**INFORME MONITOREO DE SEGUNDA LÍNEA DE DEFENSA A LOS MAPAS DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN DE LA SECRETARÍA DISTRITAL DE PLANEACIÓN**



**CORTE A 31 DE AGOSTO DE 2024**

**SECRETARÍA DISTRITAL DE PLANEACIÓN**

**SUBSECRETARÍA DE GESTIÓN INSTITUCIONAL**

**DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES**

**DIRECCIÓN DE PLANEACIÓN INSTITUCIONAL**

**27 DE SEPTIEMBRE DE 2024**



Tabla de contenido

[1 INTRODUCCIÓN 3](#_Toc182297957)

[2 RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 4](#_Toc182297958)

[2.1 PROCESOS ESTRATÉGICOS 4](#_Toc182297959)

[2.1.1 DIRECCIÓN ESTRATÉGICA INSTITUCIONAL 4](#_Toc182297960)

[2.1.2 GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN 14](#_Toc182297961)

[2.1.3 ARTICULACIÓN DEL DIÁLOGO CON EL CIUDADANO 22](#_Toc182297962)

[2.1.4 COMUNICACIÓN ESTRATÉGICA 27](#_Toc182297963)

[2.1.5 INTELIGENCIA PARA LA PLANEACIÓN 29](#_Toc182297964)

[2.1.6 ARTICULACIÓN DEL DIÁLOGO CON LAS INSTITUCIONES 37](#_Toc182297965)

[2.1.7 ARTICULACIÓN DEL DIÁLOGO SUPRADISTRITAL 43](#_Toc182297966)

[2.2 PROCESOS MISIONALES 48](#_Toc182297967)

[2.2.1 PLAN DISTRITAL DE DESARROLLO 48](#_Toc182297968)

[2.2.2 PLAN ORDENAMIENTO TERRITORIAL 53](#_Toc182297969)

[2.2.3 POLÍTICAS PÚBLICAS 62](#_Toc182297970)

[2.3 PROCESOS DE APOYO 67](#_Toc182297971)

[2.3.1 GESTIÓN DEL TALENTO HUMANO 67](#_Toc182297972)

[2.3.2 GESTIÓN CONTRACTUAL 78](#_Toc182297973)

[2.3.3 GESTIÓN DEL SERVICIO A LA CIUDADANÍA 86](#_Toc182297974)

[2.3.4 GESTIÓN ADMINISTRATIVA 88](#_Toc182297975)

[2.3.5 GESTIÓN FINANCIERA 108](#_Toc182297976)

[2.3.6 GESTIÓN JURÍDICA 115](#_Toc182297977)

[2.4 PROCESOS DE EVALUACIÓN 122](#_Toc182297978)

[2.4.1 EVALUACIÓN Y CONTROL 122](#_Toc182297979)

[2.4.2 CONTROL DISCIPLINARIO INTERNO 129](#_Toc182297980)

[3 OBSERVACIONES, ALERTAS Y RECOMENDACIONES GENERALES 136](#_Toc182297981)

[3.1 OBSERVACIONES: 136](#_Toc182297982)

[3.2 ALERTAS: 137](#_Toc182297983)

[3.3 RECOMENDACIONES: 137](#_Toc182297984)

[4 FUENTES DE CONSULTA 139](#_Toc182297985)

# INTRODUCCIÓN

La Secretaría Distrital de Planeación (SDP), en cumplimiento de su compromiso con la gestión transparente y eficiente de los recursos públicos, ha implementado un robusto sistema de gestión de riesgos alineado con los estándares nacionales e internacionales. Este informe presenta los resultados del monitoreo de los riesgos identificados en los procesos de la entidad, realizado por la segunda línea de defensa corte a 31 de agosto de 2024.

La entidad se encuentra enmarcada en el contexto normativo de la Ley 1474 de 2011 y el Decreto Distrital 189 de 2020, los cuales establecen los lineamientos para la prevención y lucha contra la corrupción. Además, la SDP ha adoptado el Modelo Integrado de Planeación y Gestión (MIPG) como marco de referencia para la gestión institucional, considerando la gestión del riesgo como un elemento fundamental para el logro de sus objetivos estratégicos.

El presente informe se encuentra enmarcado en la Política de Administración del Riesgo E-LE-030, versión 19, y se alinea con los lineamientos establecidos en las normas ISO 9001:2015 e ISO 27001:2022. Estas normas internacionales promueven la implementación de sistemas de gestión de calidad y seguridad de la información que integran la gestión de riesgos como un componente fundamental para la mejora continua de los procesos y la protección de los activos de la organización.

El monitoreo de los riesgos se ha llevado a cabo con el objetivo de identificar nuevas amenazas, evaluar la efectividad de los controles existentes y proponer acciones de mejora para garantizar la continuidad de las operaciones y el cumplimiento de los objetivos institucionales. Este ejercicio ha permitido obtener una visión integral de los riesgos a los que está expuesta la SDP, lo que facilita la toma de decisiones informadas y la asignación de recursos de manera eficiente.

La Dirección de Tecnologías de la Información y las Comunicaciones llevó a cabo el monitoreo a los riesgos de seguridad de la información asociados a los procesos definidos en la actual plataforma estratégica de la entidad. Como resultado de esta evaluación, se presentan a continuación las principales recomendaciones de segunda línea de defensa para mitigar los riesgos identificados.

# RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

## PROCESOS ESTRATÉGICOS

### DIRECCIÓN ESTRATÉGICA INSTITUCIONAL

#### MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

**Riesgos 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.

#### OBSERVACIONES

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

La respuesta proporcionada por la primera línea confirma la alineación del proceso E-CA-001 DIRECCIONAMIENTO ESTRATÉGICO con el contexto estratégico actual. Sin embargo, la segunda línea de defensa recomienda realizar de manera proactiva la evaluación del contexto estratégico para identificar posibles cambios que puedan afectar los riesgos y los controles existentes a la luz del rediseño institucional y la nueva caracterización del proceso definida recientemente. Se aclara que la plataforma estratégica 2024-2027 se encuentra en proceso de elaboración y con base en sus lineamientos se realizará en la próxima vigencia la respectiva validación del contexto estratégico del proceso.

La segunda línea de defensa reconoce la alineación general de los riesgos identificados con los objetivos estratégicos, tal como se ha indicado en los monitoreos anteriores. Sin embargo, habida cuenta que recientemente se realizó la nueva caracterización del proceso, se recomienda realizar un análisis previo para evaluar cómo los posibles cambios en los objetivos estratégicos del proceso y las modificaciones podrían afectar a los riesgos actuales. Esto implica identificar nuevos riesgos que puedan surgir y reevaluar la relevancia de los riesgos existentes.

De acuerdo con la primera línea de defensa se reconoce la importancia de alinear los dos riesgos de seguridad de la información identificados con el objetivo actualizado del proceso E-CA-001. Ante la información proporcionada en el último monitoreo, se recomienda que, dada la modificación en la caracterización del proceso, es imperativo priorizar la actualización del mapa de riesgos de seguridad de la información bajo los lineamientos y apoyo de la Dirección de Tecnologías de la Información y las Comunicaciones para garantizar que la actualización del mapa de riesgos se realice de manera conjunta y alineada con los estándares técnicos y de seguridad de la información.

La primera línea ha identificado la necesidad de actualizar el mapa de riesgos debido a cambios en el proceso y a recomendaciones de auditoría lo cual incluye una revisión de las causas y las consecuencias identificadas inicialmente. Esto demuestra una comprensión de la dinámica de la gestión de riesgos y la importancia de mantener el mapa actualizado. La segunda línea de defensa coincide con la evaluación de la primera línea respecto a la necesidad de actualizar el mapa de riesgos. Los cambios en el proceso, la implementación de nuevas herramientas y las recomendaciones de auditoría justifican plenamente esta actualización, por ejemplo, se pueden introducir nuevos riesgos, identificar nuevas causas, generar nuevas consecuencias o modificar la severidad de las existentes.

1. ***Autoevaluación de la efectividad de los controles****:*

La segunda línea de defensa reconoce los esfuerzos realizados por la primera línea para implementar los controles para mitigar los dos riesgos identificados; para el primer riesgo, se formuló la actualización anual del formato A-FO-209 Formato Registro de Activos de Información y la revisión cada vez que se requiera, del lugar de almacenamiento de los documentos permanezca cerrado. En el caso del segundo riesgo, validar cada vez que se requiera que la información generada por el proceso se ajuste a los datos que reposan en los sistemas de información correspondientes y permanezcan en formatos no editables, verificar el resultado de la revisión de usuarios activos realizada por el Oficinal de Seguridad y solicitar mediante incidencia en la Mesa de Ayuda la depuración de usuarios y nivel de acceso a la información con el diligenciamiento del A-FO-010, revisar anualmente los usuarios activos del directorio activo de los servidores de la Dirección de Planeación.

Las respuestas de la primera línea indican que se están implementando controles para mitigar los riesgos identificados y sugiere que se realizan revisiones periódicas con el fin de verificar que se están aplicando de manera consistente y efectiva y que los actores involucrados en el proceso están cumpliendo con sus responsabilidades.

De acuerdo con la respuesta de la primera línea de defensa, no hay hallazgos de auditoria que pusieran en duda la efectividad de los controles establecidos relacionados con las verificaciones realizadas sobre el A-FO-209, el almacenamiento de documentos, la integridad de los datos, la validación de usuarios, el uso del A-FO-10 para gestión de usuarios y el cumplimiento de las políticas de seguridad.

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

La primera línea afirmó en el primer monitoreo, que las acciones están directamente relacionadas con las causas y han sido efectivas. Sin embargo, en el segundo monitoreo, se indica que no hay acciones de tratamiento debido a que la zona de riesgo es baja. En el monitoreo de segunda línea de defensa se verificó que los dos riegos después de aplicar los controles se sitúan en una zona baja confirmando que no se requiere acciones para mitigarlos.

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.

Las respuestas de la primera línea en los monitoreos realizados indican que, no ha sido necesario formular correcciones o acciones correctivas debido a que no se han materializado los riesgos identificados. Desde la segunda línea de defensa se confirma esta evaluación que demuestra la eficacia en la prevención de riesgos, ya que los cinco controles implementados han evitado que los eventos potenciales se materialicen.

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

La gestión del riesgo realizada en el proceso continúa demostrando ser efectiva en la prevención de situaciones que podrían comprometer el cumplimiento de los objetivos y compromisos del proceso. La identificación y mitigación de potenciales amenazas ha sido fundamental para mantener el proceso en curso y la entrega de los productos identificados en el contexto del proceso que apalancan el objetivo estratégico de la entidad propendiendo por la mejora continua.

1. ***Actualización de Riesgos****:*

La primera línea ha identificado la necesidad de actualizar el mapa de riesgos debido a cambios en la caracterización del proceso. Sin embargo, se encuentra a la espera de lineamientos para realizar esta actualización. La segunda línea de defensa reconoce la proactividad de la primera línea al identificar la necesidad de actualizar el mapa de riesgos para garantizar que la gestión de riesgos siga siendo relevante y efectiva.

La segunda línea de defensa reconoce que hasta el momento no se han identificado nuevos riesgos que requieran ser documentados. Sin embargo, se recomienda revisar y en el caso que se requiera actualizar toda la documentación relacionada con el proceso, incluyendo los procedimientos, manuales y registros de incidentes, para identificar posibles riesgos ocultos.

#### ALERTAS

El mapa de riesgos de seguridad fue recientemente actualizado atendiendo los ajustes en la caracterización del proceso, incluyendo su objetivo, alcance y salidas del mismo; así como, la incorporación de las recomendaciones y observaciones generadas en el informe de auditoría al sistema de riesgos realizado por la Oficina de Control Interno, sin embargo, a pesar de las evaluaciones realizadas, siempre existe la posibilidad de que surjan nuevos riesgos que no hayan sido considerados inicialmente. Es necesario validar que el mapa de procesos este alineado a la nueva caracterización del proceso definida para La articulación con el nuevo modelo operacional producto del diseño Institucional.

#### RECOMENDACIONES

Se recomienda que, para garantizar la adecuada gestión de los riegos de seguridad de la información y facilitar la implantación del módulo de seguridad de la información de la solución tecnológica GESTIONATE adquirido recientemente, se capacite a todo el equipo de trabajo en su uso.

Se recomienda la modificación del contexto del proceso, alineándolo con la plataforma estratégica 2024-2027, una vez sea formalizada mediante acto administrativo y aprobada por parte del Comité Institucional de Gestión y Desempeño.

#### MEJORAMIENTO CONTINUO

##### MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN (proceso fusionado con el DIRECCIÓN ESTRATÉGICA INSTITUCIONAL

**Riesgos 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 ramsomware 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 backups de la información.

#### OBSERVACIONES

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

Coincidimos en que los cambios institucionales, especialmente la fusión del proceso con el de Dirección Estratégica Institucional, requieren una revisión integral del mapa de riesgos actual del proceso Dirección Estratégica Institucional incluyendo los riesgos introducidos producto de la unificación de los procesos.

Es importante actuar con celeridad, se recomienda realizar un análisis exhaustivo del nuevo proceso, interfaces, y puntos de contacto para identificar los riesgos inherentes a la seguridad de la información. Una vez identificados los riesgos, priorizarlos en función de su probabilidad de ocurrencia e impacto potencial en la entidad, establecer controles específicos para mitigar los riesgos identificados, considerando las mejores prácticas de seguridad de la información y los lineamientos de la Dirección TIC.

En la Incorporación de la nueva plataforma estratégica el proceso debe asegurarse de que la actualización del mapa de riesgos esté alineada con los objetivos y estrategias de la plataforma estratégica 2024-2027.

En el análisis sobre la coherencia con el objetivo estratégico al cual le aporte el proceso, podemos decir que, en cuanto al primer riesgo, "Pérdida de Integridad por fallas humanas y destrucción de la información", la pérdida de información, especialmente aquella relacionada con procesos, procedimientos y lecciones aprendidas, puede obstaculizar el desarrollo de habilidades del talento humano al limitar el acceso a conocimiento clave.

Producto de la fusión se debe evaluar el impacto en la simplificación de procesos. La destrucción de documentos históricos puede dificultar la identificación de oportunidades de mejora y la simplificación de procesos. La falta de información confiable puede llevar a la toma de decisiones erróneas o basadas en datos incompletos, afectando la eficiencia de la gestión.

En lo referente al segundo riesgo, " Pérdida de integridad por destrucción, hurto y ramsomware de la información de planes de mejoramiento", la pérdida de información sobre planes de mejora puede interrumpir los procesos de seguimiento y evaluación, dificultando la implementación de mejoras continuas. Así mismo, La pérdida de datos puede generar retrasos en la ejecución de tareas y aumentar los costos operativos afectado la eficiencia administrativa.

los riesgos identificados representan una amenaza directa para el logro de los objetivos de la Secretaría y, por lo tanto, requieren una atención especial y medidas de mitigación adecuadas. En el proceso de fusión de los procesos se debe tener especial cuidado en la identificación de los riesgos y evaluar si la destrucción, daño o pérdida de acceso a documentos, registros y datos importantes para la gestión de la Secretaría sigue siendo relevante. De igual forma, se debe revisar y evaluar si la falta de capacitación adecuada en seguridad de la información puede aumentar la vulnerabilidad a amenazas y errores humanos.

La fusión del proceso de mejora continua con el de direccionamiento estratégico institucional introduce un nuevo contexto que requiere una reevaluación exhaustiva de los riesgos identificados inicialmente. Es probable que algunas causas se mantengan, mientras que otras puedan surgir o modificarse debido a los cambios organizacionales y a las nuevas dinámicas del proceso fusionado.

la fusión de procesos representa una oportunidad para fortalecer la gestión de riesgos y mejorar la eficiencia de la entidad. Sin embargo, es fundamental realizar una evaluación exhaustiva de los riesgos existentes y adaptar las medidas de control a las nuevas circunstancias en el nuevo proceso, esto con el fin de poder identificar y gestionar de manera proactiva los riesgos asociados al proceso fusionado, contribuyendo así al logro de sus objetivos estratégicos.

Al igual que las causas, las consecuencias de los riesgos identificados inicialmente pueden experimentar cambios significativos tras la fusión del proceso de mejora continua con el de direccionamiento estratégico institucional. La fusión amplía el alcance del proceso, lo que puede exponer a la entidad a nuevas consecuencias en caso de materialización de los riesgos. Así mismo, se puede generar nuevas consecuencias para los riesgos existentes y dar lugar a la aparición de nuevos riesgos. Es fundamental realizar una evaluación exhaustiva de las consecuencias y desarrollar planes de respuesta adecuados para garantizar la resiliencia de la entidad.

1. ***Autoevaluación de la efectividad de los controles****:*

Si bien se han implementado controles para mitigar los riesgos 1 y 2, es necesario profundizar en el análisis para garantizar su efectividad a largo plazo, especialmente considerando la fusión del proceso de mejora continua con el de direccionamiento estratégico institucional.

Es de resaltar aspectos positivos adelantados con antelación a la fusión. La evidencia presentada y soportada con registros, demuestra un compromiso con la sensibilización de los colaboradores que intervienen en el proceso en materia de seguridad de la información, la implementación de copias de seguridad periódicas es una medida fundamental para proteger la información y la eliminación del archivador metálico y la adopción de una nueva estrategia para el manejo de archivos de gestión son pasos en la dirección correcta.

La observación de la OCI sobre la necesidad de actualizar el mapa de riesgos es crucial para gestionar el cambio de forma adecuada dado que los cambios en el proceso y el entorno pueden generar nuevos riesgos o modificar la relevancia de los riesgos existentes.

Es necesario que desde el nuevo proceso se realice evaluaciones periódicas de la efectividad de los controles para identificar posibles brechas y ajustar las medidas de mitigación según sea necesario. La fusión con el proceso de direccionamiento estratégico institucional puede modificar el impacto de los riesgos existentes. Es necesario realizar un análisis detallado de las interrelaciones entre los procesos y ajustar los controles en consecuencia.

Basado en la información proporcionada, se puede concluir que los controles implementados para los riesgos 1 y 2 son han sido efectivos lo cual se expresa en los siguientes argumentos:

**Riesgo 1 (Pérdida de integridad por fallas humanas y destrucción de la información):**

*Controles implementados:* Divulgación de políticas de seguridad, control de acceso físico, eliminación del archivador metálico.

*Efectividad:* Los controles implementados reducen la probabilidad de pérdida de información debido a acceso no autorizado o manejo inadecuado. Sin embargo, la falta de un plan de acción específico para mitigar este riesgo deja una brecha. Es necesario definir acciones concretas para gestionar la transición de los documentos históricos a un formato digital seguro y establecer un procedimiento para su conservación.

**Riesgo 2 (Pérdida de integridad por destrucción, hurto y ransomware):**

*Controles implementados:* Divulgación de políticas de seguridad, copias de seguridad periódicas.

*Efectividad:* Los controles implementados ayudan a proteger la información de pérdidas accidentales o intencionales. Sin embargo, la falta de un plan de acción específico para mitigar este riesgo deja una brecha. Es necesario definir acciones concretas para mejorar la concientización sobre las amenazas cibernéticas, asegurar que se realicen pruebas de restauración de las copias de seguridad y verificar regularmente los sistemas de seguridad.

La fusión con el proceso de direccionamiento estratégico institucional puede generar nuevos riesgos o modificar el impacto de los riesgos existentes. Es necesario realizar un análisis detallado de las interrelaciones entre los procesos y ajustar los controles en consecuencia.

Si bien el primer monitoreo de primera línea y la primera evaluación de segunda línea no reportaron hallazgos de auditoría directamente relacionados con los cinco controles, el segundo monitoreo de primera línea introduce un nuevo elemento: las recomendaciones de la OCI en el informe de auditoría al sistema de riesgos.

Estas recomendaciones, aunque no son directamente hallazgos de auditoría asociados a cada control específico, sí indican áreas de mejora en la gestión de riesgos y en la implementación de los controles. Sugieren que la efectividad de los controles podría verse comprometida si no se toman las acciones correctivas necesarias, por esta razón, es importante que se evalúen estas recomendaciones en la integración con el nuevo proceso.

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

Las evaluaciones iniciales sugieren que las acciones implementadas están alineadas con las causas de los riesgos. Sin embargo, la ausencia de planes de acción dificulta una evaluación más rigurosa de esta afirmación. Aunque se mencionan las acciones implementadas, no se presenta evidencia cuantitativa o cualitativa que demuestre su eficacia en la reducción de las causas de los riesgos.

La fusión del proceso puede generar nuevas interdependencias y riesgos que no han sido completamente considerados en las acciones actuales. En la transición al nuevo proceso se debe tener presente las recomendaciones de la OCI que señalan la necesidad de revisar y ajustar las acciones implementadas, especialmente en lo que respecta a la identificación de las causas raíz de los riesgos.

Se recomienda revisar a fondo los controles y acciones implementados para asegurar que estén directamente vinculados al proceso y no delegados a otras áreas como la Dirección de TIC. Así mismo, es necesario revisar y, de ser pertinente, modificar el tratamiento asignado a los dos riesgos identificados. En particular, se debe prestar atención al hecho de que, aunque se definió mitigar o reducir los riesgos, no se han formulado planes de acción concretos para alcanzar este objetivo.

La información proporcionada sobre las acciones realizadas para mitigar cada riesgo corresponde a los controles implementados y no a planes de acción formulados desde el proceso. No obstante, desde la segunda línea de defensa se realizó una evaluación detallada por cada riesgo.

**Riesgo 1: Posibilidad de Pérdida de Integridad por fallas humanas y destrucción de la información**

**Divulgación de políticas de seguridad:** La evidencia presentada (A-LE-375) demuestra que se han realizado esfuerzos para difundir las políticas de seguridad. Sin embargo, es necesario evaluar la efectividad de estas capacitaciones a través de encuestas o pruebas de conocimiento para asegurar que los empleados hayan interiorizado las políticas.

**Control de acceso físico:** La verificación del registro de ingresos por parte de la empresa de vigilancia es una práctica positiva. No obstante, se debe evaluar la frecuencia de estas verificaciones y si existen mecanismos para garantizar que las personas autorizadas sean las únicas que ingresen a las áreas restringidas.

**Eliminación del archivador metálico:** Esta medida es un paso importante para reducir el riesgo de pérdida física de documentos. Sin embargo, es fundamental garantizar que la transición a un sistema de gestión de documentos digital se haya realizado de manera segura y que se hayan establecido los controles necesarios para proteger la información digital.

**Riesgo 2: Posibilidad de Pérdida de Integridad por destrucción, hurto y ransomware**

**Divulgación de políticas de seguridad:** Al igual que en el riesgo 1, es necesario evaluar la efectividad de las capacitaciones y la comprensión de las políticas por parte de los funcionarios.

**Copias de respaldo:** La realización de copias de respaldo periódicas es una práctica esencial. Sin embargo, se deben establecer procedimientos claros para realizar pruebas de restauración de forma regular y garantizar que las copias de respaldo estén almacenadas en un lugar seguro y accesible.

Durante la fusión del proceso, es necesario analizar cuidadosamente si los riesgos identificados previamente siguen siendo relevantes. Aquellos riesgos que se consideren pertinentes deben ser integrados al nuevo proceso, asegurando que se formulen planes de acción detallados para su mitigación.

Aunque hasta el momento no se ha evidenciado la materialización de los riesgos, las recomendaciones de la OCI indican la necesidad de realizar mejoras en la gestión del riesgo. Es fundamental tomar las acciones necesarias para garantizar la efectividad continua de los controles y prevenir la materialización de los riesgos identificados. 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.

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

Si bien la gestión de riesgos ha sido adecuada y útil para evitar situaciones indeseables que afecten el cumplimiento de los objetivos y compromisos a cargo del proceso, es necesario fortalecerla mediante la implementación de planes de acción detallados, la definición de indicadores de desempeño y el seguimiento continuo de los riesgos. La fusión con el proceso de direccionamiento estratégico representa una oportunidad para mejorar la gestión de riesgos y alinear las acciones con los objetivos estratégicos de la organización.

1. ***Actualización de Riesgos****:*

La integración con el proceso de Dirección Estratégica Institucional y la implementación del sistema de gestión GESTIONATE generan nuevas dinámicas y riesgos en el proceso. Por lo tanto, resulta crucial actualizar el mapa de riesgos de seguridad de la información del nuevo proceso para garantizar la alineación con los objetivos y alcance actualizados. La Dirección de Planeación Institucional (DPI) está a la espera de las directrices de la Dirección TIC para llevar a cabo esta actualización, considerando los cambios institucionales y las funcionalidades del nuevo software.

El líder del proceso no ha identificado nuevos riesgos de seguridad durante el período evaluado (hasta el 30 de agosto de 2024). Sin embargo, se recomienda una revisión más exhaustiva, considerando las nuevas funcionalidades del software y los posibles impactos en la seguridad de la información.

Es necesario actualizar el mapa de riesgos del nuevo proceso para reflejar los cambios en el entorno organizacional.

#### RECOMENDACIONES

A partir del análisis detallado de los hallazgos y conclusiones presentados en los capítulos anteriores, se proponen en este apartado una serie de recomendaciones estratégicas y operativas para el nuevo proceso. Estas sugerencias tienen como finalidad fortalecer y optimizar los procesos en pro de mitigar los riesgos identificados.

* Revisar el nuevo proceso para identificar las actividades que exponen la información a riesgos y establecer controles adecuados.
* Priorizar la actualización del mapa de riesgos considerando los cambios en el proceso y las recomendaciones de la OCI.
* Establecer un sistema de gestión de la documentación que permita registrar de manera sistemática la aplicación de los controles y los resultados de las evaluaciones.
* Estar atentos a los programas de capacitación para que el personal vinculado al proceso adquiera conocimientos sólidos en seguridad de la información, especialmente en relación con el software Gestionate y las mejores prácticas.

### GOBIERNO DE TECNOLOGÍAS DE LA INFORMACIÓN

#### MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

**Riesgos de Seguridad de la Información**

1. 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.

#### OBSERVACIONES

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

El proceso ha sido actualizado para reflejar los cambios organizacionales recientes, especialmente aquellos derivados del Decreto 432 de 2022. Se han revisado y actualizado instrumentos clave como la caracterización y la matriz DOFA. A pesar de estos avances, se sugiere continuar trabajando en la alineación del proceso con la nueva caracterización definida para el proceso de Gobierno de TI, a fin de garantizar una completa adaptación a la nueva realidad organizacional. Asimismo, se recomienda estar atentos a la formalización y puesta en marcha del nuevo modelo estratégico de la entidad para asegurar que el proceso contribuya de manera efectiva a los objetivos estratégicos.

La coherencia entre los riesgos identificados y el objetivo estratégico de Gobierno Digital (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.) es evidente. Los riesgos planteados son relevantes y su materialización podría tener un impacto significativo en el logro de los objetivos de transformación digital.

Las respuestas proporcionadas por la primera línea de defensa demuestran una comprensión clara de la relación entre los riesgos identificados y el objetivo del proceso de Soporte Tecnológico (ahora Gobierno de TI). Se ha establecido una conexión directa entre los riesgos y la capacidad del proceso para cumplir con su objetivo principal de garantizar la prestación de servicios de TI de manera oportuna y efectiva. La coherencia entre los riesgos identificados y el objetivo del proceso de Gobierno de TI es indudable dado que los cinco (5) riesgos planteados son relevantes y su materialización podría comprometer directamente la capacidad del proceso para cumplir con su objetivo de garantizar la prestación de servicios de TI de manera oportuna y efectiva.

Las respuestas proporcionadas por la primera línea de defensa evidencian la alineación con la guía del DAFP para la gestión del riesgo, los ajustes a las causas para reflejar nuevos hallazgos o recomendaciones y un seguimiento adecuado de las causas de los riesgos identificados.

Se ha realizado una revisión periódica de las causas y en algunos casos se han realizado ajustes menores para reflejar cambios en el entorno o nuevas recomendaciones, como por ejemplo: las contenidas en el Rad. 3-2024-26859 Informe de seguimiento a la Gestión del Riesgo en la Secretaría Distrital de Planeación con corte al 30/04/2024. En general, las causas identificadas inicialmente para los riesgos se mantienen vigentes.

En general, las consecuencias identificadas inicialmente para los riesgos se mantienen vigentes y han sido adecuadamente actualizadas para reflejar los cambios en el entorno. Sin embargo, es importante destacar que la creciente dependencia de las tecnologías de la información aumenta la potencialidad y gravedad de las consecuencias de los riesgos por ello se recomienda contar con un plan de respuesta a incidentes que detalle las acciones a seguir en caso de materialización de los riesgos.

1. ***Autoevaluación de la efectividad de los controles****:*

Dada la especificidad en el monitoreo de primera línea de defensa, La evaluación detallada de la efectividad de los controles implementados por el proceso para mitigar los cinco riesgos identificados con la tecnología de la información se condensó el análisis por cada riesgo en el mapa de procesos.

En este apartado se resumen de las observaciones para cada riesgo así:

**Riesgo 1: Pérdida de Disponibilidad de Activos de Hardware**

El proceso de Gestión de TI ha implementado controles preventivos y correctivos integrales para garantizar la disponibilidad de los activos de hardware. Estos incluyen mantenimiento regular, monitoreo y procedimientos de respuesta a incidentes. El monitoreo de primera línea proporciona evidencia detallada, como registros de mantenimiento, informes de incidentes y datos de monitoreo, para respaldar estas afirmaciones.

**Riesgo 2: Pérdida de Integridad de Activos de Hardware**

El proceso ha tomado medidas para proteger la integridad de los activos de hardware a través de controles de acceso de usuarios, medidas de seguridad física y monitoreo regular. Las evidencias proporcionadas dan cuenta de la aplicación de controles como revisiones de acceso de usuarios, inspecciones de seguridad física y evaluaciones de vulnerabilidades.

**Riesgo 3: Pérdida de Disponibilidad de Activos de Software**

Al interior del proceso se ha implementado controles para garantizar la disponibilidad de los activos de software, incluidos procedimientos de respaldo, procesos de gestión de cambios y gestión de vulnerabilidades. Esto se evidencia en la ejecución de programas de respaldo, solicitudes de cambio y escaneos de vulnerabilidades.

**Riesgo 4: Pérdida de Confidencialidad de Activos de Software**

Desde el proceso se informó que se ha implementado controles para proteger la confidencialidad de los activos de software, como el cifrado, los controles de acceso y la gestión de vulnerabilidades. El monitoreo de primera línea incluye evidencia de certificados de cifrado, controles de acceso y evaluaciones de vulnerabilidades.

Basándose en la evidencia proporcionada, el proceso de Gestión de TI parece tener un sólido entorno de control para abordar los riesgos identificados. Algunos puntos clave surgen de reporte de primera línea de defensa son:

* Se ha implementado una amplia gama de controles para abordar diversos riesgos propendiendo por la integralidad en la gestión.
* Existe evidencia de monitoreo y pruebas regulares de los controles.
* El proceso busca activamente mejorar su entorno de control a través de evaluaciones y actualizaciones continuas.
* El informe proporciona un alto nivel de detalle, incluyendo procedimientos específicos, evidencia y referencias a documentación de soporte.

El informe incluye enlaces a varios documentos y evidencia, lo que es útil para el monitoreo y la identificación de posibles desviaciones. Es importante tener en cuenta que la gestión de riesgos es un proceso continuo y la efectividad de los controles debe reevaluarse periódicamente.

Desde la segunda línea se analizó como los controles previenen o mitigan los riesgos, evidenciado la efectividad de los controles internos implementados por la primera línea de defensa para la mitigación de los riesgos identificados. A través de una revisión detallada de la información proporcionada, se concluyó por cada riesgo lo siguiente:

**Riesgo 1: Pérdida de Disponibilidad de Activos Tipo Hardware**

*Fortalezas:* Se cuenta con un plan de mantenimiento preventivo y correctivo, monitoreo diario de equipos, y un proceso de gestión de cambios.

*Áreas de mejora:* Se recomienda profundizar en el análisis de causas raíz de las fallas, integrar el mantenimiento preventivo y correctivo, y utilizar herramientas de monitoreo más sofisticadas.

**Riesgo 2: Pérdida de Integridad de Activos Tipo Hardware**

*Fortalezas:* Se realizan inspecciones regulares a los controles de acceso físico, se gestiona el acceso de usuarios privilegiados, y se cuenta con un modelo de seguridad y privacidad.

*Áreas de mejora:* Se sugiere especificar los controles relacionados con la integridad de los activos de hardware en el modelo de seguridad y evaluar la vulnerabilidad de los sistemas de control de acceso.

**Riesgo 3: Pérdida de Disponibilidad de Activos Tipo Software**

*Fortalezas:* Se realizan copias de seguridad periódicas, se gestionan los cambios de manera controlada, y se realizan pruebas funcionales y no funcionales.

*Áreas de mejora:* Se recomienda asegurar que las pruebas de restauración se realicen con regularidad y que se cubran todos los tipos de cambios en el proceso de gestión de cambios.

**Riesgo 4: Pérdida de Confidencialidad de Activos Tipo Software**

*Fortalezas:* Se implementan certificados seguros, se mantiene actualizado el software, y se gestiona el acceso a los datos de pruebas.

*Áreas de mejora*: Se sugiere revisar la frecuencia de las depuraciones de usuarios y evaluar la necesidad de implementar medidas adicionales para proteger la confidencialidad de los datos de pruebas.

**Riesgo 5: Pérdida de Confidencialidad por Divulgación Ilegal de Información**

*Fortalezas:* Se cuenta con políticas de seguridad y privacidad actualizadas, se gestiona el acceso a la información a través del directorio activo, y se mantiene un inventario actualizado de los activos de información.

*Áreas de mejora:* Se recomienda evaluar la necesidad de implementar medidas adicionales para proteger la información confidencial, como la encriptación de datos en reposo y en tránsito.

De manera general, el proceso cuenta con una sólida base de controles, existe un reconocimiento de la necesidad de mejorar continuamente los controles y procesos y se cuenta con una documentación detallada de los controles y procedimientos. Se identificaron algunas áreas donde se pueden fortalecer los controles, como la integración del mantenimiento preventivo y correctivo, la evaluación de la vulnerabilidad de los sistemas de control de acceso, y la implementación de medidas adicionales para proteger la confidencialidad de la información.

En general, las respuestas dadas desde el proceso indican que no se han encontrado hallazgos significativos que cuestionen la efectividad de los controles implementados para mitigar los riesgos de seguridad de la información. Sin embargo, es importante verificar si existen otras causas raíz de los riesgos identificados para identificar oportunidades de mejora. Esto permitirá implementar medidas de prevención más efectivas y reducir la probabilidad de futuros incidentes.

Es importante realizar una evaluación detallada de la naturaleza de los controles implementados para cada riesgo, se debe asegurar que exista un equilibrio adecuado entre controles preventivos y detectivos, y que los controles sean suficientes para mitigar los riesgos identificados.

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

Las acciones formuladas para dar tratamiento al riesgo están bien alineadas con las causas identificadas y demuestran un enfoque proactivo para la gestión de la seguridad de la información. Las respuestas proporcionadas por la primera línea de defensa demuestran una comprensión clara de cómo las acciones implementadas abordan las causas raíz de los riesgos identificados. Por ejemplo: las actividades de depuración de usuarios y capacitación son fundamentales para fortalecer la seguridad de la información.

Desde el proceso se proporcionan ejemplos concretos de cómo las acciones contrarrestan las causas con un enfoque integral de riesgos ejecutando acciones que abordan múltiples riesgos para su mitigación. Es importante resaltar que la evaluación de la eficacia de las acciones debe ser un proceso continuo. Los riesgos y el entorno de seguridad evolucionan constantemente, por lo que es necesario adaptar las acciones en consecuencia.

Las respuestas proporcionadas y La evidencia presentada por la primera línea de defensa indican que las acciones formuladas para tratar los riesgos se están implementando de manera adecuada. La existencia de un seguimiento periódico, la generación de evidencias y la implementación de mecanismos de control son prácticas positivas que contribuyen a garantizar la eficacia de las acciones.

De acuerdo con la primera línea de defensa, los riesgos identificados no se han materializado en incidentes de seguridad y no han sido detectados en auditorías. Esto sugiere que las acciones de mitigación y los controles implementados son efectivos. Al no haberse materializado los riesgos, no ha sido necesario implementar acciones correctivas específicas. Sin embargo, es importante destacar la importancia de mantener una postura proactiva y prepararse para posibles incidentes.

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

Las respuestas proporcionadas por la primera línea de defensa demuestran claramente que la gestión de riesgos ha sido una herramienta valiosa para la entidad. Al identificar y mitigar los riesgos de manera proactiva, se ha logrado proteger la información, garantizar la continuidad del negocio y cumplir con los objetivos y compromisos estratégicos y del proceso

1. ***Actualización de Riesgos****:*

Las respuestas proporcionadas por la primera línea de defensa evidencian una comprensión de la importancia de mantener actualizados los riesgos. Se reconoce que los cambios en el contexto estratégico y el entorno tecnológico pueden generar nuevos riesgos o modificar los existentes. Coincidimos con la primera línea en que la falta de documentación formal sobre los cambios derivados del rediseño institucional dificulta una evaluación precisa del impacto en los riesgos identificados. Sin embargo, es fundamental realizar un análisis más profundo y detallado una vez se formalice la nueva plataforma tecnológica.

No se han identificado nuevos riesgos que requieran ser documentados y gestionados de manera inmediata. Los cambios en el entorno pueden generar nuevos riesgos y es importante mantener un enfoque proactivo. Sin embargo, es fundamental definir de manera concreta los tipos de nuevos riesgos que podrían surgir y realizar el proceso establecido por la entidad para identificarlos y gestionarlos.

#### ALERTAS

Algunos controles están clasificados como correctivos lo cual no es claro dado que se indica que no se ha materializado ninguno de los riesgos identificados. Es importante establecer una clasificación consistente para facilitar la evaluación y el seguimiento.

#### RECOMENDACIONES

A partir del análisis detallado de los procesos de gestión de TI evaluados, se identificaron oportunidades de mejora significativas. El presente numeral presenta un conjunto de recomendaciones estratégicas orientadas a optimizar la eficiencia, la seguridad y la alineación de los servicios de TI con los objetivos organizacionales:

* Realizar evaluaciones de riesgos periódicas: Para identificar nuevos riesgos y actualizar los controles existentes.
* Implementar un programa de concientización sobre seguridad: Para sensibilizar a los empleados sobre la importancia de la seguridad de la información.
* Realizar pruebas de intrusión: Para evaluar la efectividad de los controles de seguridad.
* Mantenerse actualizado sobre las últimas amenazas y vulnerabilidades: Para adaptar los controles a las nuevas amenazas.
* Este resumen proporciona una visión general de los hallazgos del informe. Para una evaluación más detallada, se recomienda revisar el informe original y las evidencias presentadas.

