AGENCIA DE DESARROLLO RURAL – ADR

Oficina de Control Interno

N° INFORME: OCI-2025-026

DENOMINACIÓN DEL TRABAJO: Auditoría Interna al proceso de Modelo de Seguridad y Privacidad de la Información MSPI

DESTINATARIOS:[1]

- Cesar Augusto Pachón Achury, Presidente.
- Cesar Augusto Ramírez Chaparro, Jefe Oficina de Planeación Secretario General (E)
- Claudia Patricia Herrera Vallejo, Vicepresidente de Integración Productiva
- Eliana Teresa Zambrano Almansa, Vicepresidente de Proyectos.
- José Luis Valenzuela Rodríguez, Vicepresidente de Gestión Contractual.
- Amanda Lucia Camargo Jiménez, Jefe de la Oficina Jurídica (*Delegado de Presidencia – Comité de Coordinación del Sistema de Control Interno – Resolución 819 de 2022.)*

EMITIDO POR:

Carlos Alberto Cortés Riaño, Jefe de la Oficina de Control Interno.

AUDITOR (ES):

Carlos Arturo Guarnizo García, Rol líder de Auditoria.
Diana Marcela Cuervo Espinosa, Rol Auditor.
Waltencir Suárez Castillo, Rol Auditor.
María Alejandra Arrechea, Rol Auditor.

[1] En virtud de lo establecido en el Decreto 1083 de 2015 Artículo 2.2.21.4.7, Parágrafo 1° (adicionado por el Artículo 16 del Decreto 648 de 2017) *"Los informes de auditoría, seguimientos y evaluaciones* [emitidos por la Oficina de Control Interno] *tendrán como destinatario principal al representante legal de la Entidad y al Comité de Coordinación de Control Interno (…)"*

OBJETIVO(S): Evaluar de forma independiente el diseño y la eficacia operativa de los controles internos implementados en la Agencia de Desarrollo Rural (ADR) para gestionar los riesgos del proceso *"Modelo de Seguridad y privacidad de la Información"*.

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

Periodo Evaluado: marzo de 2023 a septiembre de 2025

LIMITACIÓN: No aplicó en el desarrollo de la presente auditoría.

DECLARACIÓN:

Esta auditoría fue realizada con base en el análisis de diferentes muestras aleatorias seleccionadas por los auditores a cargo de la realización del trabajo. Una consecuencia de esto es la presencia del riesgo de muestreo, es decir, el riesgo de que la conclusión basada en la muestra analizada no coincida con la conclusión a que se habría llegado en caso de haber examinado todos los elementos que componen la población.

CRITERIOS: Para la realización de este trabajo se consideraron como principales criterios, los siguientes:

- Ley 1680 de Ley 80 de *1993 "Por la cual se expide el Estatuto General de Contratación de la Administración Pública"*.
- Decreto 2364 de 2015 "Por el cual se crea la Agencia de Desarrollo Rural - ADR, se determinan su objeto y su estructura orgánica".
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 1078 de 2015. Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Ley 1712 de 2014*. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.*
- CONPES 3920 de 2018.
- CONPES 3975 de 2019. Política Nacional de Transformación Digital e Inteligencia Artificial.
- Resolución 500 de 2021. Lineamientos y estándares para la estrategia de seguridad digital y adopción del modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital
- Plan Nacional de Infraestructura de Datos (PNID). MinTIC, DNP, DAPRE. Diciembre de 2021.
- Decreto 338 de 2022. Adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto 1078 de 2015.
- Resolución 746 de 2022. Fortalece el Modelo de Seguridad y Privacidad de la Información establecido en la Resolución 500 de 2021.
- Resolución 460 de 2022. Expide el Plan Nacional de Infraestructura de Datos.
- Decreto 767 de 2022. Lineamientos generales de la política de Gobierno Digital y subroga el capítulo 1 del Título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015.
- MAE.G.UA – Uso y Apropiación de la Práctica de Arquitectura Empresarial. Ministerio de Tecnologías de la Información y las Comunicaciones. 2023
- Resolución 1978 de 2023. Adopta la versión 3 del Marco de Referencia de Arquitectura Empresarial para el Estado Colombiano.
- Norma ISO 27001:2022. Seguridad de la información, ciberseguridad y protección de la privacidad.
- ISO 27001:2024. Actualización que incorpora consideraciones sobre cambio climático en el Sistema de Gestión de Seguridad de la Información.
- Resolución 02277 de 2025. Actualiza el Anexo 1 de la Resolución 500 de 2021 y deroga disposiciones relacionadas.
- Documento Maestro del Modelo de Seguridad y Privacidad de la Información dirigido a las entidades. Versión 5. MinTIC. 21 de abril de 2025.
- Decreto 2364 de 2015. Crea la Agencia de Desarrollo Rural (ADR) y define su objeto y estructura orgánica.

- Resolución 529 de 2024. Adopta el Sistema Integrado de Gestión y actualiza el Comité de Gestión y Desempeño de la ADR.
- Plan Estratégico de Tecnologías de la Información – PETI 2023–2026. Versión 1. 23 de enero de 2023.
- Caracterización del proceso Gestión de Tecnologías de la Información. CP- GTI-001. Versión 1. octubre de 2023.
- Proceso Gestión de Tecnologías de la Información y las Comunicaciones. Gestión de incidentes, eventos y debilidades de Seguridad de la Información. PR-GTI-007. Versión 1. diciembre de 2023.
- Procedimiento de Gestión de Cambios de Seguridad de la Información. PR- GTI-002. Versión 1. marzo de 2024.
- Información. PR- GTI-002. Versión 1. Marzo de 2024.
- Manual Operativo de Políticas de Seguridad y Privacidad de la Información. MO-GTI-001. Versión 2. Diciembre de 2024.
- Manual de Gestión de Activos de Seguridad de la Información. MO-GTI-003. Versión 2. Diciembre de 2024.
- Proceso Gestión de Tecnologías de la Información y las Telecomunicaciones. Gestión de incidentes, eventos y debilidades de Seguridad de la Información. PR-GTI-002. Versión 2. Diciembre de 2024.
- Procedimiento de formulación, seguimiento y ajustes al plan de acción y plan estratégico institucional. PR-DER-008. Versión 2. Diciembre de 2024.
- Plan Estratégico de Tecnologías de la Información – PETI 2024–2027. Versión 2. 23 de enero de 2025.
- Plan de Seguridad y Privacidad de la Información OTI. Enero de 2025.
- Procedimiento de Gestión de Cambios de Seguridad de la Información. PR- GTI-002. Versión 2. Año 2025.

RESUMEN EJECUTIVO:

Como resultado de la evaluación practicada, se identificaron oportunidades de mejora relacionadas con los siguientes aspectos, sobre las cuales se suscribió el respectivo reporte de hallazgo:

1. Inobservancia en la implementación de los lineamientos establecidos en la normatividad aplicable respecto a la preparación de las TIC para la continuidad del negocio para las vigencias 2023-2025.
2. Deficiencias en el análisis continuo de amenazas y en la implementación de acciones de mitigación para la seguridad de la información
3. Debilidades estructurales en la implementación del modelo de seguridad y privacidad de la información (MSPI) y en la evaluación de la efectividad de sus controles.

