SECRETARIA DISTRITAL DE DESARROLLO ECONOMICO 28-01-2026 08:25
Al Contestar Cite Este No.: 2026IE0001714 Fol:1 Anex:1 FA:11
ORIGEN 14000 OFICINA DE CONTROL INTERNO
DESTINO 10000 DESPACHO / MARIA CRISTINA DIAZ BELLO
ASUNTO INFORME FINAL DE EVALUACIÓN INDEPENDIENTE DEL DISEÑO
OBS

2026IE0001714

MEMORANDO

Referencia: **OCI 14000**

PARA: **MARÍA DEL PILAR LÓPEZ URIBE**
Secretaria de Despacho

DE: **DUMAR ERNESTO CARVAJAL CARRILLO**
Jefe Oficina de Control Interno

ASUNTO: Informe Final de Evaluación independiente del diseño y efectividad de las actividades de administración del riesgo en la SDDE.

Respetada Secretaria:

En desarrollo de las funciones a cargo de la Oficina de Control Interno y del Plan Anual de Auditoría vigencia 2026, me permito remitir el Informe del asunto que contiene el resultado del monitoreo a la gestión de riesgos (4to trimestre de 2025) del proceso TIC.

El detalle del análisis, así como las observaciones y recomendaciones realizadas por la Oficina de Control Interno sobre este asunto, se encuentran en el documento anexo.

Cordial saludo,

CARVAJAL CARRILLO DUMAR ERNESTO
Firmado digitalmente por CARVAJAL CARRILLO DUMAR ERNESTO
Fecha: 2026.01.27 15:29:11 -05'00'

DUMAR ERNESTO CARVAJAL CARRILLO
Jefe Oficina de Control Interno

C.C. Miembro del CICCI
Anexo: Informe Final de Evaluación independiente del diseño y efectividad de las actividades de administración del riesgo en la SDDE.

NOMBRE, CARGO O CONTRATO		FIRMA
Elaboró:	Angélica Liliana Rodríguez/OCI	ALRM

Nota: Por responsabilidad ambiental no imprima este documento. Cuida los recursos naturales, ahorra agua y energía.

1. INFORMACIÓN GENERAL DE LA EVALUACIÓN INDEPENDIENTE			
Evaluación del diseño y efectividad de las actividades de administración del riesgo en la SDDE.			
Fecha de Suscripción	31-enero-2026	**Equipo Evaluador**	Angélica Liliana Rodríguez
Objetivo General	Evaluar el cumplimiento de los lineamientos de monitoreo realizado parte de la primera línea de defensa a los riesgos de los procesos de la entidad durante el 4to trimestre de 2025, mediante la verificación de los lineamientos de la Política V7 y la Guía para el Diligenciamiento de la Matriz de Gestión de Riesgos 2024-V3 de la SDDE, con el fin de determinar la efectividad de los controles implementados por la entidad.		
Objetivo Específico	Comparar las evidencias relacionadas con el monitoreo de los riesgos de gestión, corrupción, Lavado de Activos, Financiamiento del Terrorismo y seguridad de la información, realizado por la primera línea de defensa establecidos en los lineamientos internos, con el fin de establecer la efectividad de los controles implementados por la entidad para mitigar la materialización de los riesgos.		
Criterios Evaluados	De acuerdo a lo establecido en el numeral "***5.6.1 Monitoreo"*** **de la Política de Administración de Riesgos de la SDDE** *"Una vez identificado, valorado y establecido el tratamiento de los riesgos de gestión, corrupción, fiscales, seguridad de la información y LA/FT (plan implementación), el líder del proceso junto con su equipo, realizará el monitoreo permanente y debe registrarlo como mínimo de manera trimestral, el avance de las acciones del plan de implementación frente a la zona residual resultante, la referencia a la continuidad y efectividad de los controles y si se materializó o no el riesgo…"*		
Alcance	Esta evaluación independiente comprende la revisión del monitoreo ejecutado por la primera línea de defensa sobre los riesgos de TIC, correspondiente al cuarto trimestre de 2025		
LIMITACIONES DE LA EVALUACIÓN INDEPENDIENTE			
Para enero de 2026 la Oficina de Control Interno no contó con el total del equipo de trabajo ocasionando una reducción del 66% en su capacidad de operación; razón por la cual, fue necesario reducir el alcance de la evaluación a los procesos estratégicos, frente a los cuales se prioriza para este seguimiento los riesgos del proceso TIC; sin embargo, los riesgos de los demás procesos serán evaluados durante la vigencia 2026.			