Recomendaciones específicas por Control:

* Control C1 (R1): Si bien se actualiza el plan de mantenimiento, sería importante evaluar la frecuencia con la que se revisan y actualizan los activos incluidos en el plan. Además, se podría considerar la implementación de un sistema de gestión de activos de TI para tener un inventario más preciso y actualizado.
* Control C6 (R1): Aunque se realiza un plan de gestión de vulnerabilidades, se recomienda profundizar en el análisis de las causas raíz de las vulnerabilidades encontradas para implementar medidas preventivas más efectivas.
* Control C1 (R2): La periodicidad de la depuración de usuarios debería estar alineada con los riesgos asociados a cada tipo de usuario y con las mejores prácticas de seguridad.
* Control C2 (R2): Se recomienda realizar evaluaciones periódicas del Modelo de Seguridad y Privacidad de la Información para identificar áreas de mejora y garantizar su continua adecuación.
* Control C3 (R3): Es importante verificar que las pruebas de restauración se realicen con regularidad y que se documenten los resultados.
* Control C1 (R4): Se ha implementado un proceso sólido para identificar y proteger las aplicaciones críticas. Sin embargo, es importante evaluar la periodicidad de las evaluaciones de criticidad y asegurarse de que los certificados estén siempre actualizados.
* Control C2 (R4): Se evidencia un compromiso con la actualización del software y la migración a infraestructuras seguras. No obstante, es fundamental establecer métricas para medir la efectividad de estas acciones y garantizar que se aborden todas las vulnerabilidades identificadas.
* Control C3 (R4): Se ha establecido un proceso para solicitar y gestionar los datos de prueba. Sin embargo, se debe prestar atención a la confidencialidad de estos datos y establecer medidas de protección adicionales, como la encriptación.
* Control C4 (R4): La depuración de usuarios se realiza de manera periódica, pero es importante evaluar si la frecuencia es adecuada y si se están utilizando herramientas automatizadas para facilitar el proceso.
* Control C4 (R4): Se recomienda establecer un proceso formal para la clasificación de las aplicaciones críticas y para la priorización de las medidas de seguridad.
* Control C1 (R5): Se ha priorizado la revisión y actualización de las políticas de seguridad, pero es necesario acelerar la transición al nuevo sistema de gestión para garantizar una gestión más eficiente de las políticas.
* Control C2 (R5): La política de bloqueo de pantalla se aplica de manera consistente, pero se debe evaluar la posibilidad de implementar medidas de autenticación más robustas, como la autenticación de dos factores.
* Control C3 (R5): Se ha iniciado el proceso de actualización de los registros de activos de información, pero es importante completar esta tarea lo antes posible para tener una visión completa y actualizada de los activos de la SDP.

### ARTICULACIÓN DEL DIÁLOGO CON EL CIUDADANO

#### MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN (PARTICIPACIÓN Y COMUNICACIÓN)

**Riesgos de Seguridad de la Información**

1. Posibilidad de Pérdida de Disponibilidad por fallas humanas, fallas del equipo, destrucción de la información, hurto de la información y saturación del sistema de información, de las bases de datos, evidencias de los procesos de participación y comunicación 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 backup de la información, deficiencia en la autorización de permisos de la información, ausencia o deficiencia en los sistemas de autenticación de los aplicativos.

2. Posibilidad de Pérdida de Confidencialidad por fallas humanas, uso no autorizado del equipo, copia fraudulenta del software, hurto de Información 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 por desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información, deficiencia en la autorización de permisos de la información, copias no controladas, ausencia de validación de autenticación de la información.

#### OBSERVACIONES

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

Si bien el contexto estratégico identificado inicialmente se mantiene como base, la primera línea de defensa reconoce que es fundamental revisar la dinámica y evolución del entorno en el que opera la SDP. Los cambios en el marco normativo, las nueva tecnologías, los cambios y definición de nuevas iniciativas, las demandas ciudadanas, las prioridades gubernamentales definidas en el nuevo plan de desarrollo distrital y la articulación con la nueva plataforma estratégica pueden generar alteraciones en el contexto estratégico y el del proceso, razón por la cual, desde el proceso se está a la espera de la formalización del nuevo contexto estratégico para dar inicio a la alineación con el del proceso.

La alineación inicial de los riesgos con los dos objetivos estratégicos; 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 segundo, diseñar y generar espacios colaborativos de participación ciudadana con enfoque diferencial, en la formulación, seguimiento y evaluación de los instrumentos y procesos de planeación, parece adecuada. En este sentido, de acuerdo con la respuesta de primera línea de defensa es fundamental realizar una revisión exhaustiva y actualizada en el marco del nuevo contexto estratégico de la entidad para garantizar que los riesgos identificados siguen siendo relevantes.

Si bien los riesgos identificados parecen estar inicialmente alineados con el objetivo del proceso, elaborar e implementar estrategias de participación y comunicación internas y externas de acuerdo a los lineamientos establecidos por la Administración Distrital, para posicionar a la SDP y fortalecer las decisiones de la planificación del desarrollo integral de la ciudad. Es fundamental verificar si los objetivos del proceso han evolucionado o si se han definido nuevos objetivos como resultado de los cambios en el entorno o en la estrategia organizacional estableciendo una relación clara entre cada riesgo y el impacto que puede tener en el logro de los objetivos del proceso. La coherencia entre los riesgos y los objetivos del proceso es esencial para garantizar la eficacia de las medidas de mitigación, especialmente en un contexto de cambio como el que experimenta actualmente la SDP con relación al rediseño institucional.

Si bien las causas identificadas inicialmente para los riesgos como la ausencia de mecanismos de identificación y autenticación, el desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información, la configuración incorrecta de parámetros y la falta de mantenimiento adecuado parecían pertinentes en el momento de la evaluación inicial, considerando los cambios en el entorno tecnológico, la evolución del proceso, es fundamental realizar una revisión exhaustiva y actualizada.

Las consecuencias identificadas inicialmente, como la pérdida de disponibilidad de la información de las evidencias de los procesos de participación y comunicación y documentos de gestión administrativa y misional, la pérdida de confidencialidad de las evidencias de los procesos de participación y comunicación y documentos de gestión administrativa y misional, y el impacto en la reputación parecen se pertinentes. Se recomienda que una vez se cuente con la formalización de la nueva plataforma estratégica, el proceso "Articulación del diálogo con el ciudadano", reevalúe las consecuencias de los riesgos en función de su impacto en los objetivos estratégicos de la entidad. Es posible que las consecuencias iniciales ya no sean tan relevantes o que hayan surgido nuevas consecuencias.

1. ***Autoevaluación de la efectividad de los controles****:*

La respuesta de primera línea sugiere que los controles implementados para mitigar los riesgos de pérdida de disponibilidad y confidencialidad están siendo utilizados en cierta medida. Sin embargo, al revisar la evidencia dispuesta se encontró actas de las reuniones de equipo de la OPDC, donde de cierta forma se sensibiliza sobre el manejo de evidencias y disponibilidad de información, cumplimiento de registro de evidencias y capacitaciones que soporta la gestión de los procesos de participación y que hace parte del primer control del riesgo 1 “Posibilidad de Pérdida de Confidencialidad 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”, no se logró establecer la inclusión en la agenda de temas relacionados con los nueve controles establecidos para los dos riesgos de seguridad identificados en el mapa de procesos, tampoco se pudo observar de forma clara que, en el desarrollo de las reuniones se mencione la aplicación de los controles; la aplicación de los procedimientos para asignar y revocar los derechos de acceso a los usuarios para todos los sistemas y servicios, el mantenimiento preventivo a los equipos para asegurar su correcto funcionamiento, revisión de la ubicación de los equipos y acceso seguro a la información, acceso restringido a la información de acuerdo con la políticas de seguridad y privacidad de la información, la realización de copias de respaldo de la información.

Es importante corroborar que los controles se están aplicando de manera consistente en todas las áreas del proceso y en todos los casos, por ello, para los próximos monitoreos se recomienda presentar registros y evidencias claras, completas y actualizadas que faciliten la verificación de la aplicación y cumplimiento de los controles.

Si bien la ausencia de incidentes de seguridad es un indicador positivo, es fundamental realizar una evaluación más profunda para determinar si los controles implementados para mitigar los riesgos específicos de pérdida de disponibilidad y pérdida de confidencialidad son realmente efectivos. Es crucial verificar que cada control esté diseñado para abordar de manera directa los riesgos identificados. Por ejemplo: Para la pérdida de disponibilidad, los respaldos regulares, los planes de recuperación ante desastres y el mantenimiento preventivo a los equipos para asegurar su correcto funcionamiento están diseñados para garantizar el acceso continuo a la información. Para la pérdida de confidencialidad: Los controles de acceso, la encriptación de datos, las políticas de seguridad y las capacitaciones en seguridad de la información están destinados a proteger la confidencialidad de los datos.

La respuesta de la primera línea de defensa infiere que la ausencia de hallazgos de auditoría asociados a los controles implementados en el proceso es un indicador positivo que sugiere que los controles están funcionando de manera efectiva. No obstante, la ausencia de hallazgos en una auditoría puntual no garantiza que no existan problemas en otros momentos. Se recomienda realizar autoevaluaciones pueden ayudar a identificar posibles desviaciones de los controles antes de que se conviertan en problemas mayores.

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

Aunque la primera línea de defensa ha indicado que las acciones están alineadas con las causas de los riesgos, es necesario realizar un análisis más detallado para confirmar esta afirmación, por cuanto no se observa la definición de planes de acción como complemento a los controles en el mapa de riegos. En el caso que se llegaren a formular se sugiere detallar las acciones implementadas, las fechas de cumplimiento, los responsables y los resultados obtenidos y realizar un seguimiento continuo.

Así mismo, se recomienda revisar el tratamiento definido después de la aplicación de los controles, es de recordar que, si la opción 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.

Si bien la primera línea de defensa ha indicado que las acciones se están implementando adecuadamente, es fundamental realizar una evaluación más profunda para confirmar esta afirmación y garantizar que las medidas de mitigación estén siendo efectivas, especialmente considerando la ausencia de planes de acción formales.

Se recomienda que en el caso de formular acciones, se presente evidencia tangible de la implementación de las acciones, como registros de reuniones, informes de progreso, correos electrónicos, etc. Esta evidencia debe demostrar que las acciones se están llevando a cabo de acuerdo con lo planificado.

Dada la ausencia de planes de acción formales, se recomienda a la primera línea de defensa revise la valoración de los riesgos después de la aplicación de controles y en el caso que aplique, elabore planes de acción detallados para cada acción, incluyendo objetivos específicos, responsables, plazos y métricas de seguimiento. Estos planes de acción deben estar directamente vinculados a los riesgos identificados y a los controles establecidos. De esta manera, se podrá asegurar que las acciones implementadas sean realmente efectivas en la protección de la información de la entidad y en la mejora continua del proceso E-CA-003 PARTICIPACIÓN Y COMUNICACIÓN.

La afirmación de la primera línea de defensa de que los riesgos identificados no se han materializado y no se han evidenciado en hallazgos de auditoría es un indicador positivo, la ausencia de hallazgos en una auditoría puntual no garantiza que no existan problemas en otros momentos. Es importante realizar un autodiagnóstico periódico para identificar cualquier desviación de los controles antes de que se conviertan en problemas mayores y que el resultado permita confirmar la efectividad de las medidas de control implementadas y garantizar la sostenibilidad de esta situación.

En relación con los riesgos específicos identificados en el proceso PARTICIPACIÓN Y COMUNICACIÓN, dada la naturaleza de la información manejada en este proceso se sugiere monitorear de cerca los riesgos de pérdida de disponibilidad y confidencialidad, y ajustar las medidas de control si es necesario. Así mismo, se recomienda prestar especial atención a los riesgos relacionados con la participación ciudadana, como la falta de aplicación de políticas de seguridad o la manipulación de la información.

La primera línea de defensa ha indicado que los riesgos identificados no se han materializado y no se han evidenciado en hallazgos de auditoría, no ha sido necesario formular correcciones o acciones correctivas específicas hasta el momento. Esta afirmación indica una gestión de riesgos efectiva para para minimizar el impacto sobre las operaciones de la entidad.

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

La primera línea de defensa ha indicado que la gestión de riesgos ha sido útil para evitar situaciones que afecten el cumplimiento de los objetivos. Desde la segunda línea de defensa, se identifica que ha contribuido a mantener la disponibilidad de la información necesaria para la toma de decisiones de manera oportuna y confiable, lo cual indica que los controles de seguridad están funcionando correctamente y se están aplicando los estándares internacionales de seguridad de la información.

Además de lo anterior, es importante resaltar la visión sobre la efectividad de la gestión de riesgos realizada por el líder del proceso y la identificación de áreas de mejora para garantizar que los riesgos estén bajo control y su gestión sea cada vez más efectiva contribuyendo al éxito a largo plazo del proceso PARTICIPACIÓN Y COMUNICACIÓN. y a que la entidad esté preparada para enfrentar futuros desafíos.

1. ***Actualización de Riesgos****:*

Desde la primera línea de defensa se ha identificado la necesidad de evaluar y ajustar los riesgos de seguridad de la información a la luz de los cambios en el proceso y la nueva plataforma estratégica. En particular, se hace necesario realizar un análisis detallado de los nuevos procesos de Comunicación Estratégica y Articulación del diálogo con el ciudadano para identificar los nuevos riesgos asociados a cada uno de ellos, esto permitirá identificar cambios que pueden afectar los riesgos existentes o generar nuevos riesgos y facilitará el establecimiento de las acciones necesarias para mitigar los nuevos riesgos identificados. De esta manera, se podrá garantizar que la gestión de riesgos esté actualizada y sea efectiva en la protección de la información de la entidad.

#### ALERTAS

Coincidimos con la primera línea de defensa en que los cambios significativos en la estructura organizacional y la implementación de una nueva plataforma estratégica demandan una revisión exhaustiva y actualización de los riesgos de seguridad de la información identificados previamente. Bajo esta óptica, una vez dispuesta la nueva plataforma estratégica y la definición del nuevo mapa de riesgos, se debe emprender al interior del proceso un plan de actualización documental que responda a los cambios y nuevos riesgos identificados.

#### RECOMENDACIONES

Con relación a los riesgos específicos del proceso PARTICIPACIÓN Y COMUNICACIÓN, se sugiere:

* Evaluar los riesgos asociados a la gestión de grandes volúmenes de datos. Con la creciente digitalización de los procesos de participación ciudadana, es necesario evaluar los riesgos asociados a la gestión de grandes volúmenes de datos, como la privacidad, la integridad y la disponibilidad de los datos.
* Considerar los riesgos asociados a la interacción con terceros. Evaluar los riesgos asociados a la interacción con terceros, como proveedores de servicios y socios estratégicos, en el marco de los procesos de participación ciudadana.

### COMUNICACIÓN ESTRATÉGICA

#### MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

**Riesgos de Seguridad de la Información**

1. No se ha construido el mapa de riesgos por ser un proceso nuevo.

#### OBSERVACIONES

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

Con la puesta en marcha de la nueva operación por procesos de la Secretaría Distrital de Planeación, se crea el proceso CES-CA-001 Comunicación Estratégica con el propósito de “Implementar la estrategia de comunicaciones de acuerdo con los objetivos institucionales para mantener informados a sus públicos de interés, posicionando a la entidad”.

Dado que el proceso es nuevo, es fundamental priorizar la elaboración de un mapa de riesgos detallado es esencial para un monitoreo efectivo a largo plazo. Este mapa debe identificar los riesgos potenciales, sus causas, consecuencias y los controles existentes.

El proceso debe enfocarse en la coherencia entre el riesgo identificado, el contexto estratégico y los objetivos del proceso. Aunque no exista un mapa de riesgos formal, se pueden análisis documentales para identificar los riesgos más relevantes.

Dada la ausencia del mapa de riesgos, se recomienda realizar una evaluación cualitativa de las causas y consecuencias identificadas inicialmente.

1. ***Autoevaluación de la efectividad de los controles****:*

Desde la segunda línea de defensa, se recomienda recopilar toda la evidencia disponible (registros, informes, etc.) para que una vez identificados los riesgos se pueda evaluar la efectividad de los controles. Se pueden utilizar técnicas como reuniones internas para obtener información adicional.

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

Se hace necesario que en la construcción del mapa de riesgos de seguridad se identifique si es necesario formular acciones complementarias a los controles que se implementen y asegurar que s estén alineadas con las causas identificadas y si se enfocan en lograr la mitigación de los riesgos. Se debe prestar especial atención a los hallazgos de auditoría interna y externa que se realizan en la vigencia.

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

La gestión de los riesgos implica evaluar de manera cualitativa si la gestión de los riesgos ha contribuido a prevenir situaciones no deseadas. Se sugiere utilizar indicadores clave de desempeño (KPIs) relacionados con la comunicación estratégica.

1. ***Actualización de Riesgos****:*

Se sugiere establecer un proceso regular de revisión y actualización de los riesgos, considerando los cambios en el contexto estratégico, los resultados de las auditorías y otros factores relevantes.

#### ALERTAS

**No se generan alertas.**

#### RECOMENDACIONES

Se recomienda, una vez se concluya la formulación de la nueva Plataforma Estratégica de la entidad, revisar el contexto estratégico, a fin de alineado con los riesgos identificados.

### INTELIGENCIA PARA LA PLANEACIÓN

#### MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN (antes Producción, Análisis y Divulgación de la Información)

**Riesgos 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 con 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.

#### OBSERVACIONES

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

La proactividad de la primera línea de defensa en abordar los cuatro riesgos identificados y en implementar los controles correspondientes. Desde la segunda línea de defesa se reconoce los esfuerzos realizados para alinear las operaciones con el nuevo diseño institucional, el cambio de nombre del proceso de “Producción, Análisis y Divulgación de la Información" a "Plan de Ordenamiento Territorial" y las funciones definidas en el nuevo manual de funciones de la entidad.

Se recomienda estar prepararos para evaluar el contexto una vez se tenga formalizada la nueva plataforma estratégica y verificar que en el nuevo contexto se incluya las áreas: Subsecretaría de Planeación de la Inversión, Dirección Distrital de Programación y Seguimiento a la Inversión y Plan de Desarrollo, Dirección de Programación y Seguimiento a la Inversión y Planes de Desarrollo Locales y la Dirección de Inversiones Estratégicas, como parte integral del proceso, con el objeto de realizar análisis completo de los riesgos que podría afectar el nuevo proceso derivado del rediseño institucional.

Es fundamental continuar trabajando de manera conjunta para asegurar que los riesgos estén adecuadamente gestionados y que el proceso se ejecute de manera eficiente y eficaz en el nuevo contexto organizacional.

Los cuatro riegos son coherentes con el objetivo estratégico "Fortalecer la generación, procesamiento y disponibilidad de la información estratégica de Bogotá Región, que favorezcan la toma de decisiones efectivas alrededor de la formulación, gestión, seguimiento y evaluación de las políticas públicas." por cuanto, la materialización de los riesgos relacionados con la confidencialidad, integridad y disponibilidad del SISBEN afectaría el cumplimiento de los objetivos estratégicos de la entidad.

Los cuatro riesgos identificados son coherentes con el objetivo del proceso "Capturar, recolectar, administrar, actualizar, analizar y producir información estratégica del Distrito Capital y la región, mediante la gestión de información gráfica y alfanumérica y de las herramientas de focalización del gasto, la base de datos geográfica y los estudios socioeconómicos, 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". Esta afirmación se soporta en el hecho que, la materialización de un riesgo sobre el activo de información SISBEN, impactaría los procesos y los procedimientos que soportan el objetivo general del proceso.

1. ***Autoevaluación de la efectividad de los controles****:*

El proceso definió nueve controles para mitigar los riesgos identificados en el sistema de información Sisbén. La respuesta proporcionada por la primera línea indica que se realizan mejoramientos al aplicativo periódicamente para resolver inconsistencias en el aplicativo desarrollado en Oracle. Las solicitudes se realizan a través de la mesa de ayuda de sistemas, también se mantiene copias de la información como respaldo, estas se realizan semanal y mensualmente. Se realiza la solicitud de usuarios a través de la mesa de ayuda de la dirección de sistemas remitiendo los A-FO-10 de los usuarios, a vuelta de sistema se remite el A-FO-212 de compromiso de uso. Para respaldar esta afirmación, dispuso las siguientes evidencias:

* A-FO-225 PRUEBAS DE SOLUCIONES DE SOFTWARE
* A-FO-212 ACTA DE COMPROMISO PARA EL USO DE RECURSOS Y/O SERVICIOS INFORMÁTICOS
* A-FO-010 SOLICITUD GESTION DE USAURIOS
* Relación de los BCK Información.

En el contexto general, desde el proceso se aplican los siguientes controles:

* **Solicitud formal de acceso:** Los usuarios deben solicitar formalmente el acceso al sistema a través de la mesa de ayuda, lo cual genera un registro de las solicitudes.
* **Compromiso de uso:** Los usuarios deben firmar un compromiso de uso de los recursos informáticos, lo que evidencia su conocimiento de las políticas de seguridad.
* **Mejoras periódicas al aplicativo**: Se realizan mejoras continuas al aplicativo para solucionar inconsistencias y mejorar su rendimiento.
* **Copias de seguridad:** Se generan copias de seguridad de la información de manera semanal y mensual, lo cual permite restaurar la información en caso de pérdida.

Si bien la evidencia presentada, sugiere que se están implementando controles, es necesario realizar un análisis más profundo para determinar si estos controles son suficientes y efectivos para mitigar los riesgos identificados. Se recomienda las siguientes mejoras en los controles:

Riesgo 1: Pérdida de Confidencialidad

Controles:

Verificación de mecanismos de identificación y autenticación.

Configuración de parámetros de seguridad.

* Mejoras:
* Implementar autenticación de dos factores.
* Solicitar auditorías regulares de los registros de acceso.
* Sensibilizar a los usuarios sobre las prácticas de seguridad.

Riesgo 2: Pérdida de Disponibilidad

Controles:

Pruebas de software antes de la implementación.

Copias de respaldo regulares.

* Mejoras:
* Revisar los acuerdos de nivel de servicio (SLA) con el proveedor de Oracle.
* Implementar sistemas de monitoreo continuo del rendimiento del sistema.
* Desarrollar un plan de recuperación ante desastres.

Riesgo 3: Pérdida de Integridad

Controles:

Coordinación con el DNP para cumplir con los parámetros técnicos.

Actualización regular del software.

* Mejoras:
* Implementar controles de acceso basados en roles.
* Realizar validaciones cruzadas de los datos.
* Revisar el proceso de aprobación para los cambios en el sistema.

Riesgo 4: Pérdida de Confidencialidad

Controles:

Establecimiento de controles de acceso y copia de información.

Configuración de mecanismos de identificación y autenticación.

* Mejoras:
* Encriptar la información sensible.
* Revisar que el firewall, el WAF y sistemas de detección de intrusiones de la SDP respalden el sistema.

Los 9 Controles definidos en el mapa de riesgos se describen a continuación:

**1. Restricción de acceso a usuarios:** Se establecen límites y restricciones para determinar quién puede acceder al sistema y qué acciones pueden realizar.

**2. Configuración de parámetros de seguridad:** Se configurarán los ajustes de seguridad del sistema y el servicio de Oracle para proteger la información.

**3. Lineamientos de prueba previa a la implementación**: Se define y siguen procedimientos de prueba rigurosos antes de poner en marcha nuevas funcionalidades del sistema.

**4. Validación de nuevas operaciones:** Se verifica que las nuevas operaciones del sistema no comprometan la seguridad de la información.

**5. Copias de respaldo:** Se establece políticas y procedimientos para realizar copias de seguridad de la información de forma regular.

**6. Cumplimiento de condiciones técnicas**: Se garantiza que el sistema cumpla con todos los requisitos técnicos y de seguridad establecidos por el proveedor del software.

**7. Verificación de la versión del software:** Se verifica periódicamente que la versión del software utilizado sea la más actualizada y segura.

**8. Establecimiento de controles de acceso y copia de información:** Se define los mecanismos para controlar el acceso, descarga y copia de la información, asegurando que solo el personal autorizado pueda realizar estas acciones.

**9. Configuración de mecanismos de identificación y autenticación:** Se establece mecanismos robustos para identificar y autenticar a los usuarios, evitando el acceso no autorizado.

En resumen, estos nueve controles se centran en:

* **Seguridad del acceso:** Restringir el acceso a personas no autorizadas y garantizar que solo el personal autorizado pueda acceder a la información.
* **Integridad de la información:** Proteger la información de alteraciones, destrucciones o pérdidas accidentales o intencionales.
* **Disponibilidad del sistema:** Asegurar que el sistema esté disponible y funcione correctamente en todo momento.
* **Cumplimiento normativo:** Garantizar el cumplimiento de las políticas de seguridad de la entidad y de las regulaciones aplicables.

El resultado del análisis de los riesgos frente a los riesgos es el siguiente:

Riesgo 1 y 4 (Pérdida de Confidencialidad): Los controles 1, 2, 8 y 9 están directamente relacionados con la protección de la confidencialidad de la información, al restringir el acceso, establecer mecanismos de seguridad y autenticación, y controlar la copia de datos.

Riesgo 2 (Pérdida de Disponibilidad): Los controles 2, 3, 4, 5, 6 y 7 están diseñados para garantizar la disponibilidad del sistema, a través de pruebas, configuraciones adecuadas, copias de respaldo y actualizaciones.

Riesgo 3 (Pérdida de Integridad): Los controles 2, 3, 4, 6 y 7 contribuyen a preservar la integridad de la información, al asegurar que los datos no sean alterados o destruidos.

En general, los nueve controles examinados parecen estar bien diseñados para prevenir o mitigar los cuatro riesgos identificados. Sin embargo, es importante considerar los siguientes puntos:

* Solapamiento de controles: Algunos controles contribuyen a mitigar varios riesgos, lo cual es positivo ya que refuerza la seguridad del sistema.
* Eficacia de los controles: La eficacia de los controles dependerá de su correcta implementación, mantenimiento y actualización.
* Riesgos residuales: Incluso con los controles en su lugar, puede existir un nivel de riesgo residual. Es importante evaluar este riesgo y determinar si es aceptable.
* Controles compensatorios: En algunos casos, puede ser necesario implementar controles compensatorios para mitigar los riesgos residuales.

La primera línea de defensa, es decir, los responsables directos de la operación y ejecución de los controles, ha respondido que en el periodo evaluado no se identificaron hallazgos de auditoría asociados al control en cuestión. Con base a la información proporcionada por la primera línea de defensa, se confirma que en el periodo evaluado no se han registrado hallazgos de auditoría directamente relacionados con los nueve controles. Sin embargo, es importante destacar que la ausencia de hallazgos no necesariamente implica que el control esté funcionando de manera óptima y efectiva en todos los aspectos.

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

En el primer monitoreo, la primera línea de defensa indicó que las acciones formuladas para tratar los riesgos estaban orientadas a contrarrestar sus causas. Sin embargo, nuestra revisión del mapa de riesgos ha revelado una inconsistencia: a pesar de que los riesgos 1 y 4 se clasificaron como moderados después de aplicar los controles iniciales, no se definieron planes de acción complementarios para ninguno de los cuatro riesgos identificados.

Esta discrepancia plantea interrogantes sobre la exhaustividad de la evaluación de riesgos y la efectividad de las medidas de mitigación implementadas. Recomendamos lo siguiente:

* Revisión detallada de los riesgos 1 y 4: Se debe realizar un análisis profundo de estos riesgos, incluyendo una reevaluación de sus causas raíz y la identificación de posibles acciones adicionales para reducirlos a un nivel aceptable.
* Para los riesgos 1 y 4, es imperativo formular planes de acción detallados que incluyan:

- Objetivos claros y medibles.

- Responsables definidos.

- Un cronograma de implementación.

- Indicadores de desempeño para medir la eficacia de las acciones.

* Integrar los planes de acción al sistema de gestión de riesgos existente para garantizar su seguimiento y actualización

La ausencia de planes de acción dificulta significativamente la evaluación de la implementación efectiva de las medidas de mitigación. Aunque se menciona el uso de una bitácora, no se encuentra registrada en el mapa de riesgos como una acción formalizada en el proceso.

En el primer monitoreo, la primera línea de defensa indicó que ninguno de los riesgos identificados se ha materializado ni ha sido objeto de un hallazgo de auditoría. Si bien esta información es relevante, la segunda línea de defensa considera necesario revisar el informe de seguimiento de los riesgos realizado por la Oficina de Control Interno en el cual se dan recomendaciones sobre la gestión de los riesgos a nivel general. En particular para este proceso, se recomienda analizar si la opción para el tratamiento final para los cuatro riesgos identificados es mitigar o deber ser reevaluada.

En el primer monitoreo, la primera línea de defensa indicó que la pregunta ¿Cómo producto de la materialización del riesgo, ¿Se han formulado las correcciones y/o acciones correctivas necesarias para darle tratamiento?, no aplica debido a la no materialización de los riesgos. Si bien es positivo que hasta el momento no se hayan materializado riesgos significativos, es fundamental que el proceso esté preparado para responder de manera efectiva en caso de que ocurran.

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

La primera línea de defensa ha indicado que la gestión de riesgos ha sido útil para evitar errores y garantizar la calidad de la información. Esta afirmación es alentadora y refleja los esfuerzos realizados para mitigar los riesgos identificados.

La gestión de los cuatro riesgos identificados ha demostrado ser fundamental para garantizar el cumplimiento del objetivo del proceso "Producción, Análisis y Divulgación de Información". Adicionalmente, los controles implementados han sido efectivos en mitigar las siguientes amenazas:

**Riesgo de pérdida de confidencialidad:** Los controles establecidos, como los mecanismos de identificación y autenticación robustos, han protegido la información sensible del proceso, evitando posibles filtraciones o accesos no autorizados. Esto ha sido crucial para mantener la confianza de los ciudadanos y las entidades involucradas.

**Riesgo de pérdida de disponibilidad:** Al implementar copias de respaldo y pruebas de software, se ha minimizado el riesgo de interrupciones en el servicio y pérdida de datos, garantizando así la continuidad de las operaciones y la disponibilidad de la información para la toma de decisiones.

**Riesgo de pérdida de integridad:** Los controles implementados para asegurar la configuración correcta de los sistemas y la realización de actualizaciones periódicas han protegido la integridad de la información, evitando alteraciones no autorizadas y garantizando la confiabilidad de los datos.

**Riesgo de pérdida de confidencialidad por copias fraudulentas:** Los controles de acceso y seguridad de la información han minimizado el riesgo de copias no autorizadas de la base de datos, protegiendo así la confidencialidad de la información y cumpliendo con los requisitos legales y normativos.

Al mitigar estos riesgos, el proceso ha logrado los siguientes beneficios:

**Mayor calidad de la información:** Los controles implementados han contribuido a mejorar la calidad de la información producida y divulgada, asegurando su precisión, integridad y confiabilidad.

Mayor eficiencia: La prevención de incidentes relacionados con la seguridad de la información ha permitido optimizar los recursos y mejorar la eficiencia del proceso.

**Cumplimiento normativo:** La gestión de riesgos ha garantizado el cumplimiento de las normas y regulaciones aplicables, evitando sanciones y multas.

**Protección de la reputación:** Al minimizar los riesgos de incidentes de seguridad, se ha protegido la reputación de la entidad y la confianza de los ciudadanos.

En conclusión, la gestión de riesgos ha demostrado ser una herramienta esencial para garantizar el cumplimiento de los objetivos del proceso y proteger los activos de información de la entidad.

1. ***Actualización de Riesgos****:*

La primera línea de defensa ha informado que no se han identificado cambios en los riesgos existentes. Sin embargo, considerando el contexto de rediseño institucional y la nueva caracterización del proceso, la segunda línea de defensa considera necesario realizar un análisis más detallado para garantizar que la evaluación de riesgos siga siendo precisa y completa.

Se recomienda lo siguiente:

* Realizar una revisión exhaustiva de la nueva caracterización del proceso para identificar cualquier cambio en los objetivos, actividades, o interacciones con otros procesos que puedan generar nuevos riesgos o modificar los existentes.
* Evaluar cómo los cambios estratégicos derivados del Decreto 432 de 2022 impactan en el perfil de riesgo del proceso. Es necesario identificar si estos cambios generan nuevas vulnerabilidades o si modifican la probabilidad o el impacto de los riesgos existentes.

La primera línea de defensa ha indicado que no se ha identificado la necesidad de documentar y gestionar nuevos riesgos. Sin embargo, al igual que en la pregunta 5.1, la segunda línea de defensa debe realizar una evaluación más profunda considerando los cambios en el contexto estratégico y el rediseño institucional.

#### ALERTAS

Dada la importancia de mantener actualizado el mapa de riesgos de seguridad de la información. En el segundo monitoreo, se ha identificado la necesidad de:

* Realizar la revisión del mapa de riesgos y actualizar teniendo en cuenta la nueva caracterización del proceso y los cambios en el contexto estratégico.
* Profundizar en el análisis de los riesgos 1 y 4.
* Desarrollar planes de acción detallados.
* Revisar la clasificación de los riesgos.
* Fortalecer la comunicación entre las líneas de defensa.

#### RECOMENDACIONES

* Realizar un análisis más detallado de los riesgos 1 y 4, especialmente considerando los cambios en el contexto institucional y la nueva plataforma estratégica.
* Establecer planes de acción detallados para cada riesgo cuyo tratamiento después de aplicar los controles sea mitigar, incluyendo objetivos claros, responsables, cronogramas y métricas de seguimiento.
* Evaluar si la clasificación de los riesgos como moderados sigue siendo adecuada después de implementar los controles y considerar si es necesario reclasificarlos.
* Implementar un proceso de monitoreo continuo para evaluar la eficacia de los controles y realizar ajustes si es necesario.
* Estar atentos a nuevos riesgos que puedan surgir como resultado de los cambios en el entorno o en el proceso.

### ARTICULACIÓN DEL DIÁLOGO CON LAS INSTITUCIONES

#### MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN (LABORATORIO DE CIUDAD)

**Riesgo de Seguridad de la Información**

1. Posible pérdida de integridad de la información contenida en los documentos relacionados con el reto de innovación abierta por la presencia de fallas humanas y/o errores en el uso o abuso de derechos y privilegios debido a deficiencia en la autorización de permisos de la información y/o insuficiente entrenamiento y capacitación sobre las políticas de seguridad y privacidad de la información.

#### OBSERVACIONES

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

Si bien el proceso ha identificado la necesidad de alinear su contexto estratégico con la plataforma estratégica 2024-2027, se recomienda que mientras se formaliza la nueva alineación estratégica se realice un análisis comparativo detallado entre el contexto estratégico actual del proceso y la caracterización definida con el fin de identificar nuevos riesgos o modificar los existentes, evaluar si los controles actuales siguen siendo adecuados para mitigar los riesgos identificados y asegurar que todos los involucrados en el proceso estén al tanto de los cambios en el contexto estratégico y de las implicaciones para sus actividades.

La respuesta de la primera línea, que indica que el proceso está a la espera de la plataforma estratégica 2024-2027 para alinear sus objetivos y riesgos, es un primer paso importante. Sin embargo, desde la perspectiva de la segunda línea de defensa, es necesario profundizar en este análisis. Si bien aún no se cuenta con la plataforma estratégica final, se recomienda realizar un análisis preliminar de la caracterización del proceso en relación con los riesgos identificados para determinar si, de manera general, están alineados con los objetivos estratégicos actuales del proceso. Esta acción garantiza que todos los riesgos estén alineados con los nuevos objetivos y que se hayan identificado los nuevos riesgos emergentes. Adicionalmente, con este ejercicio se preparará el camino para afrontar los cambios que se puedan suscitar una vez se tenga definida la plataforma estratégica de la entidad.

Desde la primera línea de defensa se informó que el riesgo de posible pérdida de integridad de la información se encuentra alineado con el objetivo "Desarrollar capacidades de innovación en la gestión pública de la Secretaría Distrital de Planeación, enmarcadas en el diálogo interinstitucional y articuladas con el sistema de innovación de la Administración Distrital." definido en la caracterización nueva del proceso.

La transformación del proceso a estratégico es un cambio fundamental que requiere una revisión exhaustiva de los riesgos asociados para garantizar que la gestión de riesgos sea efectiva y proporcional a la nueva importancia del proceso. Se recomienda evaluar la pertinencia de identificar nuevos riesgos como por ejemplo:

**Pérdida de integridad de la información:** El riesgo identificado específicamente en el documento, relacionado con la pérdida de integridad de la información debido a fallas humanas o errores en la gestión de permisos, es un ejemplo claro de este tipo de riesgo.

**Divulgación de información confidencial:** Dada la naturaleza del proceso, que involucra el intercambio de información con diversas partes interesadas, existe el riesgo de que información confidencial se divulgue a personas no autorizadas.

**Interrupción de la disponibilidad de la información:** Fallas en los sistemas o equipos utilizados para almacenar y procesar la información pueden causar interrupciones en la disponibilidad de la misma, afectando la continuidad del proceso.

**Pérdida de datos:** La pérdida accidental o intencional de datos puede tener un impacto significativo en el proceso, especialmente si se trata de información crítica para la toma de decisiones.

Riesgos adicionales a Considerar

Además de los riesgos mencionados, se pueden identificar otros riesgos potenciales:

**Ataques cibernéticos:** El proceso podría ser blanco de ataques cibernéticos como phishing, malware o ransomware, que podrían comprometer la seguridad de la información.

**Errores humanos:** Además de los errores mencionados en el documento, otros errores humanos como la pérdida de dispositivos o la configuración incorrecta de sistemas pueden representar un riesgo.

**Vulnerabilidades en las aplicaciones:** Las aplicaciones utilizadas en el proceso podrían contener vulnerabilidades que podrían ser explotadas por atacantes.

**Falta de actualización de software:** El uso de software obsoleto puede aumentar la exposición a vulnerabilidades conocidas.

**Riesgos asociados a la colaboración externa:** La colaboración con instituciones externas puede introducir nuevos riesgos, como la falta de control sobre los sistemas y procesos de estas organizaciones.

