AGENCIA DE DESARROLLO RURAL – ADR

Oficina de Control Interno

N° INFORME: OCI-2019-024

DENOMINACIÓN DEL TRABAJO: Auditoría Interna al Proceso "Gestión de Tecnologías de la Información"

DESTINATARIOS:[1]

- Claudia Sofía Ortiz Rodríguez, Presidente.
- Carolina Leonor Ramos Castellanos, Jefe Oficina de Planeación.
- Luis Alejandro Tovar Arias, Vicepresidente de Gestión Contractual, encargado del empleo Vicepresidente de Integración Productiva.
- Diego Edison Tiuzo García, Jefe de la Oficina Jurídica, encargado del empleo Secretario General.
- Néstor Fernando Mora Téllez, Gestor T1, asignado temporalmente a algunas actividades asociadas a las funciones de la Oficina de Tecnologías de la Información (Dependencia Responsable del Proceso Auditado).

EMITIDO POR: Héctor Fabio Rodríguez Devia, Jefe Oficina de Control Interno.

AUDITOR (ES): Carlos Eduardo Buitrago Cano, Contratista.

Iván Arturo Márquez Rincón, Contratista.

Luis Miguel Cuadros Alfonso, Contratista.

[1] Decreto 1083 de 2015 Artículo 2.2.21.4.7, Parágrafo 1° (modificado mediante el Artículo 1 del Decreto 338 de 2019) *"Los informes de auditoría, seguimientos y evaluaciones* [emitidos por la Oficina de Control Interno] *tendrán como destinatario principal el representante legal de la Entidad y el Comité Institucional de Coordinación de Control Interno y/o Comité de Auditoría y/o Junta Directiva (…)"*

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 "Gestión de Tecnologías de la Información".

ALCANCE: El alcance establecido para la realización de este trabajo comprendió la evaluación de los controles internos propios del proceso auditado, incluyendo lo relacionado con:

- Elaboración, actualización, implementación y seguimiento del Plan Estratégico de Tecnologías de la Información (PETI).
- Implementación del plan de acción de Gobierno Digital (antes Gobierno en Línea).
- Administración y mantenimiento de la infraestructura de Tecnologías de la Información (incluyó desarrollo, mejora o actualización de herramientas informáticas).
- Generación e implementación de Políticas de la Información.
- Seguimiento a mecanismos de seguridad de la información.
- Seguimiento al cumplimiento del Plan Operativo Anual - POA e indicadores del proceso.

Período Auditado: Septiembre de 2017 a Mayo de 2019.

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: La Oficina de Control Interno no cuenta con recurso humano calificado en el área de las Tecnologías de la Información y las Telecomunicaciones (Ingeniería de Sistemas, Ingeniería Informática, Ingeniería de Telecomunicaciones, etc.), razón por la cual, esta actividad fue ejecutada con las limitaciones propias derivadas de la carencia de las competencias técnicas específicas en tal área del conocimiento.

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

Decreto 1078 de 2015	Decreto 1083 de 2015, Art. 2.2.22.3.8
Decreto 2364 de 2015	Decreto 0415 de 2016
Decreto 0612 de 2018	Decreto 1008 de 2018
Resolución 1397 de 2017 (ADR)	Resolución 0409 de 2019 (ADR)

- Documentos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC):
  - G.ES.06 "Guía cómo estructurar el Plan Estratégico de Tecnologías de la Información – PETI" versión 1.0 del 30 de marzo de 2016.
  - Modelo de Gestión IT4+. Versión actualizada. Julio de 2016.
  - Lineamientos del Marco de Referencia de Arquitectura Empresarial para la Gestión de TI. Versión 1.1 del 11 de mayo de 2017.
  - Manual de Gobierno Digital. Versión 7 de abril de 2019.
- Plan Estratégico de Tecnologías de Información (2018 – 2022). ADR versión 1.
- Plan de Acción Institucional (vigencias 2018 y 2019).
- Documentación aplicable del Sistema Integrado de Gestión (CP-GTI-001, PR-GTI-002, PR-GTI-003, PR-GTI-004, DE-GTI-002, DE-GTI-003, IN-GTI-001, Mapas de Riesgo y Política de Administración de Riesgos)
- Demás normatividad aplicable.

DECLARACIÓN: Esta Auditoría fue realizada con base en el análisis de 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

hubiera llegado en caso de haber examinado todos los elementos que componen la población.

RESUMEN EJECUTIVO: Como resultado de la evaluación practicada, se identificaron oportunidades de mejoramiento relacionadas con los siguientes aspectos:

1. Plan Estratégico de Tecnologías de la Información (PETI) sin aprobar e implementar.
2. Insuficiencia de recursos humanos para cumplir con la estructura organizacional de Tecnologías de la Información y las Comunicaciones.
3. Políticas de Gobierno Digital y de Seguridad y Privacidad de la Información sin implementar y/o fortalecer.
4. Incumplimiento en los términos de ejecución y reporte del grado de avance de los productos del Plan de Acción Institucional.
5. Falta de instrumentación de mecanismos para la aplicación de la Política de Seguridad y Privacidad de la Información e incumplimiento de controles para la instalación de software.
6. Gestión de incidentes de seguridad de la información y desarrollo de software sin el cumplimiento de los lineamientos procedimentales.
7. Incumplimiento de los procedimientos establecidos para la generación y almacenamiento de las copias de seguridad de las bases de datos.
8. Navegación web y gestión de solicitudes de tecnologías de la información sin el cumplimiento de los requerimientos establecidos por la Entidad.
9. Incumplimiento de lineamientos en el desarrollo de inventario y clasificación de activos de información.
10. Mapa de riesgos de gestión del proceso sin construir y deficiencias en la valoración de los controles asociados a los riesgos de corrupción.

RIESGOS CUBIERTOS:

Incluidos en el Mapa de Riesgos del proceso

DESCRIPCIÓN	CUBIERTO EN LA AUDITORIA
Uso de software no licenciado. *(Mapa riesgos de la vigencia 2018)*	Si

Incluidos en el Mapa de Riesgos de Corrupción del proceso

DESCRIPCIÓN	CUBIERTO EN LA AUDITORIA
Ocultar o alterar la información dentro de los aplicativos que prestan servicios en la ADR, en beneficio propio o de un tercero.	Si

Identificados por la Oficina de Control Interno:

DESCRIPCIÓN	CUBIERTO EN LA AUDITORIA
Plan Estratégico de Tecnologías de la Información (PETI) inconsistente y/o que no apalanque la misionalidad de la Entidad.	Si
Inadecuada o falta de implementación de la Política de Gobierno en Línea (Gobierno Digital).	Si
Afectación de la continuidad de las operaciones por inoportunidad o inadecuada solución de incidentes y/o atención de éstos sin una categorización de riesgo e impacto (valoración).	Si
Inadecuada administración de datos y/o toma de decisiones por información no confiable, inoportuna e inexacta.	Si
Imposibilidad de recuperación de la información por ausencia y/o generación, disponibilidad y custodia inadecuada de las copias de seguridad de las bases de datos institucionales.	Si
Pérdidas económicas o estancamiento de los procesos por desarrollo de aplicaciones o herramientas informáticas sin la calidad y resultados esperados, y/o acuerdos de niveles de servicio ineficientes.	Si
Pérdida de información por accesos inadecuados, no autorizados y/o ausencia de controles que facilita la realización de actividades no permitidas sin posibilidad de trazabilidad y/o rastreo.	Si

DESCRIPCIÓN	CUBIERTO EN LA AUDITORIA
Apropiación indebida por parte de un servidor público del licenciamiento, código fuente y/o derechos de autor de un software desarrollado con ocasión de satisfacer necesidades de la Agencia. *(Riesgo de Corrupción)*	Si
Inobservancia del Plan de Acción Institucional	Si
Inobservancia de los lineamientos que en materia de gestión integral del riesgo ha adoptado la Agencia de Desarrollo Rural (ADR).	Si

FORTALEZAS: El proceso *"Gestión de Tecnologías de la Información"* se encuentra catalogado como un proceso estratégico de la Agencia de Desarrollo Rural (ADR), aprobado el 30 de agosto de 2017 y adoptado en el Sistema Integrado de Gestión de la Entidad con el objetivo de *"Evaluar la eficiencia de la Entidad, a través de políticas, planes, programas y proyectos para el desarrollo de servicios y productos TIC, propendiendo por la disponibilidad, confidencialidad e integridad de la información."*

Como resultado de la evaluación practicada, la Oficina de Control Interno identificó las siguientes fortalezas a resaltar:

- La Oficina de Tecnologías de la Información (dependencia responsable del proceso auditado) aprobó el 12 de febrero de 2018 el Manual de Operaciones "Política de Navegación Web" (DE-GTI-002), el cual en sus numerales 6 y 7 determina los grupos de navegación al interior de la Agencia de Desarrollo Rural (ADR) y el tipo de usuarios que los conforman. En este sentido la Oficina de Control Interno identificó la asignación a cada uno de los veinte (20) servidores seleccionados como muestra en su respectivo grupo de navegación, así como el seguimiento constante que se realiza a cada servidor registrado en el directorio activo de la Entidad respecto de su activación, inactivación y estado de la contraseña.

- Entre los meses de enero y junio de 2019, la Oficina de Tecnologías de la Información (dependencia responsable del proceso auditado), en virtud del Programa de Mantenimiento, ha ejecutado siete (7) visitas a igual número de Unidades Técnicas

Territoriales (Cúcuta, Pasto, Cartagena, Medellín, Montería, Popayán y Tunja), con el fin de realizar mantenimiento preventivo y correctivo a los equipos de cómputo de la Entidad ubicados en las mismas, como también identificar necesidades *"(…) que permita prevenir, mitigar y corregir fallas o daños, relacionados con los equipos, sistemas de información, seguridad informática y de red de datos de la Unidad Técnica Territorial (…); asegurando la prolongación de la vida útil y confiabilidad de los componentes de la infraestructura tecnológica, con niveles de calidad adecuados, programando el mantenimiento preventivo y dando solución eficaz a los eventos por medio de mantenimiento correctivo. Garantizando de manera efectiva la disponibilidad de la infraestructura tecnológica de la entidad*." (sic).

- Mediante la Resolución 0409 del 3 de julio de 2019 la Entidad adoptó la "Política de Seguridad y Privacidad de la Información" como habilitador transversal de la Política de Gobierno Digital. Lo anterior, en virtud de lo establecido en el numeral 1.5. del Manual de Gobierno Digital emitido por el Ministerio de Tecnologías de la información y las Comunicaciones (MINTIC), el cual, al respecto menciona que con la adopción de esta política se "*busca que las entidades públicas implementen los lineamientos de seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información con el fin de preservar la confidencialidad, integridad y disponibilidad y privacidad de los datos. (…)*"

- La Agencia de Desarrollo Rural (ADR) cuenta con una mesa de servicio, a través del aplicativo ARANDA, en el que los funcionarios y contratistas de la Entidad pueden reportar problemas de soporte de hardware y software, tales como: instalación de aplicativos, restauraciones de copias de seguridad, recuperaciones de documentos, entre otros, y gestionar las soluciones.

AVANCE DEL PLAN DE MEJORAMIENTO VIGENTE AL INICIO DE LA AUDITORÍA: No aplica. Esta actividad de aseguramiento corresponde al primer ejercicio de auditoría interna practicado por la Oficina de Control Interno sobre el proceso de Gestión de Tecnologías de la Información.

HALLAZGOS:

HALLAZGO N° 1. Plan Estratégico de Tecnologías de la Información sin aprobar e implementar.

Descripción: El documento G.ES.06 "Guía cómo estructurar el Plan Estratégico de Tecnologías de la Información – PETI" versión 1.0 del 30 de marzo de 2016 indica en su numeral 2 *"Plan Estratégico de Tecnologías de la Información"* que éste es *"(…) el artefacto que se utiliza para expresar la estrategia de TI. (…) hace parte integral de la estrategia de la institución y es el resultado de un adecuado ejercicio de planeación estratégica de TI. (…)"*. Por su parte, el numeral 2.2 *"Alcance del documento"* alude que: *"(…) debe proyectarse a máximo cuatro años y debe actualizarse cada año. (…)"*. Finalmente, el Decreto 1083 de 2015 en su artículo 2.2.22.3.14 "*Integración de los planes Institucionales y estratégicos al Plan de Acción"* menciona que: *"Las entidades del Estado (…), deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año: (…) 10. Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETI (…)".*

Para verificar el cumplimiento de lo anteriormente descrito, la Oficina de Control Interno llevó a cabo una reunión el 18 de junio de 2019 con el equipo delegado para atender la auditoría, en la cual se informó que: "*El PETI no está aprobado; no ha tenido cambios desde la versión preliminar que existe. Las personas que lo manejaban eran contratistas que ya no están vinculados.*"

De acuerdo con la información recibida, se inspeccionó el acta N° 005 del 12 de diciembre de 2018 de la quinta sesión no presencial del Comité Institucional de Gestión y Desempeño, en la cual se corroboró que, en efecto el PETI 2018-2022 fue presentado más no aprobado, en virtud de que se requirieron ajustes a su contenido. Así mismo, se revisó el documento "Plan Estratégico de Tecnologías de la Información PETI 2018-2022 Versión 1" de la Agencia de Desarrollo Rural y en su contenido se evidenciaron rezagos asociados a la inclusión y alineación de los objetivos estratégicos de la Entidad con los

del Sector Agricultura, y en general con los del Plan Nacional de Desarrollo 2018-2022 puesto que se incluyeron los del Gobierno anterior (2014- 2018). Pese a que el documento indicaba que fue actualizado en julio de 2018, no se evidenció la aprobación inicial, por lo que se infiere que no sólo carece de actualización sino de emisión de su versión final para aprobación.

Adicional a lo anterior, se realizó una comparación entre la estructura de contenido del PETI, teniendo en cuenta lo establecido en la Guía G.ES.06, frente al documento PETI, identificando que los siguientes temas no fueron tratados o detallados en el PETI presentado:

TEMA	OBSERVACIÓN
7.5.6 Procedimientos de Gestión	Aunque en el documento borrador se identificaron sendos títulos, no se evidenció ampliación en detalle de los temas.
8. Modelo de Planeación	
8.5 Plan de Intervención sistemas de información	No se identificaron en el documento estos apartados.
8.6 Plan de Proyectos de Servicios Tecnológicos	

De otra parte, el no contar con un PETI aprobado por el Comité Institucional de Gestión y Desempeño, afectó su integración en el Plan de Acción Institucional de la vigencia 2019 publicado en la página web de la Entidad en enero de 2019, incumpliéndose los términos del artículo 2.2.22.3.14 del Decreto 1083 de 2015.

Posible(s) Causa(s) identificada(s) por la Oficina de Control Interno:

- Insuficiencia de personal y ausencia del rol de Jefe de OTI para atender los temas relacionados con la estructuración adecuada del PETI.
- Desfinanciamiento o falta de presupuesto suficiente para la OTI, que permita estructurar y alinear un PETI con los objetivos de la Entidad y el Sector Agricultura.
- Rotación del personal encargado de adelantar las actividades asociadas a la estructuración del PETI.

- Incumplimiento en la aplicación de ajustes solicitados sobre el PETI para la presentación y aprobación del Comité Institucional de Gestión y Desempeño.
- Falta de fortalecimiento y/o implementación de la Estrategia y Gobierno de TI en la Entidad.
- Desconocimiento y/u omisión de las mejores prácticas y guías para la estructuración del PETI en la Entidad.

Descripción del (los) Riesgo(s): Plan Estratégico de Tecnologías de la Información (PETI) inconsistente y/o que no apalanque la misionalidad de la Entidad.

Descripción del (los) Impacto(s):

- Posible incumplimiento de los objetivos misionales de la ADR que están apalancados o sustentados en el componente tecnológico.
- Materialización de riesgos derivados de la inadecuada gestión de Tecnologías de la Información (pérdidas de información, vulnerabilidad de la seguridad y privacidad entre otros).
- Incumplimientos normativos por inobservancia de políticas de TI.

Recomendación(es):

La estructuración de un PETI siempre estará supeditada a la implementación eficiente y funcional de una Estrategia de Tecnologías de la Información apalancada en el Gobierno de TI. Para lograr esta sinergia, es necesario que la Entidad contemple dentro de su Administración la vinculación del servidor que ejerza las funciones correspondientes de la OTI, con poder de decisión sobre las actividades del área y con participación en el Comité Directivo de la ADR (o quien haga sus veces) para visibilizar las necesidades y requerimientos de la Entidad. Aunado a lo anterior, y con el fin de seguir la metodología de las Políticas de Gobierno Digital y de Seguridad y Privacidad de la Información, se insta a que el equipo de la OTI:

a. Realice un análisis de brechas, esto es, que identifique los requerimientos normativos frente a los recursos disponibles del área (se deberían considerar análisis financieros sobre recursos necesarios versus presupuesto aprobado). En aquellos casos donde se detecten vacíos, se deberán manifestar las necesidades de recursos (humanos, presupuestales o de infraestructura) que permitan acometer los proyectos y/o identificar aquellos tópicos que no podrán ser atendidos por dificultades o restricciones. En todo caso, se deberán asignar las actividades al personal pertinente atendiendo a sus competencias en relación con la gestión de TI.

b. Construya un tablero de control o diseñe una hoja de ruta de todos los hitos que debe abordar para cumplir con los proyectos, planes o programas que identificó en el paso anterior, indicando en un cronograma las fechas en las que espera cumplirlos con sus respectivos entregables. Es importante acompañar este esquema de un monitoreo continuo sobre el desarrollo de las actividades. Entre los temas a cubrir se encuentran, entre otros: elaboración / actualización del PETI, implementación de políticas de Gobierno Digital, de Servicios Ciudadanos Digitales, modelo de Arquitectura Empresarial y Protocolo de Internet versión 6 (IPv6). Se resalta que esta tarea es diferente a la de formulación de planes de acción.

c. Retomar los compromisos descritos en el Acta 005 de 2018 y darles cumplimiento para, subsecuentemente, citar al Comité Institucional de Gestión y Desempeño para el análisis y aprobación del PETI y demás asuntos relacionados con la Gestión de TI (desde luego, previa ejecución de los pasos anteriores).

d. Finalmente, fomentar espacios de capacitación para los funcionarios y contratistas de TI en temas relacionados con su área de conocimiento, tales como: mejores prácticas de TI, marcos de calidad ITIL (Biblioteca de Infraestructura de Tecnologías de Información o ITIL, por sus siglas en inglés), COBIT, IT4+, ISO 27001 etc., que ayuden al cumplimiento de la estrategia de TI que se consigne en el PETI.

Respuesta del Auditado: Aceptado.

Causa(s) identificada(s) por el Responsable del Proceso Auditado:

- Falta de comunicación directa y constante con los directivos respecto a proyectos de TI que apalanquen los procesos misionales de la ADR.
- No se ha definido una estrategia de TI alineada a los objetivos misionales considerando los retos establecidos en los diferentes planes institucionales y sectoriales.

Plan de Mejoramiento:

ACCIÓN(ES) PROPUESTA(S)	META(S)	TIPO DE ACCIÓN	RESPONSABLE(S)	FECHA INICIAL	FECHA FINAL
Gestionar espacios con los líderes de la ADR, con el fin de conocer sus necesidades y establecer proyectos de TI que impacten la misionalidad de la Agencia.	Definir estrategia de TI de manera conjunta con los directivos de la ADR	Correctiva	Equipo de Trabajo de la OTI	19-ago-19	30-sep-19
Conforme la nueva guía y los diagnósticos de TI, formular el Plan Estratégico de Tecnologías de la Información.	Plan Estratégico de Tecnologías de la Información formulado	Correctiva	Equipo de Trabajo de la OTI	19-ago-19	18-nov-19

Concepto de la Oficina de Control Interno: Aceptado con Observaciones.

Al analizar el plan de mejoramiento propuesto, se identificaron los siguientes aspectos, los cuales podrían ser considerados para su ajuste o complemento:

- Para la acción "*Gestionar espacios con los líderes de la ADR con el fin de conocer sus necesidades y establecer proyectos de TI que impacten la misionalidad de la Agencia*" se estableció como meta "*Definir estrategia de TI de manera conjunta con los directivos de la ADR*". Al respecto, esta Oficina de Control Interno considera que emprender esta actividad no garantizará que el PETI continúe sin actualizaciones y aprobación para posterior ejecución, toda vez que se remite a tratar una de las varias temáticas que debe contemplar dicho documento (la identificación de nuevos proyectos y su impacto en la misión), más no plantea la manera como se dará a

conocer el resto del contenido, su aprobación por parte de los usuarios y, finalmente, del Comité Institucional de Gestión y Desempeño para sanción de los Directivos. Se recuerda que la meta debe corresponder a un producto tangible, por lo que es necesario establecer qué tipo de resultado se producirá a partir de las reuniones al interior de la ADR.

