder del proceso indica que existe una alineación directa entre el riesgo identificado y el objetivo estratégico al que contribuye el proceso de gestión documental, lo que sugiere una comprensión clara de cómo la gestión de riesgos se integra con los objetivos de la organización. Esta coherencia demuestra la importancia de abordar los riesgos de manera efectiva para garantizar que el proceso de gestión documental contribuya de manera óptima a la consecución de los objetivos estratégicos de la organización, especialmente en lo que respecta a la preservación y disponibilidad de la información.

La confirmación de que el riesgo identificado es coherente con el objetivo del proceso muestra una comprensión sólida de cómo los riesgos afectan directamente a las actividades y resultados del proceso de gestión documental, lo que resalta la importancia de abordar adecuadamente estos riesgos. Esta coherencia subraya la necesidad de integrar la gestión de riesgos en todas las etapas del proceso de gestión documental para garantizar la efectividad y eficiencia en la protección y preservación del patrimonio documental de la entidad.

La respuesta afirmativa del líder del proceso indica que las causas identificadas inicialmente para el riesgo persisten, lo que sugiere que las condiciones subyacentes que generan el riesgo aún están presentes y requieren atención continua para mitigar adecuadamente el riesgo. Es fundamental abordar estas causas de manera proactiva para prevenir la ocurrencia de eventos no deseados que pudieran comprometer la integridad y disponibilidad de la información, lo que destaca la importancia de mantener un monitoreo constante y una mejora continua en las medidas de control implementadas.

La confirmación de que las consecuencias identificadas inicialmente para el riesgo se mantienen resalta la importancia de abordar adecuadamente el riesgo para evitar posibles impactos negativos en la organización, lo que evidencia la necesidad de implementar y mantener efectivamente las actividades de control y los planes de acción formulados.

Estas consecuencias pueden tener repercusiones significativas en la integridad, disponibilidad y reputación de la información de la entidad en su conjunto, lo que refuerza la necesidad de mantener una vigilancia constante y una respuesta proactiva para minimizar los riesgos y maximizar la resiliencia ante posibles eventos adversos.

2. ***Autoevaluación de la efectividad de los controles****.*

Existen evidencias de que los controles están siendo utilizados, como lo demuestran las actualizaciones realizadas en los formatos pertinentes, la aplicación de las políticas de uso de medios removibles, control de acceso y gestión de activos de información.

La actualización y aplicación de políticas indica un compromiso activo por parte del equipo responsable en la implementación y mantenimiento de los controles establecidos para mitigar los riesgos identificados. Estas evidencias refuerzan la efectividad del proceso de gestión documental y su capacidad para adaptarse a las necesidades cambiantes del entorno.

El líder del proceso confirmó que el control utilizado previene o mitiga el riesgo. En la observación indica que las consecuencias identificadas inicialmente se mantienen. Para

próximas revisiones es pertinente validar que las observaciones realizadas en el monitorio de primera línea respondan de manera más directa a las preguntas en cada criterio.

La respuesta anterior, sugiere que los controles implementados están diseñados para abordar las causas subyacentes y reducir las posibles consecuencias negativas del riesgo. Sin embargo, podría ser beneficioso para el proceso evaluar la efectividad real de estos controles en la mitigación del riesgo y considerar posibles mejoras adicionales para fortalecer la protección de la información.

El líder del proceso informó que no hay hallazgos de auditoría en este momento y que se están planificando mesas de trabajo para definir estrategias en el futuro.

La ausencia de hallazgos de auditoría puede ser un indicio positivo de que los controles implementados están funcionando según lo previsto. Sin embargo, la planificación de mesas de trabajo para definir estrategias futuras sugiere un enfoque proactivo para abordar posibles áreas de mejora y fortalecer aún más los controles de gestión documental. Es importante seguir de cerca estos procesos para garantizar la efectividad continua de los controles y la gestión de riesgos en el tiempo.

3. ***Autoevaluación de la eficacia de las acciones:***

El líder del proceso confirmó que las acciones formuladas están orientadas a contrarrestar las causas del riesgo identificado. Esta respuesta indica que el proceso de gestión documental ha identificado adecuadamente las causas subyacentes del riesgo y ha desarrollado acciones específicas para abordarlas. Es fundamental que estas acciones estén dirigidas directamente a las raíces del problema para garantizar una mitigación efectiva del riesgo.

El líder del proceso confirmó que las acciones para el tratamiento del riesgo se están implementando adecuadamente. La implementación efectiva de las acciones es esencial para garantizar que los controles propuestos sean efectivos en la reducción del riesgo. Es importante seguir monitoreando de cerca la implementación para abordar cualquier desviación o problema que pueda surgir durante este proceso.

El líder del proceso informó que el riesgo identificado no se ha materializado ni ha sido determinado como hallazgo de auditoría. La falta de materialización del riesgo es una señal positiva de que los controles implementados hasta la fecha han sido efectivos para prevenir la ocurrencia del riesgo. Sin embargo, es crucial continuar monitoreando de cerca la situación para detectar cualquier señal temprana de riesgo y tomar medidas preventivas adecuadas.

El líder del proceso confirmó que no se han formulado correcciones ni acciones correctivas, ya que el riesgo no se ha materializado. Aunque el riesgo no se ha materializado hasta la fecha, es importante tener planes de contingencia y estar preparado para actuar rápidamente en caso de que ocurra. La falta de acciones correctivas puede indicar una oportunidad para revisar y fortalecer los planes de respuesta ante posibles escenarios de riesgo en el futuro.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

El líder del proceso respondió afirmativamente, indicando que la gestión realizada ha sido útil para evitar los riesgos. Esta respuesta refleja una evaluación positiva de la efectividad de la gestión de riesgos dentro del proceso de gestión documental.

Es importante destacar que una gestión efectiva de riesgos no solo implica la identificación y mitigación de riesgos, sino

también la capacidad de anticiparse a posibles situaciones adversas y tomar medidas proactivas para prevenirlas o mitigar su impacto. Al implementar actividades de control y planes de acción, el proceso ha demostrado su compromiso con la protección del patrimonio documental y la garantía de la disponibilidad de la información como un activo institucional. Esta evaluación positiva refuerza la importancia de mantener un enfoque continuo en la gestión de riesgos para asegurar el logro de los objetivos estratégicos y del proceso en el largo plazo.

5. ***Actualización de Riesgos**:*

El líder del proceso indicó que no se hace necesario modificar y/o actualizar el riesgo establecido actualmente. La respuesta del líder del proceso sugiere que, tras un análisis exhaustivo que incluyó cambios en el contexto estratégico y resultados de auditoría, no se han identificado cambios significativos que justifiquen la modificación o actualización del riesgo establecido previamente. Esto puede ser un indicio de la efectividad y relevancia continua de las actividades de control y planes de acción implementados para abordar el riesgo. Sin embargo, es importante que el proceso de gestión de riesgos permanezca dinámico y esté abierto a ajustes en caso de cambios en el entorno operativo o estratégico.

En cuanto documentar nuevos riesgos el líder del proceso respondió negativamente, indicando que no se hace necesario. La respuesta del líder del proceso sugiere que no se han identificado nuevos riesgos que requieran documentación y gestión adicionales en este momento. Esto puede reflejar una comprensión sólida de los riesgos existentes y las medidas de control implementadas para abordarlos. Sin embargo, es importante continuar monitoreando de cerca el entorno operativo y estratégico para identificar cualquier nuevo riesgo emergente y estar preparado para documentarlo y gestionarlo adecuadamente en el futuro.

La falta de identificación de nuevos riesgos puede ser una señal positiva de que las actividades de control existentes son efectivas, pero también puede requerir una vigilancia continua para mantener la adaptabilidad del proceso de gestión de riesgos.

4.4.3.2 ALERTAS:

De acuerdo con el monitoreo de primera línea de defensa referente a los riesgos identificados de seguridad de la información del Proceso de Gestión documental, no se reportan alertas que indiquen que los riesgos se han materializado.

4.4.3.3 RECOMENDACIONES:

Se recomienda implementar el plan de acción en pro de seguir mejorando la efectividad de los controles que están operativos actualmente por parte de Gestión documental y la DTIC para la gestión de los riesgos de seguridad de la información y que están relacionados con la preservación y conservación digital.

Se recomienda implementar un plan de respuesta a incidentes para mitigar los impactos de la materialización de un riesgo.

Se recomienda realizar un plan de continuidad de negocio para garantizar que en caso de una afectación grave, las operaciones puedan continuar con el fin de garantizar la prestación de los servicios.

Por la naturaleza y criticidad de la información, se recomienda mantener evidencia como por ejemplo: Informes de auditoría interna o externa que no encuentren hallazgos relacionados con el riesgo, casos documentados en los que la

implementación de medidas de control haya evitado la materialización de un riesgo, Indicadores de riesgo que muestren una tendencia a la baja en la probabilidad o el impacto del riesgo, evidencias de la utilización de los controles.	Se recomienda realizar la revisión de los controles y planes de trabajo que se formulan en el proceso, esto en el sentido de proyectar acciones que se puedan gestionar y ejecutar al interior del proceso y evitar que estas deban ser desarrolladas en otros procesos como la Dirección TIC.
Se recomienda realizar capacitaciones y entrenamiento continuo en gestión de riesgos dirigido a las personas que participan en la gestión de los activos de tipo información para los integrantes de las áreas que hacen parte del proceso.	Se recomienda asistir a las sesiones de capacitación y socialización en temas de seguridad y privacidad de la información.

4.5 SOPORTE TECNOLÓGICO

4.5.1 A-LE-303 MAPA DE RIESGOS DE GESTIÓN DEL PROCESO SOPORTE TECNOLÓGICO VERSIÓN 10 ACTA DE MEJORAMIENTO 70 DE ENERO 31 DE 2024

Riesgos de Gestión

1. Posibilidad de afectación económica y reputacional por insuficiente destinación para cubrir las necesidades de la sostenibilidad y mejoramiento de la operación de servicios tecnológicos, debido a la variación de la tasa representativa del mercado (TRM) y limitada asignación de recursos presupuestales.

2. Posibilidad de afectación reputacional por recurso humano insuficiente para soportar los diferentes servicios de tecnologías de la información con componente de infraestructura, debido a aumento en la demanda de requerimientos y crecimiento en componentes de infraestructura tecnológica de la entidad.

3. Posibilidad de afectación reputacional por cambios en los requerimientos funcionales pactados en el instrumento A-FO-227 al momento de la entrega de la solución de software al usuario funcional, debido a insuficiente dimensionamiento del alcance y de los requerimientos entre el nivel directivo y el usuario funcional.

4. Posibilidad de afectación reputacional por insuficiente alineación de las áreas externas a tecnologías frente a los procedimientos, estándares y herramientas establecidos por la Dirección de TIC para la construcción y mantenimiento de soluciones de software, debido a desarticulación entre los procesos de la entidad con el proceso de TI, incumplimiento de las políticas y procedimientos establecidos para el desarrollo y mantenimiento del software.

5. Posibilidad de afectación reputacional por reprocesos por la falta de continuidad en la prestación del servicio por parte del contratista de mesa de ayuda con personal idóneo y capacitado, debido a pérdida de conocimiento por la rotación y poca trazabilidad del conocimiento específico de los roles.

6. Posibilidad de afectación reputacional por falta de oferta de servicios de soporte y garantías para componentes de TI, debido a obsolescencia tecnológica.

4.5.1.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias.***

De acuerdo con el análisis realizado por la primera línea de defensa, el contexto estratégico se mantiene entre tanto se culmina la oficialización del Mapa de Procesos en la entidad. La actualización del contexto estratégico mediante la matriz DOFA propende a la mejora de servicios digitales alineados con Gobierno de TI.

Los riesgos de gestión identificados (6 en total), guardan coherencia con el objetivo estratégico al cual le aporta el proceso "Impulsar una estrategia de transformación digital de la SDP, por medio del desarrollo tecnológico de herramientas que permitan generar valor a los procesos misionales y los servicios digitales de la entidad para los grupos de valor e interés".

A s vez, los riesgos de gestión identificados guardan coherencia con el objetivo del proceso "Fortalecer, administrar y soportar

los servicios de las tecnologías de la información y las comunicaciones TIC mediante la gestión integral de su operación, mantenimiento y actualización". Es relevante tener presente los cambios significativos que se reflejarán con la nueva plataforma estratégica, la transición del proceso actualmente "de apoyo" a un proceso "estratégico", la incorporación de lineamientos, interacciones y aspectos propios de la operación de Gobierno de las Tecnologías de Información en la SDP, tal como lo manifiesta el proceso.

De conformidad con el monitoreo a riesgos de gestión por la primera línea de defensa, las causas y consecuencias identificadas se mantienen.

2. ***Autoevaluación de la efectividad de los controles****.*

Existe evidencias de la utilización de los controles establecidos para los riesgos de gestión. Se adjuntaron los ID correspondientes a las evidencias generadas por la aplicación de cada uno de los controles establecidos para los 6 riesgos de gestión.

En el ámbito del seguimiento llevado a cabo por el proceso, realiza reuniones de la Dirección de TIC para verificar la aplicación de los controles, la revisión y actualización periódica de los instrumentos de registro asociados a los procedimientos del proceso. De igual forma, en el marco de la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI 2024, se realiza seguimiento del plan de controles.

Los controles establecidos para los 6 riesgos de gestión identificados por el proceso previenen la materialización de los riesgos, *contribuyen a mitigar los riesgos, de acuerdo* al resultado reflejado en el monitoreo a riesgos de la primera línea de defensa. Además, no se tienen hallazgos en relación con los controles establecidos en el mapa de riesgos de gestión, provenientes de auditoría.

3. ***Autoevaluación de la eficacia de las acciones:***

Según el nivel de Riesgo residual en zona Moderada, no se requiere formulación del Plan de tratamiento al riesgo. Sin embargo; se generó un acción de mejora para fortalecer las actividades de los controles que se vienen ejecutando. Como resultado del análisis realizado por el proceso durante el presente monitoreo a riesgos de gestión, en seguimiento llevado a cabo mediante reunión del 24 de abril, se encontró que la acción formulada para dar tratamiento al riesgo no contrarresta directamente las causas identificadas, razón por la cual se formula una acción orientada a contrarrestar la causa raíz: "Crear y mantener la base de conocimiento en la mesa de ayuda de la Dirección de TIC", definiendo los criterios asociados a la ejecución y seguimiento (fórmula, meta, periodicidad, responsable del cálculo, responsables del monitoreo y fecha de seguimiento). Evidencia ID SDP-2024-4334. Teniendo en cuenta que la acción para dar tratamiento al riesgo fue formulada el pasado 24 de abril/2024, el seguimiento aplica para el próximo monitoreo.

De conformidad con el monitoreo a riesgos del presente periodo, los riesgos de gestión no se han materializado ni tampoco se ha determinado como hallazgo de ejercicios de auditoria interna o externa.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

De acuerdo al monitoreo de la primera línea de defensa, la gestión de los riesgos ha permitido fortalecer sus controles, definiendo acciones de mejora en el plan de tratamiento, logrando contribuir en el cumplimiento del objetivo del proceso de Gobierno de TI. En consecuencia, se infiere que su gestión le ha

sido útil para evitar situaciones o hechos que puedan afectar el cumplimiento de los objetivos y compromisos a su cargo.

5. ***Actualización de Riesgos**:*

Por el momento no se identifica la necesidad de modificar y/o actualizar, los riesgos de gestión establecidos actualmente ni la necesidad de documentar o incluir nuevos riesgos. No obstante, cuando surja el cambio del proceso a nivel estratégico, se realizará la alineación y actualización requerida.

4.5.1.2 ALERTAS:

No se generan alertas por la posibilidad de materialización de los riesgos de gestión identificados para el proceso. Lo anterior, conforme al resultado arrojado con la gestión del riesgo, en términos de efectividad.

4.5.1.3 RECOMENDACIONES:

Continuar con la efectiva gestión a los riesgos, y la ejecución de los controles.

Revisar y validar los riesgos una vez se implemente la plataforma estratégica 2024-2027, y actualizar el contexto estratégico del proceso.

4.5.2 A-LE-520 MAPA DE RIESGOS DE CORRUPCIÓN DEL PROCESO SOPORTE TECNOLÓGICO VERSIÓN 3 ACTA DE MEJORAMIENTO 60 DE ENERO 31 DE 2024

Riesgos de Corrupción
1. Posibilidad de asignación indebida de permisos para el acceso y uso de servicios tecnológicos no autorizados con el fin de obtener beneficio propio o de un tercero.

4.5.2.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias***.

De acuerdo con el análisis realizado por la primera línea de defensa, el contexto estratégico se mantiene hasta culminar la actualización del Mapa de Procesos en la entidad. La actualización del contexto estratégico mediante la matriz DOFA propende a la mejora de servicios y procesos alineado con Gobierno de TI.

El riesgo de corrupción identificado, guarda coherencia con el objetivo estratégico al cual le aporta el proceso "Impulsar una estrategia de transformación digital de la SDP, por medio del desarrollo tecnológico de herramientas que permitan generar valor a los procesos misionales y los servicios digitales de la entidad para los grupos de valor e interés". De igual forma, se observa coherencia entre el riesgo de corrupción identificado y el objetivo del proceso "Fortalecer, administrar y soportar los servicios de las tecnologías de la información y las comunicaciones TIC mediante la gestión integral de su operación, mantenimiento y actualización". Es relevante tener presente los cambios significativos que se reflejarán con la nueva plataforma estratégica, la transición del proceso actualmente "de apoyo" a un proceso "estratégico", la incorporación de lineamientos, interacciones y aspectos propios de la operación de Gobierno de las Tecnologías de Información en la SDP, tal como lo manifiesta el proceso.

Las causas y consecuencias identificadas inicialmente para el riesgo de corrupción se mantienen.

2. ***Autoevaluación de la efectividad de los controles***.

Los controles examinados previenen y mitigan la materialización del riesgo de corrupción, conforme al análisis realizado para cada uno de ellos. Sin embargo, según el monitoreo de la primera línea de defensa, los controles actuales contrarrestan una de las causas, por lo cual se realizará la actualización de los controles en la matriz de riesgos, de tal forma que abarquen todas las causas.

No se tienen hallazgos producto de auditorías, asociados a los controles, de acuerdo con el monitoreo a riesgos de corrupción, llevado a cabo con corte al 30 de abril /2024.

3. ***Autoevaluación de la eficacia de las acciones:***

Se observa que las 2 acciones establecidas en el Plan de Tratamiento del riesgo de corrupción están orientadas a contrarrestar las causas y contribuyen para fortalecer las actividades de los controles, según el análisis adelantado por el proceso, en el marco del monitoreo a riesgos de primera línea de defensa.