	SI		**NO**	**X**	**FECHA ENTREGA DEL PLAN DE MEJORAMIENTO A LA OCI**	No aplica

2. INFORME EJECUTIVO

Para verificar que el monitoreo de riesgos del proceso de **Gestión TIC** (realizado por la Primera Línea de Defensa en el último trimestre) cumpla con los lineamientos de la Política V7 y la Guía para el Diligenciamiento de la Matriz de Gestión de Riesgos de la SDDE del 2024 v3 de la SDDE, la OCI definió la siguiente metodología.

Metodología:

Al cierre de 2025, la entidad consolidó 58 riesgos y 104 controles en total. Para el seguimiento de la vigencia 2026, la OCI ha definido un periodo de transición para que todas las áreas y la Oficina de Planeación ajusten sus matrices a la nueva Guía DAFP v7. Durante este tiempo, también se busca que las oficinas integren las recomendaciones de las evaluaciones realizadas en el año

2025 por esta oficina. Por esta razón, el enfoque del año 2026 será verificar cómo la entidad monitorea los riesgos que ya tiene identificados.

Con el fin de organizar este trabajo, se establecieron criterios para elegir qué evaluar primero, lo que conllevo a seleccionar el Proceso Estratégico. De los cuatro procesos que lo componen (Planeación, Comunicaciones, Atención al Ciudadano y TIC), se decidió profundizar en el Proceso TIC, ya que es el único del grupo estratégico que tiene un riesgo de corrupción detectado, lo que lo vuelve prioritario.

En esa misma línea, para que la revisión sea más efectiva, se decidió enfocarnos en los riesgos cuyos controles son más críticos (calificados como altos o extremos). Al aplicar este filtro al Proceso TIC, se logró pasar de 7 riesgos reportados a los 3 de mayor impacto (R2, R3 y R7).

A continuación, se presentan los resultados obtenidos a la evaluación de monitoreo de los riesgos de Gestión, Corrupción y Seguridad de Información del proceso de Gestión Tic:

- Si bien la dependencia cumple con la periodicidad de monitoreo establecida en la Política y Guía de Administración de Riesgos, se identificó que los controles actuales implementados por la dependencia presentan deficiencias en su diseño, por lo que es necesario rediseñar estos hacia un enfoque preventivo, detectivo o correctivo garantizando que mitiguen de forma efectiva la materialización de los riesgos asociados al proceso.

- Se identificó que de los 4 controles evaluados 2 no cuentan con periodicidad y 4 no tienen establecido la evidencia, por lo cual no se cumplen con los criterios establecidos en el Literal C "*identificación y valoración de controles"* página 26 de la Guía para el Diligenciamiento de la Matriz de Gestión de Riesgos de la SDDE.

- Se observó que el objetivo registrado en la Matriz de Riesgos no está articulado con la caracterización oficial del proceso publicado en la intranet. Esta falta de alineación puede generar que los controles actuales no mitiguen efectivamente los riesgos reales del proceso.

ASPECTOS LOGRADOS

No se identificaron aspectos logrados.

FORTALEZAS

No se identificaron aspectos que representen valor agregado a la gestión en este asunto.

OPORTUNIDADES DE MEJORA

- Asegurar que las actividades de control se diseñen de manera adecuada, así mismo, que el seguimiento de los riesgos realizado por los líderes de proceso (1era línea de defensa) cuenten con soportes sólidos. El propósito es integrar la gestión de riesgos como un componente de apoyo a la toma de decisiones, que mediante alertas tempranas identifique amenazas potenciales y permita gestionar estos eventos con el fin de minimizar los impactos negativos.

- Dar cumplimiento a los lineamientos establecidos en el Literal C "*identificación y valoración de controles"* página 26 de la Guía para el Diligenciamiento de la Matriz de Gestión de Riesgos de la SDDE.

- Alinear el objetivo de la Matriz de Riesgos con la versión de la caracterización publicada en la intranet y revisar que los controles actuales sigan siendo útiles para minimizar la materialización del riesgo identificado.

