AGENCIA DE DESARROLLO RURAL – ADR

Oficina de Control Interno

N° INFORME: OCI-2023-022

DENOMINACIÓN DEL TRABAJO: Auditoría al *"Modelo de Seguridad y Privacidad de la Información".*

DESTINATARIOS:[1]

- Luis Alberto Higuera Malaver, Presidente.
- Mónica Rocío Adarme Manosalva, Jefe de la Oficina Jurídica (Delegado de Presidencia - Comité de Coordinación del Sistema de Control Interno) y Secretaria General (E).
- Javier Edilberto Fernández Nope Vicepresidente de Gestión Contractual (E).
- Onis Johanna Fierro Hernández, Jefe de la Oficina de Planeación.
- Javier Enrique Cely Amézquita, Vicepresidente de Proyectos (E).
- Yineth Esperanza del Pilar Guarnizo Rojas, Vicepresidente de Integración Productiva (E).

EMITIDO POR: Wilson Giovanny Patiño Suárez, Jefe Oficina de Control Interno.

AUDITOR (ES): Juan Harbey Numpaque Fonseca, Contratista.

Jorge Iván Flórez Franco, Contratista.

[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:

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 asociados al *"Modelo de Seguridad y Privacidad de la Información"*.

ALCANCE:

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

CP-ETI-001 ESTRATEGIA DE TECNOLOGÍAS DE LA INFORMACIÓN

- Definición de planes estratégicos en materia de TI.
- Definición de Manual de Políticas de TI.
- Formulación el Plan de implementación del MIPG relacionado con las políticas de Gobierno digital y Seguridad digital.
- Identificación, análisis, valoración de los Activos de seguridad digital.
- Identificación, análisis, valoración de los Riesgos de seguridad digital.
- Implementación de políticas, lineamientos y estrategias para el desarrollo de proyectos TIC.
- Implementación de los lineamientos de gestión de riesgo de seguridad digital.

CP-GTI-001 OPERACIÓN DE LOS SERVICIOS TECNOLÓGICOS

- Gestionar la seguridad informática.

Periodo Auditado: Abril de 2021 al mes de abril de 2023.

Nota: El establecimiento de este período no limitaba 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.

LIMITACIÓN:

No aplicó en el desarrollo de la 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:

- **Decreto 1078 de 2015** *"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".*
- **Decreto 767 de 2022** *"Por el cual se establecen los lineamientos generales de la política de Gobierno digital y se subroga el capítulo 1 del Título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de las Tecnologías de la Información y las Comunicaciones".*
- **Decreto 088 de 2022** - *"Por el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"* Proyectos de transformación digital.
- **Manual de Gobierno Digital** *"El Manual de Gobierno Digital es el documento que establece los lineamientos y estándares de los componentes de la política (TIC para el Estado y TIC para la Sociedad) y de los habilitadores transversales (arquitectura, seguridad y privacidad de la información y servicios ciudadanos digitales)".*
- **Resolución 081 de 21 de abril de 2021** *"Por la cual se adopta la política general de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios, así como definir lineamientos frente al uso y manejo de la información de la Agencia de Desarrollo Rural - ADR".*
- **Caracterización del proceso Estrategias de Tecnologías de la Información: (CP-ETI-001) versión 1.**

  Manual de Operaciones: MO-ETI-001 manual con las Políticas de Seguridad y Privacidad de la Información
- **Caracterización del proceso Operación de los Servicios Tecnológicos: (CP-GTI-001) versión 3.**

PR-OST-003 Desarrollo, implementación y mantenimiento de sistemas de información.
PR-OST-004 Gestión de incidentes de seguridad de la información.
PR-OST-005 Administración de redes
PR-OST-006 Administración de usuarios y Sistemas de Información
PR-OST-007 Gestión de Incidentes y Requerimientos Tecnológicos
PR-OST-008 Gestión de cambios tecnológicos
PR-OST-010 Gestión del Conocimiento de servicios de TI

▪ Demás normatividad aplicable.

RESUMEN EJECUTIVO:

Como resultado de la auditoría realizada, se identificaron oportunidades de mejora relacionadas con los siguientes tópicos:

1. Incumplimiento de la *"Política de Seguridad para la Adquisición, Desarrollo y Mantenimiento de Sistemas"* definida en la resolución 081 de 2021 *"Por la cual se adopta la política general de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios, así como definir lineamientos frente al uso y manejo de la información de la Agencia de Desarrollo Rural".*
2. Falta de efectividad del control "*Definir y elaborar el catálogo de sistemas de información que tiene como propósito identificar y conservar una lista completa y actualizada de los sistemas de información en la ADR, con el fin de identificar como es el acceso y evaluar el control".*
3. Debilidades en el cumplimiento de la Política de Seguridad Digital, frente a la inactivación de los servicios tecnológicos de funcionarios desvinculados de la Entidad.
4. Incumplimiento de la gestión de vulnerabilidades identificadas de acuerdo con el Manual de Operaciones: MO-OST-003 Guía de aseguramiento de Servicios en la Red.
5. Asignación de calificación no congruente con las evidencias obtenidas en la fase de Diagnóstico MSPI.
6. Incumplimiento de la política de control de acceso por la falta de actualización de contraseñas de cuentas genéricas.

RIESGOS IDENTIFICADOS EN LA AUDITORÍA:

Tabla 1. Riesgos identificados en la Auditoria

DESCRIPCIÓN	CUBIERTO EN LA AUDITORÍA
Incluidos en el mapa de riesgos de gestión	
Posibilidad de afectación económica y reputacional por perdida de un servicio o recurso tecnológico que afecta la continuidad de la operación de TI debido a la falta de configuración y monitoreo de la infraestructura tecnológica	SI
Incluidos en el mapa de riesgos de corrupción	
Posibilidad de alteración o sustracción de información de la Entidad por parte de un funcionario y/o contratista, haciendo uso de los privilegios asignados para el beneficio propio o de un tercero, generando la desviación de la gestión de los recursos públicos	SI
Identificados por la Oficina de Control Interno	
Posibilidad de afectación reputacional y económica por multa y sanción del ente regulador debido a la inadecuada Gestión de riesgos de seguridad digital definido en su Plan de Tratamiento de Riesgos.	SI
Posibilidad de afectación reputacional y económica por multa y sanción del ente regulador debido al incumplimiento de la política de seguridad de los recursos humanos.	SI
Posibilidad de afectación reputacional y económica por multa y sanción del ente regulador debido al incumplimiento de la política de gestión de los activos de la ADR.	SI
Posibilidad de afectación reputacional y económica por multa y sanción del ente regulador debido al incumplimiento de los criterios de control y acceso definidos en la resolución 081 de 2021	SI
Posibilidad de afectación reputacional y económica por multa y sanción del ente regulador debido al incumplimiento de política de criptografía definida en la resolución 081 de 2021	SI
Posibilidad de afectación reputacional y económica por multa y sanción del ente regulador debido al incumplimiento de política de seguridad física y del entorno definido en la resolución 081 de 2021.	SI
Posibilidad de afectación reputacional y económica por multa y sanción del ente regulador debido al incumplimiento de política de seguridad de las operaciones definidas en la resolución 081 de 2021.	SI
Posibilidad de afectación reputacional y económica por multa y sanción del ente regulador debido al incumplimiento de política de seguridad de las telecomunicaciones definida en la resolución 81 de 2021.	SI

DESCRIPCIÓN	CUBIERTO EN LA AUDITORÍA
Posibilidad de afectación reputacional y económica por multa y sanción del ente regulador debido al incumplimiento de la Política de Seguridad para la Adquisición, Desarrollo y Mantenimiento de Sistemas	SI
Posibilidad de afectación reputacional y económica por multa y sanción del ente regulador debido al incumplimiento de la política de Gestión de Incidentes de Seguridad de la información definido en la resolución 81 de 2021.	SI
Posibilidad de afectación reputacional y económica por multa y sanción del ente regulador debido al incumplimiento de la Política de la Continuidad de la Operación del Servicio definida en la resolución 081 de 2021.	SI
Posibilidad de afectación reputacional y económica por multa y sanción del ente regulador debido al incumplimiento de la política general de seguridad y privacidad de la información y sus objetivos, dada una operación inadecuada del MSPI en una de sus cinco fases (diagnóstico, planificación, operación, evaluación del desempeño, mejoramiento continuo).	SI

Fuente. Elaboración propia Oficina de Control Interno

FORTALEZAS*:*

En la ejecución del trabajo, la Oficina de Control Interno observó la siguiente situación a destacar dentro del *"Modelo de Seguridad y Privacidad de la Información":*

- Disposición en la aplicación ISOLUCION de la información documentada del proceso Oficina de Tecnologías de la Información - OTI, en lo que tiene que ver con el "*Modelo Seguridad y Privacidad de le Información MSPI"* de forma organizada.

OPORTUNIDADES DE MEJORA:

De igual manera la Oficina de Control Interno evidenció las siguientes oportunidades de mejora:

- El procedimiento **DE-GTI-006 Gestión de Cambios Tecnológicos** requiere ser socializado y aplicado en la Entidad de acuerdo con las actividades definidas.
- Definir las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información, por lo cual estos eventos se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.

- convocar a todos los servidores y contratistas que usan los servicios y sistemas de información de la Agencia, que informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
- Identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de datos.
- Establecer, documentar, implementar y mantener procesos, procedimientos y controles para garantizar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa.

AVANCE DEL PLAN DE MEJORAMIENTO VIGENTE AL INICIO DE LA AUDITORIA:
No Aplica. Esta actividad de aseguramiento corresponde al primer ejercicio de auditoría interna practicado por la Oficina de Control Interno al *"Modelo de Seguridad y Privacidad de la Información"*.

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 el auditor que practicó 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*: Incumplimiento de la "Política de Seguridad para la Adquisición, Desarrollo y Mantenimiento de Sistemas"* definida en la resolución 081 de 2021 *"Por la cual se adopta la política general de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios, así como definir lineamientos frente al uso y manejo de la información de la Agencia de Desarrollo Rural"*

Con el fin de verificar el cumplimiento de lo establecido en la Resolución No 081 de 2021, Articulo Décimo Tercero: "*Política de seguridad para la adquisición, desarrollo y mantenimiento de sistemas", que indica: "(…)En el marco del Plan Estratégico de Tecnologías de la Información (PETI), la Oficina de Tecnologías de la Información es la*

única dependencia de la Agencia con la capacidad de adquirir, desarrollar e implementar soluciones tecnológicas para la ADR, así como de avalar la adquisición y recepción de software de cualquier tipo en el marco de convenios y contratos con terceros, conforme con los requerimientos de las diferentes dependencias, con el fin de garantizar la conveniencia, soporte, mantenimiento y seguridad de la información de los sistemas que operan en la ADR(…)", la Oficina de Control Interno solicitó información de la aplicación SOLUCIONES DIGITALES PARA EL CAMPO, de lo cual identificó, que la aplicación se construyó en el marco del contrato 9962021 con las siguientes características:

Link de Secop II:
https://www.secop.gov.co/CO1BusinessLine/Tendering/ContractNoticeView/Index?notice=CO1.NTC.2262150

Objeto: "*Prestar el Servicio Público de Extensión Agropecuaria a través de la metodología digital en los términos establecidos en la Ley 1876 de 2017 y la resolución 407 del 30 de octubre de 2018, en los treinta (30) departamentos que cuentan con el Plan Departamental de Extensión Agropecuaria – PDEA, adoptado por Ordenanza Departamental*".

Plazo de ejecución del proyecto: 10 meses, hasta el 31 de Julio de 2022

Valor del contrato: DIECISÉIS MIL NOVECIENTOS CINCO MILLONES QUINIENTOS MIL PESOS M/CTE ($16.905.500.000).

