Ministerio de
Vivienda, Ciudad y Territorio

MEMORANDO

MINISTERIO DE VIVIENDA, CIUDAD Y TERRITORIO 20-10-2025 17:03
Al Contestar Cite Este No.: 2025IE0011011 Fol:0 Anex:0 FA:0
ORIGEN 70200 OFICINA DE CONTROL INTERNO
DESTINO 70400 OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES / JESUS FERNANDO SARRIA LOPEZ
ASUNTO INFORME FINAL DE AUDITORÍA AL PROCESO DE GESTIÓN DE TECNOLOGÍAS DE LA OBS

2025IE0011011

Bogotá, octubre 20 de 2025

PARA: **JESUS FERNANDO SARRIA LÓPEZ**
Jefe Oficina de Tecnologías de la Información y Comunicaciones

DE: OFICINA DE CONTROL INTERNO

ASUNTO: **Informe Final de Auditoría al Proceso de Gestión de Tecnologías de la Información y las Comunicaciones**.

Cordial saludo Dr. Sarria,

Dando cumplimiento al Plan Anual de Auditoría Interna aprobado para la vigencia 2025, y de acuerdo con lo previsto en el literal g del art. 4o y los literales h, j y k del artículo 12 de la Ley 87 de 1993, nos permitimos socializar, mediante la presente, el Informe Final correspondiente a la Auditoría realizada al Proceso de Gestión de Tecnologías de la Información y las Comunicaciones del Ministerio de Vivienda, Ciudad y Territorio, el cual se encuentra adjunto, y adicionalmente se puede consultar por medio del siguiente enlace: https://www.minvivienda.gov.co/ministerio-planeacion-gestion-y-control-sistema-de-control-interno-rol-de-evaluacion-y-seguimiento-auditorias-de-gestion-auditorias-de-gestion

Cabe resaltar que los días 14 y 17 de octubre de 2025 se llevó a cabo la socialización con el equipo de trabajo de la Oficina TIC. En dichas sesiones se concluyó que el resultado evidenciado en el informe se encuentra alineado con la situación actual de la gestión del proceso.

Con lo anterior, La Oficina de Tecnologías de la Información y las Comunicaciones procederá a formular el correspondiente plan de mejoramiento con las respectivas acciones preventivas y/o correctivas procedentes tendientes a subsanar las causas identificadas en los hallazgos expuestos.

Se precisa que, de conformidad con lo establecido en la actividad No. 26 del "EIA-P-07 - Procedimiento de Auditoría Interna", el término perentorio para la formulación y remisión a esta oficina del respectivo plan de mejoramiento es de 5 días hábiles, contados a partir de esta radicación del Informe Final de Auditoría.

Agradecemos de antemano la disposición y colaboración de todo el equipo de la Oficina TIC que participó en el desarrollo de este ejercicio de auditoría.

Cordialmente,

JOSÉ JORGE ROCA MARTÍNEZ
Jefe Oficina de Control Interno

Anexos: Informe final de auditoría al proceso Gestión TIC 2025.

Elaboró: Carlos Alberto Quinones Cardenas – Conmtratista OCI
Revisó: José Jorge Roca Martínez – Jefe OCI.
Fecha: 20 de octubre de 2025

FECHA DE REALIZACIÓN DEL INFORME	DÍA	10	MES	10	AÑO	2025

PROCESO

Gestión de Tecnologías de la Información y las Comunicaciones.

TIPO DE INFORME	PRELIMINAR		AUDITORIA	x

NOMBRE DE LA AUDITORIA INTERNA, DEPENDENCIA, PROYECTO, OTROS

Auditoría al Proceso de Gestión de Tecnologías de la Información y las Comunicaciones.

OBJETIVO

El objetivo del informe de auditoría es evaluar el cumplimiento de los objetivos y metas de los principales planes del proceso de Gestión de TI, como lo es el Plan Estratégico de Tecnología de Información (PETI), el Plan de Seguridad y Privacidad de la Información, y el Plan de Tratamiento de Riesgos de Seguridad de la Información. Así mismo, evaluar la implementación de los lineamientos y procedimientos de la gestión y servicios de TI, infraestructura tecnológica, información y sistemas de información, y otros aspectos clave relacionados con la transformación digital, la modernización de trámites, uso y apropiación y gestión de proveedores de TI.

Este informe busca proporcionar una visión sobre el estado actual de dichos planes, destacando fortalezas, e identificando oportunidades de mejora y recomendaciones estratégicas para optimizar la gestión de tecnologías de la información, mitigar riesgos y fortalecer el control interno institucional.

ALCANCE

Para las actividades realizadas en las vigencias 2024 y 2025, se evaluará el Plan Estratégico de Tecnología de Información (PETI), verificando la ejecución de proyectos y oportunidades de mejora. Se revisará el cumplimiento del modelo de seguridad y privacidad de la información (MSPI) y la gestión de riesgos, junto

con la evaluación de procedimientos clave de Gestión de TI, como mesa de servicios, conectividad y administración de infraestructura tecnológica. También se analizarán la actualización y soporte de sistemas de información, el aprovechamiento de datos, la interoperabilidad y la modernización de trámites digitales. Además, se validará la ejecución del plan de formación en TI y la gestión de proveedores.

CRITERIOS

De orden nacional:

- **Decreto 1413 de 2017 de MinTic** – El cual define los lineamientos para el acceso a los servicios ciudadanos digitales, y la seguridad de los portales Web.
- **Resolución 1519 de 2020 de MinTic; Anexo 3** – El cual define los criterios Mínimos de Seguridad Digital.
- **Decreto 767 de 2022.** Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital, entre estos:
  - Plan Estratégico de Tecnologías de la Información - PETI.
  - Marco de Referencia de Arquitectura Empresarial - MRAE.
  - Modelo de Seguridad y Privacidad de la Información - MSPI.
  - Estrategia de Uso y Apropiación.
  - Interoperabilidad por medio de la plataforma X-Road.
  - Servicios ciudadanos digitales y lineamientos de acceso a información.
  - Digitalización y Automatización.
  - Analítica avanzada, Tableros de control Power BI.
  - Datos Abiertos.
- **Resolución 1978 de 2023 de MinTic –** Por la cual se adopta el Marco de Referencia de Arquitectura Empresarial**.**

A nivel Institucional:

- **GTI-M-03_V5** Manual de políticas de seguridad y privacidad de la información y seguridad digital.
- **GCT-F-50** Formato de Paz y Salvo para Contratistas.

METODOLOGÍA

La auditoría se realizó mediante una metodología estructurada que garantizó la cobertura de aspectos clave y la participación de los equipos involucrados. Las principales etapas fueron:

- **Planeación**: Se investigó el contexto del proceso, se identificaron riesgos y se definieron los objetivos, revisando documentación interna y normativa aplicable.
- **Reunión de Apertura**: Se presentó el alcance, objetivos y metodología de la auditoría, estableciendo roles y una comunicación clara desde el inicio.
- **Definición de Temáticas y Cronograma**: Se acordaron los temas a revisar y se organizó un cronograma de reuniones con el área auditada.
- **Levantamiento de Información**: Se realizaron sesiones temáticas para levantar información, aclarar dudas y recopilar y analizar evidencias documentales remitidas por medio de los accesos a OneDrive.
- **Socialización y Retroalimentación**: Se mantuvo comunicación continua entre la OCI y la OTIC para aclarar dudas y resultados preliminares.
- **Cierre y Presentación de Resultados**: Se analizaron las evidencias, se consolidaron los hallazgos y se presentó el informe para validación.

AUDITADO

Oficina de Tecnologías de la Información y las Comunicaciones.

IMPEDIMENTOS:

El equipo auditor no manifiesta ningún impedimento en la realización del ejercicio debido a que el proceso auditado facilitó la entrega de la información solicitada en las mesas de trabajo de acuerdo con el alcance establecido.

INTRODUCCIÓN

En el marco de la auditoría realizada al proceso de Gestión de Tecnologías de la Información, se revisaron aspectos específicos definidos en el alcance del ejercicio analizados mediante muestreos, debido al alto volumen de información que gestiona dicha dependencia, lo que hace inviable una revisión exhaustiva de la totalidad de los procesos y registros en el tiempo disponible.

Cabe resaltar que la última auditoría a esta oficina fue realizada hace más de siete años, lo que evidencia la necesidad de fortalecer los ejercicios de control en futuras vigencias. En ese sentido, se considera importante que en próximos ciclos se incluyan nuevos temas de revisión o se profundice en aquellos ya verificados, con el fin de asegurar una evaluación más integral y actualizada del estado de los sistemas, procesos y controles tecnológicos institucionales.

DESARROLLO

ANÁLISIS DE LA INFORMACIÓN

De acuerdo con el alcance establecido, se realizó el siguiente análisis:

I.GESTION DE TI

1. PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN (PETI).

Dentro del plan de auditoría inicialmente se contempló la revisión del Plan Estratégico de Tecnologías de la Información (PETI). Sin embargo, este aspecto no fue incluido en este informe, debido a que la formulación y estado de implementación ya fueron objeto de verificación en el Informe de Seguimiento emitido por la Oficina de Control Interno el 28 de julio de 2025, cuyo resultado permitió identificar que para el primer semestre de 2025 el avance en la implementación del PETI fue del 35%, identificando ocho (8) hitos que no cumplieron el avance esperado para dicho corte. Por lo tanto, se consideró pertinente no duplicar resultados, y centrar la revisión en los demás aspectos definidos en el alcance de la presente auditoría.

2. MARCO DE REFERENCIA DE ARQUITECTURA EMPRESARIAL (MRAE).

El Marco de Referencia de Arquitectura Empresarial (MRAE) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) de Colombia, es un conjunto de lineamientos, buenas prácticas y estructuras conceptuales que orienta a las entidades públicas en la implementación de un enfoque organizacional para facilitar la implementación de las estrategias de

transformación digital, buscando una gestión más eficiente, coordinada y transparente de las Tecnologías de la Información.

Los términos y plazos para la adopción del MRAE en las entidades del Estado colombiano, se establecen la Resolución 1978 del 26 de mayo del 2023 emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTic). Con base a esto, la Oficina de Control Interno obtuvo el siguiente resultado:

La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC), ha venido trabajando en la implementación del Marco de Referencia de Arquitectura Empresarial (MRAE), el cual se compone de 106 lineamientos que están inmersos en tres modelos:

- MAE – Modelo de Arquitectura Empresarial.
- MGGTI – Modelo de Gestión y Gobierno de TI.
- MGPTI – Modelo de Gestión de Proyectos de TI.

En la vigencia 2024, la OTIC realizó una validación interna de los lineamientos de estos modelos, seleccionando los que consideró prioritarios y necesarios para el Ministerio. A partir de esto, desarrolló una estrategia para establecer las acciones de implementación, y las articuló en las iniciativas del Plan Estratégico de Tecnologías de la Información (PETI).

El Plan Estratégico de Tecnologías de la Información de la vigencia 2025 contiene 16 macroproyectos, desagregados en iniciativas específicas que trazan la ruta de implementación de la Oficina TIC, entre las cuales se encuentra el MRAE.

La iniciativa del MRAE incluye actividades de actualización del repositorio de arquitectura empresarial, estructurado según los dominios definidos por el marco de referencia (datos, información, etc.), el establecimiento de la Comisión de Sistemas de Información como espacio de articulación técnica y uso de artefactos de arquitectura, clasificados en tres tipos: Catálogos, Matrices, y Vistas.

Los catálogos y matrices se almacenan en un repositorio documental de la OTIC, mientras que las vistas (diagramas) se gestionan en la herramienta Enterprise Architect, donde se puede visualizar la arquitectura empresarial desarrollada para el Ministerio.

Actualmente, el equipo de arquitectura la Oficina TIC se encuentra trabajando en el desarrollo y actualización de artefactos, como parte del avance anual en la implementación del MRAE.

La Oficina de Control Interno evidenció la existencia de soportes documentales del avance del MRAE inmerso en el PETI, y de acuerdo con el reporte de avance

presentado el 23 de septiembre de 2025, el nivel de cumplimiento por lineamientos es el siguiente:

Tabla No. 1. Avance de implementación de los 106 lineamientos del Marco de Referencia de Arquitectura Empresarial (MRAE).

MODELO	DOMINIO	CUMPLE	NO CUMPLE
Modelo de Arquitectura Empresarial	Arquitectura de Información	3	1
	Arquitectura de Seguridad	4	
	Arquitectura de Sistemas de Información	3	
	Arquitectura Institucional	3	1
	Arquitectura Tecnológica	4	
	Proceso de Arquitectura	8	
	Uso y Apropiación	2	
Modelo de Gestión de Proyectos de TI	Cierre y Operación	1	1
	Contexto Estratégico	5	1
	Ejecución y Control	3	1
	Planeación	2	
Modelo de Gestión y Gobierno de TI	Estrategia de TI	7	2
	Gestión de Información	7	1
	Gestión de Seguridad	4	
	Gestión de Servicios de TI	13	1
	Gestión de Sistemas de Información	14	
	Gobierno de TI	9	1
	Uso y Apropiación	4	
Total		**96 (91%)**	**10 (9%)**

Fuente: Oficina de Tecnologías de la Información y las Comunicaciones.

Al respecto, se resalta de manera positiva la adopción de una metodología organizada para la implementación de los modelos, incluyendo un repositorio para los artefactos desarrollados, el uso de la herramienta Enterprise Architect,

y la articulación con el PETI para avanzar en los hitos que requieran desarrollo o actualización.

No obstante, se identificaron las siguientes situaciones:

1. La Oficina TIC realiza la planeación y seguimiento en formatos internos, pero no ha adoptado los formatos oficiales de MinTic para realizar la medición formal de avance. Dichos formatos le asignan diferentes pesos a cada uno de los 106 lineamientos teniendo en cuenta criterios de impacto y complejidad para su implementación entre otros, por lo anterior, el resultado de avance presentado de 91% puede diferir al momento de medirlo con la metodología oficial.
2. Debido a que, a la fecha de revisión de esta auditoría, la Oficina TIC han realizado avances sobre el 91% de los lineamientos del MARE, se observa incumplimiento en el plazo de implementación, teniendo en cuenta que la Resolución 1978, emitida el 26/05/2023 estableció los siguientes:
    - 11 meses para reportar el 40% de avance, plazo cumplido el 24/04/2024.
    - 18 meses para reportar el 70% de avance, plazo cumplido el 23/11/2024.
    - 25 meses para reportar el 100% de cumplimiento, plazo cumplido el 24/06/2025.

Con lo anterior se concluye que, hay cumplimiento parcial en adopción e implementación del Marco de Referencia de Arquitectura Empresarial en el MVCT.

3. GESTIÓN DE MESA DE SERVICIOS.

La gestión de la mesa de servicios brinda soporte técnico a los usuarios de recursos tecnológicos en el MVCT, básicamente por medio de radiación de solicitudes y reportes de incidentes.

La gestión de la mesa de servicios se articula principalmente a través del procedimiento GTI-P-10 gestión de tickets, complementado por otros procedimientos como GTI-P-04 Gestión de Incidentes de tecnología, GTI-P-11 Gestión de Solicitudes de Servicio y GTI-P-05 gestión de cambios. Estos están documentados en el SPG y permiten canalizar las solicitudes según su naturaleza.

La atención de casos se realiza por niveles, con escalamiento al proveedor externo cuando es necesario. La medición del cumplimiento de los Acuerdos de Nivel de Servicio (ANS) se realiza mediante informes mensuales y actas de

conciliación, que consolidan indicadores de atención, tiempos de respuesta y resolución realizados por parte del proveedor UT bajo el contrato 1643 de 2023.