Se vienen implementando las acciones formuladas en el Plan de tratamiento al riesgo, en el periodo programado (fecha 12/15/2024), realizando el seguimiento mediante mesas de trabajo con los profesionales responsables de las actividades de mejora, aportando las evidencias correspondientes. Evidencia ID SDP-2024-4315.

De conformidad con el monitoreo a riesgos del presente periodo, el riesgo de corrupción identificado no se ha materializado ni tampoco se ha determinado como hallazgo de ejercicios de auditoria interna o externa.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

El proceso considera que la gestión del riesgo de corrupción "Posibilidad de asignación indebida de permisos para el acceso y uso de servicios tecnológicos no autorizados con el fin de obtener beneficio propio o de un tercero" ha permitido fortalecer sus controles, definiendo acciones de mejora en el plan de tratamiento, logrando contribuir en el cumplimiento del objetivo del proceso de Gobierno de TI. Por lo anterior, se deduce que su gestión le ha sido útil para evitar situaciones o hechos que puedan afectar el cumplimiento de los objetivos y compromisos a su cargo.

5. ***Actualización de Riesgos****:*

Por el momento no se identifica la necesidad de modificar y/o actualizar, el riesgo establecido actualmente ni la necesidad de documentar o incluir nuevos riesgos. No obstante, cuando surja el cambio del proceso a nivel estratégico, se realizará la aleación y actualización requerida.

4.5.2.2 ALERTAS:

No se evidencian situaciones que generen alertas en relación con la posible materialización del riesgo.

4.5.2.3 RECOMENDACIONES:

Continuar con la efectiva gestión a los riesgos, y la ejecución de los controles.

Revisar y validar los riesgos una vez se implemente la plataforma estratégica 2024-2027, y actualizar el contexto estratégico del proceso.

4.5.3 A-LE-521 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DEL PROCESO SOPORTE TECNOLÓGICO VERSIÓN 3 ACTA DE MEJORAMIENTO 74 DE FEBRERO 05 DE 2024

Riesgo de Seguridad de la Información
. Posibilidad de Pérdida de Disponibilidad de los activos de información tipo hardware por fallas y/o mal funcionamiento del equipo, fallas generadas por inadecuadas condiciones físicas y ambientales y hurto de información y/o equipo de cómputo que hacen parte de la infraestructura tecnológica de la Entidad, debido a insuficiente mantenimiento (físico, lógico y aseguramiento), obsolescencia tecnológica tipo hardware, susceptibilidad a las variaciones físicas (humedad, polvo, suciedad, voltaje, temperatura, sensibilidad electromagnética) y acceso al hardware sin protección o protocolos de seguridad. 2. Posibilidad de Pérdida de Integridad de los activos de información tipo hardware que hacen parte de la infraestructura tecnológica de la Entidad por uso no autorizado del equipo, debido al acceso sin protección o protocolos de seguridad. 3. Posibilidad de Pérdida de Disponibilidad en los activos de información tipo software relacionados en el Catálogo de sistemas de información por fallas humanas, destrucción o pérdida de la información, error en el uso o abuso de derechos y privilegios, acceso abusivo a sistema informático, mal funcionamiento de software y explotación de brechas de seguridad en las diferentes capas que soportan la solución de software debido a configuración incorrecta de parámetros, ausencia de copias de respaldo de los sistemas de información, insuficiente aplicación de las políticas de seguridad y privacidad de la información, habilitación de servicios innecesarios, ausencia o insuficiencia de pruebas de software y obsolescencia tecnológica. 4. Posibilidad de Pérdida de Confidencialidad en los activos de información tipo software relacionados en el Catálogo de sistemas de información por fallas humanas, falsificación de derechos de acceso y divulgación ilegal de la información debido a configuración incorrecta de parámetros, gestión deficiente de la contraseñas - contraseñas sin protección y asignación errada de los derechos de acceso. 5. Posibilidad de Pérdida de Confidencialidad por divulgación ilegal de la información, ingeniería social, y uso no autorizado del equipo; relacionada con la información producida por el proceso de gestión tecnológica, debido al desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información, ausencia de validación de autenticación de la información sensible sin cifrado.

4.5.3.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias.***

Si bien el contexto estratégico del proceso A-CA-007 Soporte Tecnológico sigue siendo válido, es importante destacar que la entidad se encuentra en una etapa de implementación de cambios derivados del proceso de rediseño institucional establecido en el Decreto 432 de 2022. Por lo tanto, se deben realizar ajustes en el contexto para alinearlo a la nueva estructura organizacional una vez que se cuente con el mapa de procesos actualizado y aprobado.

Existe una alta coherencia entre los riesgos identificados en el proceso A-CA-007 Soporte Tecnológico y el objetivo estratégico

"Gobierno Digital" de la Secretaría Distrital de Planeación (SDP). A continuación, se detallan los aspectos que fundamentan esta afirmación:

- El objetivo estratégico "Gobierno Digital" busca impulsar una estrategia de transformación digital en la SDP. Esta transformación depende en gran medida de la disponibilidad, integridad y confidencialidad de los activos de información de la entidad.

- Los riesgos identificados en el proceso A-CA-007 Soporte Tecnológico se relacionan directamente con la protección de estos activos de información. La materialización de cualquiera de estos riesgos podría afectar negativamente la implementación del "Gobierno Digital" en la SDP.

Los riesgos identificados afectarían los objetivos institucionales como se describe a continuación:

- Pérdida de disponibilidad de activos de información tipo hardware: podría generar interrupciones en los servicios de TI, lo que dificultaría el acceso a la información y la prestación de servicios digitales a los ciudadanos.

- Pérdida de integridad de activos de información tipo hardware: podría corromper o modificar datos importantes, afectando la confiabilidad de la información y la toma de decisiones.

- Pérdida de confidencialidad de activos de información tipo hardware o software: podría exponer información sensible a terceros no autorizados, lo que podría generar daños a la reputación de la SDP e incluso comprometer la seguridad de los ciudadanos.

En este sentido, la gestión adecuada de los riesgos identificados en el proceso A-CA-007 Soporte Tecnológico es fundamental para garantizar el éxito del objetivo estratégico ""Gobierno Digital"" de la SDP.

Existe una alta coherencia entre los riesgos identificados en el proceso A-CA-007 Soporte Tecnológico y el objetivo de este proceso.

El objetivo del proceso A-CA-007 Soporte Tecnológico es: Garantizar la prestación oportuna y efectiva de los servicios de soporte técnico a los usuarios de la SDP, asegurando la disponibilidad, integridad y confidencialidad de la información. Los riesgos identificados en este proceso se relacionan directamente con la capacidad del proceso para cumplir con este objetivo. La materialización de cualquiera de estos riesgos podría dificultar o impedir el logro del objetivo del proceso, específicamente se pueden mencionar los riesgos de:

- Pérdida de disponibilidad de activos de información tipo hardware: podría generar interrupciones en los servicios de TI, lo que imposibilitaría la prestación de servicios a la ciudadanía y a los usuarios en general.

- Pérdida de integridad de activos de información tipo hardware: podría corromper o modificar datos importantes, dificultando el diagnóstico y la resolución de problemas por parte del personal de soporte técnico.

- Pérdida de confidencialidad de activos de información tipo hardware o software: podría exponer información sensible de los usuarios a terceros no autorizados, lo que podría generar daños a la reputación de la SDP y la pérdida de confianza de los usuarios.

En este sentido, la gestión adecuada de los riesgos identificados en el proceso A-CA-007 Soporte Tecnológico es fundamental para garantizar el cumplimiento del objetivo de este proceso.

En general, las causas identificadas inicialmente para los riesgos en el proceso A-CA-007 Soporte Tecnológico se mantienen vigentes. Por ejemplo:

Riesgo 1: Pérdida de disponibilidad de activos de información tipo hardware.

Las causas identificadas inicialmente (Fallas en el hardware, errores de software, desastres naturales, sabotajes, errores humanos), siguen siendo relevantes. Sin embargo, se debe prestar especial atención a la posibilidad de ataques cibernéticos, que se han convertido en una de las principales amenazas a la disponibilidad de los sistemas de información.

Riesgo 2: Pérdida de integridad de activos de información tipo hardware

Las causas identificadas inicialmente (Fallas en el hardware, errores de software, virus informáticos, errores humanos), siguen siendo relevantes. Sin embargo, se debe prestar especial atención a la posibilidad de ataques cibernéticos dirigidos a corromper o modificar datos intencionalmente.

Riesgo 3: Pérdida de disponibilidad de activos de información tipo software relacionado con:

Las causas identificadas inicialmente (Errores de software, virus informáticos, ataques cibernéticos, errores humanos) siguen siendo relevantes. Sin embargo, se debe prestar especial atención a la obsolescencia del software y a la falta de actualizaciones de seguridad, que pueden incrementar la vulnerabilidad de los sistemas a ataques cibernéticos.

Riesgo 4: Pérdida de confidencialidad de activos de información tipo software
Causas identificadas inicialmente:

Las causas identificadas inicialmente (Errores de software, virus informáticos, ataques cibernéticos, errores humanos, divulgación no autorizada de información) siguen siendo relevantes. Sin embargo, se debe prestar especial atención a la fuga de datos a través de dispositivos móviles y a la ingeniería social, que son técnicas cada vez más utilizadas por los ciberdelincuentes para obtener información confidencial.

Riesgo 5: Pérdida de confidencialidad por divulgación ilegal de la información
Causas identificadas inicialmente:

Las causas identificadas inicialmente (Divulgación no autorizada de información, acceso no autorizado a la información, errores humanos) siguen siendo relevantes. Sin embargo, se debe prestar especial atención a la posibilidad de que el personal interno de la SDP divulgue información confidencial de manera intencional o accidental.

En general, las consecuencias identificadas inicialmente para los riesgos en el proceso A-CA-007 Soporte Tecnológico se mantienen vigentes.
A continuación, se presenta un análisis de las consecuencias identificadas para cada riesgo:

Riesgo 1: Pérdida de disponibilidad de activos de información tipo hardware

Las consecuencias identificadas inicialmente (Interrupción en la prestación de servicios de TI, pérdida de productividad, pérdida de información, daños a la reputación de la SDP.) siguen siendo relevantes. Sin embargo, se debe considerar que el impacto negativo en la prestación de servicios de TI y en la productividad podría ser aún mayor debido a

la creciente dependencia de las tecnologías de la información en las operaciones de la SDP.

Riesgo 2: Pérdida de integridad de activos de información tipo hardware

Las consecuencias identificadas inicialmente (Toma de decisiones erradas, pérdida de información, daños a la reputación de la SDP) siguen siendo relevantes. Sin embargo, se debe considerar que la toma de decisiones erradas basadas en información corrupta podría tener consecuencias aún más graves, como daños financieros o incluso riesgos para la seguridad de las personas.

Riesgo 3: Pérdida de disponibilidad de activos de información tipo software

Las consecuencias identificadas inicialmente (Interrupción en la prestación de servicios de TI, pérdida de productividad, pérdida de información, daños a la reputación de la SDP) siguen siendo relevantes. Sin embargo, se debe considerar que el impacto negativo en la prestación de servicios de TI y en la productividad podría ser aún mayor debido a la creciente dependencia de las aplicaciones de software en las operaciones de la SDP.

Riesgo 4: Pérdida de confidencialidad de activos de información tipo software
Consecuencias identificadas inicialmente:

Las consecuencias identificadas inicialmente (Robo de información confidencial, fraude, extorsión, daños a la reputación de la SDP, pérdida de la confianza de los usuarios) siguen siendo relevantes. Sin embargo, se debe considerar que el robo de información confidencial podría tener un impacto aún más grave en la SDP, como el incumplimiento de normativas legales o la pérdida de clientes.

Riesgo 5: Pérdida de confidencialidad por divulgación ilegal de la información

Las consecuencias identificadas inicialmente (Daños a la reputación de la SDP, pérdida de la confianza de los usuarios, sanciones legales) siguen siendo relevantes. Sin embargo, se debe considerar que las sanciones legales por la divulgación ilegal de información confidencial podrían ser aún más severas, incluyendo multas y penas privativas de libertad. Aunque la entidad está en un proceso de rediseño institucional que afectará la estructura del mapa de procesos, el contexto estratégico del proceso Soporte Tecnológico se mantiene vigente mientras se lleva a cabo la actualización del mapa de procesos.

2. ***Autoevaluación de la efectividad de los controles****.*

En el monitoreo de segunda línea de defensa realizado para el proceso de soporte tecnológico durante el primer trimestre de 2024 se evaluó la efectividad de la gestión de riesgos y el cumplimiento de los controles establecidos para el proceso lo cual de manera muy general se resumen así:

Gestión de Riesgos:

- Se evidencia la actualización anual y verificación aleatoria del plan de mantenimiento de la infraestructura tecnológica.

- Se comprueba la formulación y ejecución anual del plan de acción para la gestión de vulnerabilidades.

- Se verifica la gestión anual de la depuración de usuarios.

- Se comprueba el apoyo al seguimiento de la implementación del Modelo de Seguridad y Privacidad de la Información.

- La definición anual de las aplicaciones críticas y su aseguramiento es adecuada.

- La actualización del versionamiento del software y la migración de soluciones de software a infraestructura asegurada es una práctica adecuada.

- La depuración anual de usuarios es una práctica adecuada.

- La revisión y actualización anual de las políticas de seguridad y privacidad de la información es adecuada.

- El liderazgo del proceso de actualización de los registros de activos de información e índice de información clasificada y reservada de la entidad es adecuado.

Cumplimiento de Controles:

Se comprueba la actualización anual del plan de mantenimiento de la infraestructura tecnológica, la verificación aleatoria del mantenimiento correctivo y el registro de información.

Se verifica la ejecución diaria de la verificación de equipos activos, el registro de inconvenientes y la generación de solicitudes en la herramienta de mesa de ayuda.

Se comprueba la revisión diaria del estado de los servidores de procesamiento y almacenamiento.

Se verifica la generación de controles de cambio informático para acciones sobre la infraestructura tecnológica.

Se verifica la solicitud de asignación de roles para el acceso al equipo de desarrolladores.

Se comprueba la preparación y convocatoria de reuniones al equipo de gestión del cambio.

Se comprueba la ejecución de copias de seguridad diarias de la información.

Se verifica el uso del A-FO-225 para pruebas de software.

Se verifica la realización de evaluaciones de seguridad técnicas.

Se verifica la solicitud del registro del requerimiento con fines de entrega o restauración de datos de pruebas.

Se comprueba el avance en la gestión anual de la depuración de usuarios.

Se comprueba el apoyo al seguimiento de la implementación del Modelo de Seguridad y Privacidad de la Información.

Se verificó la aplicación permanente de la política del directorio activo de bloqueo de pantalla es adecuada.
De otra parte, se analizó los controles para identificar si previenen o mitigan los riesgos dando como resultado el siguiente resultado:

En general, los controles examinados en el monitoreo de segunda línea de defensa demuestran ser efectivos para prevenir o mitigar los riesgos asociados al proceso de soporte tecnológico. La SDP ha implementado una serie de medidas que contribuyen a proteger la confidencialidad, integridad y disponibilidad de los activos de información, tanto hardware como software. La evidencia aportada por la entidad respalda la efectividad de estos controles.

De manera muy sucinta se presenta un resumen del análisis realizado:

Plan de Mantenimiento de Infraestructura Tecnológica: Mitiga el riesgo de pérdida de confidencialidad de activos tipo hardware al reducir la probabilidad de fallas, permitir la detección temprana de problemas y minimizar el impacto en la disponibilidad de la

información. (Evidencia ID SDP-2024-4374, ID SDP-2024-4375)

Monitoreo del Funcionamiento de la Infraestructura: Mitiga el riesgo de pérdida de confidencialidad de activos tipo hardware al permitir la identificación de anomalías, facilitar la toma de medidas correctivas y minimizar el impacto en la disponibilidad de la información. (Evidencia ID SDP-2024-4375)

Controles de Cambio: Mitigan el riesgo de pérdida de confidencialidad de activos tipo hardware al garantizar cambios controlados, permitir la reversión de cambios y minimizar errores que comprometan la confidencialidad. (Evidencia ID SDP-2024-4354)

Gestión de Vulnerabilidades: Mitiga el riesgo de pérdida de confidencialidad de activos tipo hardware al reducir la probabilidad de ataques cibernéticos y fugas de información mediante la identificación y corrección de vulnerabilidades.

Depuración de Usuarios: Mitiga el riesgo de pérdida de confidencialidad y de integridad de activos tipo hardware al reducir la probabilidad de accesos no autorizados y ataques cibernéticos, minimizando el impacto de incidentes de seguridad y protegiendo la información almacenada. (Evidencia ID SDP-2024-4356)

Modelo de Seguridad y Privacidad de la Información (MSPI): Mitiga el riesgo de pérdida de integridad de activos tipo hardware al proporcionar un marco para la gestión de incidentes de seguridad, minimizar la probabilidad de incidentes y proteger la integridad de la información.

Acompañamiento y Monitoreo a Proveedores de Servicios: Mitiga el riesgo de pérdida de integridad de activos tipo hardware al velar por el cumplimiento de estándares de seguridad por parte de proveedores, permitiendo la identificación y el abordaje de problemas de seguridad y minimizando la probabilidad de incidentes relacionados con proveedores.

Inspección a Controles de Acceso Físico: Mitiga el riesgo de pérdida de integridad de activos tipo hardware al prevenir accesos no autorizados a instalaciones y equipos, permitiendo la identificación y el abordaje de violaciones de seguridad física y minimizando la probabilidad de robos, sabotajes y otras acciones que afecten la integridad de la información.

Verificación de la Aplicación de Controles de Acceso a Áreas Seguras: Mitiga el riesgo de pérdida de integridad de activos tipo hardware al restringir el acceso a información y activos, permitir la identificación de accesos no autorizados a áreas seguras y minimizar la probabilidad de robos, sabotajes y fugas de información.

Asignación de Roles y Permisos de Acceso: Mitiga el riesgo de pérdida de disponibilidad de activos tipo software al controlar el acceso a la información y sistemas por parte del equipo de desarrollo, reduciendo la probabilidad de errores y accesos no autorizados que afecten la disponibilidad del software.

Revisión y Aprobación de Controles de Cambio Informático: Mitiga el riesgo de pérdida de disponibilidad de activos tipo software al garantizar que los cambios no afecten la estabilidad y seguridad de los sistemas, permitiendo revertir cambios y fortalecer mecanismos para minimizar la probabilidad de fallas y vulnerabilidades.

