UNIDAD DE RESTITUCIÓN DE TIERRAS

UNIDAD ADMINISTRATIVA ESPECIAL DE GESTIÓN DE RESTITUCIÓN DE TIERRAS DESPOJADAS (UAEGRTD)

INFORME OCI-2025-27

AUDITORIA INTERNA ESPECIAL

SISTEMA DE REGISTRO DE TIERRAS DESPOJADAS Y ABANDONADAS FORZOSAMENTE (SRTDAF)

OFICINA DE CONTROL INTERNO

OCTUBRE DE 2025

DESTINATARIOS:

- **Rangel Giovani Yule Zape**, Director General.
- **Jaqueline Campos Rincón**, Secretaria General.
- **Aura Patricia Bolívar Jaime**, Subdirectora General.
- **Paula Andrea Villa Vélez**, Directora Jurídica.
- **María Estefany Checa Narváez**, Directora Territorial sede Pasto.
- **Wilson Zapata**, Jefe Oficina Asesora de Planeación.
- **Carlos Alberto De la Ossa Hurtado**, Jefe Oficina de Tecnologías de la Información.

RESPONSABLE DEL INFORME:

- **Claudia Marcela Pinzón Martínez**, Jefe Oficina de Control Interno.

EQUIPO AUDITOR:

- **Carlos Alberto Quiñones Cárdenas**, Contratista Oficina de Control Interno.

OBJETIVO:

Evaluar de forma independiente el diseño y la eficacia operativa de los controles internos implementados en la Unidad Administrativa Especial de Gestión de Restitución de Tierras Despojadas (UAEGRTD), para gestionar los riesgos asociados al funcionamiento y seguridad del Sistema de Registro de Tierras Despojadas y Abandonadas Forzosamente – SRTDAF.

ALCANCE:

El alcance establecido para la realización de este trabajo comprende la evaluación de los controles internos relacionados con el objetivo propuesto, incluyendo:

- Atención de casos de solicitud de software.
- Ejecución de actividades de control para las etapas de solicitud, análisis, diseño, desarrollo, pruebas y entrada en producción del SRTDAF establecidas en el procedimiento de soluciones de software.
- Asignación de roles y perfiles en el sistema de Registro.
- Implementación de directrices de la política de desarrollo seguro.
- Evaluación de controles de los riesgos asociados al desarrollo y gestión de software.
- Adopción y ejecución de controles para la administración y uso del SRTDAF
- Implementación de controles para garantizar la seguridad de la información del SRTDAF
- Aplicabilidad de lineamientos y controles asociados al Compendio de Políticas Complementarias de Seguridad y Privacidad de la Información.

Periodo Auditado: corte a 31 de julio de 2025.

Nota: El establecimiento de este período no limita la facultad de la Oficina de Control Interno para pronunciarse sobre hechos previos o posteriores que, por su nivel de riesgo o materialidad, deban ser revelados.

CRITERIOS:

NORMATIVIDAD EXTERNA

- Decreto 767 de 2022 *"Por medio del cual se establecen los lineamientos generales de la Política de Gobierno Digital".*
- Resolución 746 de 2022 *"Por medio de la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y adopta el Modelo de Seguridad Digital - MSPI como habilitador de la Política de Gobierno Digital".*

NORMATIVIDAD INTERNA

- Decreto 4801 de 2011 *"Por el cual se establece la estructura interna de la Unidad Administrativa Especial de Gestión de Restitución de Tierras Despojadas".*
- Documentación dispuesta en el SIPG del proceso de Gestión de Tecnologías de la Información:
  - Procedimiento GT-PR-15 - Creación de incidencias y solicitudes. Versión 9
  - Procedimiento GT-PR-01 - Atención de requerimientos de software. Versión 5
  - Procedimiento GT-PR-02 - Soluciones de software, versión 7
  - Procedimiento GT-PR-21 - Gestión de cambios de TI, Versión 2,
  - Documento Estratégico GT-ES-02 - Compendio de Políticas Complementarias de Seguridad y Privacidad de la Información, versión 7.

RIESGOS IDENTIFICADOS EN LA AUDITORÍA:

A continuación, se relacionan los riesgos evidenciados en el mapa de riesgos institucional, así como los identificados por el equipo auditor que fueron abordados dentro de la auditoría:

Tabla N°1 Riesgos abordados en la auditoría

DESCRIPCIÓN	CUBIERTO EN LA AUDITORÍA
Incluido en el Mapa de Riesgos de Gestión	
GT-RSI-3: Posibilidad de pérdida de la integridad y confidencialidad de Sistemas de información y Aplicaciones de Centros de datos y Nube debido a accesos no autorizados, porque la activación y desactivación de credenciales se hace de forma manual, esto puede ocasionar una fuga y alteración de información lo que puede llevar a afectar negativamente la reputación de la unidad.	Si
GT-RG-9: Posibilidad de afectación reputacional de la Entidad por pérdida de la disponibilidad y continuidad de los servicios de TI debido a inadecuada asignación de recursos y deficiencias en la gestión y monitoreo de la seguridad, plataforma y componentes de la infraestructura de TI.	Si

DESCRIPCIÓN	CUBIERTO EN LA AUDITORÍA
GT-RG-10: Posibilidad de afectación económica y reputacional para la Unidad por adquisición y/o desarrollo de aplicaciones no funcionales debido a insuficiente claridad, conocimiento y comunicación entre el equipo desarrollador y los usuarios para establecer y validar la necesidad y requerimientos, y deficiencias en el procedimiento de desarrollo de software.	Si
Identificados por la Oficina de Control Interno	
RI-OCI-1: Posibilidad de afectación económica y reputacional por debilidades en la segregación de ambientes de desarrollo, pruebas y producción debido a el acceso a datos y modificaciones no autorizadas en la operación del SRTDAF.	Si
RI-OCI-2: Posibilidad de afectación operativa por modificaciones no autorizadas en la herramienta GITLAB debido a la asignación errónea de privilegios de acceso y debilidades en la custodia del código fuente y versionamiento del SRTDAF.	Si
RI-OCI-3: Posibilidad de afectación económica y reputacional por deficiencia en la gestión de Logs de auditoría debido a debilidades en la generación, análisis y custodia de los registros de auditoría del módulo de seguridad del SRTDAF.	Si
RI-OCI-4: Posibilidad de afectación operativa por perdida de seguridad o privacidad de la información del SRTDAF, ante la ausencia o inaplicabilidad de controles que permitan evaluar y gestionar debilidades frente a la integridad del sistema y de su información.	Si
RI-OCI-5: Posibilidad de afectación económica y/o reputacional por procesos sancionatorios debido a la perdida de la información o de su integridad, por ausencia de controles de respaldo o inaplicabilidad de los existentes.	Si
RI-OCI-6: Posibilidad de afectación económica y/o reputacional ante el inicio de procesos administrativos o sancionatorios, por debilidades o desviaciones en la operatividad y funcionalidad del SRTDAF a causa de la ausencia de documentación para su uso.	Si