Al indagar por la documentación del contrato a la OTI el 26 de junio de 2023, se indicó por parte de esta dependencia *"La ADR se encuentra recibiendo la aplicación "Soluciones Digitales para el Campo", desarrollada por la Universidad Tecnológica de Pereira. Dicha aplicación fue contemplada como parte de los entregables del contrato y la Oficina de Tecnologías de la Información ha apoyado a la Entidad con los conceptos técnicos necesarios para el despliegue y puesta en producción de la herramienta. Así mismo, la ADR ha facilitado un servidor virtual y un certificado SSL para tal fin. Actualmente el despliegue de la aplicación se encuentra en etapa de pruebas por parte del área funcional. Para mayor información sobre este contrato y la herramienta tecnológica que de él se desprende, favor contactar a la Vicepresidencia de Proyectos,*

quienes fueron los encargados de realizar los estudios previos y la contratación con la Universidad Tecnológica de Pereira, ya que como se mencionó anteriormente, ***la Oficina de Tecnologías de la Información se ha limitado únicamente a hacer el acompañamiento para el despliegue de la aplicación****."* Negrita fuera de texto.

Dada la situación presentada se procedió a verificar la participación de la OTI en el rol de "…*que la Oficina de Tecnologías de la Información es la* ***única dependencia de la Agencia con la capacidad de adquirir****, desarrollar e implementar soluciones tecnológicas para la ADR así como de* ***avalar la adquisición*** *y recepción de software de cualquier tipo en el marco de convenios y contratos con terceros*" (Negrita fuera de texto), por lo cual, la Oficina de Control Interno revisó la documentación del contrato, donde se identificaron las siguientes situaciones:

- La Oficina de Tecnologías de la Información – OTI no participó en la construcción de los Estudios Previos del contrato, debido a que la Vicepresidencia de Integración Productiva coordinó de forma exclusiva la generación de los respectivos estudios previos.
- No se evidenció en el Acta de Comité Técnico número 1, realizado del 5 al 8 de septiembre de 2021 la participación de la Oficina de Tecnologías de la Información – OTI.
- De acuerdo con el clausulado del contrato, la supervisión del contrato fue ejercida por el Vicepresidente de Integración Productiva con apoyo de un contratista de la Dirección de Asistencia Técnica, no obstante, no se evidenció apoyo y/o participación de algún profesional de la OTI.

Teniendo en cuenta las situaciones mencionadas anteriormente, se logró evidenciar que para la aplicación SOLUCIONES DIGITALES PARA EL CAMPO desarrollada por la Universidad Tecnológica de Pereira en el marco del contrato 9962021 liderado por la Vicepresidencia de Integración Productiva de la ADR, la Oficina de Tecnologías de la Información OTI participó **únicamente en la adecuación de la infraestructura para la fase de despliegue**, incumpliendo los criterios presentados a continuación:

- **Resolución No 081 de 2021**, Articulo Décimo Tercero: *"Política de seguridad para la adquisición, desarrollo y mantenimiento de sistemas",* que indica: *"(…)En el marco*

del Plan Estratégico de Tecnologías de la Información (PETI), ***la Oficina de Tecnologías de la Información es la única dependencia de la Agencia con la capacidad de adquirir, desarrollar e implementar soluciones tecnológicas para la ADR****, así como de avalar la adquisición y recepción de software de cualquier tipo en el marco de convenios y contratos con terceros, conforme con los requerimientos de las diferentes dependencias, con el fin de garantizar la conveniencia, soporte, mantenimiento y seguridad de la información de los sistemas que operan en la ADR(…)".* Negrita fuera de texto.

- **Manual de Operación: MO-OST-009 Guía de Desarrollo Seguro**, cuyo objetivo es *"Establecer las condiciones y vigilar que el desarrollo y mantenimiento de software llevado a cabo, tanto internamente como por proveedores externos de la Agencia de Desarrollo Rural – ADR, cumpla con buenas prácticas para el desarrollo seguro, además de establecer los criterios de seguridad que deben ser considerados en todas las etapas del desarrollo."* **Numeral 3.3. RESPONSABLE**: *"La Oficina de Tecnologías de Información – OTI, es la responsable de planificar, desarrollar y ejecutar las actividades relacionadas con los desarrollos, actualizaciones e instalaciones de software. Además, debe planificar la ejecución de pruebas funcionales y de seguridad de los sistemas nuevos o modificados antes de ejecutar la instalación en los servidores de producción".*

POSIBLE(S) CAUSA(S) IDENTIFICADA(S) DESCRIPCIÓN DE LOS RIESGOS E IMPACTOS:

Tabla 2. Detalle de las Posibles causas, riesgos e impactos identificadas por la Oficina de Control Interno

Causas	Riesgos	Impactos
▪ Desconocimiento de los lineamientos establecidos en la resolución No. 081 de 2021. ▪ Debilidad en la aplicación de los lineamientos establecidos de la Seguridad y la Privacidad de la información de la Resolución No. 081 de 2021. ▪ Debilidades en la ejecución de los procedimientos establecidos para la Seguridad y la Privacidad de la Información ▪ Informalidad en la ejecución de los procedimientos de la	Posibilidad de afectación reputacional y económica por multa y sanción del ente regulador debido al incumplimiento de la Política de Seguridad para la Adquisición, Desarrollo y Mantenimiento de Sistemas	▪ Daño de la Imagen institucional. ▪ Afectación en el cumplimiento de metas y objetivos de la Entidad. ▪ Afectación en el cumplimiento de las políticas definidas en el PETI 2023-2026. ▪ Afectación económica por incremento en los costos del proyecto, por el soporte del nuevo sistema. ▪ Dependencia Tecnológica de la ADR ▪ Afectación económica por demandas en el cumplimiento de las políticas de tratamiento de datos personales.

Causas	Riesgos	Impactos
Seguridad y la Privacidad de la Información		▪ Deficiente uso y apropiación de los proyectos de TI, por parte de los Usuarios Finales.

Fuente. Elaboración propia Equipo Auditor – Oficina de Control Interno.

RECOMENDACIÓN(ES):

En virtud de las situaciones identificadas la Oficina de Control Interno insta a la Oficina de Tecnologías de la Información a tener en cuenta las siguientes recomendaciones:

- Solicitar a la Vicepresidencia de Gestión Contractual que todos los procesos contractuales que se desarrollen al interior de la Entidad y que estén asociados con la adquisición y recepción de software de cualquier tipo en el marco de convenios y contratos con terceros, conforme con los requerimientos de las diferentes dependencias, se involucre a la Oficina de Tecnologías de la Información, con el fin de dar cumplimiento al Modelo de Seguridad y Privacidad de la información de la ADR.
- Socializar los lineamientos descritos en la resolución No. 081 de 2021, ya que, en dicha resolución, se adopta el Modelo de Seguridad y Privacidad de la información de la ADR, y este se convierte en documento de obligatorio cumplimiento.
- Hacer campañas de socialización de la Resolución No. 081 de 2021, al interior de la Entidad.
- Socializar los manuales, procedimientos, protocolos, guías, instructivos y demás documentación publicada en la plataforma ISOLUCION, en materia de la Seguridad y la Privacidad de la información.

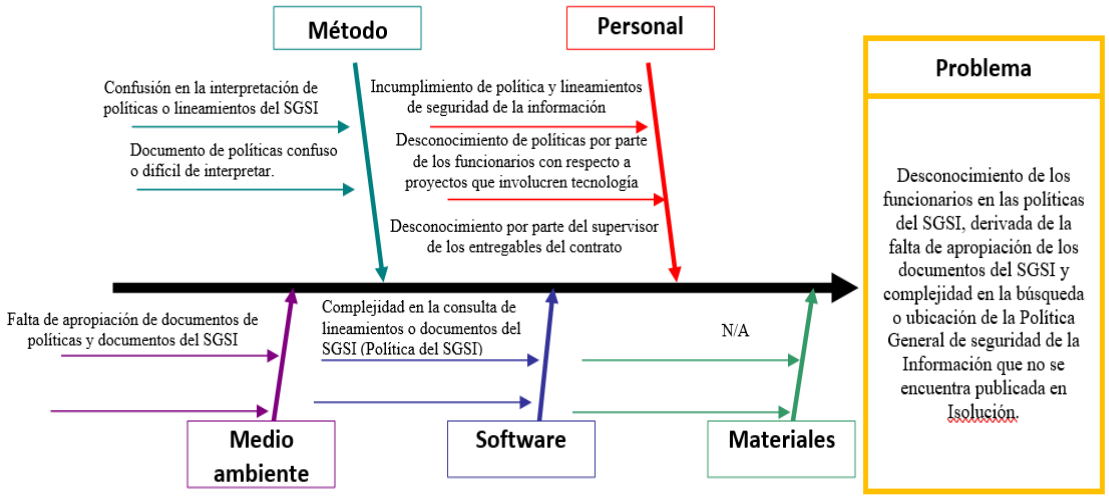
RESPUESTA DEL AUDITADO: ACEPTADO PARCIALMENTE.

JUSTIFICACIÓN:

"Respecto a la descripción del hallazgo reportado "Se logró evidenciar que para la aplicación SOLUCIONES DIGITALES PARA EL CAMPO desarrollada por la Universidad Tecnológica de Pereira en el marco del contrato 9962021 liderado por la Vicepresidencia de Proyectos de la ADR, la Oficina de Tecnologías de la Información OTI participó únicamente en la adecuación de la infraestructura para la fase de despliegue, incumpliendo los criterios presentados a continuación" indicamos que no estamos de acuerdo, teniendo en cuenta que es deber de todos los procesos escalar y

comunicar a la OTI respecto a cualquier temática relacionada con procesos de adquisición desarrollo y mantenimiento de sistemas de información o infraestructura tecnológica, de este modo, si un proceso no cumple con realizar esta comunicación, la Oficina no puede hacerse responsable de las acciones, contratos o convenios que estas celebren, sin tener en cuenta el concepto de la Oficina de Tecnología, por lo cual se solicita que se amplie el contexto del hallazgo, dado que la OTI fue informada de que en el marco del citado contrato, se recibiría un aplicativo por parte de la UTP al momento de recibir esta aplicación "finalizada", es decir, la OTI no fue informada de esta situación desde la concepción de este contrato por lo cual su participación fue limitada a la etapa final, porque así lo dispuso la vicepresidencia".