- Brindar capacitación y recursos de apoyo a la 1era línea de defensa que les permitan identificar actividades de control (preventivas, detectivas o correctivas) y posibles desviaciones a tiempo. Esto nos ayudará a estandarizar el uso de la metodología en toda la institución, asegurando que cada proceso cumpla con los mejores estándares.

HALLAZGOS

No se identificaron aspectos que ameriten ser configurados como hallazgo, en desarrollo de la presente evaluación independiente.

CONCLUSIÓN

Al verificar el monitoreo de riesgos TIC, se concluye que el proceso aplica de manera parcial la Política Institucional y la Guía de administración de riesgos de la SDDE 2024, debido a que los controles no están diseñados adecuadamente y no cuentan con medios de verificación definidos, lo que impide validar su efectividad, así mismo, limita la evidencia a actividades de gestión operativa en lugar de medidas de mitigación. De mismo modo, la desconexión entre el objetivo de la matriz de riesgos y el establecido en la descripción del proceso (caracterización intranet), puede aumentar la posibilidad que los riesgos se materialicen al no estar alineados con los objetivos estratégicos de la dependencia.

3. INFORME DETALLADO DE LA EVALUACIÓN INDEPENDIENTE

La OCI evaluó el monitoreo de los riesgos gestión TIC, con el fin de determinar si la entidad cumple lo establecido en la Política y la Guía para el Diligenciamiento de la Matriz de Gestión de Riesgos de la SDDE del 2024, para lo cual definió la siguiente metodología:

La Oficina de Control Interno para el año 2026 determinó realizar el seguimiento al **"Monitoreo de Riesgos"**, considerando los siguientes criterios:

- Ante la actualización de los lineamientos institucionales bajo los estándares de la *"Guía para la Gestión Integral del Riesgo en Entidades Públicas v7 DAFP-2025"*, es necesario facilitar la transición técnica de la entidad. Lo anterior, con el fin de ejecutar una posterior reevaluación del diseño y efectividad de los controles frente al nuevo marco normativo.

- Teniendo como base la evaluación de diseño realizada en 2025, la entidad dispondrá de un término de transición en 2026 para la armonización de sus procesos con las sugerencias de la OCI. Este periodo es esencial para asegurar que la gestión de riesgos reportada por la Primera y Segunda Línea cuente con la solidez técnica necesaria y haya integrado efectivamente las recomendaciones propuestas para la optimización institucional.

- Evaluación de los riesgos institucionales por tipología, seleccionando para cada uno el control de mayor criticidad o impacto (alto o extremo).

Aplicados los criterios de evaluación, el Proceso Estratégico fue seleccionado para la siguiente fase de análisis. De sus cuatro componentes (Planeación Estratégica, Comunicaciones, Atención al Ciudadano y TIC), se determinó profundizar en el Proceso TIC, por ser el único dentro de este grupo que presenta un riesgo de corrupción identificado.

Bajo esta misma línea, la evaluación de los riesgos institucionales se ha segmentado priorizando aquellos controles con un nivel de criticidad calificado como alto o extremo. Al aplicar este filtro específicamente sobre el Proceso TIC, se logró una focalización estratégica que reduce los 7 riesgos reportados a los 3 riesgos de mayor impacto (R2, R3 y R7).

A continuación, se presenta la priorización realizada:

Muestra riesgo – Proceso TIC			
Tipología de Riesgo	**Riesgos**	**Controles**	**Riesgo Inherente**
GESTION	R2	1	ALTO
CORRUPCION	R3	2	ALTO
SEGURIDAD DE LA INFORMACION	R7	1	ALTO

Seguidamente, se presentan los resultados obtenidos de la evaluación de monitories de los riesgos de gestión, corrupción y seguridad de la información priorizados del proceso Gestión Tic:

3.1. OBJETIVO ESPECÍFICO 1

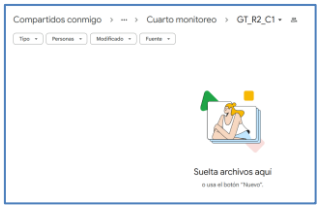
Comparar las evidencias relacionadas con el monitoreo de los riesgos de gestión, corrupción, LA/FT y seguridad de la información, realizado por la primera línea de defensa establecidos en los lineamientos internos, con el fin de establecer la efectividad de los controles implementados por la entidad para mitigar la materialización de los riesgos.