Fuente: construcción propia del equipo auditor

RESULTADOS OBTENIDOS DEL PROCESO AUDITOR:

1. FORTALEZAS:

- Se cuenta con procedimientos y formatos de Gestión de Cambios que incluyen evaluaciones de riesgo antes del despliegue de nuevos desarrollos.
- El SRTDAF cuenta con un módulo de seguridad, el cual permite registrar Logs de eventos como accesos exitosos, intentos fallidos, cambios de configuración y gestión de usuarios, con acceso restringido, permitiendo generar evidencias para analizar la ocurrencia y trazabilidad de eventos significativos del uso del sistema.
- Se cuenta con procedimientos institucionales y la herramienta GLPI para radicar y gestionar solicitudes e incidentes del SRTDAF, lo que evidencia la implementación de esquemas de soporte y atención de las necesidades de los usuarios funcionales.

- Finalmente, durante la ejecución de la prueba de recorrido realizada al Sistema de Registro de Tierras Despojadas y Abandonadas Forzosamente (SRTDAF), se verificó el funcionamiento de múltiples módulos del sistema, incluyendo: Solicitud, Vida Catastral, Trámite Administrativo, Sujetos de Especial Protección, Demanda y Sentencia. Como resultado, se evidenció que las funcionalidades evaluadas operan de manera satisfactoria, cumpliendo con los flujos establecidos, validaciones técnicas, controles documentales y condiciones previas requeridas para cada etapa del proceso. El sistema, entre otros aspectos cuenta con una interfaz guiada por etapas, que facilita el diligenciamiento de la información dentro del flujo, validaciones condicionales y técnicas, que buscan incorporar controles de calidad de los datos, funcionalidades de interoperabilidad incorporadas como la validación con la Registraduría, control documental estructurado con expedientes dinámicos para facilitar la consulta y trazabilidad, gestión de roles que permite segregación de funcionalidades por perfil. No obstante, se recomienda realizar pruebas complementarias al sistema a partir de las necesidades de los usuarios funcionales del sistema, debido a que la prueba de recorrido efectuada se abordó a partir de los requerimientos funcionales solicitados a la Oficina de Tecnologías de la Información que actualmente se encuentran en ambiente de producción.

2. HALLAZGOS:

A continuación, se presenta un resumen ejecutivo de los hallazgos elevados en el marco del proceso auditor, cuya información a detalle podrá ser consultada en los formatos de "Reporte de Hallazgo", los cuales forman parte integra del presente informe:

HALLAZGO N. 1:

Tabla N° 2 Resumen ejecutivo del Reporte de hallazgo N° 1

TÍTULO:	***Debilidades en la documentación que soporta la ejecución de los procedimientos asociados al desarrollo de software del SRTDAF.***
SITUACIÓN EVIDENCIADA:	

Con el objetivo de verificar el cumplimiento de los procedimientos asociados al desarrollo de software para el Sistema de Restitución de Tierras Despojadas y Abandonadas Forzosamente (en adelante SRTDAF), la Oficina de Control Interno llevó a cabo la verificación del cumplimiento y documentación de los procedimientos "*GT-PR-15 - Creación de incidencias y solicitudes"* Versión 9*, "GT-PR-01 - Atención de requerimientos de software"* Versión 5, *"GT-PR-02 - Soluciones de software"* versión 7, y *"GT-PR-21 - Gestión de cambios de TI" Versión 2",* de la siguiente manera:

Se analizó el listado de requerimientos de desarrollo del SRTDAF suministrado el 15 de agosto de 2025 por la Oficina de Tecnologías de la Información (OTI), el cual registraba sesenta y cinco (65) requerimientos.

A partir de lo anterior, se seleccionó la muestra de dieciséis (16) casos, para los cuales se solicitó la respectiva evidencia documental, los cuales se detallan a continuación, indicando el nombre del requerimiento, la fecha de solicitud (la cual da inicio al ciclo de desarrollo de software), y la fecha de entrada en producción.

Para los dieciséis (16) casos seleccionados que fueron objeto de verificación del cumplimiento de las disposiciones procedimentales para el desarrollo de software, se evidenció que cada uno debía de pasar por quince (15) hitos al llegar a producción, de esta manera, se concluía que el total esperado de elementos a evaluar era de 240 ítems. Sin embargo, se observó que no todos los casos habían llegado a la etapa de producción al momento de la evaluación realizada, por ende, cuarenta y siete (47) ítems de la muestra no aplicaban.

Como resultado se tuvo un total de 193 actividades objeto de verificación, producto de lo cual se evidenció lo siguiente:

1. **Cumplimiento de actividades o hitos procedimentales**

La siguiente tabla, muestra gráficamente el resultado de la revisión de los 16 casos de muestreo, y su cumplimiento con los 15 hitos de las etapas de desarrollo de software. Los resultados presentados, fueron verificados con la OTI en diversas mesas de trabajo realizadas entre el 12 de agosto hasta el 17 de septiembre de 2025:

Colorimetría:

OK	Ejecutado sin desviaciones	**X1**	El soporte está relacionado con la actividad, pero no se aporta el entregable de acuerdo con lo establecido en el procedimiento.	**X2**	El soporte remitido no evidencia la realización de la actividad establecida en el procedimiento.	**X3**	No se remitió evidencia de la realización de la actividad del procedimiento.

Tabla N° 2.1. Resultado verificación cumplimiento de hitos sobre los casos objeto de evaluación.