CAUSA(S) IDENTIFICADA(S) POR EL RESPONSABLE DEL PROCESO AUDITADO:



Fuente: Respuesta Reporte de Hallazgo

PLAN DE MEJORAMIENTO:

Tabla 3. Plan de mejoramiento

Acción(es) propuesta(s)	Meta(s)	Tipo de acción	Responsable(s)	Fecha inicial	Fecha final
Asesorar a la Vicepresidencia de Proyectos, brindando las recomendaciones necesarias para el cumplimiento de	Informes de los aspectos y criterios de seguridad de la información que	Correctiva	Jefe Oficina de Tecnología de la Información	21-jul-2023	31-dic-2023

Acción(es) propuesta(s)	Meta(s)	Tipo de acción	Responsable(s)	Fecha inicial	Fecha final
lineamientos de seguridad para la recepción de los aspectos que tengan que ver con tecnología en el convenito con la UTP	deben ser ajustadas en lo entregado por el convenito con la UTP				
Generar nuevos documentos, Política del Sistema de Gestión de Seguridad de la Información y Manual de políticas de Seguridad de la Información para el buen uso de los activos de información. De tal forma que sea más fácil su interpretación y consulta de lineamientos del SGSI. Solicitar la derogación de la resolución 081 de 2021.	Política del Sistema de Gestión de Seguridad de la Información y Manual de políticas de Seguridad de la Información para el buen uso de los activos de información claros, accesibles y que sean de fácil interpretación y búsqueda por el usuario.	Preventiva	Grupo Seguridad de la Información – Oficina Tecnología de la Información Grupo Seguridad de la Información – Oficina Tecnología de la Información	21-jul-2023 31-jul-2023	31-dic-2023 31-dic-2023
Llevar los documentos Política del Sistema de Gestión de Seguridad de la Información y Manual de políticas de Seguridad de la Información para el buen uso de los activos de información a comité Institucional de Gestión y Desempeño para aprobación. Solicitar a la Oficina de Planeación, liberar documentos en el Sistema de gestión Integrado de Gestión para que sea cargado en el software Daruma y sea de fácil acceso o consulta.	Publicación de los documentos en el Sistema Integrado de Gestión, para centralización y fácil consulta y búsqueda de los documentos.	Preventiva	Jefe Oficina de Tecnología de la Información Grupo Seguridad de la Información – Oficina Tecnología de la Información Jefe Oficina de Tecnología de la Información Grupo Seguridad de la Información – Oficina Tecnología de la Información	15-ago-2023 15-ago-2023	31-dic-2023 31-dic-2023
Llevar a cabo charlas de concientización a todo el personal de la entidad, respecto a la Política del Sistema de Gestión de Seguridad de la Información y Manual de políticas de Seguridad de la Información	Evaluación de apropiación de los lineamientos y cultura de seguridad de la información dentro de la entidad.	Preventiva	Grupo Seguridad de la Información – Oficina	31-ago-2023	31-dic-2023

Acción(es) propuesta(s)	Meta(s)	Tipo de acción	Responsable(s)	Fecha inicial	Fecha final
para el buen uso de los activos de información			Tecnología de la Información	31-ago-2023	31-dic-2023
Divulgar los documentos por los diferentes medios establecidos en el Plan de Comunicación y Concientización de Seguridad de la Información de la vigencia.			Grupo Seguridad de la Información – Oficina Tecnología de la Información	01-nov-2023	29-feb-2024
Ejecutar evaluación de seguridad para medir la cultura organizacional y el nivel de apropiación de los documentos del SGSI y establecer planes de mejora en el plan de comunicación de la próxima vigencia.			Grupo Seguridad de la Información – Oficina Tecnología de la Información		

Fuente. Respuesta Reporte de Hallazgo

CONCEPTO DE LA OFICINA DE CONTROL INTERNO: CON OBSERVACIONES

Una vez verificadas las acciones propuestas en el plan de mejoramiento presentado, estas se consideran razonables, dado que pretenden atacar las causas de las situaciones que originaron las desviaciones identificadas, sin embargo, es importante que se tengan en cuenta las siguientes recomendaciones que permitan fortalecer o identificar acciones adicionales en el plan de mejoramiento con el fin de continuar con el fortalecimiento del proceso:

- Análisis de Requisitos Funcionales y no Funcionales del Sistema Desarrollado.
- Realización de Pruebas realizadas a los Requisitos Funcionales y no Funcionales del Sistema Desarrollado y la aceptación final de estas pruebas**.**
- **Análisis de Seguridad y Privacidad del Software desarrollado**: Se requiere certificar que el nuevo desarrollo, cumpla con los lineamientos establecidos por la ADR, respecto al desarrollo seguro del nuevo sistema.
- **Análisis de Vulnerabilidades del nuevo sistema**: Se requiere hacer análisis de vulnerabilidades del nuevo sistema y la certificación de que este nuevo desarrollo, no contiene brechas de seguridad.

- **Soporte del nuevo Sistema desarrollado**: Se requiere determinar quién va a dar el soporte a este nuevo desarrollo, donde se indiquen los acuerdos de niveles de servicios: ANS y cuál va a ser el costo de este soporte.
- **Transferencia de conocimiento**: Se requiere conocer la trasferencia de conocimiento de este nuevo sistema, de la Universidad Tecnológica de Pereira hacia la Agencia de Desarrollo Rural.
- **Datos Personales**: Se requiere certificar que si el nuevo desarrollo del Sistema, captura datos personales, este cumpla con la política establecida para el tratamiento de datos personales.

HALLAZGO N° 2: Falta de efectividad del control *"Definir y elaborar el catálogo de sistemas de información que tiene como propósito identificar y conservar una lista completa y actualizada de los sistemas de información en la ADR, con el fin de identificar como es el acceso y evaluar el control".*

Con el fin de verificar que todos los sistemas de información que utiliza la Agencia de Desarrollo Rural se encuentran incluidos en el catálogo de los sistemas de información de la Entidad, se solicitó el 29 de mayo de 2023 a la Oficina de Tecnologías de Información el "***Catálogo de los Sistemas de información de la ADR".***

De igual forma se tomó el listado de sistemas de información descrito en el PETI 2023-2026 y se requirió a las diferentes dependencias de la Entidad el listado de Sistemas de Información utilizados para el desarrollo de actividades, por lo cual, la Oficina de Control Interno verificó dicha información y realizó el cruce correspondiente, evidenciando lo siguiente:

Tabla 4. Sistemas de Información Utilizados en la ADR

LISTADO DE SISTEMAS DE INFORMACIÓN UTILIZADOS PARA EL DESARROLLO DE ACTIVIDADES EN LA ADR	SE ENCUENTRA EN EL CATÁLOGO DE SISTEMAS DE INFORMACIÓN DE LA ENTIDAD	
	SI	NO
IPDR	X	
PDRET	X	
BANCO DE PROYECTOS	X	

LISTADO DE SISTEMAS DE INFORMACIÓN UTILIZADOS PARA EL DESARROLLO DE ACTIVIDADES EN LA ADR	SE ENCUENTRA EN EL CATÁLOGO DE SISTEMAS DE INFORMACIÓN DE LA ENTIDAD	
	SI	NO
GESTION DE PROYETOS	X	
PERFIL DE PROYECTOS	X	
ISOLUCION	X	
ORFEO	X	
ULISES	X	
APOTHEOSYS	X	
CAMPUS VIRTUAL ADR	X	
INTRANET ADR	X	
SEDE ELECTRONICA (PORTAL WEB)	X	
DIRECTORIO ACTIVO Y OFFICE 365	X	
GESTION RESGUARDOS CONSULTORIA CONTRATISTAS ADR	X	
NOVEDADES TALENTO HUMANO	X	
COPIAS DE SEGURIDAD: Nube, Share Point, File Server	X	
SISTEMA DE SEGUIMIENTO DE INFORMACIÓN MISIONAL SSIM		X
ARANDA		X
SIGEP-NOMINA		X
ANTIVIRUS		X
MAPA DE INFORMACIÓN		X
FACTURACIÓN ADT		X
PQRSD		X
ISSABEL PBX		X
ARCGIS		X
RGU MONTERÍA		X
VALOR +		X
TENABLE		X
NAGIOS		X
KLIC		X

Elaboración propia Equipo Auditor. Fuente: Dependencias de la Entidad, PETI y Catalogo de Sistemas de Información

De acuerdo con la tabla anterior, se evidenció que la Entidad cuenta con treinta (30) sistemas de información, no obstante, catorce (14) de ellos no se encuentran incluidos en el *"Catálogo de los Sistemas de información de la ADR".*

Se indagó por el hecho que no se encontrara el Sistema de Seguimiento de Información Misional SSIM en el catálogo, a lo que se respondió por parte de la OTI:

"El Sistema de Seguimiento de Información Misional no es una aplicación como tal. Es un tablero de control que surge como iniciativa de la vicepresidencia de Proyectos y es liderada por la Ingeniera Paola Salazar, a quien copio en este correo, y desarrollado por la OTI. Dicho tablero es el resultado de la información suministrada por todas las áreas de la entidad con respecto a los Proyectos Agropecuarios que la entidad ha manejado desde el año 2019, centralizada en un solo reporte. El origen de los datos, como se dijo anteriormente, proviene de diferentes fuentes, como el Banco de Proyectos y diferentes reportes entregados por las diferentes áreas de la entidad, que se consolidan en un solo reporte y se presenta en un micro sitio web en la Intranet de la ADR.

Se espera que en un futuro se convierta en aplicación, una vez la OTI desarrolle una interfaz para la captura de datos por parte de cada área de la entidad y la información se consolide una única base de datos, pero por el momento, ese desarrollo no se ha llevado a cabo.

Puede ser accedido por cualquier colaborador de la Agencia de Desarrollo Rural a través de la Intranet de la Entidad: https://adrgov.sharepoint.com/sites/INTRANET2"

De acuerdo con el análisis de la respuesta de la OTI, la Oficina de Control Interno concluye que el argumento de no tener una interfaz para la captura de datos de cada dependencia no configura que no sea un Sistema de Información.

Las situaciones descritas anteriormente contravienen lo establecido en el Manual de Operaciones: MO-OST-008 Ingreso Seguro a los Sistemas de Información numeral 3 Desarrollo (…) ingreso seguro que indica*: (…) Paso 1: "Definir y elaborar el catálogo de sistemas de información que tiene como propósito identificar y conservar una lista completa y actualizada de los sistemas de información en la ADR, con el fin de identificar como es el acceso y evaluar el control".*

Tabla 5. Detalle de las Posibles causas, riesgos e impactos identificadas por la Oficina de Control Interno

Causas	Riesgos	Impactos
• Desconocimiento del objetivo planteado por la elaboración del catálogo de Sistemas de información (identificar y conservar la lista completa y actualizada, con el fin de identificar como es el acceso y evaluar su control). • Debilidades en la ejecución de los procedimientos establecidos para la Seguridad y la Privacidad de la Información. • Informalidad en la ejecución de los procedimientos de la Seguridad y la Privacidad de la Información. • Desconocimiento del Manual de Operaciones: MO-OST-008 Ingreso Seguro a los Sistemas de Información.	Posibilidad de afectación reputacional y económica por multa y sanción del ente regulador debido al incumplimiento de los criterios de control y acceso definidos en la resolución 081 de 2021.	▪ Daño de la Imagen institucional. ▪ Afectación en el cumplimiento de metas y objetivos de la Entidad. ▪ Afectación en el cumplimiento de las políticas definidas en el PETI 2023-2026.

Fuente. Elaboración propia Equipo Auditor – Oficina de Control Interno.

RECOMENDACIÓN(ES):

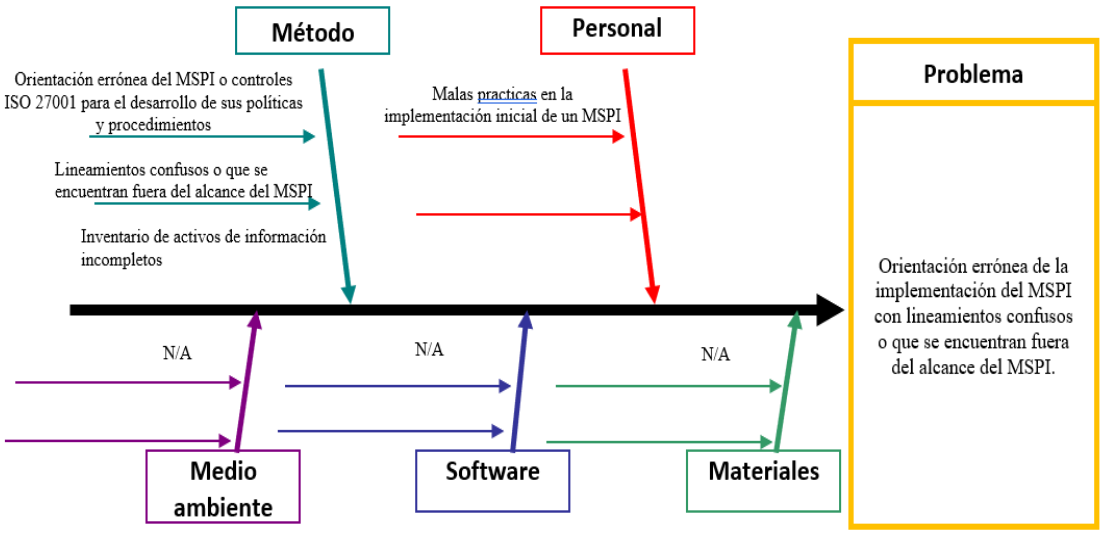
Por lo anterior la Oficina de Control Interno, hace las siguientes recomendaciones:

- Revisar los sistemas de información utilizados por las diferentes dependencias de la Entidad, actualizarlos e incluirlos en el Catálogo de los Sistemas de información de la ADR, con el fin de conservar la lista completa y actualizada, para su correspondiente evaluación y seguimiento.
- Implementar actividades de control que permitan actualizar permanentemente el Catálogo de los Sistemas de información de la ADR, para que sea un fiel reflejo de la realidad de los sistemas de información de la entidad, debido a que es un insumo de gran importancia para la generación de información que contribuye a la toma decisiones en la Entidad.