A partir de los soportes documentales suministrados por la OTIC, y los reportes de las actas de conciliación, se concluye que, durante el primer semestre de 2025, el proveedor UT Tecnologías Integradas presentó informes mensuales detallando el cumplimiento de los Acuerdos de Nivel de Servicio (ANS) establecidos con el Ministerio. La evaluación se centró en indicadores clave de desempeño relacionados con la atención de usuarios, tiempos de respuesta y solución, asignación de casos, y gestión de requerimientos VIP.

De acuerdo con los soportes suministrados, los principales Indicadores Evaluados son:

1) Atención por Chat (TEAMS):
   - Meta: Respuesta en menos de 30 segundos.
   - Cumplimiento mensual: Entre 98,28% y 99,69%.
   - Observación: Se utiliza una bitácora manual para el registro de tiempos, debido a la ausencia de herramienta de telefonía.
2) Asignación de Casos (≤10 minutos):
   - Casos asignados mensualmente: Entre 956 y 2.299.
   - Cumplimiento mensual: Entre 98,99% y 99,55%.
3) Solución de Incidentes (≤1 hora):
   - Cumplimiento mensual: Entre 98,55% y 100%.
4) Solución de Requerimientos VIP (≤1 hora):
   - Cumplimiento mensual: 100% en todos los meses.
5) Solución de Requerimientos Generales (≤2 horas):
   - Cumplimiento mensual: Entre 99,13% y 99,71%.
6) Casos Suspendidos sin Justificación:
   - Indicador mensual: Entre 0,02 y 0,07, cumpliendo la meta establecida.

Respecto al cumplimiento de metas, de acuerdo con lo reportado, los indicadores reportados se mantuvieron dentro de rangos razonales y establecidos por los ANS. Se cuenta con anexos mensuales de cada indicador disponibles en SharePoint. No obstante, se recomienda reforzar el seguimiento a los casos que se encuentra por fuera del cumplimiento de loa ANS, debido a que no hay un indicador de los rezagos, lo cual dificulta diferenciar si los casos que no cumplieron los ANS corresponden a casos solucionados con un tiempo mayor al establecido, o si por el contrario aún siguen pendientes por solucionar.

4. GESTIÓN DE LA CAPACIDAD Y DISPONIBILIDAD.

La gestión de la capacidad busca asegurar que los recursos tecnológicos sean suficientes para responder a las necesidades de la Entidad. En otras palabras, se trata de planear y controlar que la infraestructura de TI no sea insuficiente, garantizando un buen servicio a los usuarios.

La Oficina TIC cuenta con el procedimiento GTI-P-12 gestión de la capacidad, que establece mecanismos de medición de las capacidades de la infraestructura de TI, con el fin de evaluarlas y monitorearlas, para determinar las capacidades que respondan a las necesidades de procesamiento, almacenamiento y memoria requeridas para la prestación optima de los servicios de TI del Ministerio.

Adicionalmente, con enfoque preventivo, se realizan análisis predictivos mediante la presentación de un informe trimestral de capacidad con recomendaciones y escenarios de optimización de la infraestructura. Estos productos son insumos para elaborar el Plan de Capacidad Anual que define la hoja de ruta de la gestión de recursos del MVCT para la siguiente vigencia.

Frente a la disponibilidad, se cuenta con los procedimientos GTI-P-04 Gestión de incidentes y/o requerimientos, GTI-P-05_V6 gestión de cambios, GTI-P-08 Procedimiento gestión de incidentes, GTI-P-09_V1 solución de problemas, GTI-P-10_V1 gestión de Tickets, GTI-P-11_V1 gestión de solicitudes, y GTI-P-13_V2 gestión de la demanda. El proveedor UT genera mensualmente informe de tendencia de incidentes, en el cual analiza situación, causas y recomendaciones para su solución.

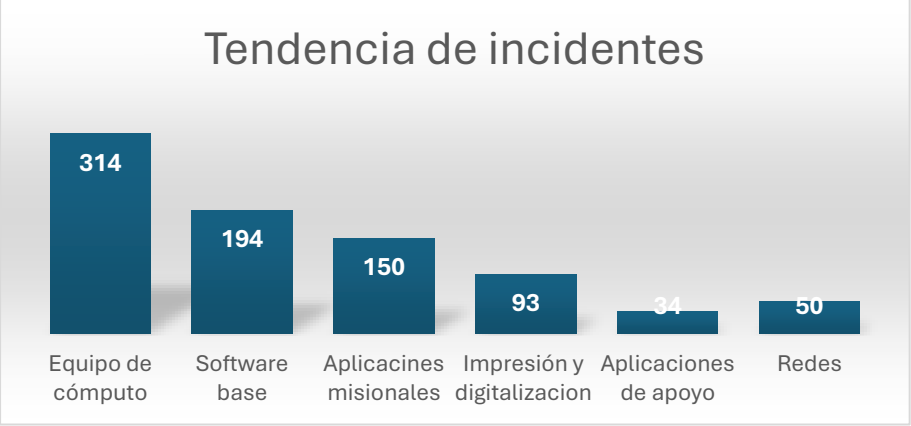
Los procedimientos indican que se generan alertas cuando la disponibilidad cae por debajo del 99.8% o cuando el uso de recursos supera el 80%. Estas alertas activan acciones correctivas como depuración de infraestructura o ajustes operativos.

La gestión de incidentes, disponibilidad y el consumo de recursos están regulados por los ANS definidos en los anexos técnicos del contrato con el proveedor Unión Temporal (UT) Tecnologías Integradas contrato 1643 de 2023, y se revisan mensualmente en comités técnicos de la OTIC.

A partir de los soportes documentales suministrados por la Oficina TIC, las actas de conciliación permiten realizar el siguiente análisis:

Respecto a la gestión de incidentes, se analizaron los siguientes tipos de incidentes, los cuales fueron los seis (6) más representativos durante el primer semestre de 2025. Se presentaron 835 incidentes, distribuidos de la siguiente manera:

Imagen No 1. Tendencia de incidentes que afectan disponibilidad.



Fuente: Actas de conciliación contrato 1643 de 2023.

El resumen del análisis de estos incidentes se presenta a continuación, el cual incluye las recomendaciones emitidas por la UT para su subsanación:

Tabla No 2. Análisis de incidentes.

Tipo de incidente	Situación	Causa	Recomendación
Equipo de cómputo	Lentitud en el funcionamiento, bloqueo de equipos, fallas de encendido que requieren formateo	Equipos antiguos, especialmente portátiles Dell Latitude 3400	Realizar una renovación tecnológica, dado que ya se han efectuado mantenimientos preventivos y repotenciaciones sin eliminar las fallas reportadas.
Software base	Bloqueos en Office, Excel, Word y PowerPoint; errores en SIIF, firma digital y token	Falta de categorización precisa en el ítem "otro"	Reinstalar periódicamente el paquete Office y realizar capacitaciones a los funcionarios.
Aplicaciones misionales	Ulises: errores en emisión de planillas, cargues y comisiones; Gesdoc: actualización de permisos; caídas en página SolarWinds	Ulises: requería actualización de perfiles de usuario; Gesdoc: se escaló al proveedor para solución	Evaluar la viabilidad de automatizar los reportes en Ulises.

Tipo de incidente	Situación	Causa	Recomendación
Impresión y digitalización	Colas de impresión bloqueadas, fallas de configuración, atascos frecuentes	Reinicio manual de colas y configuración puntual de impresoras	Realizar capacitaciones periódicas a los funcionarios y automatizar el reinicio de colas de impresión.
Aplicaciones de apoyo	caídas frecuentes en Mediacomerce y Subsidio de Vivienda	Caídas asociadas a mantenimientos preventivos por parte del proveedor	Validar con el proveedor la causa de las interrupciones para establecer medidas correctivas.
Redes	Incidente masivo reportado en Aranda	Fallas diversas; no se ha repetido una causa específica	Realizar seguimiento continuo para identificar patrones y establecer soluciones conocidas.

Fuente: Actas de conciliación contrato 1643 de 2023.

Adicionalmente, la OCI analizó los reportes de la disponibilidad de la Red WAN del primer semestre de 2025, sobre la cual el proveedor UT reportó actividades de supervisión continua de los canales de conectividad mediante la herramienta SolarWinds, y realizó registros y análisis de eventos como fallas eléctricas, cortes de fibra óptica, mantenimiento programado, afectaciones por terceros, y validación de operatividad mediante canales de respaldo.

Los eventos que se presentan son reportados y gestionados en la herramienta Aranda, con seguimiento a los tiempos de solución, por ejemplo, los indicadores ANS de disponibilidad de Red WAN presentaron el siguiente resultado:

Tabla No 3. Indicadores de disponibilidad de la Red WAN.

Mes	Disponibilidad WAN	Incidentes Registrados	Cumplimiento ANS
Enero	100%	6	100%
Febrero	100%	3	100%
Marzo	99,98%	5	80% *(con excepción aplicada)*
Abril	99,99%	6	100%
Mayo	100%	3	100%
Junio	100%	1	100%

Fuente: Actas de conciliación contrato 1643 de 2023.

De acuerdo con los resultados anteriores, se reporta una alta disponibilidad de este canal, con cumplimiento superior al 99,98% en todos los meses, a excepción de marzo debido a que se presentó demora en la documentación de un incidente, al cual se adjuntó justificación en el informe. Frente al incidente reportado, la documentación soporte destaca el uso efectivo de canales de respaldo, lo que permitió mantener la continuidad del servicio ante los eventos de afectación presentada. El reporte de ANS cuenta con la documentación técnica y anexos que respaldan los eventos y la medición revisada por la Oficina TIC.

5. GESTIÓN DE ACCESO A APLICATIVOS Y SISTEMAS DE INFORMACIÓN.

Se observa que se cuenta con el procedimiento "GTI-P-06 Solicitud de Servicios de Red y Creación de Cuentas de Usuario", por medio del cual se realiza la creación y cancelación de accesos a los aplicativos y sistemas de información del Ministerio. Los tickets radicados en Aranda son gestionados por el proveedor UT mediante el contrato 1643 de 2023.

Debido a que aún se cuenta con sistemas de información que no realizan la autenticación centralizada por medio del Directorio Activo, con el objetivo de identificar accesos que deben ser desactivados, en el marco del proceso de monitoreo de riesgos de seguridad digital, la OTIC tiene establecido realizar un cruce mensual de usuarios activos con información de Talento Humano y Contratación.

De manera corroborativa, para verificar el resultado de la gestión de usuarios en los aplicativos, el equipo auditor realizó cruces y análisis de la información de los accesos suministrada por la Oficina TIC con corte a 11 de agosto de 2025 con las bases de funcionarios y contratistas remitida por Talento Humano y Contratación respectivamente, con el siguiente resultado:

5.1 GESDOC.

GesDoc, es el Gestor Documental institucional, el cual está enfocado en organizar, almacenar, buscar y controlar los documentos al interior del Ministerio. El reporte de usuarios de GESDOC suministrado por la OTIC cuenta con 3.209 usuarios activos. Al realizar los cruces, el equipo auditor identificó las siguientes situaciones:

- 1.041 usuarios nunca han ingresado al aplicativo.
- 702 usuarios no han ingresado al aplicativo desde hace más de 9 meses; su último ingreso fue antes del 31/12/2024.

Adicionalmente, se identificaron 46 cuentas activas de usuario GESDOC de colaboradores que se encuentran en la lista de colaboradores desvinculados del Ministerio.

Tabla No 4. Usuarios de GESDOC**.**

No.	Cédula	Usuario	Nombre funcionario	Desvinculación
1	79570923	JAVillarreal	JAVIER ANTONIO VILLARREAL VILLAQUIRAN	09/01/2024
2	79724406	Svasquez	SANTIAGO VASQUEZ LOPEZ	29/01/2024
3	1032419051	ACTorres	ANDREA CAROLINA TORRES LEON	31/01/2024
4	1032363695	JARey	JESSIKA ALEXANDRA REY SEPULVEDA	31/01/2024
5	27090431	MMCordoba	MARTHA MILENA CORDOBA PUMALPA	09/02/2024
6	1032451346	Mrey	MARCELA REY HERNANDEZ	09/02/2024
7	34615124	VAngulo	VIVIANA ANGULO QUISOBONI	09/02/2024
8	67027983	MMMolinaR	MARIA MERCEDES MOLINA RENGIFO	11/02/2024
9	79054371	Jatorres	JOSE ALEJANDRO TORRES GUALTEROS	22/02/2024
10	80085299	Farbouin	FELIPE ARBOUIN GOMEZ	05/03/2024
11	1076667736	Lpaez	LINA MARIA FERNANDA PAEZ ROJAS	25/03/2024
12	1000248783	LbeltranC	LUNAVALENTINA BELTRAN CADAVID	31/03/2024
13	91476676	ERMunoz	EDGAR RENE MUÑOZ DIAZ	03/04/2024
14	1030666410	Sestevez	SERGIO ALFREDO ESTEVEZ ESTEVEZ	16/04/2024
15	51614098	Nquintero	NOHORA ELENA QUINTERO MAHECHA	21/04/2024
16	52994621	Asabogal	ADRIANA SABOGAL MORENO	05/05/2024
17	52381216	DMAvila	DIANA MARCELA ÁVILA CÁRDENAS	05/05/2024
18	80202549	Inarvaez	IVÁN NARVÁEZ FORERO	05/05/2024
19	52159628	Spedraza	SANDRA CRISTINA PEDRAZA CALIXTO	04/06/2024
20	52009661	Stibamosca	SANDRA YANETH TIBAMOSCA VILLAMARIN	25/06/2024
21	75143077	Wcastro	WILLIAM ANDRES CASTRO CAICEDO	02/07/2024
22	1032396635	DMMedina	DIANA MARCELA MEDINA HENAO	22/08/2024
23	1053779549	Jmesa	JUAN DIEGO MESA ZULUAGA	01/09/2024

No.	Cédula	Usuario	Nombre funcionario	Desvinculación
24	35420427	Lsantana	LUZ DARY SANTANA GOMEZ	01/09/2024
25	1015429790	Grincon	GINA JULIANA RINCON RODRIGUEZ	30/09/2024
26	79615256	Rperea	ROLF PEREA CUERVO	30/09/2024
27	52063618	Oaragon	OLGA YANETH ARAGÓN SANCHEZ	11/11/2024
28	16841562	AFRamirez	ANDRES FELIPE RAMIREZ RESTREPO	17/11/2024
29	7571717	Rmartinez	RODOLFO ENRIQUE MARTINEZ QUINTERO	17/11/2024
30	1075251714	CAPena	CARLOS ANDRES PEÑA FERNANDEZ	11/12/2024
31	19293137	Ysoler	YESID SOLER BARBOSA	11/12/2024
32	8162861	Dochoa	DAVID RICARDO OCHOA YEPES	22/12/2024
33	81717435	Aramirez	ANDRES FELIPE RAMIREZ JARAMILLO	31/12/2024
34	39719817	Impaez	IVETTE MARINA PAEZ RAMIREZ	31/12/2024
35	79979675	Rbeltran	RODOLFO ORLANDO BELTRAN CUBILLOS	31/12/2024
36	71336375	LRDuran	LUIS ROBERTO DURAN DUQUE	19/01/2025
37	30405194	LSGiraldo	LEIDY SORANY GIRALDO LONDOÑO	30/01/2025
38	1047392346	Ymorante	YIRA ALEXANDRA MORANTE GOMEZ	31/01/2025
39	1095922296	MVGarcia	MARIA VICTORIA GARCIA RANGEL	20/02/2025
40	51554755	Mgaray	MARTHA LUCIA GARAY CASTRO	28/02/2025
41	55155890	Frodriguez	FRANCIA ELENA RODRIGUEZ MONTEALEGRE	10/03/2025
42	77094276	Jserrano	JUAN PABLO SERRANO CASTILLA	18/03/2025
43	80222896	AGValbuena	ALEJANDRO GIOVANNI VALBUENA LOPEZ	02/04/2025
44	8729391	Jcamargo	JULIO JOSE CAMARGO AREVALO	30/05/2025
45	1053803478	MjaramilloE	MATEO JARAMILLO ECHEVERRI	01/06/2025
46	10235996	Ccastellanos	CARLOS URIEL CASTELLANOS CAÑON	23/06/2025

Fuente: Análisis del equipo auditor.