HITOS VERIFICADOS		REQUERIMIENTOS															
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Etapa de solicitud de software	1. GLPI de solicitud de software	X2	OK	OK	X3	X3	OK	X2	X3	X2	OK	X3	X2	X2	X3	X3	X3
	2. GT-FO-07 Solicitud de software, adjunto al GLPI	X1	X3	OK	X2	X2	OK	X3	X3	X2	OK	X3	X3	X3	X1	X3	X3
	3. GLPI con el resultado de análisis de viabilidad	X1	X1	X1	X1	X1	X1	X1	X1	X1	X1	X1	X1	X1	X1	X1	X1
Etapa de análisis, diseño y consolidación funcional y no funcional.	4. GT-FO-01 Documento de Levantamiento de Requerimientos entre el área solicitante y la Oficina de Tecnologías de la Información.	X2	X1	OK	OK	X1	X1	X1	X3	X1	OK	X1	OK	X1	X1	X2	X1
	5. GT-FO-48 Historia de Usuario, realizado a partir de las reuniones aclaratorias con el fin de precisar los requerimientos funcionales	X2	X3	OK	OK	X3	X3	X3	OK	OK	OK	X3	OK	OK	X1	X3	X1
	6. GD-FO-22 Acta de reunión de aprobación de Levantamiento de Requerimientos y la Historia de Usuario	X3	X3	OK	X3	X3	X2	X3	X3	X2	X2	X3	X3	X2	X3	X3	X2
Etapa de desarrollo.	7. Generación y/o actualización de la documentación técnica	X2	OK	N/A	OK	X3	X3	X3	OK	X2	X2	N/A	X3	X2	OK	OK	X3
Etapa de pruebas y control de calidad.	8. GT-FO-12 Guion casos de pruebas	X2	X3	N/A	OK	X3	X3	X3	OK	OK	OK	N/A	OK	OK	N/A	N/A	OK
	9. GT-FO-42 Reporte de incidencias	X3	X1	N/A	OK	X3	X3	X3	OK	OK	OK	N/A	OK	X3	N/A	N/A	X3
	10. GT-FO-41 Pruebas de acepción de usuario	X3	X1	N/A	OK	X2	X1	X1	OK	OK	OK	N/A	OK	OK	N/A	N/A	X1
	11. Ticket generado en la mesa de servicios del despliegue de los componentes de aplicación y base de datos en ambiente de pruebas	X3	X3	N/A	X2	X3	X3	X3	X2	OK	OK	N/A	N/A	X3	N/A	N/A	X3
Etapa de gestión para salida a producción.	12. Correo de autorización de paso a producción	N/A	X3	N/A	OK	X3	X3	X3	X2	N/A	OK	N/A	N/A	X3	N/A	N/A	X3
	13. GLPI de autorización de paso a producción	N/A	X3	N/A	OK	X3	X3	X3	OK	N/A	OK	N/A	N/A	X3	N/A	N/A	X3

	14. GT-FO-35 Solicitud de Cambio de autorización de paso a producción	N/A	X3	N/A	OK	X3	X3	X3	OK	N/A	OK	N/A	N/A	X3	N/A	N/A	X3
	15. Correo electrónico informando el resultado de la implementación del cambio en producción	N/A	X3	N/A	OK	X3	X3	X3	X3	N/A	OK	N/A	N/A	X3	N/A	N/A	X3

Fuente: elaboración propia equipo auditor

De esta manera se concluyó que:

- **OK = 28%** (54 ítems) de los soportes cumplen plenamente con lo establecido en los procedimientos internos.
- **X1 = 17.6%** (34 ítems) permiten inferir que el hito o la actividad fue realizada, pero no se aporta el entregable de acuerdo con lo establecido en el procedimiento.
- **X2 = 13%** (25 ítems) cuentan con soporte, pero este no evidencia el hito o la ejecución de la actividad esperada de acuerdo con el procedimiento.
- **X3 = 41.4%** (80 ítems) no tienen evidencia documental que respalde la realización de la actividad o hito correspondiente al proceso de desarrollo de software.

Estos resultados reflejan una baja trazabilidad documental en el proceso de desarrollo de software, lo cual afecta la capacidad de verificación del cumplimiento de los procedimientos GT-PR-01 Atención de requerimientos de software. Versión 5, GT-PR-02 Soluciones de software, versión 7, y GT-PR-21 Gestión de cambios de TI, Versión 2 aplicados al SRTDAF.

2. Debilidades frente a la conservación documental

Durante la verificación técnica al Sistema de Registro de Tierras Despojadas y Abandonadas Forzosamente (SRTDAF), se analizó el listado de requerimientos de desarrollo del Sistema de Registro de Tierras Despojadas y Abandonadas Forzosamente (SRTDAF), suministrado por la Oficina de Tecnologías de la Información (OTI) el 15 de agosto de 2025, se observó que el listado de requerimientos suministrado no daba cubrimiento a la totalidad de módulos implementados en el SRTDAF, permitiendo evidenciar que, no se cuenta con un repositorio unificado y actualizado que contenga la relación y soportes de todos los documentos asociados a los requerimientos y desarrollos del software, especialmente para los desarrollos realizados antes de la vigencia 2021. Esta situación afectó el alcance de las pruebas realizadas al cumplimiento de los procedimientos de desarrollo de software debido a que estas se realizaron sobre los requerimientos de desarrollo realizados a partir de la vigencia 2022.

CIRTERIOS ASOCIADOS:	▪ GT-PR-15 - Creación de incidencias y solicitudes. Versión 9. Ítem 7: Las solicitudes de software, deben ser enviadas a la Oficina de Tecnologías de la Información, a través de GLPI, anexando el formato GT-FO-07 Solicitud de software debidamente firmado. ▪ GT-PR-01 Atención de requerimientos de software. Versión 5. Ítem 2: Se requiere analizar la solicitud de software, y revisar la viabilidad del requerimiento. ▪ GT-PR-02 Soluciones de software, versión 7. Ítem 1: Para la solicitud de software se debe realizar la identificación de los requerimientos, y generar el GT-FO-01 Documento de Levantamiento de Requerimientos entre el área solicitante y la Oficina de Tecnologías de la Información. ▪ GT-PR-02 Soluciones de software, versión 7. Ítem 2: Se debe generar el documento GT-FO-48 Historia de Usuario, realizado a partir de las reuniones aclaratorias con el fin de precisar los requerimientos funcionales. ▪ GT-PR-02 Soluciones de software, versión 7. Ítem 3: Se debe aprobar la especificación del requerimiento a través de acta de reunión. ▪ GT-PR-02 Soluciones de software, versión 7. Ítem 9: Establece la actividad de Generación y/o actualización de la documentación técnica del desarrollo de software. ▪ GT-PR-02 Soluciones de software, versión 7. Ítem 11: Se debe generar el guion casos de pruebas por medio del GT-FO-12 Guion casos de pruebas. ▪ GT-PR-02 Soluciones de software, versión 7. Ítem 12: Se realiza ejecución de pruebas de conformidad con el Guion casos de pruebas, y generar el GT-FO-42 Reporte de incidencias. ▪ GT-PR-02 Soluciones de software, versión 7. Ítem 13: Se ejecutan las pruebas de aceptación de usuario, y generar el documento GT-FO-41 Pruebas de acepción de usuario. ▪ GT-PR-02 Soluciones de software, versión 7. Ítem 15: Se realiza el despliegue en ambiente de pruebas de los componentes de aplicación y base de datos, generando GLPI en la mesa de servicios.

