Informe Seguimiento y Evaluación

Auditoría al Plan de Privacidad y Seguridad de la Información 2023 - 2026

Unidad de Proyección Normativa y Estudios de Regulación Financiera

Contenido

1. Introducción

El presente informe expone los resultados del seguimiento y evaluación efectuado el Proceso de Control y Evaluación al Plan de Privacidad y Seguridad de la Información 2023–2026 de la Unidad de Proyección Normativa y Estudios de Regulación Financiera – URF.

El objetivo principal de esta auditoría se orientó a evaluar la coherencia, implementación y efectividad del PPSI (código GI-PN-002), verificando la trazabilidad desde su diagnóstico inicial, brechas e identificación de riesgos, hasta las acciones formuladas, los productos alcanzados, los resultados reportados y la confiabilidad de los datos que sustentan el nivel de madurez alcanzado por la entidad.

El alcance de la evaluación abarcó las fases de formulación, implementación, seguimiento y evaluación del Plan para el periodo de la vigencia 2023 a 2026, tomando como base los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), el Decreto 1078 de 2015, el Decreto 767 de 2022 y las Resoluciones 500 de 2021 y 02277 de 2025, así como los documentos normativos e instrumentos institucionales de planeación adoptados por la Unidad.

El ejercicio se desarrolló bajo una metodología con enfoque basado en riesgos, evidencia y trazabilidad. A través de revisiones documentales, análisis cruzado de datos y validaciones en el Sistema de Monitoreo de la Gestión Institucional (SMGI), se analizaron aspectos fundamentales como la actualización del contexto institucional frente a cambios organizacionales, la consistencia metodológica de la fase de diagnóstico y la correspondencia entre la ejecución real y las ponderaciones asignadas en los indicadores institucionales de cumplimiento. Asimismo, el informe contempla la evaluación del tratamiento de los riesgos asociados a los activos e información crítica y la articulación con los esquemas de mejora continua dentro de la entidad.

2. Objetivo

Evaluar la coherencia, implementación y efectividad del Plan de Privacidad y Seguridad de la Información de la Unidad de Proyección Normativa y Estudios de Regulación Financiera – URF, verificando la trazabilidad entre el diagnóstico institucional, las brechas identificadas, los riesgos de seguridad y privacidad de la información, las acciones y controles definidos, los productos establecidos y

los resultados reportados, así como la confiabilidad de la información utilizada para sustentar el nivel de madurez alcanzado por la entidad.

3. Alcance

La auditoría comprenderá la formulación, implementación, seguimiento y evaluación del Plan de Privacidad y Seguridad de la Información 2023-2026.

4. Criterios de evaluación

4.1. Marco normativo

- Decreto 1078 de 2025 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"

- Decreto 767 de 2022 "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"

- Resolución 500 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital."

- Resolución 02277 de 2025 "Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia."

- Modelo de Seguridad y Privacidad de la Información

4.2. Otros requisitos institucionales

- GI-PN-002 Plan de Privacidad y Seguridad de la Información Versión 2 del 25 de abril de 2025
- GI-PL-002 Política de Privacidad y Seguridad de la Información Versión 5 del 23 de mayo de 2025
- GI-MO-004 Manual de Privacidad y Seguridad de la Información Versión 2 del 04 de junio de 2026
- Plan de Acción Anual de las vigencias 2023 a 2026

5. Metodología de evaluación

La metodología para la aplicación de las pruebas de auditoría se desarrolló bajo un enfoque basado en riesgos, evidencia y trazabilidad, mediante la revisión documental, análisis de información, cruces de datos de las actividades, productos y resultados reportados en el Plan.

Las pruebas estuvieron orientadas a verificar la correspondencia entre el diagnóstico, las brechas identificadas, los riesgos, las acciones definidas, los productos, su implementación y los resultados obtenidos, determinando para cada aspecto su nivel de cumplimiento, implementación, operación y efectividad.

De manera particular, se realizó una prueba de trazabilidad información aportada, verificando la evidencia que sustenta las calificaciones, las acciones formuladas para atender las brechas, su ejecución y los resultados alcanzados.

Asimismo, se validó la información reportada en los mecanismos de seguimiento frente a las evidencias disponibles, con el fin de determinar la confiabilidad de los resultados y la efectividad de las acciones y controles implementados.

6. Evaluación realizada

Se realizó la revisión del Plan de Privacidad y Seguridad de la Información 2023 - 2026, identificado con código GI-PN-002, versión 2.0 del 25 de abril de 2025, con el propósito de verificar la coherencia entre el diagnóstico, las brechas identificadas, los riesgos, las actividades priorizadas y los productos definidos, así como la incorporación de los resultados derivados de los ejercicios de diagnóstico y seguimiento realizados durante el periodo de vigencia del Plan.

6.1. Formulación del Plan de Privacidad y Seguridad de la Información 2023 – 2026.

Como resultado de la revisión, se observó que, durante el periodo de vigencia del Plan, la Unidad presentó cambios administrativos y organizacionales relevantes que modificaron el contexto institucional bajo el cual fueron definidas las acciones inicialmente previstas. No obstante, en la versión revisada del documento no se evidenció de manera suficiente la actualización del análisis de contexto frente a dichos cambios, ni la valoración de su posible incidencia sobre las prioridades, riesgos, responsables, actividades y resultados esperados del Plan. En este sentido, resulta pertinente que los instrumentos de

planeación relacionados con seguridad y privacidad de la información sean objeto de revisión y actualización cuando se presenten cambios significativos en el entorno institucional, de manera que las acciones definidas mantengan su pertinencia frente a las necesidades y riesgos vigentes.

6.2. Fase de diagnóstico

En relación con la fase de diagnóstico, para la vigencia 2023 no se evidenció, dentro de la documentación inicialmente revisada y aportada por el proceso, el instrumento base utilizado para realizar el diagnóstico. No obstante, el Plan presenta de manera gráfica los resultados obtenidos de la evaluación de efectividad de controles con referencia a ISO/IEC 27001:2013 – Anexo A. Si bien esta información permite identificar de manera general el resultado del ejercicio realizado, no se logró establecer con precisión los aspectos evaluados, las brechas identificadas, los criterios utilizados para su valoración y la relación existente entre los resultados obtenidos y las acciones posteriormente incorporadas al Plan.

Por lo anterior, se considera pertinente fortalecer la documentación de los ejercicios de diagnóstico, procurando conservar y referenciar los instrumentos, resultados y evidencias que permitan establecer de manera verificable la línea base a partir de la cual se formularon las actividades del Plan. Asimismo, se **recomienda** que las brechas identificadas sean descritas con un mayor nivel de detalle, precisando las situaciones que requieren intervención, los riesgos asociados, las acciones previstas para su tratamiento y los resultados esperados.

Lo anterior adquiere especial relevancia considerando que la gestión de la infraestructura y de determinados servicios tecnológicos de la Unidad se desarrolla en articulación con el Ministerio de Hacienda y Crédito Público, por lo cual resulta conveniente diferenciar en el Plan cuáles aspectos se encuentran bajo responsabilidad directa de la Unidad y cuáles corresponden a servicios, controles o actividades administrados por el Ministerio. Esta diferenciación permitiría establecer con mayor claridad el alcance de las acciones que puede ejecutar directamente la URF y aquellas que requieren gestión, coordinación o seguimiento frente al proveedor de los servicios tecnológicos.

