

Fecha del informe	Día	27	Mes	02	Año	2026
--------------------------	------------	----	------------	----	------------	------

Nombre de la actividad	Informe de Evaluación y Seguimiento a la Gestión del Riesgo III cuatrimestre de 2025.
Objetivo del seguimiento	Evaluar de manera integral el estado de los riesgos de gestión y corrupción de los procesos determinados en la muestra de la Superintendencia Nacional de Salud durante el III Cuatrimestre de 2025. La evaluación se basará exclusivamente en la información publicada en la herramienta oficial ITS (Instrumento de Reporte Oficial), con el fin de identificar oportunidades de mejora y establecer una línea base que permita a los líderes de procesos priorizar acciones de mejora.
Alcance	Periodo comprendido entre el 1 de septiembre al 31 de diciembre de 2025 (III cuatrimestre de 2025)
Criterios normativos	<p>Ley 87 del 29 de noviembre de 1993 - Objetivos del Sistema de Control Interno. Decreto 648 de 2017. Artículo 2.2.21.5.3 - Roles de la Oficina de Control Interno. Decreto 1499 de 2017. Capítulo 2 - Políticas de Gestión y Desempeño Institucional.</p> <ul style="list-style-type: none"> • Decreto 1080 de septiembre de 2021 – Artículo 10. Funciones de la Oficina de Control Interno. • Guía rol de las unidades u oficinas de Control Interno, auditoría interna o quien haga sus veces. v3 - 2023. • Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. V7 – 2025, emitida por el DAFP. • Manual Operativo – Modelo Integrado de Planeación y Gestión – (MIPG). v6 -2024. - Dimensión de Control Interno. <p>Ley 1712 de 2014 - Transparencia y Derecho de Acceso a la Información Pública. Políticas Institucionales asociadas al SIG, DEFT13, v1 del 20.06.2023.</p> <ul style="list-style-type: none"> • Manual de Administración del Riesgo - DEMN02, v4 del 15.01.2025. • Política para la Administración del Riesgo - DEPI01, v1 del 15.01.2025.
Tabla de contenido	<p>Contenido</p> <p>1. INFORME 2</p> <p> 1.1. Introducción..... 2</p> <p> 1.2. Metodología..... 2</p> <p>2. DESARROLLO DE LA EVALUACIÓN 4</p> <p> 2.1. Riesgos de Gestión..... 4</p> <p> 2.2. Riesgos de Corrupción..... 10</p> <p> 2.3. Evaluación de Riesgos en Relación con los Hallazgos de la Contraloría General de la República..... 18</p> <p>3. HALLAZGOS..... 22</p> <p> 3.1. Hallazgos 22</p> <p> 3.2. Observaciones..... 22</p> <p>CONCLUSIONES 24</p>
Equipo auditor	<ul style="list-style-type: none"> • Luis Eduardo Perdomo Londoño – Profesional Especializado OCI • Pablo Vergara Gómez – Profesional Especializado OCI

1. INFORME

1.1. Introducción

La Oficina de Control Interno, como garante y facilitador de una cultura de integridad y gestión efectiva de riesgos en cumplimiento de las funciones asignadas en la Ley 87 de 1993 y demás normas aplicables, y en atención a su rol de Evaluación de la Gestión del Riesgo busca proporcionar un aseguramiento objetivo a la Alta Dirección sobre el diseño y efectividad de las actividades de administración de Riesgo que la entidad ejecutó para el III Cuatrimestre de 2025 (septiembre – diciembre) buscando orientar a la entidad a asegurar que los riesgos claves o estratégicos sean adecuadamente identificados y gestionados, lo que finalmente debe repercutir en la operación y eficacia del Sistema de Control Interno de la Entidad. Este informe pretende informar a la alta dirección la necesidad de tomar decisiones y acciones, que permitan la priorización y mejora de la gestión del riesgo institucional para que sean fortalecidos los mecanismos de prevención (controles) en coherencia con el compromiso de crear valor público y salvaguardar la confianza ciudadana.

1.2. Metodología

La Oficina de Control Interno, en observancia a los roles establecidos en el Decreto 648 de 2017, “*Artículo 2.2.21.5.3, “Artículo 2.2.21.5.3. De las oficinas de control interno: Las Unidades u Oficinas de Control Interno o quien haga sus veces desarrollarán su labor a través de los siguientes roles: liderazgo estratégico; enfoque hacia la prevención, evaluación de la gestión del riesgo, evaluación y seguimiento, relación con entes externos de control”* comunica a la alta dirección información relevante frente a la evaluación de la gestión del riesgo para el período comprendido entre el 1 de septiembre al 31 de diciembre de 2025 (III cuatrimestre 2025), para lo cual se tuvo como base de análisis, los siguientes documentos:

- Mapa de Riesgos Institucional consolidado y actualizado para los riesgos de Gestión, Corrupción y Fiscales el 21.07.2025, y riesgos de Seguridad y Privacidad de la Información con fecha de actualización y publicación en página web de la Entidad el 14.03.2025.
- Mapa de Riesgos v2 dispuesto en el aplicativo de Gestión ITS actualizado el 21.07.2025.
- Políticas Institucionales asociadas al Sistema Integrado de Gestión - SIG (código DEFT13 – v1) publicada el 20.06.2023.
- Manual de Administración del Riesgo (código DEMN02 – v5), publicado el 27.11.2025.
- Política para la Administración del Riesgo DEPI01 – v1 publicada el 15.01.2025.

Es así, que del universo de procesos con los que cuenta la Superintendencia Nacional de Salud, se identifican quince (15), los cuales están debidamente publicados en la página web de la entidad con vigencia 2025, el equipo responsable del seguimiento, por parte de la Oficina de Control Interno (OCI), tomará como muestra los riesgos para el presente informe enmarcado en las siguientes reglas:

1. No se evaluarán los riesgos de los procesos asociados a Auditorias ejecutadas en la vigencia 2025 ya que estos procesos ya fueron evaluados, estos son:

- Gestión Jurisdiccional y de Conciliación.
- Gestión de Mejora.
- Gestión Financiera.
- Gestión de Bienes y Servicios.
- Relacionamiento con la Ciudadanía y Grupos de Valor.
- Control.

2. No se evaluarán los riesgos de los procesos que fueron revisados en el Informe de Seguimiento a Riesgos del primer y segundo cuatrimestre de 2025, efectuado por la Oficina de Control Interno. Los procesos evaluados fueron:

- Proceso Gestión Jurídica.
- Gestión Estratégica de Personas.
- Actuaciones Disciplinarias.

3. No se evaluará el proceso de Evaluación Independiente.

4. Se evaluarán los riesgos que durante la evaluación del riesgo inherente antes de los controles encuentran zona extrema y los riesgos corrupción de los procesos no evaluados durante la vigencia 2025 en otros informes realizados por la Oficina de Control Interno. Estos procesos son:

- Direccionamiento Estratégico.
- Seguimiento y evaluación al vigilado.
- Auditorías.
- Gestión de Trámites.
- Gobierno y Gestión de Datos e Información.

Dada la publicación de la nueva Guía para la Administración del Riesgo y el diseño de controles en entidades públicas. V7 – 2025, emitida por el DAFP en noviembre de 2025 y la actualización del documento Manual de Gestión Integral del Riesgo V5 de noviembre de 2025 de la Superintendencia Nacional de Salud, en orientación al mejoramiento de la construcción de los Mapas de Riesgos de Riesgo, en el informe se evaluarán los siguientes aspectos:

- **Identificación y descripción del Riesgo:** En este aspecto se evaluará si los riesgos están redactados de forma clara y precisa el evento negativo, la causa inmediata y la causa raíz. La escritura adecuada para una descripción del riesgo, debe indicar lo siguiente: “Evento no deseado (¿qué puede pasar?) + circunstancia inmediata (¿cómo ocurre?) + causa raíz (¿por qué ocurre?)”.
- **Diseño y análisis de controles.** Las actividades de control deben diseñarse como acciones concretas y con atributos específicos que permitan identificar el responsable (¿Quién ejecuta el control?), la acción con un verbo irregular que indique la acción de control (¿qué hace el control?) y complementarse con los atributos informativos y de formalización del control (documentación, frecuencia, evidencia y otros datos de ejecución) ¿Cómo se aplica el control?
- **Valoración del Riesgo Residual.** En este aspecto se evaluará la efectividad de los controles sobre como su ejecución afecta la Probabilidad o el Impacto del Riesgo. Se evalúa la efectividad de los controles cuando de manera positiva los controles logran reducir la probabilidad y el impacto del riesgo, de lo contrario se determina que el control es no efectivo. En este aspecto el presente informe evaluara a través de la observación si hay efectividad de los controles implementados por el proceso
- **Plan de implementación de Controles (Tratamiento):** Se deberán formular un plan de acción para implementar controles o para mejorar los controles existentes cuando estos no tienen afectación significativa en la probabilidad e impacto del riesgo. Estas acciones buscan Reducir, Compartir, Aceptar o Evitar el riesgo. Por lo tanto, en esta evaluación revisará si el diseño de dichas acciones busca implementar un control o mejorarlo y si con ello se atacan la causa raíz identificada.

Finalmente, con este análisis se indica que para el presente análisis se tomaron como muestra quince (15) riesgos identificados por los procesos mencionados así:

RIESGOS			
No	Proceso	No de Riesgos de Gestión	No de Riesgos de Corrupción
		Zona de Riesgo Extrema	
1	Direccionamiento Estratégico	0	1
2	Seguimiento y Evaluación al Vigilado	0	1
3	Auditorías	0	2
4	Gestión de Trámites	0	3
5	Gobierno y Gestión de Datos e Información	4	4
Total		4	11

Fuente: Elaboración Propia – Basada en la Mapa de Riesgos v2 dispuesto en el aplicativo de Gestión ITS actualizado el 21.07.2025.

Para esta evaluación no se incluirá, el análisis a los riesgos Fiscales y tampoco los riesgos de Seguridad y Privacidad en la Información, los cuales se encuentran en proceso de construcción por parte de la entidad.

2. DESARROLLO DE LA EVALUACIÓN

A continuación, se refleja el análisis, evaluación y seguimiento a la gestión de riesgos de la entidad, correspondiente al tercer cuatrimestre de la vigencia 2025, con base en la metodología descrita en punto 1.2 de este informe, enfocando el análisis a cuatro (4) riesgos de gestión y once (11) riesgos de corrupción definidos en los procesos “Direccionamiento Estratégico; Seguimiento y Evaluación al Vigilado; Auditorías; Gestión de Trámites y Gobierno y Gestión de Datos e Información”, cuyo resultado de la revisión y análisis, arrojó la siguiente información.

2.1. Riesgos de Gestión

De acuerdo a la muestra objeto de este seguimiento y con base a la metodología señalada en el punto 1.2 del presente informe, en la siguiente tabla se ilustran los procesos de la muestra, el número de los riesgos de gestión que durante la evaluación del riesgo inherente antes de los controles encuentran zona Extrema, con los criterios seleccionados para este análisis y, los Planes de Tratamiento asociados a estos riesgos, cuyo fin es verificar la efectividad de los controles y la pertinencia de las acciones desarrolladas que mitiguen la probabilidad de que se materialicen dichos riesgos. Es así como, se determina que para el periodo (septiembre – diciembre 2025) se analizaron y evaluaron cuatro (4) riesgos de gestión así:

Proceso para evaluar	No. de Riesgos de Gestión	Zona de Riesgo Inherente	Zona de Riesgo Residual	Planes de Tratamiento
Gobierno y Gestión de Datos e Información	4	Extrema (4)	Extrema (4)	N° 1804 N° 1932 N° 1931 N° 1800

Tabla 1: Fuente propia OCI – Información extraída del mapa de **Riesgos de Gestión** aplicativo de gestión ITS actualizado el 06.01.2025.

