| **FECHA DE EMISIÓN DEL INFORME** | **Día:** | 14 | **Mes:** | 04 | **Año:** | 2026 |
|---|---|---|---|---|---|---|

| | |
|---|---|
| **Nombre de la auditoría** | Validación de la funcionalidad del software ADA. |
| **Dependencia, proceso y/o grupo de trabajo, objeto de auditoría** | Oficina Asesora de Planeación y Sistemas – OAPS<br>x<br>Líder Proceso GSTI |
| **Funcionarios directivos, coordinadores o líderes del proceso a auditar** | Angélica María Zamora Acosta; Jefe OAPS<br><br>Cesar Augusto Macias; Líder Proceso GSTI |
| **Tipo de Auditoría (Ley o Interna)** | Interna |
| **Objetivo de la actividad a realizar** | Verificar el funcionamiento del Sistema de Información Misional ADA, analizando su correcta funcionalidad y satisfacción de los usuarios. |
| **Objetivos primarios y alcances** | Para los siguientes alcances, se hará sobre lo actuado y gestionado desde el 01-01-2025 hasta 28-02-2026.<br><br>1. Verificar la funcionalidad del software ADA de acuerdo con el ciclo de desarrollo de software y los cronogramas definidos en la entidad.<br><br>2. Verificar la gestión de Incidentes y Requerimientos frente el estado de satisfacción de los usuarios.<br><br>3. Verificar el cumplimiento de los controles de los riesgos identificados y valorados del proceso a evaluar; así mismo, proponer identificación de riesgos y controles respectivos. |
| **Criterios de la Auditoría:** | • Ley 87 de 1993: Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado.<br><br>• Resolución 2023120002585 de 2023: "Por la cual se adoptaron y aprobaron el Marco Estratégico Institucional 2023 - 2026 "Super - Visión Efectiva", el Plan Estratégico Institucional 2023 -2026 y el Plan de Acción Anual Institucional 2023, de la Supersolidaria".<br><br>• Plan Estratégico de Tecnologías de la Información – PETI.<br><br>• Circular Básica Contable y Financiera, incluyendo los anexos técnicos. |

| | |
|---|---|
| | • ISO/IEC 27001:2022. Tecnología de la información — Técnicas de seguridad — Sistemas de gestión de la seguridad de la información (SGSI) — Requisitos.<br><br>• ITIL (Information Technology Infrastructure Library) Biblioteca de Infraestructura de Tecnologías de la Información (actualmente ITIL 4).<br><br>• COBIT (Control Objectives for Information and Related Technologies). Objetivos de Control para la Información y Tecnologías Relacionadas (versión vigente: COBIT 2019). |

## 1. COMPROMISO ÉTICO EN EL EJERCICIO DE LA AUDITORÍA INTERNA

i. Código de Ética del Auditor Interno que tiene como bases fundamentales, la integridad, objetividad, confidencialidad, conflictos de interés y competencia de este.

ii. Estatuto de auditoría, en el cual se establecen y comunican las directrices fundamentales que definen el marco dentro del cual se desarrollan las actividades de la Oficina de Control Interno, según los lineamientos de las normas internacionales de auditoría.

## 2. COMPROMISO DEL AUDITADO

Mediante carta de representación de 12 de marzo de 2026, suscrita por la Dra. Angélica María Zamora Acosta como jefe o líder del proceso a unidad auditada, ha declarado su responsabilidad en la oportuna preparación, presentación integral y consistencia de la información que fue entregada en el marco de la auditoría a la unidad de control interno.

## 3. ACTIVIDADES REALIZADAS DEL PLAN DE TRABAJO

Teniendo en cuenta el objetivo general, objetivos primarios y respectivo alcance, de la auditoria, mencionados anteriormente, se desarrollaron de manera previa o posterior, respectivamente, las siguientes actividades:

a) Conocimiento del proceso o dependencia.

b) Diseño del plan de auditoría: Se estableció la programación del plan de trabajo para el desarrollo de la auditoría, de modo que permitiera lograr el objetivo propuesto.

c) Reunión de apertura: La apertura de la auditoría se agendó a través del correo electrónico remitido el 26 de febrero de 2026 donde se describió la metodología a utilizar.

d) Obtención y análisis de la información: Fue solicitada la información pertinente, relacionada con el objetivo y alcances, que fuese relevante, útil, basada en hechos y confiable. Soportada en los respectivos papeles de trabajo.

e) Análisis y evaluación de la información. La revisión fue basada en factores críticos de éxito, en estrategias y objetivos del aspecto evaluable, en los riesgos altos y extremos, metas y objetivos del proceso, con enfoque hacia la consecución de los alcances de la auditoría.

f) Informe preliminar e informe final: Se socializó el informe preliminar el 8 de abril de 2026, para que se presente por parte del proceso las inquietudes sobre hallazgos y observaciones, previo a la emisión del informe final.

g) Frente al informe preliminar el proceso no presentó observaciones e informó que lo evidenciado permitirá fortalecer el proceso de desarrollo seguro.

## 4. DESARROLLO DE AUDITORÍA

Como metodología aplicada para el desarrollo de los 3 alcances definidos, se realizaron reuniones previas donde el proceso contextualizó sobre la normativa interna y externa aplicable y en forma general cómo se realizó el desarrollo del sistema misional ADA. Adicionalmente, se realizó un requerimiento el 06-03-2026 donde se solicitó información sobre los cronogramas de desarrollo, su aprobación por parte de la Entidad, documentación interna, los incidentes y requerimientos de desarrollo, usuarios y roles, ANS, encuestas de satisfacción, riesgos y controles del desarrollo de software; posteriormente, se analizaron las evidencias y soportes suministrados, y se concluyó el ejercicio de auditoría. Posteriormente, al analizar la información suministrada, se realizó una reiteración y alcance al primer requerimiento y para lo cual, se entregaron las respuestas el 27 de marzo de 2026.

A continuación, se describe el ejercicio realizado:

### 4.1. ALCANCE 1. Verificar la funcionalidad del software ADA de acuerdo con el ciclo de desarrollo de software y los cronogramas definidos en la entidad.

**CONDICIÓN.**

Se realizó una primera solicitud de informar sobre los cronogramas y planes para el desarrollo del software ADA definidos desde el 2025 a la fecha, incluyendo los soportes de su aprobación oficial y los soportes de cumplimiento de cada actividad. Al validar la información suministrada y dadas las primeras observaciones sobre información no precisa, se reiteró y solicitó ampliación de la información de la siguiente manera:

a. Exportar el cronograma Sistema ADA completo en formato excel, con las 465 filas que se presentaron en el documento PDF inicial.

b. Informar explícitamente si este cronograma remitido es el único definido y aplicado para las vigencias 2025 y lo corrido de 2026.

Al particular, el proceso indicó que:

*a. (…) se precisa que el cronograma del Sistema de Información Misional ADA se encuentra definido a partir de 17 actividades clave, las cuales corresponden a la estructura oficial de planificación y seguimiento. El documento inicialmente remitido en formato PDF presenta dichas actividades de manera consolidada. Posteriormente, se compartió un archivo en formato Excel que corresponde a un instrumento de apoyo para el seguimiento operativo, el cual no hace parte de la versión oficial del cronograma. En ese sentido, se remite el cronograma en formato Excel conforme a la estructura oficial, manteniendo las 17 actividades clave y sus respectivas fechas de cumplimiento.*
*b. (…) el cronograma remitido corresponde al único cronograma definido y aplicado para el desarrollo del Sistema de Información Misional ADA durante la vigencia 2025 y lo corrido de 2026. Este cronograma se encuentra asociado al proyecto PY01 del Plan Estratégico de Tecnologías de la Información. En cuanto a su aprobación, se precisa que mediante la sesión 07 del Comité de gestión y desempeño celebrada el 12 de diciembre de 2024 fue aprobado el PETI por los miembros del comité con voto, dentro del cual se encuentra incluido el proyecto PY01 correspondiente al Sistema de Información Misional ADA. Así mismo, el 29 de agosto de 2025 se realizó una modificación al PETI, la cual fue igualmente aprobada en sesión del comité de gestión y desempeño.*