Por otra parte, el proceso aportó como evidencia la actualización del diagnóstico realizada en agosto de 2024, así mismo se conoció en la verificación de la información en el SMGI el autodiagnóstico correspondiente a la vigencia 2025, presentado como evidencia del cumplimiento de la actividad URF2025_214 – Realizar autodiagnóstico del modelo de privacidad y seguridad

de la información y elaborar plan de acción. No obstante, se observó que los resultados de estas actualizaciones no se encuentran incorporados de manera suficiente en la versión 2 del Plan objeto de revisión. Esta situación limita la posibilidad de identificar cómo los resultados de los diagnósticos posteriores incidieron en la priorización, modificación o incorporación de nuevas actividades y en el cierre o tratamiento de las brechas inicialmente identificadas.

En este sentido, se considera importante que los resultados de los ejercicios de autodiagnóstico sean incorporados de manera sistemática en los instrumentos de planeación, de forma que permitan evidenciar la evolución del nivel de madurez, el cierre o permanencia de brechas y la necesidad de mantener, ajustar o formular nuevas acciones.

Adicionalmente, se observó que el Plan toma como referencia los resultados obtenidos por la Unidad en el marco de la medición del Índice de Desempeño Institucional a través del FURAG; sin embargo, la información incorporada corresponde a resultados de las vigencias 2018 a 2021, sin que se evidencie su actualización en la versión posterior del documento. Estos resultados pueden constituir un antecedente para establecer la evolución de la gestión, la actualización periódica de esta información permitiría contar con una línea base más representativa y facilitaría el análisis de tendencias, la identificación de brechas, la formulación de acciones y el seguimiento a los avances alcanzados por la entidad, así mismo es pertinente desagregar el análisis en los diferentes índices evaluados en el instrumento con el fin de establecer de manera específica aciertos y debilidades de la implementación de la política de seguridad digital.

De acuerdo con el análisis realizado, las actividades priorizadas en el Plan se orientaron principalmente al avance en el ciclo de funcionamiento del modelo de operación (PHVA). No obstante, en el documento no se presenta con suficiente detalle el resultado de los ejercicios de diagnóstico que dieron lugar a la priorización de dichas actividades, lo que dificulta establecer de manera directa qué debilidades o brechas fueron identificadas, cuáles fueron consideradas prioritarias, qué riesgos se pretendían tratar y cómo las actividades definidas contribuyeron a su mitigación o cierre.

En consecuencia, se identifica una oportunidad para fortalecer la trazabilidad del Plan, de manera que exista una relación claramente documentada. Esta trazabilidad resulta fundamental para determinar no solo si las actividades fueron ejecutadas, sino también si las mismas fueron pertinentes frente a las

necesidades identificadas y si contribuyeron efectivamente al fortalecimiento del Modelo de Privacidad y Seguridad de la Información.

Finalmente, se considera pertinente que el Plan incorpore de manera explícita y actualizada el nivel de madurez alcanzado por la Unidad como resultado de los diferentes ejercicios de diagnóstico realizados durante su vigencia, incluyendo, cuando corresponda, la metodología, criterios de valoración y evidencias que soportan los resultados obtenidos, sobre el particular el proceso de Gestión de la Información aclara que la información utilizada para los diagnósticos es reportada por el Ministerio de Hacienda y Crédito Público y, debido a las dificultades para su consolidación y análisis integral, no es posible determinar de manera consolidada el nivel de madurez de la Unidad.

La incorporación de esta información permitiría establecer una línea base, evidenciar la evolución del modelo, identificar las brechas pendientes y sustentar técnicamente la priorización de las acciones. Asimismo, facilitaría determinar si los resultados reportados reflejan efectivamente una mejora en la gestión de la seguridad y privacidad de la información o corresponden principalmente al cumplimiento de actividades programadas.

En términos generales, la principal oportunidad de fortalecimiento identificada se relaciona con la trazabilidad y actualización del Plan, de manera que este refleje de forma dinámica los cambios del contexto institucional y permita demostrar la relación entre los resultados de los diagnósticos, las brechas y riesgos identificados, las acciones implementadas y los resultados alcanzados.

6.3. Fase de implementación de la estrategia de seguridad digital

La Unidad estableció cinco estrategias para la implementación del Modelo de Privacidad y Seguridad de la Información (MPSI), orientadas a fortalecer el liderazgo, la gestión de riesgos, la implementación de controles, la gestión de incidentes y la cultura de seguridad de la información. A partir de estas estrategias se estructuró el plan de trabajo para el periodo 2023-2026, en el cual se definieron las actividades y acciones orientadas a su implementación y fortalecimiento.

Para efectos de dar continuidad al ciclo establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) para la implementación y mejora del modelo, esta etapa fue definida por la Unidad como la fase de planificación, orientada a establecer y priorizar las acciones

necesarias para atender las necesidades y brechas identificadas en el diagnóstico y avanzar en la implementación del modelo.

6.4. Plan de trabajo 2023 – 2026

Con el propósito de verificar las acciones que materializan el Plan de Seguridad y Privacidad de la Información en cada vigencia, se realizó la revisión a partir de la información suministrada por el proceso y de la validada en el Sistema de Monitoreo de la Gestión Institucional (SMGI). Es de indicar que para el seguimiento realizado se hizo con base en el cronograma establecidos en la versión 2 del documento con el fin de cubrir la totalidad de las acciones.

Se realiza la validación de lo documentado en los indicadores:

- INAC_URF_IND083_GI_Cumplimiento del plan de privacidad y seguridad de la información – PPSI
- URF_IND108_GI_Cumplimiento del Plan de Seguridad y Privacidad de la Información – PPSI

Así como lo proyectado en el Plan de Acción Anual de las vigencias definidas en el alcance en cumplimiento de la integración de planes institucionales del que habla el Decreto 612 de 2018 en su artículo 1. Como resultado de dicha verificación, se evidenció lo siguiente:

Estrategia	Peso	Actividades	Peso	Producto	2023	2024	2025	2026	Actividades asociadas a Plan de Acción Anual 2023	Actividades asociadas a Plan de Acción Anual 2024	Actividades asociadas a Plan de Acción Anual 2025	Actividades asociadas a Plan de Acción Anual 2026	Observación Control y Evaluación
Liderazgo	30%	1.1 Actualizar la política de seguridad de la información	12%	Política de seguridad de la información	12%				No se encontró asociación en el Plan de Acción Anual por su fecha de formulación.	No se programaron acciones para la vigencia	No se programaron acciones para la vigencia	No se programaron acciones para la vigencia	Se realizó la verificación del cumplimiento de la actividad, frente a la cual el proceso reportó: "La política se elaboró y fue aprobada por el Comité Institucional de Gestión y Desempeño". No obstante, teniendo en cuenta que el reporte no incorporaba información suficiente ni las evidencias que permitieran validar directamente su ejecución, se efectuaron verificaciones adicionales en el Sistema de Monitoreo de la Gestión Institucional – SMGI. Como resultado de la revisión, se evidenció que la Política de Privacidad y Seguridad de la Información, versión 3, fue publicada en el SMGI el 8 de junio de 2023. Asimismo, mediante la revisión del Acta No. 05 del 6 de junio de 2023, se verificó que el documento fue presentado para consideración y aprobación del Comité Institucional de Gestión y Desempeño. En consecuencia, se obtuvo evidencia que permite corroborar la ejecución de la actividad reportada. Se **recomienda** que, en el reporte de las actividades del Plan, se describa de manera precisa el avance y resultado obtenido y se incorporen las evidencias que soporten su ejecución, de manera que faciliten su verificación y permitan determinar de forma oportuna, objetiva y suficiente el nivel de cumplimiento de las actividades.