De acuerdo con la información registrada en el Sistema de Información ITS sobre el Mapa de Riesgos de Gestión, y considerando el proceso de actualización que deben realizar dichos mapas frente a la emisión de la nueva Guía para la Gestión Integral del Riesgo en Entidades Públicas, Versión 7 - 2025, se realizó un análisis en el marco del Rol Estratégico de la Oficina de Control Interno, para lo cual se presenta el siguiente análisis:

Proceso Gobierno y Gestión de Datos e Información:

No	Código del riesgo	Riesgos	Descripción del Control	Análisis de la Oficina de Control Interno	Plan de Tratamiento
1	DIPR01-7	Posibilidad de afectación reputacional por fallas en la operación tecnológica de la entidad, debido a indisponibilidad de la infraestructura tecnológica o del servicio suministrado por un tercero, por falta de seguimiento o monitoreo, salvo incumplimientos por fuerza mayor debidamente certificados	<p>Control No 1: Los profesionales asignados para realizar las labores de seguimiento a las actividades ejecutadas por los proveedores, de acuerdo con la operación, realizan verificación quincenal de los casos registrados en la herramienta de gestión CA, validando la oportunidad en la atención de los casos, para que estos no superen el porcentaje de incumplimiento permitido en los contratos. En caso de detectar fallas en el cumplimiento de los tiempos, se le indica dicha situación al proveedor que aplique a través de correos electrónicos y/o comunicación oficial y si sobrepasa el tiempo máximo establecido será penalizado sobre los Acuerdos de Niveles de Servicio -ANS pactados. Evidencias: Reportes C.A; informes mensuales de proveedores; reportes de excel de seguimiento de casos en CA (sabana de casos Mesa de servicio) e Informes de supervisión donde se valida el cumplimiento de los Acuerdos de Nivel de Servicio (ANS).</p> <p>Control No 2: Los profesionales de la Subdirección asignados para estas actividades realizan las actividades de monitoreo preventivo de: servidores, verificación de actualizaciones de los Sistemas Operativos; bases de datos; redes; control de ejecución de backups de Sistemas, DB, correo electrónico y OneDrive; monitoreo a las herramientas de trendMicro y Fortinet y Defender 365; y efectuara el registro del seguimiento en la bitácora de seguimiento. En caso de detectar fallas en alguno de estos servicios se deberá escalar al proveedor para que efectue los ajustes a que haya lugar, monitoreando el cumplimiento de los Acuerdos de Nivel de Servicio -ANS; si sobrepasa el tiempo máximo establecido, será penalizado sobre los Acuerdos de Nivel de Servicios ANS pactados de acuerdo con las cláusulas contractuales. Evidencias: Bitácoras de Monitoreo (servidores, sistemas operativos, bases de datos, redes, control de ejecución de backups, TrendMicro, Fortinet y Defender 365); informes mensuales de proveedores, correos electrónicos en caso de requerirse.</p>	<p>A continuación, se presenta la evaluación efectuada por parte de la OCI al riesgo DIPR01-7:</p> <ul style="list-style-type: none"> Identificación y descripción del Riesgo: En este aspecto no es claro si la causa raíz del riesgo corresponde a la tercerización de la operación tecnológica o a la falta de seguimiento o monitoreo. Así mismo en la redacción se permite excepciones en las cuales se materializa las fallas en la operación. Es posible que en el análisis del riesgo se requiera revisar que la afectación no solo es reputacional, sino también operativa. Diseño y análisis de controles. Respecto a los dos controles diseñados para este riesgo se observó lo siguiente: <ul style="list-style-type: none"> El Control No. 1 presenta deficiencias en su redacción y conceptualización, ya que no se identifica claramente la acción principal mediante un verbo fuerte, lo que dificulta comprender su propósito y alcance. Aunque se clasifica como preventivo, se sugiere revisar esta tipología, dado que la intervención ocurre cuando los casos ya están registrados en la herramienta de gestión CA, lo que indica que la falla tecnológica se ha materializado, acercándolo más a un control detectivo. Además, el texto menciona múltiples acciones (verificación de cumplimiento del proveedor, revisión de casos en CA, aplicación de penalizaciones), sin precisar cuál es la actividad central ni cómo se articula con la mitigación de la causa raíz del riesgo. Estas faltas de claridad afectan la trazabilidad, la evaluación de efectividad y la alineación con la metodología de riesgos. Para el control No 2 del riesgo, presenta problemas de claridad y definición. Aunque se describe como monitoreo preventivo de infraestructura tecnológica, la redacción es extensa y no define con precisión la acción principal mediante un verbo fuerte, lo que dificulta comprender su alcance. Además, no se especifica la frecuencia exacta del monitoreo, lo que limita la trazabilidad y la evaluación de efectividad. Si bien se clasifica como preventivo, se sugiere revisar esta tipología, dado que algunas actividades (como la verificación de backups y escalamiento de fallas) se ejecutan cuando el problema ya se ha presentado, lo que las acerca a controles detectivos. Finalmente, se mencionan múltiples acciones (monitoreo de servidores, bases de datos, redes, herramientas de seguridad), sin indicar cuál es la actividad central ni cómo se articula con la mitigación de la causa raíz del riesgo. Valoración del riesgo residual: Respecto a la valoración del riesgo residual, se evidencia que los controles diseñados no se pueden considerar efectivos, dado que no reducen significativamente la probabilidad ni el impacto del riesgo identificado. Esta situación indica una brecha en el diseño y la implementación de los controles, lo que impide su contribución real a la mitigación del riesgo. En consecuencia, se recomienda revisar el diseño de los controles, asegurando que estén alineados con la causa raíz del riesgo, cuenten con atributos completos (responsable, acción, frecuencia, evidencia, ejecución) y se evalúe la posibilidad de incorporar mecanismos automáticos y segregación de funciones para mejorar su efectividad. <p>Lo anterior se evidencia dado que en la evaluación del riesgo inherente la probabilidad se calificó como Muy Alta y el impacto Catastrófico y esta calificación después de evaluados los controles se mantiene por lo cual no se reduce la probabilidad y el impacto en la valoración del riesgo residual. Asimismo, se recomienda revisar el esquema de valoración del riesgo inherente, verificando que la asignación de la probabilidad y del impacto se realice conforme a los criterios técnicos definidos por la entidad, especialmente aquellos relacionados con la frecuencia real de exposición y con los umbrales de afectación económica y reputacional. Esto permitirá asegurar que la calificación del riesgo inherente refleje de manera objetiva el comportamiento del proceso y se encuentre plenamente alineada con la metodología institucional.</p> <ul style="list-style-type: none"> Plan de Tratamiento: El plan de tratamiento 1804 carece de especificidad y trazabilidad, lo que limita su efectividad para reducir el riesgo residual. Se recomienda definir acciones concretas orientadas a la causa raíz, establecer plazos y mecanismos de seguimiento concretos que permitan ver la implementación o mejora de controles. 	1804

No	Código del riesgo	Riesgos	Descripción del Control	Análisis de la Oficina de Control Interno	Plan de Tratamiento
2	DIPR01-10	Posibilidad de afectación reputacional por quejas, denuncias o solicitudes, debido a la publicación de información o datos imprecisos, desactualizados o inoportunos de la gestión de la Entidad	<p>Control No 1: El profesional encargado cada vez que recibe una solicitud valida el cumplimiento de los tiempos mínimos establecidos para la gestión verifica que el contenido de la información este completo y adicionalmente que dicha solicitud, esté aprobada por el jefe del área o profesional encargado. Evidencia: correo electrónico.</p> <p>Control No 2: Los profesionales encargados realizan cuatrimestralmente una revisión de los contenidos del sitio web, según los lineamientos establecidos en el Manual de Publicación de Contenidos del sitio Web y de ser necesario se generan alertas mediante correo electrónico a las áreas responsables cuando se identifique información desactualizada. Evidencia correo electrónico.</p>	<p>A continuación, se presenta la evaluación efectuada por parte de la OCI al riesgo DIPR01-10:</p> <ul style="list-style-type: none"> • Identificación y descripción del Riesgo: Respecto con lo indicado en la guía, se sugiere revisar la estructura de la redacción toda vez que puede no diferenciarse claramente el evento del impacto: "afectación reputacional" corresponde al impacto, mientras que "quejas, denuncias o solicitudes" se formulan como si fueran parte del evento, cuando en realidad son consecuencias o manifestaciones del riesgo. Adicionalmente la circunstancia inmediata es poco precisa, se menciona la "publicación de información o datos imprecisos, desactualizados o inoportunos", pero no se indica en qué momento del proceso ocurre o en que medio o sistema pudiendo ser amplio el espectro a controlar, es importante revisar los hechos que han ocurrido para enfocar el riesgo en esos elementos. Lo anterior puede generar también que la causa raíz no sea adecuadamente identificada o que se identifiquen múltiples causas. Por tal razón se recomienda revisar la identificación del riesgo para que este cuente con la estructura y su gestión pueda ser más eficaz. • Diseño y análisis de controles. Respecto a los dos controles diseñados para este riesgo se observó lo siguiente: Para el control No 1 del Riesgo: Se sugiere revisar su redacción para dar claridad sobre la situación del control que tipo de solicitud se debe validar y verificar, así como aclarar el propósito principal del control para entender de manera precisa como mitiga la causa raíz del riesgo. Es importante tener clara la situación del control para ser más específico sobre el rol del profesional encargado y la dependencia que lo ejecuta ya que puede ser muy amplia esta definición no identificándose quien es el responsable. Podría mejorarse la descripción de otros atributos del control aclarando la frecuencia formal de ejecución, indicarse la documentación donde se indica como se ejecuta el control, el nivel de automatización del control. Es importante revisar si la evidencia (correo electrónico) es fácilmente trazable por personas ajenas a quien ejecuta el control. Para el control No 2 del Riesgo: Se sugiere revisar la acción de control toda vez que se menciona realizar revisión y generar alertas no permitiendo determinar con claridad cual es la acción del control. Es importante determinar cómo se ejecuta la acción de control, si por ejemplo se esta se hace de manera particular a un elemento o se efectúa a todo el contenido de la página web. Importante determinar si el control esta definido en algún un procedimiento asociado al mantenimiento de la Página Web o si esta acción se articula algún 	1932