Al evaluar toda la información suministrada se identificó:

**Hallazgo 1. Deficiencias en el cronograma de desarrollo del Software ADA y de su aprobación oficial en la entidad.**

**Caso 1. Debilidades en la información del cronograma.**

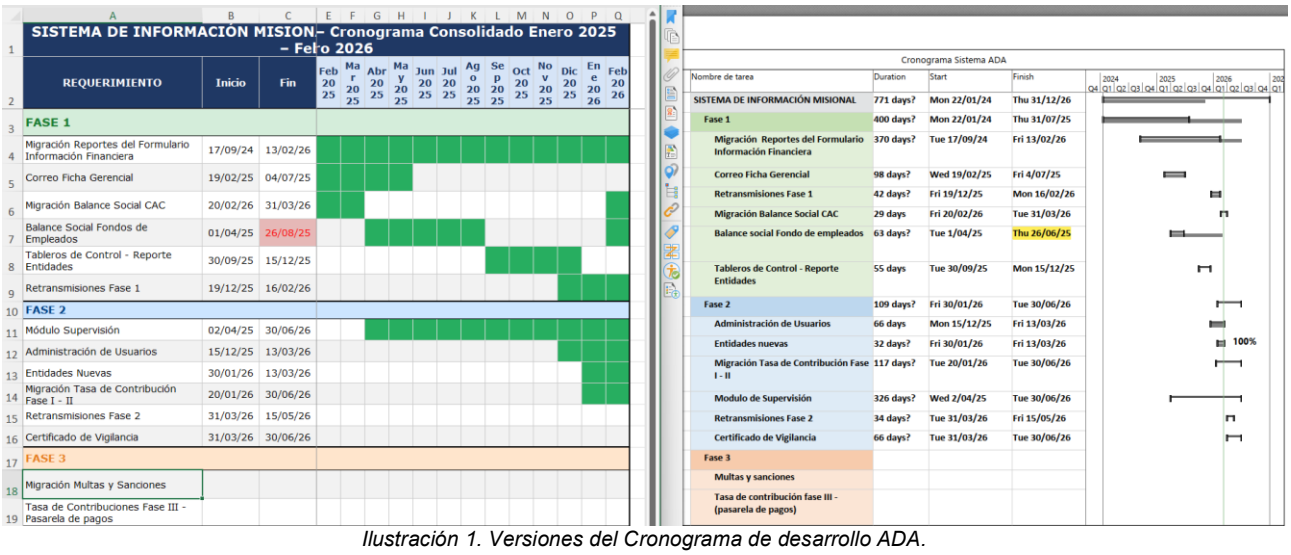
Con relación al requerimiento del punto 1 sobre cronogramas del desarrollo del software ADA, se realiza la validación de los soportes suministrados y se identifica que el cronograma del desarrollo del software ADA inicialmente entregado en PDF con las 17 actividades que se precisó como "la estructura oficial de planificación y seguimiento" difiere en una (1) actividad en su fecha comparándolo con el soporte de cronograma enviado en excel (archivo "Cronograma_ConsolidadoVF") y citado como "cronograma en formato Excel conforme a la estructura oficial".

La actividad "Balance Social Fondos de Empleados" inicialmente finalizaba en "26/06/25" y en la segunda versión del cronograma finalizó en "26/08/2025", es decir, 2 meses después.

Así mismo, el cronograma PDF contiene varias inconsistencias en las fechas:

a. La fase 1 tiene una duración desde 22-01-2024 al 31-07-2025, sin embargo:
   - Tiene tareas que inician después de la fecha máxima (19-12-2025, 20-02-2026, 30-09-2025).
   - Tienen tareas que finalizan después de la fecha máxima (13-02-2026, 16-02-2026, 31-03-2026)

b. La fase 2 tiene una duración desde 30-01-2026 al 30-06-2026, sin embargo:
   - Tiene tareas que inician antes de la fecha mínima (15-12-2025, 20-01-2026, 02-04-2025).



SISTEMA DE INFORMACIÓN MISIONAL – Cronograma Consolidado Enero 2025 – Febrero 2026

| REQUERIMIENTO | Inicio | Fin |
|---|---|---|
| FASE 1 | | |
| Migración Reportes del Formulario Información Financiera | 17/09/24 | 13/02/26 |
| Correo Ficha Gerencial | 19/02/25 | 04/07/25 |
| Migración Balance Social CAC | 20/02/26 | 31/03/26 |
| Balance Social Fondos de Empleados | 01/04/25 | 26/08/25 |
| Tableros de Control - Reporte Entidades | 30/09/25 | 15/12/25 |
| Retransmisiones Fase 1 | 19/12/25 | 16/02/26 |
| FASE 2 | | |
| Módulo Supervisión | 02/04/25 | 30/06/26 |
| Administración de Usuarios | 15/12/25 | 13/03/26 |
| Entidades Nuevas | 30/01/26 | 13/03/26 |
| Migración Tasa de Contribución Fase I - II | 20/01/26 | 30/06/26 |
| Retransmisiones Fase 2 | 31/03/26 | 15/05/26 |
| Certificado de Vigilancia | 31/03/26 | 30/06/26 |
| FASE 3 | | |
| Migración Multas y Sanciones | | |
| Tasa de Contribuciones Fase III - Pasarela de pagos | | |

Cronograma Sistema ADA

| Nombre de tarea | Duration | Start | Finish |
|---|---|---|---|
| SISTEMA DE INFORMACIÓN MISIONAL | 771 days? | Mon 22/01/24 | Thu 31/12/26 |
| Fase 1 | 400 days? | Mon 22/01/24 | Thu 31/07/25 |
| Migración Reportes del Formulario Información Financiera | 370 days? | Tue 17/09/24 | Fri 13/02/26 |
| Correo Ficha Gerencial | 98 days? | Wed 19/02/25 | Fri 4/07/25 |
| Retransmisiones Fase 1 | 42 days? | Fri 19/12/25 | Mon 16/02/26 |
| Migración Balance Social CAC | 29 days | Fri 20/02/26 | Tue 31/03/26 |
| Balance social Fondo de empleados | 63 days? | Tue 1/04/25 | Thu 26/06/25 |
| Tableros de Control - Reporte Entidades | 55 days | Tue 30/09/25 | Mon 15/12/25 |
| Fase 2 | 109 days? | Fri 30/01/26 | Tue 30/06/26 |
| Administración de Usuarios | 66 days | Mon 15/12/25 | Fri 13/03/26 |
| Entidades nuevas | 32 days? | Fri 30/01/26 | Fri 13/03/26 |
| Migración Tasa de Contribución Fase I - II | 117 days? | Tue 20/01/26 | Tue 30/06/26 |
| Modulo de Supervisión | 326 days? | Wed 2/04/25 | Tue 30/06/26 |
| Retransmisiones Fase 2 | 34 days? | Tue 31/03/26 | Fri 15/05/26 |
| Certificado de Vigilancia | 66 days? | Tue 31/03/26 | Tue 30/06/26 |
| Fase 3 | | | |
| Multas y sanciones | | | |
| Tasa de contribución fase III - (pasarela de pagos) | | | |

*Ilustración 1. Versiones del Cronograma de desarrollo ADA.*

## Caso 2. Debilidades en la planeación y aprobación del cronograma.

Con relación al requerimiento del punto 2 sobre la aprobación de los Cronogramas del desarrollo del software ADA, se indicó que "Este cronograma se encuentra asociado al proyecto PY01 del Plan Estratégico de Tecnologías de la Información", sin embargo:

a. El PETI fue aprobado con el acta 07-2024 el 12-12-2024, pero el cronograma u hoja de ruta indica que el proyecto "PY01 Sistema de información misional" inició en febrero 2024; esto mismo se confirma en el cronograma PDF donde indica que la fase 1 inició el 22-01-2024. Por lo anterior, no es claro cómo se aprobó este el PETI en diciembre de 2024 con un proyecto que inició 10 meses antes.

b. Fases 1 y 2 de los cronogramas:
   El cronograma del proyecto del PETI de Dic-2024 tienen las siguientes fechas:
   - Fase 1: Febrero 2024 - Diciembre 2024 (10 meses).
   - Fase 2: Agosto 2024 - Diciembre 2026 (17 meses).