RESPUESTA DEL AUDITADO: ACEPTADO.

JUSTIFICACION: No Aplica.

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



Fuente. Respuesta Reporte de Hallazgo

PLAN DE MEJORAMIENTO:

Tabla 6. Plan de mejoramiento

Acción(es) propuesta(s)	Meta(s)	Tipo de acción	Responsable(s)	Fecha inicial	Fecha final
Solicitar la anulación de los documentos del Sistema de Gestión de Seguridad de la Información que tengan aspectos como controles o lineamientos, que no se encuentran dentro del alcance del MSPI y que la entidad actualmente no cuenta con la capacidad para implementarlos.	Solicitud de documentos anulados a la Oficina de Planeación.	Correctiva	Grupo Seguridad de la Información – Oficina Tecnología de la Información	15-ago-2023	31-dic-2023
Establecer un plan de implementación de Seguridad de la Información, orientado a las necesidades de la entidad, normatividad vigente y estándares de seguridad internacionales.	Plan Estratégico de Seguridad de la Información actualizado y vigente	Preventiva	Grupo Seguridad de la Información – Oficina Tecnología de la Información	21-jul-2023	31-dic-2023

Fuente. Respuesta Reporte de Hallazgo

CONCEPTO DE LA OFICINA DE CONTROL INTERNO: CON OBSERVACIONES.

Una vez verificadas las acciones propuestas en el plan de mejoramiento presentado, estas se consideran razonables, dado que pretenden atacar las causas de las situaciones que originaron las desviaciones identificadas, sin embargo, respecto a la acción propuesta No. 1: "***Solicitar la anulación de los documentos del Sistema de Gestión de Seguridad de la Información que tengan aspectos como controles o lineamientos, que no se encuentran dentro del alcance del MSPI y que la entidad actualmente no cuenta con la capacidad para implementarlos***", se sugiere ajustar la redacción de la siguiente manera "***Realizar la adecuación y actualización de los documentos del Sistema de Gestión de Seguridad".***
De otra parte, se insta a definir acciones preventivas para evitar que las situaciones identificadas durante la auditoría se repitan a futuro.

HALLAZGO N° 3 – Debilidades en el cumplimiento de la Política de Seguridad Digital, frente a la inactivación de los servicios tecnológicos de funcionarios desvinculados de la Entidad.

Con el fin de verificar el cumplimiento de lo establecido en la Resolución 081 de 2021 "*Por la cual se adopta la política general de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios, así como definir lineamientos frente al uso y manejo de la información de la Agencia de Desarrollo Rural*" *Artículo* Décimo Octavo *Política de Seguridad Digital,* literal d. *Del uso de los Sistemas o Herramientas de Información* numeral 4. *"En el caso de terminación del vínculo laboral de un funcionario de planta permanente o temporal la Dirección de Talento Humano, debe informar la novedad a la mesa de servicio con la resolución, para la inactivación de los servicios tecnológicos correspondiente (…)*" la Oficina de Control Interno desarrolló la siguiente evaluación:

Se solicitó a la OTI los correos/tickets de mesa de ayuda remitidos por parte de la Dirección de Talento Humano en la vigencia 2023 donde se haya notificado la finalización del vínculo laboral de los funcionarios de planta retirados durante dicha vigencia y solicitado la inactivación del usuario, así mismo, se realizó solicitud a la Dirección de Talento Humano de los correos dirigidos a la OTI (Mesa de Ayuda) para la

inactivación de usuarios retirados durante la vigencia 2023, por lo cual, la Oficina de Control Interno realizó el análisis y la verificación de la información donde se identificó la siguiente situación:

- Se evidenció que durante el periodo solicitado se retiraron diecisiete (17) funcionarios de la Entidad, de los cuales cinco (5) de ellos fueron inactivados en días posteriores a los definidos en los actos administrativos por medio de los cuales se les acepto la renuncia, como se detalla a continuación:

Tabla 7. Resultados revisión Oficina de Control Interno

Resolución	Fecha de renuncia	Inactivación
476	22-ago-22	3-feb-23
064	13-feb-23	14-feb-23
119	9-mar-23	10-mar-23
161	10-abr-23	18-abr-23
224	22-may-23	23-may-23

Elaboración propia Equipo Auditor. Fuente: Dirección de Talento Humano y Oficina de Tecnologías de la Información

Las situaciones descritas anteriormente contravienen los criterios establecidos en:

- **Resolución 081 de 2021** "*Por la cual se adopta la política general de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios, así como definir lineamientos frente al uso y manejo de la información de la Agencia de Desarrollo Rural*" *Artículo* Décimo Octavo *Política de Seguridad Digital.* , literal d. *Del uso de los Sistemas o Herramientas de Información* numeral 4. *"En el caso de terminación del vínculo laboral de un funcionario de planta permanente o temporal la Dirección de Talento Humano, debe informar la novedad a la mesa de servicio con la resolución, para la inactivación de los servicios tecnológicos correspondiente (…)*".

- **MO-ETI- 001 Manual con las Políticas de Seguridad y Privacidad de la Información** Numeral 3.1.5 Política de Control de Acceso, literal f: "*En el caso de terminación del vínculo laboral de un funcionario de planta permanente o temporal la Dirección de Talento Humano, debe informar la novedad a la mesa de servicio con la resolución, para la inactivación de los servicios tecnológicos correspondientes, con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración o uso indebido, así como a la suplantación de identidad".*

POSIBLE(S) CAUSA(S) IDENTIFICADA(S) DESCRIPCIÓN DE LOS RIESGOS E IMPACTOS

Tabla 8. Detalle de las Posibles causas, riesgos e impactos identificadas por la Oficina de Control Interno

Causas	Riesgos	Impactos
▪ Desconocimiento de los lineamientos establecidos en la resolución No. 081 de 2021 ▪ Debilidad en la aplicación de los lineamientos establecidos de la Seguridad y la Privacidad de la información de la Resolución No. 081 de 2021. ▪ Debilidades en la ejecución de los procedimientos establecidos para la Seguridad y la Privacidad de la Información. ▪ Informalidad en la ejecución de los procedimientos de la Seguridad y la Privacidad de la Información.	Posibilidad de afectación reputacional y económica por multa y sanción del ente regulador debido al incumplimiento de los criterios de control y acceso definidos en la resolución 081 de 2021	▪ Daño de la Imagen institucional. ▪ Afectación en el cumplimiento de metas y objetivos de la Entidad. ▪ Dependencia Tecnológica de la ADR ▪ Afectación económica por demandas en el cumplimiento de las políticas de tratamiento de datos personales.

Fuente. Elaboración propia Equipo Auditor – Oficina de Control Interno.

RECOMENDACIÓN(ES):

Por lo anterior la Oficina de Control Interno, hace las siguientes recomendaciones:

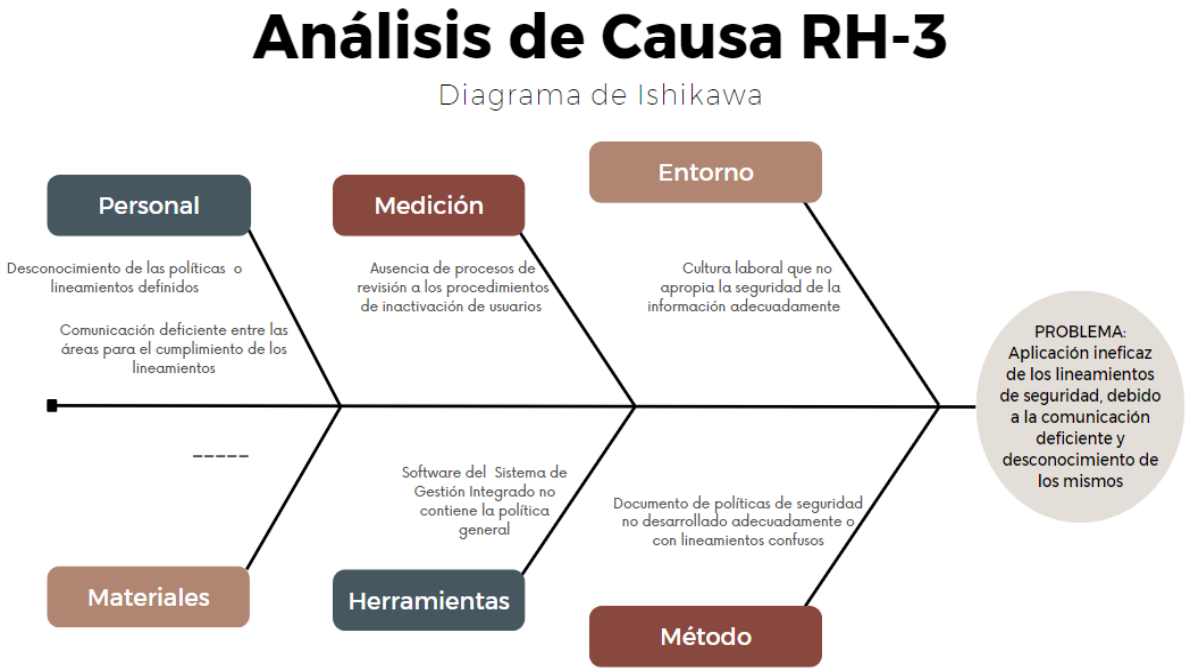
- Solicitar a la Dirección de Talento Humano notificar oportunamente los retiros de funcionarios teniendo en cuenta lo establecido en la Resolución 081 de 2021.
- Socializar y recordar los lineamientos descritos en la Resolución No. 081 de 2021 ya que, en dicha resolución, se adopta el Modelo de Seguridad y Privacidad de la información de la ADR, y este se convierte en obligatorio cumplimiento.
- Hacer campañas de socialización de la Resolución No. 081 de 2021, al interior de la Entidad.

- Socializar los manuales, procedimientos, protocolos, guías, instructivos y demás documentación publicada en la plataforma ISOLUCION, en materia de la Seguridad y la Privacidad de la información.

RESPUESTA DEL AUDITADO: ACEPTADO.

JUSTIFICACION:
Respecto al hallazgo reportado, pedimos comedidamente sea extendido a la Oficina de Talento Humano, ya que la Oficina de Tecnología de la Información depende de un reporte oportuno, para poder realizar la inactivación correspondiente con celeridad.

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



Fuente. Respuesta Reporte de Hallazgo

PLAN DE MEJORAMIENTO:

Tabla 9. Plan de mejoramiento

Acción(es) propuesta(s)	Meta(s)	Tipo de acción	Responsable(s)	Fecha inicial	Fecha final
Solicitar la derogación de la resolución 081 de 2021.	Política del Sistema de Gestión de Seguridad de la Información y Manual de políticas de Seguridad de la Información para el buen uso de los activos de información claros, accesibles y que sean de fácil interpretación.	Correctiva	Grupo Seguridad de la Información – Oficina Tecnología de la Información	25-jul-2023	31-dic-2023
Generar nuevos documentos, Política del Sistema de Gestión de Seguridad de la Información y Manual de políticas de Seguridad de la Información para el buen uso de los activos de información donde se definan claramente los roles y responsabilidades de las áreas de la ADR en materia de seguridad de la información.	Política del Sistema de Gestión de Seguridad de la Información y Manual de políticas de Seguridad de la Información para el buen uso de los activos de información claros, accesibles y que sean de fácil interpretación		Grupo Seguridad de la Información – Oficina Tecnología de la Información	25-jul-2023	31-dic-2023
Socializar las políticas de seguridad de la información a todas las áreas involucradas de manera directa en el funcionamiento del SGSI.	Lineamientos plenamente comunicados a todas las áreas que tienen responsabilidades clave en la implementacióndel SGSI	Preventiva	Grupo Seguridad de la Información – Oficina Tecnología de la Información	25-jul-2023	31-dic-2023

Fuente. Respuesta Reporte de Hallazgo

CONCEPTO DE LA OFICINA DE CONTROL INTERNO: ACEPTADO.