Copias de Seguridad Periódicas: Mitigan el riesgo de pérdida de disponibilidad de activos tipo software al permitir la restauración de la información en caso de fallas o ataques cibernéticos, minimizando el impacto en la

disponibilidad del software y facilitando la recuperación rápida del servicio.

Análisis de Vulnerabilidades del Software Propietario: Mitiga el riesgo de pérdida de disponibilidad de activos tipo software al reducir la probabilidad de ataques cibernéticos y fugas de información, minimizando el impacto de incidentes de seguridad y protegiendo la información almacenada en el software.
Pruebas Funcionales y No Funcionales: Mitigan el riesgo de pérdida de disponibilidad de activos tipo software al permitir la identificación y corrección de errores antes del despliegue en producción, reduciendo la probabilidad de fallas y problemas en el funcionamiento del software y minimizando el impacto en la disponibilidad en caso de errores.

Revisiones del Cumplimiento del SGSI: Mitigan el riesgo de pérdida de disponibilidad de activos tipo software al velar por el cumplimiento de estándares de seguridad y privacidad, proporcionar un marco para la gestión de incidentes y la toma de medidas correctivas, y minimizar la probabilidad de incidentes que afecten la disponibilidad del software.

Implementación de Certificados Seguros: Mitiga el riesgo de pérdida de confidencialidad de activos tipo software al proteger la información confidencial mediante cifrado y autenticación, propender por la integridad de la información y evitar la suplantación de identidad, minimizando la probabilidad de interceptación y robo de información confidencial.

Actualización Periódica del Software Base y Migración de Soluciones de Software a Infraestructura Asegurada: Mitiga el riesgo de pérdida de confidencialidad de activos tipo software al corregir vulnerabilidades, mejorar la seguridad de la información, reducir la probabilidad de ataques cibernéticos y fugas de información, y minimizar el impacto de incidentes de seguridad.

Registro de Requerimientos para Entrega o Restauración de Datos de Pruebas: Mitiga el riesgo de pérdida de confidencialidad de activos tipo software al controlar el acceso a la información de pruebas, evitar el uso indebido de la misma, reducir la probabilidad de errores y fugas de información, y permitir la identificación de la causa del problema y la toma de medidas correctivas en caso de errores o fugas de información relacionadas con datos de pruebas.

Gestión de Usuarios y Control de Acceso a Datos y Aplicaciones: Mitiga el riesgo de pérdida de confidencialidad de activos tipo software al restringir el acceso a la información y sistemas a personas autorizadas, permitir la identificación y el abordaje de accesos no autorizados, minimizar la probabilidad de fugas de información confidencial, y facilitar la investigación de incidentes de seguridad.

Revisión y Actualización de Políticas de Seguridad y Privacidad: Mitiga el riesgo de pérdida de confidencialidad por divulgación ilegal de la información al mantener las políticas actualizadas con los estándares más recientes, reducir la probabilidad de incidentes de seguridad que puedan ocasionar fugas de información confidencial, y facilitar la identificación de las causas de un incidente de seguridad y la toma de medidas correctivas adecuadas.

Aplicación de la Política de Bloqueo de Pantalla: Mitiga el riesgo de pérdida de confidencialidad por divulgación ilegal de la información al proteger la información confidencial en caso de que los equipos queden sin supervisión, reducir la probabilidad de accesos no autorizados y fugas de información, y minimizar el impacto de un incidente de seguridad en caso de que ocurra.

Actualización del Formato A-FO-209 para la Actualización de Registros de Activos de Información: Mitiga el riesgo de pérdida de confidencialidad por divulgación ilegal de la información al facilitar la identificación, clasificación y protección de la información de la SDP, reducir la probabilidad de pérdida, robo o acceso no autorizado a la información confidencial, y permitir la identificación rápida de la información afectada en caso de un incidente de seguridad.

En general, los controles examinados en el monitoreo de segunda línea de defensa demuestran ser efectivos para prevenir o mitigar los riesgos asociados al proceso de soporte tecnológico. La SDP ha implementado una serie de medidas que contribuyen a proteger la confidencialidad, integridad y disponibilidad de los activos de información, tanto hardware como software. La evidencia aportada por la entidad respalda la efectividad de estos controles.

Por último, en la autoevaluación de la efectividad de los controles, de acuerdo con las respuestas de líder del proceso no tiene evidencia que exista hallazgos relacionados con los riesgos de seguridad de la información identificados y los controles aplicados. Sin embargo, para el presente monitoreo se observó y aplico lo mencionado en el Informe Definitivo de Auditoría de Seguimiento del ICONTEC, según Rad. 3-2023-37838 se establece que el requisito 6.1 Acciones para abordar riesgos y oportunidades, entre otros se auditaron transversalmente por muestreo, se apropian las oportunidades de mejora identificadas por ICONTEC, aplicadas al Proceso liderado por la Dirección de TIC sobre Riesgos:
* Reconsiderar el “desconocimiento” como causa de los riesgos; es necesario profundizar más en los análisis para determinar las causas de raíz. Esto permitirá adoptar controles de mayor eficacia en la prevención de la materialización de los riesgos.
* Es conveniente verificar si los controles adoptados son de tipo preventivo; esto es importante ya que la sobrevaloración de controles (preventivo en lugar de detectivos) podría conducir a una valoración del riesgo residual que no corresponde al nivel de protección de la entidad.

Situaciones Susceptibles de Mejora según Rad. 3-2023-32707 sobre Informe de Seguimiento a la Gestión Riesgos de Corrupción de la SDP de la Oficina de Control Interno con corte al 31/08/2023: “Se identificó que en los seguimientos de la primera línea de defensa no se hace mención del monitoreo de los controles, por lo que se recomienda tanto para la primera como para la segunda línea de defensa para los futuros seguimientos compararlos con las evidencias y poder identificar su efectividad para evitar la materialización de estos riesgos".

3. ***Autoevaluación de la eficacia de las acciones:***

Respecto de si las acciones formuladas para dar tratamiento al riesgo están orientadas a contrarrestar sus causas, El Líder del Proceso respondió:

Depuración de Usuarios: Contrarresta el acceso no autorizado, el uso indebido de accesos y los errores humanos.

Plan de Capacitación y Sensibilización: Contrarresta la falta de conocimiento de las políticas de seguridad, los comportamientos inseguros y la falta de cultura de seguridad.

Análisis:
Las acciones descritas por el líder del proceso se encuentran alineadas con las causas identificadas para los riesgos R1, R2, R3 y R4. La depuración de usuarios permite eliminar accesos innecesarios y reducir la probabilidad de accesos no autorizados, mientras que el plan de capacitación y sensibilización

contribuye a fortalecer el conocimiento y la cultura de seguridad de los funcionarios.

En cuanto a la Implementación Adecuada de las Acciones, el Líder del Proceso respondió: Se realiza un seguimiento periódico a la ejecución de las acciones. Desde el proceso se generan evidencias para demostrar el cumplimiento.

Análisis:
La respuesta del líder del proceso indica que existe un mecanismo para verificar la implementación efectiva de las acciones definidas en el plan de acción. Este seguimiento y la generación de evidencias son fundamentales para garantizar la eficacia de las acciones y la mitigación de los riesgos.

Para conocer si existe la materialización del Riesgo o Hallazgos de Auditoría, el Líder del Proceso respondió:

No se ha evidenciado la materialización de los riesgos.
No se han encontrado hallazgos de auditoría interna o externa relacionados.

Análisis:
La información proporcionada por el líder del proceso es positiva, ya que indica que los riesgos identificados no se han concretado en incidentes de seguridad ni han sido detectados en auditorías. Esto sugiere que las acciones de mitigación y los controles implementados han sido efectivos.

Con relación a las correcciones y/o Acciones Correctivas ante la Materialización del Riesgo, el Líder del Proceso contestó:

No se ha identificado la materialización de los riesgos.
No se han formulado correcciones ni acciones correctivas.

Análisis:

Dado que no se ha presentado la materialización de los riesgos, no es necesario implementar correcciones ni acciones correctivas en este momento. Sin embargo, es importante mantener la vigilancia y el seguimiento continuo de los riesgos para detectar cualquier cambio en su probabilidad o impacto potencial.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

En este punto se centró la atención en la utilidad de la Gestión del Riesgo para Evitar Afectaciones al Cumplimiento de Objetivos y Compromisos. El Líder del Proceso respondió a esta pregunta así:

La gestión de riesgos ha sido útil para:

- Proteger la información de la SDP y garantizar la continuidad del negocio.
- Cumplir los objetivos y compromisos.
- Ha contribuido a prevenir situaciones o hechos con impacto negativo en las operaciones de la SDP.
- Ha permitido mantener la disponibilidad, integridad y confidencialidad de la información de la SDP.

Análisis:
La respuesta del líder del proceso destaca la importancia y los beneficios de la gestión de riesgos para la SDP. La implementación de un proceso adecuado de gestión de riesgos ha permitido proteger los activos de información, garantizar la continuidad de las operaciones y cumplir con los objetivos y compromisos de la organización.

Entre las evidencias que respaldan la Efectividad se encuentran las siguientes:

- No se ha presentado la materialización de los riesgos identificados.
- Se han implementado controles efectivos para mitigar los riesgos.
- Se ha mantenido la disponibilidad, integridad y confidencialidad de la información.
- La SDP ha cumplido con sus objetivos y compromisos.

En conclusión, la gestión de riesgos ha demostrado ser una herramienta valiosa para la SDP, contribuyendo a la protección de la información, la continuidad del negocio y el cumplimiento de los objetivos. La ausencia de incidentes de seguridad y el cumplimiento de las metas son indicadores claros de la efectividad de la gestión implementada.

5. ***Actualización de Riesgos****:*

Si bien el rediseño institucional de la SDP en 2022 (Decreto 432 de 2022) podría haber generado cambios en la forma en que opera la entidad, la falta de documentación formal sobre estos cambios dificulta la evaluación de su impacto en los riesgos identificados. Es necesario contar con información clara y precisa sobre los cambios realizados para determinar si es necesario modificar o actualizar los riesgos establecidos.

En este momento no es necesario modificar o actualizar los riesgos establecidos, ni documentar y gestionar nuevos riesgos. Sin embargo, es importante mantener un enfoque vigilante y proactivo en la gestión de riesgos. La definición del nuevo contexto estratégico y los mapas de proceso, junto con un análisis periódico de los riesgos, permitirán identificar y gestionar adecuadamente cualquier nuevo riesgo que pueda surgir.

4.5.3.2 ALERTAS:

De acuerdo con el monitoreo de primera línea de defensa referente a los riesgos identificados de seguridad de la información del Proceso de Soporte Tecnológico, no se reportan alertas que indiquen que los riesgos se han materializado

4.5.3.3 RECOMENDACIONES:

Se recomienda que, aunque no se identifica la necesidad de documentar y gestionar nuevos riesgos en este momento, se sugiere realizar evaluaciones periódicas del entorno operativo y tecnológico para identificar posibles riesgos emergentes. Además, se recomienda fomentar una cultura de gestión proactiva de riesgos en toda la entidad para garantizar una respuesta rápida y efectiva ante cualquier cambio en el panorama de riesgos.

Si bien los controles implementados son adecuados, se recomienda continuar con el monitoreo y la evaluación periódica de su efectividad. Es importante mantener los controles actualizados y adaptados a las nuevas amenazas y vulnerabilidades. Además, se recomienda fortalecer la capacitación del personal adscrito al interior del proceso en materia de seguridad de la información para garantizar un uso adecuado de los controles y la prevención de incidentes de seguridad.

Se recomienda revisar los controles existentes y las acciones planteadas teniendo en cuenta que al interior del proceso se está migrando y actualizando herramientas tecnológicas como lo son subversión, la nueva versión de mesa de ayuda GLPI. y la implementación del SGDA, entre otros. Esta situación sugiere un nuevo ambiente tecnológico que requiere identificar posibles áreas de mejora y asegurar la efectividad en la gestión del riesgo.

Se recomienda continuar con el proyecto para implementar un sistema de monitoreo continuo de riesgos que permita identificar y abordar proactivamente nuevas amenazas y vulnerabilidades a medida que surjan. Esto implica el uso de herramientas de detección de amenazas y análisis de seguridad avanzadas.

Se recomienda continuar con la implementación del módulo de seguridad de la información del sistema de gestión GESTIONATE con el fin de permitir monitorear y evaluar la implementación de los planes de acción formulados para abordar los riesgos identificados. Esto garantizaría que las acciones correctivas se implementen de manera oportuna y efectiva.

Se recomienda la adopción del estándar ISO 27001:2022, para fortalecer aún más la gestión de la seguridad de la información y garantizar el cumplimiento de las mejores prácticas en el proceso de soporte tecnológico.

Se recomienda participar en las sesiones de capacitación y sensibilización en temas de seguridad y privacidad de la información programadas por la entidad.

4.6 CONTRATACIÓN DE BIENES Y SERVICIOS

4.6.1 A-LE-304 MAPA DE RIESGOS DE GESTIÓN DEL PROCESO CONTRATACIÓN DE BIENES Y SERVICIOS VERSIÓN 7 ACTA DE MEJORAMIENTO 183 DE ABRIL 30 DE 2024

Riesgos de Gestión

1. Posibilidad de afectación económica y reputacional por inexactitud en la identificación y/o descripción de los requisitos técnicos, que no permitan satisfacer la necesidad de la entidad y/o la adquisición de bienes, productos o servicios no requeridos, que conlleven a sanciones del respectivo ente de control, debido a falencias en la estructuración de los documentos precontractuales (información y documentación incompleta).

2. Posibilidad de afectación económica y reputacional por no recepción de ofertas y/o imposibilidad para la selección de la oferta más favorable, generando reprocesos que impiden la correcta ejecución del PAA, debido a la solicitud de requisitos que no cumplen los oferentes del sector, desconocimiento o mal uso del SECOP II, por parte del oferente.

3. Posibilidad de afectación económica y reputacional por falencias en el ejercicio de la supervisión e interventoría debido a un deficiente seguimiento a obligaciones del contrato a cargo del contratista, que conlleve a la declaratoria de incumplimiento del contrato (parcial o total) y/o investigaciones del respectivo ente de control, debido a desconocimiento de la rigurosidad de la función, falta de comunicación oportuna frente a inconvenientes en la ejecución de los contratos y/o designación de supervisor que no cuenta con los conocimientos requeridos para ejercer la función, gran cantidad de contratos a vigilar-supervisar que sobrepasan la capacidad laboral del supervisor.

4.6.1.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias.***

Se pueden identificar mejoras en el proceso, según el enfoque que se le dé al Plan Distrital de Desarrollo 2024-2028, al igual que durante el proceso de formulación de la Planeación Estratégica.

2. ***Autoevaluación de la efectividad de los controles.***

Se incluyó la lista de los contratos y su ubicación en SECOP II, dentro del repositorio de evidencias de la SDP. Se sugiere cargar como evidencia un caso específico de cada etapa del proceso contractual: Solicitud contractual, verificación de los documentos por parte del Comité Evaluador, la gestión del supervisor en el cumplimiento del objeto contractual, y su aprobación para pago, así como el cumplimiento en la elaboración del acta de recibo final.

3. ***Autoevaluación de la eficacia de las acciones:***

Debido a que las opciones de tratamiento del nivel de riesgo bajo y moderado es de reducir el riesgo por medio de la aplicación de los controles existentes, no se generó un plan de acción de tratamiento. Dentro de las actividades del Plan Operativo Anual del proceso se definió para la vigencia 2024 la actividad de Realizar un (1) taller sobre la

etapa precontractual proceso de Contratación Estatal - Estudios y Documentos Previos, realizar un (1) taller sobre el ejercicio de la supervisión de contratos (Etapa contractual), realizar un taller sobre la etapa postcontractual - Liquidación de contratos y adelantar un taller sobre el uso, manejo oportuno y roles y responsabilidades del SECOP II.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

Por medio del radicado 3-2024-17585 del 16 de mayo de 2024, la Dirección de Contratación realizó la citación a las Subsecretarías para dar a conocer la nueva versión del Manual Integrado de Contratación, en la que se mejoran las actividades del proceso.

5. ***Actualización de Riesgos****:*

Como resultado del monitoreo de segunda línea de defensa de los riesgos de gestión del proceso de Contratación de Bienes y Servicios, no se ha identificado la necesidad de modificar o de documentar y gestionar nuevos riesgos.

4.6.1.2 ALERTAS:

Con la implementación de la nueva versión del Manual Integrado de Contratación, publicado el 25 de abril de 2024, en su versión 10, cuya vigencia inicia a partir del 01 de junio de 2024, según la Resolución 0701 de 2024, se pueden identificar nuevas causas asociadas a los riesgos.

4.6.1.3 RECOMENDACIONES:

Según el Plan Anual de Auditoría publicado en la página web de la SDP: https://www.sdp.gov.co/sites/default/files/control/paa_2024_version_2.pdf, se tiene programado realizar la auditoría al proceso de Contratación de Bienes y Servicios del 02 de julio al 15 de octubre de 2024, por lo que se deben tener disponibles las evidencias de aplicación de los controles.

4.6.2 A-LE-528 MAPA DE RIESGOS DE CORRUPCIÓN DEL PROCESO CONTRATACIÓN DE BIENES Y SERVICIOS VERSIÓN 1 ACTA DE MEJORAMIENTO 2 DE ENERO 31 DE 2024

Riesgos de Corrupción

1. Posibilidad de direccionamiento o ajuste de los estudios previos y demás documentos de las etapas de planeación y selección del proceso de contratación, en favor de un tercero, omitiendo el cumplimiento del principio de selección objetiva (Etapa Precontractual).

2. Posibilidad de ejercer la supervisión o interventoría de contratos de manera desleal o interés ilícito en su ejercicio a través de la manipulación y/o extralimitación y/u omisión de funciones en beneficio del contratista o de un tercero (Etapa Contractual - Postcontractual).

4.6.2.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias.***

Las causas para los riesgos de corrupción se mantienen debido a que la manipulación de los estudios previos deficientes y un ejercicio de supervisión deficiente, pueden generar un direccionamiento en la etapa de selección del proceso de contratación y una posterior supervisión con un interés ilícito.

Las consecuencias de los riesgos de corrupción identificados se relacionan con la pérdida de confianza de la entidad, afectando su reputación y la intervención de los órganos de control, de la Fiscalía u otro ente y da lugar a procesos sancionatorios y disciplinarios.

2. ***Autoevaluación de la efectividad de los controles.***

El diseño de los controles permite prevenir y mitigar los riesgos debido a que desde la Dirección de Contratación se verifican los formatos de solicitud contractual y que contengan la consulta realizada por el Oficial de Cumplimiento de la entidad.