El cronograma del proyecto del PETI de Ago-2025 tiene las siguientes fechas:
- Fase 1: Febrero 2024 - Agosto 2025 (19 meses).
- Fase 2: Septiembre 2025 - junio 2026 (9 meses).

Se identifica que la fase 1 inicialmente duraba 10 meses y se actualizó a 19 meses, y la fase 2 que inicialmente se planeó a 19 meses se redujo a 9 meses. Con lo anterior se identifica una debilidad en la planeación y aprobación del cronograma.

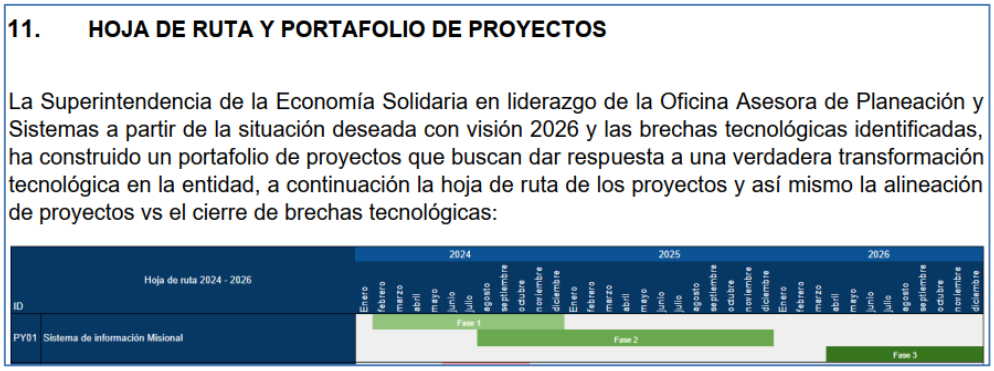



*Ilustración 2. PETI Diciembre-2024: Fase 1: Febrero 2025 - Agosto 2025. Fase 2: Septiembre 2025 - Junio 2026.*


*Ilustración 3. PETI Agosto-2025: Fase 1: Febrero 2025 - Diciembre 2024. Fase 2: Agosto 2024 - Diciembre 2025.*

El no contar con un cronograma preciso y que esté adecuadamente aprobado por la Entidad, puede implicar los siguientes riesgos:

- Riesgo de información inconsistente: Existen dos cronogramas oficiales con fechas diferentes.
- Riesgo de incumplimiento: El aplazamiento de la actividad puede afectar compromisos y plazos.
- Riesgo de falta de trazabilidad: No hay control de versiones ni gestión formal del cambio.
- Riesgo de observaciones de entes de control: Susceptible de configurarse como hallazgo administrativo.
- Riesgo de debilidad de control interno: El cambio de fecha no evidencia justificación ni aprobación formal.

**Hallazgo 2. No entrega de información o la información suministrada se encuentra inconsistente.**

**Caso 1. Soporte de la ejecución de las actividades del cronograma.**

Con relación al requerimiento del punto 3 se solicitó los soportes de cumplimiento de las actividades del cronograma, sin embargo, se entregaron las relaciones de actividades extraída de Microsoft Project, en los cuales se presentan porcentajes de avance/cumplimiento, o con fechas, lo cual no soporta que la actividad se haya desarrollado:

- Migración del Reporte F.O.R.C: Solo con fechas.
- Envió Ficha Gerencial: 100%.
- Balance Social CAC: 100%.
- Balance Social Fondos de Empleados: Documento con formato diferente; algunos con 100%, otros sin porcentaje, otros con duración de 0 días, entre otros.
- Tableros de Control - Reporte Entidades: 100%.
- Retransmisiones Fase 1: Algunos con 100% otros sin porcentaje.
- Modulo Supervisión: Todos los porcentajes en cero (0) %. El primer ítem inició el 02-04-2025.
- Administración de Usuarios: 100%.
- Entidades Nuevas: 100%.
- Migración Tasa Contribuciones: Todos los porcentajes en cero (0) %. El primer ítem inició el 20-01-2026.

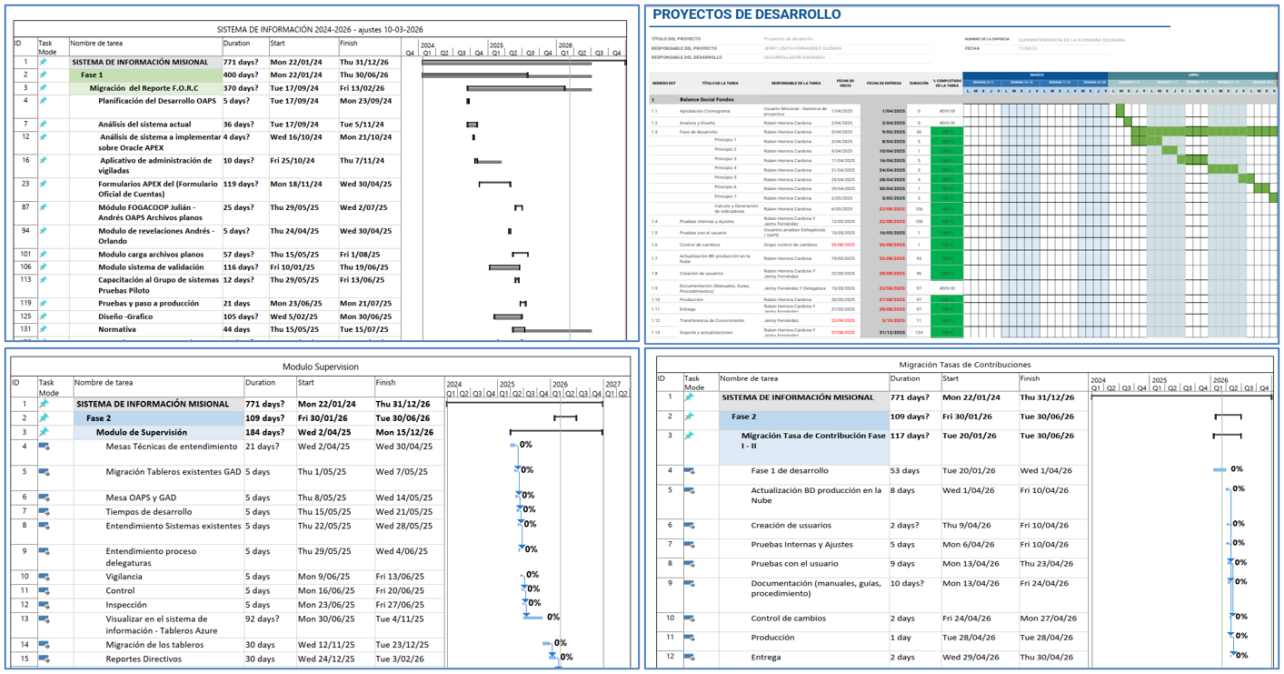



*Ilustración 4. Información suministrada proceso.*

**Caso 2. Los formatos y procedimientos suministrados como evidencias contienen imprecisiones, campos vacíos y debilidades en su diligenciamiento.**

Se solicitó con el requerimiento numeral 4 y con la reiteración realizada, la documentación interna de la Entidad para el desarrollo de software, los procedimientos, políticas y manuales definidos para el desarrollo de software y para los formatos, cómo se realizan las respectivas aprobaciones. Al particular el proceso indicó:

> *"La gestión y control de requerimientos del nuevo sistema se formaliza mediante el formato FT-GSTI-004 Formato de Requerimientos de software, disponible en el repositorio compartido. Cabe destacar que, gracias a la transformación digital del proyecto, las guías de uso y operación ahora están integradas directamente en el sistema ADA. No obstante, de manera informativa, se ha cargado el instructivo original del antiguo sistema SICSES como material de consulta. El procedimiento que rige los desarrollos de los sistemas en la Supersolidaria es el PR-GSTI-003 Procedimiento para la gestión de aplicaciones, igualmente se carga en la unidad compartida".*
> *"En el formato FT-GSTI-005, la fecha de aprobación se registra en la sección denominada "Aprobación Para Paso A Desarrollo", en la cual se consignan las fechas correspondientes a los responsables.*
> *En el formato FT-GSTI-008, la aprobación se encuentra en la sección grupo de control de cambios : Nombre, cargo, Fecha de aprobación y si fue aprobado por los integrantes del equipo de control de cambios.*
> *Los formatos FT-GSTI-005 y FT-GSTI-008 hacen parte de la operación del Sistema de Información Misional ADA, el cual corresponde a la migración del sistema previamente utilizado (SICSES). En este sentido, los requerimientos, estructuras y formatos asociados ya se encontraban definidos y en operación en el sistema anterior, bajo los mecanismos de gestión y control vigentes en su momento. Por lo anterior, no corresponden a desarrollos nuevos sujetos a aprobación individual en el marco del sistema actual, sino a la continuidad de elementos previamente implementados. En el contexto del sistema ADA, estos formatos se incorporan como parte de dicha migración y de la operación del sistema".*

Al validar las evidencias entregadas, se identificaron varias situaciones con relación a la ejecución del procedimiento y el diligenciamiento de los formatos:

1. El procedimiento "PR_GSTI_003_Gestion_De_Aplicaciones_V2" no tiene definido el formato "FTFT-GSTI-006 Pruebas de Desarrollo de Software".

2. Se validaron los formatos suministrados para todos los desarrollos y se identificó que, en casi todos los formatos, existe incompletitud de información o campos sin diligenciar:

    a. Para el formato "FT-GSTI-004" se encontraron muchos campos sin diligenciar: Responsable, Fecha de Aplicación (Vigencia), Periodicidad, Es Viable, Herramienta, Categoría, Mockup, entre otras. Versión Fecha (dd/mm/yyyy),

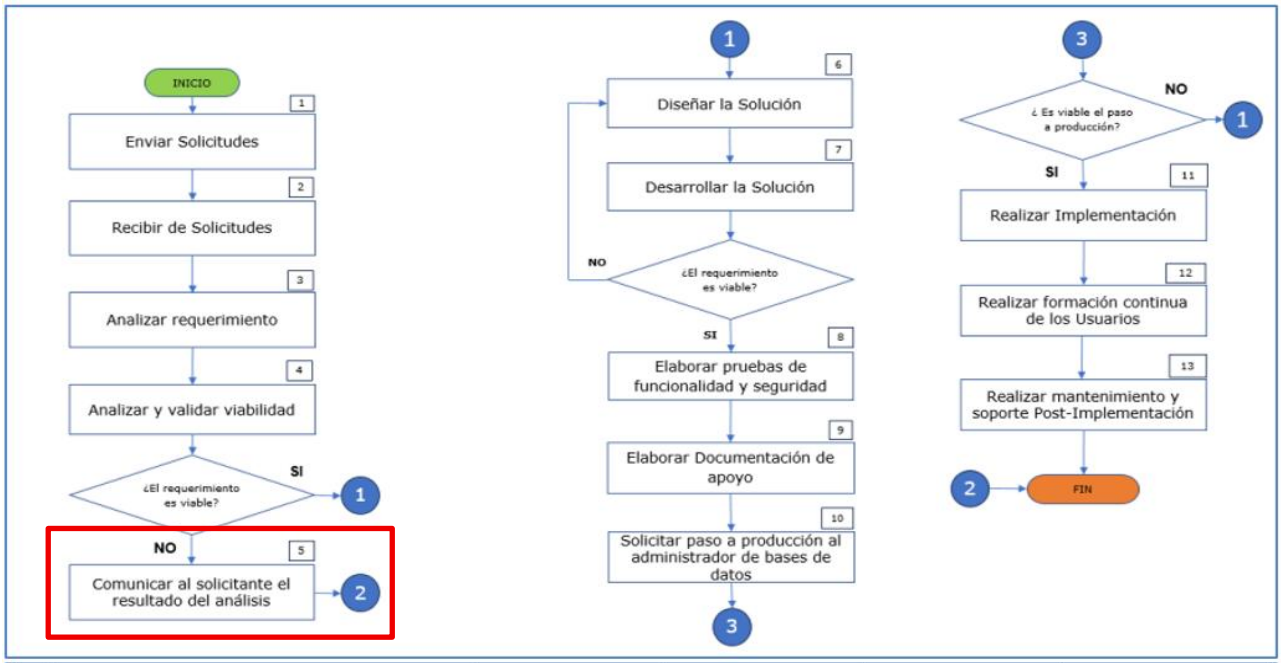
Cambios realizados, Autor, Responsable.

b. Para el formato "FT-GSTI-005" se encontraron muchos campos sin diligenciar: Nombre solicitante, Nombre líder técnico, Nombre responsable de proyecto, fecha, Observaciones del desarrollador.
c. Para el formato "FT-GSTI-006" se encontraron muchos campos sin diligenciar: campos asociados al ambiente de pruebas.
d. Para el formato "FT-GSTI-008" se encontraron muchos campos sin diligenciar: "Aprobado" y "Información resultados del despliegue".

3. Para el desarrollo "Envío de Correo Ficha Gerencial" no se entregó el formato "FT-GSTI-008".

4. La actividad 5 del procedimiento está incoherente con el flujograma "Flujograma pr-gsti-003 gestión de aplicaciones":

- La actividad 5 indica "Comunicar al solicitante el resultado del análisis: Después de realizado el análisis de viabilidad del requerimiento, se le comunica la respuesta positiva o negativa al solicitante", sin embargo,
- el flujograma precisa que solo se comunica si se responde "NO" a la pregunta "El requerimiento es viable?, es decir, solo se comunica cuando no sea viable el requerimiento".



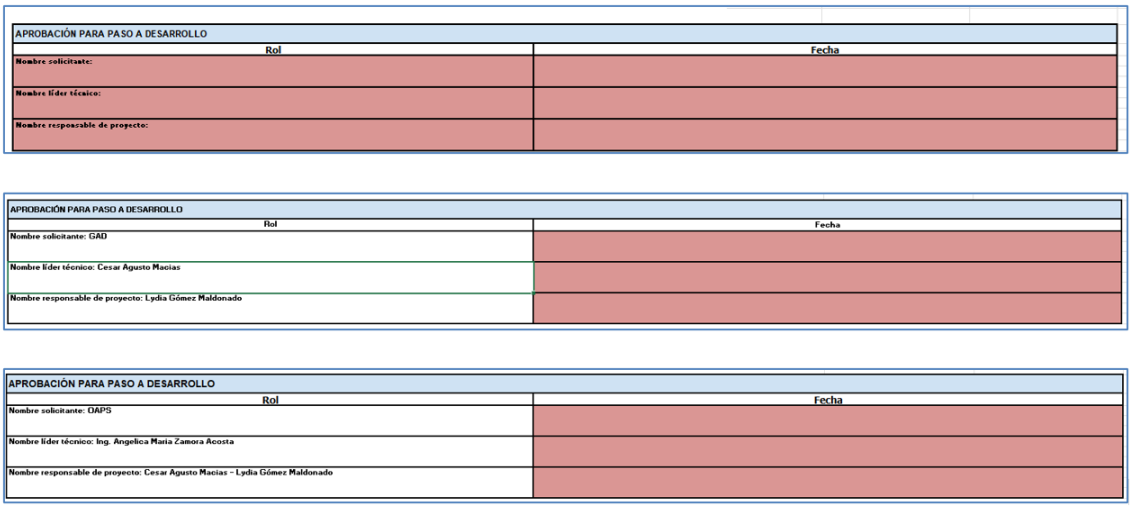

| | | | | | |
|---|---|---|---|---|---|
| 5 | **Comunicar al solicitante el resultado del análisis:** Después de realizado el análisis de viabilidad del requerimiento, se le comunica la respuesta positiva o negativa al solicitante. | Ingeniero de Requerimientos | | Viabilidad y Lista de Entregables (FT-GSTI-005) | Memorando del resultado de la viabilidad del proyecto |