3.1.1 Resultados de la Prueba y Análisis.

La Oficina Asesora de Planeación informa que la matriz de riesgos del proceso Gestión TIC fue actualizada recientemente. Al respecto, queremos hacer un reconocimiento al esfuerzo y compromiso del área por mantener este instrumento al día. No obstante, es importante aclarar que dicha actualización no será objeto de análisis en esta instancia, toda vez que el seguimiento de la OCI debe realizarse sobre la versión formalizada y aprobada al momento del reporte. El monitoreo debe responder a la ejecución de controles sobre riesgos vigentes y no sobre actualizaciones en curso, por lo anterior se tomará la matriz de riesgos de TIC V2 publicada en la intranet.

Una vez realizada la evaluada al monitoreo de los Riesgos de Gestión, Corrupción y Seguridad de la Información del Proceso TIC reportados en la matriz de riesgos V2 de la vigencia 2025 y de acuerdo a la priorización de la OCI, se obtuvo el siguiente resultado:

Tabla 5. Prueba Análisis Gestión del Riesgo de los procesos de la SDDE.

Nombre del Proceso	**Gestión de TIC**				
Objetivo del Proceso GT-CPE - v8 30/06/2025	*"Formular lineamientos, políticas, planes y proyectos en materia de Gestión de TI, Seguridad de la Información y Transformación Digital. Así mismo generar e implementar soluciones de Sistemas de Información, seguridad de la información, redes y comunicaciones y en general toda la plataforma tecnológica que permitan proveer de forma oportuna y eficiente trámites y servicios a sus grupos de interés".*				
Objetivo del Proceso (Matriz Gestión del Riesgo)	*"Garantizar la disponibilidad de los Sistemas de Información, redes, comunicaciones y en general toda la plataforma tecnológica de la Secretaría, a través de la formulación, implementación de los planes estratégicos de las TICs para cada vigencia, propendiendo por el correcto funcionamiento tecnológico de la entidad".*				
Tipo de Riesgo	**Descripción del riesgo**	**Control**	**Evidencia del Monitoreo**	**Plan de manejo**	**Observación OCI**
Gestión	*GT_R2. Afectación Económica y Reputacional ocasionada por insatisfacción de los grupos de valor debido a implementación de software que no responda a las necesidades técnicas y/o funcionales de la entidad*	*"El profesional designado en el SIS verificará el correcto diligenciamiento del formato de Solicitud de Desarrollo de Software cada vez que se reciba una nueva solicitud. Esta verificación se realizará comparando el contenido de la solicitud contra una lista de verificación de criterios y requisitos establecidos previamente. El propósito de este control es asegurar que todas las solicitudes cumplan con los requisitos antes de proceder con el desarrollo. En caso de identificar novedades o desviaciones, se notificará de inmediato al líder del proceso para que realice los ajustes necesarios.* ***La evidencia del control será registrada y gestionada a través de la mesa de ayuda o correos electrónicos con el formato adjunto establecido para tal fin."***	*No se adjuntó evidencia*	*No se identificó el Plan de Manejo correspondiente a la vigencia 2025. El documento aportado registra fechas de cumplimiento que corresponden exclusivamente al periodo 2024, por lo que no es válido como evidencia para el año en curso*	Tener presente las recomendaciones realizadas por la OCI en el seguimiento realizado en la vigencia 2025, sobre el diseño de controles, ya que el control de este riesgo o mitiga la materialización del riesgo *"insatisfacción de los grupos de valor debido a implementación de software que no responda a las necesidades técnicas y/o funcionales de la entidad*", ya que el hecho de que un formato esté "bien diligenciado" no garantiza que la necesidad técnica o funcional esté resuelta. Para este control no se adjuntó evidencia:  Asimismo, se debe llevar a cabo una depuración de la matriz de riesgos para evaluar la pertinencia de aquellos controles que carecen de periodicidad definida o que su ejecución depende de la realización de una actividad, y analizar si estos deben ser eliminados por no aportar valor a la mitigación efectiva del riesgo. Se recomienda evaluar el control, así mismos definir formalmente los entregables esperados y periodicidad con el fin de asegurar que la evidencia sea una consecuencia directa y verificable de la ejecución del control.