- Para la acción "*Conforme la nueva guía y los diagnósticos de TI, formular el plan estratégico de Tecnologías de Información*" se estableció como meta "*Plan estratégico de TI formulado*". La Oficina de Control Interno prevé que esta meta va a redundar en una situación similar a la del año 2018, en la que se diseñó y formuló el documento PETI pero no se divulgó, ni se le hicieron los ajustes requeridos para su aprobación por las instancias respectivas para su puesta en ejecución, es decir, el sólo hecho de formular el documento no producirá efectos hasta tanto no se apruebe e implemente. En este orden de ideas, se recomienda analizar la posibilidad de sustituir el PETI formulado por el PETI aprobado y divulgado.

Además, dentro de los responsables se indica "Equipo de Trabajo", por lo que, es necesario se distingan los roles que van a aportar al cumplimiento de cada meta.

HALLAZGO N° 2. Insuficiencia de recursos humanos para cumplir con la estructura organizacional de Tecnologías de la Información y las Comunicaciones.

Descripción: En el Manual para la Implementación de Gobierno Digital, numeral 1.5 *"¿Quiénes ejecutan la Política?",* el gobierno nacional incentiva el involucramiento desde la Alta Dirección hasta las Áreas específicas de la Entidad, para el desarrollo del gobierno digital y logro de su propósito, por lo que presenta las instancias y responsables de implementación que se relacionan a continuación:

- Líder de la Política de Gobierno Digital: El Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC).
- Responsable Institucional de la Política de Gobierno Digital: El Representante Legal de la Entidad.

- Responsable de orientar la implementación de la Política de Gobierno Digital: El Comité Institucional de Gestión y Desempeño.

- Responsable de liderar la implementación de la Política de Gobierno Digital: El Jefe de la Oficina de Tecnologías de la Información – OTI.

Además, dentro de los procesos de transformación digital de las entidades públicas, considera otros roles e instancias importantes, por lo que "*recomienda la creación de algunas instancias técnicas, para definir y tomar decisiones operativas y técnicas con relación a la arquitectura empresarial de la Entidad. Estas instancias deben actuar en coordinación con el Comité Institucional de Gestión y Desempeño para la toma de decisiones.*" Entre estas instancias recomendadas se encuentra el "Grupo de Trabajo de Arquitectura Empresarial" que debe estar conformado por el Líder, Jefe OTI, Jefe Oficina de Planeación, Profesionales encargados de las arquitecturas de sistemas de información y arquitectura de infraestructura tecnológica, Líder de gestión o información o Arquitecto de información de la Entidad y Líderes de las áreas funcionales y de procesos cuando se requiera.

De otra parte, el documento *"G.ES.06 Guía Cómo Estructurar el Plan Estratégico de Tecnologías de la Información – PETI"* indica en el numeral 2.5.6 *"Gobierno de TI. Estructura Organizacional y Talento Humano. (…) debe describir la estructura organizacional actual del área de TI en la institución, detallando la cantidad de personas que conforman el área, sus funciones, tipo de contratación y perfiles. Recolecta y analiza las necesidades de recurso humano de TI con relación a su formación y competencias y cantidad de personas para soportar la operación actual de TI"*.

Finalmente, el Decreto 1083 de 2015 en su artículo 2.2.35.4 "*Nivel Organizacional*" (adicionado por el artículo 1 del Decreto 415 de 2016), indica: *"Cuando la entidad cuente en su estructura con una dependencia encargada del accionar estratégico de las Tecnologías y Sistemas de la Información y las Comunicaciones, hará parte del Comité Directivo y dependerán del nominador o representante legal de la misma"*.

Así las cosas, para efectos de corroborar la adopción del esquema de Gobierno de TI antes descrito, la Oficina de Control Interno solicitó información respecto a la organización interna de la Oficina de Tecnologías de la Información (OTI) e inspeccionó el PETI con el que cuenta la Agencia de Desarrollo Rural (ADR), a fin de comparar sus contenidos e identificar brechas entre los mismos, en lo que se identificaron las siguientes discrepancias o falta de recurso para desempeñar el(los) rol(es) definidos en el PETI:

ROL SEGÚN PETI DE LA ADR	ROL HOMÓLOGO SEGÚN ORGANIZACIÓN INTERNA OTI	OBSERVACIONES
Director del Área	Jefe OTI	Desde finales de la vigencia 2018, la OTI no cuenta con un servidor público en propiedad del cargo, algunas de las funciones las ostenta un funcionario de nivel profesional (Gestor T1, Grado 8), a quien se le asignó "*temporalmente de unas actividades asociadas a las funciones de la Oficina de Tecnologías de la Información*" (Res. 030 de 2019 – ADR)
Líder de Sistemas de Información	Líder Sistemas de Información	De acuerdo con la organización interna de la OTI informada, estos roles se han asignado a funcionarios de nivel profesional como Gestores (Código T1, Grado 08).
Líder Web	Página web	
Líder de Infraestructura	Líder de Infraestructura	
Líder de Operaciones	Líder de Mesa	
Líder de Seguridad	Oficial de Seguridad	
▪ Asesor ▪ Secretaria Ejecutiva ▪ Líder de Desarrollo de Aplicaciones ▪ Líder de Uso y Apropiación ▪ Analista de Sistemas de Información	No se identificó	La Entidad no cuenta con estos roles en la organización interna de la OTI.

Aunado a lo anterior, dado que la Entidad aún no implementa completamente la Política de Gobierno Digital y que su presupuesto es bajo en comparación con las Entidades del Sector Agropecuario (según lo manifestado por los responsables del proceso auditado en reunión del 18 de junio de 2019), se concluye que no ha sido factible contar con una OTI fortalecida que apalanque la misionalidad de la Entidad, dado que actualmente por la demanda de servicios de soporte, el recurso humano del área se destina a atender

estos temas o requerimientos, más no los demás tópicos que son contemplados en la Política de Gobierno Digital conocidos como “Dominios”, a saber: Estrategia de TI, Gobierno de TI, Información, Sistemas de Información, Servicios Tecnológicos y Uso y Apropiación.

Posible(s) Causa(s) identificada(s) por la Oficina de Control Interno:

- Falta de vinculación en propiedad del Jefe de la OTI.
- Dificultades en el proceso de contratación de personal para la OTI (demoras, identificación de recurso humano en el mercado, oferta, tipo de contrato entre otros aspectos).
- Desfinanciamiento o presupuesto insuficiente para la OTI, que permita estructurar el área con personal con las habilidades requeridas por la Arquitectura Empresarial.
- No se cuenta con una Planeación Estratégica de Tecnologías de la información -PETI con objetivos claros, medibles y alcanzables con las necesidades de recursos para su logro.

Descripción del (los) Riesgo(s):

- Plan Estratégico de Tecnologías de la Información (PETI) inconsistente y/o que no apalanque la misionalidad de la Entidad.
- Inadecuada o falta de implementación de la Política de Gobierno en Línea (Gobierno Digital).

Descripción del (los) Impacto(s):

- Posible incumplimiento de los objetivos misionales de la Entidad que están apalancados o sustentados en el componente tecnológico.
- Materialización de riesgos derivados de la inadecuada gestión de Tecnologías de la Información por falta de recursos humanos en el área para su atención.

- Incumplimientos normativos por inobservancia de buenas prácticas de Tecnologías de la Información.

- Obsolescencia tecnológica y rezago frente a las demás entidades del sector.

Recomendación(es):

- La Entidad debe propender por la vinculación del Jefe de la OTI, y así dar cumplimiento a las exigencias legales que no han podido ser atendidas completamente por falta de este recurso, a la vez, considerar el equipo mínimo requerido para atender todos los frentes de trabajo que la Arquitectura Empresarial demanda de las Entidades.

- En virtud de que el fortalecimiento de las áreas de la Entidad es función de la atención y cobertura que otorga su Alta Dirección, es importante que desde el Comité Institucional de Gestión y Desempeño se apalanque la participación de la OTI a este nivel, con el fin de dar a conocer sus restricciones, problemáticas y necesidades que el proceso de Gestión de Tecnologías de la Información demanda para cumplir con sus objetivos institucionales y sectoriales, para lo que es necesario que el encargado de funciones de Jefe de la OTI prepare una propuesta de trabajo con sentido de urgencia, contentiva de sus correspondientes requerimientos, para que los presente a estas instancias. Lo anterior, en concordancia con los términos del Decreto 1083 de 2015, artículo 2.2.35.4 "*Nivel Organizacional*" (adicionado por el artículo 1 del Decreto 415 de 2016).

  De otra parte, al momento de la planeación financiera de las siguientes vigencias, el encargado de la OTI debería visibilizar, dentro de la propuesta antes comentada, los requerimientos financieros para desempeñar sus labores y las del área, utilizando los argumentos que considere pertinentes para solicitar la ampliación de su presupuesto.

- Entre tanto se realizan gestiones para la ampliación presupuestal y propuestas de trabajo del área, es importante que el equipo de trabajo actual, internamente establezca pilares de trabajo que en la medida de lo posible abarquen las demandas

normativas asociadas a Política de Gobierno Digital, Seguridad y Privacidad de la Información y Servicios Ciudadanos Digitales (próximamente), con el fin de adelantar actividades que harán parte del plan de trabajo de quien asuma las funciones de Jefe en propiedad de la Oficina de Tecnologías de la Información.

Respuesta del Auditado: Aceptado Parcialmente

Justificación: "*Se acepta parcialmente el hallazgo en tanto que se reconoce la falta de un PETI que apalanque la misionalidad de la Entidad. De otra parte, en la Guía Operativa para la ejecución del proyecto de inversión para el año 2019, se argumenta en su producto 1: "Documento para la planeación estratégica en TI", que la Oficina de Tecnologías de la Información cuenta con los recursos económicos para suplir las necesidades de personal idóneo que darán cumplimiento a la Estrategia TI; sin embargo, la ausencia de un Jefe de OTI ha impactado significativamente los procesos de contratación por Prestación de Servicios, debido a que es el Jefe OTI el principal representante para apalancar a través de la Presidencia de la ADR las necesidades de la OTI, con el fin de que surta efecto la implementación del marco de Arquitectura TI. Así mismo, los cambios constantes que se han presentado con respecto al cargo de Presidente de la Agencia, han generado demoras debido a que la toma de decisiones varía, esto se da por la rotación en dicho cargo*."

Causa(s) identificada(s) por el Responsable del Proceso Auditado: Falta de personal idóneo para que aporte estratégicamente a la implementación de los modelos de gestión TI que apalanquen los procesos misionales de la ADR.

Plan de Mejoramiento:

ACCIÓN(ES) PROPUESTA(S)	META(S)	TIPO DE ACCIÓN	RESPON SABLE(S)	FECHA INICIAL	FECHA FINAL
Gestionar ante Presidencia de la ADR la aprobación para la contratación por Prestación de Servicios del personal idóneo requerido en la OTI.	Contar con el personal profesional idóneo para la implementación del marco de Arquitectura TI	Correctiva	Equipo Humano de la OTI	Para establecer las fechas de esta acción se requiere contar con el Jefe de la OTI	

Nota: *La relación detallada del equipo humano de la Oficina de Tecnologías de la Información (OTI) responsable de cada acción propuesta se encuentra registrada en papeles de trabajo de la Oficina de Control Interno.*

Concepto de la Oficina de Control Interno: Aceptado con Observaciones.

Una vez analizada la justificación del equipo auditado, esta Oficina de Control Interno acepta los términos de la misma, toda vez que el equipo auditado admite que la estructura organizacional de la Agencia de Desarrollo Rural (ADR) debe ser fortalecida para poder ejecutar la Estrategia de Tecnologías de la Información; no obstante, no se identificó el argumento con el cual se aminora el hallazgo descrito para catalogar como "parcial" su aceptación.

Respecto al plan de mejoramiento suscrito, se observa que la meta propuesta apunta a la contratación de los recursos necesarios para la implementación de Arquitectura de TI; no obstante, es necesario identificar y registrar qué tipo de personal se requerirá, por ejemplo: Arquitecto de TI, Líder de desarrollo de aplicaciones, entre otros, dado que, el no denotarlo específicamente abre la posibilidad de que la contratación que se efectúe resulte eventualmente insuficiente o no corresponda a las necesidades y no logre los objetivos estratégicos esperados para la arquitectura que se busca implementar.

De otra parte, al no asignar unas fechas estimadas para la ejecución del plan de mejoramiento se deja en suspenso la acción propuesta, lo que muy probablemente redunde en que no se adopte una mejora al hallazgo. En este sentido, es necesario que se consulte al interior de la Entidad para que, o bien se faculte al funcionario asignado temporalmente de unas actividades asociadas a las funciones de la OTI para buscar los recursos humanos que se necesitan, o que se implemente una acción alternativa que permita ir avanzando en la adopción de la Arquitectura de TI, en tanto se concretan las contrataciones esperadas.

HALLAZGO N° 3. Políticas de Gobierno Digital y de Seguridad y Privacidad de la Información sin implementar y/o fortalecer.

Descripción: La caracterización del proceso Gestión de Tecnologías de la Información (CP-GTI-001) tiene por objetivo *"Elevar la eficiencia de la Entidad a través de políticas,*

planes, programas y proyectos, para el desarrollo de servicios y productos TIC, propendiendo por la disponibilidad, confidencialidad e integridad de la información" y su alcance se definió "*desde el diseño y definición de políticas, planes y programas para el desarrollo de servicios y productos TIC hasta la implementación de tecnologías de la información en los procesos de la ADR*", por lo cual, está compuesto de once (11) actividades relacionadas con estos aspectos. Todo este conjunto de tareas es lo que debería traducirse en Arquitectura Empresarial de las Tecnologías de la información.

Por lo anterior, la Oficina de Control Interno verificó el cumplimiento de las actividades de la caracterización del proceso relacionadas con la generación e implementación de Políticas de Información y la verificación de los indicadores del proceso (autoevaluación de gestión), como también una revisión de la suficiencia de los procedimientos de gestión de servicios tecnológicos, encontrando lo que se detalla a continuación:

- Actividad 5 "Generación e Implementación de Políticas de la Información".

  El Manual para la implementación de Gobierno Digital considera dentro de los componentes de la Política tres (3) habilitadores transversales, a saber: Arquitectura, Seguridad de la Información y Servicios Ciudadanos Digitales, por lo que, la Oficina de Control Interno realizó un análisis de cada uno de ellos soportado en la evidencia entregada por los responsables del proceso auditado, obteniendo los siguientes resultados:

  - **Arquitectura**. Al respecto, en archivo anexo remitido el 4 de julio de 2019, los responsables del proceso auditado manifestaron que: *"Respecto al modelo de arquitectura empresarial, en la generación de capacidad, se realizó medición a través el FURAG obteniendo un 71,4%. (…)"*. Con base en esta respuesta, la Oficina de Control Interno revisó el Formulario Único de Reporte de Avances de la Gestión -FURAG del año 2018 y evidenció que en el segmento de "Gobierno Digital", en particular la pregunta referida a la **Arquitectura Empresarial** se seleccionó la respuesta *"Ninguna de las anteriores"* dentro de la siguiente gama de opciones: *"a. identifica las capacidades (personas, procesos y herramientas)*

necesarias para realizar ejercicios de arquitectura empresarial; b. Hace uso de una metodología de arquitectura empresarial para el diseño y planeación de las iniciativas de tecnologías de información; c. Desarrolló o se encuentra en ejecución de uno o más ejercicios de arquitectura empresarial; d. Cuenta con un grupo de arquitectura empresarial que gobierna y toma decisiones frente al impacto o evolución de la arquitectura; (…); f. Ninguna de las anteriores."

Así las cosas, y, de acuerdo con los resultados del FURAG 2018 y los derivados de los procedimientos de auditoría efectuados, se confirma que la Entidad aún debe fortalecer su esquema de Arquitectura Empresarial, iniciando por el establecimiento de una Estrategia de TI y un Gobierno de TI instrumentados a través de un PETI debidamente divulgado y aprobado por el Cuerpo Directivo de la Entidad.

- **Seguridad de la Información.** La ADR mediante la Resolución 0409 del 3 de julio de 2019 *"Por la cual se adopta la política de seguridad y privacidad de la información de la Agencia de Desarrollo Rural y se definen lineamientos frente al uso y manejo de la información"* emitió disposiciones para abordar la normativa referida; no obstante, la Entidad se encuentra en implementación gradual de la misma, toda vez que, en indagación a la OTI sobre la existencia de un manual de políticas de tecnologías de información, esta dependencia señaló que: *"(…) estamos adelantando actualización de lineamientos y políticas conforme al modelo de privacidad y seguridad de la información"*.

- **Servicios Ciudadanos Digitales**. Este habilitador no fue considerado en virtud de que la normativa asociada (Decreto 1413 de 2017) sería subrogado por medio de la expedición de un decreto que se encuentra en fase de análisis de comentarios por parte del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), lo que indicaba que, a la fecha de esta auditoría (30 de junio de 2019) el MINTIC no había emitido lineamientos para su adopción. Lo antes comentado puede ser consultado en el link: https://www.mintic.gov.co/portal/604/w3-article-101096.html

- Actividad 11 "Verificación de los indicadores del proceso – autoevaluación de gestión".

  Para la vigencia 2019 se formularon seis (6) indicadores para el proceso "Gestión de Tecnologías de la Información", de los cuales, la Oficina de Control Interno verificó su avance y/o cumplimiento a 30 de junio de 2019 en el módulo "Medición" del aplicativo ISOLUCIÓN, donde identificó las siguientes situaciones:

INDICADOR	OBSERVACIÓN
Documentos para la planeación estratégica actualizados	Entre enero y marzo se indicó: *"La OTI no realizó actividades relacionadas con este indicador"* y entre abril y junio: *"Está en proceso la contratación del recurso humano que nos va a apoyar en el desarrollo de estas actividades".*
Índice de prestación de servicios de TI	Se identificó avance del 49%.
Número de servicios de información actualizados.	Para enero y febrero se indicó que: *"se realizó la actualización a la página web de la ADR (contenidos, link) de acuerdo a solicitudes de la Oficina de Comunicaciones de la ADR"*
Nivel de avance en la ejecución del plan de Seguridad y Privacidad de la información - vigencia 2019	Entre enero y junio se indicó que: *"La OTI no ha realizado actividades relacionadas con este indicador"*
Nivel de avance en la ejecución del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información -vigencia 2019	
Número de Servicios de Información implementados.	

  Además, es importante mencionar que el borrador del PETI no incluye estos indicadores, aunque se resalta la consideración de dos (2) indicadores asociados al diseño e implementación de la Política de Seguridad de la Información que confirma el entendimiento de avances comentados en el habilitador "Seguridad de la Información", y no se identificaron indicadores asociados a Gobierno Digital.

De otra parte, teniendo en cuenta que el numeral 2.7.5.6 *"Procedimientos de Gestión"* del documento *"G.ES.06 Guía Cómo Estructurar el Plan Estratégico de Tecnologías de la Información"* establece que: *"Se deben identificar y describir brevemente los procesos de gestión de tecnología"* incluyendo como mínimo procedimientos relacionados con mesa de servicios, gestión de incidentes, problemas, eventos, cambios, seguridad,

configuración, entrega, niveles de servicio, disponibilidad, capacidad y gestión de continuidad; por lo que, la Oficina de Control Interno procedió a verificar la existencia o no del documento o lineamiento en los procedimientos, instructivos o manuales del proceso auditado, en lo que evidenció insuficiencia en los procedimientos de gestión, teniendo en cuenta los resultados del análisis registrados en la tabla que sigue:

PROCEDIMIENTO SEGÚN GUÍA PETI	NOMBRE PROCEDIMIENTO / HOMÓLOGO EN LA ADR
Mesa de Servicios	Gestión de Solicitudes de Tecnología (PR-GTI-002)
Gestión de Incidentes	Gestión de Incidentes de Seguridad de la Información (PR-GTI-004)
Gestión Entrega	Desarrollo de Software (PR-GTI-003)
Gestión de Disponibilidad	Generación y Administración de Copias de Seguridad de las Bases de Datos (DE-GTI-003)
Gestión Capacidad	
Gestión de Problemas	No se identificó su inclusión en los procedimientos, instructivos o manuales del proceso auditado.
Gestión de Eventos	
Gestión de Cambios	
Gestión Seguridad	
Gestión Configuración	
Gestión Niveles de Servicio	
Gestión de Continuidad	

Así mismo, al observar que la Entidad no cuenta con un procedimiento de Gestión de Niveles de Servicio, el 27 de junio de 2019 la Oficina de Control Interno solicitó a los responsables del proceso auditado mediante correo electrónico: *"Detallar el catálogo de servicios de TI y los acuerdos de niveles de servicios (ANS) asociado"*, quienes manifestaron: *"Catálogo de servicios de TI no se tiene, actualmente se trabaja como catálogo el aplicativo Aranda donde se evidencia los servicios que se tienen. Con referencia a los (ANS) estos son los establecidos actualmente en el aplicativo ARANDA. En (…) se puede evidenciar los servicios como los ANS que actualmente maneja la OTI y los cuales están parametrizados en el aplicativo ARANDA. Para la vigencia 2019 se*

inició la elaboración del catálogo de servicios como los ajustes a los ANS, continuando con el reporte en el aplicativo ARANDA."