	▪ GT-PR-21 Gestión de cambios de TI, Versión 2. Ítem 5: Se autoriza o rechaza el cambio presentado por medio de GLPI, correo electrónico, y anexando el formato GT-FO-35 Solicitud de Cambio de autorización de paso a producción. ▪ GT-PR-02 Soluciones de software, versión 7. Ítem 21: Se realiza la notificación por correo electrónico a la dependencia solicitante confirmando el despliegue realizado.
RIESGOS ASOCIADOS:	▪ Posibilidad de afectación reputacional de la Entidad por pérdida de la disponibilidad y continuidad de los servicios de TI debido a inadecuada asignación de recursos y deficiencias en la gestión y monitoreo de la seguridad, plataforma y componentes de la infraestructura de TI. ▪ Posibilidad de afectación económica y reputacional para la Unidad por adquisición y/o desarrollo de aplicaciones no funcionales debido a insuficiente claridad, conocimiento y comunicación entre el equipo desarrollador y los usuarios para establecer y validar la necesidad y requerimientos, y deficiencias en el procedimiento de desarrollo de software. ▪ Posibilidad de afectación económica y/o reputacional por procesos sancionatorios debido a la perdida de la información o de su integridad, por ausencia de controles de respaldo o inaplicabilidad de los existentes. ▪ Posibilidad de afectación económica y/o reputacional ante el inicio de procesos administrativos o sancionatorios, por debilidades o desviaciones en la operatividad y funcionalidad del SRTDAF a causa de la ausencia de documentación para su uso.
RECOMENDACIONES	▪ Fortalecer la gestión documental del proceso de desarrollo de software, asegurando que cada hito cuente con evidencia clara, completa y conforme a los procedimientos establecidos, tanto para los requerimientos que están en curso, como para los que están por desarrollar. ▪ Realizar la consolidación y actualización del inventario de requerimientos asociados a los módulos del sistema SRTDAF que se encuentran en ambiente de producción. ▪ Capacitar al personal técnico de la Oficina de Tecnologías de la Información en la correcta aplicación de los formatos y procedimientos internos relacionados con el ciclo de vida del desarrollo de software. ▪ Implementar controles internos que permitan validar la existencia y calidad de los soportes del ciclo de vida del software antes de avanzar a etapas posteriores de cada desarrollo. ▪ Actualizar los procedimientos si se identifican vacíos o ambigüedades que dificulten su aplicación práctica.

Fuente: Reporte de Hallazgo Final N° 1

HALLAZGO N. 2:

Tabla N. 3 Resumen ejecutivo del Reporte de hallazgo N° 2

TÍTULO:	***Debilidad en la implementación de lineamientos de la Política de Seguridad y Privacidad de Información asociado a riesgos que pueden afectar potencialmente al SRTDAF.***
SITUACIÓN EVIDENCIADA:	

Con el objetivo de verificar el cumplimiento de los lineamientos establecidos en el documento GT-ES-02 *"Compendio de Políticas Complementarias de Seguridad y Privacidad de la Información"* en su versión 7, relacionadas con gestión de cambios, segregación de ambientes, acceso a código fuente, Log de auditoría, análisis de vulnerabilidades, revisión de la seguridad de la información, copias de respaldo y revisión de los derechos de acceso, a partir de validaciones realizadas al Sistema de Registro de Tierras Despojadas y Abandonadas Forzosamente - SRTDAF, entre el 27 de agosto y el 29 de septiembre de 2025, se realizaron mesas de trabajo entre el equipo auditor y los colaboradores delegados de la Oficina de Tecnología de la Información (OTI), en las cuales se realizó la identificación y evaluación de treinta y ocho (38) controles y/o actividades derivadas del documento GT-ES-02. Resultado de la evaluación de efectividad en la implementación de los controles para mitigar los riesgos identificados y asociados al SRTDAF, se evidenciaron las siguientes situaciones:

1. **Bajo Nivel de implementación de los lineamientos de la Política de Seguridad y Privacidad de la información para los riesgos y controles identificados del SRTDAF.**

A partir de la evaluación de los treinta y ocho (38) lineamientos de la Política de Seguridad y Privacidad de la Información, se evidenció que:

- Diez (10) de los treinta y ocho (38) lineamientos, (el 26%) se encuentran implementados con resultado efectivo.
- Seis (6) de los treinta y ocho (38) lineamientos, (el 16%) se encuentran implementados, pero presentan oportunidad de mejora.
- Veintidós (22) de los treinta y ocho (38) lineamientos, (el 58%) presentan debilidad en el diseño e implementación.

A continuación, se presenta el resumen del resultado obtenido, cuyo detalle fue revisado y socializado con la Oficina de Tecnología de la Información entre el 25 y 29 de septiembre de 2025.

Tabla No. 3.1. Resultado de la evaluación de implementación de los lineamientos de la Política de Seguridad y Privacidad de la información a partir de la verificación del SRTDAF.

ID del Riesgo	Lineamientos de la Política de seguridad - MSPI	Literal de la política	Evaluación del diseño	Resultado de la implementación
RI-OCI-1	12.1.2 Gestión de Cambios	a. Evaluaciones de riesgo	Fuerte	Efectivo
		b. Pruebas adecuadas de los cambios	Moderado	Debilidad de diseño e implementación
		c. Registros de cambios	Moderado	Debilidad de diseño e implementación
	12.1.4 Separación de los Ambientes de Desarrollo, Pruebas y Operación	a. Restricciones de acceso entre cada ambiente.	Moderado	Oportunidad de mejora del control
		b. Protocolo de migración formal	Moderado	Debilidad de diseño e implementación
		c. Revisiones de seguridad en los entornos de desarrollo y pruebas	Débil	Debilidad de diseño e implementación
RI-OCI-2	9.4.5 Control de Acceso al Código Fuente de los Programas	a. Acceso al código fuente	Fuerte	Oportunidad de mejora del control
		b. Sistemas de control de versiones	Fuerte	Oportunidad de mejora del control
		c. Revisiones de código	Fuerte	Oportunidad de mejora del control
RI-OCI-3	12.4.1.1 Registro de Eventos (Logs)	a. Intentos de acceso	Fuerte	Efectivo
		b. Cambios en la configuración	Fuerte	Efectivo
		c. Administración de usuarios.	Fuerte	Efectivo
	12.7.1 Control de Auditorías de Sistemas de Información	b. Accesos a Logs	Moderado	Oportunidad de mejora del control
		c. Revisión de Logs	Débil	Debilidad de diseño e implementación
		d. Almacenamiento de Logs	Fuerte	Efectivo
		e. Reporte de irregularidades	Fuerte	Efectivo
		f. Auditorías internas	Fuerte	Oportunidad de mejora del control
RI-OCI-4	12.6.1 Gestión de las Vulnerabilidades Técnicas	a. Análisis de vulnerabilidades	Moderado	Debilidad de diseño e implementación
	18.2.1 Revisión Independiente de la Seguridad de la Información	a. Revisión de seguridad de información	Débil	Debilidad de diseño e implementación
	18.2.2 Cumplimiento con las Políticas y Normas de Seguridad	a. Auditorías de seguridad de información	Fuerte	Efectivo