La afirmación de la primera línea de que el riesgo está recientemente determinado y que sus causas y consecuencias deben mantenerse por ser el primer monitoreo requiere una evaluación más profunda por parte de la segunda línea y para ello se recomienda evaluar si la nueva caracterización estratégica del proceso ha expuesto vulnerabilidades previamente desconocidas que puedan originar nuevas causas.

La afirmación de la primera línea de que el riesgo está recientemente determinado y que sus causas y consecuencias deben mantenerse por ser el primer monitoreo requiere una evaluación más profunda por parte de la segunda línea y para ello se recomienda evaluar si la nueva caracterización estratégica del proceso ha expuesto vulnerabilidades previamente desconocidas que puedan originar nuevas consecuencias.

1. ***Autoevaluación de la efectividad de los controles****:*

Desde el proceso se contestó que a la fecha se está iniciando los retos de innovación abierta, por lo tanto, no se ha avanzado en la generación de la ficha y los términos de referencia mencionados en el control. Esta afirmación sugiere que los controles definidos en el proceso "revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad y educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la entidad pertinentes para su cargo.", no han sido determinados los instrumentos que evidencien el uso del control. Desde la segunda línea de defensa se recomienda priorizar acciones para definir los registros necesarios para evidenciar la gestión del riesgo identificado.

Desde el proceso se contestó que a la fecha se está dando inicio a los retos de innovación abierta, por lo tanto, no se ha avanzado en la generación de la ficha y los términos de referencia mencionados en el control. Se recomienda realizar una descripción más detallada sobre cómo los dos controles previenen o mitigan el riesgo de Posible pérdida de integridad de la información contenida en los documentos relacionados con el reto de innovación abierta por la presencia de fallas humanas y/o errores en el uso o abuso de derechos y privilegios debido a deficiencia en la autorización de permisos de la información y/o insuficiente entrenamiento y capacitación sobre las políticas de seguridad y privacidad de la información y revisar la suficiencia de los mismos.

De acuerdo con la primera línea de defensa, con corte a agosto, no ha sido objeto de evaluación por parte de una auditoría, al igual que su mapa de riesgos debido a que el proceso es nuevo.

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

El proceso definió dos acciones; "Realizar socialización de la información sobre políticas y normas de seguridad de la información" y "Asegurar que el equipo conozca sobre la importancia de la seguridad de la información que se maneja en la Oficina". Se recomienda para el siguiente seguimiento atender las siguientes notas:

Las acciones propuestas por el proceso para mitigar el riesgo de pérdida de integridad de la información debido a fallas humanas son fundamentales y están directamente alineadas con las mejores prácticas en seguridad de la información, a continuación, se describe por cada control la relación con las normas de seguridad.

**1. Realizar socialización de la información sobre políticas y normas de seguridad de la información:**

*Concientización*: Esta acción busca crear conciencia en el equipo sobre la importancia de la seguridad de la información y los riesgos asociados a su mal manejo.

*Claridad en las Expectativas:* Al socializar las políticas y normas, se establecen claramente las expectativas de comportamiento en cuanto a la seguridad de la información, reduciendo la probabilidad de errores por desconocimiento.

*Empoderamiento:* La socialización permite que los empleados se sientan parte de la solución, fomentando una cultura de seguridad en la organización.

*Prevención de Errores:* Al conocer las políticas y normas, los empleados pueden identificar y evitar acciones que puedan comprometer la seguridad de la información, como compartir contraseñas o abrir archivos adjuntos sospechosos.

**2. Asegurar que el equipo conozca sobre la importancia de la seguridad de la información que se maneja en la Oficina:**

*Valoración de la Información:* Al enfatizar la importancia de la información, se fomenta un mayor cuidado en su manejo y protección.

*Proactividad:* Los empleados serán más proactivos en la identificación de posibles amenazas y en la adopción de medidas preventivas.

*Compromiso:* Al entender la importancia de la seguridad de la información para la entidad, las personas involucradas en el proceso se sentirán más comprometidos con su protección.

De otra parte, se analizó cómo estas acciones contrarrestan específicamente el riesgo identificando las siguientes razones:

* **Reducción de Errores Humanos**: Al conocer las políticas y normas, los empleados serán menos propensos a cometer errores que puedan comprometer la seguridad de la información, como compartir contraseñas o abrir archivos adjuntos sospechosos.
* **Incremento de la Conciencia:** La concientización sobre la seguridad de la información fomenta una cultura de seguridad en la organización, lo que lleva a una mayor vigilancia y detección de posibles amenazas.
* **Mayor Cumplimiento de las Políticas:** Al conocer las políticas y normas, los empleados serán más propensos a cumplirlas, reduciendo el riesgo de incumplimiento."

Revisada la respuesta de primera línea "Hasta ahora se van a iniciar las actividades que requieren la implementación del control definido para contrarrestar o mitigar la causa identificada para el riesgo", se infiere que aunque no se ha iniciado la aplicación de las dos acciones formuladas, están implementadas adecuadamente para dar tratamiento a los riesgos.

Se observa que los riesgos después de aplicar los controles se sitúan en una zona baja que no requiere formular acciones. Se resalta que desde el proceso se haya formulado acciones complementarias para asegurar la eficiente gestión del riesgo.

Adicionalmente se recomienda revisar el tratamiento definido para el riesgo dado que al estar en una zona baja una opción válida es aceptar el riesgo.

De acuerdo con la respuesta de primera línea de defensa, con corte a agosto los riesgos identificados, los controles y las acciones no han objeto de auditorías. Sin embargo, es indispensable que de manera proactiva se realice revisiones periódicas para garantizar que los riesgos no se materialicen.

El proceso contestó: "No ha habido auditorías internas o externas al proceso que generen hallazgos aunado que hasta ahora se está iniciando la actividad que implica el riesgo". Ante la ausencia de Auditorias o hallazgos descubiertos desde el proceso no se ha formulado correcciones o acciones correctivas para dar tratamiento a la materialización del riesgo.

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

Evaluar el impacto real de las acciones implementadas para gestionar el riesgo identificado como, por ejemplo: para el primer control “Realizar socialización de la información sobre políticas y normas de seguridad de la información: la disminución en el impacto de incidentes relacionados con el riesgo identificado y evitado pérdidas financieras, de reputación o de datos. Y para el segundo control “Asegurar que el equipo conozca sobre la importancia de la seguridad de la información que se maneja en la Oficina” se enfatiza la importancia de la información, se fomenta un mayor cuidado en su manejo y protección logrando que los funcionarios sean más proactivos en la identificación de posibles amenazas y en la adopción de medidas preventivas y el comprometidos con su protección.

Cómo estas acciones se han alcanzado los siguientes logros:

* **Reducción de Errores Humanos:** Al conocer las políticas y normas, los empleados serán menos propensos a cometer errores que puedan comprometer la seguridad de la información, como compartir contraseñas o abrir archivos adjuntos sospechosos.
* **Incremento de la Conciencia:** La concientización sobre la seguridad de la información fomenta una cultura de seguridad en la organización, lo que lleva a una mayor vigilancia y detección de posibles amenazas.
* **Mayor Cumplimiento de las Políticas:** Al conocer las políticas y normas, los empleados serán más propensos a cumplirlas, reduciendo el riesgo de incumplimiento.

En conclusión, la gestión del riesgo en el proceso ha contribuido en la prevención de la materialización de los riesgos y el cumplimiento del objetivo estratégico, los compromisos y las metas ligadas al mismo permitiendo la continuidad del proceso y la entrega de los productos definidos en la caracterización del proceso.

1. ***Actualización de Riesgos****:*

De acuerdo con la respuesta dada desde el proceso, dado que el riesgo fue identificado y documentado recientemente, se va a iniciar la ejecución de las actividades de control y plan de tratamiento del riesgo, no se evidencia la necesidad de actualizar, modificar o identificar nuevos riesgos para el proceso, sin embargo, considerando el proceso de ajuste en la plataforma estratégica es fundamental que una vez que esté aprobada la nueva visión y contexto estratégico realizar la revisión para asegurar que el riesgo siga siendo adecuado para tratarlo y que no se identifican nuevos riesgos.

De acuerdo con la respuesta dada desde el proceso, y dado que no se evidencia la necesidad de actualizar, modificar o identificar nuevos riesgos para el proceso, no se observa la necesidad de documentar y gestionar nuevos riesgos.

#### ALERTAS

Verificar que el contexto este alineado a la nueva estructura organizacional y que el riego siga siendo relevante.

#### RECOMENDACIONES

* Para mejorar la gestión del riesgo, se recomienda fomentar una cultura de seguridad dentro del proceso para prevenir incidentes de seguridad incluyendo capacitación del personal, revisión de políticas y procedimientos, y evaluación continua.
* Es fundamental implementar medidas para hacer seguimiento y monitorear la efectividad en la gestión del riesgo.
* Realizar un análisis profundo para identificar si con los cambios institucionales derivados del rediseño se han introducido nuevas vulnerabilidades que puedan ser explotadas y que afecten a la entidad.

### ARTICULACIÓN DEL DIÁLOGO SUPRADISTRITAL

#### MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN (COORDINACIÓN DE LAS POLÍTICAS PÚBLICAS Y DE LOS INSTRUMENTOS DE PLANEACIÓN)

**Riesgos 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

2. 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.

#### OBSERVACIONES

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

Ante la inminente transformación del proceso de COORDINACIÓN DE LAS POLÍTICAS PÚBLICAS Y DE LOS INSTRUMENTOS DE PLANEACIÓN, el cual se dividirá en los procesos de PLAN DISTRITAL DE DESARROLLO, POLÍTICAS PÚBLICAS Y ARTICULACIÓN DEL DIÁLOGO SUPRADISTRITAL, es imprescindible realizar una evaluación de riesgos actualizada. El objetivo es identificar y mitigar cualquier nueva vulnerabilidad que pueda surgir como consecuencia de estos cambios, asegurando así la protección de la información sensible de la entidad.

Los dos riesgos identificados son coherentes con el objetivo estratégico, "Fortalecer la formulación, seguimiento y evaluación de planes, programas, políticas y proyectos en la ciudad en materia económica, social y ambiental de forma coordinada y articulada con los actores de Bogotá Región" y es aceptable hasta tanto se complete y formalice la actualización de la plataforma estratégica de la SDP. Sin embargo, es necesario programar una revisión del riesgo para verificar su persistencia y pertinencia en el nuevo contexto a la luz de luz de la nueva caracterización del proceso formulada recientemente.

Los riesgos identificados son pertinentes para el proceso actual y están alineados al 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". Anticipando el cambio de proceso, desde el proceso se ha determinado que los riesgos de seguridad de la información deberán ser reevaluados y ajustados para reflejar el nuevo contexto.

Ante el cambio de proceso, es necesario revisar y actualizar las causas de los riesgos identificados. En particular, se debe prestar atención a las deficiencias en capacitación, el manejo manual de datos y la falta de copias de seguridad. Estas áreas deben adaptarse a las nuevas políticas y al contexto estratégico del rediseño institucional.

El perfil de riesgo actual permanecerá vigente hasta la finalización de la transición hacia el nuevo modelo organizacional, por lo tanto, las consecuencias identificadas inicialmente se mantienen. Una vez implementados los cambios, se realizará un análisis exhaustivo para identificar y evaluar los nuevos riesgos que se formulen en el contexto del proceso nuevo Políticas Públicas.

1. ***Autoevaluación de la efectividad de los controles****:*

El proceso Coordinación de Políticas Públicas (DEPPD) es de reciente creación razón por la cual se están implementando nuevos procedimientos y ajustando los existentes.

Los controles aplicados están orientados a cumplir con la política A-LE 429 de seguridad y privacidad de la información, dentro de estos podemos identificar los siguientes:

* **Revisión y validación de contenidos**: Los directivos revisan y validan todos los documentos antes de su emisión final.
* **Uso del SIPA:** Se utiliza el Sistema de Información para la Gestión de Proyectos (SIPA) para emitir respuestas a solicitudes, realizar solicitudes en el marco del diseño de políticas y gestionar la agenda de evaluaciones.
* **Cumplimiento de la política A-LE 429:** Se aplican los lineamientos de seguridad y privacidad de la información establecidos en esta política.
* **Desarrollo de procedimientos:** Se están desarrollando nuevos procedimientos, como el de Evaluación de Políticas Públicas, y se siguen los existentes, como el M-PD-213 Agenda de Evaluaciones.
* **Capacitación:** Se ha impartido capacitación en seguridad de la información a los colaboradores por parte de la Dirección de Tecnologías de la información y las comunicaciones.
* **Documentación de procesos:** Se están documentando los procesos y se establecen directrices para la conservación de registros.

Se proporcionan enlaces a documentos, registros que respaldan las afirmaciones anteriores y así mismo, se menciona y aporta correos electrónicos, radicados y documentos del SIPA como evidencia del cumplimiento de los controles.

En conclusión, el proceso de Coordinación de Políticas Públicas está aplicando los controles de manera consistente evidenciando un compromiso con la mejora continua de los procesos.

En el análisis de Riesgos y Controles Propuestos para el Riesgo 1 relacionado con la Pérdida de Integridad por Fallas Humanas y definido como la posibilidad de que la información sea modificada de manera no autorizada o accidental debido a errores humanos o falta de conocimiento sobre políticas de seguridad, el proceso estableció dos controles los cuales fueron revisados concluyendo que:

Riesgo 1: Pérdida de Integridad por fallas humanas debido a insuficiente capacitación

**Control:** Los directivos del proceso revisan y validan los contenidos de los conceptos antes de su emisión final.

**Prevención:** Esta revisión final actúa como una barrera adicional para detectar y corregir errores humanos que puedan comprometer la integridad de la información. Al validar los contenidos, se asegura que la información sea precisa y consistente.

**Mitigación:** Detecta y corrige errores humanos antes de la emisión final.

**Control:** El Líder del proceso vela porque todos sus procedimientos se conozcan y se cumplan aplicando los lineamientos establecidos en la política A-LE 429.

**Prevención:** Al garantizar que los colaboradores conozcan y apliquen los procedimientos establecidos, se reduce la probabilidad de errores humanos causados por desconocimiento. La política A-LE 429 proporciona una guía clara sobre las prácticas de seguridad a seguir, lo que minimiza el riesgo de violaciones a la integridad de la información.

**Mitigación:** Proporciona una guía clara sobre prácticas seguras, reduciendo errores.

Riesgo 2: Pérdida de Disponibilidad por fallas humanas debido a manejo manual de la información y ausencia de copias de respaldo

**Control:** Los colaboradores del proceso conocen y aplican los lineamientos establecidos en la política A LE 429.

**Prevención:** La política A-LE 429 probablemente incluye lineamientos sobre la gestión de copias de seguridad y la importancia de mantener la información disponible. Al conocer estos lineamientos, los colaboradores son más conscientes de la necesidad de realizar copias de respaldo y de seguir los procedimientos adecuados para garantizar la disponibilidad de la información.

**Mitigación:** Incluye lineamientos sobre gestión de copias de seguridad.

**Control:** Los colaboradores del proceso conocen y aplican los procedimientos documentados, así como las directrices de conservación de los registros.

**Prevención:** Los procedimientos documentados deben incluir instrucciones claras sobre cómo manejar la información, incluyendo la creación y almacenamiento de copias de respaldo. Al seguir estos procedimientos, se reduce el riesgo de pérdida de datos debido a errores humanos o eventos imprevistos.

**Mitigación:** Proporciona instrucciones claras sobre el manejo de la información y la creación de copias de respaldo.

Los controles propuestos para ambos riesgos están diseñados para abordar las causas subyacentes lo cual reduce significativamente la probabilidad de que ocurran pérdidas de integridad o disponibilidad de la información.

De otra parte, desde el proceso se indicó que no se han identificado hallazgos de auditoría asociados a los controles durante el período evaluado.

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

El Criterio de Monitoreo 3 busca evaluar si las acciones implementadas para gestionar un riesgo están directamente enfocadas en abordar sus causas raíz. En otras palabras, se pregunta si las acciones adicionales a los controles están diseñadas para prevenir o mitigar la ocurrencia del riesgo en el futuro. En la evaluación de la situación actual y con la información proporcionada se concluye que no se han definido planes de acción lo que significa que no se han establecido medidas específicas para complementar los controles para abordar los riesgos identificados, esto en razón a que los dos riesgos identificados en el proceso, después de aplicados los controles tiene una valoración baja.

No se han formulado planes de acción como complemento a los controles para dar tratamiento al riesgo, como consecuencia, no existen acciones concretas orientadas a contrarrestar las causas de los riesgos. De igual forma, la Primera Línea de Defensa ha determinado que, según la información disponible, los riesgos identificados no han alcanzado su estado de materialización. En consecuencia, no se han ejecutado acciones correctivas específicas.

Se recomienda realizar evaluaciones de riesgos de manera más exhaustiva, considerando no solo los riesgos identificados inicialmente, sino también aquellos emergentes o que puedan surgir a partir de cambios en el entorno o en el proceso. Así mismo, se sugiere Incorporar a más actores, esto es involucrar a un mayor número de colaboradores en el proceso de identificación de riesgos, ya que ellos pueden tener una visión más detallada de las actividades y los posibles peligros.

Es de recordar que, lograr una gestión de riesgos proactiva y efectiva, permitirá minimizar los impactos negativos de los eventos adversos asegurando la continuidad de las operaciones. La gestión de riesgos es un proceso continuo que requiere un compromiso a largo plazo por parte de toda la entidad.

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

La gestión del Riesgo 1: Pérdida de integridad de la información ha sido útil para que a través de los controles aplicados y su seguimiento se disminuya el número de errores en los documentos generando mayor confianza en la información producida. En cuanto al riesgo 2: Pérdida de disponibilidad de la información, se puede decir que ha contribuido en la generación de una cultura institucional permitiendo el conocimiento y aplicación de los lineamientos establecidos en la política A LE 429 Políticas de seguridad y privacidad de la información y en las directrices de conservación de los registros del proceso lo que ha permitido estar preparados para solventar situaciones adversas que puedan ocasionar la materialización de un riesgo. En general, la gestión del mapa de riesgos ha sido útil para disminuir la probabilidad y el impacto en el caso que se materializara alguno de los riesgos propendiendo por la continuidad de las operaciones del proceso y el complimiento de los objetivos estratégicos.

1. ***Actualización de Riesgos****:*

La Primera Línea de Defensa se identificó la necesidad de realizar una actualización completa de riesgos del proceso, 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, la evaluación de la probabilidad e impacto de todos los riesgos y la documentación detallada del nuevo mapa de riesgos de seguridad de la información.

#### ALERTAS

Con ocasión del rediseño institucional se modificó la estructura organizacional de la entidad dando origen a nuevos procesos y eliminando algunos. En esta misma línea, se publicó el nuevo manual de funciones y se realizó la caracterización de todos los procesos de la entidad. Es relevante estar atentos a los cambios institucionales que puedan afectar el mapa de riesgos de seguridad de la información y mantener una postura proactiva para mantenerlo actualizado.

#### RECOMENDACIONES

Desde la segunda línea de defensa, se recomienda:

* Asegurar que los controles internos estén diseñados de manera adecuada para mitigar los riesgos identificados y que estén debidamente documentados.
* Verificar que los controles sean implementados de forma consistente y que el personal esté capacitado para su ejecución.
* Realizar evaluaciones periódicas de la eficacia de los controles para identificar brechas y áreas de mejora.
* Asegurar que el personal adscrito al proceso participe en la capacitación continua sobre conceptos de gestión de riesgos, herramientas y técnicas.
* Establecer canales de comunicación claros y abiertos para facilitar el intercambio de información sobre riesgos y controles.
* Realizar reuniones periódicas para realizar el seguimiento sobre el cumplimiento de los controles establecidos y alinear esfuerzos.
* Estar preparados para adoptar el nuevo sistema GESTIONATE para para facilitar la identificación, evaluación y seguimiento de los riesgos, mejorando la eficiencia administrativa reduciendo al mismo tiempo la probabilidad de la ocurrencia de materialización y el impacto en el caso de la materialización de alguno de los riesgos presentes en el proceso.

## PROCESOS MISIONALES

### PLAN DISTRITAL DE DESARROLLO

#### MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN (COORDINACIÓN DE LAS POLÍTICAS PÚBLICAS Y DE LOS INSTRUMENTOS DE PLANEACIÓN)

**Riesgos 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

2. 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.

#### OBSERVACIONES

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

Ante la inminente transformación del proceso de COORDINACIÓN DE LAS POLÍTICAS PÚBLICAS Y DE LOS INSTRUMENTOS DE PLANEACIÓN, el cual se dividirá en los procesos de PLAN DISTRITAL DE DESARROLLO, POLÍTICAS PÚBLICAS Y ARTICULACIÓN DEL DIÁLOGO SUPRADISTRITAL, es imprescindible realizar una evaluación de riesgos actualizada. El objetivo es identificar y mitigar cualquier nueva vulnerabilidad que pueda surgir como consecuencia de estos cambios, asegurando así la protección de la información sensible de la entidad.

Los dos riesgos identificados son coherentes con el objetivo estratégico, "Fortalecer la formulación, seguimiento y evaluación de planes, programas, políticas y proyectos en la ciudad en materia económica, social y ambiental de forma coordinada y articulada con los actores de Bogotá Región" y es aceptable hasta tanto se complete y formalice la actualización de la plataforma estratégica de la SDP. Sin embargo, es necesario programar una revisión del riesgo para verificar su persistencia y pertinencia en el nuevo contexto a la luz de luz de la nueva caracterización del proceso formulada recientemente.

Los riesgos identificados son pertinentes para el proceso actual y están alineados al 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". Anticipando el cambio de proceso, desde el proceso se ha determinado que los riesgos de seguridad de la información deberán ser reevaluados y ajustados para reflejar el nuevo contexto.

Ante el cambio de proceso, es necesario revisar y actualizar las causas de los riesgos identificados. En particular, se debe prestar atención a las deficiencias en capacitación, el manejo manual de datos y la falta de copias de seguridad. Estas áreas deben adaptarse a las nuevas políticas y al contexto estratégico del rediseño institucional.

El perfil de riesgo actual permanecerá vigente hasta la finalización de la transición hacia el nuevo modelo organizacional, por lo tanto, las consecuencias identificadas inicialmente se mantienen. Una vez implementados los cambios, se realizará un análisis exhaustivo para identificar y evaluar los nuevos riesgos que se formulen en el contexto del proceso nuevo Políticas Públicas.

1. ***Autoevaluación de la efectividad de los controles****:*

El proceso Coordinación de Políticas Públicas (DEPPD) es de reciente creación razón por la cual se están implementando nuevos procedimientos y ajustando los existentes.

Los controles aplicados están orientados a cumplir con la política A-LE 429 de seguridad y privacidad de la información, dentro de estos podemos identificar los siguientes:

* **Revisión y validación de contenidos**: Los directivos revisan y validan todos los documentos antes de su emisión final.
* **Uso del SIPA:** Se utiliza el Sistema de Información para la Gestión de Proyectos (SIPA) para emitir respuestas a solicitudes, realizar solicitudes en el marco del diseño de políticas y gestionar la agenda de evaluaciones.
* **Cumplimiento de la política A-LE 429:** Se aplican los lineamientos de seguridad y privacidad de la información establecidos en esta política.
* **Desarrollo de procedimientos:** Se están desarrollando nuevos procedimientos, como el de Evaluación de Políticas Públicas, y se siguen los existentes, como el M-PD-213 Agenda de Evaluaciones.
* **Capacitación:** Se ha impartido capacitación en seguridad de la información a los colaboradores por parte de la Dirección de Tecnologías de la información y las comunicaciones.
* **Documentación de procesos:** Se están documentando los procesos y se establecen directrices para la conservación de registros.

Se proporcionan enlaces a documentos, registros que respaldan las afirmaciones anteriores y así mismo, se menciona y aporta correos electrónicos, radicados y documentos del SIPA como evidencia del cumplimiento de los controles.

En conclusión, el proceso de Coordinación de Políticas Públicas está aplicando los controles de manera consistente evidenciando un compromiso con la mejora continua de los procesos.

En el análisis de Riesgos y Controles Propuestos para el Riesgo 1 relacionado con la Pérdida de Integridad por Fallas Humanas y definido como la posibilidad de que la información sea modificada de manera no autorizada o accidental debido a errores humanos o falta de conocimiento sobre políticas de seguridad, el proceso estableció dos controles los cuales fueron revisados concluyendo que:

Riesgo 1: Pérdida de Integridad por fallas humanas debido a insuficiente capacitación

**Control:** Los directivos del proceso revisan y validan los contenidos de los conceptos antes de su emisión final.

**Prevención:** Esta revisión final actúa como una barrera adicional para detectar y corregir errores humanos que puedan comprometer la integridad de la información. Al validar los contenidos, se asegura que la información sea precisa y consistente.

**Mitigación:** Detecta y corrige errores humanos antes de la emisión final.

**Control:** El Líder del proceso vela porque todos sus procedimientos se conozcan y se cumplan aplicando los lineamientos establecidos en la política A-LE 429.

**Prevención:** Al garantizar que los colaboradores conozcan y apliquen los procedimientos establecidos, se reduce la probabilidad de errores humanos causados por desconocimiento. La política A-LE 429 proporciona una guía clara sobre las prácticas de seguridad a seguir, lo que minimiza el riesgo de violaciones a la integridad de la información.

**Mitigación:** Proporciona una guía clara sobre prácticas seguras, reduciendo errores.

Riesgo 2: Pérdida de Disponibilidad por fallas humanas debido a manejo manual de la información y ausencia de copias de respaldo

**Control:** Los colaboradores del proceso conocen y aplican los lineamientos establecidos en la política A LE 429.

**Prevención:** La política A-LE 429 probablemente incluye lineamientos sobre la gestión de copias de seguridad y la importancia de mantener la información disponible. Al conocer estos lineamientos, los colaboradores son más conscientes de la necesidad de realizar copias de respaldo y de seguir los procedimientos adecuados para garantizar la disponibilidad de la información.

**Mitigación:** Incluye lineamientos sobre gestión de copias de seguridad.

**Control:** Los colaboradores del proceso conocen y aplican los procedimientos documentados, así como las directrices de conservación de los registros.

**Prevención:** Los procedimientos documentados deben incluir instrucciones claras sobre cómo manejar la información, incluyendo la creación y almacenamiento de copias de respaldo. Al seguir estos procedimientos, se reduce el riesgo de pérdida de datos debido a errores humanos o eventos imprevistos.

**Mitigación:** Proporciona instrucciones claras sobre el manejo de la información y la creación de copias de respaldo.

Los controles propuestos para ambos riesgos están diseñados para abordar las causas subyacentes lo cual reduce significativamente la probabilidad de que ocurran pérdidas de integridad o disponibilidad de la información.

De otra parte, desde el proceso se indicó que no se han identificado hallazgos de auditoría asociados a los controles durante el período evaluado.

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

El Criterio de Monitoreo 3 busca evaluar si las acciones implementadas para gestionar un riesgo están directamente enfocadas en abordar sus causas raíz. En otras palabras, se pregunta si las acciones adicionales a los controles están diseñadas para prevenir o mitigar la ocurrencia del riesgo en el futuro. En la evaluación de la situación actual y con la información proporcionada se concluye que no se han definido planes de acción lo que significa que no se han establecido medidas específicas para complementar los controles para abordar los riesgos identificados, esto en razón a que los dos riesgos identificados en el proceso, después de aplicados los controles tiene una valoración baja.

No se han formulado planes de acción como complemento a los controles para dar tratamiento al riesgo, como consecuencia, no existen acciones concretas orientadas a contrarrestar las causas de los riesgos. De igual forma, la Primera Línea de Defensa ha determinado que, según la información disponible, los riesgos identificados no han alcanzado su estado de materialización. En consecuencia, no se han ejecutado acciones correctivas específicas.

Se recomienda realizar evaluaciones de riesgos de manera más exhaustiva, considerando no solo los riesgos identificados inicialmente, sino también aquellos emergentes o que puedan surgir a partir de cambios en el entorno o en el proceso. Así mismo, se sugiere Incorporar a más actores, esto es involucrar a un mayor número de colaboradores en el proceso de identificación de riesgos, ya que ellos pueden tener una visión más detallada de las actividades y los posibles peligros.

Es de recordar que, lograr una gestión de riesgos proactiva y efectiva, permitirá minimizar los impactos negativos de los eventos adversos asegurando la continuidad de las operaciones. La gestión de riesgos es un proceso continuo que requiere un compromiso a largo plazo por parte de toda la entidad.

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

La gestión del Riesgo 1: Pérdida de integridad de la información ha sido útil para que a través de los controles aplicados y su seguimiento se disminuya el número de errores en los documentos generando mayor confianza en la información producida. En cuanto al riesgo 2: Pérdida de disponibilidad de la información, se puede decir que ha contribuido en la generación de una cultura institucional permitiendo el conocimiento y aplicación de los lineamientos establecidos en la política A LE 429 Políticas de seguridad y privacidad de la información y en las directrices de conservación de los registros del proceso lo que ha permitido estar preparados para solventar situaciones adversas que puedan ocasionar la materialización de un riesgo. En general, la gestión del mapa de riesgos ha sido útil para disminuir la probabilidad y el impacto en el caso que se materializara alguno de los riesgos propendiendo por la continuidad de las operaciones del proceso y el complimiento de los objetivos estratégicos.

1. ***Actualización de Riesgos****:*

La Primera Línea de Defensa se identificó la necesidad de realizar una actualización completa de riesgos del proceso, 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, la evaluación de la probabilidad e impacto de todos los riesgos y la documentación detallada del nuevo mapa de riesgos de seguridad de la información.

#### ALERTAS

Con ocasión del rediseño institucional se modificó la estructura organizacional de la entidad dando origen a nuevos procesos y eliminando algunos. En esta misma línea, se publicó el nuevo manual de funciones y se realizó la caracterización de todos los procesos de la entidad. Es relevante estar atentos a los cambios institucionales que puedan afectar el mapa de riesgos de seguridad de la información y mantener una postura proactiva para mantenerlo actualizado.

#### RECOMENDACIONES

Desde la segunda línea de defensa, se recomienda:

* Asegurar que los controles internos estén diseñados de manera adecuada para mitigar los riesgos identificados y que estén debidamente documentados.
* Verificar que los controles sean implementados de forma consistente y que el personal esté capacitado para su ejecución.
* Realizar evaluaciones periódicas de la eficacia de los controles para identificar brechas y áreas de mejora.
* Asegurar que el personal adscrito al proceso participe en la capacitación continua sobre conceptos de gestión de riesgos, herramientas y técnicas.
* Establecer canales de comunicación claros y abiertos para facilitar el intercambio de información sobre riesgos y controles.
* Realizar reuniones periódicas para realizar el seguimiento sobre el cumplimiento de los controles establecidos y alinear esfuerzos.
* Estar preparados para adoptar el nuevo sistema GESTIONATE para para facilitar la identificación, evaluación y seguimiento de los riesgos, mejorando la eficiencia administrativa reduciendo al mismo tiempo la probabilidad de la ocurrencia de materialización y el impacto en el caso de la materialización de alguno de los riesgos presentes en el proceso.

### PLAN ORDENAMIENTO TERRITORIAL

#### MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN (PLANEACIÓN TERRITORIAL Y PLANEACIÓN DE SUS INSTRUMENTOS)

**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 Backup de la información.

#### OBSERVACIONES

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

Con base a la evaluación realizada desde la primera línea de defensa, se concluye que, es fundamental realizar una actualización del contexto y el análisis de riesgos, considerando los cambios identificados en el contexto estratégico institucional, la reciente formalización de la nueva caracterización del proceso. Es importante señalar que se debe mantener un enfoque proactivo en la gestión de riesgos y realizar evaluaciones periódicas para garantizar la protección de la información de la organización.

Adicionalmente, se recomienda que para determinar si el contexto estratégico se mantiene, se realice un análisis exhaustivo y continuo. Al verificar los factores externos e internos, que no se han experimentado cambios significativos y que los objetivos estratégicos siguen siendo relevantes, es posible concluir que el contexto estratégico se mantiene. Si algunos factores externos o internos han cambiado, pero los objetivos estratégicos fundamentales se mantienen, es necesario ajustar el proceso para adaptarse a las nuevas circunstancias. y si los factores externos e internos han cambiado de manera drástica o los objetivos estratégicos ya no son relevantes, es necesario realizar una revisión completa del proceso y posiblemente redefinir su alcance y objetivos. Al realizar este tipo de análisis y evaluar los posibles escenarios, el líder del proceso puede tomar decisiones informadas y garantizar que sus procesos internos sigan siendo relevantes y efectivos a largo plazo.

El riesgo identificado, pérdida de disponibilidad de información, presenta una amenaza directa al objetivo estratégico de la entidad. Este riesgo representa una amenaza directa a la capacidad de la Secretaría Distrital de Planeación (SDP) para cumplir con su objetivo de "Definir y promover un modelo colectivo de ciudad en el largo plazo". La pérdida de información crítica, como decretos, resoluciones y cartografía, podría dificultar la toma de decisiones dado que al no contar con información actualizada y confiable, dificultaría la evaluación de alternativas y la toma de decisiones informadas en materia de planeación territorial, retrasaría los procesos debido a que la reconstrucción de información perdida puede ser un proceso largo y costoso, lo que genera retrasos en la implementación de proyectos y en la prestación de servicios a la ciudadanía, erosionaría la confianza depositada por los usuarios teniendo en cuenta que la pérdida de información puede generar desconfianza en la capacidad de la SDP para gestionar de manera adecuada los datos y cumplir con sus compromisos. Así mismo, puede afectar la reputación institucional considerando que la pérdida de información sensible puede tener un impacto negativo en la reputación de la SDP y en la percepción de transparencia y eficiencia.

Entre otros aspectos de igual relevancia y que deben ser revisados desde el proceso pueden ser los siguientes:

* Considerando que la información recopilada y procesada en este proceso constituye la base de conocimiento para la toma de decisiones en materia de planificación territorial, es necesario analizar que la pérdida de esta información dificulta la continuidad de los proyectos, la generación de nuevos planes y la evaluación de los impactos de las políticas implementadas.
* La información sobre los procesos de planificación territorial es fundamental para garantizar la transparencia y la participación ciudadana. La pérdida de esta información socava la confianza de los ciudadanos en las decisiones tomadas y limita su capacidad para participar en los procesos de toma de decisiones.
* La información precisa y completa es esencial para garantizar la legitimidad de las decisiones tomadas en materia de planificación territorial. La pérdida de información puede llevar a decisiones basadas en datos incompletos o erróneos, lo que puede tener consecuencias negativas a largo plazo.
* La información generada en el proceso es un activo institucional valioso. La pérdida de esta información puede dificultar la continuidad de las políticas y estrategias de desarrollo urbano a largo plazo, lo que puede generar inestabilidad y afectar el desarrollo sostenible de la ciudad.

Considerando lo anterior, se deduce que el riesgo de pérdida de disponibilidad de información tiene un impacto directo y significativo en el objetivo estratégico "Definir y promover un modelo colectivo de ciudad en el largo plazo", al comprometer la base de conocimiento, la transparencia, la legitimidad y la continuidad institucional, este riesgo impide la definición y promoción efectiva de un modelo colectivo de ciudad en el largo plazo.

El riesgo identificado es coherente con 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.

A continuación, se relacionan los postulados que soportan la afirmación anterior:

* El proceso de planeación territorial depende en gran medida de la información recopilada, analizada y actualizada constantemente. Esta información, que incluye datos geográficos, estudios técnicos, normativas y decisiones anteriores, es esencial para tomar decisiones informadas y garantizar la coherencia y continuidad de los planes y proyectos.
* La pérdida de información puede llevar a la toma de decisiones erróneas o incompletas, lo que a su vez puede generar ineficiencias, retrasos y costos adicionales en la implementación de proyectos de desarrollo urbano.
* La información es fundamental para garantizar la transparencia y la participación ciudadana en los procesos de toma de decisiones. La pérdida de información puede limitar la capacidad de los ciudadanos y otros actores interesados de conocer y participar en los procesos de planeación territorial.
* Si se pierde información relevante, es posible que se deban realizar nuevos estudios o análisis, lo que implica una duplicación de esfuerzos y una pérdida de recursos.
* La pérdida de información puede generar una percepción negativa de la institución, socavando la confianza de los ciudadanos y de otras entidades gubernamentales.

Sintetizando lo anterior, se puede afirmar que la pérdida de información representa un riesgo directo para la capacidad de la entidad de cumplir con su objetivo de generar condiciones normativas y facilitar el desarrollo urbano y rural. Al afectar la disponibilidad y la integridad de la información, este riesgo compromete la calidad de las decisiones tomadas, la transparencia de los procesos y la eficiencia de la gestión.

Según la información proporcionada desde la primera línea de defensa, las causas iniciales identificadas para el riesgo de pérdida de disponibilidad de información siguen siendo relevantes. Desde la segunda línea de defensa se realizó un análisis por cada una concluyendo lo siguiente:

* **Manejo manual de la información:** La dependencia de procesos manuales para la gestión de documentos y datos aumenta la probabilidad de errores humanos y la pérdida de información.
* Insuficiente entrenamiento y capacitación: La falta de conocimiento del personal sobre las políticas de seguridad y los procedimientos adecuados para el manejo de la información puede llevar a prácticas inadecuadas y a la exposición de la información a riesgos.
* **Deficiencia en la autorización de permisos:** La falta de control sobre el acceso a la información puede permitir que personas no autorizadas modifiquen o eliminen datos de manera accidental o intencional.
* **Ausencia de copias de respaldo:** La falta de copias de seguridad periódicas de la información aumenta el riesgo de pérdida total de datos en caso de un incidente.

Las causas iniciales del riesgo se mantienen, sin embargo, considerando los cambios por los cuales atraviesa la entidad es necesario que el proceso realice un análisis exhaustivo y continuo y reportar en el próximo monitoreo los avances con el objeto de mejorar significativamente su postura de seguridad y reducir el riesgo de pérdida de información.