*Ilustración 5. Incoherencia entre el Flujograma Vs Actividades.*

5. Para el formato "FT-GSTI-008" se encontraron incoherencias entre las fechas de los formatos y adicionalmente, no es claro cuál es la fecha de aprobación:

- **Tasa de contribución:**
  - Fecha de presentación= 28/01/2026
  - Aprobación funcional del cambio (Fecha)= 29/01/2026
  - Control de cambios= 29/01/2026
  - Revisión Post-Implementación (PIR) = 10/09/2025 (8 meses después)
- **ADA:**
  - Fecha de presentación= 29/08/2025
  - Aprobación funcional del cambio (Fecha)= 1/09/2025
  - Control de cambios= 29/09/2025 (28 días posteriores)
  - Revisión Post-Implementación (PIR) = 2/09/2025
- **Balance Social fee:**
  - Fecha de presentación= 12/09/2025
  - Aprobación funcional del cambio (Fecha)= 11/09/2025 (Se aprobó 1 día antes de presentarse)
  - Control de cambios= 11/09/2025
  - la fecha del cambio=13/09/2025 de 6 pm a 8:00 pm
  - Revisión Post-Implementación (PIR) = 10/09/2025 (Se realizó la revisión 3 días antes de aprobarlo).

6. El proceso indicó que "En el formato FT-GSTI-005, la fecha de aprobación se registra en la sección denominada "Aprobación para paso a desarrollo". Se identificó que no se realizó la aprobación de todos los desarrollos por parte de la Entidad ("Balance Social Fondos de Empleados", "Balance Social Cooperativas de Ahorro y Crédito", "Envío de Correo Ficha Gerencial", "F.O.R.C", "Migración de Tasa de Contribuciones"), dado que no se registró la información: fecha, sin Nombre solicitante, Nombre líder técnico, Nombre responsable de proyecto. Lo anterior conlleva a que se implementó el desarrollo a producción sin cumplir el formato establecido.



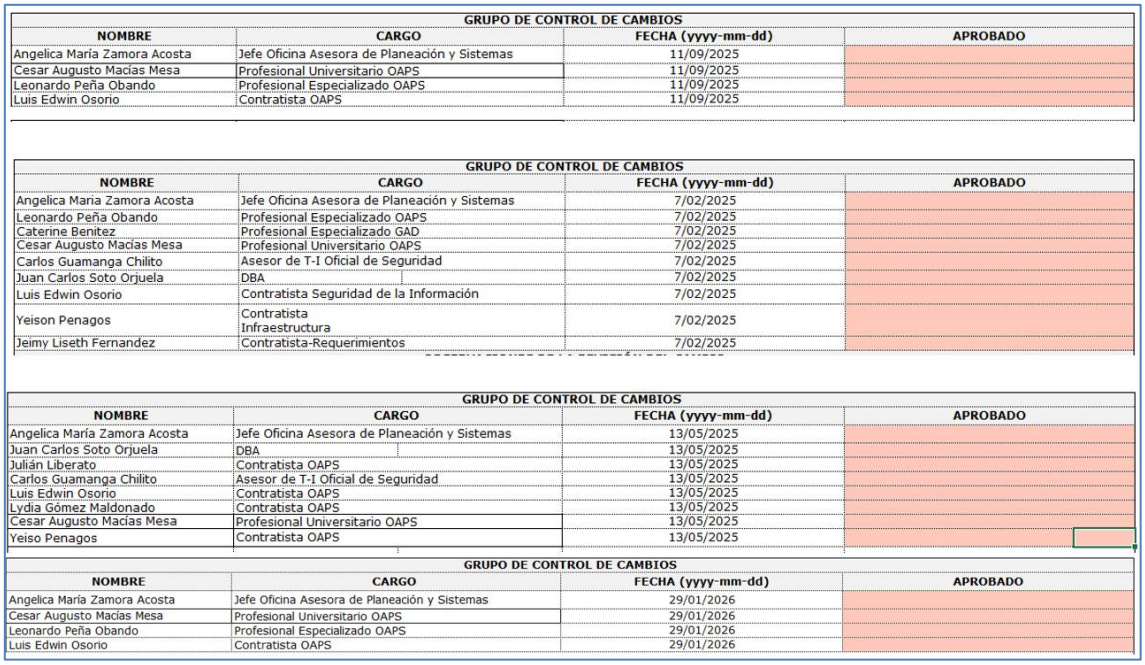
| APROBACIÓN PARA PASO A DESARROLLO | |
|---|---|
| Rol | Fecha |
| Nombre solicitante: | |
| Nombre líder técnico: | |
| Nombre responsable de proyecto: | |

| APROBACIÓN PARA PASO A DESARROLLO | |
|---|---|
| Rol | Fecha |
| Nombre solicitante: GAD | |
| Nombre líder técnico: Cesar Agusto Macias | |
| Nombre responsable de proyecto: Lydia Gómez Maldonado | |

| APROBACIÓN PARA PASO A DESARROLLO | |
|---|---|
| Rol | Fecha |
| Nombre solicitante: OAPS | |
| Nombre líder técnico: Ing. Angelica Maria Zamora Acosta | |
| Nombre responsable de proyecto: Cesar Agusto Macias - Lydia Gómez Maldonado | |

*Ilustración 6. Ejemplos: "Balance Social Fondos de Empleados", "Balance Social Cooperativas de Ahorro y Crédito", "F.O.R.C"*

7. El proceso indicó que "*En el formato FT-GSTI-008, la aprobación se encuentra en la sección grupo de control de cambios: Nombre, cargo, Fecha de aprobación y si fue aprobado por los integrantes del equipo de control de cambios*". Se identificó que no se realizó la aprobación del paso a producción de este desarrollo por parte de la Entidad, dado que no se registró toda la información: fecha, sin Nombre solicitante, Nombre líder técnico, Nombre responsable de proyecto. Lo anterior conlleva a que se implementó el desarrollo a producción sin cumplir el formato establecido.



GRUPO DE CONTROL DE CAMBIOS

| NOMBRE | CARGO | FECHA (yyyy-mm-dd) | APROBADO |
|---|---|---|---|
| Angelica María Zamora Acosta | Jefe Oficina Asesora de Planeación y Sistemas | 11/09/2025 | |
| Cesar Augusto Macías Mesa | Profesional Universitario OAPS | 11/09/2025 | |
| Leonardo Peña Obando | Profesional Especializado OAPS | 11/09/2025 | |
| Luis Edwin Osorio | Contratista OAPS | 11/09/2025 | |

GRUPO DE CONTROL DE CAMBIOS

| NOMBRE | CARGO | FECHA (yyyy-mm-dd) | APROBADO |
|---|---|---|---|
| Angelica Maria Zamora Acosta | Jefe Oficina Asesora de Planeación y Sistemas | 7/02/2025 | |
| Leonardo Peña Obando | Profesional Especializado OAPS | 7/02/2025 | |
| Caterine Benitez | Profesional Especializado GAD | 7/02/2025 | |
| Cesar Augusto Macías Mesa | Profesional Universitario OAPS | 7/02/2025 | |
| Carlos Guamanga Chilito | Asesor de T-I Oficial de Seguridad | 7/02/2025 | |
| Juan Carlos Soto Orjuela | DBA | 7/02/2025 | |
| Luis Edwin Osorio | Contratista Seguridad de la Información | 7/02/2025 | |
| Yeison Penagos | Contratista Infraestructura | 7/02/2025 | |
| Jeimy Liseth Fernandez | Contratista-Requerimientos | 7/02/2025 | |