De esta manera, se evidenció que la Entidad requiere fortalecer sus gestiones respecto al diseño y seguimiento de Acuerdos de Niveles de Servicio (ANS). Esta premisa se sustenta adicionalmente en los siguientes hechos:

- Por la inexistencia de documentos físicos, suscritos por las áreas que lo requieran y la OTI, que permitan corroborar los términos del ANS, obligaciones y tiempos de respuesta entre otros aspectos.

- Por la inspección del archivo Excel *"Parametrización Aranda – ADR – 17-05-2018"* en el cual se identificaron campos vacíos como: "Fecha revisión", "Fecha alarma revisión", "Proveedor".

- Porque los ANS que la OTI indicó como vigentes corresponden a "Soporte"; sin embargo, excluye otras opciones, tales como "Activos de Información", "Seguridad de la información" entre otros que la Entidad debe validar.

- Finalmente, porque mediante acta-e-mail del 22 de junio de 2019: "*Sobre este ANS* [el de la mesa de servicio], *se mencionó que no se tiene una persona encargada de hacer su seguimiento. De otra parte, no se ha hecho un seguimiento del ANS aludido en virtud que se están planteando cambios al mismo*".

Posible(s) Causa(s) identificada(s) por la Oficina de Control Interno:

- Insuficiencia de personal y/o dificultades en la contratación del recurso humano con las competencias para asumir y ejecutar las actividades misionales y estratégicas de TI de la Entidad.

- Falta de estructuración y/o actualización del PETI de la Agencia de Desarrollo Rural.

- Falta de fortalecimiento y/o implementación de la Estrategia y Gobierno de Tecnologías de la Información en la Entidad.

- Falta de direccionamiento estratégico en las actividades de Tecnologías de la Información a causa de la ausencia de un Jefe de OTI en propiedad del cargo.

Descripción del (los) Riesgo(s):

- Inadecuada o falta de implementación de la Política de Gobierno en Línea (Gobierno Digital).
- Pérdidas económicas o estancamiento de los procesos por desarrollo de aplicaciones o herramientas informáticas sin la calidad y resultados esperados, y/o acuerdos de niveles de servicio ineficientes.

Descripción del (los) Impacto(s):

- Desalineación y/o incumplimiento de los objetivos misionales de la ADR con los sectoriales y del Gobierno por no contar con una Arquitectura Empresarial de TI madura y/o robusta.
- Estancamiento u obstrucción de los procesos que dependen de TI por inexistencia de Acuerdos de Niveles de Servicio – ANS.
- Incumplimientos normativos por inobservancia de políticas de TI (Gobierno Digital, Seguridad de la Información y Servicios Ciudadanos Digitales).

Recomendación(es): Es necesario que la Entidad trabaje en la implementación de los lineamientos de Gobierno Digital y maduración del control interno de TI, o bien, que explore la posibilidad de contratar un consultor que apalanque la adopción de estas prácticas. También se incentiva a la participación en mesas de trabajo con entidades del sector y con el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC). En todo caso, se recomienda inspeccionar la página web de Arquitectura Empresarial Colombia (www.mintic.gov.co/arquitecturati/), en donde se describen los dominios y ámbitos de aplicación de estas políticas según las mejores prácticas en materia de TI.

De otra parte, entre tanto que se vincula un servidor público en propiedad del cargo Jefe OTI, es importante que el funcionario encargado de actividades asociadas a las funciones de la Oficina de Tecnologías de la Información:

- Propenda porque el Cuerpo Directivo de la Entidad tenga conocimiento pleno o esté enterado con la oportunidad requerida de las necesidades, prioridades y requerimientos de la OTI, entre ellos, recurso humano, arquitectura empresarial, procesos de conversión a estándares como el Protocolo de Internet versión 6 -IPv6 (Resolución 2710 de 2017 MINTIC) y la implementación de las Políticas de Gobierno Digital y Seguridad y Privacidad de la información, entre otras que el gobierno emita para tales fines.

- Elabore un plan de trabajo o proyecto que, en la medida de lo posible sea flexible pero que de cumplimiento a las directrices mínimas de implementación de las normas y/o políticas de TI, de tal manera que al momento de un empalme con la persona que asuma en propiedad el cargo de Jefe OTI, no se experimenten rezagos, traumatismos o carencias que impidan el logro de los objetivos de la ADR que están apalancados en el componente de Tecnologías de la Información -TI.

Respuesta del Auditado: Aceptado Parcialmente

Justificación: "*Se acepta el hallazgo parcialmente, debido a que la implementación de la Resolución Nº 0409 del 3 de julio de 2019, está siendo transitoriamente implementada, para que sean adoptadas por el personal de la Agencia y los procesos sean alineados conforme a la Resolución. Por otra parte, con la adquisición e implementación de Aranda se contempló e incluyeron los servicios que mencionan en el hallazgo, como se expuso en su momento en una reunión sostenida con la Oficina de Control Interno –OCI.*"

Causa(s) identificada(s) por el Responsable del Proceso Auditado:

- Insuficiencia de personal y/o dificultades en la contratación del recurso humano con las competencias para asumir y ejecutar las actividades misionales y estratégicas de TI de la Entidad.

- Falta de estructuración y/o actualización del PETI de la Agencia de Desarrollo Rural.
- Falta de fortalecimiento y/o implementación de la Estrategia y Gobierno de Tecnologías de la Información en la Entidad.
- Falta de direccionamiento estratégico en las actividades de Tecnologías de la Información a causa de la ausencia de un Jefe de OTI en propiedad del cargo.

Plan de Mejoramiento:

ACCIÓN(ES) PROPUESTA(S)	META(S)	TIPO DE ACCIÓN	RESPONSABLE(S)	FECHA INICIAL	FECHA FINAL
1. Comunicar a los Directivos de la Entidad, por medio del Comité Institucional de Gestión y Desempeño, la importancia de contar con personal para realizar las actividades que deben desarrollarse con miras a la implementación de la Política de Gobierno Digital. **2.** Formular el PETI considerando los lineamientos del MINTIC en la materia. **3.** Generar capacidades de Arquitectura Empresarial en la Agencia, conforme al marco de referencia dispuesto por el MINTIC.	**1.** Presentación Comité Institucional de Gestión y Desempeño. **2.** PETI presentado y aprobado en el Comité Institucional de Gestión y Desempeño. **3.** Avanzar en el análisis situacional de Arquitectura Empresarial considerando la totalidad de los dominios.	Correctiva	1. OTI 2. Equipo de Transformación Digital dispuesto por el Comité Institucional de Gestión y Desempeño 3. OTI	1-ago-19	31-dic-19

Concepto de la Oficina de Control Interno: Aceptado con Observaciones.

Una vez analizada la información remitida por los responsables del proceso auditado designados para atender la auditoría, la Oficina de Control Interno precisa que:

- El sustento y justificación indicados no desvirtúan las situaciones identificadas por el equipo auditor y presentadas en este hallazgo, por el contrario, las ratifican; además, no se identifica la razón por la que se aduce la aceptación parcial, toda vez que se confirma que la Política de Seguridad y Privacidad de la Información está en implementación (situación que está descrita en el hallazgo), por lo que, se considera pertinente aclarar que en los archivos de la Oficina de Control Interno (virtuales y/o

físicos) reposan los registros, papeles de trabajo y demás evidencias que soportan las afirmaciones contenidas en este hallazgo, los cuales se encuentran disponibles para consulta de las partes interesadas, previa solicitud formal de las mismas.

- El plan de mejoramiento propuesto es aceptado en razón a que las acciones de mejoramiento establecidas guardan correspondencia con las causas determinadas para este hallazgo; no obstante, en las acciones Nº 1 y 3 se indicó a la "*OTI*" como responsable de su ejecución, más no se especificó el equipo humano responsable (nombre y rol) de adelantar las gestiones necesarias para su cumplimiento, por lo que, la Oficina de Control Interno recomienda registrar esta información en el plan de mejoramiento, en atención a los lineamientos sobre controles expedidos por el Departamento Administrativo de la Función Pública (DAFP), los cuales indican que los encargados de ejecutar el control no pueden ser áreas, sino que más bien, se deben detallar los roles de quienes las efectuarán.

  Respecto al responsable de la acción Nº 2 "*Equipo de Transformación Digital dispuesto por el Comité Institucional de Gestión y Desempeño*", se insta a confirmar preliminarmente si es factible la conformación de dicho equipo, considerando los factores presupuestales, acciones de encargados y proceso de contratación, dado que, si no se da este escenario el plan de mejoramiento quedaría sin encargado directo de su ejecución.

  Adicionalmente, en la meta N° 3 es necesario indicar específicamente de qué manera se avanzará en el análisis situacional, pues no se plantea el mecanismo que ayudará a determinar el grado de implementación de la Arquitectura Empresarial (ejemplo: listas de chequeo, auto-diagnósticos acompañados de pruebas que sustenten los avances por dominios, consultorías, entre otros). Así las cosas, para la fecha final (31 de diciembre de 2019) se recomienda analizar la probabilidad de que la implementación de dichos esquemas sea factible.

HALLAZGO N° 4. Incumplimiento en los términos de ejecución y reporte del grado de avance de los productos del Plan de Acción Institucional.

Descripción: En cumplimiento de la condición especial N° 9 establecida en el procedimiento "*Formulación, seguimiento y ajustes a plan de acción y plan estratégico institucional*" (PR-DER-008), en el marco del desarrollo de esta auditoría al proceso "Gestión de Tecnologías de la Información", la Oficina de Control Interno realizó seguimiento a los Planes de Acción Institucionales aprobados para las vigencias 2018 y 2019, por lo que verificó el registro de información en el módulo "Medición" del aplicativo ISOLUCIÓN y avances con corte al 31 de diciembre de 2018 y 31 de mayo de 2019 respectivamente, respecto al cumplimiento de los productos y actividades asociadas al proceso auditado, encontrando las siguientes situaciones:

a. Reporte de avances extemporáneos, teniendo en cuenta las fechas de cumplimiento establecidas para las actividades, y/o reporte de avances sin las evidencias suficientes que permitieran corroborar el grado de avance o ejecución reportado:

ACTIVIDAD	OBSERVACIÓN(ES)
VIGENCIA 2018	
PRODUCTO: Infraestructura tecnológica para operación de los sistemas de información de la ADR adecuada.	
Contar con servicios de conectividad estable e independiente	La actividad debió cumplirse el 30-mar-2018; no obstante, en reporte de ISOLUCION del 30-abr-2018 se observó que ésta se desarrolló por medio de la Orden de Compra N° 27719 del 19-abr-2018 por valor de $83'585.838, a través de la cual la Agencia de Desarrollo Rural (ADR) amparó la contratación del Servicio de Conectividad entre las sedes de la Entidad; así las cosas, se evidenció que si bien la actividad se completó, su cumplimiento excedió los tiempos límite fijados.
PRODUCTO: Plan Estratégico de TI (PETI) para la gestión de la información de la entidad construido.	
Ajustar el Plan Maestro de TI	En reporte de ISOLUCION del 30-jun-2018 se anexó como evidencia el documento "*Plan Maestro TI Plan Estratégico de Tecnologías de Información 2018-2022 (Versión 1)*" y un listado de asistencia de una reunión llevada cabo el 20-jun-2018 cuyo objetivo fue "*Conocer el Marco de Arquitectura Empresarial IT4T*"; no obstante, al 30-jun-2019 "*la Oficina de Control Interno no logró establecer las acciones ejecutadas en la vigencia 2018, debido a que el documento adjunto no contenía fecha de emisión y éste registraba actividades o iniciativas del año 2017*", tal como se observó y registró en el Informe OCI-2019-003 "Evaluación de la Gestión Institucional por Dependencias a 31 de diciembre de 2018" emitido el 31-ene-2019. Adicionalmente, el objetivo de la reunión del 20-jun-2018 fue una socialización.
Revisar los criterios, sub-criterios y lineamientos de la política de Gobierno Digital y el Marco de Referencia para determinar el nivel de cumplimiento de la entidad.	En reporte de ISOLUCION del 31-mar-2018 se registró: *"Se revisaron los criterios y lineamientos de acuerdo a la Matriz de Seguimiento y Evaluación del MRAE, enmarcada en la política de Gobierno Digital, (…)"*; no obstante, en los soportes presentados, la Oficina de Control Interno evidenció que de 93 criterios y/o lineamientos, 24 (26%) registraban algún grado de avance, es decir, no se realizó la revisión de la totalidad de los criterios, sub-criterios y lineamientos de la política de Gobierno Digital.

ACTIVIDAD	OBSERVACIÓN(ES)
PRODUCTO: Plan de intervención de Sistemas de Información de la Agencia ejecutado.	
Diseñar el Plan de intervención de Sistemas de Información de la Agencia	Al 30-jun-2019 la Oficina de Control Interno no obtuvo evidencia que corroborara el cumplimiento de estas dos (2) actividades que conformaban el producto, por lo cual, se mantiene la observación presentada en el informe OCI-2019-003 "Evaluación de la Gestión Institucional por Dependencias a 31 de diciembre de 2018" emitido el 31-ene-2019 en relación a que, la Oficina de Tecnologías de la Información (dependencia responsable del proceso auditado) *"(...) no suministró documentación que permitiera determinar su grado de avance o cumplimiento (...)"*.
Ejecutar el Plan de intervención de Sistemas de Información de la Agencia	
PRODUCTO: Plan de Seguridad y Privacidad de la Información.	
Actualización activos de información e inventario bases de datos	No se observaron soportes de los activos de información de las 13 Unidades Técnicas Territoriales (UTT) y de 14 de los 21 procesos que conformaban el mapa de procesos de la Entidad en la vigencia 2018. Adicionalmente, en las matrices de activos de información de los siete (7) procesos que se observaron, no se evidenció la fecha de actualización, toda vez, que tales matrices no contenían fecha de diligenciamiento o actualización.
PRODUCTO: Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.	
Declaración de Aplicabilidad	Al 30-jun-2019 la Oficina de Control Interno no obtuvo evidencia que corroborara el cumplimiento de estas actividades que conformaban el producto, por lo cual, se mantiene la observación presentada en el informe OCI-2019-003 "Evaluación de la Gestión Institucional por Dependencias a 31 de diciembre de 2018" emitido el 31-ene-2019 en relación a que, la Oficina de Tecnologías de la Información (dependencia responsable del proceso auditado) *"(...) no suministró documentación que permitiera determinar su grado de avance o cumplimiento (...)"*.
Análisis de Riegos por Proceso	
Consolidación Plan de Tratamiento de Riesgos	
VIGENCIA 2019	
PRODUCTO: Documento para la planeación estratégica en TI.	
Analizar la estrategia de TI de la entidad y generar informe	En reporte de ISOLUCION del 30-abr-2019 se registró *"Está en proceso la contratación del recurso humano que nos va a apoyar en el desarrollo de estas actividades*", de lo que, al 18-jun-2019 la Oficina de Control Interno no observó registro(s) adicional(es) que indicaran el cumplimiento de la actividad, teniendo en cuenta que la fecha límite de cumplimiento se había establecido hasta el 31-may-2019.
PRODUCTO: Servicios de información actualizados.	
Definir el plan para la gestión de los proyectos de los Sistemas de Información a actualizar.	En los reportes de ISOLUCION realizados en enero y febrero de 2019 se registró *"Se realizó actualización a la página WEB de la ADR (Contenidos, link,) de acuerdo a solicitudes de la Oficina de Comunicaciones de la ADR"*; no obstante, la evidencia presentada no correspondía a la actividad evaluada. Además, al 30-abr-2019 el grado de avance o cumplimiento reportado en ISOLUCION para el producto era de 0%, lo que permite concluir que la actividad no se ejecutó al 28-feb-2019 (fecha límite de cumplimiento establecido), por lo tanto, continúa pendiente de cierre.

ACTIVIDAD	OBSERVACIÓN(ES)
PRODUCTO: Servicios de información implementados.	
Definir el plan para la gestión de los proyectos de los Sistemas de Información.	Esta actividad tenía fecha de cumplimiento 28-feb-2019, y en los reportes de enero a abril de 2019 realizados en ISOLUCION se registró que: *"(…) no realizó actividades relacionadas con este indicador, no se cuenta con el recurso humano"*, lo que permite concluir que la actividad no se ha ejecutado.
PRODUCTO: Plan de Seguridad y Privacidad de la Información con seguimiento.	
Realizar y ejecutar el Plan de Auditoria	Esta actividad tenía fecha de cumplimiento 30-abr-2019, y en los reportes de enero a abril de 2019 realizados en ISOLUCION se registró que: *"(…) no realizó actividades relacionadas con este indicador"*, lo que permite concluir que la actividad no se ha ejecutado.

b. El valor reportado en "Cumplimiento" de los siguientes productos presentó diferencias con el valor recalculado por la Oficina de Control Interno, como se presenta a continuación, teniendo en cuenta el último período informado o reportado a la fecha de esta auditoría.

Nota: La fórmula de cálculo del cumplimiento de los productos se estableció así: *(Actividades realizadas / Actividades planeadas) * 100*

ÚLTIMO PERÍODO INFORMADO	ACTIVIDADES REALIZADAS	ACTIVIDADES PLANEADAS	% DE AVANCE ISOLUCION	% DE AVANCE RECALCULADO OCI	% DE DIFERENCIA
VIGENCIA 2018					
PRODUCTO: Infraestructura tecnológica para la operación de sistemas de información de la ADR adecuada.					
Dic-2018	3,9	4	95	97.5	-2.5
PRODUCTO: Plan Estratégico de TI (PETI) para la gestión de la información de la entidad construido.					
Oct-2018	2,25	4	100	56.3	43.7
PRODUCTO: Plan de intervención de Sistemas de Información de la Agencia ejecutado.					
Dic-2018	0	2	95	0	95
PRODUCTO: Plan de Seguridad y Privacidad de la Información					
Nov-2018	4	5	85	80	5
VIGENCIA 2019					
PRODUCTO: Servicios tecnológicos					
Abr-2019	0.33	2	33	16.5	16.5

Las situaciones mencionadas contravienen lo establecido en la actividad 11 del numeral 6 del procedimiento "*Formulación, Seguimiento y Ajustes a Plan de Acción y Plan Estratégico Institucional*" (PR-DER-008) que establece la responsabilidad de todas las dependencias de *"(…) reportar los avances y cargar las evidencias que correspondan en la herramienta dispuesta para tal fin*" (Subrayado fuera de texto), dado que la debilidad o incongruencia de los soportes de las actividades, además de desconocer la realización de las mismas, conlleva a error en el cálculo de los avances del caso.

Posible(s) Causa(s) identificada(s) por la Oficina de Control Interno:

- Falta de delimitación o definición de los datos de entrada, sus fuentes y soportes, requeridos para el cálculo adecuado de los indicadores de cumplimiento de los productos.
- Fallas, errores u omisiones en el momento de realizar los reportes de avances en el aplicativo ISOLUCIÓN por parte de los encargados del proceso.
- Falta de capacitación sobre la formulación de indicadores de medición claros y suficiencia de la evidencia que respalda los planes de acción planteados.

Descripción del (los) Riesgo(s): Inobservancia del Plan de Acción Institucional.

Descripción del (los) Impacto(s):

- Incumplimiento de las metas, productos e indicadores establecidos en la Planeación Estratégica de la Entidad.
- Reportes de información o rendiciones de cuentas sobre la gestión de tecnologías de información con posibles errores, omisiones o inexactitudes.
- Sobreestimación (o subestimación) del estado real de la Oficina de Tecnologías de la Información, sus avances y necesidades.
- Posibles incumplimientos normativos con las sanciones legales correspondientes.

- Eventuales procesos disciplinarios contra los funcionarios encargados de reportar o actualizar los planes de acción institucionales en virtud de ejercicio negligente de sus funciones.