Desde la primera línea de defensa no se reportó en detalle si se han presentado incidentes o situaciones que evidencien la materialización de las consecuencias previstas o si se observa la necesidad de evaluar la pertinencia de modificar o eliminar las consecuencias identificadas. Desde la segunda línea de defensa se realizó un análisis sobre las consecuencias tipificadas y asociadas a la pérdida de disponibilidad de información concluyendo que de manera general se identificaron las siguientes consecuencias:

* Retrasos en la toma de decisiones dado que la falta de acceso a información actualizada y confiable dificulta la evaluación de alternativas y la toma de decisiones oportunas.
* Disminución de la eficiencia es una consecuencia porque la necesidad de reconstruir información perdida o dañada genera ineficiencias y aumenta los costos operativos.
* Pérdida de reputación por la incapacidad de cumplir con los compromisos lo cual debido a la pérdida de información puede dañar la reputación de la entidad.
* Incumplimiento de normativas lo cual puede generar sanciones económicas o legales.
* Disminución de la productividad teniendo en cuenta que la falta de acceso a la información necesaria puede afectar la productividad de los funcionarios y reducir la calidad del trabajo.

En conclusión, la persistencia de las consecuencias identificadas inicialmente dependerá de la efectividad de las medidas de control implementadas y de los cambios en el entorno organizacional. Es fundamental realizar un seguimiento continuo del riesgo y ajustar las medidas de control según sea necesario de conformidad con los ajustes en el rediseño, la nueva caracterización del proceso y demás factores que influyen en esta decisión.

1. ***Autoevaluación de la efectividad de los controles****:*

Se ha revisado la evidencia proporcionada por la primera línea de defensa respecto a la utilización de los controles establecidos para mitigar el riesgo de pérdida de disponibilidad de información. La documentación presentada, que incluye registros de capacitaciones, formatos diligenciados, bitácoras de copias de respaldo y reportes de gestión de usuarios, demuestra un esfuerzo significativo por parte del proceso en la implementación de estos controles. No obstante, es de recordar que se debe realizar la actualización del mapa de riesgos dado que los controles definidos por el proceso delegan la responsabilidad a la Dirección de TIC, siendo correcto que la responsabilidad y gestión debe estar en el dominio del proceso.

La evidencia de la utilización de los controles es la siguiente:

**Capacitaciones:** Se ha evidenciado la participación a las capacitaciones realizadas por la Dirección de TIC en cumplimiento del plan de capacitación, lo cual es fundamental para mantener al personal actualizado en temas de seguridad de la información.

**Gestión de activos de información:** Los formatos de entrega de bienes y documentos, así como los registros de entrega de puesto de trabajo, demuestran un seguimiento adecuado de los activos de información.

**Gestión de usuarios:** La revisión de los usuarios y la conciliación con los directorios activos muestran un compromiso por mantener actualizada la información de acceso.

Copias de respaldo: Las bitácoras de copias de respaldo confirman que se están realizando de manera periódica.

En conclusión, existe evidencia de que los controles están siendo utilizados. La documentación presentada por la primera línea de defensa demuestra que se están llevando a cabo las actividades necesarias para implementar los controles establecidos. Sin embargo, se recomienda realizar un análisis más profundo de los registros para identificar posibles áreas de mejora y garantizar la efectividad a largo plazo de los controles.

Los controles implementados, como la capacitación, la gestión de activos, la gestión de usuarios y las copias de respaldo, contribuyen a reducir la probabilidad de ocurrencia del riesgo y a minimizar sus consecuencias en caso de que se materialice. Desde el proceso se identificó el riesgo 1: Pérdida de disponibilidad de información por fallas humanas definiendo cuatro controles los cuales desde la segunda línea de defensa fueron revisados pudiendo establecer cómo cada uno aporta en la prevención y en la mitigación del riesgo lo cual se describe a continuación:

Controles implementados y su efecto:

**CAPACITACIÓN:**

Prevención: Reduce el riesgo de errores humanos al proporcionar al personal los conocimientos necesarios para manejar la información de manera segura.

Mitigación: Facilita la detección temprana de posibles amenazas y la adopción de medidas correctivas.

**GESTIÓN DE ACTIVOS DE INFORMACIÓN:**

Prevención: Establece un control sobre los activos de información, minimizando el riesgo de pérdida o daño.

Mitigación: Facilita la recuperación de la información en caso de pérdida, ya que se cuenta con un registro de los activos.

**GESTIÓN DE USUARIOS:**

Prevención: Reduce el riesgo de acceso no autorizado a la información, limitando el acceso a los usuarios autorizados.

Mitigación: Facilita la identificación de usuarios que puedan representar una amenaza y la revocación de sus permisos de acceso.

**COPIAS DE RESPALDO:**

Prevención: Aunque este control está orientado a la mitigación del riesgo, puede ser un mecanismo de preventivo al asegurar que existen copias de respaldo que previenen la perdida de datos e información.

Mitigación: Permite recuperar la información perdida o dañada en caso de un incidente de seguridad.

En general, los controles implementados demuestran un enfoque integral para mitigar el riesgo de pérdida de disponibilidad de información. La combinación de capacitación, gestión de activos, gestión de usuarios y copias de respaldo proporciona una capa de protección sólida. Sin embargo, la efectividad de estos controles dependerá de su correcta implementación y mantenimiento.

Desde el proceso no se reportó hallazgos de auditorías lo que sugiere que, al menos en las auditorías realizadas hasta el momento, no se han identificado desviaciones o incumplimientos significativos relacionados con los controles evaluados para mitigar el riesgo de pérdida de disponibilidad de información. Este aspecto es positivo dado que la ausencia de hallazgos indica que los controles implementados están funcionando de manera efectiva y que el proceso está gestionando adecuadamente el riesgo, sin embargo, es importante recordar que la ausencia de hallazgos no necesariamente significa que no existan riesgos latentes. Podría deberse a que las auditorías realizadas no fueron lo suficientemente exhaustivas o que los riesgos aún no se han materializado, por lo tanto, aunque no se hayan encontrado hallazgos, es fundamental continuar monitoreando el desempeño de los controles y realizando auditorías periódicas para detectar cualquier desviación a tiempo.

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

La respuesta de la primera línea de defensa indica que, debido a la baja valoración del riesgo, no se formularon acciones específicas para tratarlo. Sin embargo, es fundamental recordar que incluso los riesgos considerados de bajo impacto pueden tener consecuencias significativas si se materializan. Además, la percepción del riesgo puede cambiar con el tiempo debido a factores internos o externos.

Respecto a la ausencia de acciones definidas para tratar el riesgo identificado, la Segunda Línea de Defensa considera necesario realizar las siguientes observaciones:

* Reevaluar el nivel de riesgo, si bien el riesgo fue inicialmente valorado como bajo, es fundamental realizar una reevaluación periódica para verificar si esta clasificación sigue siendo válida. Cambios en el contexto interno o externo de la organización podrían aumentar la probabilidad o el impacto de este riesgo.
* Análisis de las causas raíz, es importante analizar las causas raíz del riesgo para identificar las acciones más efectivas para mitigarlo. Incluso si el riesgo es percibido como bajo, abordar las causas raíz puede ayudar a prevenir su materialización en el futuro.
* Revisión de la documentación, la ausencia de evidencia de acciones para tratar el riesgo sugiere una posible falta de documentación o de seguimiento de las medidas implementadas. Es fundamental mantener un registro claro de todas las acciones relacionadas con la gestión de riesgos.

Aunque no se hayan identificado acciones específicas para tratar el riesgo en cuestión, es fundamental adoptar un enfoque proactivo y preventivo para garantizar la seguridad de la información. La colaboración entre la Primera y Segunda Línea de Defensa es clave para lograr este objetivo.

Desde el proceso se ha indicado que no se formularon acciones específicas para tratar el riesgo debido a su baja valoración después de aplicar los controles, así las cosas, no es posible evaluar si se están implementando adecuadamente estas acciones.

Dado que se ha establecido que no se han definido acciones específicas para tratar el riesgo debido a su baja valoración y que no se han encontrado hallazgos de auditoría asociados a este, se puede inferir que, hasta el momento, el riesgo no se ha materializado de manera evidente. Sin embargo, es importante considerar que la materialización de un riesgo puede manifestarse de diferentes formas, desde una pérdida financiera hasta un incumplimiento normativo. Es fundamental tener una definición clara de lo que se considera una materialización del riesgo en el contexto específico.

En conclusión, aunque no se haya evidenciado la materialización del riesgo hasta el momento, es crucial mantener una vigilancia constante y realizar evaluaciones periódicas para detectar cualquier cambio en el perfil del riesgo.

Así mismo, teniendo en cuenta que se ha establecido que el riesgo no se ha materializado, la pregunta sobre la formulación de acciones correctivas como consecuencia de esa materialización no es aplicable en este caso. Sin embargo, es importante resaltar la importancia de la planificación y preparación para enfrentar escenarios en los que el riesgo sí se materialice.

A pesar que el riesgo aún no se ha manifestado, es fundamental tener un plan de contingencia que detalle las acciones a seguir en caso de que esto ocurra. Este plan debe incluir: la identificación de los posibles impactos, se deben definir claramente las consecuencias negativas que podrían derivarse de la materialización del riesgo, tanto a nivel operativo como financiero, la definición de acciones correctivas a tomar para mitigar los efectos del riesgo, restaurar las operaciones y prevenir que el incidente se repita, la asignación de responsabilidades claras a los equipos y personas involucradas en la ejecución del plan de contingencia, establecer un plan de comunicación para informar a las partes interesadas sobre el incidente y las acciones tomadas y realizar pruebas y simulacros periódicos para evaluar la efectividad del plan de contingencia e identificar áreas de mejora.

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

El mapa de riesgos de seguridad de la información del proceso PLANEACIÓN TERRITORIAL Y GESTIÓN DE SUS INSTRUMENTOS muestra que se identificó un riesgo significativo relacionado con la seguridad de la información y ha implementado controles para mitigarlo. La primera línea de defensa ha reportado que estos controles se están aplicando y que la gestión del riesgo ha sido efectiva. Sin embargo, como segunda línea de defensa, es crucial realizar un análisis más profundo para evaluar la efectividad de estas medidas y su contribución a los objetivos del proceso.

La protección de la información es fundamental para garantizar el cumplimiento de los objetivos del proceso. Al asegurar la disponibilidad, integridad y confidencialidad de la información, se contribuye entre otras cosas a:

* Viabilizar la estrategia de ordenamiento territorial porque la información precisa y actualizada es esencial para tomar decisiones informadas y desarrollar planes de ordenamiento territorial coherentes.
* Facilitar el desarrollo urbano y rural ya que la protección de la información garantiza la transparencia y la participación ciudadana en los procesos de planificación.
* Definir y promover un modelo colectivo de ciudad en consideración a que la información confiable y accesible es fundamental para construir un consenso social en torno a los proyectos de desarrollo urbano.

En cuanto a la contribución a los objetivos estratégicos, se puede decir que la gestión efectiva del riesgo contribuye a:

* Mejorar la reputación institucional ya que la protección de la información refuerza la confianza de los ciudadanos y las instituciones en la entidad.
* Optimizar los recursos porque al prevenir pérdidas de información, se evitan costos adicionales asociados a la recuperación de datos y a la reconfiguración de sistemas.
* Aumentar la eficiencia de los procesos por cuanto la disponibilidad de la información facilita la toma de decisiones y agiliza los procesos.

Recogiendo lo anterior, se puede decir que la gestión del riesgo ha sido efectiva hasta el momento, pero es fundamental mantener un enfoque proactivo y continuar mejorando las medidas de seguridad garantizando la protección de la información y contribuyendo al cumplimiento de los objetivos del proceso y los institucionales.

1. ***Actualización de Riesgos****:*

Las respuestas proporcionadas por la primera línea de defensa en los monitoreos realizados indican que el proceso no identifico la necesidad de modificar y/o actualizar el mapa de riesgos establecido actualmente, sin embargo, en el entendido que los cambios en el contexto estratégico, la composición interna de los procesos y el entorno tecnológico pueden generar nuevos riesgos o modificar los existentes. En este sentido se evidencia la necesidad de revisar el riesgo identificado a la luz de la implementación de los cambios derivados del rediseño institucional y la actualización de la caracterización del proceso con el fin de mantener actualizado el mapa de riesgos.

Coincidimos con la primera línea en que la falta de documentación formal sobre los cambios derivados del rediseño institucional dificulta una evaluación precisa del impacto en los riesgos identificados. Sin embargo, es fundamental realizar un análisis más profundo y detallado una vez se formalice la nueva plataforma tecnológica.

Se recomienda revisar de forma integral el mapa de riesgos y alinearlo a la reciente caracterización del proceso con el fin de mantenerlo actualizado.

#### ALERTAS

Los cambios en el contexto estratégico, la composición interna de los procesos y el entorno tecnológico pueden generar nuevos riesgos o modificar los existentes. En este sentido se evidencia la necesidad de revisar el riesgo identificado a la luz de la implementación de los cambios derivados del rediseño institucional y la actualización de la caracterización del proceso con el fin de mantener actualizado el mapa de riesgos.

#### RECOMENDACIONES

Desde la segunda línea de defensa se recomienda:

* Evaluar la necesidad de actualizar el mapa de riesgos. Los cambios en el proceso, el nuevo manual de funciones, la reciente formalización de la caracterización del proceso, la implementación de nuevas herramientas como el nuevo sistema Gestionate, entre otras situaciones justifican plenamente esta actualización.
* Priorizar la Actualización del mapa de riesgos para garantizar que la gestión de riesgos siga siendo efectiva. La actualización debe ser integral, revisando no solo las causas y consecuencias de los riesgos, sino también los controles existentes y proponiendo nuevos si es necesario.
* La actualización debe alinear el mapa de riesgos con los requerimientos de la nueva herramienta Gestiónate, considerando los nuevos riesgos y oportunidades que esta pueda presentar. Este es un mecanismo de monitoreo continuo para identificar y responder a cualquier cambio en los riesgos o en la eficacia de los controles.
* Realizar la revisión de los controles por cuanto la responsabilidad recae sobre la Dirección de Tecnologías de la Información y las Comunicaciones, siendo correcto que el proceso sea quien lidere y gestione tanto los controles como las acciones que se requiera para el tratamiento del riesgo.
* Evaluar si el riesgo identificado es el único que puede afectar la confidencialidad, integridad y disponibilidad de la información que se gestiona al interior del proceso.

### POLÍTICAS PÚBLICAS

#### MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN (COORDINACIÓN DE LAS POLÍTICAS PÚBLICAS Y DE LOS INSTRUMENTOS DE PLANEACIÓN)

**Riesgos 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

2. 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.

#### OBSERVACIONES

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

Ante la inminente transformación del proceso de COORDINACIÓN DE LAS POLÍTICAS PÚBLICAS Y DE LOS INSTRUMENTOS DE PLANEACIÓN, el cual se dividirá en los procesos de PLAN DISTRITAL DE DESARROLLO, POLÍTICAS PÚBLICAS Y ARTICULACIÓN DEL DIÁLOGO SUPRADISTRITAL, es imprescindible realizar una evaluación de riesgos actualizada. El objetivo es identificar y mitigar cualquier nueva vulnerabilidad que pueda surgir como consecuencia de estos cambios, asegurando así la protección de la información sensible de la entidad.

Los dos riesgos identificados son coherentes con el objetivo estratégico, "Fortalecer la formulación, seguimiento y evaluación de planes, programas, políticas y proyectos en la ciudad en materia económica, social y ambiental de forma coordinada y articulada con los actores de Bogotá Región" y es aceptable hasta tanto se complete y formalice la actualización de la plataforma estratégica de la SDP. Sin embargo, es necesario programar una revisión del riesgo para verificar su persistencia y pertinencia en el nuevo contexto a la luz de luz de la nueva caracterización del proceso formulada recientemente.

Los riesgos identificados son pertinentes para el proceso actual y están alineados al 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". Anticipando el cambio de proceso, desde el proceso se ha determinado que los riesgos de seguridad de la información deberán ser reevaluados y ajustados para reflejar el nuevo contexto.

Ante el cambio de proceso, es necesario revisar y actualizar las causas de los riesgos identificados. En particular, se debe prestar atención a las deficiencias en capacitación, el manejo manual de datos y la falta de copias de seguridad. Estas áreas deben adaptarse a las nuevas políticas y al contexto estratégico del rediseño institucional.

El perfil de riesgo actual permanecerá vigente hasta la finalización de la transición hacia el nuevo modelo organizacional, por lo tanto, las consecuencias identificadas inicialmente se mantienen. Una vez implementados los cambios, se realizará un análisis exhaustivo para identificar y evaluar los nuevos riesgos que se formulen en el contexto del proceso nuevo Políticas Públicas.

1. ***Autoevaluación de la efectividad de los controles****:*

El proceso Coordinación de Políticas Públicas (DEPPD) es de reciente creación razón por la cual se están implementando nuevos procedimientos y ajustando los existentes.

Los controles aplicados están orientados a cumplir con la política A-LE 429 de seguridad y privacidad de la información, dentro de estos podemos identificar los siguientes:

* **Revisión y validación de contenidos**: Los directivos revisan y validan todos los documentos antes de su emisión final.
* **Uso del SIPA:** Se utiliza el Sistema de Información para la Gestión de Proyectos (SIPA) para emitir respuestas a solicitudes, realizar solicitudes en el marco del diseño de políticas y gestionar la agenda de evaluaciones.
* **Cumplimiento de la política A-LE 429:** Se aplican los lineamientos de seguridad y privacidad de la información establecidos en esta política.
* **Desarrollo de procedimientos:** Se están desarrollando nuevos procedimientos, como el de Evaluación de Políticas Públicas, y se siguen los existentes, como el M-PD-213 Agenda de Evaluaciones.
* **Capacitación:** Se ha impartido capacitación en seguridad de la información a los colaboradores por parte de la Dirección de Tecnologías de la información y las comunicaciones.
* **Documentación de procesos:** Se están documentando los procesos y se establecen directrices para la conservación de registros.

Se proporcionan enlaces a documentos, registros que respaldan las afirmaciones anteriores y así mismo, se menciona y aporta correos electrónicos, radicados y documentos del SIPA como evidencia del cumplimiento de los controles.

En conclusión, el proceso de Coordinación de Políticas Públicas está aplicando los controles de manera consistente evidenciando un compromiso con la mejora continua de los procesos.

En el análisis de Riesgos y Controles Propuestos para el Riesgo 1 relacionado con la Pérdida de Integridad por Fallas Humanas y definido como la posibilidad de que la información sea modificada de manera no autorizada o accidental debido a errores humanos o falta de conocimiento sobre políticas de seguridad, el proceso estableció dos controles los cuales fueron revisados concluyendo que:

**Riesgo 1: Pérdida de Integridad por fallas humanas debido a insuficiente capacitación**

**Control:** Los directivos del proceso revisan y validan los contenidos de los conceptos antes de su emisión final.

**Prevención:** Esta revisión final actúa como una barrera adicional para detectar y corregir errores humanos que puedan comprometer la integridad de la información. Al validar los contenidos, se asegura que la información sea precisa y consistente.

**Mitigación:** Detecta y corrige errores humanos antes de la emisión final.

**Control:** El Líder del proceso vela porque todos sus procedimientos se conozcan y se cumplan aplicando los lineamientos establecidos en la política A-LE 429.

**Prevención:** Al garantizar que los colaboradores conozcan y apliquen los procedimientos establecidos, se reduce la probabilidad de errores humanos causados por desconocimiento. La política A-LE 429 proporciona una guía clara sobre las prácticas de seguridad a seguir, lo que minimiza el riesgo de violaciones a la integridad de la información.

**Mitigación:** Proporciona una guía clara sobre prácticas seguras, reduciendo errores.

**Riesgo 2: Pérdida de Disponibilidad por fallas humanas debido a manejo manual de la información y ausencia de copias de respaldo**

**Control:** Los colaboradores del proceso conocen y aplican los lineamientos establecidos en la política A LE 429.

**Prevención:** La política A-LE 429 probablemente incluye lineamientos sobre la gestión de copias de seguridad y la importancia de mantener la información disponible. Al conocer estos lineamientos, los colaboradores son más conscientes de la necesidad de realizar copias de respaldo y de seguir los procedimientos adecuados para garantizar la disponibilidad de la información.

**Mitigación:** Incluye lineamientos sobre gestión de copias de seguridad.

**Control:** Los colaboradores del proceso conocen y aplican los procedimientos documentados, así como las directrices de conservación de los registros.

**Prevención:** Los procedimientos documentados deben incluir instrucciones claras sobre cómo manejar la información, incluyendo la creación y almacenamiento de copias de respaldo. Al seguir estos procedimientos, se reduce el riesgo de pérdida de datos debido a errores humanos o eventos imprevistos.

**Mitigación:** Proporciona instrucciones claras sobre el manejo de la información y la creación de copias de respaldo.

Los controles propuestos para ambos riesgos están diseñados para abordar las causas subyacentes lo cual reduce significativamente la probabilidad de que ocurran pérdidas de integridad o disponibilidad de la información.

De otra parte, desde el proceso se indicó que no se han identificado hallazgos de auditoría asociados a los controles durante el período evaluado.

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

El Criterio de Monitoreo 3 busca evaluar si las acciones implementadas para gestionar un riesgo están directamente enfocadas en abordar sus causas raíz. En otras palabras, se pregunta si las acciones adicionales a los controles están diseñadas para prevenir o mitigar la ocurrencia del riesgo en el futuro. En la evaluación de la situación actual y con la información proporcionada se concluye que no se han definido planes de acción lo que significa que no se han establecido medidas específicas para complementar los controles para abordar los riesgos identificados, esto en razón a que los dos riesgos identificados en el proceso, después de aplicados los controles tiene una valoración baja.

No se han formulado planes de acción como complemento a los controles para dar tratamiento al riesgo, como consecuencia, no existen acciones concretas orientadas a contrarrestar las causas de los riesgos. De igual forma, la Primera Línea de Defensa ha determinado que, según la información disponible, los riesgos identificados no han alcanzado su estado de materialización. En consecuencia, no se han ejecutado acciones correctivas específicas.

Se recomienda realizar evaluaciones de riesgos de manera más exhaustiva, considerando no solo los riesgos identificados inicialmente, sino también aquellos emergentes o que puedan surgir a partir de cambios en el entorno o en el proceso. Así mismo, se sugiere Incorporar a más actores, esto es involucrar a un mayor número de colaboradores en el proceso de identificación de riesgos, ya que ellos pueden tener una visión más detallada de las actividades y los posibles peligros.

Es de recordar que, lograr una gestión de riesgos proactiva y efectiva, permitirá minimizar los impactos negativos de los eventos adversos asegurando la continuidad de las operaciones. La gestión de riesgos es un proceso continuo que requiere un compromiso a largo plazo por parte de toda la entidad.

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

La gestión del Riesgo 1: Pérdida de integridad de la información ha sido útil para que a través de los controles aplicados y su seguimiento se disminuya el número de errores en los documentos generando mayor confianza en la información producida. En cuanto al riesgo 2: Pérdida de disponibilidad de la información, se puede decir que ha contribuido en la generación de una cultura institucional permitiendo el conocimiento y aplicación de los lineamientos establecidos en la política A LE 429 Políticas de seguridad y privacidad de la información y en las directrices de conservación de los registros del proceso lo que ha permitido estar preparados para solventar situaciones adversas que puedan ocasionar la materialización de un riesgo. En general, la gestión del mapa de riesgos ha sido útil para disminuir la probabilidad y el impacto en el caso que se materializara alguno de los riesgos propendiendo por la continuidad de las operaciones del proceso y el complimiento de los objetivos estratégicos.

1. ***Actualización de Riesgos****:*

La Primera Línea de Defensa se identificó la necesidad de realizar una actualización completa de riesgos del proceso, 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, la evaluación de la probabilidad e impacto de todos los riesgos y la documentación detallada del nuevo mapa de riesgos de seguridad de la información.

#### ALERTAS

Con ocasión del rediseño institucional se modificó la estructura organizacional de la entidad dando origen a nuevos procesos y eliminando algunos. En esta misma línea, se publicó el nuevo manual de funciones y se realizó la caracterización de todos los procesos de la entidad. Es relevante estar atentos a los cambios institucionales que puedan afectar el mapa de riesgos de seguridad de la información y mantener una postura proactiva para mantenerlo actualizado.

#### RECOMENDACIONES

Desde la segunda línea de defensa, se recomienda:

* Asegurar que los controles internos estén diseñados de manera adecuada para mitigar los riesgos identificados y que estén debidamente documentados.
* Verificar que los controles sean implementados de forma consistente y que el personal esté capacitado para su ejecución.
* Realizar evaluaciones periódicas de la eficacia de los controles para identificar brechas y áreas de mejora.
* Asegurar que el personal adscrito al proceso participe en la capacitación continua sobre conceptos de gestión de riesgos, herramientas y técnicas.
* Establecer canales de comunicación claros y abiertos para facilitar el intercambio de información sobre riesgos y controles.
* Realizar reuniones periódicas para realizar el seguimiento sobre el cumplimiento de los controles establecidos y alinear esfuerzos.
* Estar preparados para adoptar el nuevo sistema GESTIONATE para para facilitar la identificación, evaluación y seguimiento de los riesgos, mejorando la eficiencia administrativa reduciendo al mismo tiempo la probabilidad de la ocurrencia de materialización y el impacto en el caso de la materialización de alguno de los riesgos presentes en el proceso.

## PROCESOS DE APOYO

### GESTIÓN DEL TALENTO HUMANO

#### MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

**Riesgos 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; 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.

#### OBSERVACIONES

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

La respuesta de primera línea indica que no se han evidenciado cambios significativos en el contexto estratégico, por lo que se mantiene el contexto actual identificado por el proceso, sin embargo, se recomienda evaluar si el rediseño institucional implicó cambios sustanciales en la nueva caracterización del proceso definida recientemente, responsabilidades, o sistemas de información, lo cual podría generar nuevos riesgos o modificar los existentes. Así mismo, es recomendable estar atentos a la formalización de la nueva plataforma estratégica para poder reaccionar rápidamente en el caso que se requiera hacer ajustes en el proceso. Desde la segunda línea de defensa se respondió: Este riesgo es coherente con el objetivo estratégico de la entidad en afectación e impacto a la capacidad de la entidad para el logro de sus objetivos.

En el análisis de segunda línea de defensa se realizó la revisión de los dos riesgos frente a la coherencia con el objetivo estratégico el cual se describe a continuación:

**Riesgo 1: Posibilidad de Pérdida de Confidencialidad**

**Objetivo Estratégico que apalanca**: Fortalecer la estructura y la cultura institucional para contribuir a una gestión pública efectiva.

**Coherencia:** La pérdida de confidencialidad de información sensible puede socavar la confianza de los servidores públicos, ciudadanos y entidades externas en la entidad. Esto, a su vez, puede afectar la reputación institucional, dificultar la colaboración y la toma de decisiones, y comprometer el cumplimiento de los objetivos estratégicos.

**Análisis de la Segunda Línea:** El riesgo de pérdida de confidencialidad es altamente relevante para el objetivo estratégico mencionado, ya que la protección de la información es fundamental para garantizar la integridad y transparencia de los procesos internos.

**Riesgo 2: Posibilidad de Pérdida de Disponibilidad**

**Objetivo Estratégico que apalanca:** Fortalecer la estructura y la cultura institucional para contribuir a una gestión pública efectiva.

**Coherencia:** La pérdida de disponibilidad de la información puede interrumpir las operaciones diarias del proceso, generar retrasos en la prestación de servicios y afectar la eficiencia y eficacia de la entidad. Esto, a su vez, puede comprometer el cumplimiento de los objetivos estratégicos y generar insatisfacción en los ciudadanos y empleados.

**Análisis de la Segunda Línea:** El análisis de la Segunda Línea determinó que el riesgo de pérdida de disponibilidad está directamente relacionado con el objetivo estratégico de fortalecer la estructura institucional, ya que la disponibilidad de la información es esencial para el funcionamiento adecuado de los procesos y la toma de decisiones.

No se evidenció riesgos asociados al segundo objetivo estratégico al que aporta el proceso según el contexto que definió el proceso, "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."

El proceso contestó que este riesgo es coherente con el objetivo del proceso en afectación e impacto a la capacidad de la entidad para el logro de sus objetivos. En el análisis de segunda línea de defensa sobre los dos riesgos identificados en el proceso se obtuvo como resultado lo siguiente:

**Riesgo 1: Posibilidad de Pérdida de Confidencialidad**

**Coherencia con el Objetivo del Proceso:** La pérdida de confidencialidad de la información personal de los empleados puede generar una violación a la privacidad, erosionar la confianza en la entidad y afectar la reputación institucional. Esto, a su vez, dificulta la atracción y retención del talento, lo cual es fundamental para el logro del objetivo de administrar el talento humano de manera efectiva.

**Análisis de la Segunda Línea:** El riesgo de pérdida de confidencialidad está directamente relacionado con el objetivo del proceso, ya que la gestión del talento humano implica el manejo de una gran cantidad de información personal sensible. La protección de esta información es esencial para garantizar el cumplimiento de las normativas laborales y de protección de datos, y para mantener un ambiente de trabajo seguro y confiable.

**Riesgo 2: Posibilidad de Pérdida de Disponibilidad**

**Coherencia con el Objetivo del Proceso:** La pérdida de disponibilidad de la información puede generar interrupciones en los procesos de gestión del talento humano, como la nómina, la evaluación del desempeño, y la capacitación. Esto puede afectar la satisfacción de los empleados, generar demoras en los pagos y comprometer el cumplimiento de las obligaciones laborales de la entidad.

**Análisis de la Segunda Línea:** El riesgo de pérdida de disponibilidad está directamente relacionado con el objetivo del proceso, ya que la disponibilidad de la información es esencial para la ejecución eficiente de las actividades de gestión del talento humano. La pérdida de información puede generar retrasos, ineficiencias y afectar la capacidad de la entidad para tomar decisiones basadas en datos precisos y actualizados.

Para afirmar que las causas identificadas inicialmente para los riesgos se mantienen, desde la segunda línea de defensa se analizaron los dos riesgos identificados en el proceso así:

**Riesgo 1: Posibilidad de Pérdida de Confidencialidad**

• Causas Iniciales Identificadas:

* Manejo manual de la información
* Copias no controladas

• Análisis de la Segunda Línea:

Aunque las causas definidas para el primer riesgo se mantienen, se sugiere revisar si existen otras causas, por ejemplo:

* Falta de capacitación en seguridad de la información.
* Acceso no restringido a sistemas y datos sensibles.
* Uso de dispositivos personales para fines laborales.
* Falta de políticas claras y procedimientos para el manejo de información confidencial.

**Riesgo 2: Posibilidad de Pérdida de Disponibilidad**

• Causas Iniciales Identificadas:

* Retraso en la salida de información de los sistemas
* Desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información
* Manejo manual de la información
* Ausencia de validación de autenticación de la información
* Información sensible sin cifrado
* Ausencia de validación de autenticación de la información

• Análisis de la Segunda Línea:

Aunque las causas identificadas en el segundo riesgo se mantienen, es necesario revisar si estas causas derivan e perdidas de disponibilidad o de integridad. Se recomienda analizar si existe otras causas enfocadas directamente al riesgo como, por ejemplo:

* Fallas en los sistemas de información.
* Desastres naturales.
* Errores humanos.
* Falta de redundancia en los sistemas.

Para cada riesgo identificado, la Segunda Línea de Defensa se realizó un análisis primario de las consecuencias iniciales para evaluar si se mantienen o si han surgido nuevas consecuencias. A continuación, se presenta el resultado:

**Riesgo 1: Posibilidad de Pérdida de Confidencialidad**

El riesgo tiene un impacto reputacional. Afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta directiva y accionistas y/o de proveedores

• Consecuencias Iniciales Identificadas:

Las consecuencias reconocidas por el proceso están asociadas a:

* Pérdida de reputación.
* Daño a la imagen de la entidad.

• Análisis de la Segunda Línea:

Aunque se reconoce que el impacto de las consecuencias en los objetivos estratégicos de la entidad y en los intereses de las partes interesadas principal es reputacional, no debe perderse de vista la existencia del impacto económico que pude darse por sanciones legales y a nivel interno se podría identificar consecuencias morales como la pérdida de confianza de las personas vinculadas a la entidad.

De acuerdo con lo anterior, las consecuencias identificadas en el primer riesgo se mantienen.

**Riesgo 2: Posibilidad de Pérdida de Disponibilidad**

• Consecuencias Iniciales Identificadas:

Desde el proceso se definió un impacto Económico - Reputacional, se le da mayor peso al económico considerando una afectación menor a 10 SMLMV.

• Análisis de la Segunda Línea:

Desde la perspectiva de la segunda línea de defensa, el impacto de las consecuencias en los objetivos estratégicos de la entidad y en los intereses de las partes interesadas está directamente relacionado con lo económico derivado de las siguientes consecuencias:

* Interrupción de los procesos de negocio.
* Pérdida de productividad.
* Insatisfacción de los clientes.
* Pérdidas financieras.

En conclusión, basado en el análisis las consecuencias iniciales para los dos riesgos identificados se mantienen. Si se identifican nuevas consecuencias, se debe actualizar el Mapa de Riesgos para reflejar la realidad y definir las acciones necesarias para controlar el riesgo.

1. ***Autoevaluación de la efectividad de los controles****:*

El proceso de Gestión del Talento Humano de la SDP presenta una serie de riesgos que han sido identificados y para los cuales se han establecido controles. La Segunda Línea de Defensa revisó los controles para cada riesgo con el fin de observar si están siendo utilizados de manera efectiva y si existe evidencia de su aplicación. En la revisión se detectó que no se dispuso de evidencia en el repositorio relacionada con los controles (Actividad de sensibilización para el control de la información y Actividad de sensibilización para el manejo de la información), por lo cual se solicita para el siguiente monitoreo publicarlas de conformidad con los lineamientos dados por la Dirección de Planeación Institucional.

A continuación, se presenta una descripción del análisis para los dos riesgos identificados, considerando la información proporcionada y las evidencias disponibles:

**Riesgo 1: Posibilidad de Pérdida de Confidencialidad**

• Controles Identificados:

* Capacitación en seguridad de la información.
* Uso de carpetas compartidas controladas incluyendo la restricción de hacer copias no controladas.

• Análisis de la Segunda Línea:

Teniendo en cuenta que no se encontró evidencia en el repositorio dispuesto por la Dirección de Planeación Institucional, se requiere que para el siguiente monitoreo se disponga las evidencias que soporten las respuestas a los criterios de evaluación.

Si bien se mencionan capacitaciones, se requiere evidencia más detallada sobre la efectividad de estas y soportes como formato A-FO-205 (Inducción en el puesto de trabajo), el formato de asistencia (A-FO 183) listas con nombres de participantes y A-FO 258 Bitácora Solicitud Cuentas de Usuario.

Es necesario verificar si los accesos a las carpetas compartidas están debidamente restringidos para lo cual se debe mantener registros de acceso a las carpetas compartidas (usuarios, fechas, acciones).

Se debe evaluar si las políticas y procedimientos están siendo comunicados y aplicados de manera consistente y si se está aplicando controles relacionados con la protección de datos.

**Riesgo 2: Posibilidad de Pérdida de Disponibilidad**

Aunque no se menciona, entre los controles Identificados, el uso del aplicativo PERNO es uno de ellos.

A continuación, se relacionan los controles establecidos desde el proceso y el detalle relacionado:

* Control de Acceso a la Información:
* Registros detallados: Se mantienen registros precisos de quién accede a qué información y cuándo.
* Permisos restringidos: El acceso a la información se limita a personal autorizado y se controla mediante solicitudes formales. Se requiere evidencia del diligenciamiento del formato A-FO-010 y para los retirados reporta en el A-FO-128
* Bitácoras de acceso: Se llevan registros detallados de las actividades realizadas en los sistemas de información. Se requiere evidencias del uso del A-FO-227 SOLICITUD REQUERIMIENTO USUARIO (SISTEMAS DE INFORMACIÓN/APLICACIONES DE SOFTWARE) y la creación de requerimientos a través del Sistema de Requerimientos, el desarrollo de aplicaciones o módulos.
* Capacitación en seguridad: Se imparten capacitaciones regulares al personal sobre las políticas de seguridad de la información.
* Control de la Información:
* Copias de seguridad: Se realizan copias de seguridad periódicas de la información para garantizar su recuperación en caso de pérdida.
* Uso de Herramientas Tecnológicas: Registra en la herramienta de gestión SIPA la traza de actos administrativos y se indica el uso de un sistema para el seguimiento de las solicitudes de requerimiento de usuarios.
* Actualización de políticas: Las políticas de seguridad de la información se actualizan regularmente para reflejar los cambios en el entorno y las regulaciones.
* Verificación de la información: Se verifica la precisión y la integridad de la información antes de su uso.
* Control de Procesos:
* Procedimientos estandarizados: Se establecen procedimientos claros y detallados para las diferentes actividades del proceso como por ejemplo la solicitud de permisos de acceso y las solicitudes de requerimientos de usuario.
* Seguimiento de solicitudes: Se lleva un seguimiento riguroso de las solicitudes de acceso a la información y de los cambios en los sistemas.

Se recomienda realizar la revisión de incidentes de seguridad para identificar las causas y tomar medidas correctivas y verificar que se realice un mantenimiento regular de los equipos para garantizar su correcto funcionamiento.

Los controles 4 y 5 son iguales por lo que se recomienda revisar y evaluar la eliminación de uno de los controles.

Se resalta la revisión de nuevas herramientas en el mercado que satisfagan no solo las necesidades de la entidad, sino que además procuren por la actualización tecnológica.

En resumen, los controles implementados buscan:

* Proteger la confidencialidad de la información: Limitando el acceso a la información a personal autorizado y estableciendo mecanismos de control para prevenir la divulgación no autorizada.
* Garantizar la integridad de la información: Asegurando que la información sea precisa, completa y confiable.
* Aumentar la disponibilidad de la información: Realizando copias de seguridad periódicas.
* Cumplir con las normativas y políticas: Adhiriéndose a las leyes y regulaciones aplicables en materia de protección de datos y seguridad de la información.
* Estos controles contribuyen a:
* Reducir el riesgo de pérdida de datos.
* Proteger la reputación de la Entidad.
* Cumplir con los requisitos legales y regulatorios.
* Mejorar la eficiencia y la eficacia de los procesos.

Se recomienda evaluar la formulación del segundo control, por cuanto la lectura deja entre ver que se trata de un procedimiento para la gestión 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) por ende, se debería establecer el procedimiento, así mismo, el control debería formularse en el sentido de hacer cumplir el procedimiento que se defina.