No	Código del riesgo	Riesgos	Descripción del Control	Análisis de la Oficina de Control Interno	Plan de Tratamiento
			<p>Control No 3: El profesional encargado válida cada vez que se recibe una solicitud, que la información esté completa en cuanto al grupo al que va dirigida la solicitud, que se quiere comunicar, cómo se quiere comunicar y cuándo se quiere comunicar para adelantar el proceso de comunicación. De ser necesario solicitará a través de correo electrónico información adicional al área para continuar con la gestión de la solicitud, en caso de no recibirla se devolverán. Evidencia: correo electrónico</p>	<p>elemento de control del Esquema de Publicación de la Página Web de la Entidad. Actualmente como se encuentra diseñado el control se entiende que es un control detectivo de la materialización de los riesgos. Es importante se evalúa si un correo electrónico garantiza la trazabilidad y la formalidad del control. Es importante verificar si este control se ejecuta de forma manual o automatizada. En la definición del control no es claro el medio o mecanismo a través del cual se aplica el control.</p> <p>Para el control No 3 del Riesgo: Se sugiere revisar la redacción de la acción principal del riesgo aclarando los elementos que se validan, de qué tipo de solicitud, aclarando si está asociada a un formato o un documento del sistema de gestión. Aunque se designa o se menciona el cargo del profesional que ejecuta la actividad sería importante aclarar si este rol este asignado formalmente dentro de la dependencia. Aunque se define la frecuencia por cada evento, sería adecuado se defina si existe una periodicidad de supervisión importante determinar si este control está incluido dentro de los procedimientos del proceso. No es claro si este control es manual, automática o híbrido. Aunque el control intenta prevenir errores en la solicitud, realmente actúa después del envío por lo que se considera un control detectivo y no preventivo. Importante determinar si se requiere establecer mejoras al control para que este pueda atacar las causas raíz identificadas. Así mismo, es importante cuando se habla de validar determinar cuáles son los criterios medibles que se validan y diseñar una herramienta adecuada para el fin de la validación.</p> <p>Para el control No 4 del Riesgo: Se sugiere revisar la redacción del riesgo, puede mejorarse la claridad de la acción del control para que pueda ser entendido como está mitiga las causas, la redacción parece la descripción de un proceso y no de una acción específica de control. Adicionalmente no es claro un único responsable de la acción, no se define quien hace qué dentro de la redacción. Cuando se menciona las metodologías establecidas por la entidad, esta redacción es amplia y podría ser ambigua para quien ejecute el control, pudiendo reemplazarse por mencionar un Manual, Procedimiento, Instrumento o documento que contenga el método de verificación. Cuando se indica registrarán el seguimiento en el mismo instrumento interno, no se logra identificar cual es el instrumento y como poderlo identificar y dar trazabilidad. No se indica si el control es manual, automático o híbrido.</p>	
			<p>Control No 4: El Subdirector de analítica y el profesional encargado, cada vez que recibe una solicitud de publicación de datos e información de inspección, vigilancia y control, realizarán las verificaciones de acuerdo con las metodologías establecidas por la entidad, antes de entregar a la dependencia solicitante y registrarán el seguimiento en el instrumento interno.</p>	<ul style="list-style-type: none"> • Valoración del riesgo residual: Respecto a la valoración del riesgo residual, se evidencia que los controles diseñados redujeron la probabilidad de ocurrencia en lo valorado, sin embargo estos no reducen el impacto del riesgo el cual se mantiene en Zona Extrema. Esta situación indica una brecha en el diseño y la implementación de los controles, lo que impide su contribución real a la mitigación del riesgo. En consecuencia, se recomienda revisar el diseño de los controles, asegurando que estén alineados con la causa raíz del riesgo, cuenten con atributos completos (responsable, acción, frecuencia, evidencia, ejecución) y se evalúe la posibilidad de incorporar mecanismos automáticos y segregación de funciones para mejorar su efectividad. Lo anterior se evidencia dado que en la evaluación del riesgo inherente la probabilidad se calificó Muy Alta y el impacto Catastrófico y esta calificación después de evaluados los controles redujo la probabilidad a Muy Bajo sin embargo el impacto se mantiene en la valoración del riesgo residual manteniéndose la zona de riesgo Extrema. Asimismo, se recomienda revisar el esquema de valoración del riesgo inherente, verificando que la asignación de la probabilidad y del impacto se realice conforme a los criterios técnicos definidos por la entidad, especialmente aquellos relacionados con la frecuencia real de exposición y con los umbrales de afectación económica y reputacional. Esto permitirá asegurar que la calificación del riesgo inherente refleje de manera objetiva el comportamiento del proceso y se encuentre plenamente alineada con la metodología institucional. • Plan de Tratamiento Las acciones del Plan de Tratamiento 1932 están enfocadas en acciones de capacitación, socialización y mesa de trabajo para el mejoramiento del proceso (cumplidas al 100% a 31 de diciembre de 2025), se deberá evaluar el impacto de estas acciones sobre la causa raíz del riesgo identificado. Se sugiere revisar la creación de acciones para la implementación de nuevos controles o el mejoramiento de controles existentes orientadas a atacar la causa raíz, establecer plazos y mecanismos de seguimiento concretos que permitan ver la implementación o mejora de controles. 	

No	Código del riesgo	Riesgos	Descripción del Control	Análisis de la Oficina de Control Interno	Plan de Tratamiento
3	DIPR01-11-1	Posibilidad de afectación económica, reputacional, disciplinaria por pérdida de competencia en el trámite, debido al Incumplimiento en la gestión de notificación, comunicación y publicación de los Actos Administrativos.	Control No 1: Verificar por parte del coordinador o funcionario encargado de hacer seguimiento semanalmente a la gestión de los actos administrativos en la base de datos de notificaciones, validando que las actuaciones se hayan tramitado en los tiempos establecidos y surtiendo las tareas ordenadas en cada uno de los actos. En caso de observar una falla o incumplimiento se solicitará el ajuste correspondiente. Evidencia: Sistema de Gestión, Superargo.	<p>A continuación, se presenta la evaluación efectuada por parte de la OCI al riesgo DIPR01-11-1:</p> <ul style="list-style-type: none"> Diseño y análisis de controles. Respecto al control diseñado para este riesgo se observó lo siguiente: <p>Para el control No 1 del riesgo: Se sugiere mejorar la redacción respecto a los criterios que se verifican o validen del proceso para que el control sea comprensible. No existe una designación precisa del funcionario que ejecuta la acción, no determinándose el rol de cada uno dentro del control. Aunque se indica que la frecuencia es semanalmente no se precisa la forma en como se aplica el mecanismo, tampoco los medios que se utilizan y si este documentado en un procedimiento del proceso. Es importante aclarar cual es la evidencia específica de la aplicación del control no precisa si es un formato, un informe u otro instrumento radicado en la herramienta Superargo y almacenado en un expediente. No se identifica si el control es manual, automático o híbrido. Este control puede ser del tipo detectivo ya que identifica aquellos actos que fueron tramitados con algún defecto o incumplimiento, para lo cual también es importante determinar los criterios con los que se determina su no cumplimiento.</p> Valoración del riesgo residual: Respecto a la valoración del riesgo residual, se evidencia que el control diseñado no es suficiente, dado que, aunque reduce la probabilidad no permite reducir la probabilidad al nivel más bajo y no genera reducción del impacto del riesgo identificado. En consecuencia, se recomienda revisar el diseño del control existente y de nuevos controles, asegurando que estén alineados con la causa raíz del riesgo, cuenten con atributos completos (responsable, acción, frecuencia, evidencia, ejecución) y se evalúe la posibilidad de incorporar mecanismos automáticos y segregación de funciones para mejorar su efectividad. Lo anterior se evidencia dado que en la evaluación del riesgo inherente la probabilidad se calificó Media y el impacto Catastrófico y esta calificación después de evaluados los controles redujo la probabilidad a Baja sin embargo el impacto se mantiene en Catastrófico para la valoración del riesgo residual manteniendo la zona de riesgo. Asimismo, se recomienda revisar el esquema de valoración del riesgo inherente, verificando que la asignación de la probabilidad y del impacto se realice conforme a los criterios técnicos definidos por la entidad, especialmente aquellos relacionados con la frecuencia real de exposición y con los umbrales de afectación económica y reputacional. Esto permitirá asegurar que la calificación del riesgo inherente refleje de manera objetiva el comportamiento del proceso y se encuentre plenamente alineada con la metodología institucional. Plan de Tratamiento Las acciones del Plan de Tratamiento 1932 cuenta con dos acciones: 1. Retroalimentar a las áreas, en el cumplimiento de los tiempos establecidos para envío de actos administrativos y 2 Realizar seguimiento de la sistematización del procedimiento, al área encargada. Estas acciones presentan un avance del 0% y se encuentran vencidas a fecha del informe se debieron cumplir a 31 de diciembre de 2025. Se debe revisar las razones por las cuales no se han podido ejecutar estas actividades. Igualmente sugiere revisar la creación de acciones concretas para la implementación de nuevos controles o el mejoramiento de controles existentes orientadas a atacar la causa raíz, establecer plazos y mecanismos de seguimiento concretos que permitan ver la implementación o mejora de controles. 	1931
4	DIPR01-11-2	Posibilidad de afectación reputacional por No conformidades o hallazgos identificados en las auditorías internas y/o externas, debido a la gestión y/o uso inadecuado de las herramientas de seguridad de la información existentes en la entidad.	Control No 1: El profesional asignado para esta actividad realiza monitoreo diario del comportamiento de las herramientas de seguridad con el fin de identificar alertas, validar el comportamiento de los módulos implementados e identificar y evaluar futuras opciones de implementación, con el fin de minimizar el riesgo de ataques cibernéticos. Del identificarse fallas, uso inadecuado o desactualización de la herramienta se escalará al proveedor de las mismas, con el fin de realizar las actualizaciones a nuevas versiones pertinentes y gestionar el plan de acción a seguir. Evidencias:	<p>A continuación, se presenta la evaluación efectuada por parte de la OCI al riesgo DIPR01-11-2:</p> <ul style="list-style-type: none"> Identificación y descripción del Riesgo: Se sugiere revisar la descripción del riesgo, siendo importante evaluar si el evento que se quiere atacar está asociado a las No conformidades o hallazgos identificados por terceros que puede ser una consecuencia de un evento superior como la materialización de ciberataques a los sistemas administrados por la Superintendencia Nacional de Salud. Así mismo sería importante determinar si la circunstancia está asociada a una acción operativa como el uso inadecuado o desactualizado de herramientas o si este riesgo podría tener como circunstancia una acción estratégica que planifique acciones a largo plazo de configuración, operación y mantenimiento que permitan garantizar la seguridad de la información de la entidad asociados a la continuidad administrativa de las tareas de seguridad. El riesgo 	1800

No	Código del riesgo	Riesgos	Descripción del Control	Análisis de la Oficina de Control Interno	Plan de Tratamiento
			Informe trimestral y semestral de la gestión, monitoreo y afinamiento de implementación de las herramientas y futuras opciones de implementación.	<p>actualmente descrito no incluye la descripción de la causa raíz por la cual existe un uso inadecuado de las herramientas. Por tal razón se recomienda revisar la identificación del riesgo para que este cuente con la estructura y su gestión pueda ser más eficaz</p> <ul style="list-style-type: none"> Diseño y análisis de controles. Respecto al control diseñado para este riesgo se observó lo siguiente: <p>El control no es claro respecto a la acción principal debido a que la redacción tiene una mezcla de acciones que impiden entender con precisión la acción, la redacción del control puede ser muy extensa y descriptiva. Es importante mencionar que el control no explica cómo se ejecuta de manera integral el monitoreo o como a través de él se activa unas alertas y el control de fallas. Por lo que en general el control debe ser corto preciso y medible. Respecto a otro ámbito del control, aunque se dice profesional asignado no se define de manera precisa el rol de quien lo ejecuta, lo que en relación con la frecuencia de la actividad da la responsabilidad a este profesional de ejecutar el monitoreo diario, pero no se determina si la frecuencia de las otras actividades con claridad. Es importante indicar si el control está definido en algún documento y si el mencionado control tiene una ejecución manual, automática o híbrida. Si el control es diario la evidencia debiera tener la misma periodicidad y no trimestral o semestral como se indica.</p> <p>En consecuencia, se recomienda revisar el diseño de los controles, asegurando que estén alineados con la causa raíz del riesgo, cuenten con atributos completos (responsable, acción, frecuencia, evidencia, ejecución) y se evalúe la posibilidad de incorporar mecanismos automáticos y segregación de funciones para mejorar su efectividad.</p> Valoración del riesgo residual: Respecto a la valoración del riesgo residual, se evidencia que el control diseñado no es suficiente, dado que, aunque reduce la probabilidad no permite reducir la probabilidad al nivel más bajo y no genera reducción del impacto del riesgo identificado. En consecuencia, se recomienda revisar el diseño del control existente y de nuevos controles, asegurando que estén alineados con la causa raíz del riesgo, cuenten con atributos completos (responsable, acción, frecuencia, evidencia, ejecución) y se evalúe la posibilidad de incorporar mecanismos automáticos y segregación de funciones para mejorar su efectividad. Lo anterior se evidencia dado que en la evaluación del riesgo inherente la probabilidad se calificó Alta y el impacto Catastrófico y esta calificación después de evaluados los controles redujo la probabilidad a Media sin embargo el impacto se mantiene en Catastrófico para la valoración del riesgo residual manteniendo la zona de riesgo. Asimismo, se recomienda revisar el esquema de valoración del riesgo inherente, verificando que la asignación de la probabilidad y del impacto se realice conforme a los criterios técnicos definidos por la entidad, especialmente aquellos relacionados con la frecuencia real de exposición y con los umbrales de afectación económica y reputacional. Esto permitirá asegurar que la calificación del riesgo inherente refleje de manera objetiva el comportamiento del proceso y se encuentre plenamente alineada con la metodología institucional. Plan de Tratamiento <p>Las acciones del Plan de Tratamiento 1800 cuenta con dos acciones: 1. Gestionar la transferencia de conocimiento sobre el manejo de las herramientas de seguridad y 2. Gestionar la contratación del Recurso Humano requerido para responder a los retos y demandas de la entidad en temas relacionados con Seguridad de la Información (cumplidas al 100% a 31 de diciembre de 2025), se deberá evaluar el impacto de estas acciones sobre la causa raíz del riesgo identificado ya que ninguna de las dos actúa directamente sobre el punto crítico del proceso: la configuración, operación y mantenimiento de las herramientas de seguridad, estas acciones son necesarias pero no suficientes; mitigan parcialmente la causa raíz, pero no modifican el comportamiento de la herramienta ni el proceso.</p> <p>Igualmente sugiere revisar la creación de acciones concretas para la implementación de nuevos controles o el mejoramiento de controles existentes orientadas a atacar la causa raíz, establecer plazos y mecanismos de seguimiento concretos que permitan ver la implementación o mejora de controles.</p> 	