RI-OCI-5	12.3.1 Respaldo de la Información	a. Procesos de respaldo	Moderado	Debilidad de diseño e implementación
	12.3.1.1 Frecuencia y Programación de Respaldos	b. Frecuencia de respaldo	Moderado	Debilidad de diseño e implementación
		c. Programación de respaldos	Fuerte	Efectivo
		d. Documentación de respaldo	Moderado	Debilidad de diseño e implementación
	12.3.1.2 Almacenamiento de Respaldos	a. Almacenamiento de respaldo redundante.	Fuerte	Efectivo
RI-OCI-6	9.2.5 Revisión de los Derechos de Acceso	a. Revisión de acceso al SRTDAF	Débil	Debilidad de diseño e implementación
	12.1.1 Procedimientos de Operación Documentados	a. Procesos de gestión de incidentes de seguridad.	Moderado	Debilidad de diseño e implementación
		b. Métodos de respaldo y recuperación	Moderado	Debilidad de diseño e implementación
		c. Protocolos de acceso a sistemas y datos.	Fuerte	Efectivo
GT-RG-9, GT-RG-10	14.2.1 Política de Desarrollo Seguro.	a. Requisitos de seguridad en el desarrollo	Moderado	Debilidad de diseño e implementación
		b. Principios de diseño seguro	Débil	Debilidad de diseño e implementación
		c. Directrices de codificación segura	Débil	Debilidad de diseño e implementación
		d. Pruebas de seguridad exhaustivas	Débil	Debilidad de diseño e implementación
		e. Proceso para identificar vulnerabilidades	Débil	Debilidad de diseño e implementación
		f. Procedimientos de gestión de cambios	Moderado	Debilidad de diseño e implementación
		g. Seguridad en entorno de desarrollo	Moderado	Debilidad de diseño e implementación
		h. Seudonimización o anonimización de datos	Débil	Debilidad de diseño e implementación
		i. Formación en desarrollo seguro	Débil	Debilidad de diseño e implementación

Fuente. Construcción propia del equipo auditor a partir del resultado de la Evaluación de los Riesgos y Controles para el SRTDAF.

Del resultado anterior, se destacan las siguientes buenas prácticas y controles implementados que fortalecen la gestión del SRTDAF:

- Se cuenta con procedimientos y formatos para la gestión de cambios de TI, que incluyen la realización de análisis de riesgos previo al despliegue de nuevos desarrollos en el sistema.
- El SRTDAF dispone de un módulo de seguridad que permite generar y almacenar Logs de auditoría para eventos como: ingresos exitosos e intentos fallidos de acceso al sistema, cambios en la configuración, creación y desactivación de cuentas de usuario. Los Logs de auditoría son almacenados en la base de datos con acceso restringido solamente a personal autorizado.
- Se cuenta con infraestructura y herramientas para la gestión de copias de respaldo de las máquinas virtuales y bases de datos de la plataforma Azure en donde opera el ambiente productivo del SRTDAF.
- Se cuenta con procedimientos para el soporte realizado por la mesa de ayuda de TI utilizando la herramienta GLPI, por medio del cual se radican y gestionan las solicitudes e incidentes del SRTDAF.

No obstante, a continuación, se describen las debilidades más relevantes identificadas en la evaluación de controles de seguridad de la información del SRTDAF:

- Seguridad y monitoreo del SRTDAF y sus entornos de desarrollo y pruebas:
  - Aunque se cuenta con herramientas de seguridad perimetral para la infraestructura de TI, estas no realizan monitoreo directo sobre aplicaciones específicas como el SRTDAF.
  - No se han definido actividades o controles para revisar periódicamente la seguridad de los entornos de desarrollo y pruebas, lo que podría permitir el ingreso de vulnerabilidades al ambiente de producción del SRTDAF.
  - No existe un control o actividad formal para revisar periódicamente Los logs de auditoría del SRTDAF, lo que limita la capacidad de detectar situaciones anómalas antes que se materialice un evento de seguridad.

- Análisis de vulnerabilidades:
  - Los análisis de vulnerabilidades se realizan sobre la infraestructura OnPremise, pero estos no incluyen la plataforma en la nube Azure, en la cual opera el ambiente productivo del SRTDAF.
  - No se cuenta con lineamientos, instructivos o procedimientos documentados en el SIPG para la realización de análisis de vulnerabilidades, configuración y monitoreo de alertas de seguridad mediante el software de monitoreo actualmente implementado.
  - No se han establecido lineamientos ni procedimientos para identificar, evaluar, clasificar y tratar vulnerabilidades de seguridad detectadas durante el desarrollo o después del despliegue del SRTDAF.
  - El último análisis de vulnerabilidades tipo Pen Test se realizó en 2023. Para la vigencia 2025 no se ha presupuestado ni ejecutado esta actividad, lo que incrementa el riesgo de vulnerabilidades no identificadas ni gestionadas.

- Gestión de Infraestructura y Respaldos:
  - No se cuenta con documentación adoptada en el SIPG que establezca la frecuencia ni el tipo de copias de respaldo a realizar para el SRTDAF.

- Protección contra software malicioso del SRTDAF:
  - La solución antivirus FortiEDR presenta inconvenientes en servidores Linux donde opera el SRTDAF, impidiendo su implementación completa. La solución anterior permanece activa, pero sin actualizaciones, lo que representa un riesgo de seguridad.

- Gestión de Accesos:
  - No se ha definido ni implementado una actividad de control para que la Subdirección General, en calidad de Líder del proceso de Gestión de Restitución Ley 1448 - Registro, revise periódicamente los accesos otorgados al SRTDAF, tal como lo establece la actual Política de Seguridad y Privacidad de Información. Como resultado de la revisión de efectividad de los controles para el retiro de credenciales, se identificaron dos (2) usuarios activos en el SRTDAF asignadas a excolaboradores que ya no tienen vínculo vigente con la Entidad.

- Procedimientos asociados a la Política de Gestión de Incidentes:
  - Aunque existe una política formal de gestión de incidentes de seguridad de la información, no se han establecido procedimientos en el SIPG para su implementación.