Basándonos en la descripción de los controles implementados para los dos riesgos de pérdida de confidencialidad y disponibilidad de información, podemos concluir que, los controles examinados tienen como objetivo principal prevenir y mitigar estos riesgos.

Los controles aportan en la Prevención de la siguiente manera:

* Capacitación: Al capacitar al personal en seguridad de la información, se busca prevenir errores humanos que puedan llevar a la divulgación accidental de información confidencial.
* Restricción de acceso: Al limitar el acceso a la información a personal autorizado, se reduce la probabilidad de que personas no autorizadas puedan acceder a datos sensibles.
* Procedimientos estandarizados: Los procedimientos claros y detallados ayudan a garantizar que las tareas se realicen de manera consistente y segura, reduciendo el margen de error.
* Copias de seguridad: Las copias de seguridad periódicas permiten recuperar la información en caso de pérdida o daño, minimizando el impacto de un incidente.
* Actualización de políticas: Al mantener las políticas de seguridad actualizadas, se garantiza que los controles estén alineados con las últimas amenazas y regulaciones.

Los controles aportan en la mitigación así:

* Detección temprana: Los controles permiten detectar a tiempo posibles incidentes de seguridad, lo que facilita la respuesta y reduce el impacto.
* Recuperación de datos: En caso de un incidente, las copias de seguridad permiten restaurar los datos perdidos y minimizar las interrupciones en las operaciones.
* Reducción del impacto: Al limitar el alcance de los datos a los que pueden acceder los usuarios, se reduce el impacto potencial de una brecha de seguridad.

En resumen, los controles implementados están diseñados para crear una barrera de protección alrededor de la información sensible de la organización, reduciendo la probabilidad de que ocurran incidentes de seguridad y minimizando las consecuencias en caso de que ocurran. Estos controles contribuyen a:

* Reducir el riesgo de pérdida de datos.
* Proteger la reputación de la organización.
* Cumplir con los requisitos legales y regulatorios.
* Mejorar la eficiencia y la eficacia de los procesos.

La primera línea de defensa, es decir, los responsables directos de la operación y ejecución de los controles, ha respondido que en el periodo evaluado no se identificaron hallazgos de auditoría asociados al control en cuestión.

En base a la información proporcionada por la primera línea de defensa, se confirma que en el periodo evaluado no se han registrado hallazgos de auditoría directamente relacionados con los nueve controles. Sin embargo, es importante destacar que la ausencia de hallazgos no necesariamente implica que el control esté funcionando de manera óptima y efectiva en todos los aspectos.

Se recomienda realizar un análisis más detallado de los controles, incluyendo una revisión de la documentación, entrevistas a los responsables y una evaluación del desempeño de los controles.

Evaluar si las auditorías realizadas cubrieron de manera exhaustiva todos los aspectos del control y si los procedimientos de auditoría fueron adecuados

Se sugiere continuar monitoreando el control de manera proactiva y realizar ajustes si es necesario para garantizar su efectividad a largo plazo.

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

La información proporcionada por la Primera Línea presenta inconsistencias significativas respecto a la implementación de acciones para tratar los riesgos identificados. En los monitoreos se reportó que debido al nivel del riesgo no se establecieron acciones de tratamiento, sin embargo, se pudo evidenciar en el mapa de riesgos que se formularon planes de acción con sus respectivas acciones complementarias a los controles definidos en el proceso.

Respecto al primer riesgo:

A pesar de la afirmación inicial que no se han formulado acciones, se evidencia que se han implementado dos acciones concretas para abordar el riesgo de pérdida de confidencialidad de la información: capacitación en seguridad de la información y control de acceso a los datos. Estas acciones están directamente orientadas a las causas raíz del riesgo: la falta de conocimiento del personal y el acceso no autorizado a información sensible, sin embargo, es necesario evaluar la eficacia de estas acciones a través de indicadores clave de desempeño (KPIs) y retroalimentación del personal. Se recomienda realizar un seguimiento regular de la participación en las capacitaciones y del cumplimiento de las políticas de acceso.

Respecto al segundo riesgo:

Se han implementado múltiples acciones para mitigar el riesgo de pérdida de disponibilidad de la información. Estas acciones se centran en la realización de copias de seguridad, el control de acceso a los sistemas y la mejora de los procesos. No obstante, dado que no se realizó la evaluación del riesgo residual, no es posible determinar si estas acciones han sido suficientes para reducir el riesgo a un nivel aceptable. Es fundamental realizar una evaluación exhaustiva para identificar si existen brechas o áreas de mejora. Además, es necesario analizar si las acciones implementadas abordan la causa raíz del problema. En algunos casos, puede ser necesario invertir en nuevas tecnologías o procesos para garantizar la disponibilidad de la información.

En la revisión de segunda línea de defensa se realizó el siguiente análisis:

Primer Riesgo: Se han definido acciones claras y directas para abordar el riesgo, centradas en la sensibilización y capacitación del personal. Sin embargo, no se ha proporcionado información sobre la implementación efectiva de estas acciones. Es decir, no es posible establecer si las capacitaciones se están llevando a cabo según lo programado, si los colaboradores adscritos al proceso están participando activamente o si se están evaluando los resultados de estas iniciativas.

Segundo Riesgo: Se ha establecido un plan de acción bastante detallado, pero igual que para el primer riesgo falta información sobre su implementación. No se sabe si se han realizado las copias de seguridad, si se han validado las restricciones de acceso o si se ha modificado el procedimiento A IN 019. Además, la ausencia de una evaluación del riesgo residual impide determinar si las acciones implementadas han sido suficientes para reducir el riesgo a un nivel aceptable.

La primera línea de defensa, es decir, los responsables directos de la operación y ejecución de los controles, ha respondido que en el periodo evaluado no se identificaron hallazgos de auditoría asociados al control en cuestión. Con base a la información proporcionada por la primera línea de defensa, se confirma que en el periodo evaluado no se han registrado hallazgos de auditoría directamente relacionados con los controles. Sin embargo, es importante destacar que la ausencia de hallazgos no necesariamente implica que el control esté funcionando de manera óptima y efectiva en todos los aspectos.

En el primer monitoreo, la primera línea de defensa indicó que no aplica esta pregunta debido a la no materialización de los riesgos, en el segundo monitoreo informó que no aplicaba. Si bien es positivo que hasta el momento no se hayan materializado riesgos significativos, es fundamental que la entidad esté preparada para responder de manera efectiva en caso de que ocurran.

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

La Primera Línea de Defensa ha afirmado que la gestión de los riesgos ha sido útil para evitar situaciones que afecten el cumplimiento de los objetivos del proceso. La Segunda Línea de Defensa reconoce los esfuerzos realizados por la Primera Línea para implementar controles y monitorear los riesgos asociados al proceso, sin embargo, Si bien se menciona que se realizan reuniones semanales para dar seguimiento a las actividades, se requiere evidencia más concreta de que estos controles están evitando la materialización de los riesgos, por ejemplo, incluir en la agenda temas relacionados con los riesgos identificados y los controles implementados.

Se sugiere evaluar la necesidad de implementar controles adicionales, como la realización de auditorías periódicas o la implementación de herramientas de monitoreo continuo.

1. ***Actualización de Riesgos****:*

La primera línea de defensa ha informado que no se han identificado cambios en los riesgos existentes. Sin embargo, considerando el contexto de rediseño institucional y la nueva caracterización del proceso, la segunda línea de defensa considera necesario realizar un análisis más detallado para garantizar que la evaluación de riesgos siga siendo precisa y completa.

Se recomienda lo siguiente:

Realizar una revisión exhaustiva de la nueva caracterización del proceso para identificar cualquier cambio en los objetivos, actividades, o interacciones con otros procesos que puedan generar nuevos riesgos o modificar los existentes.

Evaluar cómo los cambios estratégicos derivados del Decreto 432 de 2022 impactan en el perfil de riesgo del proceso. Es necesario identificar si estos cambios generan nuevas vulnerabilidades o si modifican la probabilidad o el impacto de los riesgos existentes.

La primera línea de defensa ha indicado que no se ha identificado la necesidad de documentar y gestionar nuevos riesgos. Sin embargo, la segunda línea de defensa debe realizar una evaluación más profunda considerando los cambios en el contexto estratégico y el rediseño institucional.

#### ALERTAS

La primera línea de defensa ha informado que no se han identificado cambios en los riesgos existentes. Sin embargo, considerando el contexto de rediseño institucional, el nuevo manual de funciones y la nueva caracterización del proceso, la segunda línea de defensa considera necesario realizar un análisis más detallado para garantizar que la evaluación de riesgos siga siendo precisa y completa.

#### RECOMENDACIONES

Con el fin de lograr una eficiente gestión de los riesgos de seguridad de la información, desde la Segunda Línea de Defensa se recomienda lo siguiente:

* Mantener un registro detallado de todas las actividades relacionadas con la gestión de riesgos, incluyendo:
* Evidencia de capacitaciones (asistencias, evaluaciones).
* Resultados de pruebas de controles.
* Evidencia de reuniones sobre gestión de riesgos.
* Soportes sobre reporte o Informes de incidentes y acciones correctivas.
* Establecer indicadores clave de desempeño (KPI): Definir métricas específicas para medir la efectividad de los controles y el avance en la mitigación de riesgos. Estos KPI deben ser claros, medibles, alcanzables, relevantes y temporales (SMART).
* Revisar periódicamente los controles: Implementar un programa de pruebas de controles para verificar su eficacia de forma regular. Priorizar las pruebas en función del nivel de riesgo asociado a cada control.
* Actualizar los análisis de riesgos: Realizar evaluaciones de riesgos de forma periódica para identificar nuevos riesgos emergentes y evaluar si los riesgos existentes han cambiado.
* Asistir a las capacitaciones sobre el uso de la herramienta GESTIONATE dispuesta por la entidad para automatizar tareas repetitivas y mejorar la eficiencia de los procesos de gestión de riesgos.
* Asistir a las capacitaciones que realiza la Dirección de TIC sobre Seguridad de la Información.
* Abordar las discrepancias identificadas en el informe, como la falta de evidencia sobre la implementación de algunas acciones.
* Realizar una evaluación más profunda de la efectividad de las capacitaciones en seguridad de la información.
* Verificar que los controles de acceso a la información sean adecuados y se apliquen de manera consistente.
* Asegurarse de que las copias de seguridad sean suficientes para recuperar la información en caso de un incidente.
* Realizar un análisis exhaustivo de los riesgos emergentes, especialmente aquellos relacionados con los cambios organizacionales y tecnológicos.
* Revisar y validar los riesgos una vez se implemente la plataforma estratégica 2024-2027, y actualizar el contexto estratégico del proceso.

### GESTIÓN CONTRACTUAL

#### MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN (CONTRATACIÓN DE BIENES Y SERVICIOS)

**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.

#### OBSERVACIONES

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

La Primera Línea de Defensa ha afirmado que el contexto estratégico del proceso se mantiene y ha justificado esta afirmación con la actualización de diversos documentos relacionados con la gestión de riesgos; Mapa Riesgos Gestión (30-Abr-2024), Mapa Riesgo Seguridad (30-Abr-2024), Mapa Riesgos Corrupción (31-Ene-2024) y el Manual Integrado de Contratación (25-Abr-2024).

Si bien la primera línea de defensa ha realizado un esfuerzo por actualizar la documentación relacionada con los riesgos, es necesario realizar un análisis más detallado para confirmar si el contexto estratégico se mantiene. La implementación de la resolución 422 de 2022 expedida por parte de la Alcaldía Mayor de Bogotá en el rediseño institucional y la definición de la nueva caracterización del proceso puede generar cambios significativos en la estructura del proceso que puedan afectar el perfil de riesgo del proceso de contratación.

Para determinar si el riesgo identificado (pérdida de integridad de la información) es coherente con el objetivo estratégico del proceso, se analizó cómo este riesgo podría afectar el cumplimiento del 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."

En el análisis del riesgo se identificó que la pérdida de integridad de la información implica que la información relacionada con los procesos de contratación puede ser alterada, destruida o perdida, lo que podría tener las siguientes consecuencias:

* Decisiones erróneas: La toma de decisiones basada en información incorrecta o incompleta puede llevar a la selección de proveedores inadecuados o a la contratación de bienes o servicios que no cumplan con los requisitos establecidos.
* Retrasos en los procesos: La pérdida de información puede generar retrasos en la ejecución de los procesos de contratación, afectando la eficiencia y la oportunidad de los proyectos.
* Problemas legales: La manipulación de información puede dar lugar a responsabilidades legales para la entidad y sus funcionarios.
* Pérdida de confianza: La pérdida de integridad de la información puede generar una pérdida de confianza por parte de los ciudadanos y los proveedores, afectando la reputación de la entidad.

Derivado de lo anterior, la pérdida de integridad de la información representa un riesgo directo para el logro del objetivo estratégico. Al comprometer la transparencia, la eficiencia y la toma de decisiones basadas en información confiable, este riesgo debilita la gestión pública efectiva. En conclusión, el riesgo identificado (pérdida de integridad de la información) es coherente con el objetivo estratégico del proceso. La protección de la integridad de la información es fundamental para garantizar la transparencia, la eficiencia y la eficacia de los procesos de contratación, lo cual es esencial para fortalecer la estructura y la cultura institucional.

Aunque la respuesta dada por el proceso no es explicita, desde la primera línea de defensa se identifica que el riesgo es altamente coherente con el objetivo del proceso "Adquirir productos, bienes y servicios de manera eficiente y transparente, a través de procesos de contratación adelantados dentro del marco que establece la normatividad vigente, con el fin de satisfacer necesidades que en materia contractual requieran las dependencias de la SDP, contribuyendo así al cumplimiento de los fines y objetivos institucionales.". La pérdida de integridad de la información puede comprometer directamente la eficiencia, la transparencia y el cumplimiento normativo del proceso de contratación, lo que a su vez dificulta la satisfacción de las necesidades de las dependencias de la SDP y el cumplimiento de los objetivos institucionales.

La pérdida de información afecta directamente la capacidad del proceso de contratación para ser eficiente y transparente, la falta de integridad de la información impide el cumplimiento normativo y puede generar decisiones incorrectas y la información confiable es esencial para satisfacer las necesidades de las dependencias y lograr los objetivos institucionales.

Desde la Primera línea de defensa se respondió que no se requiere nuevos ajustes, por lo tanto, la información se mantiene, teniendo en cuenta que la misma tiene coherencia con el objetivo estratégico del proceso de Contratación de Bienes y Servicios. Esto infiere que las razones iniciales por las cuales se identificó el riesgo de pérdida de integridad de la información siguen siendo válidas después de implementar el mapa de riesgos y las medidas de control correspondientes. En otras palabras, las causas raíz del problema persisten a pesar de las acciones tomadas.

De la respuesta enviada desde el proceso se puede inferir que, las consecuencias negativas que se previeron inicialmente al identificar el riesgo de pérdida de integridad de la información siguen siendo relevantes después de implementar las medidas de control y de realizar un seguimiento al mapa de riesgos. Las acciones tomadas han logrado mitigar o eliminar las consecuencias adversas del riesgo.

1. ***Autoevaluación de la efectividad de los controles****:*

Se observa un esfuerzo por parte de la primera línea de defensa en implementar controles para mitigar el riesgo de pérdida de integridad de la información. Sin embargo, la segunda línea de defensa ha identificado algunas inconsistencias en la presentación de evidencias y solicita para el próximo monitoreo mayor detalle en el seguimiento de los controles.

**EVALUACIÓN DE LOS CONTROLES:**

**Control: Jornadas de inducción-reinducción**

La Evidencia Presentada; A-FO-184 CONTROL DE REUNIONES con listas de asistencia y talleres realizados evidencia la realización de las jornadas, pero se recomienda verificar la profundidad de los contenidos y la evaluación de la efectividad.

**Control: Copias de seguridad**

No se evidencia reportes de respaldo, pruebas de restauración exitosas, sin embargo, se hace necesario indicar al proceso que los controles deben ser diseñados de modo que puedan ser gestionados al interior del proceso. Para el caso específico, la solicitud de la inclusión de los backup de la información a la Dirección TIC y revisión periódica pueden ser un buen ejemplo.

De la respuesta de primera línea se infiere la realización de copias de seguridad, pero se recomienda verificar la frecuencia de las pruebas de restauración y la integridad de los datos respaldados, incluyendo fechas y resultados.

**Control: Seguimiento al PAA-2024**

La primera línea de defensa facilitó presentaciones, en las cuales se evidencia el seguimiento al PAA y a la contratación, pero se puede observar un análisis detallado de las desviaciones identificadas y las acciones correctivas implementadas, así como los indicadores de cumplimiento.

**Control Gestión de usuarios**

Se informó desde la primera línea de defensa que se realiza la gestión de usuarios, sin embargo, no se pudo encontrar registros que permitan identificar su uso. Se recomienda reformular el control de modo que pueda ser gestionado desde el proceso y no delegado a otras dependencias como la Dirección de TI.

Las respuestas proporcionadas en el primer y segundo seguimiento por la primera línea de defensa indican un esfuerzo por implementar y monitorear los controles diseñados para mitigar el riesgo de pérdida de integridad de la información. Sin embargo, para dar un concepto ajustado a la realidad, es necesario describir la forma como desde el proceso visualizan que los controles previenen o mitigan los riesgos y aportar evidencia.

A continuación, se presenta una evaluación detallada de cada control, considerando las respuestas proporcionadas y los criterios generales de eficacia:

**Control 1. Sesiones de inducción y reinducción:** Potencialmente efectivo, pero requiere evidencia más sólida sobre el impacto en el comportamiento y la reducción de incidentes. No se evidencia evaluaciones de conocimiento post-capacitación, indicadores de cumplimiento de políticas, registro de incidentes relacionados con seguridad de la información. Es necesario medir el cambio de comportamiento y la reducción de errores humanos.

**Control 2. Copias de seguridad periódicas:** Efectivo si se realizan de manera regular y se verifican las restauraciones. No se evidencia reportes detallados de las copias de seguridad, pruebas de restauración exitosas, políticas de retención. Es importante establecer un plan de recuperación ante desastres y realizar pruebas periódicas.

**Control 3. Verificación de la información a tramitar:** Contribuye a la integridad de la información, pero requiere procesos formales de revisión y aprobación. No se evidencia Listas de verificación, registros de revisiones, procedimientos documentados. Es necesario definir claramente los criterios de revisión y asignar responsabilidades.

**Control 4. Cumplimiento de plazos:** Contribuye a la eficiencia del proceso, pero no garantiza por sí solo la integridad de la información. Se evidencia reuniones de seguimiento, pero no se evidencia cronogramas, reportes de avance, indicadores de cumplimiento. Es importante vincular el cumplimiento de plazos con la calidad de la información y la prevención de errores.

**Control 5. Sesiones de sensibilización sobre seguridad de la información:** Contribuye a crear conciencia, pero requiere seguimiento y refuerzo. No se evidencia encuestas de satisfacción, registro de participación, casos prácticos. Es necesario evaluar el impacto de las sesiones en el comportamiento del personal.

**Control 6. Plan de sensibilización de Seguridad de la Información**: Potencialmente efectivo, pero depende de su implementación y seguimiento. No se evidencia un Plan detallado, calendario de actividades, métricas de cumplimiento. Es importante evaluar la efectividad del plan y realizar ajustes si es necesario.

Desde el proceso se respondió que no aplica, sin embargo, todos los procesos institucionales son objeto de auditorías no solo para determinar el estado actual, sino que además permite descubrir acciones de mejora. Se solicita para el próximo monitoreo, si se mantiene la respuesta, que sea justificada informando las razones por las cuales el proceso considera que no aplica la evaluación de hallazgos de auditoria asociados a los controles.

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

Desde el proceso se contestó “Si, Las acciones establecidas para la mitigación del riesgo continúan siendo eficientes, toda vez que, como resultado de las auditorías internas y externas al proceso de Contratación de Bienes y Servicios, no se recibieron hallazgos que evidenciaran cualquier clase de materialización del riesgo o falencia en las acciones que actualmente se tienen definidas.”. Coincidimos con la primera línea de defensa en que las acciones formuladas para mitigar el riesgo están orientadas a contrarrestar sus causas, sin embargo, a fin de dejar claridad es necesario conocer desde el proceso las razones que ha determinado esta afirmación.

Desde la segunda línea se infiere que, los controles como las actividades de capacitación, copias de seguridad, verificación de información, cumplimiento de plazos y sensibilización sobre seguridad de la información siguen siendo relevantes y contribuyen a mitigar las causas subyacentes del riesgo, tales como: las fallas humanas, la pérdida de información y el uso indebido de permisos de acceso.

En cuanto a las dos acciones formuladas; hacer la revisión de los equipos críticos del proceso y solicitar la copia de respaldo de la información de dichos equipos (migración a escritorios virtuales) y revisión de los usuarios con permisos de acceso a la información contractual, en las carpetas compartidas con acceso y roles asignados en SisCo y Secop (Depuración Directorio Activo), están diseñadas de manera directa para abordar las causas raíz del riesgo identificado, que es la pérdida de integridad de la información debido a fallas humanas, pérdida de información y uso indebido de permisos de acceso. A continuación, se detalla el análisis realizado por cada acción:

**La revisión de equipos críticos y migración a escritorios virtuales produce los siguientes efectos:**

* **Reduce el riesgo de pérdida de datos**: La migración a escritorios virtuales centraliza la gestión de los datos, facilitando la creación de copias de seguridad completas y consistentes. Además, al separar los datos del dispositivo físico, se reduce el riesgo de pérdida de información por fallas en hardware o software.
* **Minimiza el riesgo de ataques maliciosos:** Los escritorios virtuales son menos vulnerables a ataques directos, ya que el sistema operativo y las aplicaciones se ejecutan en servidores centralizados. Esto dificulta la instalación de malware y la manipulación de datos.
* **Facilita la recuperación de datos:** En caso de incidentes, la recuperación de datos es más rápida y sencilla desde una imagen de respaldo del escritorio virtual.

**La revisión de usuarios con permisos de acceso y depuración del Directorio Activo contribuye a:**

* **Reduce el riesgo de acceso no autorizado**: Al revisar y depurar los permisos de acceso, se asegura que solo el personal autorizado tenga acceso a la información confidencial. Esto minimiza el riesgo de que personas no autorizadas modifiquen o eliminen datos.
* **Identifica cuentas inactivas:** La depuración del Directorio Activo permite identificar y eliminar cuentas de usuarios que ya no son necesarios, reduciendo la superficie de ataque y minimizando el riesgo de acceso no autorizado.
* **Mejora la trazabilidad:** Al mantener un registro actualizado de los usuarios y sus permisos, se facilita la investigación de incidentes de seguridad y se mejora la trazabilidad de las acciones realizadas en el sistema.

En resumen, ambas acciones trabajan en conjunto para:

* **Reducir las fallas humanas**: Al centralizar la gestión de datos y simplificar los procesos, se minimizan los errores humanos que pueden llevar a la pérdida de información.
* **Proteger la información:** Al implementar copias de seguridad regulares y controlar el acceso a los datos, se protege la información de pérdidas, daños y accesos no autorizados.
* **Mejorar la seguridad:** Al mantener actualizado el Directorio Activo y realizar revisiones periódicas, se mejora la seguridad del sistema y se reduce el riesgo de ataques cibernéticos.

Estas acciones son fundamentales para garantizar la integridad de la información y mitigar los riesgos identificados. Al abordar directamente las causas raíz del problema, se contribuye a proteger los activos de la entidad y a cumplir con los requisitos de seguridad.

A partir de la respuesta de la primera línea, se infiere un progreso en la implementación de las siguientes acciones:

* **Migración a escritorios virtuales:** Se ha migrado a una solución de escritorios virtuales y está en operación lo que supone que se ha completado para todos los equipos críticos y se han realizado el seguimiento del funcionamiento.
* **Revisión de permisos de acceso:** Se mantiene un proceso continuo de revisión de usuarios y se ha reportado a la Dirección de TIC las cuentas de usuarios que deban ser actualizadas o eliminadas del directorio activo.

Aunque no se haya dispuesto evidencias sobre los controles implementados, en el mapa de riesgos del proceso se observó que, el último seguimiento a las acciones definidas en el mapa de riesgos se realizó el 06 de mayo de 2024, por lo que se recomienda evaluar periódicamente el plan de acción y realizar los ajustes necesarios para adaptarlo a los cambios en el entorno y a los nuevos riesgos emergentes con el fin de logar su complimiento en procura de salvaguardar la seguridad de la información gestionada desde el proceso.

Aunque se ha observado un progreso en la implementación de las acciones, se requiere hacer un seguimiento periódico al plan para confirmar que se están llevando a cabo de manera adecuada y efectiva y disponer de las evidencias que demuestren su implementación.

Con base en la información proporcionada por la primera línea de defensa y los resultados de las auditorías internas y externas realizadas hasta la fecha, se concluye que el riesgo identificado no se ha materializado. La ausencia de incidentes relacionados con la pérdida de integridad de la información, sumada al avance en la implementación de las acciones de mitigación, indica que el riesgo se encuentra bajo control. Sin embargo, es fundamental mantener un enfoque proactivo y realizar un seguimiento continuo del riesgo. Es importante tener en cuenta que la ausencia de incidentes no significa necesariamente que el riesgo haya desaparecido por completo. Los ciberataques evolucionan constantemente y es necesario estar preparados para responder a nuevas amenazas.

Se recomienda que en cada monitoreo se reporte el avance en el período, con el fin de evidenciar el progreso en la implementación de las acciones y su efectividad teniendo en cuenta que las condiciones cambiantes del entorno así lo ameritan.

En el primer y segundo monitoreo, la primera línea de defensa indicó que no se recibieron hallazgos que evidenciaran cualquier clase de materialización del riesgo o falencia en las acciones que actualmente se tienen definidas. Si bien es positivo que hasta el momento no se hayan materializado riesgos significativos, es fundamental que desde el proceso se actué de manera proactiva en la identificación de falencias para su corrección y/o definición de acciones correctivas. Se debe estar preparados para responder de manera efectiva en caso de que ocurran.

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

Al realizar un análisis integral de la gestión de este riesgo, se puede deducir su utilidad para evitar situaciones que afecten el cumplimiento de los objetivos del proceso. La primera línea de defesa en su evaluación de efectividad en la gestión de los riesgos concluye que la efectividad de puede evidenciar en la ausencia de incidentes relacionados con la pérdida de integridad de la información. Esta afirmación se sustenta en el hecho que, si no se han registrado casos de pérdida, alteración o acceso no autorizado a información confidencial, es una clara señal de que las medidas de gestión del riesgo están funcionando. Desde la segunda línea de defensa se identificaron que además ha sido útil para:

* **Cumplimiento de objetivos:** La gestión del riesgo ha permitido cumplir con los objetivos del proceso de contratación, como la transparencia, la eficiencia y la legalidad. Al proteger la integridad de la información, se garantiza que las decisiones se tomen basadas en datos confiables y que el proceso se desarrolle de manera transparente.
* **Mejora continua:** La gestión del riesgo ha impulsado la mejora continua de los procesos, al identificar áreas de oportunidad y establecer acciones correctivas para reducir la exposición a riesgos. Esto se refleja en la implementación de nuevas medidas de seguridad, la actualización de los procedimientos y la capacitación del personal.
* **Satisfacción de las partes interesadas:** La gestión del riesgo ha contribuido a aumentar la satisfacción de las partes interesadas, como los procesos involucrados, los usuarios internos y los entes de control. Al garantizar la seguridad de la información, se fortalece la confianza en el proceso y se minimizan los riesgos de litigios y sanciones.
* **Cumplimiento normativo:** La gestión del riesgo ha permitido cumplir con los requisitos legales y normativos aplicables, como las leyes de protección de datos y las normas de seguridad de la información.

1. ***Actualización de Riesgos****:*

La primera línea de defensa ha informado que no se han identificado cambios en los riesgos existentes. Sin embargo, considerando el contexto de rediseño institucional y la nueva caracterización del proceso, la segunda línea de defensa considera necesario realizar un análisis más detallado para garantizar que la evaluación de riesgos siga siendo precisa y completa. Así mismo, La primera línea de defensa ha indicado que no se ha identificado la necesidad de documentar y gestionar nuevos riesgos. Sin embargo, la segunda línea de defensa debe realizar una evaluación más profunda considerando los cambios en el contexto estratégico y el rediseño institucional.

#### ALERTAS

Se identificó la necesidad de actualizar el contexto con el fin de lograr la armonización con el proceso de rediseño institucional.

#### RECOMENDACIONES

A partir del análisis detallado realizado en los items anteriores, se identificaron diversas oportunidades de mejora en el proceso de contratación de bienes y servicios. El presente numeral presenta un conjunto de recomendaciones estratégicas diseñadas para fortalecer la seguridad de la información, optimizar los procesos y garantizar el cumplimiento de los objetivos institucionales.

* Realizar una revisión exhaustiva de la nueva caracterización del proceso para identificar cualquier cambio en los objetivos, actividades, o interacciones con otros procesos que puedan generar nuevos riesgos o modificar los existentes.
* Evaluar cómo los cambios estratégicos derivados del Decreto 432 de 2022 impactan en el perfil de riesgo del proceso. Es necesario identificar si estos cambios generan nuevas vulnerabilidades o si modifican la probabilidad o el impacto de los riesgos existentes.
* Documentar los controles de manera detallada. Elaborar procedimientos detallados para cada control, incluyendo los responsables, las frecuencias de ejecución y los registros a generar.
* Mantener un registro detallado de las actividades realizadas, incluyendo fechas, responsables y resultados.
* Redefinir los controles que no están bajo el gobierno del proceso
* Establecer indicadores que permitan medir la eficacia de los controles y el cumplimiento de los objetivos.
* Realizar evaluaciones periódicas de los controles para identificar áreas de mejora.
* Establecer un proceso de seguimiento continuo para evaluar la eficacia de los controles y realizar ajustes si es necesario.

### GESTIÓN DEL SERVICIO A LA CIUDADANÍA

#### MAPA DE RIESGOS DE GESTIÓN

**Riesgos de Gestión**

1. No ha construido el mapa de riesgos por ser un proceso nuevo.

#### OBSERVACIONES

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

Dado que el proceso es nuevo, no se ha formalizado el mapa de riesgos de seguridad de la información. Al ser un proceso nuevo, la identificación de posibles cuellos de botella y áreas de mejora es crucial para garantizar su éxito desde el inicio. La falta de un mapa incrementa el riesgo de errores, retrasos y malentendidos que pueden afectar la satisfacción del ciudadano, por el contrario, un mapa del proceso permite diseñar y mejorar los servicios en función de las necesidades de los ciudadanos

Desde la segunda línea de defensa, para la construcción del mapa de riesgos de seguridad, se recomienda Identificar los riesgos más obvios y críticos para el nuevo proceso, como fallas en los sistemas de atención, demoras en la respuesta, o falta de claridad en los procedimientos. Para obtener información relevante es necesario trabajar con todos los colaboradores en el proceso realizando reuniones de trabajo periódicas y si es posible incluir a los ciudadanos, realizar encuestas y entrevistas para conocer sus percepciones sobre los riesgos y sus expectativas.

Dentro de las estrategias que se pueden adoptar está la de estudiar procesos similares en otras entidades para identificar riesgos comunes y buenas prácticas.

1. ***Autoevaluación de la efectividad de los controles****:*

Se recomienda definir indicadores que permitan medir la efectividad de los controles, como el tiempo de respuesta a las solicitudes, la tasa de resolución de problemas a la primera, y el nivel de satisfacción del ciudadano, Analizar los registros de llamadas, correos electrónicos y otros canales de atención para identificar patrones y posibles problemas y verificar si el personal suscrito al proceso cuenta con la capacitación necesaria para identificar y gestionar los riesgos.

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

El proceso debe asegurarse de que las acciones implementadas estén directamente relacionadas con las causas identificadas de los riesgos, de la misma forma debe realizar seguimiento al impacto de las acciones implementadas y ajustarlas según sea necesario.

Dentro de las actividades sugeridas está la de evaluar la satisfacción del ciudadano, para ello puede utilizar encuestas y otros mecanismos para medir la satisfacción del ciudadano con las acciones implementadas.

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

Desde el proceso se requiere estar atentos a las auditorías internas y externas para evaluar la eficacia del sistema de gestión de riesgos, evaluar el cumplimiento con estándares y mejores prácticas en la gestión de servicios al ciudadano. Los resultados de las evaluaciones pueden ser usados para identificar áreas de mejora en la gestión de riesgos.

1. ***Actualización de Riesgos****:*

El proceso debe garantizar la actualización de los riesgos e implementar un proceso regular de revisión, al menos tres veces al año, considerar cambios en el contexto, evaluar cómo los cambios en el entorno legal, tecnológico y social pueden afectar los riesgos.

Para la actualización del mapa de riesgos, se requiere que desde el proceso se Investigue a fondo los incidentes que se puedan presentar y utilizar la información relevante obtenida de las reuniones de trabajo interno, encuestas a los usuarios y auditorías para actualizar entre otros.

#### ALERTAS

Se llama la atención sobre la urgente necesidad de construir un mapa detallado del proceso de Gestión del Servicio a la Ciudadanía. La ausencia de este instrumento fundamental no permite gestionar de manera adecuada los riesgos en existentes en el proceso limitando la capacidad de la organización para identificar los puntos críticos y las posibles fallas que puedan afectar la calidad del servicio y la satisfacción del ciudadano.

#### RECOMENDACIONES

* Involucrar a todos los actores relevantes en la construcción del mapa de riesgos, desde los funcionarios de primera línea hasta el líder del proceso.
* Contar con el apoyo los directivos de los otros procesos, la Dirección de TIC, la Dirección de planeación institucional.
* Fomentar una cultura de mejora continua en la que se incentive a los funcionarios vinculados al proceso para identificar y reportar riesgos.
* Utilizar herramientas tecnológicas para facilitar la gestión de riesgos, como software de gestión de incidentes y el software de Gestión de Calidad - Gestionate para facilitar el registro y análisis de datos.
* Mantener siempre al ciudadano en el centro de la gestión de riesgos, buscando mejorar su experiencia y satisfacción.

### GESTIÓN ADMINISTRATIVA

#### MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN (ADMINISTRACIÓN DE RECURSOS FÍSICOS Y DE SERVICIOS GENERALES)

**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

#### OBSERVACIONES

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

Si bien el objetivo estratégico del proceso sigue vigente, es fundamental considerar los cambios introducidos por la implementación de lo consagrado en la Resolución 432 de 2022 lo cual puede generar nuevos riesgos o modificar la probabilidad e impacto de los riesgos existentes.

Se recomienda realizar un análisis detallado de los cambios introducidos por la resolución y evaluar su impacto en el perfil de riesgo del proceso. Además, es importante monitorear de cerca el entorno externo, incluyendo cambios en la normativa, la tecnología y las amenazas cibernéticas, ya que estos factores pueden influir significativamente en el riesgo.

Es recomendable realizar una evaluación de impacto de los cambios introducidos por la Resolución 432 de 2022, actualizar el mapa de riesgos para reflejar los nuevos riesgos y cambios en la probabilidad e impacto de los riesgos existentes, revisar y actualizar los controles existentes para garantizar que siguen siendo efectivos e implementar nuevos controles para mitigar tanto los nuevos riesgos actualmente identificados y los nuevos que puedan resultar del análisis del contexto.

El riesgo identificado está directamente relacionado con el objetivo estratégico de la SDP “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”. La pérdida de integridad de la información, especialmente aquella relacionada con planes, programas, historias e inventarios, puede comprometer seriamente la capacidad de la entidad para cumplir con sus objetivos y mantener su reputación.

Sin embargo, consideramos que es fundamental profundizar en el análisis del riesgo para garantizar que esté completamente alineado con los objetivos estratégicos. En este sentido, se propone las siguientes recomendaciones:

* Además de la pérdida de integridad, es necesario evaluar otros riesgos asociados a la información, como la confidencialidad y la disponibilidad. La pérdida de confidencialidad, por ejemplo, podría tener graves consecuencias legales y reputacionales.
* Realizar un análisis detallado del tipo asociado al riesgo. El proceso asocia la perdida de integridad al riesgo identificado causado por fuego, agua y fenómenos sísmicos, sin embargo, es claro que en un evento de esta naturaleza se evidencia la perdida de disponibilidad, generando consecuencias indirectas para las operaciones, la reputación y la continuidad del negocio.

Tanto la primera línea como la segunda línea coincidimos en que el riesgo de pérdida de integridad de la información está directamente relacionado con el objetivo del proceso de Administración de Recursos Físicos y de Servicios Generales hoy Gestión Administrativa, que es garantizar la continua operación de la entidad.

Recomendamos realizar un análisis detallado para identificar las consecuencias específicas del riesgo sobre el proceso. Este análisis debe considerar:

* Impacto en la eficiencia: ¿Cómo afectaría la pérdida de información a la eficiencia de los procesos?
* Impacto en la calidad: ¿Cómo afectaría la pérdida de información a la calidad de los servicios prestados?
* Impacto en el cumplimiento: ¿Cómo afectaría la pérdida de información al cumplimiento de las normas y regulaciones aplicables?
* Impacto financiero: ¿Cuáles serían los costos asociados a la pérdida de información?
* Además, es importante evaluar si existen otros riesgos específicos para el proceso que puedan estar relacionados con la pérdida de integridad de la información. Por ejemplo, la pérdida de información sobre la ubicación de equipos críticos podría dificultar las operaciones de emergencia.

Si bien las causas inicialmente identificadas parecen persistir, es crucial realizar una evaluación periódica y exhaustiva para confirmar esta situación. El entorno organizacional es dinámico y sujeto a cambios constantes, lo que puede generar nuevas vulnerabilidades y modificar la relevancia de las causas existentes.

Para garantizar la efectividad de las medidas de mitigación, se recomienda realizar las siguientes acciones:

* Revisar y evaluar si los controles implementados para abordar las causas iniciales del riesgo siguen siendo adecuados y eficaces. Es posible que sea necesario ajustar o reforzar algunos controles.
* Realizar un análisis exhaustivo para identificar nuevas causas potenciales del riesgo que puedan haber surgido debido a cambios en el entorno, la tecnología o los procesos.
* Revisar los incidentes de seguridad que hayan ocurrido durante el período de monitoreo para identificar las causas raíz y determinar si están relacionadas con el riesgo en cuestión.
* Evaluar el nivel de concientización de los empleados sobre los riesgos y los controles implementados. Es posible que sea necesario reforzar los programas de capacitación.