Tabla 2: Fuente propia OCI – Información extraída del mapa de **Riesgos de Gestión** aplicativo de gestión ITS

2.2. Riesgos de Corrupción

De acuerdo a la muestra objeto de este seguimiento y con base a la metodología señalada en el punto 1.2 del presente informe, en la siguiente tabla se ilustran los procesos seleccionados, el número de riesgos de corrupción identificados en las zonas inherentes y residual, con los criterios seleccionados para este análisis y, los Planes de Tratamiento asociados a estos riesgos, cuyo fin es evaluar la identificación de riesgos, descripción del riesgo y la pertinencia de los controles diseñados para mitigar la probabilidad de que se materialicen dichos riesgos. Es así como, se tomaron para análisis y evaluación dos (2) riesgos de corrupción así:

Proceso para evaluar	No. de Riesgos de Corrupción	Zona de Riesgo Inherente	Zona de Riesgo Residual	Planes de Tratamiento
Auditorías	2	Extrema	Extrema	1722/1723
Gestión de trámites	2	Extrema	Extrema	1791/1792
Direccionamiento estratégico	1	Extrema	Extrema	1774
Seguimiento y evaluación al vigilado	1	Extrema	Extrema	1727
Proceso Gobierno y Gestión de Datos e Información:	4	Extrema	Extrema	1908 1797 1796 1907

Proceso Auditorías

No	Código del Riesgo	Riesgos	Descripción del Control	Análisis de la Oficina de Control Interno	Plan de Tratamiento
1	ATPR01-1	Posibilidad de recibir o solicitar cualquier dádiva o beneficio, a nombre propio o de un tercero para alterar el Programa de Auditoría	El líder del proceso de auditoría trimestralmente consolida la información remitida por las delegaturas frente al avance de ejecución del programa de auditorías. En caso de presentar cambios en la programación estos serán debidamente justificados por el área responsable. Evidencia: Memorando de traslado al despacho	<p>• Identificación y descripción del Riesgo: El riesgo “Posibilidad de recibir o solicitar cualquier dádiva o beneficio, a nombre propio o de un tercero para alterar el Programa de Auditoría” se identifica correctamente como Soborno Entrante en el marco de riesgos de corrupción/integridad pública.</p> <p>De esta manera, la Guía No. 7 del DAFP, establece que la siguiente estructura: Posibilidad de [impacto] por [causa inmediata] [...], a causa de [causa raíz], lo cual sería un aspecto de mejora en la estructuración del riesgo.</p> <p>• Diseño y análisis de controles: El control propuesto, mitiga adecuadamente el riesgo de soborno en el Programa de Auditoría, pero requiere ajustes estructurales conforme a la Guía No. 7 DAFP para optimizar su efectividad en el mapa de riesgos. Para ello, se recomienda que incorpore aspectos relacionados en dicha guía como: Especificar si es preventivo, detectivo o correctivo y si los controles son de tipo automático o manual. Del mismo modo, no se especifica la periodicidad de la ejecución del control; así mismo no se define si el registro con el cual se llevará a cabo la actividad.</p>	1723

No	Código del Riesgo	Riesgos	Descripción del Control	Análisis de la Oficina de Control Interno	Plan de Tratamiento
				<ul style="list-style-type: none"> • Valoración del riesgo residual: Se identifica que el riesgo residual mantiene su condición “extrema”. Esto indica que las actividades de mitigación del riesgo no permiten que se disminuya dicha calificación, ocasionando su probabilidad de ocurrencia. Por lo anterior se recomienda que se incrementen controles preventivos adicionales. • Plan de Tratamiento: Se identifica que en el plan descrito En la herramienta ITS, se adelantó las siguientes actividades: Jornada de fortalecimiento en el ejercicio auditor desde la mirada de control interno. <p>Se recomienda fortalecer el plan de tratamiento del riesgo, ya que sus actividades actuales se limitan a capacitaciones, reuniones y socializaciones transitorias, sin incorporar mecanismos permanentes que garanticen continuidad y efectividad en la mitigación del riesgo de corrupción.</p>	
2	ATPR01-2	Posibilidad de recibir o solicitar cualquier dádiva o beneficio, a nombre propio o de un tercero para alterar u omitir los hallazgos de auditoría	El coordinador de auditoría emite visto bueno del informe de auditoría garantizando que los papeles de trabajo y las evidencias recopiladas se encuentren de manera completa y guarden coherencia con los hallazgos formulados en el informe. En el caso que se identifique que los papeles de trabajo y las evidencias recopiladas no guardan coherencia con los hallazgos, verificará con el equipo auditor según sea el caso, realizar los ajustes que correspondan. Evidencias: Correo electrónico con la aprobación del informe de auditoría.	<ul style="list-style-type: none"> • Diseño y análisis de controles: El control descrito busca mitigar riesgos de corrupción en la emisión de informes de auditoría mediante la revisión de coherencia entre evidencias y hallazgos. Basado en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP (v7 de 2025), este control presenta fortalezas en prevención, pero requiere mejoras en estructura, atributos y evidencia para alinearse plenamente con los lineamientos metodológicos • Valoración del riesgo residual: El riesgo residual mantiene su condición “extrema”. Esto indica que las actividades de mitigación del riesgo no permiten que se disminuya dicha calificación, ocasionando su probabilidad de ocurrencia. Por lo anterior se recomienda que se incrementen controles preventivos adicionales. • Plan de Tratamiento: Se planteó la misma actividad del plan No. 1723. Se reitera igualmente la recomendación: fortalecer el plan de tratamiento del riesgo, ya que sus actividades actuales se limitan a capacitaciones, reuniones y socializaciones transitorias, sin incorporar mecanismos permanentes que garanticen continuidad y efectividad en la mitigación del riesgo de corrupción. 	1722

Proceso Gestión de Trámites

No	Código del Riesgo	Riesgos	Descripción del Control	Análisis de la Oficina de Control Interno	Plan de Tratamiento
1	TRPR01-1	Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio para alterar los tiempos, las condiciones o requisitos mínimos del trámite del vigilado, o de cualquier otra acción de supervisión	El Director realizará trimestralmente la verificación del estado de los trámites, en caso de identificar fallas en las actuaciones del profesional designado para el trámite, se actuará de acuerdo a lo establecido por la Oficina de Talento Humano de la Entidad y a la oficina de Control Interno. Evidencias: Reporte trimestral de estado de trámites asignados. Correo o acta que evidencie el seguimiento del estado de los trámites, aclarando si se identificaron presuntas fallas.	<ul style="list-style-type: none"> • Identificación y descripción del Riesgo: El riesgo es parcialmente adecuado al identificar un evento de corrupción (soborno entrante en trámites de supervisión), pero incompleto en su estructura según la Guía No. 7 del DAFP, que exige incluir impacto, causa inmediata y causa raíz para una formulación precisa • Diseño y análisis de controles: El diseño del control es parcialmente adecuado según la Guía No. 7 del DAFP: tiene responsable, frecuencia y evidencias, pero presenta debilidades en tipología, alineación con el riesgo de corrupción y precisión del procedimiento. No menciona como se efectuará la “verificación del estado de los trámites” puesto que se aborda de manera genérica sin explicar cómo se hace la verificación: (cruces, criterios, fuentes de información, umbrales de alerta), como lo establece la Guía No. 7 del DAFP. • Valoración del riesgo residual: El riesgo residual mantiene su condición “extrema”. Esto indica que las actividades de mitigación del riesgo no permiten que se disminuya dicha calificación, ocasionando su probabilidad de ocurrencia. Por lo anterior se recomienda que se incrementen controles preventivos adicionales. 	1792