Estrategia	Peso	Actividades	Peso	Producto	2023	2024	2025	2026	Actividades asociadas a Plan de Acción Anual 2023	Actividades asociadas a Plan de Acción Anual 2024	Actividades asociadas a Plan de Acción Anual 2025	Actividades asociadas a Plan de Acción Anual 2026	Observación Control y Evaluación
		1.2 Someter la política a aprobación en el Comité Institucional de Gestión y Desempeño y tramitar su formalización	6%	Política de seguridad de la información formalizada	6%				No se encontró asociación en el Plan de Acción Anual por su fecha de formulación.	No se programaron acciones para la vigencia	No se programaron acciones para la vigencia	No se programaron acciones para la vigencia	Se realizó la verificación del cumplimiento de la actividad, frente a la cual el proceso reportó: "La política se elaboró y fue aprobada por el Comité Institucional de Gestión y Desempeño". No obstante, teniendo en cuenta que el reporte no incorporaba información suficiente ni las evidencias que permitieran validar directamente su ejecución, se efectuaron verificaciones adicionales en el Sistema de Monitoreo de la Gestión Institucional – SMGI. Como resultado de la revisión, se evidenció que la Política de Privacidad y Seguridad de la Información, versión 3, fue publicada en el SMGI el 8 de junio de 2023. Asimismo, mediante la revisión del Acta No. 05 del 6 de junio de 2023, se verificó que el documento fue presentado para consideración y aprobación del Comité Institucional de Gestión y Desempeño. En consecuencia, se obtuvo evidencia que permite corroborar la ejecución de la actividad reportada. Se **recomienda** que, en el reporte de las actividades del Plan, se describa de manera precisa el avance y resultado obtenido y se incorporen las evidencias que soporten su ejecución, de manera que faciliten su verificación y permitan determinar de forma oportuna, objetiva y suficiente el nivel de cumplimiento de las actividades.

Estrategia	Peso	Actividades	Peso	Producto	2023	2024	2025	2026	Actividades asociadas a Plan de Acción Anual 2023	Actividades asociadas a Plan de Acción Anual 2024	Actividades asociadas a Plan de Acción Anual 2025	Actividades asociadas a Plan de Acción Anual 2026	Observación Control y Evaluación
		1.3 Elaborar el manual de privacidad y seguridad de la información y tramitar su formalización	12%	Manual de seguridad y privacidad de la información formalizado	6%	6%			URF2023_307_Elaborar procedimientos de seguridad y privacidad	El alcance de la actividad fue ejecutado en la vigencia 2023	No se programaron acciones para la vigencia	No se programaron acciones para la vigencia	Se realizó la verificación del cumplimiento de la actividad, frente a la cual el proceso reportó: "El manual de elaboró y formalizó en el sistema de gestión institucional". No obstante, teniendo en cuenta que el reporte no incorporaba información suficiente ni las evidencias que permitieran validar directamente su ejecución, se efectuaron verificaciones adicionales en el Sistema de Monitoreo de la Gestión Institucional – SMGI. Como resultado de la revisión, se evidenció que el Manual de Privacidad y seguridad de la información, versión 1, fue publicada en el SMGI el 10 de agosto de 2023. En consecuencia, se obtuvo evidencia que permite corroborar la ejecución de la actividad reportada, de acuerdo con lo indicado por el proceso esta actividad que estaba prevista para ser ejecutada en 2023 y 2024 fue cumplida al 100% en el presente seguimiento. Se **recomienda** que, en el reporte de las actividades del Plan, se describa de manera precisa el avance y resultado obtenido y se incorporen las evidencias que soporten su ejecución, de manera que faciliten su verificación y permitan determinar de forma oportuna, objetiva y suficiente el nivel de cumplimiento de las actividades.

Estrategia	Peso	Actividades	Peso	Producto	2023	2024	2025	2026	Actividades asociadas a Plan de Acción Anual 2023	Actividades asociadas a Plan de Acción Anual 2024	Actividades asociadas a Plan de Acción Anual 2025	Actividades asociadas a Plan de Acción Anual 2026	Observación Control y Evaluación
Gestión de riesgos	30%	2.1 Identificar, evaluar y gestionar los riesgos de seguridad de la información	30%	Riesgos de seguridad de la información integrados al sistema gestión institucional-SGI y formalizados en SMGI			27.50%	2.50%	No se encontró asociación en el Plan de Acción Anual por su fecha de formulación.	No se programaron acciones para la vigencia	URF2025_264_Definir la metodología para identificar, evaluar y gestionar los riesgos de seguridad de la información URF2025_258_Hacer control y seguimiento a los servicios de almacenamiento en la nube	URF2026_NEI_239_Reportar el avance en la gestión de riesgos de seguridad digital a la alta dirección URF2026_NEI_172_Identificar, evaluar y gestionar los riesgos de seguridad de la información	Durante la validación del cumplimiento de la actividad, se identificó que para las vigencias 2025 y 2026 se realizó un ajuste en la ponderación asignada a su desarrollo, aspecto que fue considerado en el análisis de los resultados correspondientes a cada vigencia. Para la vigencia 2025, el proceso definió acciones complementarias orientadas al establecimiento de la metodología para la gestión de los riesgos de seguridad digital y su correspondiente seguimiento. Al respecto, el proceso informó que se realizaron varias sesiones de trabajo orientadas a definir metodológicamente la gestión de estos riesgos, de conformidad con los lineamientos impartidos por el Departamento Administrativo de la Función Pública (DAFP). Como resultado de la verificación de la documentación aportada, se observó que en el registro de la actividad se relacionan diferentes evidencias; sin embargo, dentro de los soportes suministrados se identificó principalmente el documento correspondiente a la metodología para la gestión de los riesgos de seguridad digital. En este sentido, se recomienda fortalecer la organización y trazabilidad de los soportes asociados a las actividades ejecutadas, de manera que estos permitan acreditar de forma integral el cumplimiento de las acciones reportadas. En relación con el seguimiento de los controles, se verificó la identificación del riesgo URF_36_GI – Pérdida de integridad, disponibilidad o confidencialidad de la información consignada en medios digitales, respecto del cual se evidenció la realización del monitoreo cuatrimestral correspondiente. Por su parte, para la vigencia 2026 se formularon acciones orientadas a la identificación de los riesgos de seguridad digital y al reporte de su gestión ante la Alta Dirección. No obstante, a la fecha de corte del presente informe, el plazo establecido para su ejecución aún no se había cumplido; por lo tanto, estas acciones no serán objeto de seguimiento.