RIESGOS IDENTIFICADOS EN LA AUDITORÍA:

Tabla 1. Descripción de los riesgos identificados de la Auditoría

DESCRIPCIÓN	CUBIERTO EN LA AUDITORÍA
Incluidos en el Mapa de Riesgos de Transparencia e Integridad	
Posible impacto económico y reputacional derivado de sanciones o multas impuestas por el ente regulador como consecuencia de la pérdida de confidencialidad de la información digital almacenada, procesada y manejada en los sistemas de información misional y administrativos	SI
Posibilidad de afectación de la imagen institucional como consecuencia de la degradación potencial de los sistemas y documentos digitales, los cuales están almacenados en soportes tecnológicos susceptibles de daño con el paso del tiempo.	SI
Posible impacto económico y reputacional derivado de la falta de un monitoreo y seguimiento efectivo de los incidentes de seguridad y ciberseguridad, vulneración de los controles de seguridad, comprometiendo así la integridad de los diversos activos de información de le Entidad	SI
pérdida de disponibilidad de la infraestructura que soporta los servicios y activos de información de TI.	SI
Posible impacto económico y reputacional derivado de sanciones o multas impuestas por el ente regulador como consecuencia de la ausencia de mecanismos alternos de respaldo que puede desencadenar en perdida de información reservada y/o confidencial por un ataque informático sobre las bases de datos y los sistemas de información críticos	SI
Posible impacto económico y reputacional como consecuencia de la pérdida de Integridad de la información digital almacenada, procesada y manejada en los sistemas de información misional y administrativos.	SI

Incluidos por la Oficina de Control Interno	
Posibilidad de afectación de la imagen institucional como consecuencia de sanciones, multas u otras medidas impuestas por el ente regulador, derivadas del incumplimiento o la no alineación de la estrategia de Tecnologías de la Información, la arquitectura empresarial y el Subsistema de Gestión de Seguridad de la Información, en relación con sus planes estratégicos, lineamientos, políticas, procedimientos, indicadores y procesos operativos, especialmente en materia de innovación, seguridad, transformación digital y funcionamiento institucional.	SI
Posibilidad de afectación de la imagen institucional como consecuencia del incumplimiento de los objetivos y metas institucionales, derivado de errores en la planeación, desarrollo, implementación y mantenimiento de los sistemas de información e infraestructura tecnológica, así como de fallas en los procesos de adquisición de bienes y servicios de Tecnologías de la Información de la entidad.	SI
Posible afectación económica, reputacional e institucional como consecuencia del incumplimiento de los objetivos y metas institucionales, derivado de errores en la planeación, adquisición, ejecución y mantenimiento de los sistemas de información, la infraestructura tecnológica y los recursos financieros asociados a los proyectos y servicios definidos en el Plan Anual de Adquisiciones.	SI
Posible impacto económico y reputacional derivado de sanciones o multas impuestas por el ente regulador, como consecuencia del incumplimiento en la atención oportuna y adecuada de los casos y solicitudes gestionados a través de la Mesa de Ayuda, relacionados con el Subsistema de Gestión de Seguridad de la Información.	SI
Posibilidad de afectación de la imagen institucional como consecuencia del incumplimiento en la ejecución, monitoreo y cierre de los planes, programas, proyectos, indicadores y acciones orientadas al fortalecimiento del proceso de tecnología y del Subsistema de Gestión de Seguridad de la Información, en el marco de los lineamientos estratégicos aprobados por la entidad	SI

Fuente: Mapa de Riesgos de Transparencia y Ética pública /Elaboración propia equipo auditor

FORTALEZAS*:*

Como resultado de la evaluación practicada, la Oficina de Control Interno identificó la siguiente fortaleza a resaltar, de conformidad con las pruebas de auditorías adelantadas, la cual se relaciona a continuación:

- Se evidencia que en algunos procesos el área auditada ha desplegado gran esfuerzo por el cumplimiento de la implementación de políticas públicas en aras de dar cumplimiento a ciertos criterios normativos y procedimentales.

AVANCE DEL PLAN DE MEJORAMIENTO VIGENTE AL INICIO DE LA AUDITORIA:

Con ocasión de la última auditoría practicada en el año 2023, se elevaron seis (6) hallazgos, para los cuales se formularon dieciocho (18) acciones de mejora. Como resultado del seguimiento efectuado por la Oficina de Control Interno, se evidenció un (1) hallazgo cerrado y dos acciones (cumplidas).

Tabla 2. Avance Plan de Mejoramiento vigencia 2023

Hallazgos Elevados	Hallazgos Abiertos	Hallazgos Cerrados	Acciones Propuestas	Acciones Abiertas	Acciones Cerradas
6	5	1	18	16	2
Se elevaron seis (6) hallazgos, para los cuales se propusieron dieciocho (18) acciones, producto de los seguimientos realizados por la OCI, se observaron dos (2) acciones cerradas.					

Fuente: Elaboración propia equipo auditor

HALLAZGOS:

Nota: La información detallada de las situaciones que se describen a continuación, se suministró al personal perteneciente a la unidad auditada en cada reporte de hallazgo (Formato F-EVI-013) que fue suscrito por ésta y la Oficina de Control Interno; además, dicho detalle se encuentra registrado en los papeles de trabajo elaborados por los auditores que practicaron las pruebas, los cuales son custodiados por la Oficina de Control Interno; estos documentos se encuentran disponibles para consulta de las partes interesadas, previa solicitud formal de los mismos al Jefe de la Oficina de Control Interno.

HALLAZGO N° 1 - Inobservancia en la implementación de los lineamientos establecidos en la normatividad aplicable respecto a la preparación de las TIC para la continuidad del negocio para las vigencias 2023 a 2025

DESCRIPCION DEL HALLAZGO O SITUACIÓN ENCONTRADA:

La implementación de un proceso de preservación de la información pública ante

situaciones disruptivas, permite minimizar el impacto y recuperación por perdida de activos de información de la organización, hasta un nivel aceptable mediante la combinación de controles preventivos y de recuperación.

En este proceso es conveniente identificar los procesos críticos para el negocio e integrar los requisitos de la gestión de la seguridad de la información de la continuidad del negocio con otros requisitos de continuidad relacionados con aspectos tales como operaciones, personal, materiales, transporte e instalaciones.

Las consecuencias de eventos disruptivos (desastres, fallas de seguridad, perdida del servicio y disponibilidad del servicio) se deberían someter a un análisis del impacto del negocio (BIA). Se debe desarrollar e implementar un plan de continuidad que permita garantizar la restauración oportuna de las operaciones esenciales.

Con el fin de verificar la aplicación de los lineamientos establecidos para la respectiva preparación de las TIC para la continuidad del negocio, se inspeccionó la Resolución 500 del 2021 del Ministerio de las Tecnologías de la Información y las Comunicaciones, señalando lo siguiente:

> **ARTÍCULO 6.1 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON LOS PROVEEDORES**
>
> Los sujetos obligados deben determinar e implementar los controles para mitigar los riesgos asociados a la adquisición de productos y servicios de seguridad digital señalados en el Anexo número 2 de la presente resolución, así como cumplir con los siguientes requerimientos y características.
>
> Identificar la vida útil de los productos y servicios adquiridos con el fin de planificar cualquier migración o transferencia y respaldar los datos para garantizar la continuidad de la operación.