No	Código del Riesgo	Riesgos	Descripción del Control	Análisis de la Oficina de Control Interno	Plan de Tratamiento
				<ul style="list-style-type: none"> • Plan de Tratamiento: La actividad que se planteó para darle tratamiento de mejora fue: <i>Realizar seguimiento trimestral al cumplimiento de los tiempos establecidos en el proceso, con el fin dar respuesta oportuna a las solicitudes presentadas por los vigilados.</i> Se identificó en el seguimiento “incumplimiento” en registros, lo cual permite la materialización del riesgo. En este caso, debe considerarse declarar “inefectivo” el plan de tratamiento al riesgo de acuerdo con lo observado. 	
2	TRPR01-2	Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros para favorecer la selección de profesionales para hacer parte del listado de agentes interventores, liquidadores y contralores de la Superintendencia Nacional de Salud.	El profesional asignado valida el cumplimiento de requisitos de los aspirantes a cargos de agentes interventores, liquidadores y contralores en el marco de la convocatoria que la Entidad desarrolle para tal fin. En caso de detectar algún incumplimiento rechaza la solicitud de inscripción al Registro de Interventores, Liquidadores y Contralores - RILCO, según el reglamento de la convocatoria. Evidencia: Reporte de la convocatoria (análisis de las hojas de vida presentadas en la convocatoria).	<ul style="list-style-type: none"> • Identificación y descripción del Riesgo: El riesgo está bien identificado como soborno entrante en procesos de selección de agentes, pero su descripción es incompleta según la Guía No. 7 del DAFP, al omitir impacto, causa inmediata y causa raíz en la estructura obligatoria. • Diseño y análisis de controles: El control está bien orientado como control preventivo frente al riesgo de corrupción en la etapa de selección, pero su diseño es incompleto según los atributos que exige la Guía No. 7. El control es genérico; puesto que no se describen criterios, documentos fuente, cruces (por ejemplo, con listas de sanciones, antecedentes, inhabilidades), ni doble revisión, lo que deja ventanas para arbitrariedad o errores en un proceso crítico de alto riesgo de corrupción. • Valoración del riesgo residual: El riesgo residual mantiene su condición “extrema”. Esto indica que las actividades de mitigación del riesgo no permiten que se disminuya dicha calificación, ocasionando su probabilidad de ocurrencia. Por lo anterior se recomienda que se incrementen controles preventivos adicionales. • Plan de Tratamiento: El plan fue declarado como efectivo con la siguiente observación: <i>“aunque la evidencia aportada, no está alineada con la actividad, al verificar la estrategia para la constitución del nuevo registro, se evidenció la ejecución de los espacios de capacitación a través de podcast...”</i>. De esta manera, se identifica que se efectuó el cierre de la actividad con un registro diferente de cumplimiento, lo cual debió devolverse la actividad o en su defecto declararla como “inefectiva”. 	1791
3	TRPR01-3	Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros para favorecer la selección de profesionales para hacer parte de la terna presentada al Comité de Medidas Especiales como promotor en los Acuerdos de Reestructuración de Pasivos que apruebe la Superintendencia Nacional de Salud.	El profesional responsable verifica los antecedentes de los profesionales a presentarse al Comité de Medidas Especiales como promotores en los Acuerdos de Reestructuración de Pasivos, aprobados por la Superintendencia Nacional de Salud. En caso de detectar algún incumplimiento dará aviso al Director de Medidas Especiales para Prestadores de Servicios de Salud para definir si se busca otro promotor del listado de la Superintendencia de Sociedades. Evidencia: Correo electrónico que contiene el resultado de la revisión de antecedentes	<ul style="list-style-type: none"> • Diseño y análisis de controles: El diseño del control es adecuado en enfoque preventivo para mitigar riesgos de corrupción en temas de promotores, pero incompleto en atributos clave como tipología, frecuencia y evidencia robusta según la Guía No. 7 del DAFP. De esta manera, no declara si es preventivo/detectivo/correctivo ni manual/automático, elementos obligatorios para evaluar eficacia en mapa de riesgos de corrupción. • Valoración del riesgo residual: El riesgo residual mantiene su condición “extrema”. Esto indica que las actividades de mitigación del riesgo no permiten que se disminuya dicha calificación, ocasionando su probabilidad de ocurrencia. Por lo anterior se recomienda que se incrementen controles preventivos adicionales. • Plan de Tratamiento: El plan de tratamiento fue evaluado como “efectivo”, teniendo en cuenta que para atender el Plan de Mejoramiento, se concentró la actividad en adelantar capacitaciones, socializaciones o fortalecimiento, de esta manera, no se vinculan controles clave como declaraciones juramentadas de no dádivas, cruces de inhabilidades o supervisión independiente de temas; no define responsable, frecuencia ni plazos, incumpliendo requisitos de planes de tratamiento. 	1790

Proceso Direccionamiento Estratégico

No	Código del Riesgo	Riesgos	Descripción del Control	Análisis de la Oficina de Control Interno	Plan de Tratamiento
1	DEPR01-1	Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros para alterar, modificar, manipular la elaboración, actualización, eliminación o aprobación de metodologías, lineamientos o instrumentos de supervisión	El Subdirector (a) de Metodologías e Instrumentos de Supervisión verifica que la elaboración y seguimiento de la metodología o instrumento de supervisión esté a cargo de un equipo interdisciplinario de funcionarios, y en el caso que se requiera de las otras dependencias de la Dirección de Innovación y Desarrollo-DID serán requeridas mediante correo electrónico. Evidencia: correo electrónico o memorando	<ul style="list-style-type: none"> • Identificación y descripción del Riesgo: El riesgo está correctamente identificado como soborno entrante en la elaboración de herramientas de supervisión, pero su descripción es incompleta al no seguir la estructura completa de la Guía No. 7 del DAFP (impacto, causa inmediata y raíz) • Diseño y análisis de controles: El control busca mitigar soborno mediante equipos interdisciplinarios en metodologías de supervisión, pero su diseño es parcial según la Guía No. 7 del DAFP, faltando atributos clave como tipología, frecuencia y evidencia detallada. • Valoración del riesgo residual: El riesgo residual mantiene su condición "extrema". Esto indica que las actividades de mitigación del riesgo no permiten que se disminuya dicha calificación, ocasionando su probabilidad de ocurrencia. Por lo anterior se recomienda que se incrementen controles preventivos adicionales. • Plan de Tratamiento: Se adelantaron las siguientes actividades: <ol style="list-style-type: none"> 1-Estructurar micrositio donde se dispongan las metodologías e instrumentos de supervisión. 2-Adelantar seguimiento a los proyectos en curso, en los espacios de reunión de autoevaluación de la Dirección de Innovación y Desarrollo. El cierre de la actividad fue declarado como "efectivo", y cumplió con la totalidad de las actividades programadas. Del mismo modo, las actividades se diseñaron conforme a las causas que generaron el plan. 	1774

Proceso Gobierno y Gestión de Datos e Información:

No	Código del riesgo	Riesgos	Descripción del Control	Análisis de la Oficina de Control Interno	Plan de Tratamiento
1	DIPR01-1	Posibilidad de recibir o solicitar cualquier dádiva o beneficio a terceros con el fin de extraer, modificar, cargar o eliminar información de una base de datos a favor de un vigilado.	Control No 1 Cada vez que se recepcione un requerimiento de acceso a las Bases de Datos o los sistemas de información, será escalada al Subdirector de Tecnologías de la Información, para que defina la autorización de acceso; el profesional de la Subdirección de Tecnologías de la Información, previa aprobación dará cumplimiento a la solicitud y concederá los permisos requeridos; en caso contrario se informa al usuario que requiere el servicio que no procede la solicitud. Evidencias: Casos registrados en la herramienta de gestión CA	<p>A continuación, se presenta la evaluación efectuada por parte de la OCI al riesgo DIPR01-1:</p> <ul style="list-style-type: none"> • Identificación y descripción del Riesgo: Se sugiere revisar la descripción del riesgo, el evento agrupa cuatro acciones (extraer, modificar, cargar, eliminar) esto lo hace poco específico, podría limitar el análisis y la identificación de otras situaciones que generan el riesgo. El texto de la descripción del riesgo no precisa donde sucede la conducta, por ejemplo, inadecuada gestión de identidades y accesos, administración de roles y permisos en las bases de datos o implementación parcial o deficiente de herramientas. Por último, resulta superficial en el análisis causal al mencionar solo la "posibilidad de recibir dádivas" como causa inmediata, sin profundizar en las condiciones estructurales que la habilitan —como debilidades en la segregación de funciones, el modelo de autorización o la arquitectura de seguridad—, aspectos esenciales para una correcta gestión de riesgos según las mejores prácticas. • Diseño y análisis de controles: Respecto a los tres controles diseñados para este riesgo se observó lo siguiente: 	1908

No	Código del riesgo	Riesgos	Descripción del Control	Análisis de la Oficina de Control Interno	Plan de Tratamiento
			<p>Control No 2 El profesional asignado para realizar las labores de monitoreos de usuarios y permisos en bases de datos misionales y Sistemas Operativos, debe generar Informe mensual del resultado de monitoreo. En caso de detectar accesos no autorizados, se debe requerir inmediatamente el bloqueo de acceso y escalar la solicitud para que se efectue la investigación correspondiente. EVIDENCIAS: Informe mensual del resultado de monitoreo, registros en la herramienta de gestión CA, correo electrónico y comunicación interna en caso de requerirse investigación.</p> <p>Control No 3. El profesional asignado para realizar la habilitación del Sistema de Recepción, Validación y Cargue para las "Retransmisiones", la cual es habilitada en base de datos por la Subdirección de Tecnologías de la Información STI, descarga el formato Excel con la información de la lista en SharePoint creada por la Subdirección de Análítica para tal fin y únicamente dispondrá el sistema para aquellas entidades que fueron autorizadas a la retransmisión de acuerdo con el registro realizado para cada delegatura en donde la retransmisión se encuentre en estado aprobado. En caso de recibir solicitudes por otro medio deberá informar al usuario con copia al jefe inmediato que requiere el servicio que no procede la solicitud. Evidencias: Excel descargado de la lista de SharePoint con las retransmisiones aprobadas y tramitadas durante el semestre; en caso de requerirse, correos electrónicos donde se evidencie la no procedencia de la solicitud</p>	<p>Para el control del riesgo No 1. Se ha definido un flujo de autorización jerárquico para el acceso a bases de datos, lo cual es adecuado para riesgos de corrupción; sin embargo, la descripción carece de precisión sobre elementos esenciales del diseño: criterios formales de autorización, niveles de privilegio permitidos, verificación de identidad del solicitante, mecanismos automáticos de registro y validaciones previas antes de otorgar el acceso. Tampoco se distingue con claridad la causa raíz que busca mitigar el control (la concentración o mal uso de privilegios) ni se evidencia si el responsable cuenta con capacidad técnica y autoridad suficiente, aspectos obligatorios en controles de integridad. El control tampoco especifica frecuencia, fuentes de información confiable, ni cómo se dejan evidencias verificables, lo que limita su trazabilidad y dificulta evaluar su efectividad. En suma, aunque la lógica del control es pertinente, su diseño es incompleto frente a los criterios metodológicos establecidos para controles preventivos en riesgos de corrupción.</p> <p>Para el Control del Riesgo No 2 Este se orienta a vigilar accesos y permisos, lo cual es congruente con la naturaleza del riesgo; sin embargo, la Guía exige que el control especifique acciones, herramientas y fuentes de información confiables, y en este caso la descripción no menciona si el monitoreo se realiza mediante sistemas automatizados, bitácoras, reportes de auditoría o revisiones manuales. Adicionalmente, el control no identifica qué parámetros definen una alerta, ni cómo se analizan desviaciones, ni el procedimiento formal cuando se identifican accesos indebidos. El diseño tampoco aclara la segregación de funciones, un requisito clave para riesgos de integridad, ya que el mismo encargado de monitorear podría ser quien administra permisos, lo cual debilita la independencia del control. Finalmente, falta información sobre evidencias, periodicidad garantizada, y mecanismos de verificación independiente, por lo que, aunque es un control necesario, no está descrito con el nivel de detalle que exige la metodología para considerarlo completo.</p> <p>Para el Control del Riesgo No 3 se identifica una verificación operativa respecto a qué entidades están autorizadas para realizar retransmisiones; sin embargo, desde el enfoque de la Guía, la descripción se centra en el procedimiento y no en la lógica del control, dejando vacíos sobre los criterios de validación, mecanismos de autenticación de origen de la información, calidad de los datos revisados, y dependencia del operador que ejecuta el cargue. El riesgo DIPR01-1 está asociado a manipulación deliberada de datos, pero el control no explica cómo mitiga esa causa raíz, pues se enfoca en la fuente de la solicitud y no en los riesgos de alteración, manipulación interna o colusión. Falta también precisar responsabilidades, nivel de autoridad del ejecutor, parámetros de revisión, y cómo se deja evidencia estructurada del análisis, todos ellos elementos exigidos para controles de integridad según la Guía. En consecuencia, aunque el control es pertinente para el proceso, su diseño no cumple plenamente con los atributos formales que permiten considerarlo un control robusto frente a riesgos de corrupción.</p> <p>• Valoración del riesgo residual: Aunque los controles establecidos reducen marginalmente la probabilidad del riesgo, el riesgo residual permanece en zona extrema, evidenciando que el diseño actual del control no logra mitigar adecuadamente las causas raíz, especialmente aquellas relacionadas con consolidación de privilegios, ausencia de protección estructural y alta dependencia de autorizaciones manuales. Desde la perspectiva de Control Interno, la permanencia del riesgo en niveles máximos sugiere que el control es insuficiente y que la entidad sigue altamente expuesta a manipulaciones intencionales de la información. Lo anterior se evidencia dado que en la evaluación del riesgo inherente la probabilidad se calificó Improbable y el impacto Catastrófico y esta calificación después de evaluados los controles no redujo la probabilidad y tampoco el impacto para la valoración del riesgo residual manteniendo la zona de riesgo. Asimismo, se recomienda revisar el esquema de valoración del riesgo inherente, verificando que la asignación de la probabilidad y del impacto se realice conforme a los criterios técnicos definidos por la entidad, especialmente aquellos relacionados con la frecuencia real de exposición y con los umbrales de afectación económica y reputacional. Esto permitirá asegurar que la calificación</p>	