Estrategia	Peso	Actividades	Peso	Producto	2023	2024	2025	2026	Actividades asociadas a Plan de Acción Anual 2023	Actividades asociadas a Plan de Acción Anual 2024	Actividades asociadas a Plan de Acción Anual 2025	Actividades asociadas a Plan de Acción Anual 2026	Observación Control y Evaluación
Implementación de controles	10%	3.1 Efectuar tratamiento de los riesgos	10%	Controles implementados y formalizados en los documentos de los procesos			10%		No se encontró asociación en el Plan de Acción Anual por su fecha de formulación.	No se programaron acciones para la vigencia	URF2025_265 _Identificar, evaluar y gestionar los riesgos de seguridad de la información de archivo e información almacenada en la nube	No se programaron acciones para la vigencia	Se verificó el cumplimiento de la actividad, evidenciándose que el proceso documentó la metodología establecida para la identificación de riesgos, así como el archivo base utilizado para la identificación correspondiente, los cuales fueron aportados como soportes de la actividad ejecutada.
		3.2 Hacer seguimiento a la gestión de los riesgos y la operación de los controles asociados		Informe de gestión de riesgos y operación de controles					No se encontró asociación en el Plan de Acción Anual por su fecha de formulación.	No se programaron acciones para la vigencia	No se programaron acciones para la vigencia	No se programaron acciones para la vigencia	Al realizar la verificación comparativa de las dos versiones del documento, se identificó que en la versión 2 se omitió la asignación de la ponderación correspondiente a la actividad, situación que afecta la trazabilidad de los criterios definidos para su seguimiento y evaluación. Para la vigencia 2025, se evidenció que, en el marco del Plan de Acción Anual, se incorporó una acción relacionada con el riesgo identificado. De acuerdo con el análisis realizado, se observa una oportunidad de mejora en la articulación y asociación de las actividades con sus respectivos soportes, toda vez que, para la actividad objeto de verificación, resultaba pertinente asociar como evidencia el archivo correspondiente al monitoreo del riesgo URF_36_GI – Pérdida de integridad, disponibilidad o confidencialidad de la información consignada en medios digitales. Esta articulación permitiría fortalecer la trazabilidad entre la actividad programada, el riesgo asociado, las acciones implementadas y las evidencias que soportan su cumplimiento.

Estrategia	Peso	Actividades	Peso	Producto	2023	2024	2025	2026	Actividades asociadas a Plan de Acción Anual 2023	Actividades asociadas a Plan de Acción Anual 2024	Actividades asociadas a Plan de Acción Anual 2025	Actividades asociadas a Plan de Acción Anual 2026	Observación Control y Evaluación
Gestión de incidentes	10%	4.1 Socializar los incidentes de seguridad presentados, de acuerdo con la información reportada por el Ministerio de Hacienda y Crédito Público	6%	Pieza comunicativa			4%	2%	No se encontró asociación en el Plan de Acción Anual por su fecha de formulación.	No se programaron acciones para la vigencia	No se programaron acciones para la vigencia	URF2026_NOP_173_01_Socializar los incidentes de seguridad presentados, de acuerdo con la información reportada por el Ministerio de Hacienda y Crédito Público	Se verificó el cumplimiento de la acción y se constató que, en el plan de acción correspondiente a la vigencia 2025, no se incluyeron actividades orientadas a la socialización de los incidentes de seguridad presentados, según la información reportada por el Ministerio de Hacienda y Crédito Público; situación que genera un impacto en el cumplimiento general del plan. Por su parte, para la vigencia 2026, la actividad asociada se encuentra programada para su ejecución en el mes de diciembre.
		4.2 Hacer seguimiento a los incidentes de seguridad reportados	4%	Reporte de seguimiento	1%		2%	1%	No se encontró asociación en el Plan de Acción Anual por su fecha de formulación.	URF2024_023_Hacer seguimiento a los incidentes de seguridad digital	URF2025_215_Hacer seguimiento a los incidentes de seguridad digital	URF2026_NEP_173_02_Hacer seguimiento a los incidentes de seguridad reportados	Se realizó la verificación del cumplimiento de la actividad, frente a la cual el proceso reportó: Vigencia 2023: Se verificó el cumplimiento de la actividad mediante el reporte de la Dirección de Tecnología del Ministerio de Hacienda y Crédito Público (evidencia registrada en la actividad URF2024_023). Durante el mes de diciembre se realizó el seguimiento correspondiente a 15 incidentes de seguridad reportados, todos clasificados como de bajo impacto. Vigencia 2024: Se identificó una diferencia en la ponderación asignada a esta vigencia entre las versiones del documento. En la Versión 1 se estableció una ponderación del 1 %; sin embargo, debido a que el cumplimiento de la actividad depende del insumo del Ministerio de Hacienda y Crédito Público y dicha entidad no suministró la información requerida, no fue posible ejecutar el seguimiento a los incidentes de seguridad de la Unidad. Vigencia 2025: Se elevó la consulta formal ante el Ministerio de Hacienda y Crédito Público para realizar el seguimiento de incidentes. No obstante, no se registraron eventos ni seguimientos durante el periodo. Se adjunta como evidencia la comunicación enviada y la respuesta recibida. Vigencia 2026: La ejecución de la actividad asociada se encuentra programada para el mes de noviembre, de acuerdo con el cronograma establecido.

Estrategia	Peso	Actividades	Peso	Producto	2023	2024	2025	2026	Actividades asociadas a Plan de Acción Anual 2023	Actividades asociadas a Plan de Acción Anual 2024	Actividades asociadas a Plan de Acción Anual 2025	Actividades asociadas a Plan de Acción Anual 2026	Observación Control y Evaluación
Cultura de la seguridad	20%	5.1 Socializar el modelo de privacidad y seguridad de la información	12%	Evidencias de socialización	3%	3%	3%	3%	No se encontró asociación en el Plan de Acción Anual por su fecha de formulación.	No se programaron acciones para la vigencia	URF2025_218_Socializar el manual, la política de privacidad y seguridad de la información a nivel institucional y el índice de información clasificada y reservada	URF2026_NOI_174_Socializar el modelo de privacidad y seguridad de la información	Se realizó la verificación del cumplimiento de la actividad, frente a la cual el proceso reportó: Vigencia 2023: Durante el mes de noviembre se socializó el Modelo de Privacidad y Seguridad de la Información con todos los servidores de la Unidad, de manera presencial. Es de indicar que esta evidencia no pudo ser verificada. Vigencia 2024: Se realizó capacitación relacionada con la privacidad y seguridad de la información el día 26 de noviembre de 2024. Es de indicar que esta evidencia no pudo ser verificada. Vigencia 2025: De acuerdo con lo programado para la vigencia, el proceso realizó la socialización de los documentos referentes a la privacidad y seguridad de la información a través de correo electrónico. Vigencia 2026: El proceso de socializó, por medio de correo electrónico enviado el día 29 de junio de 2026, el Manual de privacidad y seguridad de la información.