Nombre del Proceso	**Gestión de TIC**				
Objetivo del Proceso GT-CPE - v8 30/06/2025	*"Formular lineamientos, políticas, planes y proyectos en materia de Gestión de TI, Seguridad de la Información y Transformación Digital. Así mismo generar e implementar soluciones de Sistemas de Información, seguridad de la información, redes y comunicaciones y en general toda la plataforma tecnológica que permitan proveer de forma oportuna y eficiente trámites y servicios a sus grupos de interés".*				
Objetivo del Proceso (Matriz Gestión del Riesgo)	*"Garantizar la disponibilidad de los Sistemas de Información, redes, comunicaciones y en general toda la plataforma tecnológica de la Secretaría, a través de la formulación, implementación de los planes estratégicos de las TICs para cada vigencia, propendiendo por el correcto funcionamiento tecnológico de la entidad".*				
Tipo de Riesgo	**Descripción del riesgo**	**Control**	**Evidencia del Monitoreo**	**Plan de manejo**	**Observación OCI**
Corrupción	*GT_R3. Afectación Económica y Reputacional ocasionada por incumplimientos normativos debido a Posibilidad de alteraciones, eliminación o uso indebido de información almacenada en repositorios digitales o sistemas institucionales, debido a acciones malintencionadas o errores de usuarios internos*	*"El designado en Gestión TIC gestiona el registro y cancelación de usuarios en el directorio activo, registrando cada acción en la mesa de ayuda conforme a demandas operativas. Este proceso garantiza el control de acceso y la seguridad de la información, siguiendo los procedimientos para paz y salvos.* ***La evidencia de cada operación se conserva en el sistema de mesa de ayuda, permitiendo una revisión eficaz y trazabilidad completa."***	*Matrices de: mesa de servicios y Bitácora de actividades del 4to trimestre de 2025*	*No se identificó el Plan de Manejo correspondiente a la vigencia 2025. El documento aportado registra fechas de cumplimiento que corresponden exclusivamente al periodo 2024, por lo que no es válido como evidencia para el año en curso*	Tener presente las recomendaciones realizadas por la OCI en el seguimiento realizado en la vigencia 2025, sobre el diseño de controles, ya que el control de este riesgo no mitiga la materialización del riesgo "*…alteraciones, eliminación o uso indebido de información almacenada en repositorios digitales o sistemas institucionales, debido a acciones malintencionadas o errores de usuarios internos*", ya que el control asegura que solo entren quienes deben estar, pero no controla qué hacen una vez adentro. Si un usuario interno activo tiene permisos de "administrador" o "escritura" en una carpeta que no le corresponde, puede borrar o alterar información legalmente, y este control no lo detectaría. Se realizó la verificación de las evidencias aportada, observando que las matrices de Mesa de Servicios y la Bitácora de Actividades del 4to trimestre de 2025, ambas matrices documentan correctamente el proceso de gestión de usuarios (solicitudes y ejecuciones). Sin embargo, estas actividades no mitigan efectivamente el riesgo de "alteración, eliminación o uso indebido de información". El control actual es de carácter administrativo (gestión de acceso), mientras que el riesgo reside en las acciones de los usuarios activos y externos. Por lo tanto, se debe definir un control efectivo para prevenir incidentes derivados de errores humanos o malas prácticas de personal con permisos vigentes. Asimismo, se debe llevar a cabo una depuración de la matriz de riesgos para evaluar la pertinencia de aquellos controles que carecen de periodicidad definida o que no