No	Código del riesgo	Riesgos	Descripción del Control	Análisis de la Oficina de Control Interno	Plan de Tratamiento
				<p>del riesgo inherente refleje de manera objetiva el comportamiento del proceso y se encuentre plenamente alineada con la metodología institucional.</p> <ul style="list-style-type: none"> • Plan de Tratamiento: La acción definida en el Plan de Tratamiento No 1908 tiene valor de sensibilización, pero no ataca la causa raíz del riesgo (accesos indebidos y privilegios excesivos). No es una acción de control sino de articulación, y carece de indicadores que permitan evaluar su efecto. Según la Guía, las acciones del plan de tratamiento deben estar alineadas directamente con el riesgo y su causa raíz; por lo cual el impacto real de la acción de mitigación es bajo. 	
2	DIPR01-2	Posibilidad de recibir o solicitar cualquier dádiva o beneficio para ocultar o alterar la documentación análoga y/o electrónica en las diferentes fases de su ciclo de vida que esté bajo custodia en el Archivo de gestión de las dependencias y en el Archivo Central.	El profesional asignado de cada dependencia- verifica, cada vez que se requiera, la completitud, integridad y disponibilidad del expediente dado en préstamos (análogo o digital) a los funcionarios y es registrado en el formato de control de préstamos y en el repositorio del GGD. En caso de encontrar inconsistencia se levanta un acta y se remite al líder de proceso y al coordinador de gestión documental para tomar las acciones pertinentes. Adicionalmente el profesional designado del Grupo de Gestión Documental realiza seguimiento a todas las dependencias para verificar el cumplimiento de este lineamiento. Evidencia: Formato de control de préstamos, Repositorio e Informe.	<p>A continuación, se presenta la evaluación efectuada por parte de la OCI al riesgo DIPR01-2:</p> <ul style="list-style-type: none"> • Identificación y descripción del Riesgo: El riesgo está identificado en términos amplios al señalar que podrían recibirse dádivas para alterar documentación en diferentes fases del ciclo de vida del archivo. No obstante, la descripción presenta ambigüedades frente a los elementos que las metodologías de riesgos exigen: el evento no deseado no está plenamente diferenciado de la circunstancia inmediata, y la causa raíz no se enuncia con claridad. Por ejemplo, “ocultar o alterar la documentación” describe el resultado, pero no especifica qué condiciones institucionales habilitan dicho acto (falta de controles de integridad documental, ausencia de clasificación de activos, debilidades en trazabilidad, entre otros). El impacto señalado —“reconstrucción de documentos”— refleja una consecuencia operativa más que un impacto de nivel institucional, lo cual desbalancea la descripción frente al estándar metodológico de impacto económico y reputacional. En resumen, la identificación es correcta en intención, pero la descripción requiere depuración para separar evento, causa inmediata, causa raíz e impacto, tal como recomiendan los lineamientos. • Diseño y análisis de controles: Para el control definido para el Riesgo DIPR01-2 Este control atiende de forma directa el evento no deseado del riesgo, pero su diseño no desarrolla los elementos que exige la Guía para controles de integridad. No se describe cómo se realiza la verificación, qué estándares de integridad se aplican, ni cuáles son las fuentes confiables para comparar la información. La ausencia de lineamientos sobre evidencia mínima, periodicidad y parámetros objetivos para determinar inconsistencias reduce su efectividad y dificulta su evaluación. Además, el control no identifica con claridad la relación entre la actividad ejecutada y la causa raíz del riesgo (débil trazabilidad documental), lo que limita su alineación metodológica. Por estas razones, aunque pertinente, el control está formulado de manera incompleta. • Valoración del riesgo residual: La valoración muestra que el riesgo residual se mantiene en zona extrema, lo que revela que las acciones de verificación documental, aunque son útiles, mitigando la probabilidad de actos deliberados de ocultamiento o alteración. Se observa que los controles son predominantemente reactivos y manuales, sin abordar debilidades estructurales como la trazabilidad, la custodia documental y la protección de archivos sensibles, lo cual explica por qué el riesgo permanece prácticamente intacto tras aplicar el control, se sugiere revisar la posibilidad de implementar controles para mitigar el impacto. Asimismo, se recomienda revisar el esquema de valoración del riesgo inherente, verificando que la asignación de la probabilidad y del impacto se realice conforme a los criterios técnicos definidos por la entidad, especialmente aquellos relacionados con la frecuencia real de exposición y con los umbrales de afectación económica y reputacional. Esto permitirá asegurar que la calificación del riesgo inherente refleje de manera objetiva el comportamiento del proceso y se encuentre plenamente alineada con la metodología institucional. 	1797

No	Código del riesgo	Riesgos	Descripción del Control	Análisis de la Oficina de Control Interno	Plan de Tratamiento
				<p>• Plan de Tratamiento: Respecto a la primera acción del Plan de Tratamiento 1797: "Orientar a la parte interesada en la denuncia a tramitar y en la forma como puede realizarse la reconstrucción archivística de los expedientes" es una actividad reactiva, que se activa solo cuando el daño ya ocurrió. La Guía establece que los planes de tratamiento deben ser preventivos, orientados a eliminar o reducir causas estructurales. Esta acción no previene la alteración documental, solo responde al evento; por tanto, su contribución a la mitigación real del riesgo es limitada.</p> <p>En cuanto a la segunda acción "Implementar personal de seguridad dentro del inmueble del Archivo Central, que inspeccione la entrada y salida del personal, en cuanto a tenencia de documentos físicos o electrónicos", esta sí aborda una causa asociada al riesgo (ingreso no controlado a documentos sensibles). Sin embargo, la Guía exige definir claramente frecuencia, criterios, responsabilidades y trazabilidad; aquí solo se menciona "implementar", sin parámetros de control o supervisión, por lo cual se sugiere revisar.</p> <p>Acerca de la tercera acción del plan de tratamiento es una acción pertinente, pero requiere mayor formalización. No se indicó cómo se hará la verificación, qué criterios se usarán, ni cómo se registrará la evidencia. Desde Control Interno, se observa que la acción es válida pero insuficientemente detallada para asegurar su eficacia.</p> <p>Por lo anterior se sugiere revisar la creación de acciones para la implementación de nuevos controles o el mejoramiento de controles existentes orientadas a atacar la causa raíz, establecer plazos y mecanismos de seguimiento concretos que permitan ver la implementación o mejora de controles.</p>	
3	DIPR01-3	Posibilidad de recibir o solicitar cualquier dadiva o beneficio a nombre propio o de terceros para que los Actos Administrativos no sean notificados a tiempo o que se omite el trámite que ordena el acto administrativo.	El auxiliar a cargo de la base de datos del Grupo de Notificaciones mensualmente revisa y analiza los tiempos utilizados para el proceso de notificaciones, con el fin de detectar atipicidades o anomalías en los tiempos de gestión frente al proceso. En caso de detectarse alguna atipicidad o anomalía se informará al coordinador del grupo. Evidencia: Correo Electrónico.	<p>A continuación, se presenta la evaluación efectuada por parte de la OCI al riesgo DIPR01-3:</p> <p>• Identificación y descripción del Riesgo: Este riesgo se identifica como la posible solicitud o recepción de beneficios para retrasar u omitir la notificación de actos administrativos. Si bien el enunciado apunta a un riesgo real y crítico del proceso, su descripción evidencia carencias metodológicas importantes: no distingue claramente el evento no deseado (retraso u omisión en la notificación), ni la circunstancia inmediata (variaciones injustificadas en los tiempos de gestión), ni la causa raíz (deficiencias en la estandarización del procedimiento, falta de parametrización de tiempos, brechas tecnológicas o administrativas). El impacto está limitado a la apertura de procesos disciplinarios, sin contemplar afectaciones más amplias como pérdida de eficacia institucional, afectación a derechos de terceros o deterioro de la confianza pública, elementos esenciales según la Guía para la Administración del Riesgo Versión 7. Por tanto, aunque la identificación apunta en la dirección correcta, la descripción requiere mayor estructuración y alineación con los criterios de claridad, especificidad y diferenciación causal recomendados para riesgos de integridad pública</p> <p>• Diseño y análisis de controles: Para el control definido para el Riesgo DIPR01-3, aunque el control es pertinente para identificar posibles manipulaciones en la gestión de notificaciones, su diseño carece de precisión metodológica. La Guía señala que los controles deben indicar de forma explícita las fuentes confiables, el tipo de información utilizada, los criterios de detección de irregularidades y la forma en que se dejan evidencias verificables, elementos que no aparecen en la descripción. Tampoco se detalla cómo se interpretan las atipicidades ni cuál es la relación directa entre la revisión y la causa raíz del riesgo (posible manipulación intencional de tiempos), lo que limita su capacidad preventiva. La actividad es adecuada, pero su formulación no cumple con los estándares requeridos para constituir un control completo.</p> <p>• Valoración del riesgo residual: El riesgo residual también se encuentra en zona extrema, lo que indica que la revisión mensual de tiempos no es suficiente para reducir la exposición a conductas dolosas en la gestión de</p>	1796