La Oficina de Control Interno considera que las acciones propuestas en el plan de mejoramiento presentado son razonables, dado que pretenden atacar las causas de las situaciones que originaron las desviaciones identificadas, sin embargo, se insta a definir acciones preventivas para evitar que las situaciones identificadas durante la auditoría se repitan a futuro.

HALLAZGO N° 4 – Incumplimiento de la gestión de vulnerabilidades identificadas de acuerdo con el Manual de Operaciones: MO-OST-003 Guía de aseguramiento de Servicios en la Red

Con el fin de evaluar la efectividad de los controles para la gestión de vulnerabilidades tecnológicas definidos en el Manual de Operaciones: MO-OST-003 Guía de aseguramiento de Servicios en la Red, que indica en el numeral 3 Desarrollo, Pasos de Aseguramiento, Paso N. 1. *Identificar las vulnerabilidades en equipos activos de red* (…) Paso N. 2. *Analizar de vulnerabilidades (…)",* la Oficina de Control Interno mediante correo electrónico solicitó a la OTI la información relacionada con la realización de pruebas de vulnerabilidades de las plataformas ON PREMISE y CLOUD para la vigencia 2023, así:

- Herramienta utilizada para la realización de las pruebas de vulnerabilidades.
- Resultados obtenidos en el escaneo por la herramienta utilizada.
- Informe técnico donde se documentan las vulnerabilidades identificadas, su nivel de clasificación, la acción para remediar la vulnerabilidad, los tiempos recomendados de remediación y demás información pertinente técnica necesaria para entender los resultados y su remediación.

Como respuesta la OTI señaló:

"Herramienta utilizada para la realización de las pruebas de vulnerabilidades:
La herramienta utilizada para el análisis de vulnerabilidades de las Plataformas Tecnológicas ON PREMISE y CLOUD de la ADR es "Tenable Web Application Scanner (WAS)" Resultados obtenidos en el escaneo por la herramienta utilizada, de acuerdo con la información recibida, se están ejecutando Escaneos de Vulnerabilidades con la herramienta: Tenable Web Application Scanner (WAS), desde el 06 de febrero de 2023"

Se realizaron escaneos de vulnerabilidades de los sistemas:

Tabla 10. Relación de Escaneos de vulnerabilidades de sistemas de la ADR

Aplicaciones	Fecha
Aplicación UTP	Febrero 06 2023
Nuevo ORFEO Ambiente QA	Marzo 21 2023
Portal Perfil de Proyectos	Marzo 25 2023
Perfil Proyectos LOGIN	Marzo 25 2023
Gestión Proyectos	Abril 11 2023
Log4Shell - Azure	Abril 11 2023
Arcgis	Abril 18 2023
Masora 2	Abril 11 2023
Perfil Proyectos	Abril 11 2023
Banco de Proyectos	Abril 11 2023
Pagina ADR	Abril 11 2023
Campus Virtual	Abril 18 2023
Masora	Abril 11 2023
Perfil Proyectos Desarrollo	Abril 11 2023
ULISES	Abril 11 2023
PQRS	Abril 11 2023
KLICK	Abril 11 2023
ISOLUCION	Abril 11 2023
Perfil Proyectos	Junio 13 2023
KLICK	Junio 13 2023

Elaboración propia Equipo Auditor. Fuente: Oficina de Tecnologías de la Información

No obstante, la Oficina de Tecnologías de Información – OTI no presentó un informe técnico donde se documenten las vulnerabilidades identificadas, la acción para remediar la vulnerabilidad, los tiempos recomendados y demás información pertinente técnica necesaria para entender los resultados y su remediación, de acuerdo con lo anterior, si bien se evidenció la realización de escaneo técnico de vulnerabilidades, no se gestionaron las vulnerabilidades identificadas, situación que contraviene lo establecido en:

- **Norma ISO/IEC 27001:2013: A.12.6 Gestión de vulnerabilidades Técnicas** *"¿Se obtiene información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso? ¿**Se evalúa la exposición de la organización a dichas vulnerabilidades y se toman las acciones apropiadas*

para tratar los riesgos asociados, tales como instalación y pruebas de actualizaciones de seguridad*?"* Negrita fuera de texto.

- **Manual de Operaciones MO-OST-003 Guía de Aseguramiento de Servicios en la Red** Numeral 3 Desarrollo, Pasos de Aseguramiento, Paso N. 1. *Identificar las vulnerabilidades en equipos activos de red* (…) Paso N. 2 *Analizar de vulnerabilidades (…)", Paso 2: Analizar vulnerabilidades (…) Paso 5: Análisis de vulnerabilidades sistemas de información"*

- **Instrumento de Identificación de la línea Base de Seguridad, de MINTIC, que establece en el numeral T.4.6.1 "Gestión de Vulnerabilidades técnicas"** "*Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado, para lo cual, se deben establecer las siguientes directrices:*

  a) definir y establecer los roles y responsabilidades asociados con la gestión de la vulnerabilidad técnica, incluido el seguimiento de la vulnerabilidad, la valoración de riesgos de vulnerabilidad, la colocación de parches, el seguimiento de activos y cualquier responsabilidad de coordinación requerida;
  b) definir los recursos de información que se usarán para identificar las vulnerabilidades técnicas pertinentes y para mantener la toma de conciencia acerca de ellos se debe identificar para el software y otra tecnología;
  c) una línea de tiempo para reaccionar a las notificaciones de vulnerabilidades técnicas pertinentes potencialmente;
  d) establecer que una vez que se haya identificado una vulnerabilidad técnica potencial, la organización debería identificar los riesgos asociados y las acciones por tomar; esta acción puede involucrar la colocación de parches de sistemas vulnerables o la aplicación de otros controles; Si no es posible colocar controles se deben documentar en los riesgos de acuerdo a su probabilidad e impacto y colocarlo como riesgo aceptado.
  e) definir dependiendo de la urgencia con la que se necesite tratar una vulnerabilidad técnica, la acción tomada se debería llevar a cabo de acuerdo

con los controles relacionados con la gestión de cambios, o siguiendo los procedimientos de respuesta a incidentes de seguridad de la información;

f*) establecer, si está disponible un parche de una fuente legítima, se debe valorar los riesgos asociados con la instalación del parche (los riesgos que acarrea la vulnerabilidad se debe comparar con el riesgo de instalar el parche);*

g) establecer que los parches se deben probar y evaluar antes de su instalación, para asegurarse de que son eficaces y no producen efectos secundarios que no se puedan tolerar; si no hay parches disponibles, se debe considerar otros controles como:

1) dejar de operar los servicios o capacidades relacionados con la vulnerabilidad;

12) adaptar o adicionar controles de acceso, (cortafuegos, en los límites de la red);

3) incrementar el seguimiento para detectar ataques reales;

4) tomar conciencia sobre la vulnerabilidad;

h) llevar un log de auditoría para todos los procedimientos realizados;

i) hacer seguimiento y evaluación regulares del proceso de gestión de vulnerabilidad técnica, con el fin de asegurar su eficacia y eficiencia;

j) abordar primero los sistemas que están en alto riesgo;

k) establecer un proceso de gestión eficaz de la vulnerabilidad técnica alineada con las actividades de gestión de incidentes para comunicar los datos sobre vulnerabilidades a la función de respuesta a incidentes y suministrar los procedimientos técnicos para realizarse si llegara a ocurrir un incidente;

***l) definir un procedimiento para hacer frente a una situación en la que se ha identificado una vulnerabilidad, pero no hay una contramedida adecuada. En esta situación, la organización debería evaluar los riesgos relacionados con la vulnerabilidad conocida y definir las acciones de detección y correctivas apropiadas**.” Negrita fuera de Texto.*

POSIBLE(S) CAUSA(S) IDENTIFICADA(S) DESCRIPCIÓN DE LOS RIESGOS E IMPACTOS

Tabla 11. Detalle de las Posibles causas, riesgos e impactos identificadas por la Oficina de Control Interno

Causas	Riesgos	Impactos
▪ Desconocimiento de los criterios establecidos en el Manual de Operaciones MO-OST-003 Guía de Aseguramiento de Servicios en la Red. ▪ Desconocimiento de los controles establecidos en la Norma ISO/IEC 27001:2013: Literal A.12.2: Gestión de Vulnerabilidades Técnicas. ▪ Desconocimiento de los controles establecidos en el Instrumento de Identificación de la línea Base de Seguridad", de MINTIC, en el numeral T.4.6.1 "Gestión de Vulnerabilidades técnicas".	Posibilidad de afectación reputacional y económica por multa y sanción del ente regulador debido al incumplimiento de política de seguridad de las telecomunicaciones definida en la resolución 81 de 2021.	▪ Daño de la Imagen institucional. ▪ Afectación en el cumplimiento de metas y objetivos de la Entidad. ▪ Afectación en el cumplimiento de las políticas definidas en el PETI 2023-2026.

Fuente. Elaboración propia Equipo Auditor – Oficina de Control Interno.

RECOMENDACIÓN(ES):

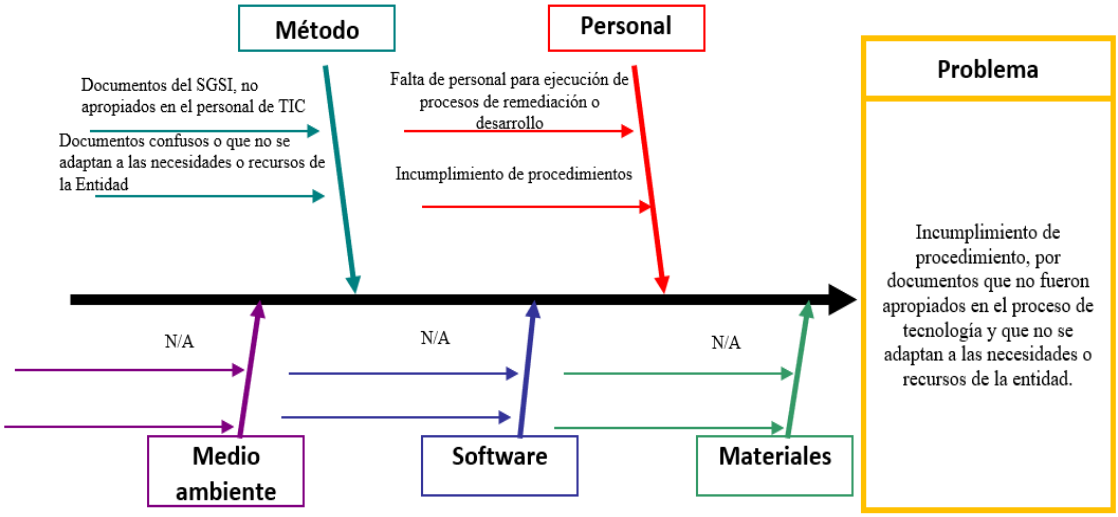
Por lo anterior la Oficina de Control Interno, hace las siguientes recomendaciones:

- Realizar gestión de pruebas de vulnerabilidades, Informes técnicos donde se documenten las vulnerabilidades identificadas, su nivel de clasificación, la acción para remediar la vulnerabilidad, los tiempos recomendados de remediación y demás información pertinente técnica necesaria para su remediación.
- Realizar escaneos continuos a la plataforma de TI de la ADR, realizar planes para remediar estas brechas de seguridad y verificar que hayan sido efectivas.
- Realizar campañas de sensibilización en temas de la seguridad y la privacidad de la información, a todos los usuarios de la ADR.
- Realizar actividades de Hackeo Ético, con el objetivo de identificar y corregir posibles vulnerabilidades.