3. ***Autoevaluación de la eficacia de las acciones:***

Las actividades del Plan de Tratamiento de los riesgos de corrupción del proceso de Contratación de Bienes y Servicios, responden a las causas de los riesgos y se complementan con la socialización de la nueva versión del Manual Integrado de Contratación

No se ha identificado la materialización del mapa de riesgos de Corrupción del proceso.

4. ***Evaluación de la efectividad de la gestión de los riesgos:***

La gestión del riesgo permite identificar, analizar y evaluar los escenarios en que los resultados del proceso se desvíen de los objetivos establecidos, y en consecuencia adoptar las medidas oportunas; de este modo, la incertidumbre vinculada al riesgo se atenúa en gran medida.

5. ***Actualización de Riesgos:***

Como resultado del monitoreo de segunda línea de defensa de los riesgos de gestión del proceso de Contratación de Bienes y Servicios, no ha identificado la necesidad de documentar nuevos riesgos. Se sugiere incluir la gestión de conflicto de intereses en el control del riesgo de los nuevos riesgos que se definan en la herramienta gestiónate en el segundo semestre de 2024.

4.6.2.2 ALERTAS:

No se presentan alertas en la aplicación de los controles y tratamientos del mapa de riesgos de corrupción del proceso de Contratación de Bienes y Servicios.

4.6.2.3 RECOMENDACIONES:

Se pueden incluir evidencias adicionales de la ejecución de los controles, como la actualización del Manual Integrado de Contratación, Versión 10 del 25 de abril de 2024. Tener en cuenta los cambios que se están generando en el A-FO-072 Certificado de Cumplimiento para pago y la creación del formato A-FO-548 Informe de ejecución y seguimiento - Contrato y/o Convenio, el registro de reuniones de las asesorías o estadísticas de los temas consultados por las áreas solicitantes y los controles relacionados con SARLAFT. Continuar con la aplicación de los controles por parte de la primera línea de defensa, tal como se ha desarrollado.

4.6.3 A-LE-529 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DEL PROCESO CONTRATACIÓN DE BIENES Y SERVICIOS VERSIÓN 2 ACTA DE MEJORAMIENTO 152 DE ABRIL 30 DE 2024

Riesgo de Seguridad de la Información

1. Posibilidad de Perdida de Integridad por fallas humanas o destrucción de la información o error en el uso o abuso de derechos y privilegios o falsificación de derechos de acceso de documentos que conforman el expediente contractual (formatos, minutas, actas, comunicaciones y demás que se expidan con ocasión a la ejecución del contrato/convenio), debido al manejo manual de la información o ausencia de copias de respaldo de la información o ausencia de validación de autenticación de la información o retraso en la entrega de información por parte del personal o insuficiente entrenamiento y capacitación sobre políticas de seguridad y privacidad de la información o ausencia o deficiencia en los sistemas de autenticación de los aplicativos.

4.6.3.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias***.

El contexto estratégico identificado por el proceso se mantiene. El mapa de riesgos ha sido actualizado y la información se ha actualizado con el nuevo Manual Integrado de Contratación, lo que garantiza que el riesgo está alineado con los objetivos estratégicos de la SDP. No obstante, en aplicación del Decreto 432 de 2022 y la formulación del Plan de desarrollo Distrital, se espera para mediados del mes de junio de 2024, actualizar todos los mapas de procesos haciendo necesario realizar un nuevo análisis para determinar los cambios que se requieran para mantener la alineación al nuevo el contexto estratégico.

El riesgo identificado es coherente con el objetivo estratégico al cual le aporta el proceso. La pérdida de integridad de la información contractual puede afectar negativamente la imagen y la reputación de la SDP, lo que dificultaría el logro de sus objetivos estratégicos.

El riesgo identificado es coherente con el objetivo del proceso objeto del seguimiento. La pérdida de integridad de la información contractual puede afectar la eficiencia y la transparencia del proceso de contratación, lo que dificultaría el logro de su objetivo de adquirir bienes y servicios de manera eficiente y transparente.

De acuerdo con la puesta en marcha del Mapa de Riesgos, es posible afirmar que las causas identificadas inicialmente para el riesgo se mantienen. Las causas del riesgo, como las fallas humanas, la destrucción de la información y el error en el uso de permisos de acceso, siguen siendo relevantes en el contexto actual.

Así mismo, las consecuencias identificadas inicialmente para el riesgo se mantienen. Las consecuencias del riesgo, como el daño a la imagen y la reputación de la SDP, la pérdida de información confidencial y la afectación de la eficiencia y transparencia del proceso de contratación, siguen siendo relevantes en el contexto actual.

2. ***Autoevaluación de la efectividad de los controles***.

El proceso presentó diapositivas que demuestran el seguimiento al PAA-2023, EVIDENCIA SDP-2024-4302, Este archivo hace parte de los registros de las actividades realizadas en el marco de la implementación de los controles. Así mismo, se mencionan

controles como las jornadas de inducción y reinducción, las copias de seguridad, la gestión de usuarios evidenciada en el registro de Mesa de ayuda (incidencias) Sistema de Requerimientos. Al revisar las evidencias aportadas para este monitorio, no se encontraron registros relacionados o muestras que de manera suficiente demuestre la utilización de los últimos controles mencionados. Se recomienda adjuntar las evidencias necesarias en el próximo seguimiento.

De acuerdo con lo establecido en el mapa de riesgos y la respuesta del Líder del proceso en el primer monitoreo, los controles examinados previenen o mitigan los riesgos así:

Control 1: Sesiones de inducción y reinducción al personal, contribuye en la Prevención/Mitigación. Las sesiones informan al personal sobre las políticas y procedimientos de seguridad de la información de la SDP, incluyendo la importancia de proteger la información confidencial, la correcta gestión de permisos de acceso y la prevención de errores humanos. Esto ayuda a reducir la probabilidad de fallas humanas que puedan ocasionar pérdida de integridad de la información. Así mismo, las sesiones educan al personal sobre los riesgos asociados al manejo de la información contractual, como la pérdida, robo o acceso no autorizado a documentos. Esto permite al personal estar alerta y tomar medidas preventivas para proteger la información.

Control 2: Copias de seguridad periódicas, este control previene y/o mitiga el riesgo dado que las copias de seguridad garantizan la recuperación de la información en caso de pérdida o daño accidental, ataques cibernéticos o fallas en los sistemas. Esto minimiza el impacto de eventos adversos que puedan afectar la integridad de la información contractual. Las copias de seguridad también permiten restaurar la información en caso de errores o fallos en los sistemas, evitando la pérdida permanente de datos y asegurando la continuidad del proceso de contratación.

Control 3: Verificación de la información a tramitar, la verificación de la información a tramitar asegura que los documentos y datos sean completos, precisos y consistentes con los lineamientos establecidos por la SDP. Esto reduce la probabilidad de errores que puedan afectar la integridad de la información contractual. La revisión de la información permite detectar inconsistencias o anomalías que podrían indicar intentos de fraude o manipulación de datos, protegiendo la integridad del proceso de contratación.

Control 4: Cumplimiento de plazos, el cumplimiento de plazos evita retrasos en el proceso de contratación, lo que reduce la posibilidad de errores o pérdida de información por falta de tiempo, permite gestionar de manera adecuada los riesgos asociados al proceso de contratación, minimizando la probabilidad de incumplimientos o eventos adversos que puedan afectar la integridad de la información.

Control 5: Sesiones de sensibilización sobre seguridad de la información, las sesiones de sensibilización crean conciencia sobre la importancia de la seguridad de la información en la SDP, promoviendo prácticas seguras entre el personal. Esto reduce la probabilidad de errores humanos que puedan comprometer la integridad de la información contractual. De la misma manera, la sensibilización permite al personal identificar y reportar posibles riesgos o incidentes de seguridad relacionados con la información contractual, facilitando la toma de medidas preventivas y correctivas.

Control 6: Plan de sensibilización de Seguridad de la Información, El plan de

sensibilización en seguridad de la información de la SDP, abarca diversos aspectos de la seguridad de la información, como la protección de datos, la gestión de contraseñas, el uso responsable de dispositivos y la prevención de ataques cibernéticos. Esto proporciona al personal las herramientas y conocimientos necesarios para proteger la integridad de la información contractual. En este punto se resalta que el plan de sensibilización se desarrolla de manera continua, asegurando que los servidores públicos, contratistas y pasante de la SDP se mantenga actualizado sobre las últimas amenazas y mejores prácticas en materia de seguridad de la información.

No se han identificado hallazgos de auditoría asociados a los controles examinados. Las auditorías realizadas al proceso no han encontrado falencias en la implementación o aplicación de los controles.

3. ***Autoevaluación de la eficacia de las acciones:***

Los controles formulados para dar tratamiento al riesgo están orientadas a contrarrestar sus causas. Las acciones se enfocan en la capacitación del personal, las copias de seguridad, la verificación de la información, el cumplimiento de plazos, la sensibilización sobre seguridad de la información y la revisión de equipos críticos. Estas acciones abordan directamente las causas del riesgo, como las fallas humanas, la pérdida de información y el uso indebido de permisos de acceso.

Las acciones formuladas en el plan de acción están orientadas a contrarrestar las causas del riesgo. La revisión de equipos críticos y la gestión de usuarios con permisos de acceso a la información contractual abordan directamente las fallas humanas, la pérdida de información y el uso indebido de permisos de acceso, que son las principales causas del riesgo identificado.

De acuerdo con la información reportada por el proceso, se observa un avance en la implementación de las acciones formuladas en el plan de acción. La SDP ha realizado la actualización de equipos de escritorio a escritorios virtuales con alta disponibilidad para respaldo de información, y está en proceso de realizar la revisión anual de usuarios con permisos de acceso a la información contractual. Se evidencia un compromiso con la ejecución del plan de acción.

Se recomienda para el siguiente monitoreo, adjuntar evidencia mediante la cual se puede sustentar las afirmaciones anteriores.

El riesgo identificado no se ha materializado ni se ha determinado como hallazgo en auditorías internas o externas. La ausencia de eventos adversos y el avance en la implementación del plan de acción indican que el riesgo sigue bajo control. Dado que el riesgo no se ha materializado, no ha sido necesario formular correcciones o acciones correctivas.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

Tomando como base la información aportada por el proceso, se concluye que la gestión del riesgo ha sido útil para evitar situaciones o hechos que puedan afectar el cumplimiento de los objetivos y compromisos del proceso de contratación de bienes y servicios. La ausencia de hallazgos en auditorías, el avance en la implementación del plan de acción y la efectividad de los controles implementados demuestran que la gestión del riesgo ha contribuido a mantener la integridad de la información contractual y a prevenir eventos adversos que podrían afectar el cumplimiento de los objetivos del proceso.

5. ***Actualización de Riesgos**:*

No se identifica la necesidad de modificar o actualizar el riesgo de pérdida de integridad en este momento. El mapa de riesgos se encuentra actualizado, alineado con el marco normativo vigente y la gestión del riesgo ha demostrado ser efectiva.

Con corte a 30 de abril de 2024, no se identifican nuevos riesgos asociados al proceso de contratación de bienes y servicios que requieran ser documentados y gestionados en este momento. El análisis realizado no ha evidenciado la necesidad de incluir nuevos riesgos en el mapa de riesgos.

4.6.3.2 ALERTAS:

De acuerdo con el monitoreo de primera línea de defensa referente a los riesgos identificados de seguridad de la información del Proceso de contratación de Bienes y Servicios, no se reportan alertas que indiquen que los riesgos se han materializado.

4.6.3.3 RECOMENDACIONES:

Se recomienda considerar la implementación de medidas adicionales de control o la revisión de los planes de acción existentes considerando los cambios en el entorno operativo o normativo que puedan afectar la seguridad de la información contractual.

Se recomienda formular acciones que estén directamente relacionadas con el proceso de modo que no dependan de otras áreas para su cumplimiento.

Se recomienda realizar el seguimiento de los planes de acción formulados y que están en curso con el fin de identificar si existe retrasos en su ejecución y las causas que dificultan su culminación.

Se recomienda seguir con la implementación de controles y el soporte de estos como se evidencia hasta el momento, en pro de seguir mejorando la efectividad de los controles de seguridad de la información que están operativos actualmente en la entidad.

Se recomienda asistir y participar activamente en las jornadas de capacitación y sensibilización en temas de seguridad y privacidad de la información programadas por la entidad.

4.7 SOPORTE LEGAL

4.7.1 A-LE-456 MAPA DE RIESGOS DE GESTIÓN DEL PROCESO SOPORTE LEGAL VERSIÓN 5 ACTA DE MEJORAMIENTO 107 DE FEBRERO 21 DE 2024

Riesgos de Gestión

1. Posibilidad de afectación económica y reputacional por incremento en fallos condenatorios en contra de la entidad y mala imagen institucional, debido a inadecuada apropiación de los temas, sistemas de información y términos de respuesta.

4.7.1.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias***.

Mediante radicado en SIPA 3-2024-16639 del 8 de mayo la Subsecretaría Jurídica remitió a la Dirección de Planeación Institucional el monitoreo de primera línea de defensa a los riesgos de Gestión y Seguridad de la información del proceso Soporte Legal.

Para el periodo de monitoreo no se han identificado cambios significativos en el contexto estratégico del proceso.

El riesgo de gestión identificado para el proceso: "Posibilidad de afectación económica y reputacional por incremento en fallos condenatorios en contra de la entidad y mala imagen de institucional, debido a inadecuada apropiación de los temas, sistemas de información y términos para dar respuesta" guarda coherencia con el objetivo estratégico el objetivo estratégico "Fortalecer la estructura y la cultura institucional para contribuir a una gestión pública efectiva, mediante el desarrollo de habilidades para el talento humano, simplificación de procesos, mecanismos eficientes para la toma de decisiones y mejora continua".

El riesgo es coherente con el objetivo del proceso, el cual se orienta a la "Asesoría y representación jurídica de la SDP a través de la revisión y proyección de actos administrativos y conceptos y la representación judicial y extrajudicial".

Conforme a la información del monitoreo de la primera línea de defensa, las causas y consecuencias identificadas para el riesgo de gestión se mantienen. En este sentido, se asume que no se han evidenciado situaciones que generen alerta o indiquen que las causas y/o consecuencias cambien o se modifiquen, en el marco de la administración del riesgo.

2. ***Autoevaluación de la efectividad de los controles***.

Conforme a lo indicado por el proceso en el monitoreo de primera línea de defensa, el control previene y mitiga los riesgos; así como se refleja en la información aportada respecto a la aplicación de los controles. De igual forma, no se evidencian hallazgos de auditoría asociados a los controles establecidos.

3. ***Autoevaluación de la eficacia de las acciones:***

No se formularon acciones en el marco del Plan de tratamiento al riesgo, dado el resultado Moderado del análisis de la zona del riesgo Inherente.

No se evidencia materialización ni hallazgos en las auditorías internas o externas

relacionados con el riesgo de gestión del proceso.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

De acuerdo con la información reportada por la primera línea de defensa y las evidencias de la aplicación efectiva de los controles formulados para el riesgo de gestión, se puede deducir que la gestión del riesgo ha permitido evitar situaciones que afecten el cumplimiento de los objetivos y compromisos a cargo del proceso.

5. ***Actualización de Riesgos****:*

Para el periodo del monitoreo, no se identificó la necesidad de modificar o actualizar el actual riesgo de gestión, ni tampoco la necesidad de documentar o gestionar nuevos riesgos de este tipo.

4.7.1.2 ALERTAS:

No se generan alertas por eventos que indiquen materialización del riesgo de gestión identificados para el proceso, teniendo en cuenta la efectividad en la aplicación de los controles y la adecuada administración del riesgo.

4.7.1.3 RECOMENDACIONES:

Continuar con la efectiva gestión a los riesgos, y la ejecución de los controles.

Revisar y validar los riesgos una vez se implemente la plataforma estratégica 2024-2027, y actualizar el contexto estratégico del proceso.

Fortalecer los argumentos que se registran en la columna Observaciones, así como la presentación de las evidencias (en el repositorio dispuesto), con el propósito de optimizar los resultados del seguimiento que contribuyan a la mejora en la gestión del riesgo.

4.7.2 A-LE-527 MAPA DE RIESGOS DE CORRUPCIÓN DEL PROCESO SOPORTE LEGAL VERSIÓN 2 ACTA DE MEJORAMIENTO 33 DE ENERO 29 DE 2024

Riesgos de Corrupción
1. Posibilidad de encausar y/o intervenir indebidamente en los trámites a cargo de la Subsecretaría Jurídica con el fin de obtener un pronunciamiento y/o una decisión administrativa con desviación de lo público y en beneficio propio o de un tercero.

4.7.2.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias***.

Mediante radicado en SIPA 3-2024-15880 del 3 de mayo la Subsecretaría Jurídica remitió a la Dirección de Planeación Institucional el monitoreo de primera línea de defensa a los riesgos del proceso Soporte Legal.

Para el periodo de monitoreo no se han identificado cambios significativos en el contexto estratégico del proceso.

Se observa coherencia entre el riesgo de corrupción identificado para el proceso "Posibilidad de encausar y/o intervenir indebidamente en las actividades a cargo de la Subsecretaría Jurídica con el fin de obtener un pronunciamiento y/o una decisión administrativa con desviación de lo público y en beneficio propio o de un tercero ", y el objetivo estratégico "Fortalecer la estructura y la cultura institucional para contribuir a una gestión pública efectiva, mediante el desarrollo de habilidades para el talento humano, simplificación de procesos, mecanismos eficientes para la toma de decisiones y mejora continua".

El riesgo es coherente con el objetivo del proceso, el cual se orienta la "Asesoría y representación jurídica de la SDP a través de la revisión y proyección de actos administrativos y conceptos y la representación judicial y extrajudicial".

Conforme a la información del monitoreo de la primera línea de defensa, las causas y consecuencias identificadas para el riesgo de corrupción se mantienen. En este sentido, se asume que no se han evidenciado situaciones que generen alerta o indiquen que las causas y/o consecuencias cambien o se modifiquen, en el marco de la administración del riesgo.

2. ***Autoevaluación de la efectividad de los controles***.

Se presentaron evidencias de la utilización de los controles.

De acuerdo con la ejecución de las actividades determinadas para el control de los riesgos por parte del proceso, el resultado se asocia con la prevención y la mitigación del riesgo.

De acuerdo a lo reportado en el monitoreo de la primera línea de defensa, no se evidencian hallazgos asociados a los controles establecidos.

3. ***Autoevaluación de la eficacia de las acciones:***

La acción "Realizar sensibilización a los servidores de la Subsecretaría Jurídica y sus dependencias, sobre implicaciones disciplinarias en el ejercicio de la función pública" está orientada a contrarrestar las causas del riesgo.