No	Código del riesgo	Riesgos	Descripción del Control	Análisis de la Oficina de Control Interno	Plan de Tratamiento
				<p>notificaciones respecto al impacto del riesgo inherente. Por lo cual se indica que el control actúa sobre síntomas (atipicidades) y no sobre mecanismos de prevención robustos (automatización, parametrización, doble validación), por lo cual su capacidad de mitigación es baja y el riesgo continúa en niveles críticos. Asimismo, se recomienda revisar el esquema de valoración del riesgo inherente, verificando que la asignación de la probabilidad y del impacto se realice conforme a los criterios técnicos definidos por la entidad, especialmente aquellos relacionados con la frecuencia real de exposición y con los umbrales de afectación económica y reputacional. Esto permitirá asegurar que la calificación del riesgo inherente refleje de manera objetiva el comportamiento del proceso y se encuentre plenamente alineada con la metodología institucional.</p> <p>• Plan de Tratamiento: Respecto al plan de tratamiento 1796 que tiene una acción, esta no corresponde directamente a la causa raíz del riesgo, que está relacionada con manipulación de tiempos y omisión deliberada de notificaciones. La Guía indica que la acción debe ser proporcional al riesgo y orientada a modificar el proceso o su trazabilidad. Su impacto es más cultural que operativo, por lo cual su contribución real a mitigar el riesgo es baja.</p> <p>Por tal razón se sugiere revisar la creación de acciones para la implementación de nuevos controles o el mejoramiento de controles existentes orientadas a atacar la causa raíz, establecer plazos y mecanismos de seguimiento concretos que permitan ver la implementación o mejora de controles.</p>	
4	DIPR01-4	Posibilidad de recibir o solicitar cualquier dadiva o beneficio a nombre propio o de terceros para ocultar o alterar la entrega de las comunicaciones recibidas y generadas por la Entidad.	El profesional especializado o auxiliar del grupo de correspondencia verifican y hacen seguimiento mensualmente según corresponda, la trazabilidad de cada guía en la plataforma de mensajería expresa o de 4-72, validando que las mismas sean entregadas o devueltas satisfactoriamente dentro de los tiempos establecidos en los contratos. En caso contrario, se requiere inmediatamente la prueba de entrega o la devolución al operador postal o de mensajería expresa. Igualmente se verifica que el auxiliar de 4-72 esté revisando permanentemente que el motorizado realiza efectivamente la entrega de las comunicaciones o que en el evento de una devolución, la causal sea válida. Evidencia: Plataforma de las empresas postal y de mensajería expresa, bases de datos, correos electrónicos y registro en el sistema SuperArgo	<p>A continuación, se presenta la evaluación efectuada por parte de la OCI al riesgo DIPR01-4:</p> <p>• Identificación y descripción del Riesgo: En este riesgo se identifica como evento la posibilidad de ocultar o alterar la entrega de comunicaciones oficiales, lo cual constituye un riesgo propio y bien seleccionado dentro del proceso de correspondencia. Sin embargo, su descripción no desarrolla adecuadamente la cadena lógica exigida por la Guía: la "circunstancia inmediata" (fallas en la trazabilidad, devoluciones atípicas, manipulación en la entrega) no está separada de la "causa raíz", que debería reflejar deficiencias sistémicas como falta de estandarización en el flujo de comunicaciones, dependencia operativa del operador postal, o debilidades en la autenticidad y verificación de entrega. El impacto se enuncia de manera general ("afectación de procesos"), sin medir la afectación institucional real, lo que limita su utilidad para el análisis posterior. Aunque la identificación del riesgo es coherente, la descripción debe depurarse para incorporar los componentes estructurales del riesgo y responder plenamente a la estructura que la Guía establece para documentar riesgos de corrupción.</p> <p>• Diseño y análisis de controles: Para el control definido para el Riesgo. La verificación de trazabilidad es una acción coherente con la naturaleza del riesgo, pero su diseño presenta vacíos importantes según los criterios de la Guía de Riesgos se especifica qué parámetros se revisan, qué constituye una desviación, ni qué fuentes de información se consideran confiables (plataforma del operador postal), lo cual reduce la capacidad del control para detectar alteraciones deliberadas. La descripción tampoco contempla la forma de evidenciar la revisión, ni mecanismos de validación independiente que reduzcan el riesgo de colusión o manipulación por parte del operador postal. Al no explicitar la relación con la causa raíz (falta de trazabilidad robusta), el control queda formulado de manera parcial y requiere fortalecerse para cumplir los estándares de integridad que exige la Guía de Riesgos.</p>	1907

No	Código del riesgo	Riesgos	Descripción del Control	Análisis de la Oficina de Control Interno	Plan de Tratamiento
				<p>• Valoración del riesgo residual: A pesar del control preventivo basado en trazabilidad, el riesgo residual persiste en zona extrema, lo cual evidencia que la verificación mensual no enfrenta adecuadamente las causas operativas y de integridad asociadas al riesgo para reducir el impacto. Desde el enfoque de Control Interno se observa que, la persistencia del riesgo demuestra que el control depende excesivamente del operador postal y carece de una estructura independiente de validación, por lo que la exposición a manipulación o interferencia en la entrega de comunicaciones sigue siendo muy alta.</p> <p>• Plan de Tratamiento: Respecto al Plan de Tratamiento 1907 que contiene dos acciones, indicamos para la primera acción que es “Solicitar al contratista del personal en misión que mínimo dos veces al año comunique y recuerde mediante correo electrónico el cumplimiento del Código de Integridad de Servicios Postales Nacionales”, se considera que es una acción débil frente al riesgo: un recordatorio anual no reduce la probabilidad de manipulación deliberada. La Guía indica que las acciones deben ser concretas, medibles y orientadas al proceso; esta acción no modifica controles ni condiciones operativas.</p> <p>Acerca de la segunda acción “Incluir en los contratos de correo, las cláusulas que hagan referencia a seguridad de la información”, se puede considerar como una acción adecuada y alineada con el riesgo, pues fortalece las obligaciones del operador. Sin embargo, debe especificarse cómo se hará seguimiento al cumplimiento, ya que la Guía exige trazabilidad, responsables y mecanismos de verificación.</p> <p>Por tal razón se sugiere revisar la creación de acciones para la implementación de nuevos controles o el mejoramiento de controles existentes orientadas a atacar la causa raíz, establecer plazos y mecanismos de seguimiento concretos que permitan ver la implementación o mejora de controles.</p>	

2.3. Evaluación de Riesgos en Relación con los Hallazgos de la Contraloría General de la República

La revisión de los hallazgos emitidos por la Contraloría General de la República permite identificar relaciones directas entre las deficiencias evidenciadas en los procesos institucionales y los riesgos registrados en el Mapa de Riesgos de la entidad. Este análisis resulta fundamental para fortalecer el Sistema de Control Interno, dado que los hallazgos actúan como señales de alerta sobre situaciones que ya se han materializado y que, por tanto, requieren acciones correctivas y preventivas por parte de los líderes de los procesos y demás responsables. La identificación de estas correspondencias facilita una visión integral del desempeño institucional y proporciona insumos para orientar la toma de decisiones a nivel estratégico, táctico y operativo.

A continuación, se presenta la relación de los hallazgos identificados por la Contraloría General de la República, asociados a los riesgos de gestión de la entidad. Esta información constituye un insumo relevante para el análisis por parte de los líderes de las dependencias, quienes podrán utilizarla como referencia en sus procesos de revisión y toma de decisiones.

DESCRIPCIÓN DEL HALLAZGO	CAUSA DEL HALLAZGO	RIESGO RELACIONADO MAPA DE RIESGO
Auditoria de Flujo de Recursos Proceso de recursos reconocidos sin justa causa por concepto de UPC, No UPC y reclamaciones	Las anteriores situaciones tienen lugar por la inoportuna expedición de los actos administrativos y las gestiones ineficaces e ineficientes para el recaudo	Posibilidad de afectación económica, reputacional, disciplinaria por pérdida de competencia en el trámite, debido al Incumplimiento en la gestión de notificación, comunicación y publicación de los Actos Administrativos.
Auditoria de Flujo de Recursos Fallos de tutelas y prestación de servicios de salud	Las fallas de información y debilidades intersectoriales por la falta de cumplimiento de los deberes de cada una de las instituciones especialmente de las EPS quienes limitan la autorización de los servicios requeridos, y de la SNS en su función de inspeccionar, vigilar y controlar la garantía del derecho a la salud en el marco de la obligatoriedad, calidad y eficiencia.	Posibilidad de afectación económica y reputacional por multa o sanción de los entes reguladores, por falta de oportunidad y calidad en la entrega de información de las áreas fuente.
Auditoria de cumplimiento 2023 Derechos de cobro Incapacidades (A – D – F – OI)	La pérdida del recurso se originó por falta de control, seguimiento y supervisión al cobro de las incapacidades ante las EPS/ARL, generando una sobreestimación del activo un detrimento patrimonial por 72.561.994 COP.	Posibilidad de afectación económica y reputacional por detrimento patrimonial, debido a que no se ejerce la acción de cobro dentro de los términos establecidos por la ley.
Auditoria de cumplimiento 2023 Pérdida de inventario (A – D – F)	Se debe a la falta de un procedimiento para la custodia de los bienes propiedad de la entidad, así mismo, la inoportuna reclamación ante la aseguradora, para hacer efectiva la póliza.	Posibilidad de afectación económica por hallazgos de auditorías internas, debido a la inadecuada administración de los bienes y elementos a cargo de los funcionarios de la Entidad
Auditoria de cumplimiento 2023 Pago de intereses por mora (A)	Por la inoportunidad en el pago de las obligaciones adquiridas por la entidad, derivadas de sentencias judiciales en contra de la SNS. Generando retrasos e incumplimientos que ocasionan el cobro de intereses moratorios.	Posibilidad de afectación reputacional por sanción en contra del Superintendente o directivos, impuesta por los despachos judiciales, debido al incumplimiento de orden judicial en el marco de incidentes de desacato.
Auditoria de cumplimiento 2023	La revelación de la información de los EE FF en las notas a los mismos; las cuales, deben ser claras, amplias y suficientes en sus revelaciones para todas las operaciones y variaciones importantes de la	Posibilidad de afectación económica y reputacional al no reflejar la información oportuna y razonable de las cuentas por cobrar, induciendo a decisiones erradas por

DESCRIPCIÓN DEL HALLAZGO	CAUSA DEL HALLAZGO	RIESGO RELACIONADO MAPA DE RIESGO
Notas a los Estados financieros (A)	entidad del periodo al que correspondan, tal como lo establecen el Catálogo General de Cuentas y el Marco Conceptual para Entidades de Gobierno según la Resolución 533 de 2015.	parte del deudor y de las áreas que adelantan su gestión con base en estos informes, por fallas en la calidad y oportunidad en el procesamiento de las operaciones financieras.
Auditoria de cumplimiento 2023	por no contar con un procedimiento de conciliación de cifras entre el presupuesto ejecutado y los registros contables para el cierre de la vigencia fiscal; asimismo, se desestima el disciplinario teniendo en cuenta que la información de la ejecución presupuestal se encuentra registrada en el SIIF	Posibilidad de afectación económica y reputacional debido a la expedición incorrecta de los Certificados de Disponibilidad Presupuestal (CDP) y Registros Presupuestales (RP), como consecuencia del incumplimiento de la normatividad vigente.
Conciliación entre el proceso contable y presupuestal (A)		
Auditoria de cumplimiento 2023	No solo limita la capacidad de recuperación de recursos, sino que también lleva a una acumulación de procesos, procedimientos judiciales, y gestiones administrativas que no fueron planificadas. Además, afecta la efectividad de la gestión pública en cumplimiento de sus objetivos. También, se evidencia debilidades por parte de la Oficina de control Interno de la SNS.	Posibilidad de afectación económica por observaciones, hallazgos o no conformidades de los entes de control y de la oficina de control interno de la entidad, debido al incumplimiento de las disposiciones legales para la celebración de contratos.
Inoportunidad en la Radicación de acreencias (A – D – F)		
Auditoria de cumplimiento 2023	Necesidad de mejorar los mecanismos de control y seguimiento sobre la ejecución presupuestal, que permitan mitigar la materialización de riesgos sobre la inejecución o baja ejecución de gastos públicos que se esperan realizar durante la vigencia fiscal respectiva	Posibilidad de afectación económica por sobre costos conforme a la medición del indicador de eficiencia, en el pago de servicios públicos de agua, energía y compra de insumos
Saldos de apropiación (A)		
Auditoria financiera 2024	Las incapacidades presentan inconsistencias que impiden su reconocimiento y pago. Hay inoportunidad en la radicación ante EPS, incumplimiento de funciones del personal responsable, deficiencias en control interno y debilidad en el manejo de incapacidades falsificadas, dadas de baja sin concepto firme de Control Disciplinario Interno, generando un presunto detrimento patrimonial.	Posibilidad de afectación reputacional por investigaciones de órganos de control debido a la inoportunidad en la resolución de los trámites a cargo de la Superintendencia Nacional de Salud.
Hallazgo No. 1 Castigo de cartera por incapacidades (A-D-F-OI)		

DESCRIPCIÓN DEL HALLAZGO	CAUSA DEL HALLAZGO	RIESGO RELACIONADO MAPA DE RIESGO
Auditoría financiera 2024	Inoportunidad en el cobro y radicación ante EPS por incapacidades y licencias, incumpliendo funciones según Resolución 2021910010016791-6 y la Ley 1438 de 2011.	Posibilidad de afectación reputacional por investigaciones de órganos de control debido a la inoportunidad en la resolución de los trámites a cargo de la Superintendencia Nacional de Salud.
Hallazgo 2 Inoportunidad en derecho de cobro de incapacidades (A- D)	Se registran saldos no recuperados en la subcuenta 138426001, afectando la situación financiera por sobreestimación de recursos y deficiente seguimiento a incapacidades pendientes.	