GRUPO DE CONTROL DE CAMBIOS

| NOMBRE | CARGO | FECHA (yyyy-mm-dd) | APROBADO |
|---|---|---|---|
| Angelica María Zamora Acosta | Jefe Oficina Asesora de Planeación y Sistemas | 13/05/2025 | |
| Juan Carlos Soto Orjuela | DBA | 13/05/2025 | |
| Julián Liberato | Contratista OAPS | 13/05/2025 | |
| Carlos Guamanga Chilito | Asesor de T-I Oficial de Seguridad | 13/05/2025 | |
| Luis Edwin Osorio | Contratista OAPS | 13/05/2025 | |
| Lydia Gómez Maldonado | Contratista OAPS | 13/05/2025 | |
| Cesar Augusto Macías Mesa | Profesional Universitario OAPS | 13/05/2025 | |
| Yeiso Penagos | Contratista OAPS | 13/05/2025 | |

GRUPO DE CONTROL DE CAMBIOS

| NOMBRE | CARGO | FECHA (yyyy-mm-dd) | APROBADO |
|---|---|---|---|
| Angelica María Zamora Acosta | Jefe Oficina Asesora de Planeación y Sistemas | 29/01/2026 | |
| Cesar Augusto Macías Mesa | Profesional Universitario OAPS | 29/01/2026 | |
| Leonardo Peña Obando | Profesional Especializado OAPS | 29/01/2026 | |
| Luis Edwin Osorio | Contratista OAPS | 29/01/2026 | |

*Ilustración 7. Desarrollos sin información de aprobación.*

**CRITERIO**:

- Ley 87 de 1993: Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado.
- Resolución 2023120002585 de 2023: "Por la cual se adoptaron y aprobaron el Marco Estratégico Institucional 2023 - 2026 "Super - Visión Efectiva", el Plan Estratégico Institucional 2023 -2026 y el Plan de Acción Anual Institucional 2023, de la Superintendencia de la Economía Solidaria".
- Plan Estratégico de Tecnologías de la Información – PETI.
- Circular Básica Contable y Financiera, incluyendo los anexos técnicos.

Igualmente, existen las directrices del Sistema de Control Interno, en donde define los principios de calidad de la información (exactitud, completitud, oportunidad) y de Responsabilidad del custodio del activo.

**CAUSAS**:

- Falta de una planificación formal y estandarizada del cronograma del desarrollo.

- Ausencia de un proceso claro de revisión y aprobación del cronograma por las instancias competentes.
- Debilidades en la gestión documental y control de evidencias del proyecto

- Uso inadecuado de formatos, falta de lineamientos para su diligenciamiento y escaso control de calidad de la información.

**CONSECUENCIAS O EFECTOS**:

- Dificultad para hacer seguimiento efectivo al avance del desarrollo del software.
- Riesgo de retrasos, reprocesos o desviaciones no identificadas oportunamente.
- Falta de trazabilidad y soporte de las actividades ejecutadas.
- Posibles hallazgos y no conformidades en procesos de auditoría o control interno.
- Debilitamiento de la toma de decisiones y de la rendición de cuentas.

**RECOMENDACIONES DEL EQUIPO AUDITOR.**

- Definir y formalizar un cronograma integral, con actividades, responsables, fechas y criterios de seguimiento.
- Establecer un proceso de revisión y aprobación formal del cronograma y sus actualizaciones.
- Implementar mecanismos de control documental, asegurando evidencias completas, consistentes y oportunas.
- Estandarizar los formatos y procedimientos, y capacitar a los responsables en su correcto diligenciamiento.
- Realizar revisiones periódicas de la información del proyecto para garantizar su calidad y consistencia.

### 4.2. Alcance 2. Verificar la gestión de Incidentes y Requerimientos frente el estado de satisfacción de los usuarios.

**CONDICIÓN 1.**

Con el requerimiento con numeral 6 se solicitó indicar y remitir los procedimientos, políticas y manuales definidos en la Entidad para la gestión de incidentes del software ADA (de todas sus etapas de desarrollo de software) y requerimientos incluyendo el reporte de los incidentes registrados o gestionados durante el 2025 y 2026. Se precisó sobre los conceptos de incidentes, no para los eventos de seguridad de la información, sino los incidentes propios de un desarrollo de software:

- ITIL (Gestión de servicios de TI): Cualquier interrupción no planificada de un servicio de TI, una reducción en la calidad del servicio, o un evento que aún no ha impactado el servicio, pero que puede hacerlo.
- ISO/IEC 20000 (estándar internacional): Una interrupción no planificada a un

servicio, una reducción en la calidad del servicio, o un evento que aún no ha impactado al cliente.
- DevOps: Cualquier evento en producción que degrade la experiencia del usuario, viole acuerdos de nivel de servicio (SLA/SLO), o comprometa la estabilidad del sistema.
- Ejemplos: Caída de una aplicación en producción; Error crítico tras un despliegue; Fallo de base de datos que afecta a usuarios.

Al respecto, el proceso indicó que:

> "*(…) se informa que, durante el periodo comprendido entre enero de 2025 y febrero de 2026, no se han presentado incidentes asociados al funcionamiento del Sistema de Información Misional ADA en ambiente de producción (…).*
> *En la Entidad se dispone del Procedimiento de Gestión de Incidentes, código PR-GETI-005, el cual establece lineamientos aplicables de manera transversal a todos los sistemas de información implementados para la atención de incidentes desde el enfoque de seguridad de la información.*
> *En relación con la solicitud de versiones y documentos aplicables durante el periodo comprendido entre enero de 2025 y febrero de 2026, se informa que no se cuenta con documentos específicos adicionales en materia de incidentes del software ADA*".

Con la información y respuestas suministradas se identificó que:

**Hallazgo 3. No se identificó un procedimiento para gestión de incidentes de los sistemas de información (No eventos de seguridad de la información o ciberseguridad).**

En el procedimiento "PR_GSTI_003_Gestion_de_aplicaciones_v2" suministrado se identifica que en la actividad 13 precisan estos incidentes como: "*(...) resolviendo las fallas y errores que se puedan presentar con el fin de brindar el apoyo para el uso y aprovechamiento adecuado del aplicativo Permanentemente se actualiza y se aplican las mejoras continuas al aplicativo*" y genera como registros de evidencia los "Reportes de mantenimiento y mejoras", incluyendo la documentación soporte.

El proceso informó que durante el 2025 y 2026, no se han presentado incidentes asociados al funcionamiento del Sistema de Información Misional ADA en ambiente de producción, sin embargo, es necesario disponer de un procedimiento formal para que los usuarios de los sistemas de información, herramientas y software instalados puedan reportarlos, generar una base de datos de conocimiento y definir las lecciones aprendidas.

Adicionalmente, se reiteró la solicitud en la entrega del procedimiento para el manejo de incidentes relacionados con el software ADA "*en cualquiera de sus etapas de desarrollo*" incluyendo desarrollo y producción, sin embargo, el proceso solo respondió parte del alcance solicitado, aclarando los incidentes en el ambiente productivo: "*no se*

*han presentado incidentes asociados al funcionamiento del Sistema de Información Misional ADA en ambiente de producción*", por lo cual, no se dio respuesta particular a las demás etapas.

De acuerdo con las definiciones de "Incidente" presentadas anteriormente, es cualquier interrupción no planificada o degradación de un servicio o sistema, y puede ocurrir antes de que el software esté en producción, es decir, durante el ciclo de vida del desarrollo:

- Diseño: Errores de requisitos, fallas de arquitectura, dependencias no consideradas.
- Desarrollo: Fallos en compilación, integraciones defectuosas, bloqueos técnicos.
- Pruebas: Interrupciones de ambientes, defectos críticos sin priorización clara.
- Producción: Caídas del servicio, errores funcionales, degradación del desempeño.