ARTÍCULO 17. ETAPAS GENERALES DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DIGITAL.

Los sujetos obligados deben incluir en su estrategia de seguridad digital las actividades a realizar en las etapas de prevención; protección y detección; respuesta y comunicación; recuperación y aprendizaje, como mínimo deberán incorporar:

- 1.6. Considerar dentro del plan de continuidad del negocio la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques de seguridad de la información.
- 1.7. Realizar pruebas del plan de continuidad del negocio que simulen la materialización de ataques de seguridad de la información.

7. PLANIFICACIÓN

7.3.2 Valoración de los riesgos de seguridad de la información

- Identificar los riesgos que causen la perdida de confidencialidad, integridad, disponibilidad, privacidad de la información, así como la continuidad de la operación de la Entidad dentro del alcance del MSPI.

Tabla 3. Controles del Anexo A del estándar ISO/IEC 27001:2013 y dominios a los que pertenece

A-17	Aspectos de seguridad de la Información de la gestión de continuidad de negocio	
A.17.1	Continuidad de seguridad de la información	Lineamiento: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización
A.17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de

		la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son validados y eficaces durante situaciones adversas.

Fuente: Resolución 500 de 2021 Normativa - MINTIC

Tabla 4 Responsabilidades - Marco de Arquitectura Empresarial

Dominio	Responsabilidades
Servicios tecnológicos	a. Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de información de la institución. b. Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información. c. Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad. d. Supervisar la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias. e. Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio. f. Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y

	oportunidades de mejora a nivel de seguridad de la información
Estrategia de TI	Definir la estrategia informática que permita lograr los objetivos y minimizar de los riesgos de la institución. Es el encargado de guiar la prestación del servicio y la adquisición de bienes y servicios relacionados y requeridos para garantizar la seguridad de la información
Sistemas de información	Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la entidad. a. Apoyar la implementación segura de los sistemas de información, de acuerdo con el modelo de seguridad y privacidad de la información del estado colombiano. b. Desarrollar pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información. c. Liderar el proceso de gestión de incidentes de seguridad, así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados. d. Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio

Fuente: Resolución 500 de 2021 Normativa - MINTIC

Tabla 5 Controles de la seguridad de la información

5.30	Preparación de las TIC para la continuidad del negocio	Control: La resiliencia de las TIC debe planificarse, implantarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC.

Fuente: Norma ISO 27001:2022

Teniendo en cuenta los lineamientos previamente descritos, la Oficina de Control Interno solicitó la documentación soporte mediante correo electrónico del 5 de diciembre del año en curso, obteniendo respuesta el 9 del mismo mes. En dicha respuesta se evidenció que el *"Plan de Continuidad de la Operación de*

los Servicios de la ADR", elaborado en diciembre de 2021, no se encuentra alineado con lo establecido en la Resolución 500 de 2021 del MinTIC, la norma ISO 27001:2022 y la *Guía para la preparación de las TIC para la continuidad del negocio*.

Frente a esta solicitud, la Oficina de Tecnologías de la Información (OTI) manifestó lo siguiente:

"(…) De conformidad con lo expuesto durante la prueba de recorrido realizada por el personal auditor, la Oficina de Tecnologías informó al equipo auditor que actualmente la Agencia de Desarrollo Rural no cuenta con un Plan de Recuperación Ante Desastres formalizado, en donde notificó que a nivel entidad solo existe un documento en borrador, el cual es que se presentó como evidencia según solicitud de información realizada por el equipo auditor. (…)".

POSIBLE(S) CAUSA(S) IDENTIFICADA(S) POR LA OFICINA DE CONTROL INTERNO:

- Desatención en la elaboración del Plan de Recuperación y secuencia de escalamiento ante Desastres Tecnológicos (DRP) elaborado por la OTI.
- Omisión en la presentación del consolidado de las actividades relacionadas con los servicios críticos (DRP)
- Requerimientos y controles de seguridad de la información aplicables a escenarios de contingencia o interrupción de servicios (DRP).
- Ausencia de las estrategias de continuidad tecnológica alineadas con los servicios críticos.
- Incumplimiento con la documentación de los planes de continuidad para cada componente tecnológico relevante.

- Falta de evidencias en las pruebas realizadas sobre las estrategias de continuidad y el DRP.
- Ausencia de resultados documentados y verificados relacionados con la materialización de hallazgos, las lecciones aprendidas y las acciones de mejora.
- Omisión de los productos o servicios TIC subcontratados.
- Desatención de los planes de continuidad establecidos por los proveedores para garantizar la operación y evitar afectaciones a la misionalidad de la ADR.
- Omisión de los acuerdos o contratos que soporten estos compromisos.
- Incumplimiento en la identificación del personal clave interno y externo requerido para la operación de las actividades críticas del negocio.
- Exclusión de la funcionalidad mínima requerida por el negocio para su operación en escenarios de contingencia.
- Carencia en la identificación de los riesgos presentes para la continuidad.
- Omisión de los elementos esenciales requeridos en el plan de recuperación de desastres.
- Desatención de los procedimientos específicos que respondan a interrupciones del servicio con el fin de proteger y recuperar las funciones críticas del negocio.

DESCRIPCIÓN DE LA(S) CAUSA(S):

Todas las afirmaciones mencionadas anteriormente se derivan de la ausencia en la presentación de la documentación requerida.

DESCRIPCIÓN DEL(LOS) RIESGO(S):

- Posibilidad de afectación de la imagen institucional como consecuencia de sanciones, multas u otras medidas impuestas por el ente regulador, derivadas del incumplimiento o la no alineación de la estrategia de Tecnologías de la Información, la arquitectura empresarial y el Subsistema de Gestión de Seguridad de la Información, en relación con sus planes estratégicos, lineamientos, políticas, procedimientos, indicadores y procesos operativos.
- Posibilidad de afectación de la imagen institucional como consecuencia del incumplimiento de los objetivos y metas institucionales, derivado de errores en la planeación, desarrollo, implementación y mantenimiento de los sistemas de información e infraestructura tecnológica, así como de fallas en los procesos de adquisición de bienes y servicios de Tecnologías de la Información de la entidad.
- Posibilidad de afectación de la imagen institucional como consecuencia del incumplimiento en la ejecución, monitoreo y cierre de los planes, programas, proyectos, indicadores y acciones orientadas al fortalecimiento del proceso de tecnología y del Subsistema de Gestión de Seguridad de la Información, en el marco de los lineamientos estratégicos aprobados por la entidad.
- Posible impacto económico y reputacional derivado de la falta de un monitoreo y seguimiento efectivo de los incidentes de seguridad y ciberseguridad, vulneración de los controles de seguridad, comprometiendo así la integridad de los diversos activos de información de le Entidad.