RESPUESTA DEL AUDITADO: ACEPTADO.

JUSTIFICACIÓN: No Aplica.

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



Fuente: Respuesta Reporte de Hallazgos

PLAN DE MEJORAMIENTO:

Tabla 12. Plan de mejoramiento

Acción(es) propuesta(s)	Meta(s)	Tipo de acción	Responsable(s)	Fecha inicial	Fecha final
Generación de nuevo procedimiento gestión de vulnerabilidades técnicas adaptado a las necesidades y recursos existentes de la entidad y con enfoque a análisis de activos de hardware y software.	Borrador procedimiento y manual de gestión de vulnerabilidades técnicas.	Correctiva	Grupo de Seguridad de la Información de la Oficina de tecnología	24-jul-2023	31-jul-2023
Generación de plan de gestión de vulnerabilidades técnicas del SGSI para la vigencia 2023	Plan de gestión de Vulnerabilidades técnicas	Correctiva	Grupo de Seguridad de la Información de la Oficina de tecnología	24-jul-2023	31-jul-2023
Ejecutar plan de gestión de vulnerabilidades técnicas del SGSI para la vigencia 2023	Informes de Gestión de Vulnerabilidades Informes de Remediación	Correctiva	Oficina de Tecnología de la Información	24-jul-2023	31-dic-2023

Acción(es) propuesta(s)	Meta(s)	Tipo de acción	Responsable(s)	Fecha inicial	Fecha final
Solicitar la liberación del documento en el SGI a la Oficina de Planeación.	Solicitud de liberación de documento en el SGI	Preventiva	Oficina de Tecnología de la Información	24-jul-2023	31-dic-2023
Realizar la apropiación del documento gestión de vulnerabilidades técnicas al personal de la Oficina de Tecnología.	Acta de socialización del documento gestión de vulnerabilidades técnicas	Preventiva	Oficina de Tecnología de la Información	24-jul-2023	31-dic-2023

Fuente. Respuesta Reporte de Hallazgo

CONCEPTO DE LA OFICINA DE CONTROL INTERNO: CON OBSERVACIONES.

La Oficina de Control Interno acepta el plan de mejoramiento planteado, sin embargo, recomienda ajustar la meta de la acción propuesta No. 1 indicando que sea la versión revisada y aprobada del procedimiento y manual de gestión de vulnerabilidades técnicas y no el borrador, frente a la acción propuesta No. 2: *"Generación de plan de gestión de vulnerabilidades técnicas del SGSI para la vigencia 2023",* es importante tener en cuenta que en dicho plan se establezcan todas las actividades a tener en cuenta para remediar dicha vulnerabilidad, los tiempos recomendados de remediación, los costos en recurso humano y monetarios y demás información pertinente técnica necesaria para entender las vulnerabilidades y su remediación.

Este plan de gestión de vulnerabilidades debe ser conocido por todos los directivos de la Entidad, para que ellos sean conscientes de las vulnerabilidades de las plataformas tecnológicas de la Entidad.

HALLAZGO N° 5 - Asignación de calificación no congruente con las evidencias obtenidas en la fase de Diagnóstico MSPI

Con el fin de verificar el estado de avance de la evaluación de la efectividad de los controles del Autodiagnóstico de la implementación del MSPI, con la herramienta: *"Instrumento de identificación de la línea Base de Seguridad",* proveído por el Ministerio de las Tecnologías de la información y las Comunicaciones, la Oficina de Control Interno solicitó a la OTI, la información utilizada y el documento diligenciado para la evaluación

realizada en el momento de hacer el autodiagnóstico, donde se evidenció la revisión de los catorce (14) dominios de implementación del MSPI:

- A.5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN
- A6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
- A.7. SEGURIDAD DE LOS RECURSOS HUMANOS
- A.8. GESTIÓN DE ACTIVOS
- A.9. CONTROL DE ACCESO
- A.10. CRIPTOGRAFÍA
- A.11. SEGURIDAD FÍSICA Y DEL ENTORNO
- A.12. SEGURIDAD DE LAS OPERACIONES
- A.13. SEGURIDAD DE LAS COMUNICACIONES
- A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS
- A.15. RELACIONES CON LOS PROVEEDORES
- A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
- A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO
- A.18. CUMPLIMIENTO

Evaluada la información recibida se verificó que el puntaje asignado fuera congruente con las evidencias suministradas, de lo cual se obtuvo el siguiente resultado:

ADMINISTRATIVAS

Tabla 13. Autodiagnóstico de la implementación del MSPI

Control	Puntaje OTI	Puntaje OCI	Diferencia
AD.1.1	60	60	0
AD.1.2	40	40	0
AD.2.1.1	20	20	0
AD.2.1.2	0	0	0
AD.2.1.3	20	20	0
AD.2.1.4	20	20	0
AD.2.1.5	0	0	0
AD.2.2.1	20	20	0
AD.2.2.2	0	0	0
AD.3.1.1	**80**	**40**	**40**
AD.3.1.2	40	40	0
AD.3.2.1	20	20	0
AD.3.2.2	**40**	**20**	**20**
AD.3.2.3	20	20	0
AD.5.1.3	80	80	0

Control	Puntaje OTI	Puntaje OCI	Diferencia
AD.4.1.1	40	20	20
AD.4.1.2	40	20	20
AD.4.1.4	40	40	0
AD.4.2.1	80	20	60
AD.4.2.2	60	60	0
AD.4.2.3	60	60	0
AD.4.3.1	0	0	0
AD.4.3.2	0	0	0
AD.4.3.3	0	0	0
AD.5.1.1	20	20	0
AD.5.1.2	0	0	0
AD.5.1.3	0	0	0
AD.5.2.1	0	0	0
AD.6.1.1	60	60	0
AD.6.1.2	40	40	0
AD.6.1.3	80	80	0
AD.6.1.4	20	20	0
AD.6.2.1	60	60	0
AD.6.2.2	40	40	0
AD.6.2.3	0	0	0
AD.7.1	0	0	0
AD.7.2	40	40	0

Elaboración propia Equipo Auditor. Fuente: Oficina de Tecnologías de la Información

TÉCNICAS

Tabla 14. Autodiagnóstico de la implementación del MSPI

Controles	Puntaje OTI	Puntaje OCI	Diferencia
T.1.1.1	40	40	0
T.1.1.2	40	40	0
T.1.2.1	60	60	0
T.1.2.2	40	40	0
T.1.2.3	20	20	0
T.1.2.4	80	80	0
T.1.2.5	40	40	0
T.1.2.6	60	60	0
T.1.3.1	80	80	0
T.1.4.1	40	40	0
T.1.4.2	80	80	0
T.1.4.3	60	60	0
T.1.4.4	40	40	0
T.1.4.5	20	20	0
T.2.1.1	0	0	0
T.2.1.2	20	20	0
T.3.1.1	80	80	0
T.3.1.2	40	40	0
T.3.1.3	80	80	0
T.3.1.4	80	80	0
T.3.1.5	20	20	0
T.3.1.6	80	80	0
T.3.2.1	80	80	0
T.3.2.2	20	20	0
T.3.2.3	40	40	0

Controles	Puntaje OTI	Puntaje OCI	Diferencia
T.3.2.4	40	40	0
T.3.2.5	80	80	0
T.3.2.6	40	40	0
T.3.2.7	20	20	0
T.3.2.8	40	40	0
T.3.2.9	40	40	0
T.4.1.1	40	20	20
T.4.1.2	40	20	20
T.4.1.3	40	20	20
T.4.1.4	40	20	20
T.4.2.1	60	20	40
T.4.3.1	20	20	0
T.4.4.1	20	20	0
T.4.4.2	20	20	0
T.4.4.3	20	20	0
T.4.4.4	80	80	0
T.4.5.1	20	20	0
T.4.6.1	20	20	0
T.4.6.2	80	80	0
T.4.7.1	20	20	0
T.5.1.1	20	20	0
T.5.1.2	20	20	0
T.5.1.3	20	20	0
T.5.2.1	20	20	0
T.5.2.2	20	20	0
T.5.2.3	80	80	0
T.5.2.4	80	80	0
T.6.1.1	20	20	0
T.6.1.2	60	60	0
T.6.1.3	40	40	0
T.6.2.1	40	20	20
T.6.2.2	40	20	20
T.6.2.3	40	20	20
T.6.2.4	40	20	20
T.6.2.5	40	20	20
T.6.2.6	40	20	20
T.6.2.7	60	60	0
T.6.2.8	40	20	20
T.6.2.9	40	20	20
T.6.3.1	0	0	0
T.7.1.1	20	20	0
T.7.1.2	20	20	0
T.7.1.3	20	20	0
T.7.1.4	20	20	0
T.7.1.5	40	20	20
T.7.1.6	40	20	20
T.7.1.7	20	20	0

Elaboración propia Equipo Auditor. Fuente: Oficina de Tecnologías de la Información

Teniendo en cuenta lo anteriormente expuesto, se evidenció que en el proceso de autodiagnóstico para la identificación de brechas de implementación del Modelo de Seguridad y Privacidad de la Información- MSPI, la información recopilada para

sustentar la calificación dada por la OTI en cinco (5) controles asociados al tema administrativo y quince (15) controles asociados al tema técnico no es congruente con la realidad de las evidencias de acuerdo con la escala definida por el MINTIC, situación que no refleja objetivamente la implementación del MSPI en la Entidad.

Tabla 15. Detalle de las Posibles causas, riesgos e impactos identificadas por la Oficina de Control Interno

Causas	Riesgos	Impactos
• Desconocimiento de la documentación que en materia de la Seguridad y la Privacidad de la información se tiene publicada en ISOLUCION. • Desconocimiento de la implementación que se tiene al interior de la OTI, de la documentación que se tiene, en materiade la Seguridad y la Privacidad de la información. • Desconocimiento de la escala de valoración del Instrumento de identificación de la línea Base de Seguridad.	Posibilidad de afectación reputacional y económica por multa y sanción del ente regulador debido al incumplimiento de la política general de seguridad y privacidad de la información y sus objetivos, dada una operación inadecuada del MSPI en una de sus cinco fases (diagnóstico, planificación, operación, evaluación del desempeño, mejoramiento continuo).	▪ Daño de la Imagen institucional. ▪ Afectación en el cumplimiento de metas y objetivos de la Entidad. ▪ Afectación en el cumplimiento de las políticas definidas en el PETI 2023-2026.

Fuente. Elaboración propia Equipo Auditor – Oficina de Control Interno.

RECOMENDACIÓN(ES):

Teniendo en cuenta las situaciones identificadas la Oficina de Control Interno insta a seguir las siguientes recomendaciones.

- **Control de MinTic**: Se deben identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.
  Recomendación: Realizar ajuste del formato de identificación de archivos de acuerdo con las características definidas en el instructivo IN-GTI-001.

- **Control de MinTic**: Los activos mantenidos en el inventario deben tener un propietario.
  Recomendación: Establecer en el marco de las políticas de seguridad de la información los lineamientos para el etiquetado de los activos de información.

- **Control de MinTic**: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
  Recomendación: Determinar el por qué no se aplica los lineamientos en la actual lista de activos de información, plantear actividades que corrijan esta causa y desarrollarla con prioridad dada la criticidad de esta.

- **Control de MinTic:** Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
  Recomendación: Realizar un análisis de los factores de verificación adicional que la Agencia requiera en el marco de su información confidencial tales como estudios de seguridad, polígrafo, visitas domiciliarias, etc.