Nombre del Proceso	**Gestión de TIC**				
Objetivo del Proceso GT-CPE - v8 30/06/2025	*"Formular lineamientos, políticas, planes y proyectos en materia de Gestión de TI, Seguridad de la Información y Transformación Digital. Así mismo generar e implementar soluciones de Sistemas de Información, seguridad de la información, redes y comunicaciones y en general toda la plataforma tecnológica que permitan proveer de forma oportuna y eficiente trámites y servicios a sus grupos de interés".*				
Objetivo del Proceso (Matriz Gestión del Riesgo)	*"Garantizar la disponibilidad de los Sistemas de Información, redes, comunicaciones y en general toda la plataforma tecnológica de la Secretaría, a través de la formulación, implementación de los planes estratégicos de las TICs para cada vigencia, propendiendo por el correcto funcionamiento tecnológico de la entidad".*				
Tipo de Riesgo	**Descripción del riesgo**	**Control**	**Evidencia del Monitoreo**	**Plan de manejo**	**Observación OCI**
					registran ejecución anual, determinando si su ausencia realmente incrementa la exposición al riesgo o si deben ser eliminados por no aportar valor a la mitigación efectiva del proceso. Se recomienda evaluar el control, así mismos definir formalmente los entregables esperados y periodicidad con el fin de asegurar que la evidencia sea una consecuencia directa y verificable de la ejecución del control.
		"El profesional designado en la SIS es responsable de revisar y ajustar los derechos de acceso de los usuarios de forma trimestral para mantener actualizados los niveles de permisos. Los ajustes realizados se registran en el directorio activo. Este control se aplica para asegurar que los permisos de acceso sean congruentes con las necesidades operativas y los requerimientos de seguridad actuales. En caso de identificar novedades o desviaciones se notificará a la Subdirección SIS reforzando el monitoreo, ajuste de permisos y revisión de logs de auditoría que se tengan activos. ***La evidencia de los ajustes se mantiene dentro del directorio activo, facilitando la auditoría y seguimiento de cambios en los permisos de usuario."***	*Matrices de: mesa de servicios y Bitácora de actividades del 4to trimestre de 2025*		Tener presente las recomendaciones realizadas por la OCI en el seguimiento realizado en la vigencia 2025, sobre el diseño de controles. Se recomienda fortalecer este control con una revisión trimestral que incluya una confirmación o visto bueno de los jefes de área/líderes de proceso con el fin de garantizar que los derechos de acceso sean los permitidos o que esta verificación se realice contra algún documento que permita verificar que permiso tiene cada servidor. Se realizó la verificación de las evidencias aportada, observando que las matrices de Mesa de Servicios y la Bitácora de Actividades del 4to trimestre de 2025, ambas matrices documentan el proceso de gestión de usuarios (solicitudes y ejecuciones). Sin embargo, estas actividades no mitigan efectivamente el riesgo de "alteración, eliminación o uso indebido de información". Por lo tanto, se debe definir un control efectivo para prevenir incidentes derivados de errores humanos o malas prácticas de personal con permisos vigentes.

Nombre del Proceso	**Gestión de TIC**				
Objetivo del Proceso GT-CPE - v8 30/06/2025	*"Formular lineamientos, políticas, planes y proyectos en materia de Gestión de TI, Seguridad de la Información y Transformación Digital. Así mismo generar e implementar soluciones de Sistemas de Información, seguridad de la información, redes y comunicaciones y en general toda la plataforma tecnológica que permitan proveer de forma oportuna y eficiente trámites y servicios a sus grupos de interés".*				
Objetivo del Proceso (Matriz Gestión del Riesgo)	*"Garantizar la disponibilidad de los Sistemas de Información, redes, comunicaciones y en general toda la plataforma tecnológica de la Secretaría, a través de la formulación, implementación de los planes estratégicos de las TICs para cada vigencia, propendiendo por el correcto funcionamiento tecnológico de la entidad".*				
Tipo de Riesgo	**Descripción del riesgo**	**Control**	**Evidencia del Monitoreo**	**Plan de manejo**	**Observación OCI**
Seguridad de la información	*GT_R7. Pérdida de la disponibilidad del activo de información (equipos de comunicaciones) ocasionada por acceso no autorizado a la información debido a Fallas de los equipos*	*"El Administrador de Infraestructura es responsable de realizar, mensualmente, la revisión y aplicación de los parches de seguridad pertinentes en los sistemas operativos de los servidores y en las soluciones de seguridad perimetral, con el propósito de mantener los sistemas protegidos frente a posibles vulnerabilidades que puedan comprometer su operatividad. Este proceso se lleva a cabo evaluando la aplicabilidad de cada parche según las necesidades de los sistemas. En caso de detectar observaciones o desviaciones, como fallos en la instalación o incompatibilidades, se procede a su corrección inmediata a través de un rollback y, si es necesario, se escalará el problema al proveedor correspondiente.* ***La evidencia de cada revisión y parche aplicado, incluyendo fecha, hora, y sistemas actualizados****."*	captura de pantalla de un correo electrónico en el cual se informa sobre la realización de una ventana de mantenimiento	*No se identificó el Plan de Manejo correspondiente a la vigencia 2025. El documento aportado registra fechas de cumplimiento que corresponden exclusivamente al periodo 2024, por lo que no es válido como evidencia para el año en curso*	Tener presente las recomendaciones realizadas por la OCI en el seguimiento realizado en la vigencia 2025, sobre el diseño de controles. Se realizó la verificación de las evidencias aportada, observando que la evidencia adjunta (captura de pantalla de un correo electrónico), el cual informa sobre una ventana de mantenimiento programada para el 17 de septiembre de 2025. Dicha información no es coherente con el control establecido, ya que este determina que "*El Administrador de Infraestructura es responsable de realizar, mensualmente,* ***la revisión y aplicación de los*** *parches de seguridad pertinentes en los sistemas operativos de los servidores y en las soluciones de seguridad perimetral", es decir, que el soporte entregado no da cuenta de la ejecución de este control.* Se recomienda definir formalmente los entregables esperados para asegurar que la evidencia sea una consecuencia directa y verificable de la ejecución del control.