DESCRIPCIÓN DEL(LOS) IMPACTO(S):

- Deterioro de la confianza y credibilidad institucional, acompañado de afectaciones financieras y operativas derivadas de sanciones regulatorias,

retrasos en la ejecución de proyectos estratégicos y debilitamiento de la capacidad institucional para garantizar la continuidad y calidad de los servicios.

- Pérdida de credibilidad institucional y disminución de la confianza de los grupos de interés, acompañada de retrasos en la ejecución misional, incremento de costos operativos, afectación de la continuidad de los servicios y exposición a observaciones o medidas correctivas por parte de entes de control debido al incumplimiento de metas y objetivos estratégicos.
- Deterioro de la reputación institucional y pérdida de confianza por parte de los entes de control y grupos de interés, acompañado de retrasos en la ejecución misional, ineficiencias operativas, incremento de costos y exposición a observaciones, requerimientos o medidas correctivas debido a la incapacidad de demostrar cumplimiento y avance en los planes, programas y proyectos estratégicos de tecnología y seguridad de la información.
- Afectación significativa de la reputación institucional y pérdida de confianza por parte de los grupos de interés, acompañada de posibles sanciones, costos adicionales de recuperación, interrupciones en la prestación de servicios y exposición a accesos no autorizados, alteración o pérdida de información crítica debido a la ineficacia en el monitoreo, seguimiento y control de incidentes de seguridad y ciberseguridad

RECOMENDACIÓN(ES):

- Fortalecer los mecanismos de articulación, seguimiento y verificación entre la estrategia de Tecnologías de la Información, la arquitectura empresarial y el Subsistema de Gestión de Seguridad de la Información, garantizando su

alineación con los planes estratégicos, lineamientos, políticas y procedimientos institucionales.

- Implementar mecanismos fortalecidos de planeación, seguimiento y control sobre los proyectos de sistemas de información, infraestructura tecnológica y procesos de adquisición de bienes y servicios de TI, asegurando su alineación con los objetivos y metas institucionales.

- Fortalecer la planificación, seguimiento, cierre de los planes, proyectos de tecnología y del Sistema de Gestión de Seguridad de la Información, junto con controles periódicos que permitan identificar desviaciones y asegurar el cumplimiento de los lineamientos estratégicos.

- Fortalecer el monitoreo y seguimiento de incidentes de seguridad, verificando controles y consolidando evidencias que permitan identificar vulnerabilidades, aplicar acciones correctivas y proteger los activos de información.

RESPUESTA DEL AUDITADO: Aceptado

CAUSA(S) IDENTIFICADA(S) POR EL RESPONSABLE DE LA UNIDAD AUDITADA:

- No se cuenta con Procedimientos y recursos para la Recuperación Ante Desastres Tecnológicos.
- No se tiene definido el RTO y RPO.
- No se cuenta con la identificación y valoración de riesgos de Seguridad de la Información con base en los activos identificados.
- No se cuenta con Activos críticos de Tecnologías de la Información Actualizados.

- No se cuenta con Roles y Responsabilidades Definidos.

CONCEPTO DE LA OFICINA DE CONTROL INTERNO: Aceptado

JUSTIFICACIÓN:

En atención a la observación formulada por el equipo de la Oficina de Tecnologías de la Información, me permito precisar lo siguiente:

De acuerdo con lo establecido en el ***Artículo 6.1 – Gestión de la Seguridad de la Información para las Relaciones con los Proveedores***, contenido en la ***Resolución 500 de 2021***, específicamente en su numeral 5, donde se dispone: *"Identificar la vida útil de los productos y servicios adquiridos con el fin de planificar cualquier migración o transferencia y respaldar los datos para garantizar la continuidad de la operación"*, es pertinente precisar que dicha disposición no se enmarca dentro del Plan de Atención de Desastres, sino que corresponde al Plan de Continuidad del Negocio (BCP – Business Continuity Plan), atendiendo a los siguientes criterios:

- El objetivo explícito es garantizar que los procesos sigan funcionando sin interrupciones, incluso cuando se requiera migrar o transferir productos o servicios.

El análisis de la vida útil de los productos y servicios es de carácter preventivo y estratégico, orientado a mantener la operación estable en el tiempo, más propio de la continuidad que de la recuperación.

- Aunque el respaldo también es parte del Plan de Recuperación Ante Desastres (DRP), aquí se menciona como medida para asegurar la continuidad, no como respuesta a un desastre ya ocurrido.

Teniendo en cuenta la diferencia entre el Plan de Atención de Desastres, entendido como aquel que *"se activa después de un evento disruptivo (ejemplo:*

caída de sistemas, desastre natural) y define cómo restaurar la infraestructura tecnológica y los servicios críticos", y el Plan de Continuidad del Negocio (BCP – Business Continuity Plan), cuyo propósito es *"anticipar riesgos y asegurar que la organización pueda seguir operando sin interrupciones, mediante medidas preventivas y de gestión"*, se precisa que la afirmación previamente indicada hace énfasis en la planificación y prevención orientadas a garantizar la continuidad de la operación, razón por la cual corresponde al Plan de Continuidad del Negocio.

De acuerdo con reunión celebrada el día de hoy, 26 de diciembre del presente año, se procede a efectuar la desvirtualización del numeral correspondiente, atendiendo las observaciones formuladas por la Oficina de Tecnologías de la Información, en consenso con la Oficina de Control Interno.

ARTÍCULO 6.1 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON LOS PROVEEDORES

Los sujetos obligados deben determinar e implementar los controles para mitigar los riesgos asociados a la adquisición de productos y servicios de seguridad digital señalados en el Anexo número 2 de la presente resolución, así como cumplir con los siguientes requerimientos y características.

- 5. Identificar la vida útil de los productos y servicios adquiridos con el fin de planificar cualquier migración o transferencia y respaldar los datos para garantizar la continuidad de la operación.

La observación señala que la Oficina de Tecnologías de la Información (OTI) no posee responsabilidad plena sobre esta afirmación, dado que la implementación de un Plan de Continuidad del Negocio debe estar previamente enmarcada y

regida por el Plan de Atención de Desastres. Por lo anterior se considera que el Plan de Mejoramiento se ajusta para la mitigación del hallazgo correspondiente.

HALLAZGO N° 2 - Deficiencias en el análisis continuo de amenazas y en la implementación de acciones de mitigación para la seguridad de la información

DESCRIPCION DEL HALLAZGO O SITUACIÓN ENCONTRADA:

De conformidad con lo establecido en el Decreto 1078 de 2015; la Resolución 500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones, particularmente el artículo 17 sobre las Etapas generales de la gestión de incidentes de seguridad digital; el Manual Operativo de Políticas de Seguridad y Privacidad de la Información MO-GTI-001; y los procedimientos PR-GTI-007 Proceso de Gestión de la Tecnología de la Información y las Comunicaciones y PR-GTI-010 Gestión de Vulnerabilidades Técnicas, los sujetos obligados deben:

- Monitorear de manera permanente fuentes oficiales de información institucional, tales como boletines de ciberseguridad, CERT, proveedores de seguridad, plataformas tecnológicas, entre otros, con el fin de identificar amenazas existentes o emergentes.
- Analizar las amenazas identificadas, asignar incidentes, documentar acciones de corrección, realizar análisis de causas, establecer planes de mejora y lecciones aprendidas.
- Identificar y gestionar los riesgos asociados a la seguridad y privacidad de la información conforme a la metodología institucional definida.
- Implementar acciones de mitigación frente a amenazas, incluyendo controles de protección contra malware y gestión de vulnerabilidades.
- Establecer mecanismos de seguimiento, monitoreo y mejora continua que permitan detectar comportamientos anómalos y posibles incidentes de seguridad de la información, así como definir líneas base de

comportamiento normal.