- Lineamientos para el Desarrollo de software Seguro:
  - Existe un documento de lineamientos y criterios no funcionales para sistemas de información que incluye directrices de seguridad, pero aún no se han formalizado los procedimientos, formatos y controles necesarios para su aplicación efectiva en el desarrollo del SRTDAF.
  - No se ha definido ni formalizado la identificación e integración de requisitos de seguridad desde las fases iniciales del desarrollo del SRTDAF, por ejemplo, pruebas de defensa en profundidad.
  - No se han establecido directrices formales de codificación segura para prevenir vulnerabilidades comunes como inyecciones de código, desbordamientos de búfer y errores de validación de entrada.
  - No se ha definido formalmente pruebas de seguridad exhaustivas (estáticas, dinámicas, análisis de vulnerabilidades, pruebas de penetración) en las distintas etapas del desarrollo del SRTDAF.
  - No se han definido ni realizado sesiones de capacitación, fortalecimiento o socialización de políticas y lineamientos relacionados con desarrollo seguro en el marco de las actividades de uso y apropiación del SRTDAF.

- Técnicas de anonimización o seudonimización:
  - No se identificaron técnicas específicas ni evidencia de aplicación de anonimización o seudonimización de datos en el SRTDAF.

Este resultado evidencia la necesidad de fortalecer las acciones institucionales para la implementación de la Política de Seguridad, que prevengan la materialización de riesgos que impacten el SRTDAF y la información que contempla y proporciona este sistema. No obstante, vale la pena mencionar que la Oficina de Tecnología de la Información actualizó esta política en julio de 2025, por lo cual se espera que este resultado sirva apoyo o insumo en la definición de estrategias para su implementación.

2. Necesidad de alineación de la Política y el Modelo de Seguridad y Privacidad de la Información (MSPI) con la nueva versión de la norma ISO 27001-2022.

Como resultado de la etapa de entendimiento de la auditoria al SRTDAF, se observó que la actual Política de Seguridad y Privacidad de la Información institucional, está basada en el Modelo de Seguridad y Privacidad de Información (MSPI) que incorporó la norma ISO 27001 de la vigencia 2013. No obstante, teniendo en cuenta que el Ministerio de Tecnologías de la Información y las Comunicaciones, por medio la Resolución 2277, expedida el 20 de junio de 2025, actualizó los lineamientos del MSPI para alinéalos con la ISO 27001 de la vigencia 2022, se identifica la necesidad de revisar y actualizar el MSPI institucional, y planificar y ejecutar su adopción e implementación de acuerdo con las necesidades y capacidades institucionales de la UAERTD.

CIRTERIOS ASOCIADOS:	1. **GT-ES-02 Compendio de Políticas Complementarias de Seguridad y Privacidad de la Información, versión 7,** con los siguientes numerales y literales**:** **12.1.2 Gestión de Cambios** Para la gestión de cambios en los sistemas se implementará un proceso formal que asegure que todas las modificaciones a la infraestructura, sistemas y aplicaciones sean evaluadas, aprobadas, documentadas y comunicadas. Este proceso debe incluir: a. Evaluaciones de riesgo antes de la implementación de cualquier cambio. b. Pruebas adecuadas de los cambios en un ambiente controlado antes de su despliegue en producción. c. Registros de cambios que permitan rastrear la historia de modificaciones. **12.1.4 Separación de los Ambientes de Desarrollo, Pruebas y Operación** Las actividades de desarrollo, pruebas y operaciones de sistemas tendrán entornos separados para evitar interferencias no autorizadas y proteger la integridad de los sistemas de producción. Se incluirá: a. Restricciones de acceso claras y diferenciadas entre cada ambiente. b. Protocolo de migración formal para mover código y configuraciones desde los ambientes de desarrollo y pruebas hacia producción. c. Revisiones de seguridad en los entornos de desarrollo y pruebas para asegurar que no se introduzcan vulnerabilidades. **9.4.5 Control de Acceso al Código Fuente de los Programas** a. El acceso al código fuente de programas desarrollados y en uso en la UAEGRTD estará limitado a personal autorizado según sus roles y necesidades laborales. b. Se utilizarán sistemas de control de versiones que registren todas las modificaciones realizadas al código fuente, incluyendo la identidad del autor y la fecha de modificación. c. Se implementarán revisiones de código periódicas para garantizar que solo el personal autorizado esté accediendo al código y que las modificaciones sean legítimas y aprobadas. **12.4.1.1 Registro de Eventos (Logs)** En todos los sistemas y aplicaciones críticas de la UAEGRTD deben generarse registros de eventos relacionados con la seguridad de la información. Los eventos para registrar incluyen, pero no se limitan a: a. Intentos de acceso no autorizados. b. Cambios en la configuración del sistema. c. Eventos relacionados con la administración de usuarios. **12.7.1 Control de Auditorías de Sistemas de Información** b. Los registros de auditoría deberán estar protegidos y accesibles solo a personal autorizado. Los accesos deben ser monitoreados y registrados. c. Los registros de auditoría serán revisados de forma periódica para detectar actividades inusuales o no autorizadas, así como para asegurar el cumplimiento de políticas y procedimientos internos. d. Los registros de auditoría se almacenarán durante un periodo mínimo según los lineamientos dados por Gestión Documental y serán eliminados de acuerdo con las políticas de retención de datos de la UAEGRTD. e. Cualquier incidente o irregularidad detectada durante el proceso de auditoría deberá ser reportado de inmediato al responsable de Seguridad de la Información, quien evaluará la situación y coordinará acciones correctivas y preventivas. f. Al menos una vez al año se llevarán a cabo auditorías internas para evaluar la efectividad de los controles de auditoría y el cumplimiento de esta política, sujeto al plan de auditoría establecido por la Unidad. **12.6.1 Gestión de las Vulnerabilidades Técnicas** a. Se deberán realizar evaluaciones periódicas para identificar vulnerabilidades en la infraestructura y el software instalado. Para ello, se utilizarán herramientas de análisis de vulnerabilidades y se monitorearán las alertas de seguridad relevantes.