Estrategia	Peso	Actividades	Peso	Producto	2023	2024	2025	2026	Actividades asociadas a Plan de Acción Anual 2023	Actividades asociadas a Plan de Acción Anual 2024	Actividades asociadas a Plan de Acción Anual 2025	Actividades asociadas a Plan de Acción Anual 2026	Observación Control y Evaluación
		5.2 Realizar charla de tratamiento de datos personales	4%	Acta sesión- Listado de asistencia	1%	1%	1%	1%	No se encontró asociación en el Plan de Acción Anual por su fecha de formulación.	No se programaron acciones para la vigencia	URF2025_468_Realizar charla de tratamiento de datos personales	URF2026_NOI_175_Realizar capacitación de tratamiento de datos personales	Se realizó la verificación del cumplimiento de la actividad, frente a la cual el proceso reportó: Vigencia 2023: Durante el mes de noviembre se realizó la charla presencial de tratamiento de datos personales. Es de indicar que esta evidencia no pudo ser verificada. Vigencia 2024: Se reportó la realización de una capacitación relacionada con el tratamiento de datos personales, llevada a cabo el 26 de noviembre de 2024. Es de indicar que esta evidencia no pudo ser verificada. Vigencia 2025: Se verificó la realización de una jornada de sensibilización el 3 de diciembre de 2025, en la cual se abordaron los siguientes temas: • Contexto, políticas de Gobierno Digital y gestión documental. • Contexto y uso adecuado del Repositorio de Información Digital. • Tratamiento de datos personales. La evidencia revisada permite corroborar la ejecución de la actividad y los temas desarrollados durante la jornada de sensibilización. Vigencia 2026: Se verificó la realización de la capacitación denominada "Ley de Transparencia y Datos Personales", llevada a cabo el 29 de abril de 2026 mediante la plataforma Teams, con la participación de 44 servidores de la URF. Durante la jornada se desarrollaron, entre otros, los siguientes contenidos: • Concepto de transparencia y sus tipos. • Contexto nacional e internacional. • Ley 1712 de 2014: objeto y principios. • Ley 1712 de 2014: aspectos clave y desarrollo reglamentario. • Ley 1712 de 2014: publicidad y limitaciones. • Tratamiento de datos personales. La evidencia aportada permite corroborar la realización de la actividad, su fecha, modalidad y participación de los servidores, así como los principales contenidos abordados.

Estrategia	Peso	Actividades	Peso	Producto	2023	2024	2025	2026	Actividades asociadas a Plan de Acción Anual 2023	Actividades asociadas a Plan de Acción Anual 2024	Actividades asociadas a Plan de Acción Anual 2025	Actividades asociadas a Plan de Acción Anual 2026	Observación Control y Evaluación
		5.3 Enviar piezas gráficas para sensibilizar a los servidores y pasantes en torno a la privacidad	4%	Piezas gráficas	1%	1%	1%	1%	No se encontró asociación en el Plan de Acción Anual por su fecha de formulación.	No se programaron acciones para la vigencia	URF2025_469_Enviar piezas gráficas para sensibilizar a los servidores y pasantes en torno a la privacidad y la seguridad de la información	URF2026_NOI_176_Enviar piezas gráficas para sensibilizar a los servidores y pasantes en torno a la privacidad y seguridad de la información	Se realizó la verificación del cumplimiento de la actividad, frente a la cual el proceso reportó: Vigencia 2023: Durante el cuatrimestre final se remitieron seis (6) piezas comunicativas relacionadas con la privacidad y seguridad de la información. Es de indicar que esta evidencia no pudo ser verificada. Vigencia 2024: Se envió pieza comunicativa el día 20 de noviembre de 2024. Es de indicar que esta evidencia no pudo ser verificada. Vigencia 2025: El 03 de septiembre se remitió una pieza vía correo electrónico a los servidores públicos referente a tips de seguridad de la información Vigencia 2026: El martes 7 de abril de 2026 a las 2:00 p. m., se llevó a cabo una difusión por correo electrónico con el objetivo de informar y concientizar sobre la importancia de proteger la información personal durante la navegación en línea. La evidencia aportada permite corroborar la realización de la actividad, su fecha, modalidad y participación de los servidores, así como los principales contenidos abordados.

En el marco de la auditoría se realizó la revisión del Plan de Privacidad y Seguridad de la Información – PPSI correspondiente a la vigencia 2023, tomando como referencia la versión 1 del documento, de fecha 8 de junio de 2023, así como los registros de seguimiento y las evidencias suministradas por el proceso.

Como resultado de la revisión, se identificó que para la vigencia 2023 no se evidenció la incorporación de acciones específicas asociadas al PPSI en el Plan de Acción Anual – PAA. No obstante, se constató que durante la vigencia fueron ejecutadas actividades contempladas en el PPSI. Esta situación evidencia que existió gestión para avanzar en la implementación del modelo, aun cuando las actividades no se encontraban formalmente articuladas con el instrumento institucional de planeación anual, sin embargo, en el seguimiento realizado en el indicador no se adjuntan evidencias.

En relación con el seguimiento al indicador INAC_URF_IND083_GI_Cumplimiento del Plan de Privacidad y Seguridad de la Información – PPSI, se verificó que para la vigencia 2023 se había programado la ejecución del 30% del Plan, correspondiente a siete (7) actividades, y se reportó una ejecución del 36%; de acuerdo con la información suministrada por el proceso, la diferencia entre el porcentaje programado y el ejecutado se encuentra relacionada con la actividad "Elaborar el Manual de Privacidad y Seguridad de la Información y tramitar su formalización", cuya ejecución había sido distribuida porcentualmente entre las vigencias 2023 y 2024. Sin embargo, la actividad fue culminada y el Manual formalizado antes del plazo inicialmente previsto, lo que permitió registrar un porcentaje de ejecución superior al programado para la vigencia.

En cuanto al componente de oportunidad, el proceso reportó un resultado del 100%, correspondiente al cumplimiento de la meta establecida para el indicador.

Para la vigencia 2024 se identificó la programación de ocho (8) actividades en el PPSI. De acuerdo con la información reportada por el proceso, cuatro (4) actividades fueron gestionadas dentro de los plazos establecidos, lo que representó un cumplimiento del 11% respecto del total del Plan.

Las actividades restantes fueron objeto de reprogramación para el primer semestre de 2025, correspondiente al 33% de lo inicialmente proyectado para la vigencia de acuerdo con la ponderación asignada por el proceso. Según lo informado por el proceso, la reprogramación estuvo asociada principalmente a limitaciones de capacidad operativa del proceso de Gestión de la Información y a la dependencia de determinados servicios de tecnología administrados por el Ministerio de Hacienda y Crédito Público.

Al respecto, resulta pertinente que en los ejercicios de planeación y seguimiento se identifiquen de manera explícita aquellas actividades cuya ejecución depende de terceros o de otras áreas de la administración, estableciendo, cuando corresponda, responsables, hitos de seguimiento, mecanismos de coordinación y medidas de contingencia que permitan mitigar el impacto de dichas dependencias sobre el cumplimiento del Plan.

Como soporte del seguimiento fue suministrada la matriz consolidada de seguimiento del proceso de Gestión de la Información, en la cual se relacionan y describen las actividades desarrolladas durante la vigencia.

Frente al seguimiento correspondiente a la vigencia 2024, se identificó una oportunidad de mejora en la consistencia de la información utilizada para soportar el indicador, toda vez que en la matriz aportada como evidencia se registró un porcentaje de ejecución del 100%; sin embargo, de las ocho (8) actividades programadas para la vigencia, únicamente cuatro (4) fueron ejecutadas en su totalidad dentro del periodo evaluado, mientras que las restantes fueron reprogramadas para la vigencia 2025.

Esta situación evidencia la necesidad de fortalecer la metodología y los criterios empleados para determinar el porcentaje de ejecución del Plan, procurando que el resultado reportado guarde correspondencia con el estado real de cada actividad al cierre de la vigencia. En particular, se recomienda diferenciar entre actividades cumplidas, parcialmente cumplidas, no ejecutadas y reprogramadas dentro del cálculo del indicador.