Tabla 1 Comparación Hallazgos CGR Auditoría 2024 Vs Riesgos de Gestión SNS 2025

El cruce entre los hallazgos de auditoría y los riesgos institucionales evidencia patrones recurrentes relacionados con debilidades en el control interno, incumplimientos normativos, fallas en la calidad y oportunidad de la información, y limitaciones en la gestión administrativa, financiera y operativa. Se observa una concentración significativa de causas asociadas a la falta de procedimientos, deficiencias en la supervisión y control, así como inconsistencias en la planeación y seguimiento de procesos críticos, tales como la gestión de incapacidades, el recaudo de recursos, la administración de bienes y la ejecución presupuestal. Asimismo, se identifican riesgos transversales que afectan la integridad financiera, la reputación institucional y la eficiencia en el cumplimiento de la función misional, lo que evidencia la necesidad de fortalecer mecanismos de coordinación interdependencias y mejorar la interoperabilidad de la información. Este análisis confirma que varios de los riesgos reportados no solo están correctamente identificados en el Mapa de Riesgos, sino que han mostrado señales de materialización, lo que demanda una revisión de la efectividad de los controles existentes y la priorización de acciones correctivas.

La relación entre los hallazgos de la Contraloría y los riesgos institucionales demuestra la importancia de un enfoque preventivo, articulado y basado en la gestión estratégica del riesgo. Los hallazgos confirman que algunas exposiciones de riesgo previamente identificadas ya han generado impactos económicos, disciplinarios y reputacionales, lo que resalta la urgencia de fortalecer la respuesta institucional a través de la actualización de procedimientos, la mejora en la calidad de la información y el fortalecimiento del control interno. En este sentido, los líderes de las dependencias deben asumir este análisis como una oportunidad para ajustar sus procesos, reforzar los controles y promover una cultura organizacional orientada a la prevención y al cumplimiento, con el fin de mitigar futuras materializaciones de riesgo y asegurar un desempeño institucional más eficiente, transparente y alineado con las obligaciones legales y misionales.

3. HALLAZGOS

3.1. Hallazgos

Durante el proceso de evaluación al diseño e identificación de riesgos efectuado por la Oficina de Control Interno, y conforme a las funciones establecidas en la Ley 87 de 1993, el Decreto 648 de 2017 y los lineamientos metodológicos de la Guía para la Gestión Integral del Riesgo – Versión 7 de 2025, de acuerdo con lo anteriormente expuesto en cada uno de los anteriores análisis se identificaron los siguientes hallazgos:

Hallazgo No 1: Inadecuada Identificación y descripción del riesgo: Se detectó una inadecuada redacción de los riesgos en múltiples procesos, donde no se diferencia claramente evento, circunstancia inmediata, causa raíz e impacto, contrario a la estructura definida por la Guía (evento no deseado + circunstancia inmediata + causa raíz). Adicionalmente se observaron riesgos redactados con elementos redundantes, extensos o que mezclan impacto con evento y también escasa claridad en la causa raíz, lo que impide una adecuada alineación entre el riesgo y los controles orientados a mitigarlo.

Hallazgo No 2: Diseño de Controles inadecuados e incompleta: Se detectó que buena parte de los controles revisados carecen de verbos de acción claros, presentando descripciones amplias que mezclan varias actividades sin definir la acción principal del control. En algunos casos no se identifican los atributos mínimos de un control —responsable, frecuencia, evidencia, documentación y método de ejecución. Se identificaron controles clasificados como preventivos, aunque su ejecución es posterior al evento, constituyéndose realmente en controles detectivos. Se evidenció que los controles analizados son, en su mayoría, manuales, lo cual incrementa el riesgo operativo y la posibilidad de errores o manipulaciones.

Hallazgo No 3. Planes de Tratamiento sin acciones orientadas a la causa raíz del riesgo. Se observaron planes de tratamiento basados principalmente en capacitaciones, socializaciones y recordatorios, sin acciones orientadas a atacar la causa raíz. Así mismo se observó que algunos planes presentan incumplimiento de actividades y retrasos, como el PT 1931, que a la fecha de corte presenta 0% de avance. En varios casos, la evidencia reportada para el cierre de las actividades no guarda relación con la acción planeada, declarando efectividad sin demostrar mitigación real del riesgo. Las acciones propuestas en algunos planes de tratamiento son de carácter reactivo y no preventivo.

3.2. Observaciones

Como resultado del proceso de revisión, se emiten las siguientes observaciones de carácter general:

Observación No 1. Falta de alineación metodológica. Se evidencia que los procesos aún no han incorporado plenamente los lineamientos para la Gestión Integral de los Riesgos, lo que se evidencia en la formulación estructurada del riesgo y en la construcción de controles robustos.

Observación No 2. Baja Trazabilidad de los Controles. Se ha observado deficiencias en la definición de la trazabilidad de los controles, las fuentes de evidencias principalmente se determinan como correos electrónicos o registros no estandarizados que dificultan la verificación e independencia del control.

Observación No 3. Baja Articulación del Control en los Procedimientos Institucionales. Debilidad en la gestión documental y procedimental, en varios casos no existen procedimientos formalizados que respalden la operación del control, afectando el diseño y su adecuada ejecución, así como la asignación directa del responsable del control.

Observación No 4. Alta dependencia de Controles Manuales. La operación actual de los procesos revisados demuestra una alta dependencia de controles manuales, lo que aumenta la exposición al error y reduce la capacidad institucional para mitigar los riesgos.

Observación No 5. Inconsistencia articulada del riesgo, el control y el plan de tratamiento. Se evidencian acciones que no atienden las causas raíz y que no se articulan con la necesidad de mejorar los controles identificados como deficientes.

Observación No 6. Criterios de valoración de la Probabilidad e Impacto del Riesgo. La Guía de Administración del Riesgo presenta un ejemplo para determinar la frecuencia de ocurrencia del riesgo, señalando expresamente la necesidad de “...tener en cuenta que en cada entidad la cantidad y el valor de los bienes muebles del inventario pueden variar considerablemente”. Esto significa que la valoración de la probabilidad de ocurrencia del riesgo, aunque incluida en la guía elaborada por el Departamento Administrativo de la Función Pública, debe ajustarse a la realidad específica de cada entidad.

Para ilustrar dicha valoración, se tomó la probabilidad de la Guía versus el Mapa de Riesgos de la SNS-2025 así:

Probabilidad	Frecuencia de la Actividad
Muy Baja – 20%	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año
Baja – 40%	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año
Media – 60%	La actividad que conlleva el riesgo se ejecuta de 25 a 500 veces por año
Alta .80%	La actividad que conlleva el riesgo se ejecuta más de 500 veces al año y máximo 5000 veces por año
Muy Alta – 100%	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año

Ilustración 1 Tomado de Guía Administración del Riesgo DAFP No. 7 pág. No. 86

De esta manera, se identifica que el Mapa de Riesgos de la Superintendencia Nacional de Salud, se adoptaron los mismos parámetros sin atender dicha recomendación del DAFP así:

RIESGO RESIDUAL			
PROBABILIDAD	IMPACTO	ZONA DE RIESGO	OPCIONES DE MANEJO DEL RIESGO
MUY BAJA (20%)	MENOR (40%)	Zona de Riesgo BAJA	Aceptar el riesgo.

Recomendaciones

La Oficina de Control Interno recomienda:

1. Reestructurar integralmente la formulación de los riesgos, adoptando plenamente la estructura definida por la Guía para la Gestión Integral del Riesgo – Versión 7, con el fin de garantizar claridad sobre el evento no deseado, la circunstancia inmediata, la causa raíz y el impacto, elementos fundamentales para su gestión.
2. Rediseñar los controles existentes para incorporar la totalidad de los atributos exigidos — responsable, acción concreta, frecuencia, evidencia, documentación y ejecución— y clasificarlos correctamente como preventivos, detectivos o correctivos, según el momento en que actúan dentro del proceso.
3. Avanzar en la progresiva automatización de controles y en la adopción de herramientas tecnológicas que permitan mejorar la trazabilidad y efectividad del aseguramiento.
4. Revisar y reformular los planes de mejoramiento, priorizando acciones orientadas a abordar directamente las causas raíz, con metas específicas, indicadores verificables, responsables definidos y tiempos de cumplimiento claros.
5. Fortalecer los mecanismos de seguimiento y monitoreo del riesgo, estableciendo revisiones periódicas que permitan evaluar la efectividad real de los controles y ajustar las acciones cuando sea necesario.
6. Ajustar la valoración del Mapa de Riesgos de la Superintendencia Nacional de Salud a la realidad institucional, entendiendo que los parámetros propuestos en la Guía No.7 de Administración del Riesgo del Departamento Administrativo de la Función Pública, constituyen una referencia orientadora. En consecuencia, la frecuencia y probabilidad de ocurrencia de los riesgos deben determinarse considerando las particularidades, procesos y condiciones específicas de la entidad.

CONCLUSIONES

De acuerdo con los resultados obtenidos, se concluye que la entidad mantiene una exposición significativa a riesgos de gestión y de integridad, dada la permanencia de los riesgos evaluados en niveles extremos incluso después de aplicar los controles existentes. Esta situación evidencia una necesidad de mejora en busca de madurez institucional en materia de gestión del riesgo, especialmente en la identificación estructurada de los riesgos, el diseño adecuado de los controles y la articulación entre estos y los planes de tratamiento. Los controles actuales en muchos de los casos no logran modificar la probabilidad ni el impacto de los riesgos, debido principalmente a problemas de diseño, ausencia de atributos esenciales y falta de alineación con las causas raíz. Los planes de tratamiento presentan debilidades metodológicas y operativas que impiden que sus resultados contribuyan efectivamente a la mitigación del riesgo. En consecuencia, se requiere una intervención institucional decidida, liderada por la Alta Dirección, para reorientar el modelo de gestión del riesgo hacia un enfoque más preventivo, estratégico y articulado con las políticas del MIPG y el Sistema de Control Interno.

- ✓ El informe presentado, genera los siguientes hallazgos:
- ✓

Hallazgo	Observación	Recomendaciones
4	6	7

Tabla 10: Fuente propia OCI.

De conformidad con lo preceptuado en el párrafo del Literal d) del Artículo 2.2.21.3.7 del Decreto 1083 de 2015, es competencia de la Oficina de Control Interno o quien haga sus veces “(...) *Evaluar el sistema de control interno de la Entidad, con énfasis en la existencia, funcionamiento y coherencia de los componentes y elementos que lo conforman y presentar informes a la Dirección y al Comité de Coordinación de Control Interno de la Entidad, con el propósito de que allí se evalúen, decidan y adopten oportunamente las propuestas de mejoramiento del sistema (...)*”, por consiguiente, el resultado derivado del presente seguimiento será puesto en conocimiento de la Alta Dirección e integrantes del Comité Institucional de Coordinación de Control Interno - CICC, con el objeto de que se considere el diseño y la implementación de las acciones preventivas y/o correctivas a que haya lugar, en procura del mejoramiento continuo y la eventual adopción de buenas prácticas que permitan la definición y aplicación de controles adecuados, para el tratamiento de riesgos institucionales.

Cordialmente,

Miller Giovanni López Mejía
 Jefe de Oficina Control Interno (e)

Elaboró: Luis Eduardo Perdomo Londoño, Pablo Vergara Gómez: Profesionales Especialistas - OCI
 Revisó y aprobó: Miller Giovanni López Mejía, Jefe de Oficina Control Interno (e)