Así mismo, se identificó que el objetivo del proceso publicado en la intranet difiere del registrado en la matriz de riesgos. Esta falta de coherencia afecta la alineación estratégica, por lo cual se recomienda actualizar y unificar la documentación técnica. Es importante que el objetivo sea consistente en todas las herramientas institucionales para garantizar que los riesgos y controles estén correctamente orientados a mitigar los eventos de los procesos que puedan afectar el cumplimiento institucional; a continuación, se relacionan los pantallazo de los objetivos:

Objetivo caracterización: - Publicado en la Intranet

	Caracterización del Proceso	Fecha:	30 de julio de 2025
		Página:	Página 1 de 2
LIDER DEL PROCESO	Director de Gestión Corporativa - Subdirector de Informática y Sistemas		
OBJETIVO	Formular lineamientos, políticas, planes y proyectos en materia de Gestión de TI, Seguridad de la Información y Transformación Digital. Así mismo generar e implementar soluciones de Sistemas de Información, seguridad de la información, redes y comunicaciones y en general toda la plataforma tecnológica que permitan proveer de forma oportuna y eficiente tramites y servicios a sus grupos de interés.		

Objetivo – Matriz riesgos de corrupción - PE-P5-F2 – Publicado en la Página Web de la Entidad

	Proceso: Planeación Estratégica	Código:	PE-P5-F2
		Versión:	4
		Fecha:	30 de Enero de 2025
	Matriz de Riesgos de Corrupción Consolidada	Página:	Hoja 01 de 01
		Elaborado por:	Paola Andrea Pardo Cuervo Contratista Oficina Asesora de Planeación Juan Sebastián Junca Contratista Oficina Asesora de Planeación
		Revisado por:	Luz Mireya Alarcón Guevara Profesional Oficina Asesora de Planeación
		Aprobado por:	Luisa Fernanda Moreno Jefe Oficina Asesora de Planeación

A.IDENTIFICACIÓN DE RIESGOS	
Proceso	Objetivo del proceso
Gestion de TIC	Formular lineamientos, planes y estándares en materia de Gobierno Digital y Seguridad de la Información. Así mismo generar e implementar soluciones que permitan proveer de forma oportuna y eficiente los Sistemas de Información, redes y comunicaciones y en general toda la plataforma técnológica para la Secretaría.

Objetivo - Matriz de Gestión de Riesgos de Gestión y Corrupción - PE-P5-F1 – Publicada en la Intranet

	Proceso: Planeación Estratégica	Código:	PE-P5-F1
		Versión:	5
		Fecha:	20 de Agosto de 2024
	Matriz de Gestión de Riesgos de Gestión y Corrupción	Página:	Hoja 03 de 05
		Elaborado por:	Luz Mireya Alarcón Profesional Oficina Asesora de Planeación
		Revisado por:	Diego Alejando Constain Profesional Oficina Asesora de Planeación
		Aprobado por:	Luisa Fernanda Moreno Jefe Oficina Asesora de Planeación

PORTADA	
CONTEXTO DEL PROCESO	
PROCESO:	GESTIÓN TIC
OBJETIVO DEL PROCESO:	Garantizar la disponibilidad de los Sistemas de Información, redes, comunicaciones y en general toda la plataforma técnológica de la Secretaría, a traves de la formulacion, implementacion de los planes estrategicos de las TICs para cada vigencia, propendiendo por el correcto funcionamiento tecnologico de la entidad.