Una vez evaluada la información remitida por la Oficina de Tecnología de la Información, a través de la carpeta denominada "Auditoría 2025 MSPI_VF – Inicial Punto

4.1 ", se evidenció que la documentación aportada corresponde únicamente a boletines de seguridad del segundo semestre de 2025, específicamente:

- Fotiweb (julio, septiembre y noviembre de 2025)
- Boletín de Ciberinteligencia (septiembre de 2025)
- FBI Flash (septiembre de 2025)
- CSIRTSALUD (octubre de 2025)

Si bien las fuentes presentadas corresponden a información confiable y actualizada, no se aportó evidencia documental que permita verificar el monitoreo sistemático de amenazas, el análisis de las mismas, la identificación de riesgos, la implementación de acciones de mitigación, ni el seguimiento y mejora continua durante los períodos 2023, 2024 y el primer semestre de 2025.

Asimismo, la información suministrada no evidencia documentación relacionada con la asignación de incidentes, análisis de causas, planes de mejora, lecciones aprendidas, gestión de vulnerabilidades, controles de protección contra malware, ni mecanismos de monitoreo y definición de líneas base de comportamiento, conforme a lo establecido en el MO-GTI-001 y los procedimientos PR-GTI-007 y PR-GTI-010.

Causa

La Oficina de Tecnología de la Información no cuenta con un esquema documentado y consolidado que garantice la trazabilidad histórica del monitoreo de fuentes de información, el análisis de amenazas, la gestión de riesgos, las acciones de mitigación y el seguimiento de incidentes de seguridad de la información, lo cual limita la disponibilidad de evidencias frente a los períodos evaluados.

Efecto

La ausencia de soporte documental integral impide a la Oficina de Control Interno verificar el cumplimiento de los lineamientos, controles y obligaciones establecidos en el Modelo de Seguridad y Privacidad de la Información, generando un riesgo de incumplimiento normativo y de debilidades en la capacidad institucional para prevenir, detectar, responder y aprender frente a incidentes de seguridad digital.

Conclusión

La situación descrita configura un incumplimiento a lo dispuesto en el Decreto 1078 de 2015, la Resolución 500 de 2021 y los instrumentos internos que regulan la gestión de la seguridad y privacidad de la información, al no evidenciarse de manera documentada y continua la implementación de los controles relacionados con la gestión de amenazas, riesgos, mitigación y seguimiento, durante los períodos objeto de evaluación.

POSIBLE(S) CAUSA(S) IDENTIFICADA(S) POR LA OFICINA DE CONTROL INTERNO:

- Insuficiente análisis continuo de amenazas y debilidades en la mitigación de riesgos de seguridad de la información.
- Falta de evidencia del análisis permanente de amenazas emergentes y de la adopción de medidas de mitigación.
- Debilidades en la gestión integral de amenazas y en la reducción de riesgos para los sistemas institucionales.
- Incumplimiento en el análisis y tratamiento oportuno de amenazas a la seguridad de la información.
- Limitaciones en la gestión de amenazas y acciones de mitigación del Modelo de Seguridad y Privacidad de la Información.

DESCRIPCIÓN DE LA(S) CAUSA(S):

- Debilidades en la gestión integral de amenazas y en la reducción de riesgos para los sistemas institucionales
- Incumplimiento en el análisis y tratamiento oportuno de amenazas a la

seguridad de la información

- Limitaciones en la gestión de amenazas y acciones de mitigación del Modelo de Seguridad y Privacidad de la Información

DESCRIPCIÓN DEL(LOS) RIESGO(S):

- Posibilidad de afectación de la imagen institucional como consecuencia de sanciones, multas u otras medidas impuestas por el ente regulador, derivadas del incumplimiento o la no alineación de la estrategia de Tecnologías de la Información, la arquitectura empresarial y el Subsistema de Gestión de Seguridad de la Información, en relación con sus planes estratégicos, lineamientos, políticas, procedimientos, indicadores y procesos operativos, especialmente en materia de innovación, seguridad, transformación digital y funcionamiento institucional.
- Posibilidad de afectación de la imagen institucional como consecuencia del incumplimiento de los objetivos y metas institucionales, derivado de errores en la planeación, desarrollo, implementación y mantenimiento de los sistemas de información e infraestructura tecnológica, así como de fallas en los procesos de adquisición de bienes y servicios de Tecnologías de la Información de la entidad.
- Posibilidad de afectación de la imagen institucional como consecuencia del incumplimiento en la ejecución, monitoreo y cierre de los planes, programas, proyectos, indicadores y acciones orientadas al fortalecimiento del proceso de tecnología y del Subsistema de Gestión de Seguridad de la Información, en el marco de los lineamientos estratégicos aprobados por la entidad.
- Posible impacto económico y reputacional derivado de sanciones o multas impuestas por el ente regulador como consecuencia de la pérdida de confidencialidad de la información digital almacenada, procesada y manejada en los sistemas de información misional y administrativos.
- Posible impacto económico y reputacional derivado de la falta de un monitoreo y seguimiento efectivo de los incidentes de seguridad y ciberseguridad, vulneración de los controles de seguridad, comprometiendo

así la integridad de los diversos activos de información de le Entidad.

- Posibilidad de afectación de la imagen institucional por incumplimiento de los objetivos y metas institucionales, debido a la inobservancia del Plan de Acción Institucional

DESCRIPCIÓN DEL(LOS) IMPACTO(S):

- Deterioro de la confianza y credibilidad institucional, así como impactos financieros derivados de sanciones regulatorias, retrasos en la ejecución de proyectos estratégicos y la disminución de la capacidad institucional para garantizar la continuidad y calidad de los servicios.
- Pérdida de credibilidad institucional y reducción de la confianza de los grupos de interés, junto con retrasos en la ejecución de la misión institucional, incremento de costos operativos, afectación de la continuidad de los servicios y exposición a observaciones o medidas correctivas por parte de entes de control debido al incumplimiento de metas y objetivos estratégicos.
- Pérdida de credibilidad en la Entidad por debilidades en la aplicación de controles de los procedimientos asociados a la gestión de Modelo de Seguridad de la Información.

RECOMENDACIÓN(ES):

- Fortalecer el seguimiento y verificación de la Oficina de Tecnologías de la Información, y sistema de Gestión de Seguridad de la Información, garantizando su alineación con los planes estratégicos, lineamientos, políticas y procedimientos institucionales.
- Implementar mecanismos de planeación, seguimiento y control sobre los proyectos de sistemas de información, infraestructura tecnológica y adquisición de bienes y servicios de TI, asegurando su alineación con los objetivos y metas institucionales.
- Optimizar la planificación, seguimiento del Sistema de Gestión de Seguridad de la Información, incorporando controles periódicos que permitan identificar desviaciones y garantizar el cumplimiento a los

procesos de la Seguridad de la Información.