Las consecuencias inicialmente identificadas parecen persistir, es crucial realizar una evaluación periódica y exhaustiva para confirmar esta situación. Se recomienda lo siguiente:

* Evaluar si las consecuencias inicialmente identificadas siguen siendo las más relevantes. Es posible que hayan surgido nuevas consecuencias debido a cambios en el entorno o en los procesos.
* Realizar un análisis detallado del impacto potencial de posibles consecuencias, considerando tanto los aspectos cuantitativos (por ejemplo, costos financieros) como los cualitativos (por ejemplo, impacto reputacional). Por ejemplo:

**Consecuencias Directas:**

* Pérdida de Información Crítica: Esto incluye la pérdida de datos esenciales para la operación diaria de la entidad, como registros financieros, información de proyectos, datos de contacto, etc.
* Disrupción de Procesos: La falta de información precisa y actualizada puede interrumpir los procesos internos y externos de la SDP, generando retrasos y ineficiencias.
* Decisiones Erróneas: La toma de decisiones basada en información incorrecta o incompleta puede llevar a resultados adversos y generar pérdidas económicas.
* Incumplimiento Normativo: La pérdida de información puede dar lugar al incumplimiento de las regulaciones y leyes aplicables, lo que puede resultar en sanciones y multas.

**Consecuencias Indirectas:**

* Pérdida de Confianza: La pérdida de integridad de la información puede erosionar la confianza de los ciudadanos, empleados, socios y otras partes interesadas en la SDP.
* Daño Reputacional: La divulgación de información confidencial o la publicación de datos erróneos puede dañar la reputación de la SDP y afectar su imagen pública.
* Costos Financieros: La recuperación de la información perdida, la investigación de incidentes de seguridad y la implementación de medidas correctivas pueden generar costos significativos.
* Riesgos Legales: La pérdida de información puede exponer a la SDP a riesgos legales, como demandas por daños y perjuicios.

**Consecuencias Específicas para el Proceso de Gestión Administrativa:**

* Dificultades en la Gestión de Inventarios: La pérdida de información sobre los bienes de la entidad puede dificultar el control de los inventarios y generar pérdidas económicas.
* Retrasos en los Pagos: La pérdida de información sobre los proveedores y los contratos puede generar retrasos en los pagos y afectar las relaciones comerciales.
* Problemas en la Gestión de Mantenimiento: La pérdida de información sobre el mantenimiento de los equipos puede acortar su vida útil y aumentar los costos de reparación.
* Incumplimiento de los Contratos: La pérdida de información sobre los términos de los contratos puede generar incumplimientos y disputas legales.
* Simulaciones: Realizar simulaciones o ejercicios de respuesta a incidentes para evaluar la capacidad del proceso para responder a una materialización del riesgo y mitigar sus consecuencias.

La segunda línea de defensa considera que es fundamental mantener una vigilancia constante sobre las consecuencias del riesgo y realizar evaluaciones periódicas para garantizar que se tomen las medidas necesarias para mitigarlas. Es importante recordar que las consecuencias pueden cambiar con el tiempo y que es necesario adaptarse a estos cambios para proteger los intereses de la Entidad.

1. ***Autoevaluación de la efectividad de los controles****:*

La segunda línea identificó que no se publicó las evidencias en el repositorio destinado para tal fin. Se resalta la necesidad de contar con registros que evidencien la implementación efectiva de estos controles. Los registros son esenciales para demostrar el cumplimiento de las políticas de seguridad, identificar posibles brechas y realizar mejoras continuas.

Recomendamos implementar un sistema de registro estructurado para documentar la ejecución de cada control. Estos registros pueden ser manuales o electrónicos y deben incluir información sobre la fecha de ejecución, el responsable, los resultados obtenidos y cualquier desviación identificada.

La segunda línea coincide en que los controles establecidos (mantener actualizada la información para las copias de seguridad, socialización de políticas de seguridad y planes de mantenimiento para garantizar que la ubicación de los equipos es adecuada y que estén protegidos de las condiciones ambientales que los ponga en riesgo (fuego y agua)) están diseñados para prevenir y mitigar el riesgo de pérdida de integridad de la información. Sin embargo, los registros son esenciales para demostrar el cumplimiento de las políticas de seguridad, identificar posibles brechas y realizar mejoras continuas.

Recomendamos lo siguiente:

* Identificar los tipos de registros necesarios para cada control, por ejemplo:
* Copias de Seguridad: Identificar los activos de información y solicitar a la Dirección de TIC copias de seguridad, incluyendo datos como la fecha, la hora, el contenido de la copia y cualquier dato identificador.
* Políticas de Seguridad: Registros de asistencia a capacitaciones y reportes de incidentes de seguridad.
* Mantenimiento Preventivo: Órdenes de trabajo, reportes de inspección y registros de mantenimiento.
* Definir las frecuencias con las cuales se revisarán y actualizarán los registros.
* Realizar revisiones periódicas para verificar la exactitud y la integridad de los registros
* Asegurar que los controles se estén aplicando de acuerdo con los procedimientos establecidos.

La segunda línea de defensa enfatiza la importancia de los registros para garantizar la efectividad de los controles y la seguridad de la información para fortalecer la postura de seguridad y cumplir con los requisitos legales y regulatorios aplicables.

Desde la segunda línea de defensa confirmamos que, según la información proporcionada por la primera línea de defensa, no se han registrado hallazgos de auditoría asociados a los controles evaluados. Esto es una señal positiva y sugiere que las medidas implementadas están contribuyendo a garantizar la integridad de la información.

Sin embargo, es importante mantener una actitud proactiva y continuar monitoreando la efectividad de los controles. A pesar de que no se hayan identificado hallazgos en el pasado, siempre existe la posibilidad de que nuevos riesgos o vulnerabilidades surjan en el futuro.

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

En el primer monitoreo, tanto la primera como la segunda línea de defensa identificaron la ausencia de acciones concretas para mitigar el riesgo de pérdida de integridad de la información debido a eventos como incendios, inundaciones y sismos. La segunda línea enfatizó la importancia de definir estas acciones, especialmente considerando que el tratamiento seleccionado fue "Reducir" (mitigar).

En el segundo monitoreo, la primera línea nuevamente indicó que no se han formulado acciones específicas para estos riesgos. Persisten las deficiencias en la definición y ejecución de acciones para mitigar el riesgo de pérdida de integridad de la información. A pesar de haber identificado este riesgo como crítico y de haber seleccionado el tratamiento de "Reducir", el proceso aún no ha implementado las medidas necesarias para contrarrestar sus causas. Es necesario evaluar el tratamiento o definir el plan de acción.

La ausencia de acciones concretas pone en riesgo la integridad de la información y expone a la organización a consecuencias significativas. Es fundamental que el proceso defina y ejecute un plan de acción detallado si consideró si formulación.

En el primer como en el segundo monitoreo, tanto la primera como la segunda línea de defensa han coincidido en que no se han formulado acciones específicas para mitigar el riesgo de pérdida de integridad de la información debido a eventos como incendios, inundaciones y sismos.

Reiteramos que la ausencia de acciones formuladas impide evaluar su implementación. No es posible evaluar la efectividad de algo que no existe. Sin embargo, el proceso debe evaluar y responder la pregunta ¿el tratamiento al riesgo es mitigar o aceptar?

La falta de un plan de acción concreto y su correspondiente implementación representa una brecha significativa en la gestión de riesgos de la entidad. Esta situación expone a la SDP a consecuencias adversas, como la pérdida de información crítica, interrupción de operaciones y daños a la reputación. Es fundamental que se tomen medidas inmediatas para corregir esta situación. Se recomienda lo siguiente:

* Priorizar la formulación de un plan de acción detallado: Se debe elaborar un plan que incluya acciones específicas, responsables, plazos y recursos necesarios para mitigar el riesgo identificado.
* Incluir a todos los actores relevantes: Es importante involucrar a todas las áreas de la organización que puedan verse afectadas por el riesgo, así como a expertos externos si es necesario.
* Asignar recursos adecuados: Se deben asignar los recursos necesarios para implementar el plan de acción, incluyendo presupuesto, personal y tiempo.
* Monitorear y evaluar la implementación: Se debe establecer un mecanismo para monitorear el progreso de la implementación del plan de acción y evaluar su efectividad.

La ausencia de un plan de acción no solo impide la implementación adecuada de las medidas de mitigación, sino que también dificulta la evaluación de la eficacia de la gestión de riesgos en general.

Según la información proporcionada y los resultados de la auditoría interna realizada en agosto de 2023, no se ha evidenciado la materialización del riesgo evaluado. Esto indica que los controles hasta el momento están funcionando de manera efectiva para prevenir o mitigar las consecuencias del riesgo. Sin embargo, es importante mantener una vigilancia constante y realizar evaluaciones periódicas. La ausencia de materialización del riesgo en un período determinado no garantiza que el riesgo no se materialice en el futuro. Las condiciones internas y externas pueden cambiar, generando nuevas vulnerabilidades.

Dado que el riesgo evaluado no se ha materializado, no se han formulado acciones correctivas específicas como resultado de este evento. Sin embargo, es importante reiterar que la ausencia de materialización del riesgo no debe interpretarse como una señal de que el riesgo ha desaparecido.

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

Con base en la evidencia disponible, podemos concluir que la gestión del riesgo de pérdida de integridad de la información ha sido efectiva en prevenir situaciones que podrían haber afectado el cumplimiento de los objetivos y compromisos del proceso.

Los controles implementados, mantener actualizada la información para las copias de seguridad, socialización de políticas de seguridad y planes de mantenimiento para garantizar que la ubicación de los equipos es adecuada y que estén protegidos de las condiciones ambientales que los ponga en riesgo (fuego y agua), han demostrado ser eficaces en la protección de la información crítica. Además, la alineación del proceso con el ODS 16 (Paz, justicia e instituciones sólidas) refuerza la importancia de garantizar la integridad de la información para mantener la confianza del público y el cumplimiento de las obligaciones institucionales.

1. ***Actualización de Riesgos****:*

La información disponible hasta el momento y considerando los resultados de las evaluaciones anteriores, se evidencia una necesidad inmediata de modificar o actualizar significativamente la evaluación del riesgo. Los controles implementados continúan siendo efectivos en la mitigación del riesgo identificado. Sin embargo, es fundamental mantener una vigilancia constante y realizar evaluaciones periódicas. El entorno institucional y los cambios constantes derivados del proceso de rediseño institucional que pueden introducir nuevos riesgos o modificar la naturaleza de los riesgos existentes.

Se recomienda realizar un análisis más profundo considerando los siguientes aspectos:

* Cambios en el contexto estratégico: Evaluar si los cambios en la estrategia de la entidad han introducido nuevos riesgos o modificado la importancia de los riesgos existentes.
* Avances tecnológicos: Analizar cómo los avances tecnológicos pueden afectar la vulnerabilidad del sistema y la eficacia de los controles actuales.
* Cambios en el entorno regulatorio: Identificar si existen nuevas regulaciones o cambios en las existentes que puedan impactar el perfil de riesgo.

Dada la dinámica del entorno institucional y el proceso de implementación de la nueva estructura, procesos, sistemas y cultura, producto del rediseño de la entidad, es indispensable documentar y gestionar nuevos riesgos.

El proceso de rediseño institucional introduce nuevas variables y desafíos que pueden generar riesgos desconocidos hasta ahora. Es fundamental identificar y documentar estos nuevos riesgos para poder gestionarlos de manera proactiva, así mismo, estos cambios organizacionales pueden exponer a la institución a nuevas vulnerabilidades, como, por ejemplo, en los sistemas de información, procesos internos o relaciones con terceros.

La identificación y gestión de nuevos riesgos es un componente clave de la mejora continua. Al documentar y gestionar los riesgos de manera sistemática, la entidad puede identificar oportunidades para optimizar sus procesos y mejorar su desempeño.

#### ALERTAS

Se detectan deficiencias en la implementación o el funcionamiento de los controles internos establecidos, lo que puede aumentar la exposición a riesgos. Esta situación se evidencia en la falta de formulación de planes de acción dada que la decisión tomada desde el proceso para el tratamiento del riesgo fue mitigarlo o reducirlo

Se detecta la necesidad de actualizar el mapa de riesgos con ocasión del proceso de rediseño institucional con el fin de preservar los pilares propios de la seguridad de la información.

#### RECOMENDACIONES

Desde la segunda línea de defensa se recomienda:

* Es fundamental evaluar la eficacia de los controles existentes para mitigar el riesgo de pérdida de integridad de la información. Se recomienda realizar un mapeo de controles y un análisis de brechas para identificar áreas de mejora.
* Se debe considerar el marco legal aplicable en materia de protección de datos y seguridad de la información, a fin de garantizar el cumplimiento normativo.
* Es necesario garantizar la participación en los programas de capacitación y sensibilización para concientizar a los involucrados en el proceso sobre la importancia de proteger la información y los riesgos asociados a su pérdida.
* Implementar controles de acceso más estrictos para limitar el acceso a la información a aquellos usuarios autorizados.
* Establecer un plan de copias de seguridad regular y garantizar la integridad de las copias de seguridad. Coordinar con la Dirección de TIC la ejecución del plan que se formule.
* Asegurar la asistencia del personal involucrado en el proceso en las capacitaciones sobre los riesgos asociados a la pérdida de información y las medidas de seguridad que deben adoptar.

#### MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN (GESTIÓN DOCUMENTAL)

**Riesgos 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.

#### OBSERVACIONES

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

La respuesta dada desde el proceso en los monitoreos anteriores y la de segunda línea de Defensa, ofrecen un análisis detallado y constructivo del informe de riesgos presentado para el proceso de gestión documental. Se destaca la solidez del trabajo realizado, reconociendo el análisis exhaustivo de riesgos, la alineación con objetivos estratégicos y la implementación de controles. Sin embargo, se sugiere revisar el contexto del proceso a la luz de la nueva caracterización formulada y aprobada recientemente con el objeto de identificar cambios en el contexto actual que ameriten su actualización, mejora o cambios sustanciales que lo modifiquen.

En el segundo monitoreo del mapa de riesgos, la primera línea ha confirmado que los riesgos identificados siguen siendo relevantes para el objetivo estratégico. Como segunda línea de defensa, reafirmamos esta evaluación y destacamos que la materialización de cualquiera de estos riesgos tendría un impacto directo en la capacidad de la institución para fortalecer su estructura y cultura institucional, y para brindar una gestión pública efectiva.

En particular, la pérdida de información ya sea por causas naturales, humanas o tecnológicas, socavaría la capacidad de la institución para tomar decisiones informadas, rendir cuentas a la ciudadanía y cumplir con sus obligaciones legales. Además, la interrupción de los procesos de gestión documental afectaría la eficiencia y la eficacia de la organización, generando retrasos y frustración en los ciudadanos.

Por lo tanto, es fundamental mantener una vigilancia constante sobre estos riesgos y seguir implementando las medidas de control necesarias para proteger los activos de información de la institución.

Una vez analizados cada uno de los riesgos identificados en el proceso se obtuvo el siguiente resultado:

**Riesgo 1. Pérdida de disponibilidad por destrucción de la información**

*Relación con el Objetivo Estratégico:* La pérdida de información impide la toma de decisiones informadas y basadas en evidencia, debilitando la capacidad de gestión pública efectiva.

*Consecuencias Críticas:* Pérdida de conocimiento institucional, incumplimiento normativo, reputación dañada, incapacidad para demostrar cumplimiento.

*Activos Críticos:* Documentación física y digital, sistemas de almacenamiento

Controles Relevantes: Políticas de seguridad, respaldos, capacitación, planes de continuidad del negocio.

**Riesgo 2. Pérdida de disponibilidad por mal funcionamiento del software**

*Relación con el Objetivo Estratégico:* Un sistema de gestión documental inoperativo afecta la eficiencia de los procesos y la capacidad de respuesta de la institución.

*Consecuencias Críticas:* Retrasos en la atención a ciudadanos, pérdida de productividad, aumento de costos.

*Activos Críticos:* Software de gestión documental, infraestructura tecnológica

Controles Relevantes: Mantenimiento preventivo, planes de contingencia, actualización de software.

**Riesgo 3. Pérdida de disponibilidad por mal funcionamiento del software que afecta la información almacenada en SGDEA o en el módulo de preservación digital**

*Relación con el Objetivo Estratégico:* La pérdida de datos en el sistema de gestión documental impide el seguimiento de trámites y la generación de reportes, afectando la transparencia y la rendición de cuentas.

*Consecuencias Críticas:* Pérdida de trazabilidad, dificultades en auditorías, incumplimiento de normas.

*Activos Críticos:* Base de datos del sistema de gestión documental

Controles Relevantes: Copias de seguridad, pruebas de restauración, control de acceso.

**Riesgo 4. Pérdida de disponibilidad por mal funcionamiento del equipo de cómputo o servidores**

*Relación con el Objetivo Estratégico:* La falta de disponibilidad de los sistemas informáticos afecta la continuidad de los procesos y la prestación de servicios.

*Consecuencias Críticas:* Interrupción de servicios, pérdida de productividad, insatisfacción ciudadana.

*Activos Críticos:* Servidores, equipos de cómputo, redes

Controles Relevantes: Mantenimiento preventivo, redundancia de equipos, planes de contingencia.

**Riesgo 5. Pérdida de disponibilidad por fenómenos climáticos, fuego, agua o fenómenos sísmicos**

*Relación con el Objetivo Estratégico:* La pérdida física de documentos compromete la memoria institucional y la capacidad de demostrar cumplimiento.

*Consecuencias Críticas:* Pérdida de evidencia, dificultades en la reconstrucción de procesos, multas.

*Activos Críticos:* Documentos físicos, instalaciones de almacenamiento

Controles Relevantes: Sistemas de detección temprana, planes de emergencia, seguros.

**Riesgo 6. Pérdida de disponibilidad por fallas humanas**

*Relación con el Objetivo Estratégico:* Errores humanos pueden generar pérdida de información o acceso no autorizado, afectando la integridad y confidencialidad de los datos.

*Consecuencias Críticas:* Pérdida de información sensible, filtraciones de datos, sanciones legales.

Activos Críticos: Procedimientos, políticas, personal capacitado

*Controles Relevantes:* Capacitación continua, controles de acceso, supervisión.

Se recomienda que el proceso analice con mayor profundidad las relaciones existentes entre los riesgos identificados y el objeto estratégico que apalanca. Así mismo, para el próximo monitoreo hacer una descripción clara de cómo desde su óptica hay una coherencia entre el objetivo estratégico y los riesgos identificados.

Desde la segunda línea de defensa, se ha evaluado la alineación de los riesgos identificados en el proceso Gestión Documental con el objetivo estratégico de preservar el patrimonio documental de la SDP. A continuación, presento un análisis detallado de cada riesgo y su relación con el objetivo estratégico:

**Riesgo 1: Pérdida de disponibilidad por destrucción de la información**

Este riesgo está directamente relacionado con el objetivo estratégico, ya que la destrucción de información implica una pérdida irrecuperable del patrimonio documental. La pérdida de información puede afectar la capacidad de la organización para cumplir con sus funciones, tomar decisiones informadas y cumplir con las obligaciones legales.

**Riesgo 2: Pérdida de disponibilidad por mal funcionamiento del software**

Este riesgo compromete la preservación digital de la información, un componente fundamental del objetivo estratégico. La inaccesibilidad a la información digitalizada dificulta su conservación y uso a largo plazo. La pérdida de acceso a la información digital puede limitar la capacidad de consulta y análisis de los datos, afectando la toma de decisiones y la investigación.

**Riesgo 3: Pérdida de disponibilidad por mal funcionamiento del software que afecta la información almacenada en SGDEA o en el módulo de preservación digital**

Este riesgo se centra en la integridad de los sistemas de información utilizados para la gestión y preservación documental. Un mal funcionamiento de estos sistemas puede comprometer la disponibilidad y accesibilidad de la información, afectando directamente el objetivo estratégico. La pérdida de datos en estos sistemas puede tener consecuencias graves para la organización, incluyendo la pérdida de conocimiento institucional y la incapacidad para cumplir con las obligaciones legales.

**Riesgo 4: Pérdida de disponibilidad por mal funcionamiento del equipo de cómputo o servidores**

Este riesgo está directamente relacionado con la infraestructura tecnológica necesaria para la preservación digital. Fallas en el hardware pueden comprometer la integridad de los datos y dificultar el acceso a la información. La pérdida de datos debido a fallas en el hardware puede tener un impacto significativo en la continuidad de las operaciones y en la capacidad de la organización para cumplir con sus objetivos.

**Riesgo 5: Pérdida de disponibilidad por fenómenos climáticos, fuego, agua o fenómenos sísmicos**

Este riesgo amenaza la integridad física de los documentos y los sistemas de almacenamiento, poniendo en peligro la preservación del patrimonio documental. La pérdida de documentos físicos o digitales debido a desastres naturales puede tener consecuencias irreversibles para la organización.

**Riesgo 6: Pérdida de disponibilidad por fallas humanas**

El error humano puede comprometer la seguridad de la información y la integridad de los procesos de gestión documental, afectando directamente el objetivo de preservar el patrimonio documental. La pérdida de información debido a errores humanos puede tener consecuencias graves para la organización, incluyendo la pérdida de confianza y la exposición a riesgos legales.

En conclusión, todos los riesgos identificados presentan una amenaza directa al objetivo estratégico de preservar el patrimonio documental de la SDP. Es fundamental implementar las medidas de control y mitigación establecidas para minimizar el impacto de estos riesgos y garantizar la protección de la información institucional.

La respuesta de la primera línea de defensa infiere que es probable que las causas iniciales de los riesgos persistan, especialmente aquellas relacionadas con factores intrínsecos del proceso, como la falta de capacitación del personal o la obsolescencia tecnológica, sin embargo, se debe observar que es posible que hayan surgido nuevas causas debido a cambios en el entorno institucional. Por ejemplo, nuevas caracterizaciones de los procesos, cambios en las funciones derivadas del rediseño institucional que pueden introducir nuevos riesgos o evidenciar la necesidad de cambiarlos, modificarlos, eliminarlos o trasladarlos.

Es importante anotar que la efectividad de los controles implementados para mitigar los riesgos influirá en la persistencia de las causas iniciales. Si los controles no son efectivos, las causas persistirán y los riesgos seguirán siendo relevantes.

Bajo la hipótesis que los riesgos siguen siendo los mismos y que las causas no han variado, se presenta a continuación el análisis realizado para la lectura del mismo y de modo ilustrativo para que el proceso pueda tener elementos para decidir sobre la relevancia de los riesgos y sus causas.

**Riesgo 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.**

*Causas:* La falta de capacitación, copias de seguridad inadecuadas y la ausencia de políticas claras siguen siendo causas probables.

*Monitoreo:* Verificar si se han implementado las capacitaciones previstas y si los procedimientos de respaldo se cumplen.

**Riesgo 2: 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.**

*Causas:* La obsolescencia de software (ausencia de la gestión en el versionamiento de los sistemas de información), la falta de actualizaciones y la configuración incorrecta (software nuevo o inmaduro o la ausencia de mecanismos de identificación y autenticación en los sistemas de información) pueden persistir.

*Monitoreo:* Revisar los registros de mantenimiento y actualizaciones de software, así como los reportes de incidentes.

**Riesgo 3: Pérdida de disponibilidad por mal funcionamiento del software que afecta la información almacenada en SGDEA o en el módulo de preservación digital.**

*Causas:* La falta de control de cambios (ausencia de la gestión en el versionamiento de los sistemas de información, ausencia de control de cambios en sistemas de información), software nuevo o inmaduro, gestión deficiente de las contraseñas - Contraseñas sin protección, falsificación de derechos de acceso debido a la Ausencia de mecanismo de identificación y autenticación en los sistemas de información, uso o abuso de derechos y privilegios, configuración incorrecta y los errores humanos siguen siendo factores de riesgo.

*Monitoreo:* Revisar los registros de cambios en el sistema, los reportes de errores y las estadísticas de uso, los accesos y permisos sobre los sistemas de información.

**Riesgo 4: Pérdida de disponibilidad por mal funcionamiento del equipo de cómputo o servidores que almacenan la información a preservar digitalmente.**

*Causas:* La obsolescencia del hardware, la falta de mantenimiento preventivo, uso no autorizado del equipo, abuso de derechos y privilegios, gestión deficiente de las contraseñas - Contraseñas sin protección, falsificación de derechos de acceso debido a la Ausencia de mecanismo de identificación y autenticación en los sistemas de información, Hardware sin protección o protocolos de seguridad.

*Monitoreo:* Revisar los registros de mantenimiento, los informes de fallas, los indicadores de desempeño de los equipos, los roles y permisos asignados a los colaboradores del proceso, los accesos autorizados a los equipos, la gestión de contraseñas.

**Riesgo 5: Pérdida de disponibilidad del 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.**

*Causas:* La ubicación geográfica (ubicación en un área susceptible de inundación), la infraestructura física y la falta de planes de emergencia, ausencia de mecanismos de dispersión de humo y fuego, uso inadecuado de los controles de acceso físico a las edificaciones y áreas seguras, ausencia de protección física de la edificación, puertas y ventanas. pueden seguir siendo factores de riesgo.

*Monitoreo:* Verificar el cumplimiento de los planes de emergencia, los sistemas de detección y alarma, y el estado de las instalaciones.

**Riesgo 6: Pérdida de disponibilidad por fallas humanas de personas responsables de la producción, gestión, almacenamiento y custodia de la información a preservar digitalmente.**

*Causas:* La falta de capacitación, la rotación de personal y la falta de conciencia sobre la seguridad de la información pueden persistir.

*Monitoreo:* Evaluar los resultados de las capacitaciones, los incidentes de seguridad y las encuestas de satisfacción.

En el segundo monitoreo del mapa de riesgos, hemos evaluado la persistencia de las consecuencias inicialmente identificadas para cada riesgo. Nuestras conclusiones indican que, en general, las consecuencias identificadas siguen siendo relevantes y pertinentes. Sin embargo, hemos observado algunas variaciones y matices que es importante destacar.

**Análisis por Riesgo**

* Riesgo 1: Pérdida de disponibilidad por destrucción de la información

Las consecuencias iniciales de pérdida de conocimiento institucional, incumplimiento normativo y daño a la reputación siguen siendo válidas. Además, se ha identificado un riesgo adicional de litigios legales en caso de pérdida de información sensible.

* Riesgo 2: Pérdida de disponibilidad por mal funcionamiento del software

Las consecuencias iniciales de retrasos en la atención a ciudadanos y pérdida de productividad se mantienen. Adicionalmente, se ha observado que la pérdida de datos puede generar costos adicionales asociados a la recuperación de la información.

* Riesgo 3: Pérdida de disponibilidad por mal funcionamiento del software que afecta la información almacenada en SGDEA.

Las consecuencias iniciales de pérdida de trazabilidad y dificultades en auditorías siguen siendo válidas. Además, se ha identificado un riesgo de sanciones por parte de entes de control en caso de incumplimiento normativo.

* Riesgo 4: Pérdida de disponibilidad por mal funcionamiento del equipo de cómputo o servidores

Las consecuencias iniciales de interrupción de servicios y pérdida de productividad se mantienen. Adicionalmente, se ha identificado un riesgo de ciberataques que podrían aprovechar las vulnerabilidades expuestas por fallas en el hardware.

* Riesgo 5: Pérdida de disponibilidad por fenómenos climáticos, fuego, agua o fenómenos sísmicos

Las consecuencias iniciales de pérdida de evidencia y dificultades en la reconstrucción de procesos siguen siendo válidas. Además, se ha identificado un riesgo de interrupción prolongada de las operaciones en caso de un desastre natural.

* Riesgo 6: Pérdida de disponibilidad por fallas humanas

Las consecuencias iniciales de pérdida de información sensible y filtraciones de datos siguen siendo válidas. Adicionalmente, se ha observado que los errores humanos pueden generar costos adicionales asociados a la investigación y remediación de incidentes.

En general, las consecuencias identificadas inicialmente para cada riesgo siguen siendo relevantes y representan amenazas significativas para la entidad. Sin embargo, es importante destacar que el contexto de riesgo es dinámico y que pueden surgir nuevas consecuencias a medida que cambian las condiciones internas y externas. Se recomienda realizar un monitoreo continuo de los riesgos y sus consecuencias para detectar cambios a tiempo.

Se sugiere realizar la actualización del mapa de riesgos para reflejar los cambios que surjan con base en el rediseño institucional y/o la nueva caracterización del proceso. De igual forma, es recomendable realizar una revisión en la formulación de los riesgos, reforzar los controles existentes e implementar nuevos controles para mitigar los riesgos identificados.

En resumen, las consecuencias iniciales de los riesgos siguen siendo relevantes y deben ser consideradas en la gestión de riesgos de la entidad a través de la gestión que adelanta el proceso.

1. ***Autoevaluación de la efectividad de los controles****:*

En el segundo monitoreo del mapa de riesgos, hemos evaluado la evidencia de la utilización de los controles establecidos para mitigar cada riesgo. Si bien se ha identificado la existencia de algunos registros que evidencian la implementación de ciertos controles, es necesario fortalecer la recopilación y presentación de esta información para garantizar la transparencia y la trazabilidad de las acciones realizadas.

A continuación, se presenta un análisis detallado de cada riesgo y los controles asociados, incluyendo las evidencias encontradas y las recomendaciones para mejorar la verificación de la efectividad de los controles.

**Análisis por Riesgo**

**Riesgo 1: Pérdida de disponibilidad por destrucción de la información**

*Evidencia:* Se han encontrado registros de capacitaciones sobre políticas de seguridad y algunos procedimientos de respaldo.

*Recomendaciones:* Realizar la descripción detallada de los controles aplicados a cada riesgo y mantener los registros con sus evidencias que soportan el uso de los controles, por ejemplo: En las capacitaciones podrían incluir evaluaciones de conocimientos y asistencia. Verificar la frecuencia y el alcance de las copias de seguridad.

**Riesgo 2: Pérdida de disponibilidad por mal funcionamiento del software**

*Evidencia:* No se encontró evidencia sobre registros de mantenimiento preventivo de los sistemas.

*Recomendaciones:* Revisar si existe registros de actualizaciones de software, resultados de pruebas de desempeño y reportes de incidentes o describir detalladamente el cómo los controles están siendo aplicados. Es necesario soportar con evidencias el cumplimiento de todos los controles.

**Riesgo 3: Pérdida de disponibilidad por mal funcionamiento del software que afecta la información almacenada en SGDEA.**

*Evidencia:* No se han encontrado registros de cambios en el sistema.

*Recomendaciones:* Mantener los registros de autorización de cambios, resultados de pruebas, análisis de impacto o las evidencia que el proceso gestione y que soporten la ejecución de los controles y acciones desarrolladas para el tratamiento del riesgo.

**Riesgo 4: Pérdida de disponibilidad por mal funcionamiento del equipo de cómputo o servidores**

*Evidencia:* No se encontró evidencia relacionada con registros de mantenimiento preventivo de los equipos o los mecanismos que ha dispuesto el proceso para la implementación y puesta en marcha de los controles establecidos.

*Recomendaciones:* Documentar y describir en las respuestas a los monitoreos de primera línea el uso de los controles definidos. Se pueden detallar registros de inventario de equipos, contratos de mantenimiento y resultados de las pruebas de desempeño.

**Riesgo 5: Pérdida de disponibilidad por fenómenos climáticos, fuego, agua o fenómenos sísmicos**

*Evidencia:* No se encontró evidencias sobre la aplicación de los controles definidos por el proceso para mitigar el riesgo. Dado lo crucial del riesgo, se recomienda elaborar y realizar planes de contingencia.

*Recomendaciones:* Documentar los registros que soporten el tratamiento del riesgo. Dentro de los posibles registros pueden existir el mantenimiento de sistemas de detección y alarma, así como de las evaluaciones de vulnerabilidad.

**Riesgo 6: Pérdida de disponibilidad por fallas humanas**

*Evidencia:* Se identificó registros de capacitaciones en seguridad de la información.

*Recomendaciones:* Mantener un registro de incidentes de seguridad y análisis de las causas raíz.

Resumiendo lo anterior, si bien se han identificado algunas evidencias de la implementación de los controles, es necesario fortalecer la recopilación y presentación de esta información para garantizar la transparencia y la trazabilidad de las acciones realizadas. Además, se recomienda establecer un sistema de seguimiento y evaluación continuo para asegurar la efectividad de los controles y la mejora continua del sistema de gestión de riesgos.

Es importante revisar los hallazgos de auditoría relacionados con los controles para identificar oportunidades de mejora. En este caso, el líder del proceso ha indicado que no existen hallazgos de auditoría asociados a los controles. No obstante, de acuerdo al contexto del proceso se evidencia que en la auditoría externa 2024 - ICONTEC . SIPA: 3-2023-37838 existe una oportunidad de mejora: “OM: Riesgos: es conveniente verificar si los controles adoptados son de tipo preventivo; esto es importante ya que la sobrevaloración de controles preventivos en lugar de detectivos podrían conducir a una valoración del riesgo residual que no corresponde al nivel de protección de la entidad". Se debe analizar en detalle estos hallazgos para determinar las acciones correctivas o preventivas que se deben implementar.

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

De acuerdo con el análisis en el seguimiento de Segunda Línea de Defensa, la gestión documental es un proceso crítico para la Secretaría Distrital de Planeación. Sin embargo, este proceso se enfrenta a una serie de riesgos que pueden comprometer la integridad y disponibilidad de la información. En detalle los riesgos identificados en el proceso GESTIÓN DOCUMENTAL, los controles implementados para mitigar y las acciones propuestas para fortalecer la gestión de riesgos se presenta a continuación.

A pesar de identificar riesgos significativos, varios de ellos no cuentan con planes de acción detallados. Esto impide evaluar la efectividad de las medidas de mitigación y dificulta la toma de decisiones informadas. Si bien, se mencionan acciones, no se presentan evidencias concretas de su implementación o resultados. Es fundamental contar con registros que demuestren que los controles se están llevando a cabo de manera efectiva.

Los controles se centran principalmente en medidas preventivas, lo cual es positivo. Sin embargo, es importante evaluar la necesidad de complementar estas medidas con controles detectivos y correctivos para identificar y responder a incidentes de manera oportuna.

En el mapa final solo se formuló un plan de acción para el Riesgo 1: Posibilidad de pérdida de disponibilidad por destrucción de la información. Por esta razón, solo se analizó las acciones definidas para el riesgo 1, así:

Causas Identificadas:

* Copias insuficientes
* Información sensible sin cifrado
* Ausencia de copias de respaldo

Acciones Propuestas:

*Acción 1:* Revisar la Política de uso de medios removibles A-LE-320

Relación con la Causa: Esta acción aborda la causa de "copias insuficientes" al establecer lineamientos claros sobre la gestión de copias de seguridad y la frecuencia con la que deben realizarse.

*Acción 2:* Implementar medidas de cifrado para la información sensible

Relación con la Causa: Esta acción aborda la causa de "información sensible sin cifrado" al proteger la información confidencial en caso de pérdida o acceso no autorizado.

Se recomienda elaborar Planes de Acción detallados para los riesgos que se ubican en una Zona de Riesgo Final diferente a baja y aquellos en que el impacto es moderado, alto, catastrófico y definir claramente el alcance de cada acción, incluyendo los responsables, plazos, recursos necesarios y métricas de seguimiento y Definir una frecuencia adecuada para el seguimiento de los planes de acción, considerando la criticidad de cada riesgo.

Se solicita al proceso evidencias de la implementación de los controles, como registros de capacitación, informes de auditoría, resultados de pruebas, etc. y analizar los datos recopilados para identificar tendencias y patrones que puedan indicar áreas de mejora.

De acuerdo con lo anterior, en la evaluación del proceso GESTIÓN DOCUMENTAL, se identificó varios riesgos potenciales, sin embargo, solo para el primer riesgo se formuló un plan de acción que involucra la actualización de las políticas A-LE-320 y A-LE-474, relacionadas con las políticas para el uso de medios removibles y la gestión de activos de información. Estas políticas se encuentran actualizadas hasta el 31 de diciembre de 2023. Ambas serán revisadas durante el segundo y tercer trimestre del año 2024, con la participación de las áreas involucradas. Además, se informa que se cumplió con el cronograma de capacitaciones establecido para el período comprendido entre el 11 de junio y el 16 de julio de 2024.

Teniendo en cuenta que no se ha materializado ninguno de los riesgos, No se ha formulado acciones correcciones y/o acciones correctivas necesarias para darle tratamiento.

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

Desde el proceso se respondió que "la gestión realizada ha sido útil para evitar los riesgos", consecuente con la relevancia de este proceso, desde la segunda línea de Defensa se realizó el análisis por cada riesgo identificando la utilidad de la gestión de riesgos:

**Primer riesgo: Posibilidad de pérdida de disponibilidad por destrucción de la información**

La gestión de este riesgo ha sido útil para evitar situaciones que puedan afectar el cumplimiento de los objetivos y compromisos, ya que se han implementado medidas para proteger la información contra la destrucción accidental o intencional. La evidencia disponible, como la capacitación del personal y la implementación de políticas, indica que la gestión del riesgo ha sido efectiva.

**Segundo riesgo: Posibilidad de pérdida de disponibilidad por mal funcionamiento del software**

La gestión de este riesgo ha sido útil para prevenir situaciones que puedan afectar el cumplimiento de los objetivos y compromisos, ya que se han implementado medidas para garantizar el correcto funcionamiento del software. La evidencia disponible, como la definición de políticas, la implementación de procedimientos y la ausencia de incidentes graves, indica que la gestión del riesgo ha sido efectiva.

**Tercer riesgo: Posibilidad de pérdida de disponibilidad por mal funcionamiento del software que afecte la información almacenada en SGDEA o en el módulo de preservación digital**

La gestión de este riesgo ha sido útil para prevenir situaciones que puedan afectar el cumplimiento de los objetivos y compromisos, ya que se han implementado medidas para proteger la información almacenada en SGDEA y en el módulo de preservación digital contra el mal funcionamiento del software. La evidencia disponible, como la definición de políticas, la implementación de procedimientos y la ausencia de incidentes graves, indica que la gestión del riesgo ha sido efectiva.