5.2 SIGEVAS.

SIGEVAS es el Sistema de Información para la Gestión y Control de Programas de Agua y Saneamiento Básico del Viceministerio de Agua y Saneamiento Básico. Este sistema permite realizar la autenticación de colaboradores por medio del Directorio Activo, sin embargo, también se brinda acceso a usuarios externos con credenciales gestionadas por el administrador del sistema. El reporte de usuarios de SIGEVAS suministrado por la OTIC cuenta con 786

usuarios activos. Al realizar los cruces, el equipo auditor identificó las siguientes situaciones:

- 71 usuarios nunca han ingresado al aplicativo.
- 300 usuarios no han ingresado al aplicativo desde hace más de 9 meses; su último ingreso fue antes del 31/12/2024.

Adicionalmente, se identificaron 6 cuentas activas de usuario SIGEVAS de colaboradores que se encuentran en la lista de funcionarios desvinculados del Ministerio.

Tabla No 5. Usuarios de SIGEVAS.

No.	Cédula	Usuario	Nombre funcionario	Desvinculación
1	34615124	VAngulo	VIVIANA ANGULO QUISOBONI	09/02/2024
2	1032396635	DMMedina	DIANA MARCELA MEDINA HENAO	22/08/2024
3	1053779549	Jmesa	JUAN DIEGO MESA ZULUAGA	01/09/2024
4	1015429790	Grincon	GINA JULIANA RINCON RODRIGUEZ	30/09/2024
5	11812009	ecquejada	ECCEHOMO QUEJADA VELEZ	10/03/2025
6	77094276	Jserrano	JUAN PABLO SERRANO CASTILLA	18/03/2025

Fuente: Análisis del equipo auditor.

5.3 ULISES.

ULISES, es el Sistema de Información que permite gestionar las comisiones, desplazamientos y viáticos de los funcionarios. El reporte de usuarios de ULISES suministrado por la OTIC cuenta con 1.487 usuarios activos. Al realizar los cruces, el equipo auditor identificó 44 cuentas activas de colaboradores que se encuentran en la lista de funcionarios desvinculados del Ministerio.

Tabla No 6. Usuarios de ULISES.

No.	Cédula	Usuario	Nombre funcionario	Desvinculación
1	1013596237	jching	JUAN DAVID CHING RUIZ	21/01/2024
2	80845814	aasprilla	ALAN GUILLERMO ASPRILLA REYES	29/01/2024
3	79724406	Svasquez	SANTIAGO VASQUEZ LOPEZ	29/01/2024
4	1017147098	jmarin	JULIAN ANDRES MARIN OSPINA	09/02/2024
5	1032451346	Mrey	MARCELA REY HERNANDEZ	09/02/2024
6	34615124	VAngulo	VIVIANA ANGULO QUISOBONI	09/02/2024
7	1018413907	jmonroy	JULI NATALIA MONROY NINO	29/02/2024

No.	Cédula	Usuario	Nombre funcionario	Desvinculación
8	52664177	dvillamil	DIANA PATRICIA VILLAMIL BUITRAGO	03/03/2024
9	80085299	Farbouin	FELIPE ARBOUIN GOMEZ	05/03/2024
10	33103920	dasprilla	DANIA PAOLA ASPRILLA YURGAQUI	17/03/2024
11	1076667736	Lpaez	LINA MARIA FERNANDA PAEZ ROJAS	25/03/2024
12	51614098	Nquintero	NOHORA ELENA QUINTERO MAHECHA	21/04/2024
13	52994621	Asabogal	ADRIANA SABOGAL MORENO	05/05/2024
14	29681219	vbarney	VANESSA BARNEY CABAL	20/05/2024
15	52159628	Spedraza	SANDRA CRISTINA PEDRAZA CALIXTO	04/06/2024
16	1032447358	dandrade	DAVID RICARDO ANDRADE MARTINEZ	10/06/2024
17	1075652149	dcontreras	DANIEL EDUARDO CONTRERAS CASTRO	25/06/2024
18	52009661	Stibamosca	SANDRA YANETH TIBAMOSCA VILLAMARIN	25/06/2024
19	1053779549	Jmesa	JUAN DIEGO MESA ZULUAGA	01/09/2024
20	35420427	Lsantana	LUZ DARY SANTANA GOMEZ	01/09/2024
21	1015429790	Grincon	GINA JULIANA RINCON RODRIGUEZ	30/09/2024
22	79615256	Rperea	ROLF PEREA CUERVO	30/09/2024
23	52063618	Oaragon	OLGA YANETH ARAGÓN SANCHEZ	11/11/2024
24	16841562	AFRamirez	ANDRES FELIPE RAMIREZ RESTREPO	17/11/2024
25	7571717	Rmartinez	RODOLFO ENRIQUE MARTINEZ QUINTERO	17/11/2024
26	1074556118	jbecerra	JHON ANDERSON BECERRA PRIETO	03/12/2024
27	63355394	osandoval	OLGA LUCIA SANDOVAL ROJAS	04/12/2024
28	19293137	Ysoler	YESID SOLER BARBOSA	11/12/2024
29	8162861	Dochoa	DAVID RICARDO OCHOA YEPES	22/12/2024
30	52057689	mmiranda	MANUELA MIRANDA CASTRILLON	31/12/2024
31	79979675	Rbeltran	RODOLFO ORLANDO BELTRAN CUBILLOS	31/12/2024
32	1047392346	Ymorante	YIRA ALEXANDRA MORANTE GOMEZ	31/01/2025
33	79384883	isuarez	IVAN RICARDO SUAREZ SANCHEZ	16/02/2025
34	51554755	Mgaray	MARTHA LUCIA GARAY CASTRO	28/02/2025
35	1048208431	fcarpintero	FREDDY DE JESUS CARPINTERO PERTUZ	02/03/2025
36	79600070	oflorez	OSCAR FLOREZ MORENO	02/03/2025
37	11812009	ecquejada	ECCEHOMO QUEJADA VELEZ	10/03/2025

No.	Cédula	Usuario	Nombre funcionario	Desvinculación
38	55155890	Frodriguez	FRANCIA ELENA RODRIGUEZ MONTEALEGRE	10/03/2025
39	77094276	Jserrano	JUAN PABLO SERRANO CASTILLA	18/03/2025
40	51894491	ragurto	ROSA CORALIA AGURTO NOVOA	31/03/2025
41	51772602	dnoy	DORYS PATRICIA NOY PALACIOS	04/05/2025
42	8729391	Jcamargo	JULIO JOSE CAMARGO AREVALO	30/05/2025
43	10235996	Ccastellanos	CARLOS URIEL CASTELLANOS CAÑON	23/06/2025
44	1010217972	jromero	JESSICA TATIANA ROMERO POVEDA	23/06/2025

Fuente: Análisis del equipo auditor.

5.4 SINAS.

SINAS, es el Sistema de Inversiones en Agua Potable y Saneamiento Básico, cuyo objetivo principal es planear, priorizar, viabilizar y monitorear los proyectos de inversión en infraestructura del sector. El reporte de usuarios de SINAS suministrado por OTIC cuenta con 1.494 usuarios activos. Al realizar los cruces, el equipo auditor identificó las siguientes situaciones:

- La estructura de nombre de usuario no está alineada con la establecida para el Directorio Activo, lo cual dificultó el cruce de datos para realizar validaciones sobre los accesos.
- Se identificó 1 cuenta activa de un colaborador que se encuentra en la lista de funcionarios desvinculados del Ministerio.

Tabla No 7. Usuarios de SINAS.

No.	Cédula	Usuario	Nombre funcionario	Desvinculación
1	11812009	ecquejada	ECCEHOMO QUEJADA VELEZ	10/03/2025

Fuente: Análisis del equipo auditor.

Adicional al cruce de datos para verificar los accesos activos, el equipo auditor identificó que el documento "GCT-F-50_V2 paz y salvo contratistas", que deben diligenciar los contratistas al momento de su desvinculación fue modificado en mayo de 2025, y en dicha versión del documento, la Oficina TIC no es alertada cuando se realiza la desvinculación de los contratistas, lo cual puede generar riesgos de seguridad de información debido a cuentas de usuario activas en

herramientas y sistemas de información que no sean desactivadas tras la desvinculación de los contratistas.

Las situaciones anteriores, permiten evidenciar debilidades en los resultados de la gestión de usuarios en los aplicativos del Ministerio que requieren una acción de mejora que mitigue riesgos de seguridad de información asociados.

6. GESTIÓN DEL DATACENTER.

De acuerdo con la información suministrada por la Oficina TIC, desde finales de 2021, el Ministerio migró su infraestructura a un modelo de datacenter tercerizado, contratado mediante licitación pública. Actualmente la operación del datacenter se controla mediante los ANS definidos en los anexos técnicos del contrato 1643 de 2023 con la UT, que incluyen aspectos como restauración de datos, antivirus, disponibilidad de servidores y bases de datos, y seguridad perimetral.

La supervisión se realiza a través de informes mensuales y fichas técnicas que resumen el cumplimiento de los ANS, permitiendo a la Oficina TIC validar la calidad del servicio prestado por el proveedor.

Al revisar el SPG, se identificaron documentos que ya no aplican o requieren ajuste debido a que sus actividades se ejecutan por medio de la tercerización, tal como: GTI-F-09 bitácora de ingreso centro de cómputo, GTI-F-25 formato análisis de infraestructura, y GTI-I-07 realización de copias de seguridad, por lo cual se plantea a la Oficina TIC realizar revisión y actualización de los procedimientos y demás documentos del proceso.

A partir de los soportes documentales suministrados por la Oficina TIC, las actas de conciliación del primer semestre de 2025 permiten realizar el siguiente análisis de la gestión sobre el datacenter, en aspectos de almacenamiento, backup, bases de datos, gestión de servicios y seguridad perimetral:

6.1 Almacenamiento y backup.

La disponibilidad del almacenamiento se mantuvo en niveles cercanos al 100%, con excepción de mayo y junio (99,97%) debido a eventos de seguridad de la información que afectaron la infraestructura de TI.

Los reportes indica que se realizaron respaldos diarios y mensuales durante el semestre, y que el proceso se vio afectado por un incidente de seguridad el 5 de mayo de 2025. Debido a eso, se redefinió la estrategia de respaldo, creando nuevas tareas programadas para máquinas restauradas, y se realizó la eliminaron de respaldos antiguos para liberar espacio.

Se reportó la realización de múltiples restauraciones exitosas de bases de datos SQL Server, incluyendo pruebas de recuperación en ambientes como SINAS, SISFV, ULISES y ARANDA, cumpliendo con los tiempos programados.

La disponibilidad de la infraestructura de backup fue superior al 99% en todos los meses, salvo en mayo (98,17%) debido a afectaciones en la consola de administración de los respaldos.

Todas las solicitudes de respaldo y restauración fueron atendidas dentro de los tiempos definidos, logrando un cumplimiento del 100%.

6.2 Gestión de bases de datos.

Para SQL Server (sistema de gestión de bases de datos), se reportó una alta disponibilidad en todos los meses, excepto en mayo que alcanzó un nivel de 92,73% debido a actividades de mantenimiento y el incidente de seguridad presentado.

Para Oracle (plataforma tecnológica que permite gestionar bases de datos y aplicaciones institucionales), la disponibilidad reportada fue de 99,9%, con reportes de afectaciones por fallos en nodos (servidores o equipos físicos) y conectividad.

Para PostgreSQL y MySQL (sistemas de gestión de bases de datos) la disponibilidad reportada fue del 100% durante todo el semestre, para los cuales se atendieron y resolvieron más de 140 casos en el semestre dentro de los tiempos establecidos.

6.3 Gestión de servicios en la nube.

De enero a abril y en junio, el servidor ADConnect mantuvo una disponibilidad del 100%, sin interrupciones ni eventos que afectaran la sincronización con servicios en la nube. Pero, en mayo se reportó una afectación en la disponibilidad, reduciendo el indicador a 92,77%, como consecuencia del incidente de seguridad ocurrido el 5 de mayo. A pesar de esto, el servicio fue restablecido. El resultado de la gestión de Incidentes y Requerimientos fue la siguiente:

Tabla No 8. Indicadores de disponibilidad de servicios.

Mes	Casos atendidos	Cumplimiento	Observaciones
Enero	87	98,85%	No.
Febrero	81	97,53%	No.
Marzo	61	100%	No.
Abril	61	100%	No.
Mayo	67	95,52%	El cumplimiento se vio levemente afectado por los eventos de indisponibilidad derivados del incidente de seguridad y fallos en infraestructura.
Junio	54	100%	No.

Fuente: Actas de conciliación contrato 1643 de 2023.

6.4 Seguridad perimetral.

a) Disponibilidad de Sistemas de Seguridad Firewall (ANS-S1).

De acuerdo con los soportes suministrados por la Oficina TIC, este indicador reportó el siguiente resultado de ANS:

- En enero a abril y junio se reportó disponibilidad del 100%, con interrupciones menores por ventanas de mantenimiento o reinicios controlados que fueron exceptuadas.
- En febrero con disponibilidad de 99,69%, afectada por una falla eléctrica en la sede Botica los días 17 y 18.
- En mayo no se reportaron afectaciones, indicando que todos los equipos de seguridad operaron sin interrupciones.

Al respecto, a la Oficina de Control Interno le recomienda a la Oficina TIC analizar la medición realizada por el proveedor, la configuración y efectividad del sistema de Firewall implementado, debido a que en mayo no reportaron afectaciones de falla o novedades de los sistemas de seguridad Firewall medidos con este indicador pese a que en dicho mes se presentó el incidente de seguridad del ransomware que afectó parte de la infraestructura de Ti del Ministerio.

b) Disponibilidad de Sistemas de Filtrado de Correo (ANS-S2).

Al revisar la documentación suministrada por la Oficina TIC, se identificó que, a lo largo del primer semestre de 2025 no se realizó ninguna medición ni reporte

de este indicador, debido a que no se renovó el licenciamiento de la herramienta de filtrado de correo FortiMail.

Al respecto, la Oficina TIC manifiesta que, si bien no se renovó la licencia de FortiMail, actualmente se cuenta con la herramienta ATP – AVANCE TREAT PROTECTION (protección avanzada de amenazas) de Microsoft, la cual suple las funcionalidades básicas de la Herramienta Fortimail.

La Oficina de Control Interno recomienda a la Oficina TIC realizar un análisis y comparación técnica de las funcionalidades de estas dos herramientas, para garantizar que ATP supla la ausencia de FortiMail, y realizar los ajustes que se requieran en los ANS para garantizar que el proveedor UT gestione y reporte todas las actividades y responsabilidades que tiene establecidas contractualmente.

c) Disponibilidad de Web Application Firewall -WAF (ANS-S3).

El WAF (Web Application Firewall) es una herramienta de seguridad cuyo objetivo principal es proteger las aplicaciones web contra ataques maliciosos, sirviendo de filtro o escudo que se coloca entre Internet y el portal web para revisar todo el tráfico que entra y sale. Su función principal es detectar y bloquear amenazas como intentos de hackeo, robo de datos, inyecciones de código malicioso, y otros ataques comunes que buscan aprovecharse de fallas en las aplicaciones web.