- Fortalecer el monitoreo y seguimiento de incidentes de seguridad, verificando la efectividad de los controles y consolidando evidencias que permitan identificar vulnerabilidades, aplicar acciones correctivas y proteger los activos de información.

RESPUESTA DEL AUDITADO: Aceptado

JUSTIFICACIÓN: No indican.

CAUSA(S) IDENTIFICADA(S) POR EL RESPONSABLE DE LA UNIDAD AUDITADA:

- Identificar los recursos tecnológicos susceptibles de actualizaciones de seguridad.
- Registrar las vulnerabilidades identificadas sobre los recursos tecnológicos de la Oficina de Tecnologías.
- Registrar los incidentes de seguridad materializados de manera histórica.
- Actualización Procedimiento de Gestión de Incidentes y Gestión de Vulnerabilidades.

CONCEPTO DE LA OFICINA DE CONTROL INTERNO: Aceptado

JUSTIFICACIÓN:

En relación con el Plan de Mejoramiento, la Oficina de Control Interno considera razonables las acciones propuestas para gestionar las causas identificadas por el equipo auditado y atender las observaciones formuladas en el presente informe

HALLAZGO N° 3 - Debilidades estructurales en la implementación del modelo de seguridad y privacidad de la información (MSPI) y en la evaluación de la efectividad de sus controles

DESCRIPCION DEL HALLAZGO O SITUACIÓN ENCONTRADA:

La oficina de control interno de la Agencia de Desarrollo Rural, en cumplimiento de sus funciones; y dentro del marco de la Auditoria de aseguramiento, del

DIRECCIONAMIENTO ESTRATEGICO INSTITUCIONAL, realizada a la ***oficina de Tecnologías de la Información,*** dio cumplimiento al Programa de Trabajo EVI-008, con el propósito de verificar a implementación de las cinco fases del Modelo de Seguridad y Privacidad de la Información (MSPI) así como el estado de avance de la evaluación de la Efectividad de los Controles del Autodiagnóstico de la implementación del MSPI;
Como resultado, se identificaron incumplimientos normativos, y al procedimiento materializando el hallazgo como ***debilidades estructurales en la implementación del modelo de seguridad y privacidad de la información (MSPI) y en la evaluación de la efectividad de sus controles***

DEBILIDADES ESTRUCTURALES EN LA IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI) Y EN LA EVALUACIÓN DE LA EFECTIVIDAD DE SUS CONTROLES

En el marco de la auditoria al Modelo de Seguridad y Privacidad de la Información (MSPI), que realizo la oficina de Control interno a la Oficina de Tecnologías de la Información (OTI), se evidenció que la implementación del MSPI y la evaluación de la efectividad de sus controles, presentan debilidades estructurales, que se reiteran y no fueron subsanadas en las 3 vigencias auditadas, lo que impidió la verificación de la operación efectiva, controlada y sostenible del sistema de seguridad de la información, tal como se describe a continuación:

CRITERIO UNO: ***IMPLEMENTACIÓN FASES MSPI:*** Verificar la implementación de las cinco fases del Modelo de Seguridad y Privacidad de la Información (MSPI)—diagnóstico, planificación, operación, evaluación del desempeño y mejoramiento continuo—de acuerdo con lo establecido en el Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones, con el fin de asegurar el cumplimiento de sus directrices y la eficacia del sistema.

Se solicitó evidencias a la Oficina de Tecnologías de la Información (OTI), mediante correo electrónico el día 03 de diciembre 2025 y el día 10 de Diciembre

2025 donde se peticionó el resultado del autodiagnóstico diligenciado por la OTI, encontrándose que, **en lo que respecta al segundo semestre de 2023**, si bien se efectuó un ejercicio de evaluación del MSPI mediante el diligenciamiento del instrumento de evaluación de fecha 18 de diciembre de 2023, donde se identificaron algunos elementos asociados a las fases de diagnóstico y planificación, se observaron brechas significativas en las fases de operación, evaluación del desempeño y mejoramiento continuo, viéndose reflejadas en la ausencia de indicadores de gestión del MSPI, la inexistencia de revisión por la dirección, la falta de actualización de instrumentos de planeación y la carencia de evidencia verificable sobre la ejecución y seguimiento del tratamiento de riesgos en la matriz integral de riesgo TI.

En lo que atañe la **vigencia 2024**, a pesar de los requerimientos efectuados a fin de que se aporte la información por parte de la oficina audita, no se remitió documental, registros, evidencias o resultados que permitiesen verificar la ejecución de cualquiera de las 5 fases del MSPI, lo cual imposibilitó verificar que el modelo hubiese sido implementado para ese periodo.

En lo que concierne al periodo de **enero a septiembre de 2025**, se denotó un nuevo ejercicio de autoevaluación MSPI de fecha 01 de junio de 2025, donde se reportó un nivel de madurez general "no alcanza a nivel inicial". En esta oportunidad, nuevamente acompañado de brechas relevantes relacionadas con la definición de roles y responsabilidades, la inexistencia de indicadores de desempeño, la ausencia de revisión por la dirección. Aunado a ello, no sé arribaron registros que permitieran verificar la ejecución y seguimiento del tratamiento de riesgos de seguridad de la información.

Por lo anterior, para ninguna de las vigencias auditadas fue posible verificar la implementación integral y efectiva de las 5 fases del MSPI, pues se evidenciaron ejercicios parciales y que no pudieron ser verificados, incurriéndose así en los siguientes incumplimientos:

Incumplimientos asociados:

- Al procedimiento PR- GTI-002

<u>Numeral 5.2 – Se definen lineamientos generales, que buscan orientar una adecuada gestión de cambios en la ADR y sus sistemas de información</u>

El procedimiento exige que cuando se quieran efectuar cambios sobre algún sistema de información o dispositivo en ambiente de producción deberá plantear planes de reversión y tratamiento de riesgos enfocados a mitigación y planes de contingencia, los cuales tendrán que estar documentados dentro de la plataforma o formato definido. Encontrando que no se remitieron documentos de planificación ni operación de controles; tampoco se logró verificar la ejecución de controles exigidos por el MSPI.

<u>Actividades 1 y 2 – Realizar el registro de solicitud de cambio mediante la plataforma de mesa de ayuda y Adjuntar el formato GESTIÓN DE CAMBIOS DE SEGURIDAD DE LA INFORMACIÓN y PLAN GENERAL DE PRUEBAS TIC según las condiciones establecidas – sin evidencia</u>

La Oficina auditada debe verificar que las actividades queden registradas en la mesa de ayuda / módulo de gestión de cambios: No se aportan registros, por lo que no se pudo verificar ninguna fase del MSPI de manera completa.