Un procedimiento formal de gestión de incidentes permite registrar, clasificar, priorizar, resolver y aprender de estas interrupciones, evitando la atención informal o reactiva por parte de la Entidad; el no contar con este procedimiento de manera formal, implica estar en contravía de lo dispuesto en varias de las buenas prácticas que la Entidad vienen adoptando:

- ITIL - Gestión de Incidentes: La gestión de incidentes garantiza que el funcionamiento normal del servicio se restablezca lo más rápido posible después de un incidente, minimizando el impacto adverso en las operaciones. Impacta dado que la Entidad realiza una atención de incidentes sin trazabilidad ni priorización uniforme.

- ISO/IEC 20000 - Gestión de incidentes y solicitudes de servicio. Exige un proceso definido para identificar, registrar, categorizar, priorizar y resolver incidentes que afecten los servicios de TI. Impacta dado que no se puede demostrar una gestión controlada de interrupciones durante el desarrollo y operación del software.

- Otros como COBIT. Indican que los incidentes deben registrarse, clasificarse y priorizarse para garantizar una resolución oportuna y minimizar las interrupciones en el negocio. Impacta en la Entidad dado que la inexistencia del procedimiento impide demostrar control sobre interrupciones técnicas que afectan el desarrollo y continuidad del sistema.

**CRITERIO**:

- ITIL Versión 4. Práctica de Gestión de Incidentes.
- ISO/IEC 27001:2022. Controles A.8.29 – Pruebas de seguridad en el desarrollo y la aceptación, A.8.31 – Separación de los entornos de desarrollo, prueba y producción, A.5.24. Planificación y preparación de la gestión de incidentes de seguridad de la información.
- ISO/IEC 20000. Sistema de Gestión de Servicios de TI. Cláusula 8.2. Gestión de incidentes y solicitudes de servicio

- COBIT 2019. DSS02 – Gestionar solicitudes de servicio e incidentes.
- Ley 87 de 1993: Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado.
- Resolución 2023120002585 de 2023: "Por la cual se adoptaron y aprobaron el Marco Estratégico Institucional 2023 - 2026 "Super - Visión Efectiva", el Plan Estratégico Institucional 2023 -2026 y el Plan de Acción Anual Institucional 2023, de la Superintendencia de la Economía Solidaria".
- Plan Estratégico de Tecnologías de la Información – PETI.
- Circular Básica Contable y Financiera, incluyendo los anexos técnicos.

Igualmente, existen las directrices del Sistema de Control Interno, en donde define los principios de calidad de la información (exactitud, completitud, oportunidad) y de Responsabilidad del custodio del activo.

**CAUSAS**:

- Enfoque de incidentes solo en producción.
- Falta de alineación entre desarrollo, pruebas y producción.
- Ausencia de lineamientos institucionales de Gestión de Servicios de TI - ITSM para proyectos.
- Dependencia de prácticas informales o conocimiento tácito.

**CONSECUENCIAS O EFECTOS**:

- Pérdida de control y trazabilidad de los incidentes del proyecto durante todas sus fases.
- Despliegues a producción con defectos conocidos.
- Observaciones y hallazgos en auditorías de TI o control interno.
- Afectación a la continuidad del servicio y a la confianza institucional.

**RECOMENDACIONES DEL EQUIPO AUDITOR.**

- Definir e implementar un procedimiento formal de Gestión de Incidentes, aplicable a todas las fases del ciclo de vida del software.
- Establecer mecanismos de registro, clasificación, priorización y cierre de incidentes.
- Integrar el procedimiento con pruebas, despliegues y gestión de cambios.
- Mantener evidencias y métricas (tiempo de resolución, recurrencias, ANS, entre otros) para ejecutar la mejora continua.

**CONDICIÓN 2.**

**Hallazgo 4. No se identificó una segregación de usuarios, ni segregación de ambientes, ni un adecuado control de usuarios.**

Con el requerimiento con numeral 14 se solicitó el Reporte en excel de los usuarios y roles del software ADA con información de Usuario; Nombre completo; Dependencia; Fecha de creación; Fecha de desactivación; Roles y perfiles; Módulos a los que accede; Tipo de autenticación; (Incluir los usuarios administradores, técnicos, desarrolladores, etc.).

Dado que no se suministró información de fechas de creación o desactivación, o de sus tipos de autenticación. Se reiteró el requerimiento y se solicitó aclarar si los accesos a contienen restricciones o parámetros de creación o desactivación de usuarios y cómo se autentican los usuarios al ADA (por DA, propios en una BD con usuario/contraseña, u otros tipos diferentes de autenticación).

Al respecto el proceso indicó:

> *"El Sistema de Información Misional ADA cuenta con controles para la gestión de usuarios, incluyendo parámetros de creación, asignación de roles y desactivación, los cuales actualmente permiten: Registro de auditoría para usuarios creados en la versión actual del sistema, incluyendo: Fecha de creación, Usuario que realiza la asignación, Fecha y responsable de desactivación (cuando aplica).*
>
> *No obstante, es importante precisar que una parte de los usuarios proviene del sistema anterior (SICSES), el cual no contaba con mecanismos de auditoría completos, por lo que no se dispone de información histórica de nombres completos de los usuarios ni de la fecha de inactivación. En la matriz que se adjunta se tienen registros con campos en blanco, que indican que fueron creados durante el proceso de migración para que el usuario tuviera acceso al sistema ADA una vez se implementó oficialmente (1 de septiembre de 2025).*
>
> *En relación con el campo de dependencia, no se ha desarrollado el módulo de administración de usuarios internos de la Supersolidaria, por lo que no se cuenta con una discriminación de los usuarios por dependencia. Cabe resaltar que existen usuarios externos (entidades vigiladas) y usuarios exclusivos de la OAPS para la gestión y desarrollo del sistema.*
>
> *Para la autenticación de los usuarios, el sistema cuenta con un método de doble factor de autenticación mediante el envío de un PIN de cuatro dígitos al correo registrado, el cual debe ser ingresado por el usuario en el sistema. Adicionalmente, se debe completar una operación matemática tipo CAPTCHA. La validación y autenticación de los correos se cruza con la base de datos alojada en la OCI (Oracle Cloud Infrastructure)".*

Al validar la matriz de usuarios remitida, se identificaron las siguientes situaciones:

**Caso a. Matriz de usuarios, roles y permisos con debilidades de información.**

1. Presenta varios campos vacíos: nombre, codentidad, nit, nombre entidad, tipo entidad, o inconsistencias: con nombre de usuario: ”901-980-165-9”, “FONDO.FEGOSQGMAIL.COM”, “TEMPORAL”, etc.; con nombre: “a a”, “c a”, “AN Ce”, vacíos, etc.

2. Se compara con la hoja "Matriz de Usuarios del Sistema" y no hay similitud de los nombres de los perfiles o roles con los roles asociados en esta matriz. Hay 11 roles únicos en la matriz, pero 5 roles con definición.

| Categoría de Usuario | Rol o Perfil | Capacidades y Funciones Principales | Nivel de Permisos / Visualización |
|---|---|---|---|
| Externos (Entidades Vigiladas) | Administrador | •Gestiona todos los usuarios de su entidad (crear, editar, activar, eliminar).<br>• Visualiza el historial completo de accesos y cambios de los usuarios.<br>• Acceso total a todos los módulos asignados a la entidad. | • Edición: Puede consultar, registrar y modificar.<br>• Solo lectura: Únicamente consulta sin poder editar. |
| | Operador | • Accede y gestiona información en módulos operativos específicos (ej. F.O.R.C., Balance Social).<br>• No tiene permisos para administrar otros usuarios. | • Edición: Puede consultar, registrar y modificar.<br>• Solo lectura: Únicamente consulta sin poder editar. |
| OAPS (Oficina Asesora de Planeación) | Jefa de la OAPS | • Acceso directo a los tableros de control (dashboards).<br>• Revisión de métricas, reportes y estados de las entidades vigiladas. | Revisión y Consulta: Acceso de alto nivel orientado a la toma de decisiones en relación al reporte y cargue de información financiera de las entidades vigiladas. |
| | Gestores ADA / Líder de Desarrollo | • Realizan consultas globales sobre la información reportada de los módulos gestionados.<br>• Brindan soporte técnico/operativo a las entidades vigiladas.<br>• Gestionan y priorizan los desarrollos o requerimientos del sistema. | Gestión y Soporte:Permisos de consulta avanzada. |
| | Desarrollo (Equipo Técnico) | • Modo Consulta: Diagnóstico de errores reportados por soporte.<br>• Creación, prueba y despliegue de nuevas funcionalidades.<br>• Modificación de código fuente y validaciones del sistema.<br>• Revisión de logs o registros del sistema. | Acceso Técnico Total (Backend/Frontend):Permisos de escritura y ajuste en los desarrollos del Sistema ADA; de acuerdo al módulo asignado. |