3.1.2 Aspectos logrados

No se identificaron.

3.1.3 Fortalezas

No se identificaron aspectos que representen valor agregado a la gestión en este asunto.

3.1.4 Oportunidades de mejora.

- Rediseñar los controles actuales para garantizar su efectividad frente a los riesgos detectados. Actualmente, la entidad registra en algunos casos actividades de gestión (tareas rutinarias) que no cumplen una función de control preventivo, detectivo o correctivo. Se deben establecer mecanismos que permitan monitorear y mitigar proactivamente las vulnerabilidades, más allá del flujo administrativo habitual.

- Dar cumplimiento a la metodología institucional para la identificación y valoración de controles, de acuerdo con lo estipulado en la Guía para el Diligenciamiento de la Matriz de Gestión de Riesgos (Literal C, pág. 26)

- Actualizar el objetivo de la Matriz de Riesgos institucional conforme a la documentación de la caracterización del proceso; asimismo, validar si los controles actuales mantienen su efectividad frente al nuevo planteamiento.

- Implementar sesiones de capacitación técnica y herramientas de seguimiento que permitan detectar inconsistencias de manera temprana, asegurando que la metodología institucional se aplique con rigor y calidad técnica en todas las dependencias.

3.1.5 Hallazgos

No se identificaron aspectos que ameriten ser configurados como hallazgo, en desarrollo de la presente evaluación independiente.

4. RECOMENDACIONES GENERALES

La Subdirección de Informática debe fortalecer el diseño de sus controles, pasando de registros administrativos hacia un esquema de monitoreo preventivo, detectivo o correctivo, asegurando que el control sea proporcional a la probabilidad de materialización del riesgo identificado.

Actualizar y estandarizar el objetivo del proceso en todos los instrumentos institucionales. La falta de coherencia detectada puede desviar el enfoque de los controles; por lo tanto, es necesario asegurar que tanto la documentación operativa (intranet) como la de gestión (riesgos) hablen el mismo lenguaje para mitigar los eventos que afecten el cumplimiento de meta

Se insta a la Oficina Asesora de Planeación, en su rol de Segunda Línea, a fortalecer los mecanismos de validación y supervisión de los reportes emitidos por la Primera Línea. Para ello, es fundamental implementar un programa de capacitación técnica continua y diseñar herramientas de monitoreo que permitan identificar y subsanar inconsistencias de forma proactiva. Estas acciones deben estar orientadas a garantizar que la metodología institucional se aplique con el rigor y la calidad técnica requeridos en todas las dependencias de la entidad

5. CONCLUSIONES GENERALES

Una vez realizada la evaluación al monitoreo de riesgos TIC se concluye que el proceso estratégico de TIC aplica parcialmente lo dispuesto en la Política y la Guía para el Diligenciamiento de la Matriz de Gestión de Riesgos de la SDDE del 2024, por cuanto se observó que el diseño de controles es deficiente; así mismo, las evidencias aportadas no dan cuenta de controles implementados sino de actividades de gestión.

Asimismo, se observó que el objetivo definido en la matriz de riesgos no se encuentra alineado con el objetivo de la caracterización (publicado en la intranet). Esta desconexión puede derivar en fallas de control, por lo cual es fundamental articular ambos elementos. Esto garantizará que los controles estén correctamente diseñados para mitigar los riesgos que realmente amenazan el cumplimiento de los objetivos institucionales.

Cordial saludo,

CARVAJAL CARRILLO DUMAR ERNESTO

Firmado digitalmente por CARVAJAL CARRILLO DUMAR ERNESTO
Fecha: 2026.01.27 15:27:34 -05'00'

DUMAR ERNESTO CARVAJAL CARRILLO
Jefe Oficina de Control Interno