Recomendación(es): Teniendo en cuenta que los responsables del proceso auditado incluyeron en los Planes de Acción Institucional (Vigencia 2018 y 2019) indicadores que responden al cumplimiento de las normativas relacionadas con Gobierno Digital, Seguridad y Privacidad de la Información y Arquitectura Empresarial (todos ellos con cobertura dentro del PETI), se insta a que la Oficina de Tecnologías de la Información (dependencia responsable del proceso auditado), apoyada en el acompañamiento de la Oficina de Planeación, ejecute las siguientes actividades con el fin de evitar incumplimientos o incongruencias en el reporte de avance de las actividades o hitos establecidos en el Plan de Acción:

- Se asigne a personal específico de la dependencia para realizar el reporte en el aplicativo ISOLUCION, evitando variar o rotar a los encargados, y así conservar la uniformidad en la presentación de la información.

- Se capacite al personal asignado sobre cómo deben construirse los indicadores de cumplimiento/seguimiento de los productos contenidos en los Planes de Acción Institucional. En este punto, deberían abordarse temas como: validez, suficiencia y competencia de la evidencia a suministrar, fuentes de origen de los datos utilizados para el cálculo de los indicadores, frecuencia de reporte y señales de alerta frente a posibles rezagos para cumplir las metas, entre otros que se consideren relevantes.

- Establecer esquemas de monitoreo supeditados a la frecuencia de cumplimiento de los indicadores, es decir, conforme a un cronograma previamente establecido. Para el efecto, se pueden parametrizar alertas de Outlook o diseñar un tablero de control que se pueda actualizar con base al resultado de reuniones semanales (o con la periodicidad que se determine al interior de la dependencia), que permitan corroborar los avances y acciones pendientes, con el fin de tomar los correctivos del caso que

permitan ajustar o solicitar una oportuna modificación de los términos de cálculo de los indicadores.

Respuesta del Auditado: Aceptado

Causa(s) identificada(s) por el Responsable del Proceso Auditado:

- Falta de capacitación sobre la formulación de indicadores de medición claros y suficiencia de la evidencia que respalda los planes de acción planteados.
- Falta de delimitación o definición de los datos de entrada, sus fuentes y soportes, requeridos para el cálculo adecuado de los indicadores de cumplimiento de los productos.
- Fallas, errores u omisiones en el momento de realizar los reportes de avances en el aplicativo ISOLUCIÓN por parte de los encargados del proceso.

Plan de Mejoramiento:

ACCIÓN(ES) PROPUESTA(S)	META(S)	TIPO DE ACCIÓN	RESPONSABLE(S)	FECHA INICIAL	FECHA FINAL
Se asigne a personal específico de la dependencia para realizar el reporte en el aplicativo ISOLUCION, evitando variar o rotar a los encargados, y así conservar la uniformidad en la presentación de la información.	Disminuir los errores u omisiones en el momento de reportar los avances en el aplicativo ISOLUCION por parte de los encargados de la OTI.	Correctiva	Equipo Humano de la OTI	1-ago-19	21-ago-19
Se capacite al personal asignado sobre cómo deben construirse los indicadores de cumplimiento/seguimiento de los productos contenidos en los Planes de Acción Institucional. En este punto, deberían abordarse temas como: validez, suficiencia y competencia de la evidencia a suministrar, fuentes de origen de los datos utilizados para el cálculo de los indicadores, frecuencia de reporte y señales de alerta frente a posibles rezagos para cumplir las metas, entre otros que se consideren relevantes.	Realizar la capacitación sobre formulación de medición y establecer la suficiencia de la evidencia que respalda el plan de acción.	Preventiva	Equipo Humano de la OTI	2-sep-19	16-sep-19

ACCIÓN(ES) PROPUESTA(S)	META(S)	TIPO DE ACCIÓN	RESPONSABLE(S)	FECHA INICIAL	FECHA FINAL
Establecer esquemas de monitoreo supeditados a la frecuencia de cumplimiento de los indicadores, es decir, conforme a un cronograma previamente establecido, diseñando un tablero de control en la herramienta planner donde se actualicen los resultados de reuniones quincenales, que permitan corroborar los avances y acciones pendientes, con el fin de tomar los correctivos del caso que permitan ajustar o solicitar una oportuna modificación de los términos de cálculo de los indicadores.	Definición de los datos de entrada, sus fuentes y soportes, con el fin de realizar el cálculo adecuado de los indicadores de cumplimento de los productos.	Correctiva	Equipo Humano de la OTI	1-ago-19	31-dic-19

Nota: *La relación detallada del equipo humano de la Oficina de Tecnologías de la Información (OTI) responsable de cada acción propuesta se encuentra registrada en papeles de trabajo de la Oficina de Control Interno.*

Concepto de la Oficina de Control Interno: Aceptado con Observaciones.

Analizado el plan de mejoramiento propuesto por los responsables del proceso auditado, la Oficina de Control Interno lo acepta en razón a que las acciones de mejoramiento establecidas guardan correspondencia con las causas determinadas para este hallazgo; no obstante, recomienda completar o definir metas concretas que puedan ser medibles y verificables del cumplimiento del plan de mejoramiento, debido a que se describe en la meta "*Disminuir los errores u omisiones (…)*" y "*Definición de los datos de entrada, (…)*" sin registrar un producto, un resultado a obtener después de emprender las acciones específicas o una herramienta de medición, como por ejemplo, reporte(s) de errores u omisiones para analizar la disminución, entre otras.

HALLAZGO N° 5. Falta de instrumentación de mecanismos para la aplicación de la Política de Seguridad y Privacidad de la Información e incumplimiento de controles para la instalación de software.

Descripción: En virtud de la adopción de la "Política de Seguridad y Privacidad de la Información" a través de la Resolución 0409 el 3 de julio de 2019, esta Oficina de Control Interno realizó una verificación de los controles y actividades existentes tendientes a su implementación, en lo que identificó la necesidad de que la Entidad fortalezca los

controles, debido a que los actuales son insuficientes para abordar las situaciones de riesgo derivadas, tales como, el acceso a / uso inapropiado de código fuente de los aplicativos, entre otras, como se describe a continuación:

POLÍTICA RESOLUCIÓN 0409 de 2019 (ADR)	**OBSERVACIÓN(ES)**
ARTÍCULO SÉPTIMO. Política de Control de Acceso. "*Los propietarios de los activos de información y teniendo en cuenta el tipo de activo, deberán establecer medidas de control de acceso: a nivel de red, sistema operativo, sistemas de información, servicios de tecnologías (…).*"	No se identificó un control relacionado con seguridad o restricciones de acceso a código(s) fuente de las aplicaciones por parte de los funcionarios y/o contratistas, más allá de la cláusula incluida en los contratos de prestación de servicios (en el caso de contratistas).
ARTÍCULO DÉCIMO. Política de Seguridad de las Operaciones. "*La Oficina de Tecnologías de la Información (…), velará por la eficiencia de los controles asociados a los recursos tecnológicos protegiendo la confidencialidad, integridad y disponibilidad de la información, y para que los cambios efectuados sobre los recursos tecnológicos y sistemas de información en ambientes de prueba y producción sean controlados y debidamente autorizados*."	
ARTÍCULO OCTAVO. Criptografía. "*La Oficina de Tecnologías de la Información brindará a solicitud herramientas que permitan el cifrado para proteger la confidencialidad, integridad y disponibilidad de la información clasificada y reservada, (…)*"	No se evidenció la existencia de un control relacionado con protección de información clasificada y reservada a través de cifrado u otro método de criptografía.

De otra parte, el procedimiento "Gestión de Solicitudes de Tecnología" (PR-GTI-002) establece en el literal g) del numeral 5 *"Condiciones Especiales"* que: "*Las solicitudes de las áreas que no hagan parte de la Oficina de Tecnologías de la Información, que impliquen la instalación de licenciamiento u otro aplicativo, deberá contar con la previa aprobación de la Oficina de Tecnologías de la Información, teniendo en cuenta lo dispuesto en las Políticas de Seguridad de la Información".* (Subrayado fuera de texto)

Para efectos de verificar el cumplimiento de tal condición, la Oficina de Control Interno seleccionó una muestra aleatoria de veinte (20) equipos de cómputo, tanto de la Sede Central (CAN) como del Edificio World Business Port (WBP) asignados a diferentes dependencias, para lo que el 8 de julio de 2019 realizó un ejercicio de descarga para instalación de un software libre (Acrobat Reader) obteniendo como resultado que, en tres

(3) equipos (15% de la muestra) el sistema permitió que el usuario ejecutara la instalación del software sin evidenciarse alertas o restricciones del Administrador para evitarlo:

SERIAL EQUIPO	DEPENDENCIA
ADR 02378	Vicepresidencia de Gestión Contractual
ADR 02232	Oficina de Comunicaciones
ADR 02135	Punto de Atención al Ciudadano (WBP)

Cabe mencionar que, el incumplimiento de este lineamiento había sido evidenciado y revelado anteriormente por la Oficina de Control Interno el 7 de marzo de 2019 mediante la emisión del informe "*OCI-2019-008 Seguimiento al Cumplimiento de las Normas de Derechos de Autor y Uso de Software"* en el numeral 3 "*Mecanismos de control para evitar la instalación de Software no Licenciado*" (específicamente en la página 11); no obstante, por los resultados obtenidos en esta prueba se concluye que la Oficina de Tecnologías de la Información no adoptó las medidas correctivas pertinentes para dar cumplimiento a lo establecido en el procedimiento.

Posible(s) Causa(s) identificada(s) por la Oficina de Control Interno:

- Falta o insuficiente identificación de riesgos asociados a salvaguardar la información de la Entidad.
- Falta o inadecuada parametrización de los sistemas mediante los cuales se establecen los permisos y accesos de controles de cambio en los equipos de cómputo.
- Omisión o falta de implementación de mecanismos de control o revisiones periódicas que aseguren el cumplimiento de los procedimientos establecidos, en relación con la Política de Seguridad y Privacidad de la Información.
- Insuficiencia de recurso humano en la Oficina de Tecnologías de la Información a raíz de restricciones presupuestales o requerimientos de perfiles específicos que dificultan la asignación y distribución de las labores de Seguridad de la Información.

Descripción del (los) Riesgo(s):

- Apropiación indebida por parte de un funcionario del licenciamiento, código fuente y/o derechos de autor de un software desarrollado con ocasión de satisfacer necesidades de la Agencia.

- Pérdida de información por accesos inadecuados, no autorizados y/o ausencia de controles que facilita la realización de actividades no permitidas sin posibilidad de trazabilidad y/o rastreo.

- Uso de software no licenciado

Descripción del (los) Impacto(s):

- Fuga o robo de información, acceso abierto a datos o a información reservada, confidencial o restringida por parte de terceros no autorizados.

- Uso inadecuado de información.

- Violación de leyes de derechos de autor o de habeas data.

- Corrupción en divulgación de software no licenciado o no autorizado para su reproducción.

- Multas o sanciones pecuniarias contra la Entidad y sus Representantes Legales y servidores públicos involucrados en manejo no autorizado (licenciado) de software.

Recomendación(es):

- Tanto por buenas prácticas como para el cumplimiento de los requerimientos de la Política de Gobierno Digital y de Seguridad y Privacidad de la Información, se insta a que la Oficina de Tecnologías de la Información efectúe un auto-diagnóstico actualizado sobre el nivel de madurez de su sistema de control interno en TI, con el fin de identificar riesgos y las brechas de los requerimientos frente a las necesidades y recursos de la Entidad para cumplir sus actividades misionales, institucionales y

sectoriales; de tal manera que, se diseñen los proyectos y hojas de ruta a emprender dentro de los objetivos del Plan Estratégico de Tecnologías de la Información (PETI).

Para lo anterior, puede resultar útil que la OTI recopile los hallazgos u observaciones identificados por la Oficina de Control Interno como resultado de otras actividades que involucran a dicha Oficina (por ejemplo, Derechos de Autor) e identifique y ejecute mecanismos de seguimiento o monitoreo a los planes de acción diseñados (por ejemplo, tableros de control, reuniones periódicas semanales, mensuales o con la periodicidad que se requiera), para mitigar la materialización de los riesgos que en su momento se identificaron.

- Es importante que el funcionario encargado de actividades asociadas a las funciones de la Oficina de Tecnologías de la Información participe activamente en los Comités Directivos de la Entidad (o en los comités que para el efecto existen en la ADR) para que visibilice en estas instancias la preponderancia de los proyectos de cumplimiento normativo de Gobierno Digital y Seguridad y Privacidad de la Información, con el objetivo de obtener recursos para sus actividades estratégicas (humanos, financieros, infraestructura etc.). Para lograr lo anterior, se recomienda tomar el autodiagnóstico sugerido y exponer las falencias actuales de la OTI.

- Finalmente, se deben instrumentar mecanismos que permitan poner en operación los términos de la Política de Seguridad y Privacidad de la Información; entre ellos se sugiere considerar la ejecución de pruebas de Ethical Hacking (herramienta para descubrir vulnerabilidades de TI en la Entidad), la instalación de filtros o controles de acceso a información sensible (cifrado, requisitos de autenticación, establecimiento de niveles de autorización para el acceso a este tipo de data y/o descargas), entre otras. Todas estas rutas deberían ser identificadas en las matrices de riesgo-control de la OTI y diseñar los procedimientos que coadyuven a su logro.

Respuesta del Auditado: Aceptado

Causa(s) identificada(s) por el Responsable del Proceso Auditado:

- Falta de parametrización de los sistemas mediante los cuales se establecen los permisos y accesos de controles de cambio en los equipos de cómputo.
- Falta de mantenimiento correctivo – preventivo en los equipos tecnológicos de la ADR
- Insuficiencia de recurso humano en la Oficina de Tecnologías de la Información a raíz de restricciones presupuestales o requerimientos de perfiles específicos que dificultan la asignación y distribución de las labores de Seguridad de la Información

Plan de Mejoramiento:

ACCIÓN(ES) PROPUESTA(S)	META(S)	TIPO DE ACCIÓN	RESPONSABLE(S)	FECHA INICIAL	FECHA FINAL
Se tiene una Política de Grupo (GPO por sus siglas en inglés) que será apoyada con los sistemas de información de Antivirus y Aranda, los cuales ayudarán a administrar las restricciones para la instalación de software de los usuarios, la cual restringe instalaciones en los equipos de la ADR que se encuentran dentro del dominio.	Brindar un sistema más seguro que no admita instalaciones de software sin autorización de la OTI.	Correctiva	Equipo Humano de la OTI	26-jul-19	31-dic-19
Dar continuidad al cronograma de mantenimientos correctivos – preventivos, el cual permita determinar de manera precisa los problemas en los computadores de los funcionarios y corregirlos de manera inmediata.	Detectar de manera presencial el estado actual del hardware y software de los computadores de la ADR.	Preventiva	Equipo Humano de la OTI	26-jul-19	31-dic-19
Se contratará personal calificado para la creación de las Políticas de Control de Acceso, Política de Seguridad de las Operaciones y Política de Criptografía, con el fin de contar con estas al interior de la Entidad.	Contratación de personal calificado para dar respuesta a las labores de seguridad de la información.	Correctiva	Equipo Humano de la OTI	15-ago-19	31-dic-19

Nota: *La relación detallada del equipo humano de la Oficina de Tecnologías de la Información (OTI) responsable de cada acción propuesta se encuentra registrada en papeles de trabajo de la Oficina de Control Interno.*

Concepto de la Oficina de Control Interno: Aceptado con Observaciones.

Analizado el plan de mejoramiento propuesto por los responsables del proceso auditado, la Oficina de Control Interno lo acepta considerando que da cobertura a las causas principales identificadas; no obstante, recomienda completar o definir metas concretas

para medir el cumplimiento del plan de mejoramiento, debido a que se describe en la meta "*Brindar un sistema más seguro (…)*", "*Detectar de manera presencial (…)*" y "*Contratación de personal (…)*" sin registrar una herramienta de medición, como por ejemplo, la cantidad de equipos en los que se verificará la parametrización, cantidad de políticas creadas e implementadas, entre otras.

HALLAZGO N° 6. Gestión de incidentes de seguridad de la información y desarrollo de software sin el cumplimiento de los lineamientos procedimentales.

Descripción: En la evaluación del cumplimiento de los procedimientos "Gestión de Incidentes de Seguridad de la Información" (PR-GTI-004) y "Desarrollo de Software" (PR-GTI-003), la Oficina de Control Interno observó:

- **Procedimiento "Gestión de Incidentes de Seguridad de la Información"** (PR-GTI-004), en el cual se estipulan lineamientos que buscan prevenir la materialización de los incidentes de seguridad de la información, a través de su oportuna detección y correcto reporte, con el fin de dar un tratamiento eficaz y efectivo para mitigar los riesgos de pérdida de la confidencialidad, integridad y disponibilidad de la información de la Agencia de Desarrollo Rural, por lo que, la Oficina de Control Interno verificó el cumplimiento de los siguientes aspectos contemplados en los ítems 3 al 5 del numeral 5 "Condiciones Especiales" del procedimiento mencionado, relacionados con incidentes de seguridad de la información:

  - 3. "*Para su correcta gestión, todos los incidentes deberán estar clasificados. Un incidente que contenga múltiples clases o tipologías debe ser clasificado por el evento de seguridad original. (…). Clasificación de incidentes. Basado en Guía Técnica Colombiana 27035:2012*."

  - 4. "*Para su correcta gestión, todos los incidentes de seguridad de la información deberán estar clasificados según su criticidad y la afectación a la Agencia, (…). Prioridad de Incidentes. Para establecer la criticidad se deben tener en cuenta los criterios de impacto y urgencia, (…)"*

- 5. *"Los Incidentes de Seguridad de la Información que se consideren en categoría de criticidad baja serán atendidos por el Gestor de incidentes de Seguridad de la Información; los que se clasifiquen en categoría Media o Alta, serán atendidos convocando a los equipos de respuesta los cuales estarán liderados por el Gestor de la Oficina de Tecnologías de la Información , y se conformaran por el Dueño y el custodio de la información, de acuerdo con la Matriz de Levantamiento de activos de información."*

En virtud de lo anterior, la Oficina de Control Interno solicitó a los responsables del proceso auditado, la base de datos contentiva de todos los incidentes de seguridad de la información presentados en la Agencia de Desarrollo Rural - ADR entre septiembre de 2017 y mayo de 2019, a lo cual, la Oficina de Tecnologías de la Información (dependencia responsable del proceso auditado) mediante correo electrónico del 11 de julio de 2019 contestó con el reporte de dos (2) eventos registrados en el aplicativo ARANDA y presentados en la Unidad Técnica Territorial Nº 10 – Pasto el 18 de octubre de 2018, descritos a continuación:

- Caso Nº 1687. *"(…). En el día de hoy he recibido llamadas a mi celular por parte de personas que han recibido el siguiente mensaje: Rama Judicial. Consejo Judicial de la Judicatura. Notificaciones y Citaciones (DEAJ). (…). Boleta de citación a juzgado 5to penal del distrito, con énfasis a declaraciones por el proceso (...) llevado en su contra. (...)."*

- Caso Nº 1719. *"(…), me permito reportar situación ocurrida con mi cuenta de correo institucional, cuya contraseña tuvo que ser cambiada de forma inmediata, debido al ingreso de varios correos sospechosos en la bandeja de salida que notifican un pago de dinero a personas ajenas a mí. Solicito amablemente revisar el tema para poder acceder a la cuenta con la debida garantía de seguridad. (…)."*

Al respecto, la Oficina de Control Interno solicitó la entrega de información que evidenciara la atención de los incidentes de seguridad reportados, de acuerdo con lo establecido en el procedimiento PR-GTI-004, y a través de correo electrónico del 11

de julio de 2019, la Oficina de Tecnologías de la Información informó: "*(…). De parte de la OTI realizamos procedimientos que permitieron contener el evento. Este fue un evento aislado. Por otro lado, no se siguieron los pasos del procedimiento descrito en el documento PR-GTI-004 por desconocimiento. En la OTI estamos trabajando en un nuevo procedimiento de Incidentes de seguridad de la información, ajustado a las necesidades actuales de la ADR.*"; es decir que, para la gestión de los dos (2) incidentes de seguridad de la información reportados, la Oficina de Tecnologías de la Información no realizó la aplicación de las directrices documentadas para tal fin.