De acuerdo con los soportes suministrados por la Oficina TIC, de enero a junio, la disponibilidad del WAF monitoreado a través de la plataforma SIEM fue del 100%, sin reportes de caída o afectación.

d) Nivel de Cobertura y Actualización de Antivirus (ANS-S4).

De acuerdo con los soportes suministrados por la Oficina TIC, se realizaron actividades para aumentar la cobertura de los agentes de seguridad implementados. La cobertura sobre los equipos registrados en el Directorio Activo (DA) fue:

- Enero: 96,9%
- Febrero: 97,8%
- Marzo: 98,3%
- Abril: 98,6%
- Mayo: 97,6%
- Junio: 98,2%

De acuerdo con el reporte, se identificaron entre 12 y 26 equipos por mes que no reportaban a la consola FortiEDR (la cual implementa configuraciones de seguridad en los computadores y servidores institucionales), principalmente por situaciones presentadas durante el alistamiento de los computadores antes de entregarlos a los funcionarios o contratistas tras los procesos de contratación de OPS y vinculación de nuevos funcionarios.

Se recomienda reforzar los seguimientos mensuales para identificar los equipos que no tienen el agente de seguridad instalado, y realizar la configuración respectiva.

e) Gestión de Incidentes y Requerimientos de Seguridad (ANS-S5).

De acuerdo con los soportes suministrados por la Oficina TIC, se gestionaron 104 casos durante el semestre.

- Enero a Mayo: 100% de cumplimiento en tiempos de atención.
- Junio: 95,24%, con una solicitud de excepción por un caso que excedió el tiempo por error en la categorización técnica (casos específicos que requieren atención y tiempos diferentes, por lo cual se suspenden los tiempos estándar inicialmente definidos).

Los datos presentados permiten concluir que la gestión de seguridad permitió una alta disponibilidad de los sistemas de protección, incluyendo firewalls, WAF y antivirus. Igualmente, atención de incidentes fue oportuna y eficiente, lo que contribuyó a la estabilidad, protección y resiliencia de la infraestructura tecnológica del Ministerio de Vivienda ante los eventos de seguridad presentados.

II.SISTEMAS DE INFORMACIÓN E INFRAESTRUCTURA

7. CATÁLOGOS DE SISTEMAS DE INFORMACIÓN Y DE INFRAESTRUCTURA.

Los catálogos de sistemas de información y de infraestructura tecnológica, son instrumentos que permiten identificar, clasificar y gestionar los activos tecnológicos. De acuerdo con los soportes suministrados, la Oficina TIC ha desarrollado estos instrumentos durante la implementación del Marco de Referencia de Arquitectura Empresarial.

El catálogo de sistemas de información permite identificar los sistemas vigentes en el Ministerio, conocer de manera general su cobertura funcional y los responsables técnicos y operativos. El formato implementado permite conocer los siguientes atributos:

- Tipo de servicio (misional, de apoyo, transversal),
- Fabricante,
- Nivel de soporte,
- Acuerdos de nivel de servicio (ANS),
- Estado del sistema (activo/inactivo).

Por otro lado, el catálogo de infraestructura describe los componentes de infraestructura tecnológica (servidores, redes, almacenamiento, etc.) implementados en el Ministerio. Este documento permite identificar que aproximadamente el 90% de la infraestructura instalada opera en entornos virtualizados. La información documentada en este catálogo incluye:

- Identificación de las máquinas virtuales con sus respectivas direcciones IP.
- Sistemas operativos y bases de datos asociadas.
- Catálogo específico de bases de datos Oracle (con virtualización reservada por licenciamiento).
- Herramientas de monitoreo utilizadas.
- Catálogo de switches y otros componentes físicos.

Actualmente, esta documentación se encuentra disponible en documentos internos de la Oficina TIC, pero sus formatos no están formalmente definidos en el SPG institucional.

8. SOPORTE Y MONITOREO DE SISTEMAS DE INFORMACIÓN E INFRAESTRUCTURA.

El soporte y monitoreo de los sistemas e infraestructura están definidos en el contrato 1643 de 2023 de operación con la Unión Temporal (UT), y sus anexos, entre los cuales se establecen procedimientos de monitoreo, indicadores de desempeño, y planes de respaldo y recuperación. A partir de los soportes documentales suministrados, las actas de conciliación y el informe del Plan de Recuperación de Desastres (DRP), se realizó el siguiente análisis:

8.1 Gestión de aplicaciones.

La gestión de aplicaciones está regulada por los ANS definidos en los anexos técnicos del contrato con el proveedor UT Tecnologías Integradas contrato 1643, y se revisan mensualmente en comités técnicos de la Oficina TIC.

Durante el primer semestre de 2025, el proveedor UT Tecnologías Integradas reportó la realización de actividades de administración y monitoreo de aplicaciones. Estas actividades se desarrollaron conforme a los siguientes Acuerdos de Nivel de Servicio (ANS):

a) Disponibilidad del Servicio de Aplicativos (ANS-AP1).

El monitoreo se realizó sobre las direcciones URL de los ambientes productivos, excluyendo aquellas de ambientes de desarrollo o pruebas que presentaron fallas justificadas. La disponibilidad mensual reportada fue la siguiente:

Tabla No 9. Disponibilidad de aplicativos.

Mes	Cumplimiento de ANS	Observaciones
Enero	99,86%	Ajustada a 100% por excepción técnica en URL específica.
Febrero	100%	Con exclusiones aplicadas por mantenimiento o migraciones.
Marzo	100%	Con exclusiones aplicadas por mantenimiento o migraciones.
Abril	99,94%	Con exclusiones aplicadas por mantenimiento o migraciones.
Mayo	92,24%	Afectada por un incidente de seguridad tipo ransomware y fallos en la infraestructura de máquinas virtuales.
Junio	100%	Con disponibilidad total en todos los grupos de aplicaciones (críticas, misionales y de apoyo.

Fuente. Actas de conciliación contrato 1643 de 2023.

Se evidenció un cumplimiento sostenido de los indicadores de disponibilidad, salvo en mayo debido al incidente de seguridad que comprometió temporalmente los servicios de TI.

b) Gestión de Incidentes y Requerimientos (ANS-AP2).

El proveedor reportó que atendió y resolvió un total de 2.462 casos durante el semestre, distribuidos entre incidentes y solicitudes, con el siguiente nivel de cumplimiento mensual:

Tabla No 10. ANS de incidentes y solicitudes.

Mes	Casos de incidentes y solicitudes	Cumplimiento de ANS
Enero	753 casos	100%
Febrero	531 casos	100%
Marzo	535 casos	99,44%
Abril	233 casos	99,57%
Mayo	262 casos	98,85%
Junio	148 casos	97,97%

Fuente. Actas de conciliación contrato 1643 de 2023.

La atención de casos se realizó dentro de los tiempos establecidos, manteniendo niveles de cumplimiento superiores al 97%, lo que refleja una gestión eficiente del soporte a aplicaciones.

Con lo anterior, se concluye que durante el primer semestre de 2025 se realizó la respectiva gestión de administración y monitoreo de aplicaciones, cumpliendo razonablemente los ANS establecidos en la mayoría de los meses evaluados. Las excepciones fueron documentadas por el proveedor en su documentación.

La Oficina de Control Interno recomienda continuar con el seguimiento detallado de los indicadores, especialmente en lo relacionado con la infraestructura tecnológica, para mitigar la posible materialización de riesgos futuros, como los ocurridos en mayo.

8.2 Gestión de infraestructura.

Durante el primer semestre de 2025, el proveedor UT Tecnologías Integradas reportó la realización de actividades de administración y monitoreo de la infraestructura tecnológica del Ministerio de Vivienda, las cuales fueron evaluadas conforme a los siguientes indicadores de los Acuerdos de Nivel de Servicio (ANS):

a) ANS-SRV1: Disponibilidad de Servidores del Data Center.

El monitoreo de disponibilidad se realizó sobre servidores agrupados en cinco grupos, incluyendo servidores alojados en AWS y en la plataforma OpenShift. Los resultados mensuales fueron:

Tabla No 11. ANS de disponibilidad de servidores.

Mes	Cumplimiento ANS	Observaciones
Enero	100%	No.
Febrero	99,93%	Afectado por reinicio controlado de nodos OpenShift.
Marzo	100%	No
Abril	100%	Con excepciones justificadas por mantenimiento controlado de nodos Oracle.
Mayo	92,59%	Debido a un ataque de ransomware y fallos en la infraestructura de máquinas virtuales.
Junio	100%	No.

Fuente. Actas de conciliación contrato 1643 de 2023.

La gestión evidenció un cumplimiento sostenido, salvo en mayo, donde se presentaron eventos críticos que afectaron la continuidad operativa.

b) ANS-SRV2: Capacidad de los Servidores.

Este indicador evalúa el uso de CPU, memoria y disco, considerando umbrales máximos del 80%. El reporte refleja un cumplimiento mensual entre 99,28% y 99,78%, superando la meta establecida. Se aplicaron exclusiones justificadas por mantenimiento, migraciones o configuraciones especiales. La herramienta SIEM fue utilizada para el monitoreo.

c) ANS-SRV3: Gestión de Incidentes y Requerimientos.

Se atendió un total de 191 casos durante el primer semestre de 2025 de la siguiente manera:

Tabla No 12. ANS de gestión de incidentes y requerimientos.

Mes	Cumplimiento ANS	Observaciones
Enero	100%	No.
Febrero	100%	No.
Marzo	100%	No.
Abril	96,15%.	No.
Mayo	98,08%.	No.
Junio	80,56%,	Presentó solicitud de excepción por categorización incorrecta de alertas de OpenShift.

Fuente. Actas de conciliación contrato 1643 de 2023.

La atención de casos se realizó mayoritariamente dentro de los tiempos establecidos, aunque en junio se identificaron necesidades de mejora en la clasificación de los requerimientos.

d) ANS-COL1: Disponibilidad de infraestructura del Data Center.

De acuerdo con la información suministrada, se cumplió con el nivel de disponibilidad de la infraestructura en todos los meses evaluados. No obstante, se identificaron eventos críticos en abril, mayo y junio que deben ser considerados en los planes de mejora continua, especialmente en lo relacionado con la seguridad de la infraestructura y la categorización de alertas técnicas, los cuales se detallan a continuación:

- Evento de abril: Fallo crítico en nodo Oracle, debido a corrupción en archivos OLR y accesibilidad a discos ASM. Se realizó apagado controlado del nodo, solicitud de respaldo completo, escalamiento a Oracle, configuración de un nuevo nodo compatible. Se aplicó excepción en el indicador de disponibilidad por tratarse de una acción preventiva y controlada.
- Evento de mayo: Ataque de ransomware, con afectación masiva de aplicaciones alojadas en máquinas virtuales con sistema operativo Windows, generando caídas reiterativas en la infraestructura, afectación directa a la disponibilidad de servidores.
- Evento de junio: Errores en la categorización de requerimientos cuando correspondían a alertas de configuración de OpenShift; la cual es la plataforma de aplicaciones para la nube híbrida.

8.3 Plan de Recuperación de Desastres – DRP:

Se realizó el análisis del reporte del Plan de Recuperación ante Desastres (DRP) de junio de 2025, elaborado por el proveedor UT bajo el contrato 1643 de 2023. Vale la pena mencionar que este Plan constituye un componente esencial de la estrategia de continuidad operativa del Ministerio. Su propósito principal es garantizar la restauración rápida y segura de los servicios críticos en caso de una interrupción significativa, ya sea por fallos tecnológicos, incidentes de seguridad o desastres naturales.

Principalmente, el plan busca minimizar el impacto sobre los usuarios y servicios institucionales, preservar la integridad y disponibilidad de los datos, coordinar una respuesta eficiente entre el personal del Ministerio y el proveedor UT Tecnologías Integradas, restaurar los servicios principales en tiempos definidos:

- RPO (Punto de recuperación objetivo): 40 minutos.
- RTO (Tiempo de recuperación objetivo): 240 minutos.

Durante el mes de junio se reportó la realización de las siguientes acciones clave:

- Prueba controlada del DRP sobre la aplicación SIGEVAS, en un entorno aislado, sin afectar los ambientes productivos.
- Evaluación de la capacidad de publicación de servicios y retorno a la infraestructura on-premise.
- Replicación completa de máquinas virtuales (VMs) como estrategia principal de recuperación, incluyendo instancias de bases de datos.
- Monitoreo continuo de la plataforma Acronis Cyber Protect, con seguimiento de métricas como disponibilidad, capacidad, latencia, uso de CPU, memoria y disco.
- Presentación del plan de trabajo y ajustes al documento DRP, incluyendo configuraciones específicas para el entorno del Ministerio.

Resultados relevantes presentados:

- La prueba evidenció que el entorno DRP puede iniciar servicios y autenticar usuarios mediante Active Directory restaurado.
- El DRP implementado proporciona una solución robusta y eficiente para la protección de los servicios críticos del Ministerio haciendo uso de la tecnología Acronis, la cual permite una restauración rápida y segura
- La estrategia de replicación completa de VMs garantiza la recuperación integral de los sistemas, aunque no se contempla la réplica específica de instancias de bases de datos.

- Se identificó la necesidad de gestionar la recuperación de datos transaccionales por otros medios o en etapas posteriores.

9. SEGURIDAD

En el marco de la verificación del Índice de Transparencia Activa (ITA) y del cumplimiento del Anexo 3 de la Resolución 1519 de 2020 del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), el equipo auditor de la Oficina de control Interno realizó una revisión independiente a las condiciones técnicas de seguridad digital del Portal Web Institucional.

Para esto, se llevó a cabo la ejecución de una prueba de penetración (Pen Test) con una herramienta Trial, con funcionalidades limitadas, pero permitieron identificar cinco (5) riesgos asociados a vulnerabilidades que, al ser aprovechadas por un tercero, podrían generar eventos que comprometan la confidencialidad, integridad o disponibilidad de la información e infraestructura del portal:

1. Se encontró una vulnerabilidad en la versión 3.4.1 de Bootstrap, específicamente en el componente de "carrusel", que podría permitir a un atacante ejecutar código malicioso (JavaScript) en el navegador de un usuario. Esto se debe a una falla en la validación de ciertos atributos del código HTML. Aunque el riesgo no se considera crítico porque fue detectado por análisis de versión, sigue siendo importante actualizar a la última versión para evitar posibles ataques.
2. El sitio web no tiene configurada la cabecera de seguridad Referrer-Policy, lo que significa que, al hacer clic en un enlace, el navegador puede enviar la dirección completa de la página de origen al sitio de destino. Esto podría exponer información sensible o permitir que otros sitios rastreen a los usuarios. Para evitar este riesgo, se recomienda configurar esta cabecera en el servidor, usando por ejemplo el valor no-referrer, que evita compartir esa información.
3. El sitio web tiene configurada la cabecera de seguridad Content-Security-Policy, pero de forma incompleta o insegura. Esto puede permitir que atacantes ejecuten código malicioso (como JavaScript) dentro del sitio, lo que representa un riesgo para los usuarios. Por ejemplo, si no se restringen los scripts o se permiten valores inseguros, un atacante podría aprovecharlo para robar información o manipular el sitio. Se recomienda ajustar esta cabecera para definir claramente qué contenido es seguro y desde qué fuentes puede cargarse.
4. Se detectó la presencia del archivo robots.txt en el sitio web. Aunque este

archivo no representa un riesgo por sí solo, puede revelar rutas internas o sensibles del sitio (como paneles de administración) si están listadas allí. Es importante tener en cuenta que este archivo es público y cualquier persona puede verlo, por lo que no debe usarse como medida de seguridad. Se recomienda revisar su contenido y eliminar cualquier ruta que pueda exponer información delicada.