	18.2.1 Revisión Independiente de la Seguridad de la Información La UAEGRTD llevará a cabo una revisión independiente de la seguridad de la información de manera regular, al menos una vez al año, o con mayor frecuencia si ocurren cambios significativos en el entorno interno o externo que puedan afectar la seguridad de la información. a. La revisión será realizada por un auditor interno o externo calificado, con experiencia en estándares de seguridad de la información **18.2.2 Cumplimiento con las Políticas y Normas de Seguridad** Al interior de la UAEGRTD se establecerá un programa de auditoría interna para verificar el cumplimiento de las políticas y normas de seguridad de la información de la Unidad. a. Las auditorías se realizarán al menos una vez al año y cubrirán todos los aspectos relacionados con la seguridad **12.3.1 Respaldo de la Información** a. La UAEGRTD implementará las medidas necesarias para que su información sea preservada y protegida contra pérdidas, daños o accesos no autorizados a través de procesos de respaldo. **12.3.1.1 Frecuencia y Programación de Respaldos** b. La frecuencia de las copias de respaldo se definirá en función de la criticidad de la información y los Objetivos de Punto de Recuperación (RPO) establecidos. Se considerarán copias completas, incrementales o diferenciales según sea necesario. c. La programación de los respaldos deberá ser documentada y comunicada por los colaboradores (funcionarios / contratistas) del área de Infraestructura, responsable de ejecutar los respaldos, siguiendo los procedimientos establecidos y utilizando las tecnologías y métodos adecuados. d. Se mantendrá una documentación clara y actualizada de los procedimientos de copias de respaldo, incluyendo la identificación de la información respaldada, la frecuencia, los medios de almacenamiento, las ubicaciones, los responsables y los procedimientos de restauración. **12.3.1.2 Almacenamiento de Respaldos** a. Se implementará una estrategia de almacenamiento que incluya al menos una copia de respaldo almacenada en una ubicación física separada del sitio principal (ubicación off-site) para proteger contra eventos que afecten la infraestructura principal. Se garantizarán condiciones ambientales adecuadas para la conservación de los medios de respaldo. **9.2.5 Revisión de los Derechos de Acceso de Usuario.** Los derechos de acceso otorgados a los usuarios en los sistemas de información y datos de la UAEGRTD serán revisados anualmente o ante cambios significativos en el rol o responsabilidades de los usuarios, para asegurar que dichos permisos sigan siendo necesarios, apropiados y estén alineados con las responsabilidades y roles actuales de cada usuario. Esta revisión será responsabilidad de cada líder de proceso y/o sistema utilizado por los usuarios respectivos, dejando un registro documental de su ejecución. **12.1.1 Procedimientos de Operación Documentados** Para todas las operaciones críticas que involucren el manejo y almacenamiento de la información en la UAEGRTD se establecerán y mantendrán procedimientos documentados. Estos procedimientos deben ser accesibles a las partes interesadas y revisados periódicamente para asegurar su eficacia y adecuación. La documentación incluirá: a. Procesos de gestión de incidentes de seguridad. b. Métodos de backup y recuperación de información. c. Protocolos de acceso a sistemas y datos. **14.2.1 Política de Desarrollo Seguro).** a. Identificación e integración de los requisitos de seguridad relevantes en las etapas iniciales del desarrollo, considerando los riesgos de seguridad de la información y los requisitos normativos y contractuales aplicables. b. Aplicación de principios de diseño seguro para minimizar las vulnerabilidades inherentes en el software, tales como la defensa en profundidad, el privilegio mínimo y la separación de funciones. c. Directrices de codificación segura para prevenir vulnerabilidades comunes, como inyecciones de código, desbordamientos de búfer y errores de validación de entrada. Estas directrices deben basarse en estándares de la industria y mejores prácticas.

	d. Pruebas de seguridad exhaustivas durante las diferentes etapas del desarrollo, incluyendo pruebas estáticas y dinámicas, análisis de vulnerabilidades y pruebas de penetración, según sea apropiado. e. Implementar un proceso para identificar, evaluar, clasificar y tratar las vulnerabilidades de seguridad descubiertas durante el desarrollo y después del despliegue. f. Implementar procedimientos de gestión de cambios seguros para garantizar que las modificaciones al software y a los sistemas de información se realicen de manera controlada y sin introducir nuevas vulnerabilidades. g. Mantener medidas de seguridad adecuadas para proteger el entorno de desarrollo, incluyendo el control de acceso, la segregación de entornos y la protección contra software malicioso. h. Promover e implementar y técnicas para que los datos sean adecuadamente seudonimizados o anonimizados considerando todos los elementos de la información que sean sensibles. i. Proporcionar formación y concientización. 2. **Resolución 2277 del 20 de junio de 2025 expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones** *"Por medio de la cual se actualizan los lineamientos del MSPI para alinéalos con la ISO 27001 de la vigencia 2022.*
RIESGOS ASOCIADOS:	▪ Posibilidad de afectación económica y reputacional por debilidades en la segregación de ambientes de desarrollo, pruebas y producción debido a el acceso a datos y modificaciones no autorizadas en la operación del SRTDAF. ▪ Posibilidad de afectación operativa por modificaciones no autorizadas en la herramienta GITLAB debido a la asignación errónea de privilegios de acceso y debilidades en la custodia del código fuente y versionamiento del SRTDAF. ▪ Posibilidad de afectación económica y reputacional por deficiencia en la gestión de Logs de auditoría debido a debilidades en la generación, análisis y custodia de los registros de auditoría del módulo de seguridad del SRTDAF.
RECOMENDACIONES	▪ Formalizar en el SIPG todos los lineamientos, procedimientos, instructivos, guías y formatos relacionados con la configuración y acceso a los diferentes ambientes de desarrollo, la gestión de usuarios, configuraciones y flujos de trabajo del GitLab, análisis de vulnerabilidades (incluyendo nube Azure en donde opera el ambiente de producción del SRTDAF), respaldos de información (frecuencia, medios, restauración), desarrollo seguro (codificación, pruebas, revisión de código, y jornadas de fortalecimiento) y demás elementos requeridos para fortalecer el diseño e implementación de las Políticas de Seguridad y Privacidad de la Información, en especial para el SRTDAF. ▪ Establecer o reforzar controles para la revisión periódica de los privilegios de acceso de los usuarios, monitoreo y análisis de Logs de auditoría, y evaluación y análisis de la seguridad y vulnerabilidades sobre la infraestructura tecnológica que soporta los servicios de TI de Entidad, en especial el SRTDAF. ▪ Ejecutar revisiones periódicas de la documentación técnica de la infraestructura y procesos que soportan los servicios de TI institucionales. ▪ Socializar los cambios de las Políticas de Seguridad a los líderes de los procesos, áreas técnicas y roles que, a partir de las actualizaciones les sean designadas responsabilidades para el cumplimiento de la política. ▪ Implementar y configurar herramientas y actividades de control que fortalezcan la capacidad de análisis de los Logs de auditoría para la detección temprana de anomalías previo a la materialización de riesgos de seguridad de información sobre la infraestructura y el SRTDAF. ▪ Fortalecer las jornadas de fortalecimiento, socialización y capacitación sobre políticas, lineamientos, procedimientos y herramientas de seguridad de información y flujos de trabajo para el desarrollo de software seguro. ▪ Establecer o fortalecer el plan de trabajo para la implementación de la Política de Seguridad y Privacidad de la información a medida que esta se actualiza, y realizar las actividades necesarias para alinear la Política institucional con la versión más reciente de la norma ISO 27001, la cual fue liberada en 2022, y su adopción para las entidades del estado a través del Modelo de Seguridad y Privacidad de la Información (MSPI) se estableció recientemente en la Resolución 2277 de 2025 del Ministerio de Tecnologías de la información y las Comunicaciones.