- **Procedimiento "Desarrollo de Software"** (PR-GTI-003) en el cual se establecen actividades relacionadas con la elaboración de un producto de software, que garanticen la calidad y seguridad en las fases de su definición, implementación y despliegue. De esta manera, la Oficina de Control Interno corroboró el cumplimiento de la secuencia de las actividades indicadas en el numeral 6 *"Desarrollo"* del procedimiento, por lo que, solicitó a la Oficina de Tecnologías de la Información una relación de software desarrollado entre septiembre de 2017 y mayo de 2019 acompañado de una descripción de su funcionamiento, obteniendo el siguiente detalle:

NOMBRE SOFTWARE	OBJETIVO DEL SOFTWARE
Categoría: **Servicios informativos digitales**	
Página Web	*Página web de la Entidad con el objeto de publicar la información relevante para la comunidad, las entidades de control y los funcionarios de la Agencia de Desarrollo Rural.*
Centro de Información Rural de Colombia - CENTIR	*El Centro de Información Rural – CENTIR es una herramienta web que difunde indicadores e información estadística de la ADR, DANE y de otras entidades del sector para la toma de decisiones y el control ciudadano. Esta herramienta difunde información de manera estática, donde se carga periódicamente y de manera manual la información. Sin embargo, se tiene proyectado que inter-opere con sistemas como el Banco de Proyectos e información del DANE para que la información expuesta sea dinámica y en tiempo real.*

NOMBRE SOFTWARE	OBJETIVO DEL SOFTWARE
Categoría: **Sistemas Misionales**	
Consulta SISBEN	*Servicio de consulta de la información consolidada de SISBEN.*
Gestión de Proyectos	*Permitir la integración de los diferentes proyectos manejados por las vicepresidencias del ADR de manera centralizada permitiendo la generación de informes únicos y consistentes para cada una de sus fases Iniciativas, Estructuración, Evaluación e Implementación.*
Adecuación de Tierras	*Gestión de la Información del Portafolio de Adecuación de Tierras. Aplicación que soporta el Servicio de Adecuación de Tierras: estudios y diseños, obras necesarias e implementación.*

Del listado anterior, la Oficina de Control Interno seleccionó como muestra aleatoria dos (2) software denominados: "*Centro de Información Rural de Colombia - CENTIR*" y "*Gestión de Proyectos*", evidenciando las siguientes situaciones:

- El numeral 6, actividad 2 del procedimiento "*Desarrollo de Software*" (PR-GTI-003) establece que en el documento "*Plan de Proyecto*", entre otros aspectos se *"(...), realiza la estimación de los recursos del proyecto, (…)"*; no obstante, en el numeral 8 "*Presupuesto*" del documento "*Acta Constitución del Proyecto V 1.0 (…) "CENTIR""* emitido el 5 de febrero de 2018, no se evidenció una estimación desagregada de los recursos (humanos, físicos, financieros y/o tecnológicos) necesarios y puestos a disposición para la ejecución del proyecto de desarrollo de software.

- En la revisión de los archivos compartidos por la Oficina de Tecnologías de la Información el 4 de julio de 2019, no se identificó evidencia o registro de la ejecución de las siguientes actividades, de acuerdo con las establecidas en el numeral 6 del procedimiento PR-GTI-003:

  - **Centro de Información Rural de Colombia – CENTIR**. No se evidenciaron los documentos: Casos de uso (actividad 3), Plan de Pruebas y Aceptación de la versión (actividad 7) y Plan de Despliegue (actividad 8).

- **Gestión de Proyectos**. No se evidenciaron los documentos: Plan del Proyecto (actividad 2), Casos de uso (actividad 3), Plan de Pruebas y Aceptación de la versión (actividad 7), Plan de Despliegue (actividad 8) y Manuales de usuario (actividad 9).

Adicionalmente, respecto al "Aceptación de la versión" del software "Gestión de Proyectos" se observaron los documentos: *"Acta Entrega Seguimiento a la Gestión de Proyectos"* y *"Acta Reunión Entrega Gestión Proyectos"* emitidos el 21 de enero de 2019; no obstante, éstos no corresponden a la aceptación de la versión, considerando *"(...) que el Proyecto se entregó a Producción en agosto 15 de 2018"*.

De otra parte, considerando que tanto el software CENTIR y Gestión de Proyectos se encuentran en producción, se asume la aceptación de los softwares desarrollados; no obstante, no se observaron los documentos que en virtud del procedimiento PR-GTI-003 se deben emitir.

- El literal e) del numeral 5 establece que: *"Todo el código fuente de los productos nuevos y de los cambios realizados debe estar documentado. El estándar de documentar el código es el siguiente: (...) • Los archivos donde contiene código fuente, al inicio deben contener como mínimo el autor, una descripción y una fecha de creación. (...)"*; no obstante, en los archivos que contienen el código fuente del software CENTIR y Gestión de Proyectos, la Oficina de Control Interno no evidenció el cumplimiento de dichos atributos.

  Adicionalmente, el mencionado literal establece que *"(...) • Cuando se realice una modificación se debe incluir el autor de la modificación y la fecha de modificación"*; no obstante, la Oficina de Control interno no evidenció ni el autor y ni la fecha de la modificación realizada a los software CENTIR y Gestión de Proyectos, aun cuando se observa en el Catálogo de Sistemas de Información remitido por la Oficina de Tecnologías de la Información el 4 de julio de 2019, que la última fecha de actualización de estos software se realizó en junio y agosto de 2018, respectivamente.

Posible(s) Causa(s) identificada(s) por la Oficina de Control Interno:

- Desconocimiento parcial de los procedimientos aplicables para la gestión de los incidentes de seguridad y el desarrollo de software al interior de la Agencia de Desarrollo Rural – ADR por parte de los funcionarios y contratistas designados para el desarrollo de las respectivas actividades.

- Inadecuada supervisión contractual que permitiera garantizar la gestión de los incidentes de seguridad de la información y el desarrollo de software bajo los lineamientos procedimentales establecidos por la Oficina de Tecnología de la Información.

Descripción del (los) Riesgo(s):

- Pérdidas económicas o estancamiento de los procesos por desarrollo de aplicaciones o herramientas informáticas sin la calidad y resultados esperados, y/o acuerdos de niveles de servicio ineficientes.

- Afectación de la continuidad de las operaciones por inoportunidad o inadecuada solución de incidentes y/o atención de éstos sin una categorización de riesgo e impacto (valoración).

Descripción del (los) Impacto(s):

- Falta de uniformidad en la evidencia documental del desarrollo de nuevos software.

- Posible estancamiento de la operatividad de los programas desarrollados en virtud de no contar con un repositorio definido y estándar para su creación y la gestión de incidentes.

- Subvaloración en tipología y criticidad de un incidente de seguridad de la información, que probablemente revista mayor importancia de la otorgada, genere importantes afectaciones en la operación de la Entidad y haya requerido una mejor atención y gestión para su mitigación.

Recomendación(es):

- Realizar un diagnóstico de las labores y dinámicas de la operación del proceso Gestión de Tecnologías de la Información y contrastar el resultado con los términos de los procedimientos asociados y vigentes, a fin de validar la existencia de brechas y planteamiento de acciones para su correspondiente cierre, identificando la actualización o ajustes pertinentes en los lineamientos. Una vez se culmine esta actividad, se recomienda realizar su divulgación al personal de la OTI y a nuevos funcionarios o contratistas al momento de su vinculación.

- Alinear y supeditar la ejecución de las actividades que se planteen en los procedimientos a los deberes que deben acreditar los contratistas para respaldar el cumplimiento de sus obligaciones, lo que significa incluir estas actividades mínimas como responsabilidades en los contratos de prestación de servicios. Otra alternativa consiste en manejar listas de chequeo o mapa de actividades relacionadas por sub-temas: gestión de incidentes, desarrollo de software, navegabilidad, etc.

Respuesta del Auditado: Aceptado

Causa(s) identificada(s) por el Responsable del Proceso Auditado:

- Desconocimiento parcial de los procedimientos aplicables para la gestión de los incidentes de seguridad y el desarrollo de software al interior de la Agencia de desarrollo Rural – ADR por parte de los funcionarios y contratistas designados para el desarrollo de las respectivas actividades.

- Inadecuada supervisión contractual que permitiera garantizar la gestión de los incidentes de seguridad de la información y el desarrollo de software bajo los lineamientos procedimentales establecidos por la Oficina de Tecnología de la Información.

Plan de Mejoramiento:

ACCIÓN(ES) PROPUESTA(S)	META(S)	TIPO DE ACCIÓN	RESPON SABLE(S)	FECHA INICIAL	FECHA FINAL
Se modificarán los procedimientos "Gestión de incidentes de seguridad de la información" y "Desarrollo de software" actualizándolos en la plataforma ISOLUCION.	Procedimientos acorde a las políticas de la Oficina de Tecnologías de la Información	Correctiva	Equipo Humano de la OTI	15-ago-19	31-ago-19
Se hará divulgación del procedimiento "Desarrollo de software" a los ingenieros designados por el Jefe de la Oficina de Tecnologías de la Información.	Personal capacitado en los procedimientos de la Oficina de Tecnologías de la Información	Correctiva	Equipo Humano de la OTI	1-sep-19	30-sep-19
Alinear y supeditar la ejecución de las actividades que se planteen en los procedimientos a los deberes que deben acreditar los contratistas para respaldar el cumplimiento de sus obligaciones.	Elementos que permitan la obtención de productos que den cumplimento con los procedimientos de la Oficina de Tecnologías de la Información	Correctiva	Equipo Humano de la OTI	1-oct-19	31-dic-19

Nota: *La relación detallada del equipo humano de la Oficina de Tecnologías de la Información (OTI) responsable de cada acción propuesta se encuentra registrada en papeles de trabajo de la Oficina de Control Interno.*

Concepto de la Oficina de Control Interno: Aceptado con Observaciones.

Analizado el plan de mejoramiento propuesto por los responsables del proceso auditado, la Oficina de Control Interno lo acepta en razón a que las acciones de mejoramiento establecidas guardan correspondencia con las causas determinadas para este hallazgo; no obstante, es pertinente indicar respecto a las metas definidas las siguientes observaciones, para su análisis y ajuste:

- Meta: "*Personal capacitado en los procedimientos de la Oficina de Tecnologías de la Información.*" Es necesario que se defina puntualmente el resultado de la acción, porque aunque se plantea el escenario buscado (que todos los ingenieros queden capacitados en la materia), no se indica la manera en la que se medirá el resultado, como por ejemplo, evaluación del entendimiento de las políticas sobre las cuales se capacita, nivel de asistencia a estos espacios, etc.

- Meta: "*Elementos que permitan la obtención de productos que den cumplimento con los procedimientos de la Oficina de Tecnologías de la Información*." La meta no es clara, pues no estipula un producto final que permita medir el grado de ejecución de

dicha acción, en particular, la atención de los incidentes de seguridad o el desarrollo de software In-house. En este sentido, es necesario indicar la manera en la que se instrumentarán las obligaciones de los contratistas y los requisitos que acreditarán su cumplimiento.

HALLAZGO N° 7. Incumplimiento de los procedimientos establecidos para la generación y almacenamiento de las copias de seguridad de las bases de datos.

Descripción: El instructivo "Generación y Administración de Copias de Seguridad de las Bases de Datos" (DE-GTI-003) contiene directrices y actividades específicas en su numeral 5 para el "*desarrollo de las actividades de copia de seguridad de información*", respecto a:

- **Determinación del crecimiento de las bases de datos**. Ítem 5.4. *"Verificar los servicios del motor de bases de datos y recursos del Servidor. (…) Se debe comprobar que los dispositivos de almacenamiento que se definan para albergar las copias de seguridad posean el espacio libre suficiente para almacenamiento. Este espacio se proyectará de acuerdo con el crecimiento de las bases de datos objeto de copia de seguridad"*.

- **Programación de la ejecución de copias de seguridad.** Ítem 5.3. *"Se realiza la programación de la copia se seguridad diaria y semanal en el rango de las 12 a.m. a 5 a.m."*

- **Verificación del cumplimiento de la copia de seguridad en el almacenamiento.** Ítem 5.6. "*De acuerdo con la frecuencia de la copia de seguridad definida (…), se descargan los archivos de respaldo de las copias de seguridad del almacenamiento en el servidor de bases de datos, mediante código T-SQL. Se realiza la validación de consistencia e integridad de la copia de seguridad, la cual arroja como resultado un indicador que informa el estado de la copia de seguridad*."

- **Verificación de la consistencia del respaldo.** Ítem 5.7. *"Realizar una verificación aleatoria de tres bases de datos en el semestre de cada servidor de base de datos*

que se encuentre bajo la administración de la Oficina de Tecnologías de la Información".

- **Reporte.** Ítem 5.8. "*Realizar un informe detallado trimestralmente de las anteriores actividades y presentar al Jefe de la Oficina*"

En consonancia con lo anterior, la Oficina de Control Interno solicitó el listado de las bases de datos que tenía la Agencia de Desarrollo Rural (ADR) a 31 de mayo de 2019 y seleccionó una muestra de quince (15) de ellas, con el fin de comprobar la ejecución de las actividades antes descritas por parte de la Oficina de Tecnologías de la información (dependencia responsable del proceso auditado), en lo que identificó las siguientes situaciones:

Descripción de la muestra seleccionada:

SERVIDOR - INSTANCIA	BASE DE DATOS	MOTOR
SRVBANPROYSQL01-MSSQLSERVER	ADR_ProjectWebApp	Microsoft SQL Server 2016
SRVBANPROYSQL01-MSSQLSERVER	StateServiceDB	Microsoft SQL Server 2016
SRVCENTIRPORT01-MSSQLSERVER	PRODUCTORES360	Microsoft SQL Server 2014
SRVBANPROYSQL01-MSSQLSERVER	DB_Adjuntos_ADR	Microsoft SQL Server 2016
SRVBANPROYSQL01-MSSQLSERVER	DBProyectos	Microsoft SQL Server 2016
SRVCENTIRPORT01-MSSQLSERVER	ACTUALIZACION_RGU	Microsoft SQL Server 2014
SRVCENTIRPORT01-MSSQLSERVER	ADECUACION_TIERRA	Microsoft SQL Server 2014
SRVCENTIRPORT01-MSSQLSERVER	ASISTENCIA_TECNICA	Microsoft SQL Server 2014
SRVCENTIRPORT01-MSSQLSERVER	CENTIR_SDMX	Microsoft SQL Server 2014
SRVCENTIRPORT01-MSSQLSERVER	DBProyectos	Microsoft SQL Server 2014
SRVBANPROYSQL01-MSSQLSERVER	ADR_BancoProyectos_Reporting	Microsoft SQL Server 2016
SRVDBADR01	SGD_ORFEO	Microsoft SQL Server 2014
SRVDBADR01	Isolucio40Produccion	Microsoft SQL Server 2014
SRVNOMDB	NOMIPROD	Oracle Database 11g Release 11.2.0.4.0
SRVBANPROYSQL01-MSSQLSERVER	Master	Microsoft SQL Server 2016

Descripción de las situaciones identificadas:

a. No fue presentada la información de siete (7) bases de datos (47% de la muestra), informando las siguientes razones.

BASE DE DATOS	JUSTIFICACIÓN
PRODUCTORES360	*"(…) no presentan actividad debido a que fueron creadas con un propósito específico de consulta, por lo tanto son estáticas en su crecimiento y no se presenta variación en su tamaño y sobre las cuales no se presenta información."*
ACTUALIZACION_RGU	
DBProyectos	
Master	"*Base de datos propias del motor las cuales son auto-creadas al momento de configurar la instancia en el servidor y generalmente no se presenta variación en su tamaño y sobre las cuales no se presenta información.*"
ADR_BancoProyectos_Reporting	"*No se reporta actividad ya que las funciones de administrador de bases de datos no estaban contratadas*"
ASISTENCIA_TECNICA	
DBProyectos	

Respecto a las observaciones previamente expuestas por los responsables del proceso auditado para las bases de datos PRODUCTORES360, ACTUALIZACION_RGU, DBProyectos y Master, en relación a que estas "*(...) no presentan actividad debido a que fueron creadas con un propósito específico de consulta, por lo tanto son estáticas en su crecimiento y no se presenta variación en su tamaño (…)*", es importante mencionar que el ítem 5.4 del Instructivo DE-GTI-003 no contempla excepciones o diferencias en el tratamiento de las bases de datos para el registro y análisis de crecimiento histórico, en virtud de su propósito (consulta o producción) o su origen de creación.

Adicionalmente, para seis (6) bases de datos (ADR_ProjectWebApp, StateServiceDB, DB_Adjuntos_ADR, CENTIR_SDMX, SGD_ORFEO, NOMIPROD), si bien fue remitido un archivo Excel donde se relaciona su tamaño inicial, final y promedio (en términos de Megabytes - MB), no fue posible por parte de la Oficina de Control Interno validar la oportunidad en la ejecución del control de determinación de crecimiento histórico, toda vez que esta evidencia registraba fecha de modificación del 10 de julio de 2019, por lo cual, da lugar a la generación de dudas razonables ante terceros sobre

el origen de ejecución del control. Para confirmar la inquietud expuesta, la Oficina de Control Interno se reunió con el administrador de bases de datos de la Entidad el 15 de julio de 2019, quien mencionó que *"(...) en el momento no hay evidencia documental para corroborar la oportunidad para ejecutar el control"*, situación que dificulta por parte de cualquier órgano de control o tercero establecer el cumplimiento de los términos del ítem 5.4 del Instructivo DE-GTI-003 citado al comienzo de este documento.

De otra parte, tampoco fue posible por parte de la Oficina de Control Interno validar la oportunidad en la ejecución del control relacionado con la verificación de la consistencia e integridad de la copia de seguridad realizado para siete (7) bases de datos (ADR_ProjectWebApp, StateServiceDB, DB_Adjuntos_ADR, ACTUALIZACION_RGU, CENTIR_SDMX, SGD_ORFEO, NOMIPROD) según los términos del ítem 5.6 del Instructivo DE-GTI-003, toda vez que, si bien fue entregado un archivo Excel donde se relacionaba un resultado de verificación, éste presentaba la misma condición de la evidencia citada previamente (registraba fecha de modificación del 10 de julio de 2019) y con la misma conclusión de falta de evidencia documental.

b. El horario de programación de la ejecución de la copia de seguridad de catorce (14) bases de datos (93% de la muestra) se observó programado entre las 20:00 y 23:59 horas, el cual no corresponde al establecido en el ítem 5.3. del Instructivo DE-GTI-003.

c. No se evidenció la verificación del cumplimiento de la copia de seguridad en el almacenamiento de cinco (5) bases de datos (33% de la muestra), de conformidad con lo establecido en el numeral 5.6. del Instructivo DE-GTI-003.

Adicionalmente, para la base de datos "Master" no fue presentada por parte del equipo auditado la evidencia solicitada por la Oficina de Control Interno mediante correo electrónico del 5 de julio de 2019, aduciendo que son "*Bases de datos propias del motor las cuales son auto-creadas (sic) al momento de configurar la instancia en el*

servidor y generalmente no se presenta variación en su tamaño (…)". Al respecto, esta Oficina de Control interno reitera que el procedimiento no contempla excepciones, además de considerar que no pierde su calidad de base de datos administrada por la Oficina de Tecnologías de la Información, sujeta a las condiciones y requisitos descritos en el Instructivo DE-GTI-003.

d. Respecto a la verificación de la consistencia del respaldo y generación de reportes (ítems 5.7 y 5.8 del instructivo DE-GTI-003), los responsables del proceso auditado mediante correo electrónico del 9 de julio 2019 suministraron las "Planillas de Generación de Respaldo de Bases de Datos" de los servidores con la siguiente información:

SERVIDOR – INSTANCIA	FECHA BACKUP	
	2018	2019
SRVDBADR01	31-ago-18	31-may-19
DSRVPORTALSQL01\SQLSHP2023		
SRVBANPROYSQL01-MSSQLSERVER		
SRVCENTIRPORT01-MSSQLSERVER		
SRVDBADR011\PORTALESTADISTIC		No se evidenció planilla

En el análisis efectuado a la evidencia suministrada, se determinó que ésta no corresponde a la ejecución del control o que aborda su cumplimiento parcial, por las siguientes razones:

- La evidencia versa sobre el registro de la ejecución del ítem 5.1. "*Periodicidad en que se realiza el respaldo de la información*" del Instructivo DE-GTI-003, mas no al informe detallado de la ejecución de todas las actividades del instructivo DE-GTI-003.

- Las planillas registran la ejecución de copias de seguridad de dos (2) meses específicos (agosto de 2018 y mayo de 2019); no obstante, no se evidenciaron los reportes del segundo, tercero y cuarto trimestre de la vigencia 2018 y primer

trimestre de la vigencia 2019, de conformidad con lo establecido en el ítem 5.8 del mencionado Instructivo.