5. Se identificaron varias tecnologías y versiones utilizadas por el sitio web (como Bootstrap, jQuery, PHP, Drupal, entre otras). Aunque esto no es un fallo por sí mismo, puede facilitar que un atacante identifique vulnerabilidades conocidas en esas versiones específicas y las use para atacar el sistema. Por eso, se recomienda ocultar o limitar la información técnica visible en las respuestas del servidor (como cabeceras HTTP o etiquetas HTML), para reducir el riesgo de explotación.

Adicionalmente, la Oficina de Control Interno, realizó una validación de estándares del lenguaje HTML5 del Portal Web Institucional, analizando 156 elementos del código HTML, identificando 37 alertas, y 43 errores.

El detalle de estas dos pruebas fue reportado a la Oficina TIC el 28 de agosto de 2025 por correo electrónico, para el análisis con el proveedor de infraestructura y de seguridad del Ministerio, y la respectiva definición de acciones de subsanación que consideren pertinentes.

III.INFORMACIÓN

10. FOMENTO DE USO Y APROVECHAMIENTO DE DATOS.

10.1 Proyectos e iniciativas.

Al indagar sobre proyectos e iniciativas de uso y aprovechamiento de datos en el Ministerio, se resalta de manera positiva las siguientes tres lideradas por la Oficina TIC:

1) Bodega de datos misionales.

Se consolidó una bodega de datos que integra información de sistemas misionales como vivienda y agua. Esta estrategia ha permitido estructurar datos transaccionales y habilitar el uso de herramientas como Power BI, facilitando la generación de tableros de control para la toma de decisiones.

2) Estrategia Geoespacial.

Se implementó una base de datos geográfica empresarial (GDB) mediante la plataforma ArcGIS Enterprise, que permite almacenar y compartir datos espaciales (puntos, líneas, polígonos) relevantes para los procesos misionales. Esta estrategia incluye herramientas como ArcGIS Pro, ArcGIS Online, y Survey 123, utilizadas para la recolección, visualización y análisis de datos georreferenciados.

3) Alineación con la Estrategia Nacional de Datos del DNP.

El Ministerio ha adoptado lineamientos y productos definidos por el Departamento Nacional de Planeación (DNP). Se observan soportes documentales de esta iniciativa con hojas de ruta y entregables de las vigencias 2024 y 2025, incluyendo temas como gestión documental, articulación sectorial, datos maestros, datos abiertos, analítica, interoperabilidad y cultura de datos, entre otros.

10.2 Instrumentos y actividades para el fomento y uso de los datos.

Con el objetivo de identificar si, el Ministerio cuenta con instrumentos institucionales para guiar el fomento y uso adecuado de los datos, se analizaron documentos establecidos en el SPG, con lo cual, se observan instrumentos como el GTI-F-03 Formato de solicitud de publicación de datos abiertos, y el procedimiento GTI-P-01 Gestión de datos abiertos.

No obstante, a la fecha no se evidencian instrumentos procedimentales para asegurar la calidad de los datos a cargo de los responsables de producir y gestionar la información, lo cual pueda requerir la colaboración y lineamientos por parte de OAP para modelos operativos de gobierno de datos.

Al respecto, la Oficina TIC manifiesta que actualmente se está trabajando con la Oficina Asesora de Planeación en la formulación del "DOCUMENTO MODELO OPERATIVO DE GOBIERNO DE DATOS".

La Oficina de Control Interno revisó el borrador de este documento, observando que este busca garantizar que la información generada sea de calidad, confiable y útil como activo estratégico para la toma de decisiones operativas, tácticas y estratégicas.

Para su implementación de ese modelo, se adoptan referentes internacionales como el modelo DAMA y el cuerpo de conocimiento DMBoK, así como guías nacionales de MinTIC. Su implementación requiere el respaldo del equipo de

gestión del cambio y el patrocinio de altos directivos, alineándose con los objetivos misionales del MVCT. Se espera que, la implementación de este modelo operativo impulse la toma de decisiones basada en datos, y la reducción de riesgos de seguridad de la información, y la explotación de datos.

Adicionalmente, se observa que la Oficina TIC ha realizado jornadas de capacitación dirigidas a funcionarios y contratistas sobre uso de herramientas tecnológicas, buenas prácticas en calidad de datos, y aprovechamiento de datos abiertos. Estas capacitaciones son clave para fortalecer la cultura de datos dentro del Ministerio.

Por último, se resalta que en la sección de Transparencia del Portal Web Institucional se han publicado conjuntos de datos abiertos a disposición de la ciudadanía. No obstante, aunque se cuenta con un documento con el "Plan de Apertura de Datos Abiertos", dicho Plan no está formalmente incorporando dentro del SPG institucional, lo cual pone en riesgo su implementación, debido a que las metas y actividades establecidas para su implementación no está formalmente incorporadas en el sistema integral de gestión institucional.

11. SERVICIOS DE INTEROPERABILIDAD.

La Oficina TIC ha desarrollado e implementado varios servicios de interoperabilidad, algunos de ellos utilizando la plataforma X-Road, entre los cuales se destacan los siguientes:

Tabla No 13. Servicios de interoperabilidad.

Entidad	Descripción del servicio	Canal
SNR - Superintendencia de Notariado y Registro	• A partir de la identificación del postulante al subsidio se valida si tiene propiedades registradas en la SNR, para validar las condiciones al acceso del subsidio familiar de vivienda.	X-ROAD. En producción.
RNEC - Registraduría Nacional del Estado Civil	• Verificación de la autenticación de la identidad de los ciudadanos.	VPN. En producción.
UARIV - Unidad para la Atención y Reparación Integral a las Victimas	• Corte mensual del registro de víctimas reconocidas, incluyendo toda la información de victimización que reposa en el registro único de víctimas. • Corte semestral de hogares asignados cruzados con el registro de víctimas reconocidas.	SFTP. En producción.

Entidad	Descripción del servicio	Canal
DNP – Departamento Nacional de Planeación	• Descarga la base de datos de SISBEN 4 en la bodega de datos del Ministerio para diferentes procesos misionales. • Entrega información de proyectos.	VPN. En producción.
Superintendencia del Subsidio Familiar	• Consulta de información de subsidios asignados y postulados de vivienda de interés social (VIS) al ciudadano.	Archivos planos. En producción.
COPNIA	• Expone la información correspondiente a matriculas y sanciones de un matriculado registrado en COPNIA	VPN
Migración Colombia	• Consulta de documentos de identificación emitidos por Migración Colombia para identificación de personas extranjeras. MVCT recibe información de los documentos en un archivo plano.	VPN
IDEAM	• Listas de autoridades, usuarios, predios, concesiones, captaciones, usos, permisos de vertimiento, tramos, muestras, mediciones, y otros.	Otros
ART - Agencia de Renovación del Territorio	• Información de sistema/acueducto en comunidades rurales. • Información de prestadores de servicio rurales.	X-ROAD. En desarrollo.

Fuente. Matriz de interoperabilidad suministrada por la OTIC

Debido a que la solución de interoperabilidad sobre X-Road no se encuentra implementado por parte de algunas entidades, el Ministerio debe recurrir a otros canales o mecanismos de interoperabilidad. Según las actividades de indagación realizadas con la Oficina TIC, se identificaron retrasos en la puesta en marcha de algunos servicios, debido a la falta de acuerdos con la Agencia Nacional Digital por parte del Ministerio TIC. No obstante, recientemente se han logrado avances gracias a nuevos acercamientos entre las partes.

Aunque el Ministerio cuenta con herramientas propias para realizar monitoreo de disponibilidad sobre los servicios de TI, la Oficina de Control Interno identificó que actualmente no se tienen esquemas de monitoreo sobre la disponibilidad de los servicios de interoperabilidad implementados, lo cual impide reaccionar ante una falla antes que el usuario final reporte el incidente por medio de un Aranda en la mesa de servicios. Al respecto, la Oficina TIC informa que luego de verificación es realizadas junto con el proveedor, si están en capacidad de implementar esquemas de monitoreo para los servicios de interoperabilidad.

Teniendo en cuenta que uno de los principales objetivos de la implementación de los servicios de interoperabilidad es la disminución de los tiempos de respuesta a los tramites internos y servicios prestados al ciudadano, la Oficina

de Control Interno, recomienda realizar periódicamente mediciones sobre de los servicios implementados, para conocer el impacto de la mejora en la eficiencia de la gestión institucional. Para esto, es importante tener en cuenta que, si bien la Oficina TIC proporciona y da soporte a los servicios de interoperabilidad, los resultados de la medición de impacto en la eficiencia administrativa la deben suministrar los procesos que hace uso de estos servicios.

IV.TRÁMITES Y SERVICIOS

12. DIGITALIZACIÓN DE INFORMACIÓN Y TRÁMITES.

Con el objetivo de identificar si el Ministerio cuenta con mecanismos y proyectos digitalizar y sistematizar información, trámites y procedimientos, se realizó una revisión de documentos en el SPG, identificando que la Oficina TIC cuenta con el GTI-P-13 Procedimiento para la gestión de la demanda tecnológica, el cual permite identificar, canalizar y priorizar necesidades institucionales, entre ellas las relacionadas con digitalización, automatización y sistematización.

Para estas implementaciones, se cuenta con un Comité de Gestión de la Demanda, que se reúne periódicamente para revisar casos, asignar responsables y definir líneas de acción de los desarrollos.

Se mantiene un backlog o inventario de requerimientos, que incluye tanto solicitudes en curso como proyectos ya implementados. Se cuenta con un tablero en Power BI con indicadores para planear y hacer seguimiento a las implementaciones.

Uno de los proyectos más relevantes en 2025 es el llamado Proyecto RUBI, orientado a consolidar, gestionar y proteger la información clave de los procesos institucionales en una única plataforma centralizada sobre SharePoint. Este proyecto promueve la gobernanza de la información, de la seguridad de los datos y la eficiencia operativa, estableciendo controles para mitigar la fuga de información y fortalecer la toma de decisiones.

Adicionalmente, se han desarrollado las siguientes automatizaciones:

- Seguimiento de contratos y cuentas de cobro.
- Comisiones financieras.
- Gestión de proveedores.
- Además, se han implementado visores y buscadores sobre archivos digitalizados, organizados por temática y área funcional, con base en las Tablas de Retención Documental (TRD).

La digitalización se articula con el área de gestión documental, que lidera el modelo de archivo electrónico y realiza diagnósticos de madurez. La Oficina TIC apoya técnicamente en aspectos como almacenamiento, infraestructura y herramientas de consulta, respetando la gobernanza documental definida por dicha área.

V.USO Y APROPIACIÓN

13. PLAN DE USO Y APROPIACIÓN.

La metodología de implementación, uso y apropiación de las Tecnologías de la Información y las Comunicaciones (TIC) se fundamenta en un proceso articulado y progresivo liderado por la Oficina TIC, en coordinación con los convenios establecidos y los valores agregados ofrecidos por los diferentes proveedores de TI contratados.

Este enfoque incluye la planificación estratégica de actividades, la ejecución técnica de soluciones y el acompañamiento permanente a los usuarios, buscando garantizar la transferencia de conocimiento y el fortalecimiento de competencias digitales.

Asimismo, el proceso cuenta con el apoyo del Plan Institucional de Capacitación (PIC) de la Entidad, el cual refuerza la apropiación tecnológica mediante jornadas formativas, talleres prácticos y estrategias de sensibilización que permiten a los funcionarios integrar de manera efectiva las TIC en sus labores, asegurando su sostenibilidad y el logro de los objetivos institucionales.

De acuerdo con los soportes suministrados por la Ofician TIC, durante el primer semestre de 2025, se han desarrollado múltiples actividades orientadas al fortalecimiento del dominio de Uso y Apropiación de TI, enmarcadas en el Plan Estratégico de Tecnologías de la Información (PETI) y alineadas con los lineamientos del Modelo de Arquitectura Empresarial (MAE) y la Política de Gobierno Digital. A continuación, se describen las más relevantes:

Enero:

- Socialización de canales de atención: Difusión de los servicios disponibles a través de la mesa de ayuda.
- Ventanas de mantenimiento: Comunicación proactiva sobre intervenciones en la infraestructura tecnológica.

Febrero:

- Publicación de información GTIC: Inclusión de planes de seguridad y privacidad en el micrositio institucional.
- Fortalecimiento en seguridad digital: Divulgación de estrategias de protección de la información.

Marzo:

- Socialización de la plataforma IfindIT: Uso de IA generativa en tableros de información.
- Actualización de información TIC: Integración de contenidos del MinTIC.
- Estrategia "OTIC al Día": Comunicación interna para fortalecer el dominio UYA – Uso y Apropiación.
- Planeación de la Semana TIC: Articulación con proveedores como ESRI Colombia.

Abril:

- Campañas de autoaprendizaje: Promoción de contenidos formativos en seguridad y gobierno digital.
- Socialización de GESDOC: Plataforma institucional para gestión documental.
- Activación de MFA – multi factor de autenticación: Campaña de seguridad en cuentas institucionales.
- Avances en Semana TIC: Inclusión del componente de georreferenciación.
- Gestión del conocimiento: Pruebas técnicas con Viva Learning.
- Transformación digital SISFV: Charlas institucionales con proveedor Nexpass.

Mayo:

- Capacitación en ARCGIS: Inicio de formación en estrategia geográfica.
- Autoaprendizaje: Continuación de campañas internas.
- Transformación digital SISFV: Envío de información para análisis de fases.
- Participación en magazín institucional.
- Pruebas del Chatbot OTIC: Nivel 0 de autogestión.
- Socialización de incidentes de seguridad.
- Campaña de sensibilización en seguridad digital.
- Avances en Semana TIC.
- Medidas de seguridad post-incidente.
- Comunicación con dependencias: Difusión de capacitaciones.

Junio:

- Talleres PNID: Participación institucional.
- Socialización de ARANDA: Plataforma de gestión de servicios técnicos.
- Capacitación en ARCGIS: Segunda fase de formación.
- Socialización de GESDOC.
- Autoaprendizaje: Promoción de formación en gerencia de proyectos.
- Charla de seguridad digital: Análisis de respuestas.
- Participación en magazín institucional.

Este conjunto de actividades refleja un avance del 42% en la ejecución del proyecto de Uso y Apropiación para la vigencia 2025, con énfasis en las siguientes cuatro iniciativas clave, lo cual refleja un avance razonable teniendo en cuenta que la fecha de corte es el primer semestre de 2025:

- Capacitación en sistemas de información geográfica (ArcGIS).
- Fortalecimiento de la seguridad de la información.
- Autoaprendizaje en temas TIC.
- Eventos de alto impacto (Semana TIC).

VI.GESTIÓN DE PROVEEDORES

14. PROVEEDORES DE SERVICIOS DE TI.

Durante la indagación inicial del equipo auditor con la Oficina TIC, se revisó de manera general el estado de los contratos tecnológicos gestionados por la OTIC, así como los mecanismos de supervisión, ejecución y documentación asociados a cada proveedor.

Se conoció que, la Oficina TIC tiene relación contractual vigente con diversos proveedores de servicios tecnológicos, distribuidos en varias vigencias:

- Vigencia 2023: Se observaron 13 contratos, de los cuales 7 finalizaron en esa misma vigencia, y los otros 6 aún están vigentes y finalizan en 2025. Algunos de estos contratos tienen vigencias futuras aprobadas, lo que habilitó su ejecución hasta el 31 de diciembre de 2025.
- Vigencia 2024: Se observa un contrato activo.
- Vigencia 2025: Se observan 3 contratos vigentes, correspondientes a los servicios de ESRI, Creangel y OpenShift.