Fuente: Reporte de Hallazgo Final N° 2

HALLAZGO N. 3:

Tabla N. 4 Resumen ejecutivo del Reporte de hallazgo N° 3

TÍTULO:	***Ausencia de un manual o instructivo técnico y operacional del SRTDAF***
SITUACIÓN EVIDENCIADA:	
Con el objetivo de verificar el cumplimiento de los lineamientos establecidos en el Decreto 767 de 2022 *"Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital (…)"*, los lineamientos del Marco de Referencia de Arquitectura Empresarial (MRAE), y los requerimientos de la norma ISO 27001-2022 relacionados con la documentación técnica, funcional y operativa de los sistemas de información, como resultado de la etapa de entendimiento de la auditoria, el equipo auditor identificó que no se cuenta con un manual de usuario, funcional u operativo del SRTDAF, que permita a las procesos que operan este sistema, conocer, entender y utilizar las funcionalidades de cada módulo, según los roles y obligaciones de cada perfil definido, lo cual se corroboró al consultar en el listado maestro de documentos oficializados, en el módulo de Calidad de STRATEGOS. Esta situación podría limitar la capacidad de entendimiento de los usuarios para operar el sistema de manera autónoma, dificultar la resolución de problemas comunes, afectar la experiencia de uso e impactar la calidad y/o seguridad de la información que este dispone.	
CIRTERIOS ASOCIADOS:	▪ Decreto 767 de 2022, el cual establece los criterios generales para la implementación de la Política de Gobierno Digital, y el Marco de Referencia de Arquitectura Empresarial (MRAE): o MGGTI.LI.SI.02 – Catálogo de Sistemas de Información: Requiere que cada sistema cuente con documentación funcional, técnica y de soporte. o MGGTI.LI.SI.08 y 10 - Manual del usuario, técnico y de operación de los sistemas de información: La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe asegurar que todos sus sistemas de información cuenten con la documentación técnica y funcional debidamente actualizada. ▪ ISO 27001-2022. El cual, junto con los requisitos de seguridad de información, establece la necesidad de contar con la documentación operativa y técnica para cumplir con los controles del Anexo A, respeto a la Información documentada: o Cláusula 7.2: Requiere evidencia de competencias, lo que puede incluir manuales de capacitación o instructivos. o Cláusula A.12.1.1: Exige procedimientos de operación para la gestión de TI, lo que puede incluir documentación técnica y manuales para soporte. o Cláusula A.14.2.5: Principios de ingeniería de sistemas seguros, que implican documentación técnica de funcionalidades y flujos.
RIESGOS ASOCIADOS:	▪ Posibilidad de afectación operativa por perdida de seguridad o privacidad de la información del SRTDAF, ante la ausencia o inaplicabilidad de controles que permitan evaluar y gestionar debilidades frente a la integridad del sistema y de su información. ▪ Posibilidad de afectación económica y/o reputacional por procesos sancionatorios debido a la perdida de la información o de su integridad, por ausencia de controles de respaldo o inaplicabilidad de los existentes. ▪ Posibilidad de afectación económica y/o reputacional ante el inicio de procesos administrativos o sancionatorios, por debilidades o desviaciones en la operatividad y funcionalidad del SRTDAF a causa de la ausencia de documentación para su uso.
RECOMENDACIONES	▪ Elaborar y publicar el manual de usuario del SRTDAF, detallando funcionalidades por módulo y perfil, integrando los procesos o dependencias necesarias que garanticen integridad y completitud. ▪ Diseñar y mantener actualizada la documentación técnica, incluyendo diagramas de flujo, arquitectura funcional y descripción de componentes. ▪ Crear un manual técnico para el equipo de soporte, con procedimientos de atención, solución de incidentes y mantenimiento. ▪ Establecer un procedimiento formal de documentación como parte del ciclo de desarrollo y mantenimiento del sistema.

	▪ Asignar responsables y recursos para la gestión documental de sistemas de información. ▪ Realizar capacitaciones periódicas basadas en los manuales generados.

Fuente: Reporte de Hallazgo Final N° 3

Notas:

- La naturaleza de la labor de auditoría interna ejecutada por la Oficina de Control Interno, al estar supeditada al cumplimiento del Plan Anual de Auditoría, se encuentra limitada por restricciones de tiempo y alcance, razón por la que procedimientos más detallados podrían develar asuntos no abordados en la ejecución de esta actividad.
- La evidencia recopilada para propósitos de la evaluación efectuada versa en información suministrada por los responsables de atender el proceso auditor, a través de solicitudes y consultas realizadas por la Oficina de Control Interno. Nuestro alcance no pretende corroborar la precisión de la información y su origen.
- Es discrecional de Entidad determinar si se acogen las recomendaciones elevadas por la Oficina de Control Interno ante las situaciones observadas, no obstante, se invita a que las mismas sean consideradas en el establecimiento de los planes de mejoramiento a que haya lugar.

CLAUDIA MARCELA PINZON MARTINEZ

Firmado digitalmente por CLAUDIA MARCELA PINZON MARTINEZ
DN: T=JEFE DE OFICINA ASESORA CODIGO 0137 GRADO 22, SN=PINZON MARTINEZ, STREET="Calle 13A #29-24 BARRIO ED ALLIANZ", S=BOGOTA D.C., OU=TOKEN VIRTUAL, SERIALNUMBER=2280032, OID.1.3.6.1.4.1.23267.2.3=9004988799, OID.1.3.6.1.4.1.23267.2.2=53077880, OID.1.3.6.1.4.1.23267.2.1=364, O=UNIDAD DE RESTITUCION DE TIERRAS, L=BOGOTA D.C., G=CLAUDIA MARCELA, C=CO, CN=CLAUDIA MARCELA PINZON MARTINEZ
Razón: Yo soy el autor de este documento
Ubicación:
Fecha: 17/10/2025 12:18:34 -05'00'

CLAUDIA MARCELA PINZÓN MARTÍNEZ
Jefe Oficina de Control Interno

Anexos: Tres (3) reportes de hallazgos (formato CI-FO-34).
Elaboró: Carlos Alberto Quiñones Cárdenas, Oficina de Control Interno.
Revisó: Maicol Stiven Zipamocha Murcia, Oficina de Control Interno.