De otra parte, los responsables del proceso auditado mencionaron respecto a la entrega de reportes al Jefe de la OTI, a través de correo electrónico del 9 de julio de 2019, que: "*Los informes (...) se entregan en los informes de actividades y/o se almacenan en el sitio documental del (SIC) OTI*"; no obstante, es pertinente precisar que los informes de actividades presentados con ocasión de la ejecución de los contratos de Prestación de Servicios (367 y 580 de 2018 y 246 de 2019) son elaborados en cumplimiento de las obligaciones contractuales suscritas entre los contratistas y la Agencia de Desarrollo Rural – ADR, mas no corresponden a los informes que deben ser elaborados en virtud del Instructivo DE-GTI-003, más aun considerando que allí no se detalla específicamente la ejecución de cada una de las actividades del citado Instructivo.

Posible(s) Causa(s) identificada(s) por la Oficina de Control Interno:

- Insuficiencia de personal adscrito a la Oficina de Tecnologías de la Información para ejercer las funciones de administrador de bases de datos en reemplazo del contratista con ocasión de la culminación del contrato y durante el periodo de trámite administrativo para su renovación.

- Desconocimiento de los lineamientos procedimentales establecidos para la administración de las bases de datos por parte de los responsables de este rol.

- Falta de compromiso por parte de los funcionarios y/o contratistas en la apropiación e interiorización de los lineamientos procedimentales establecidos para la administración de las bases de datos a cargo de la OTI.

Descripción del (los) Riesgo(s):

- Inadecuada administración de datos y/o toma de decisiones por información no confiable, inoportuna e inexacta.

- Imposibilidad de recuperación de la información por ausencia y/o generación, disponibilidad y custodia inadecuada de las copias de seguridad de las bases de datos institucionales.

Descripción del (los) Impacto(s):

- Pérdida de información de las bases de datos que alimentan los softwares misionales, de apoyo y/o estratégicos de la Entidad ante un posible fallo de los sistemas de información que obligue a la restauración de las copias de seguridad.

- Ausencia de evidencia que permita corroborar la ejecución de obligaciones contractuales y/o funciones ante posibles solicitudes de información por parte de los entes de control y/o investigaciones disciplinarias.

- Re-procesos de actividades ejecutadas por los servidores públicos (funcionarios y contratistas) de la Entidad.

Recomendación(es): Es necesario que la Oficina de Tecnologías de la Información como dependencia responsable del proceso auditado, evalúe y analice la implementación de los siguientes cursos de acción:

- Disminuir la intervención manual en el proceso, es decir, se explore la posibilidad de automatizar las tareas de copias de seguridad y administración de bases de datos. Esto podría lograrse a través de la generación de Jobs (tareas programadas), réplica de scripts (sentencias a través de códigos) o formulación de macros, para así evitar que se incurra en olvidos u omisiones y garantizar el cumplimiento de las actividades que se especifiquen en los instructivos o manuales operativos.

- Revisar, ajustar, fortalecer y/o establecer nuevos controles en el Instructivo DE-GTI-003, a través de la documentación de la dinámica operativa de la gestión de tecnologías de información. Para el efecto, se insta a la consulta y aplicación de los términos de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas -Riesgos de Gestión, Corrupción y Seguridad Digital, como

también, buscar el acompañamiento de la Oficina de Planeación para lograr estos fines.

- Ejecutar reuniones y/o capacitaciones con cada grupo de trabajo establecido al interior de la Oficina de Tecnologías de la Información, en las cuales se socialicen y debatan los lineamientos procedimentales y normatividad aplicable para la ejecución de sus funciones, identificando vulnerabilidades, brechas, oportunidades y demás aspectos en la ejecución de labores.

- Alinear o vincular el quehacer operativo con la documentación existente y aquella nueva que se genere, a fin de fortalecer las evidencias y trazabilidad de los procedimientos que garanticen la oportunidad y réplica de su ejecución. Así las cosas, debería analizarse alternativas como la generación de notificaciones, reportes, alertas de correo o logs de auditoría, una vez los jobs o rutinas programadas culminen, según la frecuencia estipulada para su funcionamiento.

Respuesta del Auditado: Aceptado Parcialmente

Justificación: "***Punto a. <u>No Aceptado</u>:*** *La verificación de los recursos de los servidores de bases de datos se realiza para efectos prácticos y de control, sobre las bases de datos en constante actividad u operación, para el caso de estas bases de datos (PRODUCTORES360, ACTUALIZACION_RGU, DBProyectos y Master), las cuales fueron creadas con el objetivo de implementar aplicaciones que en su momento no se subieron a producción; por lo tanto, son bases de datos que en tamaño no impacta el cálculo que se realiza sobre el almacenamiento disponible que se debe contar en cada servidor para el alojamiento temporal de la copia de seguridad. (…).*

Como evidenció la Oficina de Control Interno -OCI en las dos (2) visitas realizadas a la OTI relacionadas con el procedimiento "Generación y Administración de Copias de Seguridad de las Bases de Datos" y tal como quedó consignado en el documento "Listado de Asistencia a Reuniones" en el apartado acta de reunión "se verificó en sitio, de qué manera el ingeniero genera la información histórica de tamaños de bases de datos", se

comprueba que a través de una sentencia "select" se invoca la base y se muestra el histórico referido. Dentro de las evidencias solicitadas por la OCI, se observa que la información relacionada a este control se almacena dentro de los servidores de bases de datos y se genera para efectos del control de forma visual o para los informes que solicitó la OCI. De otra parte, no existe dentro del procedimiento la obligatoriedad de llevar evidencia documental al respecto. Es importante recalcar que, la información utilizada para efectos del monitoreo de los recursos del servidor permanece generada en los servidores de bases de datos, pero no se genera capturas de pantalla de la misma, solo reportes a solicitud. (…).

En la misma línea del punto inmediatamente anterior, la información de la realización de las copias de seguridad queda almacenada en los servidores de bases de datos; por lo tanto, es de allí que se genera los reportes o informes solicitados, los cuales están disponibles a cualquier momento para efectos de las validaciones o comprobaciones que se requieran. En la visita de la OCI, se mostró con un ejercicio real como se realiza el procedimiento de verificación de las copias de seguridad y el resultado visualizado en la consola de administración de bases de datos y sobre el cual se le informó a la OCI que no se toman capturas de pantallas de este resultado. Si se llegase a encontrar inconsistencias en estas verificaciones, es responsabilidad del encargado de la administración de las bases de datos tomar los correctivos inmediatos y necesarios para corregir estas inconsistencias. (…).

Punto b. <u>No Aceptado</u>: *En este punto se debe aclarar que se manejan dos (2) horarios para las copias de seguridad, el primero corresponde al establecido en el motor de bases de datos el cual es definido de acuerdo con criterios de oportunidad, operación y duración de la copia de seguridad; el segundo horario corresponde a la programación de la copia desde el agente de backup de Azure (Cloud) el cual se programó en el rango de horario definido en el ítem 5.3 del Instructivo DE-GTI-003. (…).*

Punto c. <u>No Aceptado</u>: *Las bases de datos, de las cuales no se evidenció el cumplimiento de la copia de seguridad, corresponden a bases de datos que se encuentran en el servidor cuyo rol es de pruebas, esto debido a que durante este año*

2019 no se ha presentado desarrollo de aplicaciones; por lo tanto, no se ha requerido el uso del servidor para estos propósitos; sin embargo, en el mes de diciembre de 2018 se realizó las copias de seguridad sobre las bases de datos que estaban siendo utilizadas de pruebas (…).

La base de datos "Master" propia del sistema, que es creada automáticamente al instalar una instancia de SQL Server, si se realiza copia de seguridad de la misma (…).

***Punto d. <u>Aceptado Parcialmente</u>:** El instructivo DE-GTI-003 menciona en el ítem 5.8 "Realizar un informe detallado trimestralmente de las anteriores actividades y presentar al Jefe de la Oficina" y seguidamente se hace referencia a la "Planilla de generación de respaldo de bases de datos" y no se hace mención de ningún otro informe o se especifica un formato o guía para desarrollarlo como si está especificado dicha planilla, que en resumen, para ser generada se deben cumplir los requisitos o ítems descritos en el instructivo DE-GTI-003.*

Al igual que todas las operaciones realizadas en el cumplimiento del instructivo DE-GTI-003 se almacenan en los servidores de bases de datos (tal como las planillas, tamaño de bases de datos, etc.); estas planillas se pueden generar a solicitud o petición en cualquier momento. No se evidenció planilla del servidor SRVDBADR011\ PORTALESTADISTIC en el año 2019 por la misma razón expuesta en el punto c: "Las bases de datos, de las cuales no se evidenció el cumplimiento de la copia de seguridad, corresponden a bases de datos que se encuentran en el servidor cuyo rol es de pruebas, esto debido a que durante este año 2019 no se ha presentado desarrollo de aplicaciones; por lo tanto, no se ha requerido el uso del servidor para estos propósitos; sin embargo, en el mes de diciembre de 2018 se realizó las copias de seguridad sobre las bases de datos que estaban siendo utilizadas de pruebas (…).

Como se indica en el punto d, "El instructivo DE-GTI-003 menciona en el ítem 5.8 "Realizar un informe detallado trimestralmente de las anteriores actividades y presentar al Jefe de la Oficina" y seguidamente se hace referencia a la "Planilla de generación de respaldo de bases de datos" y no se hace mención de ningún otro informe o se especifica

un formato o guía para desarrollarlo como si está especificado dicha planilla, que en resumen, para ser generada se deben cumplir los requisitos o ítems descritos en el instructivo DE-GTI-003." Esto hace relación a que no se está solicitando ningún informe adicional al mencionado específicamente que es la "Planilla de generación de respaldo de bases de datos" que se genera mensualmente y se anexa como soporte a las actividades realizadas en el marco del contrato de prestación de servicios.

Nos permitimos informar que las tareas relacionadas a las copias de seguridad de las bases de datos se encuentran automatizadas, tanto desde el lado del motor de bases de datos como en el agente de backup de Azure, (…)."

Causa(s) identificada(s) por el Responsable del Proceso Auditado:

- Fortalecer las evidencias y trazabilidad de los procedimientos.
- Automatización de actividades de aseguramiento de recursos de espacio.

Plan de Mejoramiento:

ACCIÓN(ES) PROPUESTA(S)	META(S)	TIPO DE ACCIÓN	RESPONSABLE(S)	FECHA INICIAL	FECHA FINAL
Enviar mensualmente al inicio de cada mes el informe "Planilla de generación de respaldo de bases de datos" por correo electrónico al Jefe de la OTI para su información.	Generar el informe digital "Planilla de generación de respaldo de bases de datos" con la información requerida de las copias de seguridad realizadas con corte a fin de mes.	Preventiva	Equipo Humano de la OTI	1-ago-19	31-dic-19
Enviar mensualmente al inicio de cada mes un informe de la disponibilidad de almacenamiento en cada servidor de base de datos por correo electrónico al Jefe de la OTI para su información.	Generar un informe digital de la disponibilidad de almacenamiento en cada servidor de base de datos con la siguiente información: nombre servidor, volumen (unidad), nombre volumen, capacidad total del volumen, espacio disponible del volumen (espacio libre), porcentaje espacio disponible.	Preventiva	Equipo Humano de la OTI	1-ago-19	31-dic-19
Se programará una tarea que recopilará datos del espacio de almacenamiento en el servidor.					

Nota: *La relación detallada del equipo humano de la Oficina de Tecnologías de la Información (OTI) responsable de cada acción propuesta se encuentra registrada en papeles de trabajo de la Oficina de Control Interno.*

Concepto de la Oficina de Control Interno: No Aceptado.

Una vez analizadas las justificaciones del equipo auditado, esta Oficina de Control Interno expone sus argumentos en el mismo orden en que fueron detallados en su justificación:

Punto a. Se reitera la no aceptación de la exposición, debido a que el procedimiento no contempla excepciones sobre el estado de las bases de datos, es decir, si éstas permanecen estáticas o son auto-creadas por los servidores para aplicar el control; además, es importante tener en cuenta que la naturaleza de este control es manual, lo que significa que su ejecución necesariamente requiere de la intervención del responsable, que para este caso, debe determinar los tamaños de las bases de datos y monitorear su crecimiento (nuevamente, sin perjuicio del propósito o grado de uso de las bases de datos).

Aunque el procedimiento explícitamente no indica que debe documentarse el control, esta Oficina de Control Interno entiende, por la idea previamente citada, que los soportes necesariamente deben corresponder a evidencias verificables y trazables que permitan en cualquier momento determinar la ejecución del control por parte de cualquier tercero o ente de control que desee replicar su realización y, dado que este no es el caso (en virtud de la prueba in situ donde se confirmó que no era posible corroborar el rastro de la ejecución del control), se insta a buscar un mecanismo que corrobore la actividad. Ahora bien, identificamos que el proceder del responsable se basa en la práctica y eficiencia de las acciones, por lo que se plantea la necesidad de analizar si el procedimiento vigente requiere actualizaciones que consideren excepciones y maneras particulares de proceder frente a la actividad.

Punto b. La exposición suministrada indica que existe una consideración adicional de programación (la del motor de base de datos) que no está abordada dentro del procedimiento, por lo que, a la luz de la verificación de cualquier ente de vigilancia y control, se constituye en incumplimiento del Procedimiento (al no detallar su manejo

particular) y por tanto, demanda de la actualización de éste para incluir dicha programación adicional, lo cual redunda en confirmar que no se está desvirtuando el hallazgo frente a los procedimientos documentales auditados.

Punto c. La Oficina de Control Interno no acepta la argumentación entregada, toda vez que, se está entregando evidencia nueva que no fue suministrada en el momento de las pruebas de auditoría y ésta adolece de las mismas características de validez y suficiencia para corroborar la oportunidad de ejecución de la actividad, es decir, el archivo es reciente y genera dudas razonables para cualquier tercero sobre el momento en que se llevó a cabo el control. De otra parte, se refuerza con el mismo hecho descrito en el "punto a", en el sentido de que las excepciones o tratamientos especiales que se aplican no están incluidos o descritos en el procedimiento DE-GTI-003.

Punto d. No se está desvirtuando el hallazgo, toda vez que el equipo auditado está aduciendo que las planillas corresponden al formato del informe trimestral de actividades y que no existe otro formato; no obstante, al hacer la inspección de dicho documento se observa que no contempla los siguientes campos, los cuales corresponden a actividades del procedimiento y que, por lo estipulado en el numeral 5.8 deben detallarse: i) Horario de programación de la copia de seguridad (numeral 5.3 y teniendo en cuenta lo que se comentó en el punto b); ii) Validación del espacio libre y proyección del mismo atendiendo al tamaño de las bases de datos; iii) Automatización y iv) Verificación de la consistencia del respaldo. También es importante aclarar que, por el formato de dicha planilla no es verificable el detalle que se solicita de la actividad, pues sólo se remite a listar instancias y bases de datos con los demás campos. Para el caso de las tareas automatizadas, se insta a informar en los reportes en qué consistió la actividad y cuándo se efectuó, entregando los soportes que a bien se determine para su aprobación por el Jefe OTI.

Respecto al plan de mejoramiento establecido por los responsables del proceso auditado, la Oficina de Control Interno no lo acepta debido a:

- Aunque se registra la utilización de la técnica o herramienta de "Los 5 ¿Por qué?" para análisis de las causas, sus resultados no corresponden a una técnica sistemática de

preguntas que permita llegar a la causa raíz que originó la situación o problema identificado, de tal forma que, cuando no se puede contestar una de las preguntas significa que se ha llegado a la causa raíz del problema. Lo anterior, explica la falta de pertinencia en las causas principales determinadas "*Fortalecer las evidencias y trazabilidad de los procedimientos*" y "*Automatización de actividades de aseguramiento de recursos de espacio*". La finalidad de esta herramienta es que, al encontrar respuestas detalladas a preguntas incrementales, las respuestas se vuelven más claras y concisas cada vez, y lo ideal es que el último "¿Por qué?" conduzca a la falla del proceso o actividad.

- Para la primera y segunda acción de mejoramiento propuesta es necesario que el equipo de la OTI analice si el formato utilizado para el reporte requiere ajustes, toda vez que, no está considerando todos los campos necesarios para demostrar la ejecución de las actividades. Ahora bien, el sólo hecho de diligenciar este reporte no le permite a cualquier tercero trazar la oportunidad en la ejecución de los controles (dado que el envío del reporte es mensual), por lo que se insta a buscar mecanismos que permitan demostrar la ejecución de las actividades en cualquier momento, tales como logs, reportes automáticos de respuesta sobre la terminación de un job o script entre otros pertinentes; por lo tanto, se debe determinar si los procedimientos existentes requieren ajustes respecto de la frecuencia, forma y excepciones en los que se realizan las actividades.

- Para la acción "*Se programará una tarea que recopilará datos del espacio de almacenamiento en el servidor*" en la que se definió como meta "*Generar un informe digital de la disponibilidad de almacenamiento en cada servidor de base de datos (…)*" es necesario fortalecer la evidencia final, de tal manera que, permita a cualquier tercero cerciorarse de que la programación se cumplió conforme a los tiempos declarados, dejando constancias complementarias como correos electrónicos de notificación o logs que permitan concluir sobre la frecuencia de ejecución de las pruebas.

Por lo anterior, la Oficina de Control Interno recomienda identificar claramente la(s) causa(s) por la(s) cual(es) se presentó la deficiencia o incumplimiento reportado en este hallazgo, por lo que, los planes de mejoramiento propuestos deberían ser complementados en relación con tal(es) causa(s), proponiendo actividades que intervengan el proceso de forma estructural para que tal situación no se vuelva a presentar en el futuro y así evitar que los riesgos asociados se materialicen.

Nota: *Aunque en las justificaciones se busca desvirtuar este hallazgo, consideramos pertinente aclarar que en los archivos de la Oficina de Control Interno (virtuales y/o físicos) reposan los registros, papeles de trabajo y demás evidencias que soportan las afirmaciones contenidas en este informe, los cuales se encuentran disponibles para consulta de las partes interesadas, previa solicitud formal de las mismas.*

HALLAZGO N° 8. Navegación web y gestión de solicitudes de tecnologías de la información sin el cumplimiento de los requerimientos establecidos por la Entidad.

Descripción: El manual de operaciones "Política de Navegación Web" (DE-GTI-002) establece directrices sobre los permisos y restricciones de navegación web que tienen los funcionarios y contratistas de la Agencia de Desarrollo Rural (ADR), con el fin minimizar el riesgo ocasionado por el acceso a internet y redes públicas que comprometan la integridad, disponibilidad y confidencialidad de la información de la Entidad. Para el efecto, la Oficina de Control Interno verificó el bloqueo de acceso a páginas web no autorizadas, el otorgamiento de permisos de navegación y la expiración de permisos de acceso y navegación a páginas web, en lo que identificó las siguientes situaciones:

a. Bloqueo de acceso a páginas web no autorizadas.

En una muestra de catorce (14) funcionarios o contratistas (13 del Grupo Navegación General y 1 del Grupo Navegación OTI), se corroboró en sus terminales de trabajo o equipos de cómputo asignados los permisos de acceso o restricciones de navegación web, por lo que se les solicitó acceder con su usuario a las siguientes páginas web:

PÁGINA WEB	LINK/URL DE ACCESO	CATEGORÍA *(Según Política de Navegación Web ADR)*
Grupo de Navegación: GENERAL Y OTI		
You Tube	https://www.youtube.com/?gl=CO&hl=es-419	• Redes Sociales • Entretenimiento • Streaming Radio / TV • Streaming Media
Fox Play	https://foxplay.com/co/forme	• Entretenimiento • Streaming Radio / TV • Streaming Media
Directv Sports	https://www.directvsports.com/	• Entretenimiento • Streaming Radio / TV • Streaming Media • Deportes
Jet Set: Semana	https://www.semana.com/noticias/jet-set/103023	• Entretenimiento
Noticias Caracol	https://noticias.caracoltv.com/	• Entretenimiento • Streaming Radio / TV • Streaming Media
WhatsApp Web	https://web.whatsapp.com/	• Mensajería Instantánea
InfoArmas	https://infoarmas.com.co/	• Armas
Rush Bet	https://www.rushbet.co/?page=sports#filter/all/	• Juegos de Azar
Grupo de Navegación: OTI		
We Transfer	https://wetransfer.com/	• Sitios para Compartir Información
Aprende a Hackear	http://www.aprendeahackear.com/	• Actividades de Hacking/Computer

De lo anterior, se observó que el acceso a las páginas web relacionadas en la tabla que sigue no fue bloqueado por el Firewall de la Agencia de Desarrollo Rural (ADR), en contravía de lo establecido en el Manual de Operaciones "Política de Navegación Web" (DE-GTI-002), en:

- Numeral 4 "*Responsabilidad de la ADR*", literal c) "*La Agencia controlará haciendo uso de mecanismos técnicos el acceso a sitios que puedan afectar la seguridad de la información. (...).*" y literal f) *"La Agencia realiza control a todos los usuarios con acceso al servicio de navegación Web, además de limitar el acceso a determinadas páginas de Internet en horarios de alta demanda, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otra actividad ajena a las tareas relacionadas con el desarrollo de las funciones de la dependencia*."