**Cuarto riesgo: Posibilidad de pérdida de disponibilidad por mal funcionamiento del equipo de cómputo o servidores que almacenan la información a preservar digitalmente**

La gestión de este riesgo ha sido útil para prevenir situaciones que puedan afectar el cumplimiento de los objetivos y compromisos, ya que se han implementado medidas para garantizar el correcto funcionamiento del equipo de cómputo y servidores que almacenan la información a preservar digitalmente. Sin embargo, la falta de un plan de acción específico para este riesgo limita la evaluación de su efectividad a largo plazo. Se recomienda al líder del proceso definir un plan de acción que incluya acciones concretas para mitigar el riesgo.

**Quinto riesgo: Posibilidad de pérdida de disponibilidad por fenómenos climáticos, fuego, agua o fenómenos sísmicos**

La gestión de este riesgo ha sido útil para prevenir situaciones que puedan afectar el cumplimiento de los objetivos y compromisos, ya que se han implementado medidas para proteger la información almacenada contra fenómenos climáticos, fuego, agua o fenómenos sísmicos. La evidencia disponible, como la definición de políticas, la implementación de procedimientos y la ausencia de incidentes graves, indica que la gestión del riesgo ha sido efectiva. Sin embargo, la falta de un plan de acción específico para este riesgo limita la evaluación de su efectividad a largo plazo. Se recomienda al líder del proceso definir un plan de acción que incluya acciones concretas para mitigar el riesgo, como la implementación de un plan de recuperación de desastres.

**Sexto riesgo: Posibilidad de pérdida de disponibilidad por fallas humanas**

La gestión de este riesgo ha sido útil para prevenir situaciones que puedan afectar el cumplimiento de los objetivos y compromisos, ya que se han implementado medidas para capacitar y sensibilizar al personal sobre la importancia de la seguridad de la información y las buenas prácticas para la preservación digital. La evidencia disponible, como la capacitación del personal, la implementación de campañas de sensibilización y la ausencia de incidentes graves, indica que la gestión del riesgo ha sido efectiva. Sin embargo, es importante continuar con las actividades de capacitación y sensibilización para mantener un alto nivel de conciencia sobre el riesgo.

Se ha evidenciado que la implementación de políticas, procedimientos y capacitaciones ha contribuido a proteger la información y los sistemas. Sin embargo, se han identificado algunas áreas de mejora, particularmente en lo que respecta a la necesidad de planes de acción más detallados para los riesgos asociados a desastres naturales y fallas en el equipo de cómputo.

Del análisis anterior se puede deducir que, aunque la gestión de riesgos ha sido positiva, se recomienda al líder del proceso fortalecer aún más la mitigación de riesgos mediante la definición de planes de acción más específicos y la continuidad de las actividades de capacitación y sensibilización del personal

1. ***Actualización de Riesgos****:*

Las respuestas proporcionadas por la primera línea de defensa evidencian una comprensión de la importancia de mantener actualizados los riesgos. Se reconoce que los cambios en el contexto estratégico y el entorno tecnológico pueden generar nuevos riesgos o modificar los existentes.

Coincidimos con la primera línea en que la falta de documentación formal sobre los cambios derivados del rediseño institucional dificulta una evaluación precisa del impacto en los riesgos identificados. Sin embargo, es fundamental realizar un análisis más profundo y detallado una vez se formalice la nueva plataforma tecnológica.

No se han identificado nuevos riesgos que requieran ser documentados y gestionados de manera inmediata. No obstante, los cambios en el entorno pueden generar nuevos riesgos. Es fundamental definir de manera concreta los tipos de nuevos riesgos que podrían surgir y realizar el proceso establecido por la entidad para identificarlos y gestionarlos.

#### ALERTAS

A pesar de que se identificaron varios riesgos potenciales, solo para uno se formuló un plan de acción. Esto indica que algunos riesgos podrían estar materializándose sin ser debidamente gestionados.

#### RECOMENDACIONES

* Disponer las evidencias en el repositorio donde se almacenen todos los registros relacionados con la gestión de riesgos, como capacitaciones, informes de incidentes, resultados de auditorías, etc.
* Evaluar la formulación de los seis riegos y alinearlos a las directrices dadas por la Dirección de Planeación y el DAFP.
* Promover una cultura de seguridad de la información que valore la identificación temprana de riesgos y la implementación de medidas preventivas involucrando a todos los intervinientes el proceso. Es necesario asegurar que los intervinientes en el proceso participen en las socializaciones y capacitaciones impartidas por la entidad sobre seguridad y privacidad de la información.
* Implementar un proceso estructurado para monitorear los riesgos de manera regular y evaluar la efectividad de las medidas de control.
* Es necesario documentar de manera clara y concisa los riesgos identificados, así como las acciones de mitigación implementadas.

### GESTIÓN FINANCIERA

#### MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN (GESTIÓN DE RECURSOS FINANCIEROS)

**Riesgo de Seguridad de la Información**

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.

#### OBSERVACIONES

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

La respuesta de la primera línea de defensa da cuenta del compromiso con la seguridad de la información. El análisis de riesgos, las causas y consecuencias realizado hasta el momento, son una clara muestra. Sin embargo, para la evaluación del contexto se recomienda los siguientes puntos clave para fortalecer aún más la gestión de riesgos:

Aunque la nueva plataforma estratégica no ha sido formalizada en la entidad, es importante tener presente que el rediseño institucional puede tener un impacto significativo en el contexto estratégico del proceso. Adicionalmente, con la reciente actualización de la caracterización del proceso Gestión Financiera, es fundamental realizar un análisis en profundidad de cómo los nuevos los objetivos y estructura definida podría afectar el contexto del proceso.

Realizar de manera proactiva una revisión exhaustiva del DOFA a la luz de los cambios institucionales y la caracterización nueva del proceso, permitirá identificar nuevas fortalezas, debilidades, oportunidades y amenazas que puedan impactar el proceso.

La primera línea de defensa ha mantenido su posición de que el riesgo identificado es coherente 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.”, incluso después de la actualización de la caracterización.

El rediseño institucional en curso implica cambios significativos en la estructura y los procesos de la entidad. Es necesario evaluar si estos cambios han introducido nuevos riesgos o si han modificado la probabilidad o el impacto de los riesgos existentes. Así mismo, la implementación del nuevo mapa de procesos institucional podría generar nuevas interdependencias y puntos de riesgo. Es fundamental realizar un análisis anticipado para identificar y mitigar estos riesgos.

De otra parte, manteniendo la posición en el primer monitoreo de la segunda línea de defensa, es necesario insistir en que la gestión de recursos financieros implica el manejo de información altamente sensible, por ello es crucial evaluar si se están implementando todas las medidas necesarias para garantizar la confidencialidad de esta información y cumplir con las regulaciones aplicables.

El criterio 1.3 para el análisis sobre la definición del riesgo, sus causas y consecuencias busca evaluar si el riesgo identificado está directamente relacionado con el objetivo del proceso. La primera línea de defensa ha mantenido su posición de que el riesgo es coherente con el objetivo del proceso, mientras que la segunda línea ha enfatizado la importancia de considerar el impacto del riesgo en la eficiencia y oportunidad de la gestión financiera. En este sentido, es importante analizar el riesgo de integridad de los “Instrumentos de apoyo no oficiales, para el cumplimiento de los objetivos del proceso, almacenados en los repositorios oficiales de la entidad”, basado en los siguientes aspectos:

* El riesgo de pérdida de integridad puede generar retrasos en los procesos, errores en los datos y dificultades en la toma de decisiones, lo que a su vez puede afectar la eficiencia y oportunidad en la gestión de los recursos financieros.
* La pérdida de integridad de la información puede generar incumplimientos normativos y legales, lo que puede tener consecuencias financieras y reputacionales para la entidad.
* La integridad de la información financiera es fundamental para mantener la confianza de las partes interesadas, como los ciudadanos, los entes de control y los usuarios.

La evaluación de las causas del riesgo es fundamental para garantizar la efectividad de las medidas de mitigación. Si bien la primera línea de defensa ha concluido que las causas iniciales del riesgo se mantienen, consideramos importante profundizar en este análisis, especialmente a la luz de los cambios organizacionales en curso. Es posible que las causas iniciales del riesgo hayan evolucionado o que hayan surgido nuevas causas como resultado de los cambios en el entorno o en los procesos internos.

Se recomienda evaluar si las medidas de mitigación implementadas están siendo efectivas en la reducción de las causas identificadas (desconocimiento o no aplicación de las políticas de seguridad y privacidad, manejo manual de los archivos y deficiencia en la autorización de permisos de la información) y las relacionadas a continuación:

* **Falta de conciencia:** Si bien es importante evitar el término "desconocimiento", es necesario reconocer que la falta de conciencia sobre los riesgos de seguridad de la información puede ser una causa subyacente. Se recomienda fortalecer las actividades de sensibilización y capacitación.
* **Procedimientos inadecuados:** Los procedimientos existentes pueden no ser suficientes para garantizar la seguridad de la información. Es necesario revisar y actualizar los procedimientos para reflejar los cambios en el entorno y las mejores prácticas.
* **Controles técnicos insuficientes:** Los controles técnicos implementados pueden no ser suficientes para proteger la información. Es necesario evaluar la efectividad de los controles técnicos existentes y considerar la implementación de nuevas medidas de seguridad.
* **Errores humanos:** Los errores humanos siguen siendo una causa importante de incidentes de seguridad. Es necesario implementar medidas para reducir los errores humanos, como la automatización de tareas y la doble verificación de procesos críticos.

El criterio 1.5 busca evaluar si las consecuencias inicialmente identificadas para el riesgo siguen siendo válidas. La primera línea de defensa ha mantenido su posición de que las consecuencias no han cambiado, mientras que la segunda línea ha enfatizado el impacto reputacional potencial.

Es posible que el rediseño institucional y los cambios en el entorno introduzcan nuevas consecuencias para el riesgo. Por ejemplo, la pérdida de integridad de la información puede tener un impacto más significativo en la reputación de la entidad en un contexto de mayor transparencia y exigencia ciudadana. De igual forma, Las consecuencias inicialmente identificadas pueden amplificarse debido a los cambios organizacionales. Por ejemplo, una brecha de seguridad que antes afectaba a un área específica puede ahora tener un impacto más amplio en toda la entidad.

Se recomienda realizar una revisión sobre la base de los criterios enunciados en esta evaluación, con el objeto de identificar la relevancia actual de las consecuencias identificadas inicialmente por el proceso y otras como por ejemplo:

* **Impacto reputacional:** La pérdida de integridad de la información puede dañar la reputación de la entidad, lo que puede llevar a la pérdida de confianza de los ciudadanos, los usuarios, grupos de interés y grupos de valor.
* **Pérdida financiera:** Los incidentes de seguridad pueden generar costos significativos para la entidad, incluyendo gastos legales, costos de recuperación de datos, y pérdidas de ingresos.
* **Incumplimiento normativo:** La pérdida de integridad de la información puede dar lugar a sanciones por parte de las autoridades reguladoras.
* **Disrupción de las operaciones:** Un incidente de seguridad puede interrumpir las operaciones de la entidad, lo que puede tener un impacto negativo en la prestación de servicios.

1. ***Autoevaluación de la efectividad de los controles****:*

La respuesta y la evidencia presentada por la primera línea de defensa, como la socialización de actualizaciones, el diligenciamiento del Formato A-FO-010 y los registros de comunicaciones, indica que los dos controles relacionados con la gestión de usuarios y el acceso a la información están siendo utilizados y se mantiene registro de las actividades realizadas. El análisis de los dos controles para determinar su aplicación se describe a continuación:

**Control 1: Socialización de políticas de seguridad:**

Evidencia: Socialización de comunicaciones recibidas por parte de la Dirección de Tecnología. La evidencia demuestra que se han realizado actividades de socialización, pero es necesario verificar la profundidad y alcance de dicha socialización. Se deben realizar evaluaciones periódicas para asegurar que las persona involucradas en el proceso comprendan y apliquen las políticas de seguridad.

**Control 2: Gestión de usuarios:**

Evidencia: Diligenciamiento del Formato A-FO-010 para la gestión de usuarios (Andres Vergara Ballén y Neftali Pardo Nieves), esta evidencia indica que se está utilizando un formato para solicitar la creación de cuentas de usuario. Se debe verificar si este formato se utiliza de manera consistente para todos los usuarios, si se realiza un seguimiento adecuado de las solicitudes y si se revocan los accesos cuando ya no son necesarios.

Se recomienda revisar la formulación del control 1. "El oficial de seguridad de la información de la entidad define, revisa, actualiza y socializa cada año las políticas de seguridad de la información y buenas prácticas del manejo de la información de la entidad", teniendo en cuenta que los controles deben ser formulados de modo que el proceso tenga la gobernanza y no como en este caso que se delega a la Dirección TIC. Un ejemplo puede ser: El líder del proceso implementa los mecanismos para garantizar que todas las personas adscritas al proceso participen en las jornadas de socialización y capacitación realizadas en la entidad.

Se recomienda para los próximos monitoreos, realizar una descripción sobre cómo desde el punto de vista del proceso los controles están siendo utilizados. Así mismo, en respuesta a los ítems de la evaluación es imprescindible incluir los argumentos necesarios para la mayor comprensión de la efectividad en la gestión del riesgo.

Los controles implementados en el proceso Gestión de Recursos Financieros, ahora Gestión Financiera, buscan mitigar el riesgo de pérdida de integridad de la información a través de las siguientes acciones:

**Control 1. Socialización de Políticas de Seguridad:**

Prevención: Al comunicar de manera clara y concisa las políticas de seguridad a todas las personas vinculadas al proceso, se fomenta una cultura de seguridad y se reduce la probabilidad de que ocurran errores humanos debido al desconocimiento de las normas.

Este control es fundamental en la mitigación del riesgo identificado por cuanto en caso de que ocurra un incidente, la socialización de las políticas facilita la identificación rápida de las acciones a seguir y la minimización de sus consecuencias.

**Control 2. Gestión de Usuarios:**

Prevención: Al controlar el acceso a los sistemas y datos, se limita la posibilidad de que personas no autorizadas accedan a información confidencial.

El control 2. Gestión de Usuarios contribuye en la mitigación porque en caso de que un usuario pierda su acceso o se vaya de la organización, se pueden revocar sus permisos de forma rápida y efectiva, reduciendo el riesgo de acceso no autorizado.

En los dos monitoreos del mapa de riesgos de seguridad, la primera línea de defensa respondió que los controles identificados para este riesgo son los adecuados, por lo anterior, no se requiere actualizarlos. Sin embargo, revisando el contexto del proceso se identificó que como resultado de las auditorias se dejó la siguiente nota: "Se cuenta con un contexto ajustado dentro de la planeación estratégica. Se recomienda incorporar el DOFA que hace parte del soporte del Plan Estratégico, recientemente expedido, en las nuevas versiones de los mapas de riesgo."

Los hallazgos y recomendaciones de auditoría pueden ser utilizados para actualizar el DOFA del proceso, identificando nuevas debilidades y amenazas, así como nuevas oportunidades para mejorar los controles. Al incorporar los hallazgos y/o recomendaciones de auditoría al DOFA, se puede obtener una visión más completa de la situación actual de la entidad y tomar decisiones más informadas sobre la asignación de recursos y la priorización de las acciones de mejora. Para este caso en particular, se recomienda realizar una revisión exhaustiva para corroborar si existe informes de auditoría internos y externos. Estos informes deben proporcionar información detallada que permitan evaluar si los controles se están implementando de acuerdo con los procedimientos establecidos y si los controles están logrando los objetivos de seguridad establecidos.

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, sin embargo, como parte de la mejora continua, se invita a realizar un auto análisis para identificar posibles mejoras en la gestión de los riesgos.

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

El riesgo identificado desde el proceso es la "Posibilidad de Pérdida de Integridad por fallas humanas y error en el uso o abuso de derechos y privilegios". Las causas principales identificadas son:

* Desconocimiento o no aplicación de las políticas de seguridad y privacidad.
* Manejo manual de los archivos.
* Deficiencia en la autorización de permisos de la información.

Desde la vista de la segunda línea de defensa se observó que las acciones implementadas, a saber, la socialización de las políticas de seguridad y la gestión de usuarios a través del formato A-FO-010, están directamente orientadas a abordar estas causas. esta afirmación se sustenta en las siguientes razones:

* Actividad 1. Socialización de políticas de seguridad: Esta acción busca directamente abordar la causa del desconocimiento de las políticas. Al informar a los empleados sobre las normas y procedimientos, se reduce la probabilidad de que cometan errores debido a la falta de conocimiento.
* Actividad 2. Gestión de usuarios a través del formato A-FO-010: Esta acción busca abordar las causas relacionadas con el manejo manual de archivos y la deficiencia en la autorización de permisos. Al formalizar el proceso de gestión de usuarios, se reduce la probabilidad de errores humanos y se asegura que solo las personas autorizadas tengan acceso a la información.

Con base en la evidencia proporcionada y considerando las respuestas de la primera y segunda línea de defensa en los monitoreos anteriores, se puede concluir que:

* Acción 1. Control 1 Socialización de actualizaciones: La Dirección Financiera ha cumplido con su compromiso de socializar las comunicaciones recibidas por parte de la Dirección de Tecnología. Esto demuestra un compromiso con mantener a los colaboradores informados sobre las últimas medidas de seguridad.
* Acción 2. Gestión de usuarios: El diligenciamiento del formato A-FO-010 para cambios de usuarios indica que se está llevando a cabo un proceso formal para gestionar los accesos a la información. Los ejemplos proporcionados de Neftalí Pardo Nieves y Andrés Vergara Ballen respaldan esta afirmación.

Se revisó la información proporcionada por la primera línea de defensa, dado que no hay evidencia de lo contrario, se confirma que, hasta la fecha no se ha reportado ningún incidente de seguridad relacionado con la pérdida de integridad de la información debido a fallas humanas o abuso de privilegios. Así mismo, las auditorías internas y externas realizadas no han identificado este riesgo como un hallazgo significativo. Dado que, hasta el momento, el riesgo de "Posibilidad de Pérdida de Integridad por fallas humanas y error en el uso o abuso de derechos y privilegios" no se ha materializado, no ha sido necesario implementar acciones correctivas específicas relacionadas con un incidente particular. Sin embargo, aunque el riesgo no se haya materializado, es fundamental mantener un enfoque preventivo y proactivo. Esto implica continuar con las acciones de mitigación existentes y evaluar si se requieren ajustes o mejoras, incluso es un ejercicio de preparación para enfrentar futuros escenarios y responder a posibles materializaciones del riesgo en el futuro.

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

La gestión del riesgo identificado ha demostrado ser efectiva en la prevención de situaciones que podrían afectar el cumplimiento de los objetivos del proceso. La ausencia de incidentes significativos relacionados con la posibilidad de Pérdida de Integridad por fallas humanas y error en el uso o abuso de derechos y privilegios, en la actual vigencia es una evidencia clara de la eficacia de las medidas de control implementadas. Además, el seguimiento y la actualización continua de los controles han permitido identificar y abordar de manera proactiva posibles vulnerabilidades. Como resultado de la gestión del riesgo se puede afirmar que la entidad ha podido mantener la continuidad de sus operaciones y fortalecer su reputación.

Dicho de otra forma, la gestión del riesgo ha sido útil para evitar situaciones o hechos que puedan afectar el cumplimiento de los objetivos y compromisos del proceso, por ejemplo:

* La fuga de información confidencial puede dañar la reputación de la Entidad, afectar la confianza de los usuarios, y generar pérdidas financieras significativas
* Los ataques cibernéticos pueden interrumpir las operaciones de la entidad, afectar la disponibilidad de la información
* El incumplimiento de las normas sobre protección de datos o las normas financieras pueden conllevar a sanciones importantes para la entidad
* 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 entidad.

1. ***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 formulación de la nueva caracterización del proceso, 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 y realizar una valoración periódica para determinar la necesidad de documentar y gestionar nuevos riesgos.

#### ALERTAS

Los cambios organizacionales en curso introducen nuevos riesgos y pueden modificar la probabilidad o el impacto de los riesgos existentes. Es necesario realizar un análisis detallado de cómo estos cambios afectan el perfil de riesgo del proceso.

La actualización de la caracterización de la Gestión Financiera requiere una revisión exhaustiva del mapa de riesgos para identificar nuevas vulnerabilidades y ajustar los controles existentes.

Estar atentos a las capacitaciones sobre el uso del sistema GESTIONATE mediante el cual se gestionarán los riesgos de seguridad de la información de la SDP.

#### RECOMENDACIONES

* La gestión de los riesgos en un proceso continuo y busca contribuir en la eficiencia administrativa de todos los procesos de la entidad. Para el fortalecimiento de la postura de seguridad del proceso se recomienda lo siguiente:
* Realizar un análisis más profundo de las causas del riesgo, considerando los cambios organizacionales y el contexto actual. Identificar si existen nuevas causas subyacentes que no fueron consideradas inicialmente.
* Fortalecer la Cultura de Seguridad de la información participando en programas de capacitación y sensibilización dispuestos por la entidad.
* Realizar una revisión exhaustiva de los procedimientos y controles para garantizar que sean adecuados y estén actualizados.
* Teniendo en cuenta que la pérdida de integridad de la información puede tener un impacto significativo en la reputación de la entidad, especialmente en un entorno cada vez más digitalizado y transparente, se recomienda evaluar y hacer seguimiento a los controles establecidos para reducirlo.
* Evaluar cómo un incidente de seguridad podría afectar la capacidad del proceso para prestar sus servicios y cumplir con sus objetivos. En este sentido, se debe realizar simulacros y mantener un plan de continuidad de las operaciones
* Definir y mantener actualizada la matriz de roles y responsabilidades de cada uno de los actores involucrados en la gestión de riesgos.
* Revisar y validar los riesgos una vez se implemente la plataforma estratégica 2024-2027, y actualizar el contexto estratégico del proceso.

### GESTIÓN JURÍDICA

#### MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN (SOPORTE LEGAL)

**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.

#### OBSERVACIONES

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

El proceso ha informado que no se han identificado situaciones que generen cambios en el contexto estratégico. Desde la segunda línea de defensa se recomienda validar los cambios organizacionales recientes, especialmente aquellos derivados del Decreto 432 de 2022. Así mismo, es necesario revisar y actualizar los instrumentos clave como la caracterización y la matriz DOFA y la alineación con la nueva caracterización definida por el proceso de Gestión Jurídica, a fin de garantizar una completa adaptación a la nueva realidad organizacional. Asimismo, se recomienda estar atentos a la formalización y puesta en marcha del nuevo modelo estratégico de la entidad para asegurar que el proceso contribuya de manera efectiva a los objetivos estratégicos.

El proceso identificó en el mapa de riesgos el objetivo estratégico al que aporta, "Fortalecer la estructura y la cultura institucional para contribuir a una gestión pública efectiva." y el riesgo de Pérdida de confidencialidad por fallas humanas, divulgación ilegal de la información y/o uso no autorizado de equipos. La pérdida de confidencialidad de información jurídica sensible puede generar un impacto negativo en la reputación institucional, erosionar la confianza de los ciudadanos y afectar la toma de decisiones informadas. Además, puede exponer a la entidad a riesgos legales y financieros. Por lo tanto, este riesgo es altamente relevante para el objetivo estratégico de fortalecer la institución.

El riesgo identificado es altamente coherente con el objetivo del proceso Gestión Jurídica. esto se sustenta en las siguientes razones:

* Asesorar y representar jurídicamente a la entidad implica brindar un servicio legal de alta calidad, basado en el conocimiento profundo de la normativa y de los casos específicos que se manejan.
* Garantizar la defensa de los intereses de la entidad conlleva la protección de los activos de la entidad, incluyendo su reputación y su posición legal.
* Contribuir a la toma de decisiones estratégicas incluye que los especialistas en derecho que representan a la SDP deben proporcionar asesoramiento jurídico sólido para respaldar las decisiones de la entidad.
* Se induce una relación entre el riesgo y el objetivo del proceso dado que la confidencialidad es un pilar fundamental para la prestación de servicios jurídicos de calidad. Si se pierde la confidencialidad de la información, se pone en riesgo la capacidad del equipo jurídico para brindar asesoramiento objetivo y estratégico. Adicionalmente, la divulgación de información confidencial puede debilitar la posición legal de la entidad en litigios o negociaciones, exponiéndola a mayores riesgos y la pérdida de confidencialidad puede llevar a una toma de decisiones basada en información incompleta o errónea, lo que puede tener consecuencias negativas para la entidad.

En conclusión, la pérdida de confidencialidad de la información es una amenaza directa a la capacidad del proceso Gestión Jurídica para cumplir sus objetivos. Al comprometer la confianza, la reputación y la capacidad de la entidad para tomar decisiones informadas, este riesgo socava los fundamentos mismos del proceso.

La afirmación del proceso, indica que "No se han presentado situaciones o circunstancias que conlleven la identificación de nuevas causas ", si bien es cierto que la ausencia de nuevas causas no necesariamente implica que los riesgos iniciales hayan cambiado, es importante recordar que los riesgos son dinámicos y pueden evolucionar con el tiempo debido a cambios en el entorno, la tecnología, o las políticas de la entidad.

El riesgo Identificado es la pérdida de confidencialidad de la información 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 y las causas Iniciales Identificadas son:

* **Manejo manual de la información:** La manipulación directa de documentos físicos o digitales puede aumentar el riesgo de pérdida o divulgación accidental.
* **Desconocimiento o no aplicación de las políticas de seguridad y privacidad de la información:** La falta de conciencia o el incumplimiento de las políticas establecidas pueden facilitar la ocurrencia de incidentes de seguridad.
* **Información sensible sin cifrado:** La ausencia de medidas de protección como el cifrado puede facilitar el acceso no autorizado a la información en caso de pérdida o robo de dispositivos.

Si bien no se han reportado nuevas causas directas del riesgo, es necesario realizar una evaluación más profunda para determinar si las causas iniciales se mantienen o si han surgido nuevas. Se sugiere:

* Revisar si se han presentado incidentes menores o intentos de acceso no autorizado que puedan indicar la presencia de nuevas vulnerabilidades.
* Verificar si los controles implementados para mitigar el riesgo están funcionando de manera efectiva y si se han identificado nuevas debilidades.
* Analizar si se han producido cambios en el entorno de la SDP que puedan afectar el riesgo, como la introducción de nuevas tecnologías, cambios en la estructura organizacional o modificaciones en la normativa legal.
* Solicitar retroalimentación a los usuarios del proceso para identificar cualquier preocupación o dificultad relacionada con la seguridad de la información.

En el análisis del riesgo “pérdida de confidencialidad de la información 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” definido en el proceso, se identificaron las siguientes consecuencias Iniciales:

* **Deterioro de la reputación institucional:** La divulgación de información confidencial puede dañar la imagen de la entidad y generar desconfianza en los ciudadanos y otras instituciones.
* **Vulnerabilidad legal:** La filtración de información puede exponer a la entidad a demandas legales y sanciones.
* **Pérdida de ventajas competitivas:** La divulgación de estrategias legales o información comercial sensible puede perjudicar la posición competitiva de la entidad.
* **Obstaculización de la toma de decisiones**: La falta de confidencialidad puede dificultar la toma de decisiones informadas y estratégicas.

Desde la Segunda Línea de Defensa se concluyó que, si bien las consecuencias iniciales siguen siendo relevantes, se recomienda considerar los siguientes aspectos:

* Validar la evolución del contexto teniendo en consideración el cambio del entorno organizacional y tecnológico que podría generar nuevas consecuencias o modificar la gravedad de las existentes.
* Revisar cambios en la legislación por cuanto las nuevas regulaciones en materia de protección de datos y privacidad podrían introducir nuevas obligaciones y consecuencias legales.

Así mismo, aunque las consecuencias iniciales siguen siendo válidas, es fundamental realizar un análisis más profundo para garantizar que se están considerando todos los posibles impactos del riesgo.

1. ***Autoevaluación de la efectividad de los controles****:*

Se ha observado una evolución en la presentación de evidencias por parte del proceso a lo largo de los monitoreos. En el primer monitoreo, se presentaron afirmaciones generales sobre la implementación de los controles, mientras que en el segundo monitoreo se incluyeron algunos documentos como evidencia. Sin embargo, existen oportunidades de mejora. A continuación, se describe algunas sugeridas:

**Para el control 1: Clasificación de la información:**

*Evidencia****:*** Formato de registro de activos de información.

*Evaluación:* Si bien la presentación del formato es un primer paso, es necesario verificar que este formato se esté utilizando de manera consistente y que la información contenida sea actualizada y precisa.

*Recomendación:* Aportar en los monitoreos una muestra de los registros completados para verificar la calidad y el detalle de la información clasificada.

**En los controles 2 y 3: Capacitación e implementación de políticas:**

*Evidencia:* No se encontró evidencias como listas de asistencia a capacitaciones y aplicación de herramientas como TRD.

*Evaluación*: La asistencia a capacitaciones es un buen indicador, se recomienda aportar evidencia que garantice la comprensión y aplicación efectiva de los conocimientos adquiridos. En cuanto a la aplicación de herramientas como TRD sugiere un avance en la implementación de las políticas, pero se requiere mayor evidencia.

*Recomendación:* Aportar evidencia sobre la asistencia a las capacitaciones y contextualizar como este control apoya el proceso y el objetivo estratégico de la entidad. Además, es necesario aportar ejemplos concretos de cómo se han aplicado las políticas en situaciones reales.

**Evidencias Faltantes**

* Formato de registro de activos de información, si bien se ha presentado el formato, se solicita una muestra de los registros completados para verificar su uso efectivo.
* Asistencia a capacitaciones. Se solicita presentar evidencia de asistencia y la apropiación de los conocimientos adquiridos (Ejemplo: Formularios que evalúan el conocimiento)

Con el objeto de realiza un monitoreo consistente, preciso y completo, se recomienda:

Verificar inconsistencias en la evidencia. Existe una inconsistencia entre las afirmaciones iniciales sobre la implementación de los controles y las evidencias presentadas.

Soportar el proceso de gestión de los riesgos con evidencia más robusta. Se requiere evidencia más sólida y detallada para demostrar la efectividad de los controles implementados.

Fortalecer el proceso de seguimiento. En este sentido es necesario establecer un proceso de seguimiento más estructurado para garantizar que las evidencias se recolecten y mantengan de manera sistemática.

Los tres controles evaluados están diseñados para prevenir o mitigar el riesgo de pérdida de confidencialidad de la información. A continuación, desde la segunda línea de defensa se realizó el análisis de cada uno de los controles indicando como previenen o mitigan el riesgo así:

**Control Clasificación de la información:**

*Prevención:* Al clasificar la información según su nivel de sensibilidad, se establece un marco para aplicar medidas de seguridad diferenciadas. Esto significa que la información más confidencial recibirá un nivel de protección mayor.

*Mitigación:* La clasificación permite identificar claramente qué información es más vulnerable y requiere medidas de seguridad más robustas. Al conocer la clasificación de cada dato, se pueden implementar controles específicos para protegerla.

**Control Capacitación en seguridad de la información:**

*Prevención:* La capacitación concientiza a los empleados sobre la importancia de proteger la información y les proporciona las herramientas necesarias para identificar y reportar posibles amenazas.

*Mitigación:* Al capacitar a los empleados, se reduce la probabilidad de errores humanos que pueden conducir a la pérdida de información confidencial. Además, los empleados estarán más atentos a las señales de posibles ataques o intrusiones.

**Control Implementación de políticas de seguridad de la información:**

*Prevención:* Las políticas de seguridad establecen las normas y procedimientos que deben seguir los empleados para proteger la información. Al definir claramente las responsabilidades y los procesos, se reduce el riesgo de desviaciones y errores.

*Mitigación:* Las políticas de seguridad proporcionan un marco de referencia para la toma de decisiones en materia de seguridad de la información. Al seguir estas políticas, se minimiza el riesgo de exposición de la información confidencial.

Estos tres controles están interrelacionados y se refuerzan mutuamente. Por ejemplo, la clasificación de la información es la base para la implementación de políticas de seguridad específicas y para la capacitación de los empleados. A su vez, la capacitación y las políticas ayudan a garantizar que la clasificación se realice de manera correcta y consistente.

Se recomienda revisar la formulación de los controles 2 y 3 dado que no están bajo el gobierno del proceso de Gestión Jurídica. Los controles deben ser definidos de manera que desde el proceso se tenga el control absoluto, por ejemplo: el control relacionado con la asistencia a las socializaciones realizadas por el Líder de Seguridad de la Información sobre las políticas de Sistema de Gestión de Seguridad de la Información y los lineamientos para el manejo adecuado de la información debe reconsiderar la delegación de la actividad de modo que este en el dominio del proceso. Es de recordar que el control debe ser orientado a eliminar la causa raíz y prevenir sus consecuencias y debe esta soportado con evidencia.

En general, las respuestas dadas desde el proceso indican que no se han encontrado hallazgos significativos que cuestionen la efectividad de los controles implementados para mitigar los riesgos de seguridad de la información. Sin embargo, es importante verificar si existen otras causas raíz de los riesgos identificados para identificar oportunidades de mejora. Esto permitirá implementar medidas de prevención más efectivas y reducir la probabilidad de futuros incidentes.

Es importante realizar una evaluación detallada de la naturaleza de los controles implementados para cada riesgo. Se debe asegurar que exista un equilibrio adecuado entre controles preventivos y detectivos, y que los controles sean suficientes para mitigar los riesgos identificados.

Es importante mencionar que la ausencia de hallazgos en las auditorías no implica necesariamente que los riesgos estén completamente mitigados. El monitoreo continuo y la evaluación de los controles son fundamentales para identificar y abordar cualquier debilidad que pueda surgir.

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

Desde el proceso se indica que no se formularon acciones para dar tratamiento al riesgo, dado que, después de aplicar los controles el riesgo está catalogado en zona leve moderada.

Al revisar el impacto determinado en el mapa de riesgos, se observó que es moderado por lo que se sugiere formular un plan de acción para reducir el impacto. Es importante resaltar que la evaluación de la eficacia de los controles debe ser un proceso continuo. Los riesgos y el entorno de seguridad evolucionan constantemente, por lo que es necesario realizar la revisión periódica para identificar si los controles están bien formulados y suficientes o si es necesario establecer acciones complementarias para atacar la probabilidad y el impacto.

Desde el proceso se informó que, no se ha materializado el riesgo permitiendo inferir que la gestión de riesgos basada en la identificación, evaluación y tratamiento de riesgos ha demostrado ser eficaz en la protección de la información confidencial. Los controles implementados, como la clasificación de la información y la capacitación del personal, han reducido significativamente la exposición a amenazas y han minimizado el impacto de posibles incidentes de seguridad.

Tomando como referencia la respuesta que no se ha materializado el riesgo dada por la primera línea de defensa, es recomendable que, aunque el riesgo no se ha concretizado, es necesario realizar la evaluación preventiva lo cual nos permite estar preparados y responder de manera eficaz ante cualquier eventualidad y la identificación de oportunidades de mejora.

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

La gestión del riesgo ha sido fundamental para garantizar el cumplimiento de los objetivos y los compromisos ya que ha permitido identificar, evaluar y tratar de manera proactiva las amenazas potenciales que podrían afectar el desempeño del proceso.

La gestión de riesgos y la integración a los procesos de planificación y ejecución al interior del proceso, ha facilitado el logro de los objetivos y metas establecidos al minimizar las desviaciones causadas por eventos inesperados e identificar y mitigar los riesgos, optimizando los recursos y reduciendo las pérdidas, lo que se traduce en una mayor eficiencia y productividad del proceso.

De otra parte y no menos importante, la información proporcionada por la gestión de riesgos permite tomar decisiones más informadas y estratégicas, al considerar los posibles riesgos y oportunidades lo cual se traduce en una gestión transparente y efectiva generando confianza en las partes interesadas, como clientes, proveedores y reguladores, al demostrar que la entidad está comprometida con la gestión de riesgos y el cumplimiento de sus obligaciones.

1. ***Actualización de Riesgos****:*

Las respuestas proporcionadas por la primera línea de defensa reconocen las recomendaciones contenidas en el informe de seguimiento a la gestión del riesgo elaborado recientemente por la OCI lo que podría generar nuevos riesgos o modificar los existentes.

La falta de documentación formal sobre los cambios derivados del rediseño institucional dificulta una evaluación precisa del impacto en los riesgos identificados. Sin embargo, es fundamental realizar un análisis más profundo y detallado una vez se formalice la nueva plataforma tecnológica. No obstante, se sugiere adelantar un análisis a partir de la nueva caracterización del proceso recién formulada. Las respuestas proporcionadas por la primera línea de defensa demuestran una comprensión de la necesidad de mantener un enfoque proactivo en la gestión de riesgos. No se han identificado nuevos riesgos que requieran ser documentados y gestionados de manera inmediata.

Los cambios en el entorno y las observaciones contenidas en el informe de seguimiento integral del riesgo en la vigencia 2024, presentado por la Oficina de Control interno, pueden dar cuenta de nuevos riesgos y por ello es importante mantener un enfoque proactivo. Sin embargo, es fundamental definir de manera concreta los tipos de nuevos riesgos que podrían surgir y realizar el proceso establecido por la entidad para identificarlos y gestionarlos.

#### ALERTAS

Realizar la actualización del contexto y la identificación de nuevos riesgos considerando la nueva caracterización del proceso y los cambios suscitados en el rediseño institucional.

#### RECOMENDACIONES

* A pesar de los avances en la presentación de evidencias, se observa que aún existen brechas en la documentación de la implementación de los controles. Si bien se ha presentado el formato de registro de activos de información y se ha informado sobre la asistencia a capacitaciones, se requiere evidencia adicional para corroborar la efectividad de estos controles.
* Desarrollar una base de conocimientos que contenga jurisprudencia, legislación, modelos de contratos y otros recursos legales relevantes, facilitando la consulta y el acceso a la información.
* Asegurar la participación del personal involucrado en el proceso en las capacitaciones que realiza la entidad sobre los temas de seguridad y privacidad de la información.

## PROCESOS DE EVALUACIÓN

### EVALUACIÓN Y CONTROL

#### MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

**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.

#### OBSERVACIONES

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

La evaluación de primera línea indica que el contexto estratégico identificado para el proceso sigue siendo altamente pertinente y alineado con los objetivos estratégicos de la entidad. Desde la segunda línea se identificó que esta afirmación se puede sustentar en los siguientes postulados:

* El proceso continúa desempeñando un papel fundamental en el fortalecimiento de la gestión de riesgos, control y gobierno, lo cual es esencial para garantizar la eficacia y eficiencia de nuestras operaciones.
* El riesgo identificado relacionado con la integridad de la información, siguen siendo válidos y requieren atención continua.
* El control ha demostrado ser efectivo en la mitigación de los riesgos identificados, reduciendo su impacto potencial en la organización.
* La implementación de un marco de monitoreo y la realización de ajustes periódicos demuestran el compromiso de la entidad con la mejora continua de sus procesos de gestión de riesgos.