No se evidencia materialización ni hallazgos en las auditorías internas o externas relacionados con el riesgo de corrupción del proceso.

4. ***Evaluación de la efectividad de la gestión de los riesgos:***

La información reportada por la primera línea de defensa y las evidencias de la aplicación efectiva de los controles formulados para el riesgo de corrupción, infieren que la gestión del riesgo ha sido adecuada y útil para evitar situaciones indeseables que afecten el cumplimiento de los objetivos y compromisos a cargo del proceso.

5. ***Actualización de Riesgos****:*

Para el periodo del monitoreo, no se identificó la necesidad de modificar o actualizar el actual riesgo de corrupción, ni tampoco la necesidad de documentar o gestionar nuevos riesgos de este tipo.

4.7.2.2 ALERTAS:

No se identifican alertas respecto a la posible materialización del riesgo de corrupción, debido al balance positivo generado gracias a la administración del riesgo llevada a cabo por el proceso.

4.7.2.3 RECOMENDACIONES:

Continuar con la efectiva gestión a los riesgos, y la ejecución de los controles.

Revisar y validar los riesgos una vez se implemente la plataforma estratégica 2024-2027, y actualizar el contexto estratégico del proceso.

Fortalecer los argumentos que se registran en la columna Observaciones, así como la presentación de las evidencias (en el repositorio dispuesto), con el propósito de optimizar los resultados del seguimiento que contribuyan a la mejora en la gestión del riesgo.
.

4.7.3 A-LE-526 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DEL PROCESO SOPORTE LEGAL VERSIÓN 1 ACTA DE MEJORAMIENTO 106 DE MARZO 23 DE 2023

Riesgo de Seguridad de la Información

1. Posibilidad de Pérdida de confidencialidad por fallas humanas, divulgación ilegal de la información y/o uso no autorizado de equipos en la proyección de conceptos, actos administrativos, documentos de acciones judiciales y conciliaciones extrajudiciales, debido a manejo manual de la información, desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información, y/o información sensible sin cifrado.

4.7.3.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias***.

El contexto estratégico identificado por el proceso se mantiene y sigue siendo coherente con los objetivos estratégicos de la entidad (Fortalecer la estructura y la cultura institucional para contribuir a una gestión pública efectiva) y con el objetivo del proceso A-CA-003 SOPORTE LEGAL (Asesorar y representar jurídicamente a la SDP a través de la revisión y proyección de actos administrativos y conceptos y la representación judicial y extrajudicial.)

La respuesta del líder del proceso indica que el riesgo identificado es coherente con el objetivo estratégico. Sin embargo, es necesario estar atentos a los cambios que pueden darse a la luz de la actualización de los objetivos estratégicos. Se recomienda analizar en el momento de entrada en vigor de los nuevos mapas de procesos, si el riesgo sigue siendo relevante para el logro de los nuevos objetivos y si es necesario realizar ajustes en su definición o tratamiento.

De acuerdo con la respuesta del líder del proceso, el riesgo identificado es coherente con el objetivo del proceso objeto del seguimiento. La materialización de cualquiera de los riesgos identificados en el proceso A-CA-003 Soporte Legal podría dificultar la prestación de los servicios jurídicos y el logro del objetivo del proceso. Por ejemplo, si se produce una pérdida de integridad de la información, esto podría afectar la calidad de los servicios prestados.

El líder del proceso indica que las causas identificadas inicialmente para el riesgo se mantienen. Sin embargo, es importante realizar una revisión detallada de las causas a la luz de los cambios en el contexto estratégico, la actualización de la plataforma estratégica, los objetivos del proceso y los objetivos de la entidad.

Las causas identificadas inicialmente para el riesgo son:

- Manejo manual de la información: La falta de herramientas adecuadas para la gestión de la información puede aumentar el riesgo de errores humanos que podrían ocasionar la pérdida de confidencialidad.

- Desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información: La falta de capacitación o el desconocimiento de las políticas de seguridad y privacidad de la información por parte del personal puede aumentar el riesgo de fuga de información.

- Información sensible sin cifrado: La falta de cifrado de la información sensible puede aumentar el riesgo de acceso no autorizado y robo de datos.

Las consecuencias identificadas inicialmente para el riesgo se mantienen vigentes. El análisis interno realizado en el mes de enero al Mapa de Riesgos confirmó que estas consecuencias siguen siendo relevantes para el proceso de Soporte Legal de la SDP y que están directamente relacionadas con los riesgos establecidos.

Producto del análisis se identificaron las consecuencias relacionadas a continuación:

- Pérdida de la confianza de los ciudadanos en la SDP: La materialización del riesgo de pérdida de confidencialidad, integridad o disponibilidad de la información podría afectar negativamente la confianza de los ciudadanos en la SDP, lo que podría tener un impacto significativo en la imagen pública de la entidad y en la aceptación de los servicios digitales.

- Daños a la reputación de la SDP: La divulgación de información confidencial o la alteración de datos sensibles podría dañar la reputación de la SDP, lo que podría tener consecuencias negativas para la credibilidad de la entidad y para la capacidad de cumplir con sus objetivos estratégicos.
- Perjuicios económicos: La pérdida de información o la interrupción de los servicios jurídicos podría generar perjuicios económicos para la SDP, tanto por los costos directos de la reparación del daño como por los ingresos dejados de percibir.

- Sanciones legales: El incumplimiento de las normativas de protección de datos o de seguridad de la información podría conllevar sanciones legales para la SDP, lo que podría tener un impacto significativo en los recursos financieros de la entidad.

- Dificultades para el cumplimiento de los objetivos: La materialización del riesgo de pérdida de confidencialidad, integridad o disponibilidad de la información podría dificultar el cumplimiento de los objetivos del proceso de Soporte Legal, lo que podría afectar negativamente a la prestación de los servicios jurídicos y a la satisfacción de las necesidades de los usuarios.

2. ***Autoevaluación de la efectividad de los controles****.*

La evaluación de segunda línea de defensa, de acuerdo con las respuestas dadas en el monitoreo realizado por al líder del proceso, ha identificado que la Subsecretaría Jurídica ha implementado los siguientes registros para documentar la utilización de los controles:

Actualización del formato de registro de activos de información e índice de información clasificada y reservada, lo que permite identificar los niveles de confidencialidad y los requisitos de seguridad asociados a cada tipo de información.

Registros de asistencia a las capacitaciones realizadas sobre las políticas de Sistema de Gestión de Seguridad de la Información y los lineamientos para el manejo adecuado de la información.

Se recomienda que la Subsecretaría Jurídica continúe documentando la utilización de los controles de manera consistente y completa dejando evidencia suficiente para soportar el cumplimiento en la ejecución de los controles.

La evaluación de segunda línea de defensa, de acuerdo con la información aportada por el proceso, ha identificado que los controles implementados por la Subsecretaría Jurídica son adecuados para prevenir o mitigar los riesgos de pérdida de confidencialidad, integridad y disponibilidad de la información. Esta afirmación se obtuvo del siguiente análisis:

Control 1: Clasificación de la información, este control permite identificar los niveles de confidencialidad de la información y los requisitos de seguridad asociados a cada tipo de información ayudando a prevenir la divulgación no autorizada de información confidencial y a proteger la integridad de la información sensible.

Control 2: Capacitación en seguridad de la información, este control permite que los funcionarios de la Subsecretaría Jurídica comprendan los riesgos de seguridad de la información y las medidas que deben tomar para protegerla previniendo errores humanos que podrían poner en riesgo la información.

Control 3: Aplicación de las políticas de seguridad de la información, este control garantiza que las actividades de la Subsecretaría Jurídica se realicen de acuerdo con las normas y procedimientos establecidos para la protección de la información con lo cual se busca prevenir incidentes de seguridad que podrían tener un impacto significativo en la entidad.

Se recomienda, para los próximos monitoreos aportar y relacionar las evidencias que permitan verificar la utilización del control.

La evaluación de segunda línea de defensa con corte a 30 de abril de 2024, de acuerdo con la información aportada por el líder del proceso, no evidencia hallazgos de auditoría recientes que indiquen que los controles no sean efectivos en la prevención o mitigación de los riesgos.

3. ***Autoevaluación de la eficacia de las acciones:***

La evaluación de segunda línea de defensa incluyó la revisión de las acciones formuladas por el líder del proceso para el tratamiento del riesgo de pérdida de confidencialidad, integridad y disponibilidad de la información, estableciendo como resultado que son adecuadas para abordar las causas identificadas. Esta afirmación se sustenta en lo siguiente:

La definición de la clasificación de la información permite identificar los niveles de confidencialidad de la información y los requisitos de seguridad asociados a cada tipo de información. Esto ayuda a prevenir la divulgación no autorizada de información confidencial y a proteger la integridad de la información sensible.

La socialización de las políticas de Sistema de Gestión de Seguridad de la Información da herramientas para que los funcionarios del proceso comprendan los riesgos de seguridad de la información y las medidas que deben tomar para protegerla. Adicionalmente esta acción ayuda a prevenir errores humanos que podrían poner en riesgo la información.

La generación de las políticas de Sistema de Gestión de Seguridad de la Información propende por que las actividades del proceso se realicen de acuerdo con las normas y procedimientos establecidos para la protección de la información, previniendo incidentes de seguridad que podrían tener un impacto significativo en la entidad.

Revisado el contexto, las respuestas del proceso en el monitoreo de primera línea de defensa, se puede afirmar que las acciones formuladas para dar tratamiento al riesgo se vienen implementando adecuadamente. La evaluación de segunda línea de defensa encontró que la Subsecretaría Jurídica ha

implementado acciones de tratamiento del riesgo como la clasificación de la información que produce, capacitaciones sobre las políticas de Sistema de Gestión de Seguridad de la Información y ha aplicado las políticas de Sistema de Gestión de Seguridad de la Información en el desarrollo de sus actividades. Es importante tener presente que para los próximos monitoreos se cuente con las evidencias necesarias para validar las afirmaciones anteriores.

La evaluación de segunda línea de defensa con base en la respuesta dada por el líder del proceso y dado que no existen registros de incidentes de seguridad que indiquen que el riesgo se haya materializado, se determinó que el riesgo identificado no se ha materializado ni se ha determinado como hallazgo de auditoría interna o externa.

En razón a que de acuerdo con lo reportado en el seguimiento de primera línea de defensa el riesgo no se ha materializado por ello no se identifica la necesidad de formular correcciones y/o acciones correctivas necesarias para darle tratamiento.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

La gestión del riesgo ha sido útil para evitar situaciones o hechos que puedan afectar el cumplimiento de los objetivos y compromisos del proceso A-CA-003 SOPORTE LEGAL: La Prevención de la divulgación no autorizada de información confidencial ayuda a prevenir que información confidencial sea divulgada a personas no autorizadas y la capacitación en seguridad de la información y la aplicación de los lineamientos para el manejo adecuado de la información han ayudado a prevenir errores humanos que podrían poner en riesgo la integridad de la información.

Las acciones adoptadas por el proceso han permitido la continuidad de las operaciones internas y el logro de los objetivos del proceso.

5. ***Actualización de Riesgos****:*

No se identifica la necesidad de modificar y/o actualizar el riesgo establecido actualmente. La evaluación de segunda línea de defensa ha verificado que la definición del riesgo de pérdida de confidencialidad, integridad y disponibilidad de la información en el proceso A-CA-003 SOPORTE LEGAL sigue siendo válida y adecuada.

No obstante, es importante que el líder del proceso continúe monitoreando los cambios en el contexto estratégico, los resultados de informes de auditoría internos y externos, y otros aspectos que puedan afectar la probabilidad o el impacto del riesgo. En caso de que se identifiquen cambios significativos, el líder del proceso deberá actualizar la definición del riesgo y si es el caso formular planes de tratamiento del riesgo.

No se identifica la necesidad de documentar y gestionar nuevos riesgos en este momento. La evaluación de segunda línea de defensa no evidenció nuevos riesgos que puedan afectar significativamente el cumplimiento de los objetivos del proceso A-CA-003 SOPORTE LEGAL.

Sin embargo, es importante que el líder del proceso continúe alerta a la aparición de nuevos riesgos. En caso de que se identifiquen nuevos riesgos, el líder del proceso deberá documentarlos y gestionarlos de acuerdo con el procedimiento establecido por la SDP.

4.7.3.2 ALERTAS:

De acuerdo con el monitoreo de primera línea de defensa referente a los riesgos identificados de seguridad de la información del Proceso de soporte Legal, no se reportan alertas que indiquen que los riesgos se han materializado.

4.7.3.3 RECOMENDACIONES:

Se recomienda mantener una vigilancia continua sobre el entorno operativo para detectar y gestionar oportunamente cualquier nuevo riesgo que pueda surgir en el futuro.

Se recomienda mantener una cultura interna sobre la recolección de evidencias que soporten las respuestas dadas en el monitoreo de primera línea de defensa.

Se recomienda revisar la definición de controles, en el sentido de establecer acciones que se gestionen desde el interior del proceso y que faciliten su seguimiento como parte de las actividades internas. Al delegar las acciones en otras áreas o agentes externos del proceso se puede aumentar el riesgo de no cumplimiento por cuanto la responsabilidad se diluye.

Se recomienda asistir a los eventos programados por la Dirección de TIC relacionados con los temas en seguridad y privacidad de la información.

5 PROCESOS DE EVALUACIÓN

5.1 EVALUACIÓN Y CONTROL

5.1.1 S-LE-014 MAPA DE RIESGOS DE GESTIÓN DEL PROCESO EVALUACIÓN Y CONTROL VERSIÓN 8 ACTA DE MEJORAMIENTO 85 DE FEBRERO 12 DE 2024

Riesgos de Gestión

1. Posibilidad de afectación reputacional por informes emitidos por la Oficina de Control Interno que contengan información de fuentes que no se ajustan a la realidad de la entidad, debido a información errónea o incompleta suministrada por los auditados para la evaluación del Sistema de Control interno.

5.1.1.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias***.

   El proceso Evaluación y Control remitió a la Dirección de Planeación Institucional el monitoreo de primera línea de defensa a los riesgos asociados al mismo, mediante radicado en SIPA 3-2024-15952 del 3 de mayo.

   Para el periodo de monitoreo, no se han identificado situaciones o aspectos en el ámbito interno o externo que represente cambios en el contexto estratégico del proceso.

   Se observa coherencia entre el riesgo de gestión identificado para el proceso "posibilidad de afectación reputacional por informes emitidos por la oficina de control interno que contengan información de fuentes que no se ajustan a la realidad de la entidad, debido a información errónea o incompleta suministrada por los auditados para la evaluación del sistema de control interno", y el objetivo estratégico "Fortalecer la estructura y la cultura institucional para contribuir a una gestión pública efectiva, mediante el desarrollo de habilidades para el talento humano, simplificación de procesos, mecanismos eficientes para la toma de decisiones y mejora continua".

   El riesgo de gestión guarda coherencia con el objetivo del proceso, el cual se orienta a proveer aseguramiento, asesoría y análisis basados en riesgos, de forma independiente y objetiva. Está enfocado hacia la prevención y pretende proteger el valor de la entidad y mejorar la eficacia de las actividades de gestión de riesgos, control y gobierno.

   Conforme a la información del monitoreo de la primera línea de defensa, las causas y consecuencias identificadas para el riesgo de gestión se mantienen, por lo cual se infiere que no se han evidenciado situaciones que generen alerta o indiquen que las causas y/o consecuencias cambien o se modifiquen, en el marco de la administración del riesgo.

2. ***Autoevaluación de la efectividad de los controles***.

   De acuerdo al monitoreo a riesgos, por parte de la primera línea de defensa se ejecutan los controles y las evidencias se encuentran en un expediente ubicado en

drive. En el repositorio subieron capturas de pantalla de la carpeta que contiene un grupo de archivos (Evidencia SDP-2024-4238), sin embargo; no se observa el contenido, ni se tiene acceso a estos archivos. En este sentido, no se cuenta con la información disponible para verificar los registros y evidencias de la utilización de los 4 controles formulados para el riesgo de gestión. Adicionalmente, el proceso manifiesta que el control examinado previene o mitiga los riesgos y se observa que las diferentes actividades que contemplan los controles se centran en verificaciones que previenen la materialización del riesgo.

Para el periodo de monitoreo, la primera línea de defensa reporta que no se han declarado hallazgos asociados a los controles establecidos.

3. ***Autoevaluación de la eficacia de las acciones:***

No se formularon acciones en plan de acción de tratamiento al riesgo debido al resultado obtenido en el Nivel de riesgo Residual "Bajo" zona para la cual no se hace necesario en la gestión del riesgo de gestión.

No se evidencia materialización ni hallazgos en las auditorías internas o externas relacionados con el riesgo de gestión del proceso.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

Conforme al monitoreo de la primera línea de defensa y la ejecución de los controles formulados para el riesgo, indica que la gestión frente al riesgo por parte del proceso resulta útil para evitar hechos que puedan afectar el cumplimiento de los objetivos y compromisos a su cargo.

5. ***Actualización de Riesgos****:*

Para el periodo del monitoreo, no se identificó la necesidad de modificar o actualizar el actual riesgo de gestión, ni tampoco la necesidad de documentar o gestionar nuevos riesgos. Lo anterior, dado el reporte de la primera línea de defensa, así como; el proceso de revisión y actualización llevado a cabo bajo la metodología de DAFP adoptada por la entidad y los informes de auditoría interna y externa.

5.1.1.2 ALERTAS:

No se generan alertas por eventos que indiquen la posible materialización del riesgo de gestión identificado para el proceso, teniendo en cuenta la efectividad en la aplicación de los controles y la adecuada administración del riesgo.

5.1.1.3 RECOMENDACIONES:

Continuar con la efectiva gestión a los riesgos, y la ejecución de los controles.

Revisar y validar los riesgos una vez se implemente la plataforma estratégica 2024-2027, y actualizar el contexto estratégico del proceso.

Fortalecer las evidencias aportadas de la aplicación de cada control y garantizar el acceso para la verificación por parte de la segunda línea de defensa y entes de control en el momento que se requiera.

5.1.2 S-LE-060 MAPA DE RIESGOS DE CORRUPCIÓN DEL PROCESO EVALUACIÓN Y CONTROL VERSIÓN 2 ACTA DE MEJORAMIENTO 72 DE ENERO 31 DE 2024

Riesgos de Corrupción

1. Posibilidad de omitir o incluir información en beneficio propio o de un tercero que afecte intencionalmente la evaluación independiente al Sistema de Control Interno, al omitir o encubrir hechos irregulares detectados.

5.1.2.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias***.