Lo anterior resulta relevante para garantizar la confiabilidad, trazabilidad y razonabilidad de los resultados reportados, dado que un porcentaje de ejecución del 100% podría generar una percepción de cumplimiento integral del Plan, pese a que parte de las actividades inicialmente programadas no habían sido ejecutadas al cierre de la vigencia y debieron ser trasladadas al periodo siguiente.

Adicionalmente, mediante la consulta del Plan de Acción Anual correspondiente a la vigencia evaluada, se identificó la existencia de acciones adicionales relacionadas con el Plan de Privacidad y Seguridad de la Información.

- URF2024_013_Sensibilizar a los servidores sobre la política de gobierno digital
- URF2024_014_Sensibilizar a los servidores sobre temas relacionados con la seguridad digital
- URF2024_017_Reportar el avance en el cargue de documentos en SIED y presentar los resultados en las revisiones de procesos_C1-2024

- URF2024_018_Reportar el avance en el cargue de documentos en SIED y presentar los resultados en las revisiones de procesos_C2 - 2024
- URF2024_025_Elaborar política de gobierno de datos
- URF2024_026_Identificar, formalizar y gestionar los indicadores de privacidad y seguridad de la información
- URF2024_002_Realizar diagnóstico del modelo de privacidad y seguridad de la información

Esta situación resulta relevante frente a la trazabilidad de la planeación institucional, toda vez que evidencia que algunas acciones relacionadas con la implementación y fortalecimiento de la seguridad y privacidad de la información se gestionaron a través del PAA, mientras que otras se encontraban contenidas directamente en el PPSI.

En este sentido, se considera pertinente fortalecer la articulación entre el PPSI y el Plan de Acción Anual, de manera que exista una identificación clara y consolidada de las acciones que contribuyen al cumplimiento del Plan, independientemente del instrumento en el que se encuentren formalmente programadas. Esto facilitaría el seguimiento integral de los compromisos, evitaría posibles duplicidades u omisiones y permitiría establecer con mayor precisión el avance real del Plan frente a sus objetivos y resultados esperados.

Frente al seguimiento del Plan de Privacidad y Seguridad de la Información – PPSI correspondiente a la vigencia 2025, como resultado de la revisión, se identificaron diferencias entre las actividades contempladas en el documento del PPSI y aquellas formalmente incorporadas en el Plan de Acción Anual de la vigencia 2025, así como en las diferentes versiones del documento. Si bien se observó que la ponderación total asignada a las acciones corresponde a la establecida para la vigencia, se evidenció que algunas de estas fueron asociadas o distribuidas entre los diferentes componentes del Plan, sin que dicha correspondencia se encontrara reflejada de manera consistente en el documento del PPSI.

Al respecto, es pertinente señalar que, como resultado de los ejercicios de autodiagnóstico, seguimiento y análisis interno realizado por el proceso, pueden identificarse necesidades adicionales que hagan necesario incorporar o ajustar acciones para fortalecer los componentes inicialmente definidos. Esta dinámica resulta coherente con el enfoque de mejora continua y permite adaptar el Plan a las necesidades identificadas durante su ejecución. No obstante, para garantizar la coherencia, integridad y trazabilidad del instrumento de planeación, se considera necesario que las modificaciones o decisiones adoptadas queden formalmente documentadas y se incorporen en

las actualizaciones posteriores del PPSI, de manera que el documento vigente refleje las acciones efectivamente priorizadas y gestionadas por la Unidad.

Frente al cumplimiento del plan en la vigencia 2026, este actualmente se encuentra en ejecución, sin embargo a la fecha del presente informe se han finalizado 3 actividades de 7 programadas; se encontró diferencia en la asignación de la ponderación entre en documento del PPSI y aquellas formalmente incorporadas en el Plan de Acción Anual de la vigencia 2026.

Se **recomienda** al proceso de Direccionamiento y Planeación Institucional, en el marco de sus funciones de asesoría técnica, fortalecer los mecanismos de validación que aseguren la trazabilidad y la coherencia técnica entre los documentos descriptivos de los planes y las actividades programadas en el Plan de Acción Anual.

Si bien para las vigencias 2025 y 2026 se evidencia el fortalecimiento en la documentación y gestión de las actividades a través del SMGI, para las vigencias anteriores se identificaron oportunidades de mejora en la documentación y conservación de los soportes, toda vez que no fue posible verificar de manera integral la evidencia que acreditara el cumplimiento de las actividades programadas. Se **recomienda** fortalecer el reporte de seguimiento de las actividades del Plan, procurando que la información registrada describa de manera clara, precisa y detallada las acciones ejecutadas, el alcance, los resultados obtenidos y, cuando corresponda, las situaciones que hayan afectado su desarrollo. Asimismo, se recomienda adjuntar o referenciar las evidencias que soporten la ejecución reportada, de manera que estas faciliten su verificación y permitan determinar, de forma objetiva, oportuna y suficiente, el nivel de cumplimiento de las actividades programadas.

6.5. Fase de seguimiento y evaluación

De acuerdo con lo indicado en el documento el seguimiento al Plan de Privacidad y Seguridad de la Información – PPSI se realizará por medio del indicador asociado al cumplimiento de las actividades propuestas, de acuerdo con el peso porcentual asignado a cada una y para cada vigencia.

Para lo anterior se consulto el Sistema de Monitoreo a la Gestión Institucional – SMGI del cual se identificaron los indicadores:

- INAC_URF_IND083_GI_Cumplimiento del plan de privacidad y seguridad de la información – PPSI

La evaluación del indicador se efectuó con periodicidad anual, abarcando el seguimiento y la verificación de los resultados correspondientes a las vigencias 2023 y 2024.

Respecto a la documentación soporte, se realizó la revisión del grado de cumplimiento de las metas programadas, analizando de manera cualitativa las situaciones operativas y administrativas que incidieron en la ejecución de las actividades asociadas.

No obstante, se identificó que para la vigencia 2024 no se realizó el registro ni la parametrización de la meta en el SMGI. Al respecto, se hace necesario garantizar oportunamente la inclusión de los valores meta en la plataforma, con el fin de asegurar la disponibilidad de datos históricos, la trazabilidad del desempeño y un análisis comparativo adecuado del indicador.

Si bien para las vigencias 2025 y 2026 se evidencia el fortalecimiento en la documentación y gestión de las actividades a través del SMGI, para las vigencias anteriores se identificaron oportunidades de mejora en la documentación y conservación de los soportes. Por lo tanto, se **recomienda** la implementación de herramientas o repositorios de consolidación documental que permitan compilar de manera sistemática, ordenada y verificable la evidencia que sustenta el cumplimiento integral de las actividades, así como la descripción detallada de las mismas.

- URF_IND108_GI_Cumplimiento del Plan de Seguridad y Privacidad de la Información – PPSI

El análisis del indicador se genera de manera automática a partir del avance registrado para las actividades programadas en el Plan de Acción Anual – PAA para las vigencias 2025 y 2026.

El seguimiento del indicador se realiza con periodicidad trimestral, permitiendo efectuar monitoreo sobre el avance de las acciones asociadas al cumplimiento del Plan.

Como resultado de la revisión, se identificaron diferencias entre las actividades contempladas en el documento del PPSI y aquellas formalmente incorporadas en el Plan de Acción Anual de la vigencia 2025 y 2026 asociadas a la gestión de privacidad y seguridad de la información. Si bien se observó que la

ponderación total asignada a las acciones corresponde a la establecida para la vigencia, se evidenció que algunas de estas fueron asociadas o distribuidas entre los diferentes componentes del Plan, sin que dicha correspondencia se encontrara reflejada de manera consistente en el documento del PPSI.