De otra parte, es pertinente enunciar que claramente otras normas de rango supra también se ven vulneradas pues téngase en cuenta que los incumplimientos al procedimiento interno vienen sustentados y direccionados por normas macro como los son:

- Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información – MinTIC:

<u>Sección 6 (Diagnóstico: exige la obtención de insumos claros que permitan establecer el estado real del MSPI)</u>;

Si bien la entidad realizó ejercicios de diagnóstico en 2023 y 2025 mediante instrumentos de evaluación, dichos ejercicios no se encuentran soportados con insumos verificables, ni se evidencia su uso como línea base formal para la toma de decisiones. Para la vigencia 2024 no se aportó diagnóstico alguno. En

consecuencia, el diagnóstico no cumple su propósito de reflejar el estado real y verificable del MSPI en todas las vigencias auditadas.

Sección 7 (Fase de Planificación: que la entidad realice la planeación del tiempo, recursos y presupuesto de las actividades que va a desarrollar relacionadas con el MSPI);

No se evidencian planes derivados de los diagnósticos realizados (planes de acción, cronogramas, responsables, recursos o metas). La ausencia de documentación de planificación impide verificar que la entidad haya definido cómo cerrar las brechas identificadas, incumpliendo el principio de planeación del MSPI.

Sección 8 (Fase de Operación: establece la necesidad de ejecutar y controlar operacionalmente el MSPI.);

No se remitieron evidencias que permitan verificar la ejecución operativa de controles de seguridad de la información (registros, actas, reportes, tickets, bitácoras, pruebas o controles en funcionamiento). En consecuencia, no es posible constatar que el MSPI haya sido implementado y operado de manera efectiva.

Sección 9 (Evaluación del Desempeño: dispone la medición mediante indicadores y la realización de la revisión por la dirección.)

No se evidencian mediciones, indicadores, resultados documentados ni seguimiento al desempeño del MSPI. La entidad no aportó información que permita evaluar si los controles implementados, de llegar a existir, están siendo efectivos, ni reportes periódicos de desempeño del sistema.

Sección 10 (Fase de mejoramiento continuo: diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.)

No se evidencian acciones de mejora, planes de mejoramiento ni seguimiento al cierre de brechas identificadas en los diagnósticos. Al no existir evaluación ni

revisión por la dirección, tampoco se materializan acciones de mejora, rompiendo las fases del MSPI.

- ISO/IEC 27001:2022

Cláusula 6 (Acciones para tratar los riesgos y oportunidades; evaluarlos, tratarlos)

Se incumple porque no se evidencian acciones planificadas para tratar riesgos ni para alcanzar objetivos de seguridad de la información derivados de los diagnósticos.

Cláusula 8 (Operación: no se evidenciaron operación de controles)

Se incumple porque no se aportan evidencias de que los controles de seguridad se encuentren operando bajo condiciones controladas.

Cláusula 9.1 (Seguimiento, medición, análisis y evaluación)

Se incumple porque la oficina auditada no arribó mediciones documentadas ni análisis de desempeño del MSPI.

Cláusula 9.3 (Revisión por la dirección)

Se incumple porque no se evidencia revisión del sistema por la alta dirección.

Cláusula 10 (mejorar de manera continua la idoneidad, adecuación y eficacia del sistema de gestión de la seguridad de la información)

Se incumple porque no existen acciones de mejora documentadas ni seguimiento a brechas.

- MO-GTI-001:

Sección 7.2 (Objetivos del Subsistema de Seguridad y Privacidad de la Información)

Se incumple porque, aunque los objetivos del MSPI están definidos, no se evidencia su ejecución, seguimiento ni evaluación, lo que impide verificar su cumplimiento.

Sección 11 (Medición y seguimiento del Subsistema de Seguridad y Privacidad de la Información.

Se incumple porque no se aportaron indicadores, reportes ni resultados de medición del MSPI, pese a que el manual define frecuencias y responsables.

CRITERIO DOS: ***EFECTIVIDAD DE LOS CONTROLES DEL AUTODIAGNÓSTICO DEL MSPI:*** Se solicitó evidencias a la Oficina de Tecnologías de la Información (OTI), mediante correo electrónico el día 03 de diciembre 2025 y el día 10 de Diciembre 2025 para constatar que se cuenta con las evidencias de los avances de cada uno de los controles establecidos y el Porcentaje que la OTI se autocalifico: Se encuentra que para el segundo semestre en la vigencia 2023, no se remiten evidencias específicas por control que permitieran corroborar los soportes utilizados para sustentar las calificaciones y porcentajes de avance auto asignado, lo que imposibilitó verificar la coherencia entre la evaluación realizada y la implementación real de los controles. Para la vigencia 2024, no se allegó ningún instrumento de autodiagnóstico ni documentación que permita verificar la realización de un ejercicio formal de evaluación de la efectividad de los controles. Finalmente, para la vigencia 2025, si bien existió un instrumento de autodiagnóstico y diligencia, junto a éste nuevamente se abstuvieron de aportar evidencias que permitiera verificar la objetividad de la efectividad de los controles y la coherencia entre la auto calificación y su soporte documental, por lo que en ninguna de las vigencias auditadas fue posible verificar la efectividad de los controles MSPI, ni efectuar la comparación evidencia calificación exigida.

Incumplimientos asociados:

- Al procedimiento PR- GTI-002

Numeral 5.1 – ROLES Y RESPONSABILIDADES EN LOS PROCEDIMIENTOS DE GESTIÓN DE CAMBIOS TECNOLÓGICOS: se establecen los roles encargados de llevar a cabo una adecuada gestión de cambios:

Se incumple porque no se puede verificar la efectividad de los controles de seguridad asociados a los cambios.

Numeral 5.2 – Se definen lineamientos generales, que buscan orientar una adecuada gestión de cambios en la ADR y sus sistemas de información

Se incumple porque no se aportaron documentos exigidos para soportar controles evaluados.

Numeral 5.4 – Se definen los requisitos documentales para la apertura y autorización de cambios

Se incumple porque no se evidencian los soportes mínimos exigidos para autorizar y evaluar cambios.

Numeral 5.7 – Se definen los lineamientos para la ejecución de los cambios y las pruebas de funcionalidad y verificación posteriores

Se incumple porque no existen pruebas documentadas que respalden la efectividad de los controles.

De otra parte, es pertinente enunciar que claramente otras normas de rango supra también se ven vulneradas pues téngase en cuenta que los incumplimientos al procedimiento interno vienen sustentados y direccionados por normas macro como los son:

- Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información – MinTIC:

Sección 9 (Evaluación del Desempeño: dispone la medición mediante indicadores y la realización de la revisión por la dirección.)

Se incumple porque la entidad no logró demostrar, con evidencia verificable, la efectividad real de los controles evaluados en los autodiagnósticos.

Sección 9.1. (Seguimiento, medición y análisis.)

Se incumple porque no se aportaron soportes que respalden las calificaciones asignadas a cada control ni análisis de resultados.

- ISO/IEC 27001:2022

Cláusula 9.1 (Seguimiento, medición, análisis y evaluación)

Se incumple porque no existe evidencia objetiva que permita medir la efectividad de los controles.

Cláusula 9.2 (Auditoria interna)

Se incumple porque la ausencia de evidencia documentada impide realizar auditorías internas confiables.