- Numerales 7, 8 y 9 que determinan las categorías bloqueadas para los diferentes grupos de navegación web. Ejemplo. Numeral 8. "*Los grupos de navegación tienen las siguientes categorías bloqueadas: (...) navegación general: Redes Sociales, Entretenimiento, Streaming Radio / TV, Streaming Media, Deportes, Mensajería Instantánea, Juegos de Azar (...). Navegación OTI: Sitios para Compartir Información, Actividades de Hacking/Computer (...).*"

GRUPO DE NAVEGACIÓN / PÁGINA WEB	GENERAL	OTI	GENERAL	OTI	GENERAL	OTI
	CANTIDAD DE FUNCIONARIOS					
	Evaluados		Con Acceso Restringido		Con Acceso Permitido	
You Tube	13	1	0	0	13	1
Fox Play	13	1	0	0	13	1
Directv Sports	13	1	0	0	13	1
Jet Set: Semana	13	1	0	0	13	1
Noticias Caracol	13	1	10	0	3	1
WhatsApp Web	13	1	0	0	13	1
InfoArmas (*)	4	0	0	N/A	4	N/A
Rush Bet	13	1	0	0	13	1
We Transfer (**)	0	1	N/A	0	N/A	1
Aprende a Hackear (**)	0	1	N/A	0	N/A	1

(*) Para el caso de esta página, se practicó la prueba a un total de cuatro personas.
(**) En virtud de que el grupo de navegación pertenece a la OTI, se hizo la prueba de navegación a estas páginas a una persona de dicha área.

b. Otorgamiento de permisos de navegación.

Los numerales 4 "*Responsabilidad de la ADR*" y 5 "*Responsabilidad de los usuarios de la ADR*" del Manual de Operaciones "Política de Navegación Web" (DE-GTI-002) establece una serie de lineamientos procedimentales para el otorgamiento de permisos especiales de navegación en sitios web restringidos, en los literales:

- Literal d) –numeral 4. *"(...) La Agencia brinda sólo a los usuarios que lo requieran y en cumplimiento de un objetivo misional, la autorización para visitar sitios restringidos por la Agencia de manera explícita o implícita, o sitios que afecten la productividad de la misma. (...)*."

- Literal g) –numeral 4. *"(...) La Agencia cuenta con los procedimientos necesarios para asignación o modificación de permisos de navegación a usuarios, en casos excepcionales,* ***mediante el diligenciamiento del Formato Solicitud Servicios de Tecnología.***" (Negrita y subrayado fuera de texto).

- Literal c) –numeral 5. *"En caso de que el usuario sea autorizado para el acceso a navegación total, este acceso solo se permitirá por un tiempo máximo de tres (3) meses. Finalizado este tiempo será notificado del vencimiento del término concedido y si fuere el caso de necesitar renovación, esta solicitud debe contar con la debida autorización de su jefe inmediato o del supervisor del contrato*."

Adicionalmente, el procedimiento "Gestión de Solicitudes de Tecnología" (PR-GTI-002) establece lineamientos para la solicitud de requerimientos de tecnologías de la información, indicando en el literal b, del numeral 5 que: *"Las solicitudes que requieran contar con el Formato Solicitud Servicios de Tecnología, deberán adjuntarlo debidamente diligenciado, en caso contrario no se gestionará la solicitud"* y en la actividad 4, del numeral 6 que: *"De acuerdo al tipo de solicitud, revisa si requiere que se adjunte formato. (…)".*

En este sentido, con el objetivo de probar la eficacia operativa de los controles para el otorgamiento de permisos especiales de navegación en páginas web, cuya

categoría se encuentra bloqueada considerando el grupo de navegación al que pertenecen los funcionarios o contratistas de la Agencia de Desarrollo Rural (ADR), la Oficina de Control Interno seleccionó una muestra de veintiséis (26) permisos solicitados a través de la mesa de servicio (aplicativo ARANDA) y otorgados entre septiembre de 2017 y mayo de 2019, respecto de los cuales, mediante correo electrónico del 5 de julio de 2019 la Oficina de Control Interno solicitó a la Oficina de Tecnologías de la información la remisión del *"Formato de Solicitud de Servicios de Tecnología"* que debió ser adjuntado en el aplicativo ARANDA al momento de radicación de la solicitud de permisos de navegación; no obstante, mediante correo electrónico del 9 de julio de 2019, fue remitido a esta Oficina el archivo denominado *"Seguimiento a Permisos de Navegación Especial a Usuarios"* en el cual se menciona que ninguno de los veintiséis (26) permisos especiales de navegación otorgados y verificados por la Oficina de Control Interno, adjuntaba en Aranda dicho formato, incumpliendo así los lineamientos procedimentales previamente expuestos.

c. Expiración de permisos de acceso y navegación a páginas web.

En la muestra de los veintiséis (26) permisos otorgados mencionados anteriormente, la Oficina de Control Interno identificó doce (12) permisos o accesos (46% de la muestra) que, de acuerdo con la fecha de solicitud y, considerando el tiempo máximo de activación de tres (3) meses (Literal c), numeral 5 del manual DE-GTI-002), se encontraban expirados a 30 de junio de 2019.

Nº ARANDA	FECHA SOLICITUD	ÁREA / DEPENDENCIA
Permiso especial a: GOOGLE-DRIVE-Y-WETRANSFER		
3050	10-abr-2019	Dirección de Participación y Asociatividad
1206	22-jun-2018	Vicepresidencia de Proyectos
1193	20-jun-2018	Dirección de Activos Productivos
Permiso especial a: ACCESO A PÁGINAS DE AEROLÍNEAS		
857	2-abr-2018	Dirección de Comercialización

Nº ARANDA	FECHA SOLICITUD	ÁREA / DEPENDENCIA
Permiso especial a: ACCESO A YOUTUBE		
1088	25-may-2018	Oficina de Control Interno
990	3-may-2018	VIP
872	6-abr-2018	Dirección Administrativa y Financiera
872	6-abr-2018	Dirección Administrativa y Financiera
Permiso especial a: COMUNICACIONES		
2854	18-mar-2019	Dirección de Participación y Asociatividad
1159	13-jun-2018	Dirección Administrativa y Financiera - Gestión Documental
1102	31-may-2018	Vicepresidencia de Gestión Contractual
Permiso especial a: MEGA		
277	29-dic-2017	Dirección de Asistencia Técnica

Resultado de la validación in situ de las terminales de trabajo o equipos de cómputo a las que se otorgaron los permisos, de acuerdo con las solicitudes de servicio radicadas en el aplicativo ARANDA, la Oficina de Control Interno evidenció en cinco (5) de ellas (casos ARANDA Nº 3050, 2854, 1159 y 872, para este último se tienen en cuenta 2 permisos independientes) que al 30 de junio de 2019 los funcionarios o contratistas responsables del equipo de cómputo aún tenían acceso a las páginas web habilitadas.

Las demás terminales correspondientes a los siete (7) casos de ARANDA restantes, no fueron validadas en virtud de que los funcionarios o contratistas responsables del equipo de cómputo se encontraban en comisión, en un evento institucional o ya no estaban vinculados con la Entidad.

Posible(s) Causa(s) identificada(s) por la Oficina de Control Interno:

- Falta de identificación o cobertura inadecuada de páginas web susceptibles de bloqueo mediante el Firewall para las diferentes categorías restringidas y de acuerdo con los grupos de navegación web establecidos.

- Desconocimiento de los lineamientos procedimentales establecidos para la navegación web.
- Falta o insuficiencia de lineamientos para el adecuado seguimiento a las solicitudes de navegación libre.
- Insuficiencia de recursos de infraestructura o de recursos humanos en la OTI para cumplir con las actividades de supervisión, monitoreo y restricción de navegación web.

Descripción del (los) Riesgo(s): Pérdida de información por accesos inadecuados, no autorizados y/o ausencia de controles que facilita la realización de actividades no permitidas sin posibilidad de trazabilidad y/o rastreo.

Descripción del (los) Impacto(s):

- Disminución de la productividad de los funcionarios y contratistas al tener acceso a páginas web que brinden contenido ocioso.
- Desarrollo de actividades por parte de funcionarios y contratistas en páginas web que por su contenido son consideradas ilegales y/o inapropiadas desde direcciones IP's (Protocolos de Internet) relacionados con la Entidad, que podrían implicar la intervención de entes de control e investigación de delitos informáticos.
- Disminución de la velocidad y el rendimiento de la navegación de la infraestructura de red de la Entidad debido al mayor número de páginas web con acceso.
- Materialización de eventos de phishing (obtención de contraseñas u otros datos) y vulnerabilidades por programas malignos (malware) que pueden permear la infraestructura de red de la Entidad, virus que atenten contra la seguridad y privacidad de la información y logren paralizar la operación de la Entidad.
- Ataques cibernéticos.

Recomendación(es):

- Considerando que las páginas web utilizadas por la Oficina de Control Interno para la validación del bloqueo por el firewall son de fácil acceso mediante una búsqueda por el explorador web "Google" para cada categoría, es pertinente que la Oficina de Tecnologías de la Información (dependencia responsable del proceso auditado) amplíe el espectro de búsqueda de páginas web susceptibles de ser bloqueadas mediante este mecanismo. Se insta a la consulta con otras entidades del sector, así como con proveedores de servicios de Tecnología que cuenten con este tipo de listados, a fin de configurarlos dentro del listado del Firewall, previo análisis del costo/beneficio de inhabilitar accesos a estos sitios web.

- Debido a que la Entidad no cuenta con herramientas de software suficientes que ayuden a monitorear o generar alertas automáticas sobre "picos" de navegación y páginas con mayor demanda de consulta, entre otras versatilidades, se insta a que la Oficina de Tecnologías de la Información considere dentro de sus presupuestos y objetivos estratégicos para el soporte, el acceso a estos mecanismos. Entre tanto, es importante que con el recurso humano disponible se establezcan una serie de actividades periódicas (debidamente monitoreadas por una segunda instancia en el área) que garanticen la cobertura para todo el personal y contratistas de la Agencia de Desarrollo Rural, ayudando a minimizar la materialización de riesgos asociados a seguridad de la información.

- Configurar en el aplicativo ARANDA o establecer un repositorio virtual para el almacenamiento y seguimiento de los permisos especiales de navegación web, previo surtimiento de los controles de autorización por parte de las instancias pertinentes (Jefe de la OTI, Jefes de Área u otras que se consideren). Así mismo, configurar alertas de caducidad de los permisos y/o configurar temporizadores de acceso a las páginas supeditados al período de acceso concedido según los permisos.

- Llevar a cabo reuniones y/o capacitaciones con cada grupo de trabajo establecido al interior de la Oficina de Tecnologías de la Información en las cuales se socialicen y

debatan los lineamientos procedimentales y normatividad aplicable para la ejecución de sus funciones, en este caso específico, relacionado con la implementación de la Política de Navegación Web al interior de la Agencia de Desarrollo Rural (ADR). También se insta a la divulgación de las directrices a todo el personal de la Entidad (funcionarios y contratistas), haciendo pedagogía sobre los peligros y vulnerabilidades que representa un inadecuado uso del internet.

Respuesta del Auditado: Aceptado Parcialmente

Justificación: "*(…).*

a. ***Bloqueo de acceso a páginas web no autorizadas**. En este ítem se identifica el hallazgo en el acceso a algunas páginas que deben estar bloqueadas por su contenido, como es el caso de la de la página web www.infoarmas.com.co, www.rushbet.co. El firewall tiene habilitado filtro web; sin embargo, se evidencia que no se realiza el bloqueo esperado; por esto, se propone la verificación de los filtros web del firewall, con el apoyo del soporte técnico del fabricante Fortinet. Se requiere validar que el firewall tenga las últimas actualizaciones de las firmas de filtros web y actualizarlas si es necesario.*

b. ***Otorgamiento de permisos de navegación.** En este ítem se identifica un hallazgo al comprobar el acceso de algunos usuarios a páginas web, a las cuales no deberían tener acceso según el grupo de navegación al que pertenece; sin embargo, estos usuarios se le asignaron permisos especiales por solicitud justificada de los usuarios. Adicionalmente, se reporta que no está diligenciado el formato de solicitud de servicios tecnológicos anexo a la solicitud de permisos especiales, esta es la razón por la cual, se acepta parcialmente el hallazgo, porque en la nueva política de navegación web (en proceso de aprobación) se requiere sólo la apertura de un caso en la herramienta de gestión Aranda y la aprobación del Jefe del área a través de la misma herramienta o de un correo electrónico. Para este hallazgo se propone como mejora, adelantar la aprobación de la nueva política de navegación web y socializar el procedimiento para la asignación de permisos web especiales.*

c. ***Expiración de permisos de acceso y navegación a páginas web****. En este ítem el hallazgo está relacionado con las fechas límites de caducidad de los permisos especiales otorgados a algunos usuarios. Después de mirar diferentes opciones para realizar el control de caducidad de los permisos, se encuentra que la mejor opción es habilitar la funcionalidad de fecha de expiración de las políticas en el firewall, lo cual realizaría un control automatizado de la caducidad de las políticas web, evitando la necesidad de recurso humano adicional para realizar este control*."

Causa(s) identificada(s) por el Responsable del Proceso Auditado:

- Falta de identificación o cobertura inadecuada de páginas web susceptibles de bloqueo mediante el Firewall para las diferentes categorías restringidas y de acuerdo con los grupos de navegación web establecidos.
- Desconocimiento de los lineamientos procedimentales establecidos para la navegación web.
- Falta o insuficiencia de lineamientos para el adecuado seguimiento a las solicitudes de navegación libre.
- Insuficiencia de recursos de infraestructura o de recursos humanos en la OTI para cumplir con las actividades de supervisión, monitoreo y restricción de navegación web.

Plan de Mejoramiento

ACCIÓN(ES) PROPUESTA(S)	META(S)	TIPO DE ACCIÓN	RESPON SABLE(S)	FECHA INICIAL	FECHA FINAL
Realizar verificación de los filtros web definidos en el firewall con el apoyo del canal de soporte del fabricante -Soluciones Integrales ADSUM. Adicionalmente, gestionar la aprobación de la nueva Política de Navegación Web, ajustada a las necesidades actuales de la ADR.	Revisar los 9 filtros web configurados, correspondientes a los 9 grupos de navegación definidos en la Política de Navegación Web e incluir en las políticas del firewall los nuevos grupos de navegación web definidos en la nueva Política de Navegación Web.	Correctiva	Equipo Humano de la OTI	28-jul-19	27-ago-19

ACCIÓN(ES) PROPUESTA(S)	META(S)	TIPO DE ACCIÓN	RESPONSABLE(S)	FECHA INICIAL	FECHA FINAL
Socializar la nueva Política de Navegación Web con todos los usuarios de la ADR y publicarla en el Sistema Integrado de Gestión (aplicativo ISOLUCIÓN).	En los próximos 15 días, a partir de la aprobación de la nueva Política de Navegación Web, socializarla con el apoyo de la Oficina de Comunicaciones.	Preventiva	Equipo Humano de la OTI	28-ago-19	15-sep-19
Configurar una plantilla de políticas de los permisos especiales, en el firewall con fecha de caducidad.	Ajustar las políticas actuales definidas para permisos especiales durante las últimas dos (2) semanas del mes de septiembre de 2019.	Correctiva	Equipo Humano de la OTI	16-sep-19	30-sep-19
Automatizar los controles actuales en el firewall con el fin de no recurrir a recurso humano adicional para las labores de supervisión, monitoreo y restricción de navegación web.	Automatizar controles en el firewall mediante funcionalidades de calendario para todas las políticas de navegación web especiales.	Preventiva	Equipo Humano de la OTI	1-oct-19	31-oct-19

Nota: *La relación detallada del equipo humano de la Oficina de Tecnologías de la Información (OTI) responsable de cada acción propuesta se encuentra registrada en papeles de trabajo de la Oficina de Control Interno.*

Concepto de la Oficina de Control Interno: Aceptado con Observaciones.

En cuanto a la aceptación parcial del literal b) de este hallazgo, la Oficina de Control Interno considera que la justificación dada no desvirtúa las situaciones observadas por el equipo de auditoria, y al respecto aclara que, la prueba de otorgamiento de permisos no buscó probar la funcionalidad del permiso, sino el aval sobre el permiso concedido por la Oficina de Tecnologías de la Información (OTI), es decir, la existencia del formato de solicitud (diligenciado por el usuario o quien corresponda) debidamente justificado, por lo que, al no contar con ellos se evidenció que la desviación del control en efecto se originó.

Respecto al plan de mejoramiento propuesto por los responsables del proceso auditado, una vez analizado la Oficina de Control Interno no presenta observaciones teniendo en cuenta que las acciones de mejoramiento establecidas guardan correspondencia con las causas determinadas para este hallazgo.

HALLAZGO N° 9. Incumplimiento de lineamientos en el desarrollo de inventario y clasificación de activos de información.

Descripción: El Instructivo *"Desarrollo de Inventario y Clasificación de Activos de Información"* (IN-GTI-001) prevé en su numeral 2 *"Información Mínima"* los campos que se establecen para el levantamiento de Activos de Información. Así mismo, indica en el ítem 1.1 que la identificación se hará de la siguiente manera: *"Desde la Oficina de Tecnologías de la Información se solicitará a los líderes de los procesos, la realización del levantamiento, revisión y/o actualización del inventario de activos de acuerdo con la periodicidad definida y el acompañamiento de los Profesionales de la Oficina de Tecnologías de la Información encargados de la implementación y mantenimiento del Sistema Gestión Seguridad la Información. Se deberá dejar constancia mediante registro la identificación, validación, revisión y/o actualización de los activos de información y sus componentes (...), con la finalidad de que se soporte su aprobación. (...)".*

Al respecto, la Oficina de Control Interno verificó el contenido y estructura del documento "20181214 Activos de Información Consolidado" publicado en la página web de la Entidad (www.adr.gov.co) en el link "*Transparencia y Acceso a la Información / Activos de Información*" e identificó las siguientes deficiencias, teniendo en cuenta lo establecido en el instructivo antes mencionado:

a. Los procesos "*Implementación de Proyectos Integrales*" y "*Fortalecimiento competitivo para la comercialización de productos de origen agropecuario*" no contaban con el inventario de activos de información, situación que fue confirmada por los responsables del proceso auditado mediante correo electrónico el 9 de julio de 2019.

b. En el documento se observaron doscientos diecisiete (217) activos de información inventariados por dieciocho (18) de los veinte (20) procesos con los que contaba la Entidad en la vigencia 2018, en los que se identificaron las siguientes desviaciones con respecto a lo establecido en el instructivo:

   - Dieciocho (18) activos de información no contaban con la información correspondiente a disponibilidad, según lo establecido en el numeral 2 *"Información Mínima"*, ítem II *"Seguridad de la Información. (…). Disponibilidad:*

Tiempo estimado que podría tardar el suministro de la información, en caso de ser requerida por el peticionario (funcionario o ciudadano). El tiempo se puede expresar en: inmediato, horas, días, meses, años u otro." Para efectos de ejemplificar dicha desviación, se exhiben dos (2) casos:

NOMBRE O TÍTULO DE LA INFORMACIÓN Y DESCRIPCIÓN DEL CONTENIDO	PROCESO	DEPENDENCIA RESPONSABLE DE:	
		Producción de la Información	**Custodia y Acceso a la Información**
Instrumentos de Clasificación y Retención Documental: Tablas de Retención Documental (TRD)	Gestión Documental	Secretaría General - Gestión Documental	Secretaría General - Gestión Documental
Tablas de Control de Acceso: Acto administrativo de adopción			

- Veintidós (22) activos de información no contenían datos respecto a la fecha de generación de la información, frecuencia de actualización y lugar de consulta, incumpliendo lo establecido en el numeral 2 *"Información Mínima"*, ítem III *"Esquema de publicación. Fecha de generación de la información: Identifica el momento de la creación de la información. Frecuencia de actualización: Identifica la periodicidad o el segmento de tiempo en el que se debe actualizar la información, de acuerdo a su naturaleza y a la normativa aplicable. Lugar de consulta: Indica el lugar donde se encuentra publicado o puede ser consultado el documento, tales como lugar en el sitio web y otro medio en donde se puede descargar y/o acceder a la información cuyo contenido se describe."* Para efectos de ejemplificar dichas desviaciones, se exhiben dos (2) casos:

NOMBRE O TÍTULO DE LA INFORMACIÓN Y DESCRIPCIÓN DEL CONTENIDO	PROCESO	DEPENDENCIA RESPONSABLE DE:	
		Producción de la Información	**Custodia y Acceso a la Información**
Plan Estratégico de Tecnologías de la Información – PETI: Herramientas administrativas que establecen políticas y estrategias en materia de tecnologías de la información para la ADR.	Gestión de Tecnologías de la Información	Oficina de Tecnologías de la Información	Oficina de Tecnologías de la Información
Informes Organismos de Control: Documento que incluye las respuestas a organismos de control de las actividades que se efectúan en la Oficina de Tecnologías de la Información			

- Dos (2) activos de información con nivel de clasificación "Información pública clasificada" no contaban con el diligenciamiento del "*Índice de información clasificada y reservada (Art. 38 Decreto 103-2015)*", incumpliendo lo estipulado en el numeral 2 *"Información Mínima"*, ítem IV *"Índice de Información Clasificada y Reservada. Aplica únicamente para información catalogada como reservada o publica clasificada"*:

NOMBRE O TÍTULO DE LA INFORMACIÓN Y DESCRIPCIÓN DEL CONTENIDO	PROCESO	DEPENDENCIA RESPONSABLE DE:	
		Producción de la Información	Custodia y Acceso a la Información
Comprobantes de Ingreso de Almacén de Bienes de Consumo: Registros del ingreso de bienes de consumo al Almacén	Gestión Administrativa	Secretaría General - Dirección Administrativa y Financiera	Secretaría General - Dirección Administrativa y Financiera
Nómina: Suma de todos los registros financieros de los sueldos de los empleados, incluyendo los salarios, las bonificaciones y las deducciones.	Gestión Financiera		

Nota: *La información detallada de los activos de información en los que se identificaron las desviaciones se encuentra registrada en los papeles de trabajo elaborados por el auditor que practicó las pruebas; tales papeles son custodiados por la Oficina de Control Interno y se encuentran disponibles para consulta de las partes interesadas, previa solicitud formal de los mismos.*

Adicionalmente, la Oficina de Control Interno solicitó a los responsables del proceso auditado la *"Constancia mediante registro de la identificación, validación, revisión y/o actualización de los activos de información y sus componentes"*, a lo que, mediante correo electrónico el 9 de julio de 2019 se informó: "*No existe constancia en la OTI (…)";* así mismo, tampoco se obtuvo evidencia de la actualización de los activos de información en la vigencia 2019, toda vez que los responsables manifestaron que: *"Se cuenta solo con el levantamiento y/o actualización de los activos de la información hasta el corte del 2018, ya que en el 2019 cambiaron los formatos por ende el área de Planeación de la ADR debe solicitar dichos documentos actualizados de acuerdo a los lineamientos del*

Departamento Administrativo de la Función Pública (DAFP) para el levantamiento y/o actualización de los activos de información (…)".