Se **recomienda**, que en lo sucesivo se garantiza la coherencia en las actividades programadas y las registradas en el documento descriptivo de manera que el este refleje las acciones efectivamente priorizadas y gestionadas por la Unidad.

6.6. Fase de mejora

La Unidad contempla mecanismos orientados a incorporar los resultados de la fase de seguimiento y evaluación en el proceso de mejora continua, mediante la implementación de acciones de mejora, acciones de mitigación y lecciones aprendidas, las cuales podrán ser incorporadas en el plan de mejoramiento o en el Plan de Acción de cada vigencia. Lo anterior evidencia la definición de un esquema para retroalimentar la gestión a partir de los resultados obtenidos.

No obstante, para fortalecer la efectividad de este mecanismo, resulta pertinente que se establezca y documente de manera clara la trazabilidad entre los resultados identificados, las oportunidades de mejora o situaciones de impacto, las acciones formuladas, el instrumento en el que serán incorporadas, los responsables, los plazos y los resultados esperados. Esto permitirá verificar que los resultados de la evaluación no se limiten a su identificación, sino que efectivamente se traduzcan en acciones concretas orientadas al cierre de brechas y al fortalecimiento continuo del Plan de Privacidad y Seguridad de la Información.

Se **recomienda** elaborar un informe consolidado de los resultados de implementación del Plan, que integre tanto el análisis cuantitativo de su cumplimiento como una valoración cualitativa de los principales logros, avances, dificultades, retos y lecciones aprendidas. Lo anterior, con el propósito de que los resultados constituyan un insumo para la formulación y actualización del siguiente Plan, facilitando la identificación y priorización de acciones de mejora y su correspondiente trazabilidad en los instrumentos de planeación o mejoramiento institucional. Asimismo, se **recomienda** utilizar este informe como resultado del proceso para su socialización ante la Alta Dirección y los servidores de la Unidad, fortaleciendo la retroalimentación y la apropiación de las acciones orientadas al mejoramiento continuo.

7. Gestión del riesgo

Se identificaron los siguientes riesgos asociados al Modelo de Privacidad y Seguridad de la Información administrado por el proceso de Gestión de la Información.

URF-GI-03 Pérdida de integridad, disponibilidad o confidencialidad de la información en aplicativos críticos de la URF cuya descripción es Posibilidad de afectación reputacional y económica por la pérdida de integridad y disponibilidad de la información en aplicativos críticos de la URF, debido accesos no autorizados.

El cual fue identificado desde el 2025 y actualizado de acuerdo a la actualización de la Política de Administración de Riesgos en el mes de agosto de 2026.

CONTROLES	MONITOREO DEL CONTROL
A.12.6.1-Gestión de las vulnerabilidades técnicas aplicativos críticos URF **Evidencia:** Formato control de auditoría.	Las plataformas auditadas (Carnetización, Trazabilidad, Directorio Grupo de Valor, Moodle y SARA) cuentan con ambientes de desarrollo. En el caso particular de SARA, las pruebas dependen del proveedor Unión Soluciones frente a cambios normativos, corrección de fallas o actualizaciones. Por su parte, las demás plataformas corresponden a desarrollos propios, los cuales se rigen bajo la metodología interna de desarrollo de software. Se adjunta archivos de auditoría de cada plataforma. **Evidencia:** Archivos en Excel con la auditoria del login de los aplicativos.
A.6.1.1-Seguridad de la información roles y responsabilidades - Monitorear los roles y responsabilidades en los sistemas de información **Evidencia:** Formato control de auditoría	A partir de la revisión de la hoja USUARIOS_ROLES Las plataformas auditadas (Carnetización, Trazabilidad, Directorio Grupo de Valor y SARA), se identificó que durante el segundo cuatrimestre de 2026 se crearon 3 nuevos usuarios: <u>Carnetización</u> A partir del 1 de mayo de 2026, se registró la creación del siguiente usuario: Yuly Paola Baracaldo Rivera: rol Crear Carnés, creado el 5 de agosto de 2026. Con este registro, el aplicativo de Carnetización cuenta actualmente con 4 usuarios, distribuidos en los siguientes roles: Administrador Completo: 1 usuario Impresión: 1 usuario Crear Carnés: 2 usuarios <u>SARA</u> Para el aplicativo SARA, no se identificaron usuarios creados después del 1 de mayo de 2026. Por lo tanto, no se reportan nuevos usuarios correspondientes al segundo cuatrimestre de 2026. El aplicativo de SARA cuenta actualmente con 72 usuarios,

	distribuidos en los siguientes roles: Administrador Completo: 5 usuario Usuario Aplicación: 67 usuario <u>Trazabilidad</u> A partir del 1 de mayo de 2026, se registró la creación del siguiente usuario: Angie Johanna Corredor Estrella: rol Auditora, creado el 3 de Julio de 2026. Con este registro, el aplicativo de Trazabilidad cuenta actualmente con 5 usuarios, distribuidos en los siguientes roles: Administrador Completo: 1 usuario Perfil para gestionar Trazabilidad: 3 usuario Perfil Auditoria: 1 usuarios <u>Horas extras</u> Para el aplicativo Horas extras, no se identificaron usuarios creados después del 1 de mayo de 2026. Por lo tanto, no se reportan nuevos usuarios correspondientes al segundo cuatrimestre de 2026. El aplicativo de Horas extras cuenta actualmente con 6 usuarios, distribuidos en los siguientes roles: Administrador Completo: 1 usuario Administrador Herramienta: 3 usuario Usuario Aplicación: 2 usuario **Evidencia:** Archivos en Excel con la auditoria del login de los aplicativos.

URF-GI-04 Pérdida de confidencialidad de la información de activos críticos cuya descripción es Posibilidad de afectación reputacional por la pérdida de confidencialidad de la información, actas del Consejo Directivo; historias laborales o información de nómina debido errores en la asignación de permisos de acceso.

CONTROLES	MONITOREO DEL CONTROL
A.13.2.4-Acuerdos de confidencialidad o de no divulgación **Evidencia:** Formato de acuerdo de confidencialidad de consejo directivo	Durante el cuatrimestre se gestionó la suscripción y cargue de siete (7) acuerdos de confidencialidad de la información, correspondientes a servidores, pasantes y miembros del Consejo Directivo, así: Servidor vinculado: Jenny García. Pasantes: Johan Beltrán, Mónica Montiel y César Rodríguez. Miembros del Consejo Directivo: Jorge Lemus, Lina Rodríguez y Jorge coronel. Los acuerdos fueron formalizados y cargados de acuerdo con la vinculación y participación de cada persona, con el propósito de establecer los compromisos relacionados con el manejo, reserva y protección de la información institucional. Lo anterior contribuye al fortalecimiento de los controles de confidencialidad y seguridad de la información, mediante la

	formalización de las obligaciones de quienes tienen acceso a información institucional, contribuyendo a prevenir su divulgación, uso o acceso no autorizado. **Evidencia:** Acuerdos de confidencialidad por CD y por vinculación
A.9.4.1-Restricción de acceso a información - Gestionar el acceso a la información física y digital **Evidencia:** Matriz control de accesos	Durante el segundo cuatrimestre de 2026, se realizó seguimiento a los permisos de acceso a los archivos físicos y digitales mediante el control de accesos al SharePoint y al RID. Se evidenciaron ajustes asociados principalmente a desvinculaciones, cambios de funciones y otorgamiento de permisos temporales, los cuales fueron gestionados oportunamente de acuerdo con las necesidades de los servidores. No se evidenció materialización del riesgo, toda vez que los accesos fueron retirados, modificados o asignados según correspondía, manteniendo el control sobre la información y restringiendo su acceso al personal autorizado. **Evidencia:** Matriz de control de accesos

Durante el mes de agosto, la Unidad realizó la actualización de los riesgos institucionales, en atención a los lineamientos establecidos en la nueva versión de la Política de Administración del Riesgo. Esta actualización estuvo orientada a validar la identificación, valoración y tratamiento de los riesgos, así como a asegurar su articulación con los cambios y directrices definidos en la política.