- MO-GTI-001:

Sección 11 (Medición y seguimiento del Subsistema de Seguridad y Privacidad de la Información.

Se incumple porque no se evidencian mediciones ni resultados que soporten la evaluación del desempeño del MSPI.

Ley 1952 de 2019 – Código General Disciplinario, establece el deber de Cumplir funciones asignadas, Observar normas internas y externas, Actuar con diligencia y responsabilidad: Encontrando que los incumplimientos descritos podrían configurar **omisiones funcionales** y **desatención de deberes**, sujetas a análisis disciplinarios.

DECRETO 403 DEL 2020 "Por el cual se dictan normas para la correcta implementación del Acto Legislativo 04 de 2019 y el fortalecimiento del control fiscal", que en su artículo 151 señala: ***"Deber de entrega de información para el ejercicio de las funciones de la unidad u oficina de control interno. Los servidores responsables de la información requerida por la unidad u oficina de control interno deberán facilitar el acceso y el suministro de información confiable y oportuna para el debido ejercicio de sus funciones, salvo las excepciones establecidas en la ley. Los requerimientos de información deberán hacerse con la debida anticipación a fin de garantizar la oportunidad y completitud de la misma"***

El incumplimiento reiterado al suministro de la información solicitada por la unidad u oficina de control interno dará lugar a las respectivas investigaciones disciplinarias por la autoridad competente."

NOTA: La presente prueba se ve limitada respecto a que la información no fue dispuesta de manera suficiente, toda vez que, en correos enviados el 19 de septiembre de 2025, y 06 de noviembre de 2025 a la Oficina de Tecnologías de la Información (OTI) se solicitó la información relacionada con la implementación de las fases del MSPI y su cumplimiento, así como el avance de cada uno de los controles establecidos. Pues para las vigencias auditadas no se arribó la información suficiente y para a videncia 32024, se abstuvo de aportar evidencia alguna.

POSIBLE(S) CAUSA(S) IDENTIFICADA(S) POR LA OFICINA DE CONTROL INTERNO:

- Implementación parcial y no continua del MSPI en las vigencias auditadas (2023–2025).
- Ausencia total de evidencia de implementación del MSPI para la vigencia 2024.
- Falta de planes de acción derivados de los diagnósticos y autodiagnósticos.
- No se evidencian controles de seguridad operando de forma verificable.
- No se evidencian indicadores, medición de desempeño ni seguimiento del MSPI.
- No se evidencian actas de revisión por la dirección.
- No se evidencian acciones de mejora ni seguimiento al cierre de brechas.
- Autodiagnósticos del MSPI sin evidencias por control que soporten la auto calificación.
- Imposibilidad de comparar las evidencias con calificación de controles.

DESCRIPCIÓN DE LA(S) CAUSA(S):

- Implementación parcial y no continua del MSPI en las vigencias auditadas (2023–2025).
- Falta de planes de acción derivados de los diagnósticos y autodiagnósticos.
- No se evidencian controles de seguridad operando de forma verificable.

- Autodiagnósticos del MSPI sin evidencias por control que soporten la auto calificación.

DESCRIPCIÓN DEL(LOS) RIESGO(S):

- Posibilidad de afectación de la imagen institucional como consecuencia del incumplimiento en la ejecución, monitoreo y cierre de los planes, programas, proyectos, indicadores y acciones orientadas al fortalecimiento del proceso de tecnología y del Subsistema de Gestión de Seguridad de la Información, en el marco de los lineamientos estratégicos aprobados por la entidad.
- Posibilidad de afectación de la imagen institucional como consecuencia del incumplimiento de los objetivos y metas institucionales, derivado de errores en la planeación, desarrollo, implementación y mantenimiento de los sistemas de información e infraestructura tecnológica, así como de fallas en los procesos de adquisición de bienes y servicios de Tecnologías de la Información de la entidad.
- Posible impacto económico y reputacional derivado de la falta de un monitoreo y seguimiento efectivo de los incidentes de seguridad y ciberseguridad, vulneración de los controles de seguridad, comprometiendo así la integridad de los diversos activos de información de la Entidad.

DESCRIPCIÓN DEL(LOS) IMPACTO(S):

- Impacto reputacional e institucional, por la afectación de la imagen de la entidad ante el incumplimiento reiterado de los compromisos estratégicos asociados al fortalecimiento del proceso de tecnología y del Subsistema de Gestión de Seguridad de la Información.
- Impacto operativo y estratégico, derivado del incumplimiento de los objetivos y metas institucionales relacionados con la seguridad de la información, lo que limita la capacidad de la entidad para gestionar adecuadamente sus sistemas de información e infraestructura tecnológica.

- Impacto económico y reputacional, como consecuencia de la falta de monitoreo y seguimiento efectivo de los controles e incidentes de seguridad de la información, aumentando la probabilidad de materialización de incidentes que comprometan la integridad de los activos de información de la entidad.

RESPUESTA DEL AUDITADO: Aceptado

JUSTIFICACIÓN: No indican.

CAUSA(S) IDENTIFICADA(S) POR EL RESPONSABLE DE LA UNIDAD AUDITADA:

- Falta de actualización de Lineamientos de Seguridad de la Información.
- Falta de actualización procedimiento de Gestión de Cambios de seguridad de la información.
- Ejecución de Autodiagnóstico versión ISO27001:2022 sin análisis de brecha.
- Implementación parcial y no continua del MSPI sin indicadores de seguimiento

CONCEPTO DE LA OFICINA DE CONTROL INTERNO: Aceptado

JUSTIFICACIÓN:

En relación con el Plan de Mejoramiento, la Oficina de Control Interno considera razonables las acciones propuestas para gestionar las causas identificadas por el equipo auditado y atender las observaciones formuladas en el presente informe

RESUMEN DE HALLAZGOS:

Tabla 6. Resumen de los Hallazgos establecidos en la Auditoria

N°	Título de Hallazgo	Repetitivo	Estado
1	Inobservancia en la implementación de los lineamientos establecidos en la normatividad aplicable respecto a la preparación de las TIC para la continuidad del negocio para las vigencias 2023 a 2025	**NO**	Abierto
2	Deficiencias en el análisis continuo de amenazas y en la implementación de acciones de mitigación para la seguridad de la información.	**NO**	Abierto

3	Debilidades estructurales en la implementación del modelo de seguridad y privacidad de la información (MSPI) y en la evaluación de la efectividad de sus controles	**NO**	Abierto

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 la unidad auditada 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.

- La respuesta ante las situaciones observadas por la Oficina de Control Interno es discrecional de la Administración de la Agencia de Desarrollo Rural, más se incentiva considerar las *"Recomendaciones"* propuestas por esta Oficina para el establecimiento de los planes de mejoramiento a que haya lugar.

Bogotá D.C., 29 de diciembre del 2025.

CARLOS ALBERTO CORTÉS RIAÑO
jefe Oficina de Control Interno

Elaboró: *Diana Marcela Cuervo Espinosa, Contratista Oficina Control Interno*
Revisó: *Carlos Alberto Cortés Riaño, jefe Oficina Control Interno.*