Además, existen contratos de ejecución inmediata, como los relacionados con licenciamiento (Microsoft, Adobe, Fortinet), que se pagan en una sola cuota y no requieren supervisión continua.

La actividad de supervisión de estos contratos incluye la elaboración de informes presupuestales y de ejecución, que se almacenan en repositorios internos y sirven como evidencia del cumplimiento de las obligaciones contractuales.

Se observa que a Oficina TIC mantiene carpetas organizadas por vigencia, donde se almacenan los informes de supervisión, actas de seguimiento, y demás documentos contractuales. Estos documentos permiten verificar:

- Estado de ejecución.
- Cumplimiento de entregables.
- Vigencia y fecha de finalización.
- Modalidad de contratación (ejecución inmediata vs. vigencia extendida).

CONTRATO 1643 DE 2023

Para una revisión más detallada, el equipo auditor seleccionó el contrato 1643 de 2023 del proveedor Unión Temporal (UT) Tecnologías Integradas; cuyo objeto contractual incluye entre otros los servicios que soportan el Datacenter, conectividad, mesa de servicios, y seguridad.

Con este contrato, se procedió a realizar el siguiente análisis, con el propósito de verificar si, para la generación de la facturación de los servicios prestados por el proveedor, el supervisor del contrato tiene en cuenta las situaciones que pudieron afectar el cumplimiento de los Acuerdos de Nivel de Servicio (ANS).

Esta revisión se realizó con la documentación disponible en las carpetas de ejecución contractual, en particular los informes de servicio y las actas de conciliación correspondientes al primer semestre del año 2025.

A continuación, se presenta un resumen ejecutivo de los eventos más relevantes que pudieron generar afectaciones en la facturación mensual. Posteriormente, se incluye el consolidado de cada uno de los componentes que integran dicha facturación. Vale la pena mencionar que, debido a la extensión de los informes técnicos que componen la ejecución del contrato, el análisis se realizó de una muestra de situaciones.

EVENTOS QUE PUDIERON GENERAR AFECTACIÓN EN LA FACTURACIÓN:

Durante el primer semestre de 2025, se identificaron múltiples situaciones que impactaron directa o indirectamente el cumplimiento de los Acuerdos de Nivel de Servicio (ANS) establecidos en el contrato. A continuación, se destacan los eventos más relevantes identificados por el equipo auditor:

1. Casos suspendidos sin justificación válida:

Se registraron casos suspendidos sin soporte válido en todos los meses, con un total acumulado de 67 casos.

Aunque los indicadores mensuales se mantuvieron dentro de los umbrales permitidos, estos casos deben ser excluidos de la facturación o revisados en conciliación.

2. Ausencias de personal técnico:

Se reportaron ausencias recurrentes por vacaciones, incapacidades y días especiales. Aunque se indica que hubo cobertura operativa, estas ausencias pueden haber afectado la capacidad instalada y deben ser documentadas para análisis contractual.

3. Eventos de conectividad:

Se presentaron múltiples eventos de afectación a servicio de fibra óptica, fallas eléctricas y manipulación de terceros en sedes como Fragua, Botica, Palma y Colseguros. Aunque se mantuvo la operatividad por canales de respaldo, estos eventos deben seguir siendo registrados en los informes como excepciones técnicas.

4. Fallas en infraestructura tecnológica:

En mayo de 2025 se presentó un ataque de ransomware que afectó masivamente servidores, aplicaciones y backups. Se sumaron fallos reiterativos en la infraestructura los días 11, 13 y 20 de mayo. Estos eventos generaron afectaciones críticas en los ANS de disponibilidad y deben ser considerados para descuento en facturación.

5. Indisponibilidad en servicios específicos:

Se registraron fallas puntuales en aplicaciones (como SIPROJ y Aranda), bases de datos Oracle (bloqueo de acceso), y switches LAN/WLAN (reinicios y fallas eléctricas). Aunque se aplicaron excepciones, deben quedar documentadas para evitar cobros indebidos por parte del proveedor.

6. Incumplimiento en ANS específicos

En junio, el ANS-SRV3 (Infraestructura) tuvo un cumplimiento de 80,56%, no alcanzando la meta. Se solicitó excepción por categorización incorrecta de requerimientos Openshift, lo cual debe ser analizado en conciliación técnica.

7. Problemas con antivirus y filtrado de correo:

En todos los meses se identificaron equipos sin reporte en la consola FortiEDR (entre 12 y 26 equipos en promedio). El servicio de filtrado de correo (FortiMail) no fue prestado por falta de renovación del licenciamiento, por lo cual, se solicita al supervisor analizar si estos componentes deben ser retirados de los cobros de facturación en caso de que se aplique cobro por estos.

RESUMEN DE FACTURACIÓN

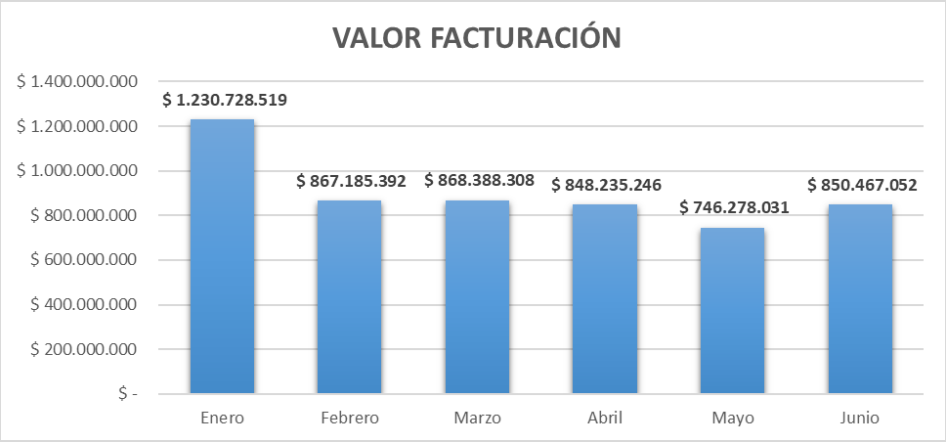
A partir de la documentación que reposa en las actas de conciliación correspondientes al primer semestre del año 2025, el equipo auditor consolidó en la siguiente tabla la facturación con el proveedor:

Tabla No 14. Relación de los ítems que componen la facturación del primer semestre de 2025 del contrato 1643 DE 2023.

ITEM	Enero	Febrero	Marzo	Abril	Mayo	Junio
Conectividad	$ 57.062.955	$ 57.062.955	$ 57.062.955	$ 57.062.955	$ 57.062.955	$ 57.062.955
Datacenter	$ 454.073.879	$ 448.671.670	$ 449.214.055	$ 449.952.751	$ 361.589.815	$ 445.298.051
Mesa de Servicios	$ 101.919.808	$ 101.919.808	$ 114.447.808	$ 101.919.808	$ 101.919.808	$ 108.657.094
Comunicaciones	$ 27.306.609	$ 27.306.609	$ 27.306.609	$ 27.306.609	$ 27.306.609	$ 27.306.609
Impresión	$ 59.468.359	$ 60.740.968	$ 61.328.495	$ 61.182.453	$ 61.514.117	$ 60.975.335
Licenciamiento	$ 321.957.061	$ -	$ -	$ -	$ -	$ -
Otros servicios	$ 12.436.975	$ 33.025.210	$ 20.378.151	$ 15.378.151	$ 17.731.092	$ 15.378.151
SUB TOTAL	**$ 1.034.225.646**	**$ 728.727.220**	**$ 729.738.074**	**$ 712.802.728**	**$ 627.124.396**	**$ 714.678.195**
IVA	$ 196.502.873	$ 138.458.172	$ 138.650.234	$ 135.432.518	$ 119.153.635	$ 135.788.857
TOTAL	**$ 1.230.728.519**	**$ 867.185.392**	**$ 868.388.308**	**$ 848.235.246**	**$ 746.278.031**	**$ 850.467.052**

Fuente. Documentos de actas de conciliación del contrato, sección "Facturación".

Gráfica No 1. Comparativo del valor total de la facturación del primer semestre de 2025 del contrato 1643 DE 2023



Fuente. Documentos de actas de conciliación del contrato, sección "Facturación".

Como resultado de este análisis, se observa que los eventos presentados en los informes de la prestación de los servicios se ven reflejados en las actas de conciliación, y en caso de identificar situaciones de afectación en los Acuerdos de Nivel de Servicio, estos son tenidos en cuenta para los descuentos en la facturación. Se recomienda al Supervisor del Contrato CTO 1643 de 2023 continuar con el análisis detallado de los eventos reportados, especialmente aquellos que:

- Impactaron directamente los ANS.
- Fueron objeto de solicitud de excepción.
- Carecen de justificación técnica o contractual.

Este seguimiento permitirá aplicar de forma justa y transparente los descuentos correspondientes en la facturación mensual, garantizando el cumplimiento del contrato y la protección de los intereses del Ministerio.

VII. GESTIÓN DE PROYECTOS DE INVERSIÓN

15. PROYECTOS DE INVERSIÓN.

Por medio de indagación, se conoció que, la Oficina TIC ha gestionado el proyecto de inversión denominado "Fortalecimiento de las tecnologías de la información y las comunicaciones en el Ministerio de Vivienda, Ciudad y

Territorio", con vigencia entre 2018 y 2025. Este proyecto ha sido el principal mecanismo de financiación para el desarrollo tecnológico institucional.

El proyecto contempla 9 actividades, pero para la vigencia 2025 solamente 5 están activas con recursos asignados. Estas actividades incluyen:

1. Adquisición y desarrollo de software.
2. Servicios de gestión de capacidad.
3. Servicios de soporte de operación.
4. Dotación de infraestructura.
5. Actualización y mantenimiento de software.

Cada actividad cuenta con indicadores de producto, metas anuales y focalización presupuestal (infraestructura, aplicaciones o servicios), conforme a los lineamientos del DNP.

Líneas base en la Plataforma Integrada de Inversión Pública PIIP.

- La línea base cero (0), es el documento que define metas y recursos proyectados inicialmente según la asignación presupuestal real por parte del Ministerio de Hacienda.
- La línea base uno (1) representa el ajuste técnico realizado entre julio y agosto de 2025 para reflejar la ejecución real y las metas alcanzables, considerando tiempos de contratación y disponibilidad presupuestal. Actualmente la plataforma PIIP refleja lo establecido en la línea base uno.

Reporte y seguimiento a la ejecución.

La OTIC realiza seguimiento mensual a la ejecución del proyecto mediante:

- Reportes en la plataforma PIIP, que incluyen:
  - Avances financieros – ejecución presupuestal,
  - Metas de producto,
  - Indicadores de producto,
  - Metas por actividad,
  - Focalización (infraestructura, aplicaciones, servicios),
  - Regionalización,
  - Soportes.
- Tableros de control en Power BI: Visualizan compromisos, obligaciones, pagos y ejecución por actividad.

- Normalización de datos financieros: Se realiza una asociación entre los códigos internos de financiera (TIC1, TIC2, etc.) y las actividades del proyecto, para garantizar coherencia entre la ejecución presupuestal y los objetivos del proyecto.

Aunque la plataforma PIIP no muestra directamente la asociación con los códigos internos de financiera (como TIC1, TIC2, etc.), la OTIC realiza esta vinculación mediante archivos propios para poder relacionar cada actividad del proyecto con su ejecución presupuestal real.

De acuerdo con la información del reporte de indicadores del proyecto de inversión suministrado por la Oficina TIC, los pagos relacionados con el proyecto de inversión durante el primer semestre de 2025 es el siguiente:

Tabla No 15. Relación de pagos del proyecto de inversión de la Oficina TIC durante el primer semestre de 2025.

OTIC	ACTIVIDAD	PAGOS					
		ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO
TICS 1	Dotar de infraestructura tecnológica al Ministerio	$ -	$ -	$ 1.230.728.519,00	$ 867.185.391,00	$ 868.388.308,00	$ 1.848.235.246,00
TICS 2	Brindar servicios de soporte y operación	$ -	$ 10.089.999,00	$ 45.946.904,00	$ 91.065.994,00	$ 96.229.797,00	$ 143.117.882,00
TICS 3	Realizar actualizaciones y mantenimiento de software	$ -	$ 129.255.420,00	$ 204.680.000,00	$ 1.038.240.000,00	$ -	$ 5.256.000,00
TICS 4	Adquirir y desarrollar software de acuerdo a los requerimientos de la Entidad para llevar a cabo sus labores misionales, estratégicas y de apoyo	$ -	$ -	$ -	$ -	$ -	$ -
TICS 5	Brindar los servicios de gestión de capacidad de ti	$ -	$ -	$ -	$ -	$ -	$ -
Total		**$ -**	**$ 139.345.419,00**	**$ 1.481.355.423,00**	**$ 1.996.491.385,00**	**$ 964.618.105,00**	**$ 1.996.609.128,00**

Fuente. Documentos de indicadores del proyecto de inversión suministrado por la Oficina TIC.

Actualmente, se está estructurando un nuevo proyecto de inversión con vigencia 2026–2035, que incluirá actividades similares, focalización, metas e indicadores. Este nuevo proyecto busca garantizar la continuidad de la financiación tecnológica del Ministerio.

Respecto a los proyectos de inversión, la Oficina de Control Interno observa lo siguiente:

- Los contratos suscritos por la Oficina TIC se realizan con financiamiento del proyecto de inversión.
- Actualmente se realiza una asociación manual de la información del avance de las actividades y entregables del proyecto de inversión

realizado por la Oficina TIC y la información que da cuenta de la ejecución financiera, por lo cual, se recomienda analizar la posibilidad de sistematizar las asociaciones para disminuir la posibilidad de ocurrencia de errores en el resultado.

RIESGOS Y CONTROLES IDENTIFICADOS

Teniendo en cuenta que, de manera paralela, junto con la emisión del presente informe, la Oficina de Control Interno liberó en octubre de 2025 el informe de seguimiento a la Gestión de Riesgos, en dicho informe se incluyó el detalle de la evaluación de diseño y efectividad de los Riesgos y Controles del Proceso de Gestión de Tecnologías de Información y las Comunicaciones. No obstante, a continuación, se hace referencia a las principales situaciones y recomendaciones emitidas.

RIESGOS DE GESTIÓN

RIESGOS IDENTIFICADOS POR la OFICINA TIC:

Tabla No 16. Descripción de Riesgos y controles de gestión.

Riesgos	Controles
GTI-5: Posibilidad de afectación reputacional por Incumplimiento de acuerdos de nivel de servicio debido a la inadecuada prestación de servicio de soporte técnico en la Entidad (Mesa de servicio)	1. Verificar el cumplimiento de los tiempos establecidos en los ANS definidos en el contrato. 2. Evaluar la calidad del servicio prestado desde la Mesa de ayuda a la Entidad por medio de Encuestas de nivel de satisfacción con el fin mejorar el servicio y la atención a los usuarios. 3. Identificar los casos en los cuales se afectó el tiempo de respuesta por parte de la mesa de ayuda en la atención al usuario, con el fin de mejorar la eficacia del servicio prestado a la Entidad. 4. Actualizar la documentación en el Sistema Integrado de Gestión en relación con los Acuerdos de Nivel de Servicio (ANS) implementados en la Entidad.

Fuente. Matriz de Riesgos de la OTIC.