De manera complementaria, se efectuó el monitoreo de los riesgos identificados, con el propósito de verificar la implementación y avance de las acciones de tratamiento, así como la evolución de los riesgos y la efectividad de los controles establecidos. Los resultados de este ejercicio constituyen un insumo para la toma de decisiones, la identificación de oportunidades de mejora y, cuando corresponda, la formulación o ajuste de acciones orientadas a fortalecer la gestión y prevenir la materialización de los riesgos.

8. Aspectos positivos, observaciones y oportunidades de mejora

8.1. Aspectos positivos

Como fuente de información para el diagnóstico y la formulación del Plan, la Unidad tuvo en cuenta los resultados obtenidos en la medición del Índice de Desempeño Institucional. Si bien en ejercicios anteriores se formularon recomendaciones orientadas a fortalecer el análisis de estos resultados, se considera pertinente que, en la actualización y formulación de los próximos planes, estos sean incorporados de manera más integral, no solo como un referente de diagnóstico, sino como línea base para establecer el nivel de

desempeño de la Unidad y determinar su evolución frente a las dimensiones y políticas relacionadas con la privacidad y seguridad de la información.

Durante el periodo evaluado se evidenció la formalización y actualización de instrumentos relacionados con la gestión de privacidad y seguridad de la información, entre ellos la Política y el Manual, así como la definición de metodologías para la gestión de riesgos de seguridad digital. Estos elementos contribuyen a consolidar el marco institucional requerido para la operación del modelo.

Se evidenció la identificación y actualización de riesgos asociados a la seguridad de la información, así como la realización de actividades de monitoreo y seguimiento. De manera particular, se verificó el seguimiento al riesgo relacionado con la pérdida de integridad, disponibilidad o confidencialidad de la información consignada en medios digitales.

Se evidenció la realización de actividades de capacitación y sensibilización relacionadas con privacidad, seguridad de la información, tratamiento de datos personales, transparencia y uso adecuado de los recursos de información.

La Unidad cuenta con indicadores asociados al cumplimiento del PPSI y ha establecido mecanismos de seguimiento a través del SMGI, el indicador se genera a partir del avance registrado en las actividades del Plan de Acción Anual y cuenta con seguimiento periódico, lo que constituye una herramienta para monitorear la ejecución de las acciones programadas.

8.2. Observaciones

De acuerdo con la evaluación realizada al Plan de Privacidad y Seguridad de la Información 2023 - 2026, no se identificaron incumplimientos que ameriten la formulación de acciones de mejora en el Plan de Mejoramiento Institucional. No obstante, durante el desarrollo de la auditoría se identificaron oportunidades de mejora y se formularon recomendaciones orientadas a fortalecer la trazabilidad y documentación del Plan.

8.3. Oportunidades de mejora

Fortalecer la trazabilidad integral del Plan, de manera que permita relacionar de forma clara y verificable los resultados del diagnóstico, las brechas identificadas, las acciones o controles definidos, los productos, responsables, resultados obtenidos y las acciones de mejora. Esto facilitará valorar no solo el cumplimiento de las actividades, sino también su pertinencia y contribución al fortalecimiento del modelo.

Fortalecer la actualización del Plan frente a cambios en el contexto institucional, incorporando de manera sistemática los cambios organizacionales, tecnológicos y operativos que puedan modificar las prioridades, riesgos, responsables o acciones previstas. De esta manera, el Plan podrá mantenerse como un instrumento dinámico y pertinente durante toda su vigencia.

Fortalecer la documentación y conservación de los autodiagnósticos, asegurando la disponibilidad de los instrumentos utilizados, criterios de valoración, resultados y evidencias que permitan establecer la línea base y sustentar técnicamente la evolución del nivel de madurez. Asimismo, incorporar los resultados de los ejercicios posteriores en las actualizaciones del Plan, evidenciando su incidencia en la priorización o ajuste de las acciones.

Fortalecer por parte del proceso de Direccionamiento y Planeación Institucional, en el marco de sus funciones de asesoría técnica, fortalecer los mecanismos de validación que aseguren la trazabilidad y la coherencia técnica entre los documentos descriptivos de los planes y las actividades programadas en el Plan de Acción Anual.

Fortalecer el análisis cualitativo de los resultados del Plan, mediante la elaboración de un informe consolidado al cierre de su ciclo de implementación que, además del porcentaje de cumplimiento, presente los principales logros, avances, dificultades, retos, brechas pendientes y lecciones aprendidas. Este producto debería constituirse en un insumo para la formulación del siguiente Plan y para su socialización ante la Alta Dirección y los servidores de la Unidad.

Así como las otras recomendaciones, que se desarrollaron a lo largo del presente informe.

9. Conclusiones

Como resultado de la auditoría realizada al Plan de Privacidad y Seguridad de la Información 2023–2026, se concluye que la Unidad ha adelantado acciones orientadas a la implementación y fortalecimiento del Modelo de Privacidad y Seguridad de la Información, evidenciándose avances en la definición de instrumentos institucionales, gestión de riesgos, implementación y seguimiento de controles, gestión de incidentes y fortalecimiento de la cultura de seguridad de la información. La estructura adoptada contempla cinco estrategias y un conjunto de actividades orientadas a desarrollar el ciclo de implementación y mejora del modelo.

Se identificaron aspectos susceptibles de fortalecimiento, orientados a contribuir a la adecuada finalización del Plan correspondiente al presente

cuatrienio y a fortalecer la formulación del próximo, los cuales se desarrollan a lo largo del presente informe.

De igual manera, se destacan aspectos positivos por parte de la Unidad el cual contempla mecanismos para que los resultados del seguimiento y evaluación alimenten el proceso de mejora continua mediante acciones de mejora, mitigación y lecciones aprendidas.

En consecuencia, se considera que el principal reto para el siguiente ciclo del Plan de Privacidad y Seguridad de la Información consiste en evolucionar de un enfoque centrado principalmente en el cumplimiento y seguimiento de actividades hacia un esquema de gestión orientado a resultados, cierre de brechas y mejora demostrable de la madurez del modelo. Para ello, será fundamental consolidar una línea base, actualizar periódicamente los diagnósticos, articular los instrumentos de planeación, fortalecer la gestión de evidencias y establecer mecanismos que permitan valorar los efectos de las acciones implementadas.

10. Elaboración del informe

Nombre del auditor:	Angie Johanna Corredor Estrella
Fecha del informe:	03 de septiembre de 2026