Posible(s) Causa(s) identificada(s) por la Oficina de Control Interno:

- Ausencia de mecanismos de control o revisiones periódicas que aseguren el cumplimiento de los instructivos o lineamientos relacionados con el inventario y clasificación de activos de información.
- Posible asignación errónea de la responsabilidad de documentar y mantener los registros y actualizaciones de los activos de información.
- Desactualización de los formatos y demás mecanismos para el registro de los activos de información.
- Falta o inadecuada verificación de la integridad de la información recopilada.

Descripción del (los) Riesgo(s): Inadecuada administración de datos y/o toma de decisiones por información no confiable, inoportuna e inexacta.

Descripción del (los) Impacto(s):

- Omisión en el diseño de controles para salvaguardar la información de los procesos.
- Activos de información no inventariados y sin asignación de un responsable de su administración y custodia.
- Generación de información o reportes erróneos, incompletos o inexactos.

Recomendación(es):

- Analizar si los términos del Instructivo "Desarrollo de Inventario y Clasificación de Activos de Información" (IN-GTI-001) continúan vigentes en cuanto a la responsabilidad que le asiste a la Oficina de Tecnologías de la Información de actualizar los registros de activos de información, así como de recopilar y mantener la

evidencia correspondiente, o si por el contrario, debe intervenir la Oficina de Planeación, en cuyo caso, se debe ajustar y actualizar el documento para que las actividades sean ejecutadas por la instancia correspondiente.

- Coordinar con la Oficina de Planeación, la ejecución de actividades que permitan delimitar la periodicidad durante la cual se deben realizar los ejercicios de actualización del inventario de Activos de Información con las áreas, previa actualización y divulgación del formato correspondiente. Se deben buscar alternativas de concientización de la responsabilidad de los procesos en esta tarea (capacitaciones, campañas de expectativa, etc.).

- Solicitar a las áreas que mantengan un inventario propio de sus registros de activos de información, de tal manera que sirva como soporte de los reportes en la plantilla de activos de información y así asegurar su integridad y existencia. Se insta a buscar automatizar este tipo de labores, con el fin de evitar la pérdida o manipulación de la información.

Respuesta del Auditado: Aceptado Parcialmente

Justificación: "*Se acepta el hallazgo parcialmente porque que el formato de activos de información versión 2 fue diligenciado para el 2018, por lo tanto, se realizará el diligenciamiento de los campos en blanco evidenciados por control interno porque el formato está incompleto, con el fin de buscar aprobación del Comité Institucional de Gestión y Desempeño de la Agencia de Desarrollo Rural y proceder a publicar en la página web institucional para lo cual se hará un plan de mejora porque se evidencia que el proceso de Tecnología de la Información tiene el procedimiento "Desarrollo de inventario y clasificación de activos de información", en el cual se diligencia el registro de activos de información, pero para la vigencia 2019 no se ha aprobado ninguna modificación de formato a versión 3, por lo tanto, este formato no se debe usar ya que para nosotros como Oficina de Tecnologías de la Información el vigente es la versión 2 con los datos del año 2018. (…).*

Se evidencia desde los lineamientos del DAFP (Departamento Administrativo de Función Pública) que este formato ya no se publica porque se deben tener publicados los siguientes formatos: Esquema de publicación de información, Índice de información clasificada y reservada, Registro de activos de información como está reportado en su página web y datos abiertos https://www.funcionpublica.gov.co/inventario-de-informacion. Por lo tanto, se debe modificar el formato registro de activos de información y crear uno nuevo, porque es conveniente que este procedimiento se haga desde la Oficina de Planeación y la Oficina de Tecnologías de la Información sea de apoyo para su diligenciamiento."

Causa(s) identificada(s) por el Responsable del Proceso Auditado: Desactualización de los formatos y demás mecanismos para el registro de los activos de información.

Plan de Mejoramiento

ACCIÓN(ES) PROPUESTA(S)	META(S)	TIPO DE ACCIÓN	RESPONSABLE(S)	FECHA INICIAL	FECHA FINAL
Se realizará el diligenciamiento de los campos en blanco.	Terminar de diligenciar los formatos de Activos de la Información 2018 que se encuentran incompletos para que no haya campos vacíos.	Correctiva	Equipo Humano de la OTI	1-ago-19	31-ago-19

***Nota:** La relación detallada del equipo humano de la Oficina de Tecnologías de la Información (OTI) responsable de cada acción propuesta se encuentra registrada en papeles de trabajo de la Oficina de Control Interno.*

Concepto de la Oficina de Control Interno: Aceptado con Observaciones.

Con base al análisis de los argumentos de justificación entregados por los responsables del proceso auditado, la Oficina de Control Interno no identificó los elementos con los cuales se demuestra que se cumplió parcialmente con los lineamientos del instructivo "Desarrollo de Inventario y Clasificación de Activos de Información" (IN-GTI-001), toda vez que, a pesar de haberse diligenciado para 2018 el archivo correspondiente, la labor se ejecutó de manera incompleta, por lo que no se desvirtúa el hallazgo respecto del diligenciamiento (campos en blanco, o incluso, procesos de la Entidad con información faltante).

Respecto a los planes de mejoramiento, la Oficina de Control Interno observa que aunque se identificaron una serie de causas que generaron el hallazgo reportado, la acción definida se centró en "*el diligenciamiento de los campos en blanco*" observados por el equipo auditor; no obstante, no se tuvieron en cuenta, ni la causa ni acciones para mitigar, por ejemplo, la "*falta de coordinación de la actividad con la Oficina de Planeación*"; además, la acción propuesta deja de lado el proceso de actualización y levantamiento de nuevo inventario de activos de información con los encargados de los procesos.

De otra parte, es importante evitar las contradicciones operativas que se plantean frente a la Oficina de Planeación, y coordinar un espacio que permita definir la mejora aplicable en las circunstancias, así como analizar la necesidad de ajustar el instructivo vigente, bien sea incluyendo nuevos aspectos o descartando algunos que no operen; en todo caso, se debe buscar la manera de evitar que se vuelvan a materializar eventos, tales como, la falta de seguimiento o desactualización del inventario de activos de información.

HALLAZGO N° 10. Mapa de riesgos de gestión del proceso sin construir y deficiencias en la valoración de los controles asociados a los riesgos de corrupción.

Descripción: Mediante correo electrónico del 10 de junio de 2019, respecto a la construcción y disponibilidad del mapa de riesgos de gestión del proceso auditado, la Oficina de Planeación comunicó que: *"Se realizaron las mesas de trabajo con los funcionarios de la Oficina de Tecnología y la Información OTI, para la socialización de la Política de Riesgos de la ADR y la Construcción de la Matriz de Riesgos de Gestión y de Corrupción en el mes de abril de la presente vigencia, (…), los resultados finales de la Matriz de Riesgos no están oficializados".*

En virtud de lo anterior, la Oficina de Control Interno no pudo acceder al contenido actualizado del mapa de riesgos de gestión comentado, por tal razón, no se pronuncia sobre el cumplimiento de la "Política de Administración del Riesgo" (DE-SIG-002) -versión 2, adoptada por la Agencia de Desarrollo Rural en noviembre de 2018, y de la "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas" -versión 4,

emitida por el Departamento Administrativo de la Función Pública, así como de la suficiencia y validez de los controles dispuestos por la Entidad en la materia.

Cabe mencionar que, la situación anterior denota que no se acataron los términos del Plan Estratégico de Tecnología de la Información (PETI) 2018-2022 -versión 1, dentro del cual se establece el "*Modelo de Gestión TI, Sistema de gestión de seguridad de la información"* que menciona: *"La Agencia implementará la seguridad y privacidad de la información, así como acciones de mitigación del riesgo, alineado con el propósito misional, protegiendo los derechos de los usuarios de la ADR y mejorar los niveles de confianza en los mismos a través de la identificación, valoración, tratamiento y mitigación de los riesgos de los sistemas de información, mediante la Implementación, Mantenimiento y Mejora continua de un Sistema de Gestión de Seguridad de la Información".* (Subrayado fuera de texto).

En este orden de ideas, la Oficina de Control Interno se enfocó en realizar un diagnóstico del diseño de los controles para el riesgo de corrupción "*Ocultar o alterar la información dentro de los aplicativos que prestan servicio en la ADR, en beneficio propio o de un tercero"* identificado en el proceso auditado, teniendo cuenta que se encuentra incluido y publicado en el Mapa de Riesgos de Corrupción (MRC) de la Entidad construido para la vigencia 2019, en lo que evidenció los siguientes aspectos:

- Dos (2) de los cuatro (2) controles asociados al riesgo no cumplieron los lineamientos establecidos en el numeral 3.2.2 "*Valoración de los controles*", esquema 11 *"Valoración de los controles para la mitigación de los riesgos"*, Tabla 6 "*Análisis y evaluación de los controles para la mitigación de los riesgos"*, criterio de evaluación 3 *"Propósito: ¿Las actividades que se desarrollan en el control realmente buscan por si solas prevenir o detectar las causas que pueden dar origen al riesgo, (…)?"* citado en la "*Guía para la administración del riesgo y el diseño de controles en entidades públicas"*, puesto que se observó lo siguiente:

DESCRIPCIÓN DEL CONTROL	PROPÓSITO	CALIFICACIÓN PROPÓSITO		CALIFICACIÓN DEL DISEÑO	
		MRC	OCI	MRC	OCI
Optimizar la planeación de los recursos para la vigencia. (Procedimiento Plan de Adquisiciones)	Priorizar las adquisiciones del proceso.	Prevenir	No es un Control	Fuerte	Débil
Se cuenta con una definición precisa de los requisitos de formación y experiencia, así como de las funciones u obligaciones a ejecutar acordes para el DBA.	Precisar el perfil y los resultados del profesional en el rol DBA.	Prevenir	No es un Control	Fuerte	Débil

Lo anterior conllevó a realizar la calificación de la solidez del conjunto de controles de forma errónea, así:

FUENTE	PUNTUACIÓN TOTAL DE LOS CONTROLES	NÚMERO DE CONTROLES	SUMA Y PONDERACIÓN DE LOS CONTROLES	CALIFICACIÓN DE LA SOLIDEZ DEL CONJUNTO DE LOS CONTROLES
Mapa de Riesgos de Corrupción	400	4	100	Fuerte
Recálculo OCI	200	4	50	Moderado

Nota: *La información detallada de las situaciones descritas se encuentran registradas en los papeles de trabajo elaborados por el auditor que practicó las pruebas, los cuales son custodiados por la Oficina de Control Interno; no obstante, estos documentos se encuentran disponibles para consulta de las partes interesadas, previa solicitud formal de las mismas.*

Posible(s) Causa(s) identificada(s) por la Oficina de Control Interno:

- Demoras o falta de cierre de compromisos conjuntos de las Oficinas de Tecnologías de la Información y de Planeación (Oficialización de resultados de las mesas de trabajo).
- Falta de fortalecimiento en el acompañamiento y asesoría a los responsables del proceso “Gestión de Tecnologías de la Información”, en materia de identificación y gestión de riesgos.

Descripción del (los) Riesgo(s): Inobservancia de los lineamientos que en materia de gestión integral del riesgo ha adoptado la Agencia de Desarrollo Rural (ADR).

Descripción del (los) Impacto(s):

- Subestimación de los efectos de los riesgos de Tecnologías de la Información que eventualmente se materialicen (errores o debilidades en la valoración).
- Inadecuado seguimiento a las acciones establecidas por parte de la Entidad para implementar la seguridad y la privacidad de la información.
- Vulnerabilidades en el sistema de control interno de tecnologías de la información asociadas a seguridad de la información y arquitectura empresarial, entre otros aspectos.

Recomendación(es): En aras de actualizar el Plan Estratégico de Tecnologías de la Información (PETI), considerando los riesgos en la gestión de tecnologías de la información, es necesario alinear esfuerzos entre la Oficina de Tecnologías de la Información (dependencia responsable del proceso auditado) y la Oficina de Planeación para sacar avante un plan de trabajo que permita identificar los riesgos a los que está expuesta la Agencia de Desarrollo Rural en materia de tecnologías de la información, y los planes de mitigación correspondientes, atendiendo a las restricciones presupuestales, de infraestructura y de recursos humanos (entre otros aspectos) que tiene el proceso "Gestión de Tecnologías de la Información".

Además, revisar el mapa de riesgos de corrupción asociado al proceso, con el fin de validar su consistencia con los requerimientos metodológicos y normativos vigentes.

Respuesta del Auditado: Aceptado Parcialmente.

Justificación: "*La matriz de riesgos se encuentra actualmente en construcción debido a una observación de la Oficina de Control Interno de estructuración, de acuerdo con la Política de Administración de Riesgos. El riesgo de corrupción se encuentra debidamente oficializado y firmado por el responsable del proceso, actualmente se le está haciendo el*

seguimiento respectivo, pendiente a realizar seguimiento al 31 de julio de 2019, por lo cual, se acepta parcialmente el hallazgo y en el plan de mejoramiento se muestra el desarrollo correctivo del proceso y las fechas establecidas."

Causa(s) identificada(s) por el Responsable del Proceso Auditado: Falta de gestión en la contratación del personal con el perfil esencial para poder realizar este tipo de tareas, aunque se encuentra incluido en la Cadena de Valor, Plan de Adquisiciones y Guía Operativa de la OTI 2019, esta contratación no se ha podido formalizar por los problemas suscitados por el cambio de Presidente en la ADR.

Plan de Mejoramiento

ACCIÓN(ES) PROPUESTA(S)	META(S)	TIPO DE ACCIÓN	RESPONSABLE(S)	FECHA INICIAL	FECHA FINAL
Incluir los riesgos que la Oficina de Tecnologías de la Información ha evaluado, los cuales pueden generar daños o pérdidas potenciales que pueden presentarse debido a los eventos mayores generados por el uso y acceso a la tecnología, originados en sucesos antrópicos, naturales, socio-naturales y propios de la operación, con el apoyo de la Oficina de Planeación y fechas establecidas por la OTI.	Cumplir la gestión del riesgo que está indicada en la NTC- ISO 9001:2015, y en el MECI: 2014 (Componente 1.3). La Guía para la administración del riesgo DAFP y en la NTC –ISO 31000 sirve de orientación para este propósito.	Correctiva	Equipo Humano de la OTI	31-jul-19	31-jul-19

Nota: *La relación detallada del equipo humano de la Oficina de Tecnologías de la Información (OTI) responsable de cada acción propuesta se encuentra registrada en papeles de trabajo de la Oficina de Control Interno.*

Concepto de la Oficina de Control Interno: Aceptado con Observaciones.

Una vez analizada la respuesta de los responsables del proceso auditado, la Oficina de Control Interno no acepta la justificación entregada, dado que la misma no desvirtúa la situación identificada del riesgo de corrupción, respecto al diseño inadecuado de los controles tendientes a mitigar el mismo, toda vez que, se indicó en el detalle del hallazgo que acciones como "*Optimizar la planeación de los recursos (...)*" y "*Definición precisa de los requisitos de formación y experiencia, así como de las funciones u obligaciones a ejecutar acordes para el DBA*" no son controles sino actividades, y por tanto, no ayudan a reducir el riesgo asociado. Además, a pesar de que se indica que se continuará

trabajando en el seguimiento del control, se estará redundando en el error antes descrito si el diseño de los controles no es revisado y ajustado, y por tanto, el resultado del ejercicio no proporcionará los resultados esperados de mitigación.

Respecto al plan de mejoramiento, aunque no se evidencia la utilización de ninguna técnica o herramienta para el análisis de causas, la Oficina de Control Interno considera que la acción propuesta guarda correspondencia con la causa identificada; no obstante, recomienda completar o definir metas concretas para medir el cumplimiento del plan de mejoramiento, debido a que se describe en la meta "*Cumplir la gestión del riesgo (…)*" sin registrar una herramienta de medición, como por ejemplo la cantidad de mapas o matrices de riesgos que se construirán o riesgos que se incluirán en atención a la Política de Administración de Riesgos y demás normativa concordante.

RESUMEN DE HALLAZGOS:

N°	Título de Hallazgo	Repetitivo	Estado
1	Plan Estratégico de Tecnologías de la Información sin aprobar e implementar.	No	Abierto
2	Insuficiencia de recursos humanos en la estructura organizacional de Tecnologías de la Información.	No	Abierto
3	Políticas de Gobierno Digital y de Seguridad y Privacidad de la Información sin implementar y/o fortalecer.	No	Abierto
4	Incumplimiento en los términos de ejecución y reporte del grado de avance de los productos del Plan de Acción Institucional.	No	Abierto
5	Falta de instrumentación de mecanismos para la aplicación de la Política de Seguridad y Privacidad de la Información e incumplimiento de controles para la instalación de software.	No	Abierto
6	Gestión de incidentes de seguridad de la información y desarrollo de software sin el cumplimiento de los lineamientos.	No	Abierto
7	Incumplimiento de los procedimientos para la generación y almacenamiento de las copias de seguridad de bases de datos.	No	Abierto
8	Navegación web y gestión de solicitudes de tecnologías de la información sin el cumplimiento de los requerimientos.	No	Abierto

N°	Título de Hallazgo	Repetitivo	Estado
9	Incumplimiento de lineamientos en el desarrollo de inventario y clasificación de activos de información.	No	Abierto
10	Mapa de riesgos de gestión del proceso sin construir y deficiencias en la valoración de los 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 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.

- Es necesario precisar que las "Recomendaciones" propuestas en ningún caso son de obligatoria ejecución por parte de la Entidad, más se incentiva su consideración para los planes de mejoramiento a que haya lugar.

- La respuesta ante las situaciones observadas por la Oficina de Control Interno es discrecional de la Administración de la Agencia de Desarrollo Rural – ADR.

Bogotá D.C., 31 de julio de 2019.

HÉCTOR FABIO RODRÍGUEZ DEVIA
Jefe Oficina de Control Interno

Elaboró: *Carlos Eduardo Buitrago Cano, Contratista.*

Revisó: *Claudia Patricia Quintero Cometa, Contratista.*