- **Control de MinTic**: Todos los empleados de la Entidad, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
  Recomendación: Establecer actividades de capacitación e inducción en los procesos de contratación y de Talento Humano, con evaluación de estas.

- **Control de MinTic**: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten
  Recomendación: Ejercer un proceso de reingeniería de los procesos y procedimientos asociados al Modelo de Seguridad y Privacidad de la Información, y que su socialización sea realizada en los procesos de inducción.

- **Control de MinTic**: Se debe controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información**.**
  Recomendación: Revisar el procedimiento de gestión de cambios y adaptarlo a la normatividad y recomendaciones de MinTic, de igual forma definir los responsables de su aplicación.

- **Control de MinTic**: Se cuenta con documentos para gestión de la capacidad, pero los mismos no fueron apropiados por lo cual no son cumplidos por el personal
  Recomendación: Realizar un análisis del procedimiento de gestión de demanda de capacidad, actualizarlo y definir los recursos para poder ejecutarlo adecuadamente.

- **Control de MinTic**: Se debe separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
  Recomendación: Definir los recursos necesarios para contar con la infraestructura adecuada de acuerdo con las necesidades de la Agencia, incluirlo en el PETI como actividad crítica para la sistematización y logro de un Gobierno Digital.

- **Control de MinTic**: Se debe implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
  Recomendaciones: Instalar y actualizar software de detección y reparación del software malicioso en los computadores y medios como una medida de control, en forma rutinaria; el análisis realizado debe incluir:
  - Analizar cualquier archivo recibido por la red o por cualquier forma de medio de almacenamiento, para detectar el software malicioso, antes de uso.
  - Analizar los adjuntos y descargas de los correos electrónicos, para determinación del software malicioso antes de uso; este análisis se debería llevar a cabo en diferentes lugares, (los servidores de los correos electrónicos, en los computadores de escritorio) y cuando se ingresa a la red de la organización; el análisis de páginas web, para determinar el software malicioso.
  - Definir procedimientos y responsabilidades relacionadas con la protección contra el software malicioso en los sistemas, formación acerca del uso de dichos procedimientos, reporte y recuperación de ataques de software malicioso.
  - Preparar planes de continuidad del negocio apropiado, para la recuperación de ataques de software malicioso, incluidos todos los datos necesarios, copias de respaldo del software y disposiciones para recuperación.

- Implementar procedimientos para verificar información relacionada con el software malicioso, y asegurarse de que los boletines de advertencia sean exactos e informativos.

- **Control de MinTic**: Se debe establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización. **Recomendaciones:** Revisar las siguientes directrices política de desarrollo de Software:
  - Definir la seguridad del ambiente de desarrollo.
  - Orientar la seguridad en el ciclo de vida de desarrollo del software.
  - Definir la seguridad en la metodología de desarrollo de software.
  - Establecer las directrices de codificación seguras para cada lenguaje de programación usado.
  - Definir los requisitos de seguridad en la fase diseño.
  - Definir los puntos de chequeo de seguridad dentro de los hitos del proyecto.
  - Establecer los depósitos seguros.
  - Definir la seguridad en el control de la versión.
  - Establecer el conocimiento requerido sobre seguridad de la aplicación.
  - Definir la capacidad de los desarrolladores para evitar, encontrar y resolver las vulnerabilidades.

- **Control de MinTic**: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización
  Recomendaciones: Revisar las siguientes directrices revisión técnica de las aplicaciones después de cambios en la plataforma de operación:
  - Revisar los procedimientos de integridad y control de aplicaciones para asegurar que no estén comprometidos debido a los cambios en las plataformas de operaciones.
  - Asegurar que la notificación de los cambios en la plataforma operativa se hace a tiempo para permitir las pruebas y revisiones apropiadas antes de la implementación.
  - Asegurar que se hacen cambios apropiados en los planes de continuidad del negocio.

- **Control de MinTic**: Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.

  Recomendaciones: Revisar las siguientes directrices restricciones en los cambios a los paquetes de software:

  - Definir el riesgo de que los procesos de integridad y los controles incluidos se vean comprometidos.
  - Obtener el consentimiento del proveedor del Sistema de Información.
  - Obtener del proveedor los cambios requeridos, a medida que se actualiza el programa estándar.
  - Evaluar el impacto, si la Agencia de Desarrollo Rural, llega a ser responsable del soporte y mantenimiento futuro del software como resultado de los cambios.

- **Control de MinTic**: Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información

  Recomendación: Implementar el Manual de Operación: MO-OST-009 Guía de Desarrollo Seguro, haciendo énfasis en las siguientes etapas definidas en la presente guía:

  - Verificar Normas de Seguridad Generales de Desarrollo Seguro
  - Verificar Normas de Seguridad para la Gestión de Vulnerabilidades
  - Verificar Normas de Seguridad para la Documentación del Software
  - Verificar Normas de Seguridad para Proyectos de Desarrollo
  - Verificar Normas de Seguridad para la Especificación Detallada de Requerimientos
  - Verificar Normas de Seguridad para el Diseño del Sistema
  - Verificar Normas de Seguridad para el Diseño del Sistema
  - Verificar Normas de Seguridad para la Codificación y Pruebas

- **Control de MinTic**: Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistema

Recomendación: Revisar las siguientes directrices para ambiente de desarrollo seguro:

- Definir los requisitos externos e internos aplicables, (reglamentaciones o políticas).
- Definir los controles de seguridad ya implementados por la Agencia de Desarrollo Rural, que brindan soportar al desarrollo del sistema.
- Definir la necesidad de separación entre diferentes ambientes de desarrollo.
- Definir el control de acceso al ambiente de desarrollo.
- Establecer el seguimiento de los cambios en el ambiente y en los códigos almacenados.
- Definir que las copias de respaldo se almacenan en lugares seguros fuera del sitio, o en la Plataforma CLOUD.
- Definir el control sobre el movimiento de datos desde y hacia el ambiente.

- **Control de MinTic**: Durante el desarrollo se debe llevar a cabo pruebas de funcionalidad de la seguridad.
  Recomendación: Verificar en una muestra obtenida, que para pasar al ambiente de producción, los desarrollos se les realizan pruebas de seguridad. También verificar que los procesos de detección de incidentes a la Seguridad y la Privacidad de la información son probados periódicamente.

- **Control de MinTic**: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se debe establecer programas de prueba para aceptación y criterios de aceptación relacionados
  Recomendación: Revisar las pruebas de aceptación de sistemas, para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.

- **Control de MinTic**: Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados
  Recomendación: Implementar el Procedimiento: PR-OST-007 Gestión de Incidentes y Requerimiento Tecnológicos, dando énfasis en las siguientes etapas definidas en el procedimiento:
  - Solicitar servicio de Gestión de Incidentes y Requerimiento Tecnológicos

- Recibir la solicitud Gestión de Incidentes y Requerimiento Tecnológicos
- Evaluar viabilidad Gestión de Incidentes y Requerimiento Tecnológicos
- Atender Incidente o Requerimiento
- Cerrar el incidente o requerimiento
- Realizar seguimiento a incidentes y requerimientos

- **Control de MinTic**: S El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros

  Recomendación: Entender cuál fue el impacto del incidente de la Seguridad de la Información presentado. Las lecciones aprendidas deben ser usadas para actualizar los planes de respuesta a los incidentes de Seguridad de la Información, ya que La Entidad aprende continuamente sobre los incidentes de seguridad presentados.

RESPUESTA DEL AUDITADO: NO ACEPTADO.

JUSTIFICACIÓN:

"Este hallazgo en particular la oficina no lo acepta, teniendo en cuenta que los criterios de evaluación de los controles son subjetivos, si bien existen criterios y escalas para la evaluación, estas están sujetas a interpretaciones por parte de quien lo diligencia, adicionalmente, en las brechas están todas las actividades pendientes por ejecutar respecto a cada control, de este modo no se desconocen las falencias existentes. Por lo que este hallazgo no es aceptado por la oficina de tecnologías de la información".

CONCEPTO DE LA OFICINA DE CONTROL INTERNO: CON OBSERVACIONES

La Oficina de Control Interno no comparte la justificación de la Oficina de Tecnologías de la Información debido a:

1. No se presentó información o evidencia que desvirtúen las situaciones identificadas.
2. Cada nivel de la escala utilizada para evaluar los controles contiene las características únicas que permiten determinar la valoración dada, eliminando la subjetividad relacionada.
3. La escala está definida por la norma ISO 27001:2013, la cual es utilizada por el Instrumento de identificación de la línea base de seguridad: Autodiagnóstico.

Tabla14. Escala de Valoración de Controles

Descripción	Calificación	Criterio
No Aplica	N/A	No aplica.
Inexistente	0	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados, pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Fuente: ISO 27001:2013 ANEXO A

HALLAZGO N°6 – Incumplimiento de política de control de acceso por no actualización de contraseñas de cuentas genéricas

Con el fin de verificar el cumplimiento de lo establecido en el MO-ETI- 001 Manual con las Políticas de Seguridad y Privacidad de la Información, numeral 3 *Política de Seguridad y Privacidad de la Información Política de Tratamiento de Protección de Datos (…) Control de acceso a sistemas y aplicaciones literal b) Con el fin de controlar el acceso no autorizado a sistemas y aplicaciones, las contraseñas de cuentas de administración genéricas deben ser cambiadas cada vez cada vez que expiren el tiempo de acceso concedido a un funcionario, exfuncionario, contratista y/o proveedor y diligenciar los registro para cambios de contraseñas de administrador destinado para esta actividad(…)"* la Oficina de Control Interno solicitó a la OTI evidencias del uso y actualización de cuentas genéricas en el directorio activo presentando la última fecha de actualización, evidenciando lo siguiente:

Tabla 16. Relación actualización cuentas genéricas

Display Name	SAM Account Name	Days since password last set
Access Point Manager	apmanager	819
AD Connect	AdminADConnect	278
ad sync	adsync	2366
Admin Office 365	office365	631
Administración BP	bp_sp_admin2016	160
Administración BP Pruebas	pr_bp_sp_admin2016	727
Administrador de dominio	Administrador	234
admt migración	Admt	2298
Antivirus ADR	antivirus	224
aprobador migración	migracion.aprobador	79
Aranda Software	aranda	1342
arcgis arcgis	arcgis	2155
autorizador migración	migracion.autorizado	79
Banco de Proyectos	banco.proyectos	133
Banco de Proyectos	ftp.bancoproyectos	1764
Banco de Proyectos Pruebas	banco.proyectospru	986
Bases de datos BP	bp_sp_sql_admin2016	727
Bases de datos BP Pruebas	pr_bp_sp_sql_adm2016	727
bp.Crawl	bp.Crawl	1370
bp.DistributedCache	bp.DistributedCache	1370
bp.SD	bp.SD	1370
bp.Search	bp.Search	1370
bp.ServiceApp	bp.ServiceApp	1370
Centir ADR	centiradr	1647
CGN Aplicaciones	cgn.aplicaciones	1090
Cofinancia Migracion	migra.cofinancia	79
Comunicación Organización	info.organizacion	13
Contraloria General de la Nación	adrcontraloria	79
Contraloria General Nación	contraloria	1210
Correspondencia	correspondencia	76
Cuenta de acceso al contenido BP	bp_sp_busqueda2016	727
Cuenta de acceso al contenido BP Pru	pr_bp_sp_busq2016	727
Ejecucion Migracion	migra.ejecucion	79
Escaner adr	escaneradr	2221
estructuracion migración	migracion.estructura	79
estructurador migra	migra.estructurador	79
evaluacion migración	migracion.evaluacion	79
evaluador migración	migracion.evaluador	79
Fortinet 600D	fortinet	2133
Infraestructura ADR	infraestructura	1639
iniciativas migración	migracion.iniciativa	79
Instalación Cuenta de granja BP	bp_sp_granja2016	160
Instalación Cuenta de granja BP Pruebas	pr_bp_sp_granja2016	727
Integración Productiva Klic	i.productiva	78
Inventario Equipos	inventario	586
Invitado ADR	Invitado	146
Invitado And	invitado.and	727
Isolucion ADR	isolucion.adr	699
Mapa Información	mapa.informacion	232
Mesa de Servicio	mesadeservicio	637
Oficina de Comunicaciones	comunicaciones	723
Orfeo Servicio	orfeoservicio	1353