El proceso Evaluación y Control remitió a la Dirección de Planeación Institucional el monitoreo de primera línea de defensa a los riesgos asociados al mismo, mediante radicado en SIPA 3-2024-15952 del 3 de mayo. Luego de realizar algunas observaciones se generan ajustes, remitiendo el mapa de corrupción por correo electrónico, el 6 de mayo.

Para el periodo de monitoreo, no se han identificado situaciones o aspectos en el ámbito interno o externo que represente cambios en el contexto estratégico del proceso.

Se observa coherencia entre el riesgo de corrrupción identificado para el proceso "posibilidad de omitir o incluir información en beneficio propio o de un tercero que afecte intencionalmente la evaluación independiente al Sistema de Control Interno, al omitir o encubrir hechos irregulares detectados", y el objetivo estratégico "Fortalecer la estructura y la cultura institucional para contribuir a una gestión pública efectiva, mediante el desarrollo de habilidades para el talento humano, simplificación de procesos, mecanismos eficientes para la toma de decisiones y mejora continua".

El riesgo de corrupción guarda coherencia con el objetivo del proceso, el cual se orienta a proveer aseguramiento, asesoría y análisis basados en riesgos, de forma independiente y objetiva. Está enfocado hacia la prevención y pretende proteger el valor de la entidad y mejorar la eficacia de las actividades de gestión de riesgos, control y gobierno.

Conforme a la información del monitoreo de la primera línea de defensa, las causas identificadas para el riesgo de corrupción se mantienen, por lo cual se infiere que no se han evidenciado situaciones que generen alerta o indiquen que las causas y/o consecuencias cambien o se modifiquen, en el marco de la administración del riesgo.

2. ***Autoevaluación de la efectividad de los controles***.

Durante el periodo del presente monitoreo a riesgos, la primera línea de defensa registra que no ha habido lugar a aplicación de los controles, lo cual se relaciona con el hecho de no haber ejecutado las actividades inmersas en los controles como lo son la realización de auditorias y presentación de denuncias en la entidad, al no estar programadas auditorías para este periodo ni surgir denuncias en particular. El proceso confirma que los controles previenen o mitigan los riesgos. Conforme a los resultados obtenidos en monitoreos anteriores los controles han sido efectivos.

Para el periodo de monitoreo, la primera línea de defensa reporta que no se han declarado hallazgos asociados a los controles establecidos.

3. ***Autoevaluación de la eficacia de las acciones:***

En cuanto a la acción formulada para el tratamiento del riesgo "Realizar la rotación de las actividades y temas de la Oficina de Control Interno, de conformidad con las competencias del equipo de trabajo y la experiencia en la ejecución de las tareas asignadas", y el reporte de avance registrado (en la sección correspondiente Plan de acción - tratamiento del Riesgo) "Se ha realizado la reasignación de temas al interior de la Oficina de Control Interno, por ejemplo la designación del enlace del Sistema de Gestión realizada mediante radicado 3-2024-14251de abril 16 de 2024". Evidencia SDP-2024-4306, se observa que está orientada a contrarrestar las causas y se viene implementando en el periodo programado.

No se evidencia materialización ni hallazgos en las auditorías internas o externas relacionados con el riesgo de corrupción del proceso.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

Aún cuando no se realizó la aplicación de los controles formulados para el riesgo de corrupción (como se menciona en el numeral 2.1), conforme a la información reportada por la primera lìnea de defensa y el resultado en la gestión del riesgo, se encuentra que no se ha materializado el riesgo y se ha dado cumplimiento a los objetivos; resultando útil para evitar desviaciones o situaciones de incumplimiento.

5. ***Actualización de Riesgos****:*

Para el periodo del monitoreo, no se identificó la necesidad de modificar o actualizar el actual riesgo de corrupción, ni tampoco la necesidad de documentar o gestionar nuevos riesgos. Lo anterior, dado el reporte de la primera línea de defensa, así como; el proceso de revisión y actualización llevado a cabo bajo la metodología de DAFP adoptada por la entidad y los informes de auditoría internos y externos.

5.1.2.2 ALERTAS:

No se evidencian situaciones que generen alertas en relación con la posible materialización del riesgo, denotando efectividad en la gestión al riesgo adelantada por el proceso.

5.1.2.3 RECOMENDACIONES:

Continuar con la efectiva gestión a los riesgos, y la ejecución de los controles.

Revisar y validar los riesgos una vez se implemente la plataforma estratégica 2024-2027, y actualizar el contexto estratégico del proceso.

Fortalecer las evidencias aportadas de la aplicación de cada control y garantizar el acceso para la verificación por parte de la segunda línea de defensa y entes de control en el momento que se requiera.

5.1.3 S-LE-059 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DEL PROCESO EVALUACIÓN Y CONTROL VERSIÓN 2 ACTA DE MEJORAMIENTO 91 DE FEBRERO 13 DE 2024

Riesgo de Seguridad de la Información

1. Posibilidad de pérdida de Integridad por fallas humanas; de actas, informes de auditoría y seguimiento, PAA, debido a manejo manual de la información.

5.1.3.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias***.

El contexto estratégico identificado por el proceso se mantiene. La evaluación de segunda línea de defensa de acuerdo con lo informado por el proceso identificó que el contexto estratégico del proceso S-CA-001 EVALUACIÓN Y CONTROL sigue siendo válido y relevante. Los principales elementos del contexto estratégico, como la necesidad de fortalecer la gestión de riesgos, control y gobierno en la entidad siguen vigentes. no obstante, se recomienda realizar de manera proactiva un análisis frente a la implementación de posibles cambios que se introducirán en el proceso con la formalización de los nuevos mapas de procesos lo cual se prevé para mediados de la vigencia 2024.

El riesgo identificado (Posibilidad de pérdida de Integridad por fallas humanas; de actas, informes de auditoría y seguimiento, PAA, debido a manejo manual de la información) es coherente con el objetivo estratégico al cual le aporta el proceso. El objetivo estratégico del proceso es "Proveer aseguramiento, asesoría y análisis basados en riesgos, de forma independiente y objetiva, a través del liderazgo estratégico, evaluación y seguimiento, enfoque hacia la prevención, evaluación a la gestión del riesgo y relación con entes externos de control y vigilancia, con el fin de proteger el valor de la entidad y mejorar la eficacia de las actividades de gestión de riesgos, control y gobierno". La pérdida de integridad de la información podría afectar significativamente el logro de este objetivo estratégico.

En el análisis del proceso se identificó que la pérdida de integridad de la información podría afectar directamente la capacidad del proceso para cumplir con su objetivo.

Las principales causas del riesgo, como son el manejo manual de la información y la falta de capacitación en seguridad de la información, siguen siendo relevantes.

Las principales consecuencias del riesgo como por lo son el daño a la reputación de la entidad y la pérdida de confianza de los usuarios, siguen siendo significativas.

2. ***Autoevaluación de la efectividad de los controles***.

De acuerdo con la respuesta del líder del proceso, existe evidencia de que el Control 1 está siendo utilizado. El jefe de la Oficina de Control Interno revisa los registros de inducción y reinducción en seguridad de la información para verificar que los servidores de la Oficina hayan pasado por estos procesos. Sin embargo, es importante destacar que la inducción no ha sido programada por la Dirección de Talento Humano en el primer período del año, por lo que no se ha podido realizar la inducción a todos los funcionarios de la Oficina.

El Control 1 es un control efectivo para prevenir o mitigar el riesgo de pérdida de integridad de la información. La capacitación en seguridad de la información permite a los

funcionarios comprender los riesgos asociados al manejo de la información y tomar las medidas necesarias para protegerla. Además, la revisión del cumplimiento de la política de seguridad de la información permite identificar y corregir posibles fallos en la implementación de los controles de seguridad.

El Control 2, “Cuando se presenten incidentes de integridad, el jefe de la Oficina de Control Interno revisa con su equipo de trabajo y con el oficial de seguridad el cumplimiento de la política de seguridad de la información al interior de la OCI”, es un control efectivo para prevenir o mitigar el riesgo de pérdida de integridad de la información. Este control permite identificar y corregir rápidamente las fallas de seguridad que puedan ocasionar la pérdida de integridad de la información. Al revisar los incidentes de seguridad, el jefe de la Oficina de Control Interno puede identificar las causas de los incidentes y tomar las medidas necesarias para prevenir que se repitan. Además, la revisión del cumplimiento de la política de seguridad de la información permite verificar que los funcionarios de la Oficina están cumpliendo con las normas de seguridad y que están tomando las medidas adecuadas para proteger la información.

En cuanto al control 2, con base en la respuesta del proceso, el jefe de la Oficina de Control Interno revisa los registros de incidentes de seguridad y verifica que se han realizado las revisiones correspondientes con el equipo de trabajo y el oficial de seguridad.

Sin embargo, es importante destacar que no se han presentado incidentes de seguridad en el primer período del año, por lo que no ha sido posible aplicar el Control 2 en su totalidad.

Con el fin de soportar las respuestas en los procesos de seguimiento y monitoreo se recomienda constituir un repositorio de evidencias y disponerlas para lograr validar de manera eficiente la utilización de los controles, estas evidencias pueden ser: registros de incidentes de seguridad y actas de las revisiones realizadas por el jefe de la Oficina de Control Interno.

No se han identificado hallazgos de auditoría asociados a los controles. No se han realizado auditorías internas o externas que hayan evaluado la efectividad de los controles. Se recomienda que el líder del proceso incluya los controles en el alcance de las próximas auditorías internas.

3. ***Autoevaluación de la eficacia de las acciones:***

La acción formulada, "gestionar una sesión de socialización en asuntos de seguridad de la información en los temas de la Oficina de Control Interno"", no está orientada a contrarrestar las causas del riesgo de pérdida de integridad de la información. La falta de entendimiento de la herramienta creada para la identificación y clasificación del riesgo de seguridad de la información es una barrera para la implementación de la acción, pero no es la causa del riesgo.

Se recomienda continuar con la evaluación interna sobre las acciones que deben establecer para contrarrestar las causas del riesgo de pérdida de integridad de la información como son: el manejo manual de la información, la falta de capacitación en seguridad de la información y las debilidades en los controles de seguridad de la información.

Algunas de las acciones recomendadas son:

- Gestionar y actualizar la información para incorporar en el nuevo sistema de gestión de la seguridad de la información GESTIONATE.

- Realizar capacitaciones en seguridad de la información para los colaboradores al interior del proceso.

- Identificar los controles de seguridad de la información como por ejemplo el desarrollo de aplicaciones que reduzcan el manejo manual de la información.

- Gestionar el control de acceso y accesos privilegiados a la información sensible que se gestiona desde el proceso.

Las acciones formuladas para dar tratamiento al riesgo no se están implementando adecuadamente. por ejemplo: la acción formulada, "gestionar una sesión de socialización en asuntos de seguridad de la información en los temas de la Oficina de Control Interno", no se ha implementado hasta la fecha debido a la falta de entendimiento de la herramienta creada para la identificación y clasificación del riesgo de seguridad de la información.

El riesgo identificado no se ha materializado y tampoco se ha determinado como hallazgo de auditoría interna o externa.

Si bien el riesgo de pérdida de integridad de la información no se ha materializado hasta la fecha, es importante destacar que este tipo de riesgos pueden materializarse en cualquier momento. Se recomienda que el líder del proceso continúe monitoreando el riesgo y tome las medidas necesarias para prevenir su materialización máxime cuando los controles nos son adecuados para el tratamiento del riesgo.

No se han formulado las correcciones y/o acciones correctivas necesarias para darle tratamiento al riesgo, ya que el riesgo no se ha materializado.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

Para la prevención de la pérdida de integridad de la información, la OCI identificó la implementación de controles como la verificación de los procesos de inducción y reinducción en seguridad de la información para los servidores de la Oficina y la revisión del cumplimiento de la política de seguridad de la información en caso de incidentes. Estos controles han permitido prevenir la materialización del riesgo de pérdida de integridad de la información. Al evitar la pérdida de información, la Oficina de Control Interno puede proteger activos valiosos de la entidad y garantizar la continuidad de sus operaciones.

En segundo lugar, para el cumplimiento de objetivos y compromisos, La gestión efectiva del riesgo ha contribuido al logro del objetivo del proceso de "Proveer aseguramiento, asesoría y análisis basados en riesgos, de forma independiente y objetiva, a través del liderazgo estratégico, evaluación y seguimiento, enfoque hacia la prevención, evaluación a la gestión del riesgo y relación con entes externos de control y vigilancia, con el fin de proteger el valor de la entidad y mejorar la eficacia de las actividades de gestión de riesgos, control y gobierno". Al mitigar los riesgos, la Oficina de Control Interno puede aumentar la probabilidad de alcanzar sus objetivos y cumplir con sus compromisos.

Así mismo, en cuanto al fortalecimiento de la estructura y cultura institucional, La gestión del riesgo ha contribuido al logro del objetivo estratégico de "Fortalecer la estructura y la cultura institucional para contribuir a una gestión pública efectiva, mediante el desarrollo de habilidades para el talento humano, simplificación de procesos, mecanismos eficientes para la toma de decisiones y mejora continua". Al implementar prácticas de gestión de riesgos,

la Oficina de Control Interno puede mejorar la toma de decisiones, la asignación de recursos y la rendición de cuentas.

En cuanto al componente de monitoreo y evaluación, la Oficina de Control Interno ha realizado un seguimiento periódico de la efectividad de los controles para mitigar el riesgo, lo que le ha permitido identificar áreas de mejora y tomar las medidas correctivas necesarias. Este monitoreo y evaluación continuo es esencial para garantizar la eficacia de la gestión del riesgo en el tiempo.

Se recomienda que la Oficina de Control Interno desarrolle mecanismos para documentar las lecciones aprendidas de la gestión del riesgo, lo que le permitirá mejorar sus prácticas en el futuro. Compartir estas lecciones aprendidas con otras dependencias de la entidad puede contribuir a una cultura de gestión de riesgos más sólida en toda la organización.

5. ***Actualización de Riesgos****:*

El riesgo de pérdida de integridad de la información sigue siendo relevante para la Oficina de Control Interno. No ha habido cambios significativos en el contexto estratégico, los resultados de las auditorías internas y externas, u otros aspectos que sugieran que la naturaleza o la probabilidad del riesgo haya cambiado.

Si bien es importante estar atento a la aparición de nuevos riesgos, en este momento no se han identificado nuevos riesgos que sean relevantes para la Oficina de Control Interno y por tanto, no se Identifica la necesidad de documentar y gestionar nuevos riesgos.

5.1.3.2 ALERTAS:

De acuerdo con el monitoreo de primera línea de defensa referente a los riesgos identificados de seguridad de la información del Proceso de Evaluación y Control, no se reportan alertas que indiquen que los riesgos se han materializado.

5.1.3.3 RECOMENDACIONES:

Se recomienda llevar a cabo el análisis planteado por el líder del proceso para asegurar que el riesgo identificado aún sea relevante y esté alineado con el contexto actual del proceso y de la entidad. Esto garantizará una gestión de riesgos efectiva y adaptada a los cambios.

Se sugiere continuar con la iniciativa de revisar los controles y el plan de acción para lograr definir los adecuados para contrarrestar las causas y mitigar las consecuencias en el caso de la materialización del riesgo.

Se recomienda asistir a las sesiones de capacitación y sensibilización en temas de seguridad y privacidad de la información programadas por la entidad.

5.2 MEJORAMIENTO CONTINUO

5.2.1 S-LE-013 MAPA DE RIESGOS DE GESTIÓN DEL PROCESO MEJORAMIENTO CONTINUO VERSIÓN 9 ACTA DE MEJORAMIENTO 89 DE FEBRERO 12 DE 2024

Riesgos de Gestión

1. Posibilidad de afectación económica y reputacional por sanciones y/o multas por parte de órganos de control, requerimientos de grupos de valor y grupos de interés y/o pérdida de confianza y credibilidad, debido a la debilidad en la apropiación de los principios de autocontrol, autogestión y autorregulación en las líneas de defensa (estratégica, primera, segunda y tercera línea) en la formulación, ejecución, reporte, monitoreo y seguimiento de los planes de mejoramiento.

5.2.1.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias***.

Para el periodo de monitoreo no se han identificado cambios significativos en el contexto estratégico del proceso. Sin embargo, teniendo en cuenta que en el segundo semestre de la vigencia se realizará la formulación de la plataforma estratégica 2024-2027, se evaluará nuevamente el contexto estratégico del proceso. Según el reporte de la primera línea de defensa se evidencia la relación directa con el objetivo estratégico: "Fortalecer la estructura y la cultura institucional para contribuir a una gestión pública efectiva, mediante el desarrollo de habilidades para el talento humano, simplificación de procesos, mecanismos eficientes para la toma de decisiones y mejora continua".

Según lo reportado por la primera línea de defensa se puede observar que el riesgo de gestión identificado para el proceso, guarda coherencia con el objetivo del proceso. Sin embargo, se deja claridad que una vez se formalice el nuevo mapa de procesos de la entidad, este proceso se fusionará con el de Dirección Estratégica Institucional, por lo que nuevamente se tendrá que evaluar la coherencia del riesgo identificado con el objetivo del proceso.

Para el periodo de monitoreo, la primera línea de defensa manifiesta que las causas y consecuencias identificadas inicialmente se mantienen, razón por la cual se infiere que durante la normal operación del proceso no se han evidenciado alertas de nuevas causas y/o consecuencias que puedan incidir en la materialización del riesgo de corrupción.

2. ***Autoevaluación de la efectividad de los controles***.

El riesgo de gestión cuenta con tres (3) controles para la mitigación del riesgo. El primer control asociado a la verificación de la formulación del plan de mejoramiento en términos de oportunidad y pertinencia por parte del responsable con su equipo de trabajo y el segundo control enfocado a la verificación metodológica de dichos planes por parte de la Dirección de Planeación Institucional se aplicaron en las mesas de trabajo realizadas, con la participación de las áreas involucradas.

En cuanto al tercer control, la verificación del plan de mejoramiento por parte del responsable y su equipo de trabajo, se realiza antes y al momento de reportar los avances de las acciones en el marco del monitoreo de

primera línea de defensa en el módulo en SIPA. El proceso desarrolló actividades que dan cuenta de la aplicación efectiva de los dos controles formulados para el riesgo de gestión, razón por la cual estos se mantienen para mitigar su posible ocurrencia. Para el periodo de monitoreo la primera línea de defensa reporta no tener hallazgos asociados a los tres (3) controles.