OBSERVACIONES Y RECOMENDACIONES DE LA OFICINA DE CONTROL INTERNO:

Se observa que, para el riesgo definido actualmente, los controles se enfocan únicamente en el soporte tecnológico. Debido a esto, se recomienda analizar la posibilidad de establecer riesgos adicionales con sus respectivos controles, por ejemplo:

- Posibilidad de interrupción en la disponibilidad de los sistemas de información institucionales y afectación de la continuidad operativa de procesos misionales y administrativos generando fallas en la infraestructura tecnológica o en los servicios de conectividad debido a deficiencias en el mantenimiento preventivo de los equipos o en la gestión de proveedores de servicios tecnológicos.
- Posibilidad de disminución en el rendimiento y funcionalidad de los sistemas tecnológicos y afectación en la eficiencia operativa y en la capacidad de respuesta institucional por uso de software o hardware desactualizado u obsoleto debido a alta de planificación estratégica para la renovación tecnológica o insuficiencia presupuestal
- Posibilidad de sanciones y observaciones por parte de entes de control y afectación de la imagen institucional y posibles consecuencias legales por implementación incorrecta de políticas de protección de datos, gobierno digital y otras normativas, debido a desconocimiento o interpretación errónea de la normatividad vigente por parte del personal TIC
- Posibilidad de retrasos o fallas en la implementación de soluciones tecnológicas y afectación en la ejecución de planes y proyectos institucionales y pérdida de recursos por deficiencias en la planificación o seguimiento de los proyectos TIC debido a falta o inadecuadas metodologías de gestión de proyectos o debilidades en la articulación con las áreas solicitantes y usuarias.
- Posibilidad de errores operativos, incumplimientos normativos, pérdida de trazabilidad en la gestión tecnológica, afectación de la calidad, eficiencia y legalidad de los procesos de la Oficina TIC por ausencia o desactualización de procedimientos, manuales técnicos y registros de activos de información, debido a falta o debilidades de implementación del sistema de gestión documental actualizado.

RIESGOS DE CORRUPCIÓN

RIESGOS IDENTIFICADOS POR la OFICINA TIC:

Tabla No 17. Descripción de Riesgos y controles de gestión.

Riesgos	Controles
GTI-2: Posibilidad de manipulación o acceso no autorizado a cuentas de correo institucional para beneficio propio o de terceros mediante la creación fraudulenta de cuentas institucionales por parte de administradores o personal autorizado.	1. Verificar que las solicitudes de creación de cuenta tengan una solicitud aprobada por contratos o talento humano. 2. Identificar las causas por las cuales se permitió la creación de cuentas de usuario sin las autorizaciones requeridas.

Fuente. Matriz de Riesgos de la OTIC.

OBSERVACIONES Y RECOMENDACIONES DE LA OFICINA DE CONTROL INTERNO:

El riesgo definido en la actualidad solamente está enfocado en el acceso no autorizado a las cuentas de correo institucional. Sin embargo, la situación descrita se podría presentar en todos los sistemas y aplicativos institucionales. Adicionalmente, teniendo en cuenta los diferentes perfiles que se pueden asignar en los sistemas y herramientas de TI, se podría especificar diferentes tipos de riesgo de acceso, unos enfocados a la lectura, con lo cual se estaría dando acceso a información clasificada, y enfocado a la escritura o modificación, lo cual estaría dando acceso a manipulación de información afectando la integridad.

Respecto al riesgo, se recomienda ampliar el alcance al riesgo actual para que cubra los sistemas de información institucionales, y pueda especificar escenarios de acceso a información reservada o a su modificación no autorizada.

Se recomienda analizar la posibilidad de incluir riesgos de corrupción que puedan abarcar por ejemplo los siguientes aspectos:

- Riesgo de direccionamiento en la adquisición de software o hardware, haciendo uso del poder para favorecer a proveedores específicos en procesos de compra tecnológica, debido a la elaboración de especificaciones técnicas que excluyen competidores o se ajustan a un proveedor en particular, generando sobrecostos, baja calidad en los productos adquiridos, pérdida de transparencia. Con posibles causas en

el conflicto de interés y falta de control en la formulación de requerimientos.

- Riesgo de manipulación de sistemas de información para ocultar irregularidades, dando posibilidad de que funcionarios alteren bases de datos o sistemas para encubrir actos indebidos, por medio de la modificación de registros, eliminación de trazabilidad, y alteración de reportes, generando pérdida de información crítica, obstrucción de auditorías, y sanciones legales. Con posibles causas por acceso privilegiado sin control, ausencia de segregación de funciones, y cultura permisiva.
- Riesgo de contratación de personal técnico sin criterios de mérito, generando la posibilidad de que se vincule personal en áreas TIC por razones políticas o personales, sin cumplir requisitos técnicos, ocasionando bajo desempeño, errores en la gestión tecnológica, y dependencia de terceros, provocando ineficiencia operativa, vulnerabilidad en sistemas, y pérdida de confianza institucional. Con posibles causas en la falta de controles en selección, y presión externa.
- Riesgo de uso indebido de recursos tecnológicos para fines personales o externos, debido a la posibilidad de que funcionarios utilicen equipos, software o infraestructura tecnológica para fines no institucionales, permitiendo el uso de servidores para actividades privadas, instalación de software no autorizado, y desvío de recursos, generando deterioro de activos, sanciones disciplinarias, y afectación a la operación institucional. Con posibles causas en la falta de supervisión, ausencia de políticas de uso, y cultura organizacional permisiva.

RIESGOS DE SEGURIDAD DIGITAL

RIESGOS IDENTIFICADOS POR la OFICINA TIC:

Tabla No 18. Descripción de Riesgos y controles de gestión.

Riesgos	Controles
GTI-1: Posibilidad de afectación reputacional por interrupción de la continuidad de negocio debido a un a un ataque informático que explote vulnerabilidades en la plataforma tecnológica de la Entidad.	1. Ejecutar de forma oportuna y efectiva la aplicación de parches y actualizaciones de seguridad en la plataforma tecnológica de la entidad. 2. Verificar el monitoreo de seguridad en la plataforma tecnológica por medio de registros y análisis de manera continua sobre las actividades y eventos

	relacionados con la seguridad Informática sobre la plataforma tecnológica de la Entidad.
GTI-2: Posibilidad de afectación económica por uso de software no licenciado debido a la inadecuada configuración de permisos de instalación de los equipos de usuario final	1. Verificar la información detallada sobre los programas instalados, versiones, licencias correspondientes y cualquier software no autorizado o no licenciado en los equipos de la Entidad. 2. Establecer la configuración de línea base de software y la restricción de privilegios de usuario/administrador en los sistemas y equipos de la entidad. Esto implica establecer una configuración estándar y segura de los sistemas, restringir los privilegios de usuario y administrador, y limitar la instalación de software no autorizado o no licenciado. 3. Desinstalar y revocar permisos de administrador cuando se identifique software no autorizado e instalado en los equipos de la Entidad.
GTI-3: Posibilidad de afectación reputacional por perdida de información debido a daños irreversibles en la información o documentos contenidos dentro de los repositorios administrados por el proceso GTIC.	1. Validar los backup generados sobre un ambiente de producción con el fin de asegurar que no existan errores y que se hayan creado exitosamente las copias de seguridad. 2. Verificar que el operador cumpla con las políticas de respaldo de información establecidas dentro del contrato.
GTI-4: Posibilidad de afectación reputacional por la indisponibilidad de los servicios de tecnología debido a la utilización de cuentas nombradas en el directorio activo asignadas a usuarios no existentes en la Entidad.	1. Validar que solo los usuarios autorizados y existentes reciban cuentas en el directorio activo. 2. Identificar las causas por las cuales se permitió la creación de cuentas de usuario sin las autorizaciones requeridas y la depuración de cuentas sin su respectiva autorización o inexistencia del usuario.

Fuente. Matriz de Riesgos de la OTIC.

OBSERVACIONES Y RECOMENDACIONES DE LA OFICINA DE CONTROL INTERNO:

- De acuerdo con Función Pública, la estructura para riesgos de seguridad de información es: "posibilidad de pérdida de integridad, disponibilidad, o confidencialidad", seguido por la identificación del activo de información

afectado, junto con la descripción de la amenaza y la consecuencia. Aunque la definición de los riesgos incluye elementos clave (amenaza, activo, consecuencia), la forma no se ajusta al formato requerido, no cumple completamente con la estructura establecida por la Función Pública.

- No se evidencian acciones de tratamiento de los riesgos de seguridad digital.

RIESGOS FISCALES

OBSERVACIONES Y RECOMENDACIONES DE LA OFICINA DE CONTROL INTERNO:

Para la matriz de riesgos de la vigencia 2025, La Oficina TIC no formuló riesgos fiscales ni controles asociados.

ACCIONES DE MEJORAMIENTO

No se estableció en el alcance para el presente informe.

HALLAZGOS

FORTALEZAS:

A continuación, se referencian aspectos positivos identificados durante el proceso de auditoría que evidencian buenas prácticas, cumplimiento normativo, eficiencia operativa o mejoras implementadas por la entidad. Las fortalezas reflejan elementos que contribuyen al logro de los objetivos institucionales y pueden servir como referencia para otras áreas o procesos:

1. Del Marco de Referencia de Arquitectura Empresarial (MRAE), se resalta el uso de herramientas como Enterprise Architect para visualizar la documentación de arquitectura empresarial, la existencia de repositorio documental organizado con los artefactos generados (catálogos, matrices, vistas), y la articulación del MRAE con el PETI y establecimiento de la Comisión de Sistemas de Información.
2. De la Mesa de Servicios, altos niveles de cumplimiento en los indicadores de atención: Respuesta por chat: hasta 99,69%, Asignación de casos: hasta 99,55%, y Solución de incidentes y requerimientos VIP: 100%.

3. Para la Gestión de Capacidad y Disponibilidad, se cuenta con procedimientos definidos para monitoreo y alertas preventivas, e informes trimestrales de capacidad con recomendaciones.
4. De la Gestión del Datacenter, se resalta el cumplimiento de ANS en almacenamiento, backup y bases de datos, la realización de restauraciones exitosas de bases de datos y respaldo diario/mensual, y avances en la implementación de Plan de Recuperación de Desastres (DRP) con ejecución de pruebas controladas.
5. Sobre el fomento del Uso y Aprovechamiento de Datos, la implementación de los proyectos de Bodega de datos misionales, la Estrategia geoespacial con ArcGIS, y la alineación con la Estrategia Nacional de Datos del DNP
6. De Uso y Apropiación de TIC, la ejecución del plan con avance del 42% en el primer semestre, y la realización continua de actividades de capacitación, campañas de seguridad, socialización de herramientas.
7. Frente a la Gestión de Proveedores, la Organización documental de los contratos, la supervisión activa de contratos con informes y actas, y la aplicación de descuentos cuando se identifican incumplimientos en ANS.

OPORTUNIDADES DE MEJORA:

Durante el desarrollo de la auditoría al proceso de Gestión de Tecnologías de la Información, se identificaron diversas oportunidades de mejora que, de ser atendidas oportunamente, podrían fortalecer la eficiencia operativa, la seguridad de la información, la calidad del servicio y el cumplimiento normativo de la Oficina TIC. A continuación, se presentan las principales oportunidades de mejora:

1. Al analizar la caracterización del proceso de Gestión de TIC, documento GTI-C-01, se observa que el objetivo del proceso es: "*Planificar, implementar y realizar seguimiento al Plan Estratégico de las Tecnologías de la Información - PETI en el Ministerio de Vivienda, Ciudad y Territorio, dando cumplimiento a los requisitos de las normas, políticas y lineamientos vigentes, permitiendo la toma de decisiones oportunas en pro del desempeño institucional y sectorial en materia de Tecnologías de la Información.".* Se recomienda revisar con la Oficina Asesora de Planeación cuales son los lineamientos para la estructuración de los objetivos de los procesos, debido a que el objetivo de la OTI está orientado al instrumento PETI, el cual es un medio para un fin, pero no es un objetivo de proceso. Generalmente los objetivos de los procesos se orientan en la prestación de servicios de TI con algunos criterios

institucionales como la calidad y oportunidad, por ejemplo: "Diseñar, prestar y mantener a disposición servicios TIC a las partes interesadas del MVCT garantizando su uso eficiente y seguro, alineado estos servicios con los objetivos institucionales, para optimizar la gestión administrativa interna y de cara al ciudadano."

2. Se recomienda adoptar los formatos establecidos por MinTIC para la medición del avance en la implementación del Marco de Referencia de Arquitectura Empresarial permitiendo una validación formal del cumplimiento, mejora la alineación con estándares nacionales y facilita la rendición de cuentas ante entes de control.
3. Se sugiere implementar un indicador específico para identificar rezagos en la atención de casos que no cumplen los Acuerdos de Nivel de Servicio para mejora la trazabilidad, permite identificar cuellos de botella y optimiza la atención al usuario.
4. Se evidenció la necesidad de desactivar cuentas de usuarios desvinculados en sistemas como GESDOC, SIGEVAS, ULISES y SINAS, así como avanzar en la autenticación centralizada para los que permitan la integración con el Directorio Activo, reduciendo así riesgos de seguridad, mejorando el control de accesos.
5. Algunos documentos del SPG requieren ajuste, dado que las actividades ahora se ejecutan mediante tercerización para el caso del Datacenter, lo cual busca mejorar la coherencia documental y facilita la ejecución operativa, y supervisión contractual.
6. Se recomienda analizar la configuración y desempeño del sistema de seguridad perimetral, especialmente tras el evento de ransomware, debido a que, pese a la ocurrencia del incidente de seguridad por el ataque de Ransomware el Firewall reportó una alta disponibilidad.
7. Dado que no se renovó la licencia de FortiMail, se sugiere validar si ATP cubre adecuadamente las funcionalidades requeridas necesarias para garantizar la continuidad de la protección del correo electrónico y evitar brechas de seguridad.
8. Implementar esquemas de monitoreo de disponibilidad para los servicios de interoperabilidad, con el objetivo de tener la capacidad de detectar fallas de forma proactiva, mejorar la eficiencia operativa y la experiencia del usuario.
9. Aunque existe un documento con el Plan de Apertura de Datos Abiertos, este no está incorporado formalmente en el sistema institucional, por lo cual se

recomienda su inclusión formal, asegurando su implementación, mejorando la transparencia y fortaleciendo la cultura de datos.

10. Se recomienda finalizar y adoptar el Modelo Operativo de Gobierno de Datos en colaboración con la Oficina Asesora de Planeación, lo cual espera impacto positivo en la mejora de la calidad de la información, facilitar la toma de decisiones y reduciendo riesgos asociados a datos.
11. Realizar acciones de sistematización de la asociación entre ejecución financiera y actividades para los reportes de avance de los proyectos de inversión para disminuir la posibilidad de incluir errores al ingresar los datos a reportar, mejorando la trazabilidad presupuestal y facilita el seguimiento técnico.