No obstante, se recomienda revisar el contexto frente a la nueva caracterización recientemente formulada con el fin de asegurar que no se hayan incluido factores que puedan afectar la organización del proceso, sus funciones o los objetivos estratégicos a los que apunta. La implementación de la Resolución 422 de 2022 podría introducir nuevos riesgos o modificar la naturaleza de los riesgos existentes.

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", presenta una clara relación con el objetivo estratégico del proceso, que es "Proveer aseguramiento, asesoría y análisis basados en riesgos".

La anterior afirmación se sustenta en las siguientes razones:

* La pérdida de integridad de la información, como actas, informes y planes de auditoría, compromete directamente la confiabilidad de los resultados de las evaluaciones y análisis realizados por el proceso. Esto, a su vez, afecta la calidad de las asesorías y el aseguramiento proporcionados.
* La divulgación de información incorrecta o incompleta puede dañar la reputación de la entidad y socavar la confianza de las partes interesadas.
* La información no confiable puede llevar a la toma de decisiones equivocadas, con consecuencias negativas para la entidad.

Considerando los puntos anteriores, se concluye que el riesgo identificado es completamente coherente con el objetivo estratégico del proceso. La pérdida de integridad de la información representa una amenaza directa para la calidad y confiabilidad de los servicios que brinda el proceso, lo cual a su vez afecta la capacidad de la organización para alcanzar sus objetivos estratégicos.

La evaluación inicial de la primera línea de defensa sugiere que los riesgos identificados mantienen una coherencia directa con el objetivo del proceso. A continuación, presentamos un análisis más profundo del riesgo identificado, destacando como impacta directamente el logro del objetivo del proceso:

**Riesgo 1: Pérdida de Integridad de la Información:**

La pérdida de integridad de información crítica para el proceso, como actas, informes y planes de auditoría, compromete la calidad y confiabilidad de los resultados de las evaluaciones y análisis. Esto, a su vez, afecta la capacidad del proceso para proporcionar aseguramiento y asesoría basados en riesgos de manera objetiva e independiente.

El objetivo del proceso es garantizar la calidad de los servicios de aseguramiento y análisis. La pérdida de integridad de la información socava directamente este objetivo, ya que compromete la base sobre la cual se construyen dichos servicios.

La evaluación realizada confirma que el riesgo identificado en el proceso mantiene una estrecha relación con su objetivo principal. La pérdida de integridad de la información, por ejemplo, representa una amenaza directa para la calidad de los servicios de aseguramiento y análisis proporcionados por el proceso.

Es fundamental que la entidad continúe monitoreando estos riesgos y tomando las medidas necesarias para mitigarlos. De esta manera, se garantizará que el proceso siga contribuyendo al logro de los objetivos estratégicos de la entidad.

La primera línea de defensa indica que las causas identificadas para el riesgo de pérdida de integridad de la información, como el manejo manual de la información y la falta de capacitación en seguridad de la información, siguen siendo relevantes y persisten en el tiempo.

Desde la segunda línea de defensa se analizó la causa identificada en el proceso así:

**Manejo manual de la información:** A pesar de los esfuerzos realizados, el manejo manual de la información sigue siendo una práctica común en muchas áreas del proceso, lo que expone la información a un mayor riesgo de errores humanos y pérdida de integridad. La persistencia de esta causa subraya la necesidad de acelerar la implementación de soluciones tecnológicas para automatizar los procesos y reducir la dependencia del manejo manual de la información.

De otra parte, se analizó la causa raíz, falta de capacitación en seguridad de la información. Si bien se han realizado esfuerzos de capacitación, la rotación del personal y la evolución constante de las amenazas cibernéticas requieren un programa de capacitación continuo y actualizado. La falta de conocimiento sobre las mejores prácticas de seguridad de la información por parte del personal aumenta la probabilidad de errores humanos que pueden comprometer la integridad de la información.

Basados en este análisis, se recomienda reforzar el programa de capacitación en seguridad de la información, asegurando que el personal esté actualizado sobre las últimas amenazas y mejores prácticas. En este mismo sentido, se debe realizar un seguimiento continuo al plan propuesto y documentarlo.

Al evaluar la persistencia de las consecuencias identificadas para el riesgo, es fundamental considerar que estas están estrechamente ligadas a las causas subyacentes. Dado que hemos confirmado en el punto anterior que las causas principales del riesgo (manejo manual de la información y falta de capacitación) persisten, es lógico concluir que las consecuencias también se mantienen.

La Pérdida de integridad de la información genera consecuencias directas como, por ejemplo:

* **Decisiones erróneas:** La información incorrecta o incompleta puede llevar a la toma de decisiones equivocadas, con consecuencias negativas para la organización.
* **Pérdida de confianza:** La divulgación de información confidencial o errónea puede erosionar la confianza de las partes interesadas, tanto internas como externas.
* **Incumplimiento normativo:** La pérdida de integridad de la información puede dar lugar a incumplimientos legales y regulatorios, lo que puede resultar en sanciones económicas y reputacionales.

Así mismo, puede generar consecuencias indirectas entre ellas las siguientes:

* **Disminución de la eficiencia:** La necesidad de corregir errores y rehacer trabajos puede generar ineficiencias y retrasos en los procesos.
* Aumento de costos: Los incidentes de seguridad de la información pueden generar costos significativos relacionados con investigaciones, remediación y recuperación de datos.

En conclusión, las consecuencias identificadas inicialmente para el riesgo de pérdida de integridad de la información siguen siendo relevantes y persisten en el tiempo. Es fundamental que desde el proceso se continúe trabajando en la mitigación de este riesgo para proteger sus activos de información y garantizar la continuidad de sus operaciones.

1. ***Autoevaluación de la efectividad de los controles****:*

Si bien la primera línea de defensa ha indicado en el primer monitoreo que existen registros de la verificación del cumplimiento de los procesos de inducción y reinducción en seguridad de la información, y que en el segundo monitoreo respondió que la dinámica de la Oficina sigue igual, la segunda línea de defensa al revisar el repositorio dispuesto por la Dirección de Planeación, no encontró evidencias relacionadas con seguridad de la información lo que no permitió emitir un concepto sobre la utilización del control.

En el primer monitoreo se mencionan registros de inducción y reinducción sin que se proporcionara evidencia tangible que demuestre que estos procesos se hayan llevado a cabo de manera sistemática y completa para todas las personas adscritas al proceso. Adicionalmente, dado que la inducción en seguridad de la información, depende de la coordinación con otras áreas de la entidad (en este caso, la Dirección de Talento Humano). Esto puede generar retrasos y afectar la efectividad de los controles.

Es fundamental establecer un sistema de documentación claro y conciso para registrar todas las actividades relacionadas con la implementación y el seguimiento de los controles. Para el caso de las capacitaciones, esta documentación debe incluir fechas, nombres de los participantes y cualquier otra información relevante. Se debe mantener evidencias para verificar la efectividad del control 1 basado en capacitaciones y sesiones de inducción y reinducción y del control 2 sobre la revisión conjunta del cumplimiento de las políticas de seguridad de la información.

En conclusión, si bien se menciona que existe evidencia de que se están realizando esfuerzos para implementar los controles diseñados para mitigar el riesgo de pérdida de integridad de la información, es necesario fortalecer el sistema de seguimiento y evaluación para garantizar que estos controles sean efectivos y mantener evidencias tangibles de las actuaciones que adelante el proceso.

Desde la Segunda línea de defensa se realizó en el primer monitoreo, el análisis de cada control emitiendo algunas razones por las cuales podría considerar que los controles previenen o mitigan el riesgo identificado en el proceso. En este monitoreo se presenta el siguiente resultado:

**Control 1: Verificación de procesos de inducción y reinducción en seguridad de la información**

Este control tiene el potencial de prevenir el riesgo al garantizar que los funcionarios cuenten con el conocimiento necesario para proteger la información. Aunque se menciona la existencia de registros, la falta de evidencia concreta limita la efectividad de este control en la práctica.

**Control 2: Revisión de incidentes de seguridad y cumplimiento de la política de seguridad**

Este control es fundamental para detectar y corregir rápidamente cualquier brecha en la seguridad de la información. la ausencia de incidentes reportados dificulta evaluar la efectividad de este control. Sin embargo, el hecho de que exista un proceso establecido para revisar incidentes de seguridad es positivo.

Se recomienda fortalecer la recopilación de evidencia. Adicionalmente, tratándose de un tema crucial para la entidad, se sugiere que, en la medida de lo posible, se automatice los procesos de seguimiento y registro de la implementación de los controles. Esto permitirá reducir el margen de error y facilitar la generación de informes.

Desde la Primera Línea de Defensa se informó que, "No se tienen hallazgos de ninguna auditoría relacionados", en la revisión realizada por la Segunda línea de Defensa sobre el contexto y las respuestas dadas en los monitoreos anteriores, se infiere que no se tiene hallazgos de auditoria asociados a los dos controles establecidos desde el proceso.

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

Si bien la primera línea de defensa ha indicado que las acciones identificadas son adecuadas para contrarrestar las causas del riesgo, desde la visión de la segunda línea de defensa se identificaron algunas áreas de oportunidad:

* A pesar de que se mencionan acciones específicas "Gestionar una sesión de socialización en asuntos de seguridad de la información en los temas de la Oficina de Control Interno", no se ha proporcionado evidencia tangible que demuestre que se estén implementando de manera efectiva y que estén logrando los resultados esperados.
* Si bien la acción incluida en el plan de acción es importante para prevenir incidentes de seguridad, es necesario complementar estos controles con medidas de detección y respuesta para poder mitigar el impacto de los incidentes que puedan ocurrir.
* Se ha proporcionado información sobre la acción "Gestionar una sesión de socialización en asuntos de seguridad de la información en los temas de la Oficina de Control Interno", pero no se ha actualizado los reportes de seguimiento en el mapa de riesgos sobre este plan, que faciliten observar el avance en su ejecución y su cumplimiento.

Para un mejor enfoque, se presenta a continuación el análisis de las dos acciones establecidas en el plan.

**Acción 1:** **Socialización de las políticas de seguridad de la información:** Este control está orientado a aumentar la conciencia de los empleados sobre los riesgos de seguridad de la información y a promover la adopción de prácticas seguras.

Su efectividad se da en que la socialización de las políticas es muy importante, pero por sí sola no garantiza que los empleados sigan las políticas. Se requieren controles adicionales para verificar el cumplimiento.

**Acción 2:** **Diligenciamiento del Formato A-FO-010 para la gestión de cuentas de usuarios:** Este control está orientado a controlar el acceso a los sistemas y datos de la organización, lo cual es fundamental para prevenir el acceso no autorizado. El control es efectivo si se implementa de manera consistente y se revisan periódicamente los permisos de acceso.

En este mismo contexto, si bien en el primer seguimiento de la primera línea de defensa, se ha identificado la necesidad de reevaluar la acción de socialización de las políticas de seguridad de la información, es evidente que se requiere un mayor esfuerzo para garantizar la implementación efectiva de las acciones y la consecuente reducción del riesgo.

Recomendamos que la primera línea de defensa trabaje para desarrollar un plan de acción detallado que incluya: Un análisis exhaustivo de las causas de las dificultades encontradas en la implementación de la acción, la definición de objetivos claros y medibles para la implementación de las acciones, la asignación de responsabilidades y plazos, un plan de seguimiento y evaluación. Así mismo, debe diligenciar en el mapa de riesgos, los campos relacionados con <Indicador Clave del Riesgo> y que hacen parte del plan de acción formulado.

Coincidimos con la evaluación realizada en los monitoreos anteriores en cuanto a que el riesgo de pérdida de integridad de la información no se ha materializado hasta el momento. Sin embargo, es fundamental destacar que la ausencia de incidentes no implica necesariamente que el riesgo haya desaparecido.

El riesgo de pérdida de integridad de la información sigue siendo relevante y persistente debido a la naturaleza dinámica de las amenazas derivadas de errores humanos y las vulnerabilidades en los sistemas que pueden ser explotadas por atacantes para acceder a información confidencial. Hasta el momento, no se ha evidenciado la materialización de este riesgo a través de incidentes reportados. Sin embargo, la persistencia de las causas subyacentes (manejo manual de la información y falta de capacitación) mantiene el riesgo latente.

Dado que en los monitoreos anteriores ni en este, se ha determinado que el riesgo de pérdida de integridad de la información no se ha materializado, no es pertinente evaluar en este momento la existencia de correcciones ni acciones correctivas específicas, sin embargo, es fundamental tener un plan interno de respuesta a incidentes bien definido y actualizado.

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

Coincidimos con la evaluación realizada en los monitoreos anteriores en cuanto a que la gestión del riesgo ha sido útil para prevenir la materialización del riesgo identificado y para contribuir al cumplimiento de los objetivos del proceso.

Tomando como base la información de los monitoreos anteriores, se infiere que la gestión efectiva del riesgo ha proporcionado los siguientes beneficios tales como: Al identificar y mitigar los riesgos, la Oficina de Control Interno ha evitado pérdidas financieras y de reputación, así mismo, la gestión del riesgo ha fomentado una cultura de control al interior del proceso, lo que ha contribuido a mejorar la calidad de los servicios prestados.

Se recomienda fortalecer aún más la gestión del riesgo, documentando los controles, las acciones formuladas en el plan de acción y las lecciones aprendidas para mejorar continuamente las prácticas del proceso.

1. ***Actualización de Riesgos****:*

Si bien hasta el momento el riesgo de pérdida de integridad de la información no se ha materializado, tal como lo indica el proceso, es fundamental mantener una evaluación continua del riesgo para garantizar que siga siendo relevante y que las medidas de control implementadas sean efectivas.

Se recomienda para el próximo monitoreo, evaluar cambios en el contexto estratégico considerando las modificaciones en los procesos internos de la entidad derivados del Decreto 432 de 2022. Debemos recordar que la implementación de nuevos procesos o la modificación de los existentes puede generar nuevos puntos de vulnerabilidad.

A partir de las repuestas en los monitoreos de primera línea, no se identifica la necesidad de documentar y gestionar nuevos riesgos. Se recomienda realizar el análisis de la nueva caracterización y los cambios en el contexto estratégico institucional para determinar si existen nuevos riesgos que puedan afectar las actividades propias del proceso y ameriten la necesidad de documentar o gestionar nuevos riesgos.

#### ALERTAS

Se observó que desde el proceso se actualizó el mapa de proceso alineándolo a la nueva estructura organizacional lo cual hace necesario la revisión del contexto definido en el mapa de riesgos para permitir identificar cambios que puedan generar nuevas vulnerabilidades que puedan ser explotadas en perjuicio de la entidad.

#### RECOMENDACIONES

La gestión eficaz de los riesgos es un imperativo estratégico en el entorno operativo de la SDP cada vez más volátil y complejo. **La primera línea de defensa, como primera barrera de protección, desempeña un papel esencial en la identificación y mitigación de amenazas.** A través de este apartado, proporcionaremos recomendaciones prácticas para potenciar las capacidades de la primera línea de defensa y asegurar una gestión de riesgos proactiva y efectiva. A continuación, se relacionan algunas sugerencias para su aplicación:

* Implementar un proceso de revisión periódica del mapa de riesgos para garantizar que esté alineado con los cambios en el contexto estratégico, regulatorio y tecnológico.
* Realizar análisis de riesgos más detallados, considerando no solo los riesgos actuales, sino también los potenciales riesgos emergentes.
* Asegurar que la documentación del proceso de gestión de riesgos sea clara, concisa y actualizada, facilitando la comprensión y el seguimiento por parte de todos los involucrados.
* Empoderar a los involucrados en el proceso para que reporten cualquier desviación o irregularidad que identifiquen.

### CONTROL DISCIPLINARIO INTERNO

#### MAPA DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

**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.

#### OBSERVACIONES

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

La evaluación de primera línea indica que el contexto estratégico identificado para el proceso sigue siendo altamente pertinente y alineado con los objetivos estratégicos de la entidad. Desde la segunda línea se identificó que esta afirmación se puede sustentar en los siguientes postulados:

* El proceso continúa desempeñando un papel fundamental en el fortalecimiento de la gestión de riesgos, control y gobierno, lo cual es esencial para garantizar la eficacia y eficiencia de nuestras operaciones.
* El riesgo identificado relacionado con la integridad de la información, siguen siendo válidos y requieren atención continua.
* El control ha demostrado ser efectivo en la mitigación de los riesgos identificados, reduciendo su impacto potencial en la organización.
* La implementación de un marco de monitoreo y la realización de ajustes periódicos demuestran el compromiso de la entidad con la mejora continua de sus procesos de gestión de riesgos.

No obstante, se recomienda revisar el contexto frente a la nueva caracterización recientemente formulada con el fin de asegurar que no se hayan incluido factores que puedan afectar la organización del proceso, sus funciones o los objetivos estratégicos a los que apunta. La implementación de la Resolución 422 de 2022 podría introducir nuevos riesgos o modificar la naturaleza de los riesgos existentes.

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", presenta una clara relación con el objetivo estratégico del proceso, que es "Proveer aseguramiento, asesoría y análisis basados en riesgos".

La anterior afirmación se sustenta en las siguientes razones:

* La pérdida de integridad de la información, como actas, informes y planes de auditoría, compromete directamente la confiabilidad de los resultados de las evaluaciones y análisis realizados por el proceso. Esto, a su vez, afecta la calidad de las asesorías y el aseguramiento proporcionados.
* La divulgación de información incorrecta o incompleta puede dañar la reputación de la entidad y socavar la confianza de las partes interesadas.
* La información no confiable puede llevar a la toma de decisiones equivocadas, con consecuencias negativas para la entidad.

Considerando los puntos anteriores, se concluye que el riesgo identificado es completamente coherente con el objetivo estratégico del proceso. La pérdida de integridad de la información representa una amenaza directa para la calidad y confiabilidad de los servicios que brinda el proceso, lo cual a su vez afecta la capacidad de la organización para alcanzar sus objetivos estratégicos.

La evaluación inicial de la primera línea de defensa sugiere que los riesgos identificados mantienen una coherencia directa con el objetivo del proceso. A continuación, presentamos un análisis más profundo del riesgo identificado, destacando como impacta directamente el logro del objetivo del proceso:

**Riesgo 1: Pérdida de Integridad de la Información:**

La pérdida de integridad de información crítica para el proceso, como actas, informes y planes de auditoría, compromete la calidad y confiabilidad de los resultados de las evaluaciones y análisis. Esto, a su vez, afecta la capacidad del proceso para proporcionar aseguramiento y asesoría basados en riesgos de manera objetiva e independiente.

El objetivo del proceso es garantizar la calidad de los servicios de aseguramiento y análisis. La pérdida de integridad de la información socava directamente este objetivo, ya que compromete la base sobre la cual se construyen dichos servicios.

La evaluación realizada confirma que el riesgo identificado en el proceso mantiene una estrecha relación con su objetivo principal. La pérdida de integridad de la información, por ejemplo, representa una amenaza directa para la calidad de los servicios de aseguramiento y análisis proporcionados por el proceso.

Es fundamental que la entidad continúe monitoreando estos riesgos y tomando las medidas necesarias para mitigarlos. De esta manera, se garantizará que el proceso siga contribuyendo al logro de los objetivos estratégicos de la entidad.

La primera línea de defensa indica que las causas identificadas para el riesgo de pérdida de integridad de la información, como el manejo manual de la información y la falta de capacitación en seguridad de la información, siguen siendo relevantes y persisten en el tiempo.

Desde la segunda línea de defensa se analizó la causa identificada en el proceso así:

**Manejo manual de la información:** A pesar de los esfuerzos realizados, el manejo manual de la información sigue siendo una práctica común en muchas áreas del proceso, lo que expone la información a un mayor riesgo de errores humanos y pérdida de integridad. La persistencia de esta causa subraya la necesidad de acelerar la implementación de soluciones tecnológicas para automatizar los procesos y reducir la dependencia del manejo manual de la información.

De otra parte, se analizó la causa raíz, falta de capacitación en seguridad de la información. Si bien se han realizado esfuerzos de capacitación, la rotación del personal y la evolución constante de las amenazas cibernéticas requieren un programa de capacitación continuo y actualizado. La falta de conocimiento sobre las mejores prácticas de seguridad de la información por parte del personal aumenta la probabilidad de errores humanos que pueden comprometer la integridad de la información.

Basados en este análisis, se recomienda reforzar el programa de capacitación en seguridad de la información, asegurando que el personal esté actualizado sobre las últimas amenazas y mejores prácticas. En este mismo sentido, se debe realizar un seguimiento continuo al plan propuesto y documentarlo.

Al evaluar la persistencia de las consecuencias identificadas para el riesgo, es fundamental considerar que estas están estrechamente ligadas a las causas subyacentes. Dado que hemos confirmado en el punto anterior que las causas principales del riesgo (manejo manual de la información y falta de capacitación) persisten, es lógico concluir que las consecuencias también se mantienen.

La Pérdida de integridad de la información genera consecuencias directas como, por ejemplo:

* **Decisiones erróneas:** La información incorrecta o incompleta puede llevar a la toma de decisiones equivocadas, con consecuencias negativas para la organización.
* **Pérdida de confianza:** La divulgación de información confidencial o errónea puede erosionar la confianza de las partes interesadas, tanto internas como externas.
* **Incumplimiento normativo:** La pérdida de integridad de la información puede dar lugar a incumplimientos legales y regulatorios, lo que puede resultar en sanciones económicas y reputacionales.

Así mismo, puede generar consecuencias indirectas entre ellas las siguientes:

* **Disminución de la eficiencia:** La necesidad de corregir errores y rehacer trabajos puede generar ineficiencias y retrasos en los procesos.
* Aumento de costos: Los incidentes de seguridad de la información pueden generar costos significativos relacionados con investigaciones, remediación y recuperación de datos.

En conclusión, las consecuencias identificadas inicialmente para el riesgo de pérdida de integridad de la información siguen siendo relevantes y persisten en el tiempo. Es fundamental que desde el proceso se continúe trabajando en la mitigación de este riesgo para proteger sus activos de información y garantizar la continuidad de sus operaciones.

1. ***Autoevaluación de la efectividad de los controles****:*

Si bien la primera línea de defensa ha indicado en el primer monitoreo que existen registros de la verificación del cumplimiento de los procesos de inducción y reinducción en seguridad de la información, y que en el segundo monitoreo respondió que la dinámica de la Oficina sigue igual, la segunda línea de defensa al revisar el repositorio dispuesto por la Dirección de Planeación, no encontró evidencias relacionadas con seguridad de la información lo que no permitió emitir un concepto sobre la utilización del control.

En el primer monitoreo se mencionan registros de inducción y reinducción sin que se proporcionara evidencia tangible que demuestre que estos procesos se hayan llevado a cabo de manera sistemática y completa para todas las personas adscritas al proceso. Adicionalmente, dado que la inducción en seguridad de la información, depende de la coordinación con otras áreas de la entidad (en este caso, la Dirección de Talento Humano ). Esto puede generar retrasos y afectar la efectividad de los controles.

Es fundamental establecer un sistema de documentación claro y conciso para registrar todas las actividades relacionadas con la implementación y el seguimiento de los controles. Para el caso de las capacitaciones, esta documentación debe incluir fechas, nombres de los participantes y cualquier otra información relevante. Se debe mantener evidencias para verificar la efectividad del control 1 basado en capacitaciones y sesiones de inducción y reinducción y del control 2 sobre la revisión conjunta del cumplimiento de las políticas de seguridad de la información.

En conclusión, si bien se menciona que existe evidencia de que se están realizando esfuerzos para implementar los controles diseñados para mitigar el riesgo de pérdida de integridad de la información, es necesario fortalecer el sistema de seguimiento y evaluación para garantizar que estos controles sean efectivos y mantener evidencias tangibles de las actuaciones que adelante el proceso.

Desde la Segunda línea de defensa se realizó en el primer monitoreo, el análisis de cada control emitiendo algunas razones por las cuales podría considerar que los controles previenen o mitigan el riesgo identificado en el proceso. En este monitoreo se presenta el siguiente resultado:

**Control 1: Verificación de procesos de inducción y reinducción en seguridad de la información**

Este control tiene el potencial de prevenir el riesgo al garantizar que los funcionarios cuenten con el conocimiento necesario para proteger la información. Aunque se menciona la existencia de registros, la falta de evidencia concreta limita la efectividad de este control en la práctica.

**Control 2: Revisión de incidentes de seguridad y cumplimiento de la política de seguridad**

Este control es fundamental para detectar y corregir rápidamente cualquier brecha en la seguridad de la información. la ausencia de incidentes reportados dificulta evaluar la efectividad de este control. Sin embargo, el hecho de que exista un proceso establecido para revisar incidentes de seguridad es positivo.

Se recomienda fortalecer la recopilación de evidencia. Adicionalmente, tratándose de un tema crucial para la entidad, se sugiere que, en la medida de lo posible, se automatice los procesos de seguimiento y registro de la implementación de los controles. Esto permitirá reducir el margen de error y facilitar la generación de informes.

Desde la Primera Línea de Defensa se informó que, "No se tienen hallazgos de ninguna auditoría relacionados", en la revisión realizada por la Segunda línea de Defensa sobre el contexto y las respuestas dadas en los monitoreos anteriores, se infiere que no se tiene hallazgos de auditoria asociados a los dos controles establecidos desde el proceso.

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

Si bien la primera línea de defensa ha indicado que las acciones identificadas son adecuadas para contrarrestar las causas del riesgo, desde la visión de la segunda línea de defensa se identificaron algunas áreas de oportunidad:

* A pesar de que se mencionan acciones específicas "Gestionar una sesión de socialización en asuntos de seguridad de la información en los temas de la Oficina de Control Interno", no se ha proporcionado evidencia tangible que demuestre que se estén implementando de manera efectiva y que estén logrando los resultados esperados.
* Si bien la acción incluida en el plan de acción es importante para prevenir incidentes de seguridad, es necesario complementar estos controles con medidas de detección y respuesta para poder mitigar el impacto de los incidentes que puedan ocurrir.
* Se ha proporcionado información sobre la acción "Gestionar una sesión de socialización en asuntos de seguridad de la información en los temas de la Oficina de Control Interno", pero no se ha actualizado los reportes de seguimiento en el mapa de riesgos sobre este plan, que faciliten observar el avance en su ejecución y su cumplimiento.

Para un mejor enfoque, se presenta a continuación el análisis de las dos acciones establecidas en el plan.

**Acción 1:** **Socialización de las políticas de seguridad de la información:** Este control está orientado a aumentar la conciencia de los empleados sobre los riesgos de seguridad de la información y a promover la adopción de prácticas seguras.

Su efectividad se da en que la socialización de las políticas es muy importante, pero por sí sola no garantiza que los empleados sigan las políticas. Se requieren controles adicionales para verificar el cumplimiento.

**Acción 2:** **Diligenciamiento del Formato A-FO-010 para la gestión de cuentas de usuarios:** Este control está orientado a controlar el acceso a los sistemas y datos de la organización, lo cual es fundamental para prevenir el acceso no autorizado. El control es efectivo si se implementa de manera consistente y se revisan periódicamente los permisos de acceso.

En este mismo contexto, si bien en el primer seguimiento de la primera línea de defensa, se ha identificado la necesidad de reevaluar la acción de socialización de las políticas de seguridad de la información, es evidente que se requiere un mayor esfuerzo para garantizar la implementación efectiva de las acciones y la consecuente reducción del riesgo.

Recomendamos que la primera línea de defensa trabaje para desarrollar un plan de acción detallado que incluya: Un análisis exhaustivo de las causas de las dificultades encontradas en la implementación de la acción, la definición de objetivos claros y medibles para la implementación de las acciones, la asignación de responsabilidades y plazos, un plan de seguimiento y evaluación. Así mismo, debe diligenciar en el mapa de riesgos, los campos relacionados con <Indicador Clave del Riesgo> y que hacen parte del plan de acción formulado.

Coincidimos con la evaluación realizada en los monitoreos anteriores en cuanto a que el riesgo de pérdida de integridad de la información no se ha materializado hasta el momento. Sin embargo, es fundamental destacar que la ausencia de incidentes no implica necesariamente que el riesgo haya desaparecido.

El riesgo de pérdida de integridad de la información sigue siendo relevante y persistente debido a la naturaleza dinámica de las amenazas derivadas de errores humanos y las vulnerabilidades en los sistemas que pueden ser explotadas por atacantes para acceder a información confidencial. Hasta el momento, no se ha evidenciado la materialización de este riesgo a través de incidentes reportados. Sin embargo, la persistencia de las causas subyacentes (manejo manual de la información y falta de capacitación) mantiene el riesgo latente.

Dado que en los monitoreos anteriores ni en este, se ha determinado que el riesgo de pérdida de integridad de la información no se ha materializado, no es pertinente evaluar en este momento la existencia de correcciones ni acciones correctivas específicas, sin embargo, es fundamental tener un plan interno de respuesta a incidentes bien definido y actualizado.

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

Coincidimos con la evaluación realizada en los monitoreos anteriores en cuanto a que la gestión del riesgo ha sido útil para prevenir la materialización del riesgo identificado y para contribuir al cumplimiento de los objetivos del proceso.

Tomando como base la información de los monitoreos anteriores, se infiere que la gestión efectiva del riesgo ha proporcionado los siguientes beneficios tales como: Al identificar y mitigar los riesgos, la Oficina de Control Interno ha evitado pérdidas financieras y de reputación, así mismo, la gestión del riesgo ha fomentado una cultura de control al interior del proceso, lo que ha contribuido a mejorar la calidad de los servicios prestados.

Se recomienda fortalecer aún más la gestión del riesgo, documentando los controles, las acciones formuladas en el plan de acción y las lecciones aprendidas para mejorar continuamente las prácticas del proceso.

1. ***Actualización de Riesgos****:*

Si bien hasta el momento el riesgo de pérdida de integridad de la información no se ha materializado, tal como lo indica el proceso, es fundamental mantener una evaluación continua del riesgo para garantizar que siga siendo relevante y que las medidas de control implementadas sean efectivas.

Se recomienda para el próximo monitoreo, evaluar cambios en el contexto estratégico considerando las modificaciones en los procesos internos de la entidad derivados del Decreto 432 de 2022. Debemos recordar que la implementación de nuevos procesos o la modificación de los existentes puede generar nuevos puntos de vulnerabilidad.

A partir de las repuestas en los monitoreos de primera línea, no se identifica la necesidad de documentar y gestionar nuevos riesgos. Se recomienda realizar el análisis de la nueva caracterización y los cambios en el contexto estratégico institucional para determinar si existen nuevos riesgos que puedan afectar las actividades propias del proceso y ameriten la necesidad de documentar o gestionar nuevos riesgos.

#### ALERTAS

Se observó que desde el proceso se actualizó el mapa de proceso alineándolo a la nueva estructura organizacional lo cual hace necesario la revisión del contexto definido en el mapa de riesgos para permitir identificar cambios que puedan generar nuevas vulnerabilidades que puedan ser explotadas en perjuicio de la entidad.

#### RECOMENDACIONES

La gestión eficaz de los riesgos es un imperativo estratégico en el entorno operativo de la SDP cada vez más volátil y complejo. La primera línea de defensa, como primera barrera de protección, desempeña un papel esencial en la identificación y mitigación de amenazas. A través de este apartado, proporcionaremos recomendaciones prácticas para potenciar las capacidades de la primera línea de defensa y asegurar una gestión de riesgos proactiva y efectiva. A continuación, se relacionan algunas sugerencias para su aplicación:

* Implementar un proceso de revisión periódica del mapa de riesgos para garantizar que esté alineado con los cambios en el contexto estratégico, regulatorio y tecnológico.
* Realizar análisis de riesgos más detallados, considerando no solo los riesgos actuales, sino también los potenciales riesgos emergentes.
* Asegurar que la documentación del proceso de gestión de riesgos sea clara, concisa y actualizada, facilitando la comprensión y el seguimiento por parte de todos los involucrados.
* Empoderar a los involucrados en el proceso para que reporten cualquier desviación o irregularidad que identifiquen.

# OBSERVACIONES, ALERTAS Y RECOMENDACIONES GENERALES

A nivel general, se establecen las siguientes observaciones, alertas y recomendaciones:

## OBSERVACIONES:

Se ha detectado que varios procesos no han construido y otros no han actualizado sus mapas de riesgos de conformidad con los cambios recientes en sus respectivos contextos operativos. Esta situación expone a la organización a riesgos emergentes y reduce la efectividad de las medidas de control existentes.

Se ha evidenciado una deficiencia generalizada en la presentación de pruebas tangibles (registros, reportes, etc.) que sustenten la autoevaluación de la efectividad de los controles implementados. Esta falta de evidencia impide una evaluación objetiva del desempeño de los controles y dificulta la identificación de áreas de mejora.

Las respuestas proporcionadas por algunos procesos a los criterios de evaluación han sido consideradas superficiales y poco detalladas, lo que limita la capacidad de realizar un monitoreo efectivo de segunda línea de defensa. Se requiere una mayor profundidad en el análisis de los riesgos y los controles asociados.

Se ha observado que, en algunos casos, a pesar de haber identificado la necesidad de mitigar o reducir ciertos riesgos después de la implementación de controles, no se han formulado planes de acción complementarios. Esta omisión puede comprometer la eficacia de las medidas de control y exponer a la organización a riesgos residuales.

Se han identificado casos en los que se han definido controles correctivos sin que exista un registro claro de la materialización del riesgo correspondiente. Esta situación sugiere una falta de comprensión de los principios de gestión de riesgos y puede llevar a la implementación de controles innecesarios o ineficaces.

Se ha detectado una variabilidad en la clasificación de los riesgos entre los diferentes procesos, lo que dificulta la comparación y priorización de los mismos. Es necesario establecer criterios claros y consistentes para la clasificación de riesgos.

No se ha evidenciado una clara comprensión de la forma de contrarrestar el impacto potencial de los riesgos identificados. Esta omisión impide una adecuada priorización de las acciones de mitigación.

En algunos casos, no se ha realizado un seguimiento adecuado a la implementación de las acciones correctivas, lo que impide evaluar su efectividad y determinar si se han logrado los objetivos planteados.

## ALERTAS:

Ante la dinámica de los cambios organizacionales y la evolución del entorno, es imperativo actualizar los mapas de riesgos de seguridad de la información de todos los procesos.

Los recientes ajustes en la estructura organizacional y las nuevas caracterizaciones de los procesos demandan una revisión exhaustiva de los riesgos a los que se encuentran expuestos. Es fundamental incorporar estos cambios en los mapas de riesgos para garantizar una protección adecuada de la información y los activos de la organización.

Se informa que la actualización de la norma ISO 27001 en febrero de 2022 ha impulsado la actualización del módulo de seguridad de la información en el software GESTIONATE. Con el fin de garantizar el cumplimiento normativo y optimizar la gestión de la seguridad de la información, se solicita a todos los procesos que participen activamente en las capacitaciones programadas para familiarizarse con las funcionalidades y mejoras de la nueva versión del módulo, así mismo, deben reevaluar y redefinir sus controles de seguridad de acuerdo con los requisitos establecidos en la última versión de la norma ISO 27001.

La actualización de estos controles es fundamental para mantener un sistema de gestión de seguridad de la información robusto y eficaz.

## RECOMENDACIONES:

* Actualizar y documentar todas las políticas y procedimientos de seguridad alineándolos a la norma ISO27001:2022 y comunicarlos a todos los funcionarios, contratistas y personal temporal de la SDP.
* Dada la dinámica del entorno y los cambios organizacionales por los que está atravesando la entidad, es fundamental estar atentos a las actualizaciones de los mapas de riesgos una vez se produzcan cambios significativos en los procesos o sistemas.
* Dedicar los recursos necesarios para completar la actualización del mapa de riesgos, considerando los cambios en el proceso y las recomendaciones de la auditoría interna.
* Identificar, evaluar y mitigar los riesgos de manera proactiva.
* Documentar (mantener registro) de todo los pertinente a la gestión del riesgo.
* Realizar una evaluación de riesgos periódica para identificar nuevos riesgos y actualizar las medidas de seguridad.
* Implementar controles técnicos, administrativos y físicos para mitigar los riesgos identificados.
* Monitorear continuamente la eficacia de los controles y realizar ajustes según sea necesario.
* Evaluar la resiliencia de los sistemas y procesos ante posibles interrupciones o desastres naturales.
* Implementar mecanismos de autenticación multifactor y controles de acceso basados en roles en todos los sistemas para proteger la información confidencial.
* Simular ataques cibernéticos para identificar vulnerabilidades y evaluar la efectividad de los controles de seguridad.
* Proteger la información confidencial mediante el uso de algoritmos de encriptación fuertes.
* **Realizar copias de seguridad regulares y probar su restauración para g**arantizar la disponibilidad de la información en caso de incidentes**.**
* Mantener la capacitación y socialización regular a todos los funcionarios, contratitas y personal temporal de la SDP sobre temas de seguridad de la información, adaptando los contenidos a los roles y responsabilidades de cada uno.
* Continuar con la promoción de una cultura de seguridad a través de campañas de concientización y la participación de los funcionarios, contratitas y personal temporal de la SDP en programas de seguridad.
* Implementar el módulo de seguridad de la información en el software GETIONATE para permitir un mejor control y acceso a la información.
* Mantener un inventario actualizado de todos los activos de TI, incluyendo hardware, software y datos, para facilitar la gestión de riesgos y la respuesta a incidentes.
* Fortalecer los controles de acceso a las zonas restringidas, sistemas y datos, asegurando que solo el personal autorizado tenga acceso a la información necesaria.
* Desarrollar **Planes de recuperación ante desastres** detallados para restaurar los sistemas y datos en caso de un desastre.
* Implementar un esquema de clasificación de datos para identificar y proteger la información confidencial.
* Utilizar la encriptación para proteger los datos tanto en reposo como en tránsito.
* Establecer políticas de retención de datos para garantizar el cumplimiento legal y regulatorio. Crear un comité de seguridad de la información para supervisar la implementación de las medidas de seguridad y tomar decisiones estratégicas.
* Establecer acuerdos con otras instituciones para compartir información y mejores prácticas.

# 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).