3. ***Autoevaluación de la eficacia de las acciones:***

No se tienen contempladas acciones adicionales para realizar tratamiento al riesgo identificado; sin embargo, los controles establecidos han permitido establecer una correlación con las causas identificados, pues a la fecha el riesgo no se ha materializado. De igual modo, no se evidencia materialización ni hallazgos en las auditorías internas o externas relacionados con el riesgo de gestión del proceso.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

Las evidencias de la aplicación efectiva de los tres (3) controles formulados para el riesgo de gestión, permiten concluir que la gestión del riesgo ha sido adecuada y útil para evitar situaciones indeseables que afecten el cumplimiento de los objetivos y compromisos a cargo del proceso.

5. ***Actualización de Riesgos****:*

Para el periodo del monitoreo, no se identificó la necesidad de modificar o actualizar el actual riesgo de gestión, ni tampoco la necesidad de documentar o gestionar nuevos riesgos de este tipo.

Es importante mencionar que el Departamento Administrativo de la Función Pública - DAFP publicó en noviembre de 2022 la versión 6 de la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, la cual contiene un nuevo capítulo para el análisis de riesgos fiscales cuya finalidad es prevenir el daño al patrimonio público, representando en el menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos o a los intereses patrimoniales del Estado. Por tal razón, la Dirección de Planeación Institucional se encuentra adelantando lo pertinente para definir la hoja de ruta que permita su incorporación a los actuales mapas de riesgos de la entidad, con el acompañamiento de las dependencias correspondientes dada la naturaleza de este tipo de riesgos.

5.2.1.2 ALERTAS:

No se evidencian alertas relacionadas con la posible materialización de los riesgos de gestión identificados para el proceso de Mejoramiento Continuo, pues la efectividad en la administración de los riesgos a través de la ejecución de los adecuados controles, ha permitido consolidar en términos de eficacia el sistema de riesgos asociados al proceso.

5.2.1.3 RECOMENDACIONES:

Se recomienda una vez entre en operación el nuevo mapa de procesos de la entidad, verificar los riesgos de gestión asociados a este proceso y validar la necesidad de incluirlos en el proceso de Dirección Estratégica Institucional, teniendo en cuenta que ambos procesos se fusionan en uno solo.

5.2.2 S-LE-062 MAPA DE RIESGOS DE CORRUPCIÓN DEL PROCESO MEJORAMIENTO CONTINUO VERSIÓN 3 ACTA DE MEJORAMIENTO 38 DE ENERO 30 DE 2024

Riesgos de Corrupción
1. Posibilidad de manipulación de la información relacionada con las acciones de los planes de mejoramiento, por acción u omisión con el fin de desviar la gestión en beneficio propio o de terceros.

5.2.2.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias***.

Para el periodo de monitoreo no se han identificado cambios significativos en el contexto estratégico del proceso. Sin embargo, se aclara que durante el segundo semestre la planeación estratégica de la entidad surtirá cambios, por lo que se evaluará el contexto del proceso. Teniendo en cuenta que el riesgo está orientado a la posibilidad de manipulación de la información relacionada con las acciones de los planes de mejoramiento, por acción u omisión con el fin de desviar la gestión en beneficio propio o de terceros, se evidencia que está relacionado directamente con el objetivo estratégico "Fortalecer la estructura y la cultura institucional para contribuir a una gestión pública efectiva, mediante el desarrollo de habilidades para el talento humano, simplificación de procesos, mecanismos eficientes para la toma de decisiones y mejora continua".

Así mismo, el riesgo de corrupción guarda coherencia con el objetivo del proceso, toda vez que se orienta manipulación de la información relacionada con las acciones de los planes de mejoramiento logísticos, que si se llegar a materializar afectaría la gestión de la Secretaría Distrital de Planeación y su mejora del desempeño de los procesos, productos y servicios. Para el periodo de monitoreo, la primera línea de defensa manifiesta que las causas y consecuencias identificadas inicialmente se mantienen, razón por la cual se infiere que durante la normal operación del proceso no se han evidenciado alertas de nuevas causas y/o consecuencias que puedan incidir en la materialización del riesgo de corrupción.

2. ***Autoevaluación de la efectividad de los controles***.

Las evidencias que dan cuenta de la aplicación del control Nº 1 asociado a la verificación de los avances de las acciones de los planes de mejoramiento por parte de los responsables, les permite establecer el estado de las mismas al momento de reportar el monitoreo de primera línea de defensa en el módulo Planes de Mejoramiento del SIPA, de acuerdo con los plazos establecidos para tal fin. Los informes de seguimiento a planes de mejoramiento elaborados por la OCI se constituyen en un insumo para que los responsables fortalezcan la gestión de sus planes de mejoramiento.

Teniendo en cuenta que la responsabilidad de este proceso es compartida entre la Dirección de Planeación Institucional y la Oficina de Control Interno, el acompañamiento inicial a las dependencias para la formulación y reformulación de planes de mejoramiento, lo realiza la Dirección de Planeación Institucional. La Oficina de Control Interno en el marco de la evaluación independiente autoriza las reformulaciones de acciones, previo análisis de la justificación presentada por el responsable de las mismas.

Así mismo, la Dirección de Planeación Institucional realiza el acompañamiento y monitoreo mensual como segunda línea de defensa al reporte de avances de acciones de

planes de mejoramiento por parte de los responsables, mediante el envío de dos correos a los enlaces, el primero recordando el plazo de inicio y fin para reporte y el segundo alertando en caso de existir acciones sin reporte y/o sin aprobación del directivo responsable, el cual se envía de manera mensual, previo al cumplimiento del plazo de reporte de seguimiento a los planes de mejoramiento establecido por la OCI.

Otro recurso valioso con el que cuenta la entidad para minimizar la ocurrencia de situaciones indeseables, es el módulo para la gestión de planes de mejoramiento en el aplicativo SIPA cuyo líder funcional es un funcionario de la Dirección de Planeación Institucional. Este sistema se constituye en una herramienta de control para efectos de mantener la trazabilidad de las acciones y planes cerrados y vigentes.

En cuanto al control Nº 2 la Oficina de Control Interno realiza el seguimiento trimestral al estado y avance de los planes de mejoramiento, el cual registra información suficiente para el análisis comparativo tanto cuantitativo como cualitativo de los planes desde la formulación hasta el cierre. El informe se envía a todas las dependencias mediante radicado en SIPA y se publica en la página WEB de la SDP.

El proceso desarrolló actividades que dan cuenta de la aplicación efectiva de los dos controles formulados para el riesgo de corrupción, razón por la cual estos se mantienen para mitigar su posible ocurrencia. Se debe mencionar que para el periodo de monitoreo la primera línea de defensa reporta no tener hallazgos asociados a los dos controles.

3. ***Autoevaluación de la eficacia de las acciones:***

La acción formulada para el tratamiento del riesgo está relacionada con la capacitación a enlaces, líderes en aspectos relacionados con planes de mejoramiento, a partir del segundo semestre de 2024, la Dirección de Planeación Institucional inició la planeación del ciclo de capacitación para enlaces SG-MIPG, proyectos y trámites, dentro del cual se programó la sesión para planes de mejoramiento.

Teniendo en cuenta que las causas identificadas para el riesgo de corrupción son los vacíos en el cumplimiento del procedimiento para la formulación y reformulación de las acciones de los planes de mejoramiento y las presiones de funcionarios con poder de decisión para ajustar o modificar acciones de los planes de mejoramiento, las jornadas del ciclo de capacitación programadas reforzarán los aspectos identificados. Así mismo, no se evidencia materialización ni hallazgos en las auditorías internas o externas relacionados con el riesgo de corrupción del proceso.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

La información reportada por la primera línea de defensa y las evidencias de la aplicación efectiva de los dos controles formulados para el riesgo de corrupción, permiten concluir que la gestión del riesgo ha sido adecuada y útil para evitar situaciones indeseables que afecten el cumplimiento de los objetivos y compromisos a cargo del proceso.

5. ***Actualización de Riesgos****:*

Para el periodo del monitoreo, no se identificó la necesidad de modificar o actualizar el actual riesgo de corrupción, ni tampoco la necesidad de documentar o gestionar nuevos riesgos de este tipo.

Es importante mencionar que el Departamento Administrativo de la Función Pública - DAFP publicó en noviembre de 2022 la versión 6 de la Guía para la Administración

del Riesgo y el diseño de controles en entidades públicas, la cual contiene un nuevo capítulo para el análisis de riesgos fiscales cuya finalidad es prevenir el daño al patrimonio público, representando en el menoscabo, disminución, perjuicio, detrimento, pérdida, o deterioro de los bienes o recursos públicos o a los intereses patrimoniales del Estado. Por tal razón, la Dirección de Planeación Institucional se encuentra adelantando lo pertinente para definir la hoja de ruta que permita su incorporación a los actuales mapas de riesgos de la entidad, con el acompañamiento de las dependencias correspondientes dada la naturaleza de este tipo de riesgos.

5.2.2.2 ALERTAS:

No se evidencian alertas relacionadas con la posible materialización de los riesgos de gestión identificados para el proceso de Mejoramiento Continuo, pues la efectividad en la administración de los riesgos a través de la ejecución de los adecuados controles, ha permitido consolidar en términos de eficacia el sistema de riesgos asociados al proceso.

5.2.2.3 RECOMENDACIONES:

Se recomienda una vez entre en operación el nuevo mapa de procesos de la entidad, verificar los riesgos de corrupción asociados a este proceso y validar la necesidad de incluirlos en el proceso de Dirección Estratégica Institucional, teniendo en cuenta que ambos procesos se fusionan en uno solo.

5.2.3 S-LE-061 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DEL PROCESO MEJORAMIENTO CONTINUO VERSIÓN 2 ACTA DE MEJORAMIENTO 96 DE FEBRERO 16 DE 2024

Riesgo de Seguridad de la Información

1. Posibilidad de Pérdida de Integridad por fallas humanas y destrucción de la información, contenida en documentos históricos de consulta y soportes (actas, resoluciones, planes) debido a manejo manual de la información y el insuficiente entrenamiento y capacitación sobre políticas y privacidad de la información.

2. Posibilidad de Pérdida de integridad por destrucción, hurto y ransomware de la información de planes de mejoramiento, debido a insuficiente entrenamiento y capacitación sobre políticas y privacidad de la información y ausencia de copias de respaldo o Backus de la información.

5.2.3.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias***.

El líder del proceso indica que no se han identificado cambios significativos en el contexto estratégico durante el período de monitoreo. Sin embargo, se menciona que en el segundo semestre de 2024 se realizará la formulación de la plataforma estratégica 2024-2027, lo que implicará una reevaluación del contexto estratégico del proceso.

El líder del proceso afirma que los riesgos de pérdida de integridad y disponibilidad de la información están directamente relacionados con el objetivo estratégico de fortalecer la estructura y cultura institucional para una gestión pública efectiva. Sin embargo, se menciona que se reevaluará la alineación con el objetivo estratégico una vez definida la nueva plataforma estratégica de la entidad.

Se confirma que los riesgos de seguridad de la información guardan coherencia con el objetivo del proceso, ya que se enfocan en proteger la integridad y disponibilidad de la información, elementos esenciales para la gestión y mejora continua del desempeño de la Secretaría Distrital de Planeación.

El líder del proceso indica que las causas identificadas inicialmente para los riesgos se mantienen durante el período de monitoreo. No se han evidenciado alertas de nuevas causas que puedan incidir en la materialización de los riesgos. Desde el proceso se confirma que las consecuencias identificadas inicialmente para los riesgos se mantienen. No se han observado cambios significativos en las potenciales repercusiones de la materialización de los riesgos.

2. ***Autoevaluación de la efectividad de los controles***.

El líder del proceso indica que existen evidencias del uso de los controles para ambos riesgos. Para el Riesgo 1, se menciona la divulgación de políticas de seguridad, la verificación del registro de ingresos por parte de la empresa de vigilancia y la desvinculación del archivador metálico para el almacenamiento de archivos. Para el Riesgo 2, se confirma la divulgación de políticas de seguridad y la realización de copias de respaldo de sistemas de información y carpetas compartidas.

Es importante contar con registros documentados que evidencien la aplicación consistente de los controles. Estos registros pueden incluir actas de reuniones, minutas de capacitación, informes de auditoría interna, entre otros. La disponibilidad de estos registros permitirá verificar la efectividad de

los controles y facilitar la identificación de áreas de mejora.

La respuesta proporcionada por el líder del proceso indica que las actividades desarrolladas en conjunto con la Dirección de Tecnologías han contribuido a la mitigación de los dos riesgos de seguridad de la información identificados, Sin embargo, es importante reforzar la recolección de evidencias del uso de los controles y su efectividad con el fin de evaluar con mayor certeza los mecanismos aplicados para la protección de la información.

De acuerdo con la respuesta del proceso, durante el período de monitoreo no se han reportado hallazgos de auditoría relacionados con los cinco controles implementados.

3. ***Autoevaluación de la eficacia de las acciones:***

En el marco del contexto del proceso, se analizó por cada riesgo el aporte para contrarrestar las causas de la siguiente manera:
Primer riesgo: Posibilidad de Pérdida de Integridad por fallas humanas y destrucción de la información
Control 1: Divulgación de políticas de seguridad y buen tratamiento de la información, Esta acción busca reducir la probabilidad de errores humanos que puedan comprometer la integridad de la información, al concientizar a los colaboradores sobre las políticas de seguridad y las buenas prácticas para el manejo de información sensible.

Control 2: Implementación de un archivador metálico, Esta acción busca mitigar los efectos de posibles eventos destructivos, como incendios o inundaciones, al proporcionar un espacio de almacenamiento seguro para los documentos históricos.

Control 3: Socialización de políticas de seguridad de la información, Similar al Control 1, esta acción busca reforzar la comprensión de las políticas de seguridad y las buenas prácticas para el manejo de información, contribuyendo a minimizar los riesgos de errores humanos y fugas de información.

Segundo riesgo: Posibilidad de Pérdida de Integridad por destrucción, hurto y ransomware

Control 1: Divulgación de políticas de seguridad y buen tratamiento de la información, Al igual que en el primer riesgo, esta acción busca reducir la probabilidad de errores humanos y comportamientos inadecuados que puedan poner en riesgo la información, mediante la concientización sobre las políticas de seguridad y las buenas prácticas.

Control 2: Realización de copias de respaldo, Esta acción busca mitigar los efectos de eventos destructivos o ataques cibernéticos, al contar con copias de seguridad que permitan restaurar la información en caso de pérdida o daño.

Con el fin de establecer si las acciones formuladas están siendo implementadas adecuadamente, se realizó el análisis por cada riesgo el cual se detalla a continuación:
Primer riesgo: Posibilidad de Pérdida de Integridad por fallas humanas y destrucción de la información

Control 1: Divulgación de políticas de seguridad y buen tratamiento de la información

Las respuestas dadas por el proceso en el monitoreo de primera línea de defensa dejan ver que se han realizado capacitaciones desde la Dirección de TIC para dar a conocer las políticas de seguridad dirigida a todos los colaboradores de la entidad. Así mismo, se ha distribuido material informativo sobre las

políticas de seguridad y las buenas prácticas a través de medios masivos como el correo corporativo

Control 2: Implementación de un archivador metálico.

El proceso informó que se ha adquirido e instalado un archivador metálico que cumple con los estándares de seguridad para el almacenamiento de documentos históricos. El cual se encuentra en un área segura y protegida de la entidad.

Control 3: Socialización de políticas de seguridad de la información

Se han realizado reuniones periódicas sobre el tema de la seguridad de la información y existe un plan de capacitaciones regulares para el personal de la SDP.

Segundo riesgo: Posibilidad de Pérdida de Integridad por destrucción, hurto y ransomware

Control 1: Divulgación de políticas de seguridad y buen tratamiento de la información

Para este control se han realizado las mismas acciones que para el Control 1 del primer riesgo, con el énfasis adicional en la importancia de proteger la información contra ataques cibernéticos y ransomware.

Control 2: Realización de copias de respaldo

La entidad cuenta con procedimientos para la realización periódica de copias de respaldo de los sistemas de información, bases de datos y carpetas compartidas, las copias de respaldo se almacenan en un lugar seguro y protegido fuera de la entidad y se realiza pruebas de restauración de las copias de respaldo para verificar su confiabilidad.

Lo anterior, evidencia la implementación de las acciones por cada control, sin embargo, se sugiere revisar la definición de los controles en procura de orientarlos a actividades que puedan ser gestionadas al interior del proceso y no depender de la gestión de otro proceso.

El líder del proceso informa que no se ha evidenciado materialización de los riesgos ni hallazgos relacionados con los mismos en las auditorías internas o externas realizadas. Con base en la información reportada no se observa que en el periodo el riesgo se haya materializado.

El líder del proceso indica que no se han formulado correcciones o acciones correctivas debido a que no se ha materializado ninguno de los riesgos.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

La gestión del riesgo ha sido útil en el proceso S-CA-002 Mejoramiento Continuo para:

Con base en las respuestas dada por el líder el proceso, se infiere que la implementación de controles adecuados ha permitido reducir la probabilidad de que se presenten eventos que puedan afectar el cumplimiento de los objetivos del proceso, se ha identificado las acciones para la gestión del riesgo ha contribuido a minimizar sus consecuencias negativas, se ha promovido la una cultura de seguridad de la información a través de sensibilización y capacitación en materia de riesgos generando mayor conciencia entre los colaboradores sobre la importancia de proteger la información.

Al reducir los riesgos, la gestión del riesgo ha contribuido a que el proceso S-CA-002 Mejoramiento Continuo pueda alcanzar sus objetivos de manera más efectiva.

5. ***Actualización de Riesgos**:*

El líder del proceso indica que no se identificó la necesidad de modificar o actualizar los riesgos de seguridad de la información durante el período de monitoreo. Esta afirmación se basa en que no se han presentado cambios significativos en el contexto estratégico, ni se han encontrado hallazgos en las auditorías internas o externas que indiquen la necesidad de modificar los riesgos actuales.

Si bien el líder del proceso menciona que no se han presentado cambios significativos en el contexto estratégico, se resalta que de manera proactiva desde el proceso se adelante la actualización del mapa de riesgos de seguridad frente a los lineamientos del DAFP y los cambios en la plataforma estratégica de la entidad, estos cambios podrían tener un impacto en los riesgos de seguridad de la información y requerir una actualización de estos.

Habida cuenta que con corte a 30 de abril de 2024 no se identificó nuevos riesgos, el líder del proceso indica que no se identificó la necesidad de documentar y gestionar nuevos riesgos de seguridad de la información durante el período de monitoreo.

5.2.3.2 ALERTAS:

No se evidencian alertas relacionadas con la posible materialización de los riesgos de gestión identificados para el proceso de Mejoramiento Continuo, pues la efectividad en la administración de los riesgos a través de la ejecución de los adecuados controles ha permitido consolidar en términos de eficacia el sistema de riesgos asociados al proceso.