OBSERVACIONES:

Las observaciones, son situaciones que en primera instancia no reflejan incumplimientos de acuerdo con el alcance del presente informe, pero podrían generar una brecha que pueda afectar negativamente el cumplimiento normativo, la gestión o eficiencia administrativa de la Oficina TIC e incluso a nivel institucional. A continuación, se presenta la observación identificada:

Observación No. 1 **Debilidad en el reporte de avance en la implementación del PETI 2023–2026 durante el primer semestre de 2025**	
Condición	Durante el seguimiento al avance del Plan Estratégico de Tecnologías de la Información (PETI) 2023–2026, con corte al 30 de junio de 2025, se evidenció un avance acumulado del 35% en la ejecución de los hitos establecidos para el segundo semestre de 2025. Este resultado refleja un cumplimiento inferior al esperado, considerando que varios proyectos presentaron avances inferiores a lo programado. Entre los hitos con bajo desempeño se destacan: 1) Actualización del diagnóstico del MSPI (60% de avance frente al 100% planeado). 2) Establecimiento de fundamentos para Zero Trust (60% frente al 100%). 3) Pruebas de continuidad de servicios de DRP (60%

	frente al 100%). 4) Mejoras al sistema de información SIGEVAS (0% frente al 50%). 5) Mejora al sistema de información SINAS (0% frente al 50%). 6) Identificación y caracterización de fuentes de información (0% frente al 100%). 7) Implementación de herramientas de Inteligencia Artificial (0% frente al 100%). 8) Actualizar el repositorio de arquitectura empresarial y consolidar la documentación de sistemas de información (80% frente al 100%).
Criterio	• **Decreto 1078 de 2015** – Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. • **Decreto 767 de 2022** – Lineamientos de la Política de Gobierno Digital. • **Hoja de Ruta** del Plan Estratégico de Tecnologías de la Información (PETI) 2023–2026 del MVCT.
Causa	Posibles causas: • Insuficiente asignación de recursos técnicos y humanos para el desarrollo de las iniciativas. • Retrasos en la definición y aprobación de herramientas normativas y técnicas necesarias para la ejecución de algunos proyectos. • Limitaciones en la articulación interinstitucional para proyectos de interoperabilidad y sistemas misionales.
Recomendación	• Fortalecer el monitoreo periódico del avance de los hitos del PETI, estableciendo alertas tempranas para mitigar desviaciones. • Revisar la programación de actividades y reasignar recursos técnicos y humanos para garantizar el cumplimiento de los hitos críticos. • Establecer mecanismos de coordinación más efectivos entre las áreas responsables de los proyectos, especialmente en iniciativas de interoperabilidad y sistemas misionales. • Priorizar la aprobación y adopción de herramientas normativas y técnicas necesarias para la ejecución de

	los proyectos.

Observación No. 2 **Ejecución de Contratos con objeto y entregables de funcionamiento financiados por Proyectos de Inversión**	
Condición	Durante el proceso de auditoría, se identificó que la ejecución de los contratos suscritos por la Oficina de Tecnología se realiza principalmente con recursos provenientes de proyectos de inversión. Se evidenció que varios de estos contratos están orientados a atender necesidades operativas y de funcionamiento del área, tales como soporte técnico, mantenimiento de infraestructura tecnológica y servicios recurrentes.
Criterio	• **Decreto 2104 de 2023, que sustituye el Título 6 del Decreto 1082 de 2015 y fortalece el Sistema Unificado de Inversión Pública (SUIP).** Según esta normativa, los recursos de inversión deben destinarse exclusivamente a proyectos que generen valor público, con viabilidad técnica, económica y social, y que estén registrados en el Banco de Programas y Proyectos del Departamento Nacional de Planeación (DNP). • **Decreto 111 de 1996 – Estatuto Orgánico del Presupuesto, Artículo 36.** Define los gastos de funcionamiento como aquellos necesarios para el ejercicio normal de las funciones de la entidad, incluyendo: Servicios personales (nómina, honorarios, viáticos, etc.), Gastos generales (mantenimiento, arrendamientos, suministros, etc.), y Transferencias. Los gastos de inversión, por el contrario, están destinados a proyectos que generan valor público, como infraestructura, desarrollo institucional, o implementación de políticas públicas. • **Concepto C-826 de 2025 – Colombia Compra Eficiente**. Aclara que un mismo contrato puede incluir gastos de funcionamiento e inversión, siempre que estén claramente justificados y respaldados presupuestalmente. Sin embargo, no se debe financiar

	el funcionamiento con recursos de inversión, salvo que estos gastos sean parte integral del desarrollo del proyecto. • **Sentencia de la Corte Constitucional (C-337 de 1993 y C-151 de 1995).** Refuerza el principio de programación integral del gasto, indicando que los proyectos de inversión deben contemplar explícitamente los compromisos de funcionamiento que acarrean, pero no deben confundirse con gastos operativos permanentes.
Causa	Los recursos asignados institucionalmente a la Oficina TIC provienen principalmente de los proyectos de inversión que formulan periódicamente.
Recomendación	Revisar la clasificación presupuestal de los contratos ejecutados por la Oficina de Tecnología, con el fin de garantizar la correcta aplicación de los recursos públicos y el cumplimiento de la normatividad vigente en materia de inversión pública, toda vez que las instancias presupuestales del Ministerio asignen a esta Oficina los valores requeridos por medio de presupuesto de funcionamiento.

NO CONFORMIDADES

A continuación, se presentan los hallazgos que evidencian incumplimiento de requisitos normativos, políticas institucionales, procedimientos internos o estándares aplicables. Las no conformidades pueden generar riesgos operativos, legales, financieros o reputacionales, y requieren acciones correctivas por parte de la entidad:

No conformidad No. 1 **Debilidad en el cumplimiento de los plazos para la implementación del Marco de Referencia de Arquitectura Empresarial – MRAE**	
Condición	La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) ha avanzado en la implementación del Marco de Referencia de Arquitectura

	Empresarial (MRAE), logrando el cumplimiento del 91% de los 106 lineamientos establecidos. Sin embargo, se evidenció que, a la fecha de corte del 23 de septiembre de 2025, no se ha alcanzado el 100% de cumplimiento requerido por la Resolución 1978 del 26 de mayo de 2023, lo que representa un incumplimiento en los plazos definidos para su adopción total. Adicionalmente, la medición del avance se ha realizado mediante formatos internos, sin aplicar la metodología oficial del MinTIC, lo que podría generar diferencias en la valoración del cumplimiento.
Criterio	La Resolución 1978, emitida el 26/05/2023 estableció los criterios para la adopción del Marco de Referencia del Arquitectura Empresarial, definiendo los siguientes plazos para su implementación: • 11 meses para implementar el 40% de avance, plazo cumplido el 24/04/2024. • 18 meses para implementar el 70% de avance, plazo cumplido el 23/11/2024. • 25 meses para implementar el 100% de cumplimiento, plazo cumplido el 24/06/2025.
Causa	Causas probables: • Aplicación de una metodología interna de seguimiento que no contempla los formatos oficiales del MinTIC, lo que dificulta la medición formal del avance conforme a los criterios de impacto y complejidad. • Priorización de lineamientos según criterios internos, lo que pudo haber postergado la implementación de algunos lineamientos considerados de menor urgencia. • Limitaciones en la capacidad operativa o técnica para abordar simultáneamente todos los lineamientos del MRAE dentro del plazo establecido.
Efecto	Incumplimiento normativo, lo que podría generar observaciones por parte de entes de control o afectar la imagen institucional frente al MinTIC.

Responsable	Oficina de Tecnologías de la Información y las Comunicaciones
Recomendación	• Adoptar de manera prioritaria los formatos oficiales de medición del MRAE establecidos por el MinTIC, para garantizar una evaluación objetiva y alineada con los criterios normativos. • Establecer un plan de acción para la revisión de los lineamientos implementados, haciendo énfasis en la implementación de los lineamientos que no se han implementado, con metas claras y responsables definidos, que permita alcanzar el 100% de cumplimiento en el menor tiempo posible. • Fortalecer los mecanismos de seguimiento y control interno, articulando los avances del MRAE con los reportes oficiales requeridos por el MinTIC, asegurando la trazabilidad y transparencia del proceso.

No conformidad No. 2 **Debilidad en la gestión de accesos a sistemas de información del Ministerio**	
Condición	La Oficina TIC cuenta con el procedimiento "GTI-P-06 Solicitud de Servicios de Red y Creación de Cuentas de Usuario" para la gestión de accesos a sistemas de información. Sin embargo, se evidenciaron debilidades en la desactivación oportuna de cuentas de usuario, especialmente de colaboradores desvinculados del Ministerio. El equipo auditor identificó cuentas activas en los sistemas GESDOC (46), SIGEVAS (6), ULISES (44) y SINAS (1) correspondientes a personas que ya no tienen vínculo laboral o contractual con la Entidad, junto con cuentas de usuarios que están activas pese a que los usuarios no acceden a estas desde antes de diciembre 31 de 2024. Además, se observó que el documento "GCT-F-50_V2 paz y salvo contratistas" no contempla alertas automáticas para la Oficina TIC al momento de la desvinculación, lo

	que limita la capacidad de respuesta para desactivar accesos de forma oportuna.
Criterio	Debilidad en la implementación de los siguientes lineamientos establecidos en el GTI-M-03_V5_MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL: • A.5.15 Control de acceso – Suministro de credenciales personales a usuarios autorizados, acceso seguro a la plataforma tecnológica, y verificación periódica de los permisos de acceso. • A.5.16 Gestión de identidad - Procedimientos para crear y cancelar usuarios, manejo de homónimos, y retiro de credenciales de quienes ya no tengan vínculo con el Ministerio. • A.5.18 Derechos de acceso – Ajuste de los accesos según cambios de rol por parte de los propietarios de los sistemas, autenticación vía directorio activo en nuevos desarrollos, y gestión de identidades mediante el administrador de la plataforma.
Causa	• Debilidad de la integración entre los procesos de desvinculación de personal y la gestión de accesos por parte de la Oficina TIC. • Falta de implementación de mecanismos automatizados de alerta o sincronización con Talento Humano y Contratación. • Persistencia de sistemas que no utilizan autenticación centralizada mediante Directorio Activo. • Omisión en la actualización del procedimiento GTI-P-06 para contemplar controles específicos ante desvinculaciones.
Efecto	• Riesgo de acceso no autorizado a información institucional por parte de personas sin vínculo vigente. • Exposición de datos sensibles o confidenciales, afectando la seguridad de la información y la reputación institucional. • Posibles observaciones por parte de entes de control, que podrían derivar en acciones correctivas o sancionatorias.

Responsable	Oficina de Tecnologías de la Información y las Comunicaciones, articulado con la Coordinación de Talento Humano y la Coordinación de Contratos.
Recomendación	• Implementar un mecanismo automatizado de alertas que permita la desactivación inmediata de cuentas de usuario al momento de la desvinculación, en coordinación con Talento Humano y Contratación. • Actualizar los procedimientos internos para incluir controles específicos ante la desvinculación de colaboradores. • Fortalecer la depuración periódica de usuarios en todos los sistemas de información, eliminando cuentas inactivas o de personas desvinculadas. • Avanzar en la autenticación centralizada de todos los sistemas mediante el Directorio Activo, para facilitar el control de accesos.

No conformidad No. 3 **Vulnerabilidades técnicas en el Portal Web Institucional que afectan la seguridad digital**	
Condición	En el marco de la verificación del Índice de Transparencia Activa (ITA) y del cumplimiento del Anexo 3 de la Resolución 1519 de 2020 del MinTIC, la Oficina de Control Interno realizó una revisión técnica independiente al Portal Web Institucional. Como resultado de una prueba de penetración básica, se identificaron cinco vulnerabilidades que podrían comprometer la seguridad del sitio, incluyendo fallas en cabeceras de seguridad, exposición de tecnologías utilizadas, presencia de cuentas obsoletas y errores en el código HTML. Estas debilidades podrían ser aprovechadas por terceros para afectar la confidencialidad, integridad o disponibilidad de la información.
Criterio	• Resolución 1519 de 2020 del MinTIC – Anexo 3: Condiciones mínimas técnicas y de seguridad digital para sitios web institucionales.

	• Ley 1712 de 2014 – Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional. • Ley 1581 de 2012 – Protección de datos personales. • Modelo de Seguridad y Privacidad de la Información (MSPI) – Recomendado por el MinTIC como marco de referencia para la gestión de seguridad digital.
Causa	Posible falta de revisión periódica de estándares de seguridad digital conforme al Anexo 3 de la Resolución 1519.
Efecto	• Exposición a ataques de tipo XSS (Cross-Site Scripting), robo de información o manipulación del sitio web. • Riesgo de rastreo de usuarios y fuga de información sensible por cabeceras mal configuradas. • Facilitación de ataques dirigidos mediante la identificación de tecnologías vulnerables. • Pérdida de confianza institucional, afectando la imagen del Ministerio ante ciudadanos y entes de control. • Incumplimiento de la normatividad vigente, lo que podría derivar en observaciones por parte del MinTIC o ColCERT.
Responsable	Oficina de Tecnologías de la Información y las Comunicaciones
Recomendación	Coordinar con el proveedor de infraestructura y seguridad para definir e implementar un plan de remediación técnica, alineado con el Modelo de Seguridad y Privacidad de la Información (MSPI) y los lineamientos del Anexo 3 de la Resolución 1519 de 2020.

En consecuencia, es preciso elaborar un plan de mejoramiento, en el cual se deben incorporar tanto las acciones preventivas en relación con las oportunidades de mejora y las acciones correctivas o acciones de mejora para atender las no conformidades, ante lo cual, se debe tener en cuenta lo definido en el Procedimiento Formulación Plan de mejoramiento vigente o el que haga sus veces.

RELACIÓN CON PAI Y PEI	APLICA		NO APLICA	X

No se estableció en el alcance para el presente informe.

CONCLUSIONES

La auditoría realizada al proceso de Gestión de Tecnologías de la Información del Ministerio de Vivienda evidenció avances en la implementación de planes estratégicos, gestión operativa y adopción de buenas prácticas en infraestructura tecnológica, seguridad digital, interoperabilidad y uso de datos.

Se destacan fortalezas como el cumplimiento de indicadores de servicio, la estructuración del Marco de Referencia de Arquitectura Empresarial (MRAE), la consolidación de proyectos de datos misionales y el desarrollo de iniciativas de apropiación tecnológica.

No obstante, se identificaron oportunidades de mejora y no conformidades que requieren atención prioritaria, especialmente en la gestión de accesos a sistemas de información, cumplimiento de plazos normativos, monitoreo de servicios de interoperabilidad y fortalecimiento de controles de seguridad digital. Estas situaciones, pueden representar riesgos latentes que deben ser mitigados para garantizar la continuidad, eficiencia y seguridad de los servicios tecnológicos institucionales.

RECOMENDACIONES

Elaborar un plan de mejoramiento integral, que incluya acciones correctivas para las no conformidades identificadas y las acciones preventivas para las oportunidades de mejora presentadas en la sección de hallazgos del presente informe, articulado con la metodología establecida por el Ministerio.

PAPELES DE TRABAJO

Se cuenta con repositorio de información en SharePoint de la auditoría con las solicitudes y remisión de evidencias proporcionadas por la Oficina TIC, junto con los registros de agendas, videos y transcripciones de las reuniones realizadas por medio de MS Teams.

CUMPLIMIENTO DE LOS PRINCIPIOS DE AUDITORIA Y LIMITACIONES

Para la realización de esta evaluación, se aplicaron Normas de Auditoría Generalmente Aceptadas, teniendo en cuenta que las pruebas realizadas se efectuaron mediante muestreo selectivo, por consiguiente, no se cubrió la verificación de la efectividad de todas las medidas de control del proceso. Igualmente, durante su desarrollo se aplicaron los principios de integridad, objetividad, confidencialidad, competencia, manifestando además que, no se presentaron limitaciones, así como tampoco, se dio lugar a la presentación de conflicto de intereses que pudiera afectar o impedir su desarrollo y resultado.

FIRMAS:

JOSÉ JORGE ROCA MARTÍNEZ	**CARLOS ALBERTO QUIÑONES C.**
JEFE OFICINA DE CONTROL INTERNO	AUDITOR OCI

ELABORÓ: CARLOS QUIÑONES – CONTRATISTA OCI

REVISÓ: JOSÉ JORGE ROCA – JEFE OCI