Display Name	SAM Account Name	Days since password last set
Perfil de Proyecto ADR	perfildeproyecto	1111
Perfiles de usuario	bp_sp_usprofile2016	727
Perfiles de usuario BP Pruebas	pr_bp_sp_usprof2016	727
Portal Web	portalweb	2170
Presidencia	presidencia	79
Prosperidad Social	prosperidad.social	848
Prueba OTI Seguridad Usuario de pruebas	pruebaseg	1934
Prueba Proyectos	prueba.proyectos	1640
Prueba Sidermail	prueba.sidermail	2291
Pruebas Navegación	navegación	946
Respuesta Mesa de Servicios	respuestas.mesadeserv	2072
Respuestas Orfeo	respuestasorfeo	2077
Seguimiento Migración	migra.seguimiento	79
Servicios BP	bp_sp_servicios2016	160
Servicios BP Pruebas	pr_bp_sp_serv2016	727
Shpadmin dev	Shpadmin_dev	2260
shpadmin_prod Administrador	shpadmin_prod	1801
shpapp_prod Conexion	shpapp_prod	2169
shpfarm_prod Granja	shpfarm_prod	1801
Shpsearch dev	Shpsearch_dev	2260
shpsearch_prod Busquedas	shpsearch_prod	2169
Shpweb dev	Shpweb_dev	2260
Sidermail	sidermail	2297
SPAdmin	SPAdmin	820
SPCacheadm	SPCacheadm	1911
SPCacherd	SPCacherd	1911
SPCrawl	SPCrawl	1911
SPExcel	SPExcel	1911
SPFarm	SPFarm	820
SPMySite	SPMySite	1911
SPPerfpoint	SPPerfpoint	1911
SPPool	SPPool	820
SPProfile	SPProfile	1911
SPProject	SPProject	1911
SPSearch	SPSearch	1911
SPVisio	SPVisio	1911
sqladmin_prod Engine	sqladmin_prod	2169
Sqlinstall dev	Sqlinstall_dev	2260
Super Lector BP	bp_sp_sreader2016	727
Super Lector BP Pruebas	pr_bp_sp_sreader2016	727
Super Usuario BP	bp_sp_suser2016	727
Super Usuario BP Pruebas	pr_bp_sp_suser2016	727
Supervisor Migracion	migra.supervisor	79
TempMigracion	TempMigracion	254
Tesorería	tesorería	286
Ulises reportes	ulises	1955
User Campus Virtual	usercampus	810
User Isolucion	userisolucion	756
User SGDA	Sgda	475

Elaboración propia Equipo Auditor. Fuente: Oficina de Tecnologías de la Información

A partir del análisis y revisión de la información, se encontraron debilidades en la ejecución del control debido a:

- En promedio las cuentas genéricas realizan actualización de contraseña cada 1078 días.
- La cuenta con mayor tiempo sin actualización de contraseña es SAM Account Name con 2366 días
- Del registro No. 39 del archivo enviado por la OTI, correspondiente a la cuenta: "Fortinet 600D" del listado de Cuentas genéricas, la contraseña no ha sido actualizada desde hace 2133 días y por la cual pueden haber pasado varios administradores del Firewall. Este dispositivo que esta de cara a Internet, si no se tienen ciertos controles establecidos, el administrador los puede ver desde la red pública y se podría acceder con las credenciales que se tiene.

Las situaciones mencionadas anteriormente contravienen los lineamientos establecidos en el MO-ETI- 001 Manual con las Políticas de Seguridad y Privacidad de la Información.

Tabla 17. Detalle de las Posibles causas, riesgos e impactos identificadas por la Oficina de Control Interno

Causas	Riesgos	Impactos
• Desconocimiento de los lineamientos de Seguridad establecidos en el *Manual: MO-ETI- 001 Manual con las Políticas de* Seguridad y Privacidad de la Información • Deficiencia en la ejecución de los lineamientos establecidos en el Manual: MO-ETI- 001 Manual con las Políticas de Seguridad y Privacidad de la Información.	Posibilidad de afectación reputacional y económica por multa y sanción del ente regulador debido al incumplimiento de los criterios de control y acceso definidos en la resolución 081 de 2021.	▪ Daño de la Imagen institucional. ▪ Afectación en el cumplimiento de metas y objetivos de la Entidad. ▪ Afectación en el cumplimiento de las políticas definidas en el PETI 2023-2026.

Fuente. Elaboración propia Equipo Auditor – Oficina de Control Interno.

RECOMENDACIÓN(ES):

Por lo anterior la Oficina de Control Interno, hace las siguientes recomendaciones:

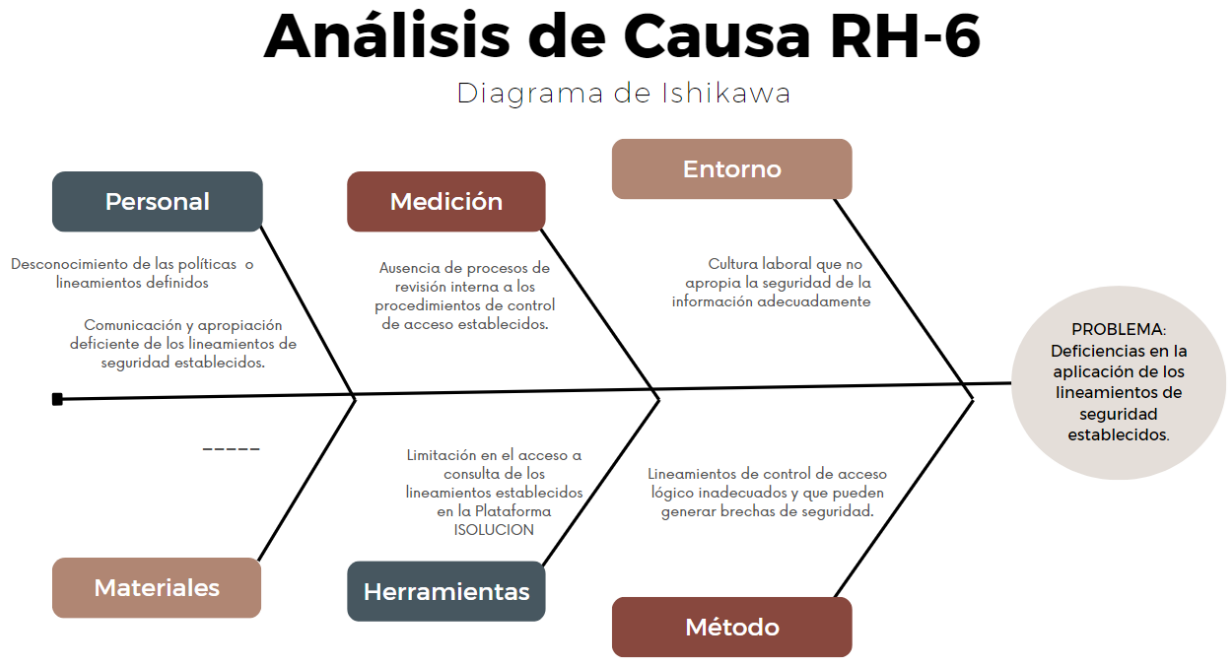
- Realizar la Gestión de actualizaciones de las cuentas genéricas de administración y el debido diligenciamiento de los formatos establecidos para tal fin.

- Redefinir la política con el fin de implementar tiempos definidos para la actualización de contraseñas.
- Socializar el manual: MO-ETI- 001 Manual con las Políticas de Seguridad y Privacidad de la Información.
- Realizar campañas de sensibilización en temas de la Seguridad y la Privacidad de la información, a todos los usuarios de la ADR.

RESPUESTA DEL AUDITADO: ACEPTADO.

JUSTIFICACIÓN:
La Oficina de Tecnologías de la Información acepta el hallazgo y formulará los planes de mejoramiento correspondientes.

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



Fuente. Respuesta Reporte de Hallazgo

PLAN DE MEJORAMIENTO:

Tabla 18. Plan de Mejoramiento

Acción(es) propuesta(s)	Meta(s)	Tipo de acción	Responsable(s)	Fecha inicial	Fecha final
Actualización de los lineamientos relacionados con el control de acceso lógico para que se adecuen.	Lineamientos actualizados y adecuados con las necesidades de la entidad.	Seleccione una opción	Grupo Seguridad de la Información – Oficina Tecnología de la Información	22-jul-2023	01-mar-2024
Solicitar a la Oficina de Planeación que se brinde acceso de lectura por defecto a toda la Oficina de TI para la documentación disponible en Isolución.	Acceso a consulta de los lineamientos vigentes del Sistema de Gestión de Seguridad para toda la Oficina de TI	Seleccione una opción	Grupo Seguridad de la Información – Oficina Tecnología de la Información	22-jul-2023	31-dic-2023
Realizar comunicación de los lineamientos establecidos a los roles que tienen una interacción directa con la gestión de control de acceso.	Lineamientos comunicados y apropiados por el personal de la Oficina de TI	Seleccione una opción	Grupo Seguridad de la Información – Oficina Tecnología de la Información	22-jul-2023	01-mar-2024

Fuente. Respuesta Reporte de Hallazgo

CONCEPTO DE LA OFICINA DE CONTROL INTERNO: ACEPTADO.

La Oficina de Control Interno considera que las acciones propuestas en el plan de mejoramiento presentado son razonables, dado que pretenden atacar las causas de las situaciones que originaron las desviaciones identificadas, sin embargo, se insta a definir acciones preventivas para evitar que las situaciones identificadas durante la auditoría se repitan a futuro.

RESUMEN DE HALLAZGOS:

N°	Título de Hallazgo	Repetitivo	Estado
1	Incumplimiento de la *"Política de Seguridad para la Adquisición, Desarrollo y Mantenimiento de Sistemas"* definida en la resolución 081 de 2021 *"Por la cual se adopta la política general de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios, así como definir lineamientos frente al uso y manejo de la información de la Agencia de Desarrollo Rural"*.	No	Abierto

N°	Título de Hallazgo	Repetitivo	Estado
2	Falta de efectividad del control *"Definir y elaborar el catálogo de sistemas de información que tiene como propósito identificar y conservar una lista completa y actualizada de los sistemas de información en la ADR, con el fin de identificar como es el acceso y evaluar el control".*	No	Abierto
3	Debilidades en el cumplimiento de la Política de Seguridad Digital, frente a la inactivación de los servicios tecnológicos de funcionarios desvinculados de la Entidad.	No	Abierto
4	Incumplimiento de la gestión de vulnerabilidades identificadas de acuerdo con el Manual de Operaciones: MO-OST-003 Guía de aseguramiento de Servicios en la Red.	No	Abierto
5	Asignación de calificación no congruente con las evidencias obtenidas en la fase de Diagnóstico MSPI.	No	Abierto
6	Incumplimiento de política de control de acceso por no actualización de contraseñas de cuentas genéricas.	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 Oficina de Tecnologías de la Información, 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.
- Las oportunidades de mejora, son situaciones que, si bien no se configuran como incumplimiento o desviación al no contar con un criterio que así lo indique, a

consideración de la Oficina de Control Interno las mismas pueden ser objeto de análisis por parte del proceso. A fin de reforzar el actuar operativo.

Bogotá D.C., 31 de julio de 2023.

WILSON GIOVANNY PATIÑO SUAREZ
Jefe Oficina de Control Interno

Elaboró: *Juan Harbey Numpaque Fonseca, Contratista, Oficina de Control Interno*
Revisó: *Claudia Marcela Pinzón Martinez, Contratista, Oficina de Control Interno*