5.2.3.3 RECOMENDACIONES:

Se recomienda una vez entre en operación el nuevo mapa de procesos de la entidad, verificar los riesgos de seguridad de la información asociados a este proceso y validar la necesidad de incluirlos en el proceso de Dirección Estratégica Institucional, teniendo en cuenta que ambos procesos se fusionan en uno solo.

La gestión del riesgo ha demostrado ser una herramienta valiosa para el proceso S-CA-002 Mejoramiento Continuo. La implementación de controles adecuados, la sensibilización en materia de riesgos y la evaluación continua de la efectividad de las acciones han contribuido a prevenir la materialización de riesgos, mitigar sus impactos y fortalecer el cumplimiento de los objetivos del proceso. Se recomienda continuar con la implementación del plan de acción en pro de mejorar la efectividad de los controles para la gestión de riesgos de seguridad de la información. En este aspecto se recomienda documentar las acciones que se realizan y dejar evidencia con el fin de mejorar el proceso de evaluación.

Se recomienda revisar en la matriz la EVALUACIÓN DEL RIESGO - NIVEL DEL RIESGO RESIDUAL en el sentido de verificar si el tratamiento definido es mitigar / reducir. En el caso de mantener esta acción, se recomienda la formulación de planes de acción.

Se recomienda participar en las jornadas de capacitación y sensibilización en temas de seguridad y privacidad de la información programadas por la entidad.

5.3 CONTROL INTERNO DISCIPLINARIO

5.3.1 S-LE-028 MAPA DE RIESGOS DE GESTIÓN DEL PROCESO CONTROL INTERNO DISCIPLINARIO VERSIÓN 6 ACTA DE MEJORAMIENTO 64 DE ENERO 31 DE 2024

Riesgos de Gestión

1. Posibilidad de afectación reputacional por ejercer inadecuadamente la potestad disciplinaria, debido a interpretación equívoca de la ley, insuficiente capacitación y actualización a los funcionarios de la oficina de control disciplinario interno y Subsecretaría Jurídica en los temas propios del proceso disciplinario, así como la prescripción y caducidad del mismo.

5.3.1.1 OBSERVACIONES:

El proceso Control Interno Disciplinario, mediante radicado en SIPA 3-2024-16165 del 6 de mayo de 2024, con el alcance 3-2024-16504 del 7 de mayo de 2024, remite a la Dirección de Planeación Institucional el monitoreo de primera línea de defensa a los riesgos con corte 30/04/2024. Con la implementación de la nueva herramienta tecnológica Gestiónate- Isolución, se hará efectiva la puesta en operación del nuevo mapa de procesos de la SDP, con la implementación de su respectiva caracterización de proceso, a la luz de una nueva planeación estratégica 2024-2027. En este contexto la nueva denominación del proceso es: S-CA-005 Control Disciplinario Interno.

1. ***Definición del riesgo, sus causas y consecuencias***.

El riesgo es coherente con el objetivo estratégico al cual le aporta el proceso, debido a que es relevante en términos de afectación e impacto económico significativo a la capacidad de la entidad para el logro de sus objetivos. Las causas se mantienen dado que el riesgo se identificó con base en las causas internas y externas según lo definido en el contexto estratégico. Con la implementación de la nueva herramienta tecnológica, Gestiónate- Isolución, se hará efectiva la puesta en operación del nuevo mapa de procesos de la SDP y se determinará si se modifican las causas. Las consecuencias identificadas para el riesgo se mantienen, debido a que éste, no se ha materializado.

2. ***Autoevaluación de la efectividad de los controles***.

Conforme a lo descrito en la revisión realizada por la primera línea de defensa se verifica el desarrollo la implementación de los controles, como se describe a continuación: Control 1: Se verifica la Evidencia SDP-2024-4266, donde se puede observar la revisión **mensual** del profesional en el Sistema de Información de Procesos Automáticos - SIPA. Actas con fechas: 16 de febrero, 1 de marzo, 3 de abril, 3 de mayo, con el asunto: Revisión y seguimiento documentos, formatos, base de datos, plataforma SID y procesos disciplinarios de la Oficina de Control Disciplinario Interno de la Secretaría Distrital de Planeación.

Control 2: El Profesional rectifica mensualmente que las Actas de Reparto S-FO-024 estén correctamente diligenciadas para la adecuada asignación de los asuntos disciplinarios a los profesionales de la oficina.

Control 3: En la evidencia suministrada por la primera línea de defensa, se identifica la

validación mensual que realiza el profesional sobre el correcto diligenciamiento del Sistema de Información Disciplinario Distrital - SIDD a través de la plataforma de la Secretaría Jurídica Distrital.

Control 4: El profesional verifica mensualmente el estado de los procesos disciplinarios activos en la base de datos S-FO-033 y en el Sistema de Información Disciplinario Distrital - SIDD.

3. ***Autoevaluación de la eficacia de las acciones:***

No aplica, dado que la zona final del riesgo residual es "bajo", por lo cual, según la Política de riesgos, no ha sido necesario formular un plan de tratamiento.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

Conforme al seguimiento de la primera línea de defensa y a partir de las evidencias consultadas en el repositorio se concluye que la gestión de riesgo ha sido útil para evitar situaciones que afecten los objetivos del proceso. Las evidencias son verificadas en el repositorio.

5. ***Actualización de Riesgos****:*

Para el proceso Control Disciplinario Interno no se identifica la necesidad de gestionar nuevos riesgos. A la luz de la nueva operación por procesos, se deben revisar los riesgos existentes.

5.3.1.2 ALERTAS:

No aplica, por cuanto el riesgo no se ha materializado.

5.3.1.3 RECOMENDACIONES:

Se recomienda aportar pantallazos específicos para la validación de los controles 3 y 4.

Se recomienda detallar y definir el alcance de los riesgos una vez entre en vigencia la nueva herramienta tecnológica Gestiónate Isolución, y a la luz de una nueva Planeación estratégica 2024-2027.

5.3.2 S-LE-057 MAPA DE RIESGOS DE CORRUPCIÓN DEL PROCESO CONTROL INTERNO DISCIPLINARIO VERSIÓN 2 ACTA DE MEJORAMIENTO 63 DE ENERO 31 DE 2024

Riesgos de Corrupción
1. Posibilidad de trámite indebido de quejas, informes, denuncias y procesos disciplinarios en beneficio de un tercero.

5.3.2.1 OBSERVACIONES:

El proceso Control Interno Disciplinario, mediante radicado en SIPA 3-2024-16165 del 6 de mayo de 2024, con el alcance 3-2024-16504 del 7 de mayo de 2024, remite a la Dirección de Planeación Institucional el monitoreo de primera línea de defensa a los riesgos con corte 30/04/2024.

1. ***Definición del riesgo, sus causas y consecuencias****.*

El riesgo es coherente con el objetivo estratégico al cual le aporta el proceso, debido a que es relevante en términos de afectación e impacto económico significativo a la capacidad de la entidad para el logro de sus objetivos. Las causas se mantienen dado que el riesgo se identificó con base en las causas internas y externas según lo definido en el contexto estratégico. Con la implementación de la nueva herramienta tecnológica, Gestiónate- Isolución, se hará efectiva la puesta en operación del nuevo mapa de procesos de la SDP y se determinará si se modifican las causas. Las consecuencias identificadas para el riesgo se mantienen, debido a que éste, no se ha materializado.

2. ***Autoevaluación de la efectividad de los controles****.*

Conforme a lo descrito en la revisión realizada por la primera línea de defensa se verifica el desarrollo la implementación de los controles, como se describe a continuación:

Control 1: Se verifica la Evidencia SDP-2024-4266, donde se puede observar la revisión **mensual** del profesional en el Sistema de Información de Procesos Automáticos - SIPA. Actas con fechas: 16 de febrero, 1 de marzo, 3 de abril, 3 de mayo, con el asunto: Revisión y seguimiento documentos, formatos, base de datos, plataforma SID y procesos disciplinarios de la Oficina de Control Disciplinario Interno de la Secretaría Distrital de Planeación.

Control 2: Se verifica la Evidencia SDP-2024-4266, donde se puede corroborar que el Jefe de Oficina mensualmente revisa los procesos disciplinarios activos, con el fin de identificar si se presentó trámite indebido. Se verifican las actas de los meses de enero, febrero, marzo y abril, donde se evidencia la revisión en el que se refleja si se presentó dicha situación.

3. ***Autoevaluación de la eficacia de las acciones:***

De acuerdo al seguimiento de la primera línea, la acción: "*Realizar una capacitación dirigida al personal de la Oficina de Control Disciplinario Interno a fin de verificar la apropiación en los temas referentes a los actos de corrupción*", se encuentra sin iniciar. Se espera verificar el desarrollo de esta acción en el monitoreo de agosto 2024.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

Conforme al seguimiento de la primera línea de defensa y a partir de las evidencias consultadas en el repositorio se concluye que la gestión de riesgo ha sido útil para evitar situaciones que afecten los objetivos del proceso. Las evidencias son verificadas en el repositorio.

5. ***Actualización de Riesgos****:*

Para el proceso Control Disciplinario Interno no se identifica la necesidad de gestionar modificar o actualizar los riesgos.

5.3.2.2 ALERTAS:

No aplica, ya que el riesgo no se ha materializado.

5.3.2.3 RECOMENDACIONES:

Se recomienda detallar y definir el alcance de los riesgos una vez entre en vigencia la nueva herramienta tecnológica Gestiónate Isolución, y a la luz de una nueva Planeación estratégica de la entidad 2024-2027.

5.3.3 S-LE-058 MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DEL PROCESO CONTROL DISCIPLINARIO INTERNO VERSIÓN 2 ACTA DE MEJORAMIENTO 92 DE FEBRERO 14 DE 2024

Riesgo de Seguridad de la Información

1. Posibilidad de pérdida de confidencialidad por fallas humanas y hurto de información de los procesos disciplinarios, debido al desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información, manejo manual de información, ausencia de copias de respaldo o backups de la información, copias no controladas e información sensible sin cifrado.

5.3.3.1 OBSERVACIONES:

1. ***Definición del riesgo, sus causas y consecuencias***.

El contexto estratégico del proceso S-CA-003 CONTROL INTERNO DISCIPLINARIO sigue siendo relevante para la Entidad. La necesidad de fortalecer la estructura y la cultura institucional, así como de garantizar la integridad y la eficacia de la gestión pública, sigue siendo una prioridad.

Se recomienda estar vigilante frente a los cambios que puedan surgir con la formalización de los nuevos mapas de procesos que se tiene previsto para mediados de la vigencia 2024.

El riesgo identificado de pérdida de confidencialidad es coherente con el objetivo estratégico de fortalecer la estructura y la cultura institucional. La pérdida de confidencialidad de la información puede tener un impacto negativo en la imagen y la reputación de la Entidad, lo que puede dificultar el logro del objetivo estratégico de fortalecer la estructura y la cultura institucional.

El riesgo identificado de pérdida de confidencialidad es coherente con el objetivo del proceso de Control Interno Disciplinario. La pérdida de confidencialidad de la información puede afectar la integridad y la eficacia del proceso disciplinario, ya que puede poner en riesgo la privacidad de las partes involucradas y dificultar la investigación y sanción de las faltas disciplinarias.

las causas identificadas inicialmente para el riesgo de pérdida de confidencialidad se mantienen. El desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información, el manejo manual de la información, la ausencia de copias de respaldo o Backup de la información, las copias no controladas e información sensible sin cifrado, siguen siendo relevantes.

las consecuencias identificadas inicialmente para el riesgo de pérdida de confidencialidad se mantienen. El daño a la reputación de la Entidad, la pérdida de la confianza de los ciudadanos y la posibilidad de sanciones legales, siguen siendo relevantes.

2. ***Autoevaluación de la efectividad de los controles***.

El líder del proceso ha proporcionado evidencia de que el control de reuniones mensuales con los profesionales para verificar el impulso de los procesos y el control de la documentación de la Oficina (entradas y salidas) se está utilizando. Esta evidencia se encuentra en el Drive dispuesto para publicación de evidencias. Código de la evidencia SDP-2024-4266 (Revisión y seguimiento documentos, formatos, base de datos, plataforma SID y procesos

disciplinarios de la Oficina de Control Disciplinario Interno de la Secretaría Distrital de Planeación. - enero)

Los controles como la capacitación continua y el control efectivo de la información reservada son medidas preventivas que ayudan a mitigar el riesgo de pérdida de confidencialidad.

El líder del proceso ha indicado que no hay hallazgos de auditoría relacionados con los 4 controles establecidos para el tratamiento del riesgo.

3. ***Autoevaluación de la eficacia de las acciones:***

Las acciones formuladas para dar tratamiento al riesgo de pérdida de confidencialidad, como la capacitación continua en seguridad de la información y el control efectivo de la información reservada, están directamente dirigidas a abordar las causas identificadas en la caracterización del riesgo, como el desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información, el manejo manual de la información, la ausencia de copias de respaldo o Backus de la información, las copias no controladas e información sensible sin cifrado.

Las acciones formuladas para dar tratamiento al riesgo se vienen implementando adecuadamente. El líder del proceso proporcionó evidencia de que las acciones de tratamiento del riesgo, como las reuniones mensuales con los profesionales para verificar el impulso de los procesos y el control de la documentación de la Oficina (entradas y salidas), se están implementando. Esta evidencia se encuentra en el Drive dispuesto por la entidad, evidencia SDP-2024-4266 (Revisión y seguimiento documentos, formatos, base de datos, plataforma SID y procesos disciplinarios de la Oficina de Control Disciplinario Interno de la Secretaría Distrital de Planeación. - enero)

El líder del proceso ha indicado que el riesgo de pérdida de confidencialidad no se ha materializado ni se ha identificado como hallazgo en auditorías internas o externas.

Al no haberse materializado el riesgo de pérdida de confidencialidad ni haberse identificado hallazgos en auditorías internas o externas, no ha sido necesario formular correcciones o acciones correctivas.

4. ***Evaluación de la efectividad de la gestión de los riesgos****:*

La implementación de controles como las reuniones mensuales con los profesionales para verificar el impulso de los procesos y el control de la documentación de la Oficina (entradas y salidas), la capacitación continua en seguridad de la información y la mejora de los procedimientos, ha contribuido a prevenir la pérdida de confidencialidad de la información y, por lo tanto, ha evitado situaciones o hechos que podrían afectar el cumplimiento de los objetivos y compromisos del proceso S-CA-003 CONTROL INTERNO DISCIPLINARIO.

5. ***Actualización de Riesgos****:*

El análisis realizado en el marco de la evaluación de segunda línea de defensa no ha identificado cambios significativos en el contexto estratégico, los resultados de las auditorías internas o externas, ni otros aspectos que sugieran la necesidad de modificar la evaluación del riesgo de pérdida de confidencialidad de la información que puedan afectar el cumplimiento de los objetivos del proceso S-CA-003 CONTROL INTERNO DISCIPLINARIO.

No se ha identificado nuevos riesgos que puedan afectar el cumplimiento de los objetivos del proceso S-CA-003 CONTROL

INTERNO DISCIPLINARIO, por lo tanto, no se identifica la necesidad de documentar y gestionar nuevos riesgos en este momento. Los controles establecidos para mitigar los riesgos existentes son adecuados y efectivos.

5.3.3.2 ALERTAS:

De acuerdo con el monitoreo de primera línea de defensa referente a los riesgos identificados de seguridad de la información del Proceso de CONTROL DISCIPLINARIO INTERNO, no se reportan alertas que indiquen que los riesgos se han materializado.

5.3.3.3 RECOMENDACIONES:

Se recomienda establecer medidas que promuevan la participación de todos los integrantes del proceso en las capacitaciones y socializaciones realizadas por la entidad en temas de seguridad y privacidad de la información.

Se recomienda solicitar capacitaciones periódicas dirigidas a todo el personal involucrado en el proceso sobre procedimientos de gestión documental y de manejo de información confidencial.

Se recomienda realizar un análisis proactivo del contexto y la definición de los riesgos frente a la formalización de la nueva plataforma estrategia y la publicación de los nuevos mapas de procesos que tiene proyectada la entidad para mediados del 2024.

Se recomienda fomentar una cultura de gestión de riesgos participativa, donde todos los miembros del equipo estén involucrados en la identificación y evaluación de riesgos, y en la implementación de controles adecuados.

6 OBSERVACIONES, ALERTAS Y RECOMENDACIONES GENERALES

A nivel general, se establecen las siguientes observaciones, alertas y recomendaciones generales:

6.1 OBSERVACIONES:

Con corte al 30 de abril de 2024, se realizó el seguimiento de primera y segunda línea de defensa de riesgos.

6.2 ALERTAS:

6.3 RECOMENDACIONES:

En general los riesgos se deben revisar a la luz del nuevo mapa de procesos y una vez se formule la nueva planeación estratégica para la entidad 2024-2027.

Se sugiere unificar las actividades de divulgación del Código General Disciplinario y del Código de Integridad (antes Código ético), en una jornada general, relacionada con los riesgos de corrupción y si es posible, identificar con la Oficina de Control Disciplinario Interno y la Dirección de Talento Humano, los temas específicos que pueden aplicar a cada proceso, como es el caso de Oficina de Participación y Diálogo Ciudadano, con el fin de prevenir comportamientos inadecuados y manipulación de las estrategias de participación para beneficios particulares.

Con el fin de corroborar la información suministrada desde los procesos, se recomienda aportar evidencia sobre la implementación de los controles y acciones adelantadas al interior de cada uno de los procesos.

Se recomienda participar activamente en las sesiones de capacitación y sensibilización en temas de seguridad y privacidad de la información programadas por la entidad.

Se sugiere adelantar sesiones de capacitación para unificar criterios sobre el diligenciamiento del monitorio de primera línea de defensa.

7 FUENTES DE CONSULTA

Reportes de Seguimiento de primera línea de defensa de los procesos de la Secretaría Distrital de Planeación.

ICONTEC, NTC ISO 31004:2016 Gestión del Riesgo Orientación para la implementación de la NTC-ISO 31000 (Anexo D Monitoreo y Revisión.

ICONTEC, NTC-IEC/ISO 31010:2020 Gestión del Riesgos. Técnicas de evaluación del Riesgo.

POVEDA y CAÑÓN. Guía para la Gestión Integral de Riesgos. Sept. 2015.

CARVAJAL LÓPEZ, Oscar. Control Organizacional. Control Organizacional.2022.

PARDO ÁLVAREZ, José Manuel. Gestión por procesos y riesgo operacional. Alpha editorial y AENOR ediciones (Página 85).