*Ilustración 8. Matriz de Usuarios del Sistema*

| ROLES ASOCIADOS ÚNICOS |
|---|
| ADMIN |
| ADMIN ENTIDAD |
| BALANCE GENERAL |
| BALANCE SOCIAL CAC |
| BALANCE SOCIAL FONDO EMPLEADOS |
| DESARROLLO |
| ENTIDAD NUEVA |
| JEFE |
| OPERADOR DELEGATURA ASOCIATIVA |
| OPERADOR DELEGATURA FINANCIERA |
| OPERADOR FORD |

*Ilustración 9. Roles únicos de la matriz de usuarios.*

3. No son claros cuales son los alcances de los roles "ADMIN" y “ADMIN ENTIDAD”.

4. De 20 usuarios en la Supersolidaria, el 50% tienen usuarios administradores:

   - 5 tienen el usuario ADMIN (el 25%): Andrea Lamprea, Delio Fabian Barbosa, Juan López, Lydia Gómez, Osaris Lobo.
   - 5 tienen el usuario ADMIN ENTIDAD (el 25%).

Lo anterior implica que existen 10 usuarios administradores que implica un alto riesgo, desde el punto de vista de seguridad, control interno y gobernanza de TI,

dado que un administrador puede crear, modificar o eliminar otros usuarios, cambiar configuraciones del sistema, acceder o modificar información sensible, o ejecutar acciones sin controles adicionales, y cuando muchos usuarios tienen privilegios administrativos, el principio básico de control de accesos se debilita.

A mayor número de usuarios administradores: i) Mayor probabilidad de cambios no autorizados o accidentales, ii) Mayor posibilidad de eliminación o modificación indebida de información, iii) Mayor cantidad de cambios de configuración sin coordinación ni pruebas. Es decir, un error de un administrador puede afectar a todo el sistema, no solo a su usuario.

5. Existen usuarios que tienen los 2 roles como "Administrador" y "Operador" al mismo tiempo, sin embargo, en la descripción de este segundo rol especifica que "No tiene permisos para administrar otros usuarios":

   - Cesar Macías:
     - OPERADOR DELEGATURA FINANCIERA
     - ADMIN ENTIDAD, OPERADOR FORD
   - Juan López:
     - ADMIN
     - OPERADOR DELEGATURA ASOCIATIVA

6. Hay un usuario con rol de "Desarrollo" con nombre "SUPERINTENDENCIA ECONOMIA SOLIDARIA", el cual cuenta con permisos de:

   - Modo Consulta: Diagnóstico de errores reportados por soporte.
   - Creación, prueba y despliegue de nuevas funcionalidades.
   - Modificación de código fuente y validaciones del sistema.
   - Revisión de logs o registros del sistema
   - Acceso Técnico Total (Backend/Frontend): Permisos de escritura y ajuste en los desarrollos del Sistema ADA; de acuerdo con el módulo asignado.

   Que un usuario desarrollador tenga acceso directo a Producción es un riesgo alto, una debilidad grave de control y ampliamente reconocido en control interno, desarrollo de software y auditoría de TI, e implicaría:

   - Cambios no autorizados y errores directos en el sistema productivo.
   - Incumplimiento de la segregación de funciones (quien desarrolla no debe operar producción).
   - Caídas del servicio, pérdida o corrupción de datos.
   - Riesgo de fraude o manipulación de información sin detección inmediata.
   - Pérdida de trazabilidad y responsabilidad ante incidentes.
   - Hallazgos de auditoría y no conformidades con buenas prácticas.

7. Se identifican usuarios sin fechas de creación o fechas de desactivación. Este tema se desarrolla en el caso c.

8. Existen usuarios de la Supersolidaria en 2 Entidades o más diferentes a la propia:

i. El usuario "LHEREDIA@SUPERSOLIDARIA.GOV.CO" se encuentra en 2 Entidades diferentes:
   - "COOPERATIVA DE DISTRIBUIDORES DE GASEOSAS COLOMBIANAS" y
   - Entidad en Blanco,
   - con roles diferentes: En una como "OPERADOR DELEGATURA ASOCIATIVA", "OPERADOR FORD".

ii. El usuario "CMACIAS@SUPERSOLIDARIA.GOV.CO" se encuentra en 2 Entidades diferentes:
   - "FONDOS DE EMPLEADOS" y
   - Entidad en Blanco,
   - con roles en una como "OPERADOR DELEGATURA FINANCIERA" y en la otra entidad como "ADMIN ENTIDAD, OPERADOR FORD".

iii. El usuario "LOSORIO@SUPERSOLIDARIA.GOV.CO" se encuentra en 2 entidades:
   - "COOPERATIVA DE DISTRIBUIDORES DE GASEOSAS COLOMBIANAS" y
   - "COOPERATIVA MULTIACTIVA CORDOBA LTDA", con roles de "ADMIN ENTIDAD".

iv. Hay en total 147 usuarios con más de 1 Entidad; algunos con 44, 27, 15 y 12 Entidades.

**Caso b. Segregación de ambientes.**

Se solicitó al proceso "Con relación a Segregación de Ambientes (Desarrollo, pruebas, producción, otros), se solicita: i) Documentos, procedimientos, manuales o políticas donde se establezca la segregación de ambientes para los desarrollos de software. ii) Confirmar si para el desarrollo del software ADA se tiene segregación de ambientes", y para lo cual, el proceso respondió que:

> *"Para el desarrollo del Sistema de Información Misional ADA, se confirma que se cuenta con segregación de ambientes, conforme a lo establecido en el procedimiento GSTI-003, evidenciado en:*
> *· Ambiente de pruebas, destinado a la validación funcional y técnica de los desarrollos.*
> *· Ambiente de producción, donde opera el sistema en uso por los usuarios finales.*
> *Como Evidencia se anexa procedimiento GSTI-003: Gestión de aplicaciones, en el capítulo de generalidades de este procedimiento, se indica que: Se debe generar un esquema de pruebas para el desarrollo inicial, previo al paso del sistema al ambiente de producción",*

sin embargo, no se aportaron evidencias y soportes sobre la segregación de los ambientes indicados. Adicionalmente, no se indicó sobre el ambiente de desarrollo, toda vez que se identificó el usuario desarrollador en el ambiente productivo. En el procedimiento no se precisa sobre el ambiente de desarrollo.

No tener ambientes segregados de Desarrollo, Pruebas y Producción expone el software

y a la Entidad a los siguientes riesgos principales:

- Errores directos en producción: cambios o pruebas pueden afectar al sistema productivo.
- Caídas del servicio y pérdida de información por pruebas o desarrollos no controlados.
- Incumplimiento de segregación de funciones, debilitando el control interno.
- Dificultad para detectar fallas antes de llegar a los usuarios finales.
- Pérdida de trazabilidad sobre qué cambios fueron probados y aprobados.
- Hallazgos de auditoría y no conformidades con buenas prácticas de TI.

**Caso c. Usuarios sin fechas de creación o desactivación.**

De acuerdo con el listado de usuarios remitido, se identificaron 26 usuarios sin fechas de creación y todos los 5764 usuarios del listado sin fecha de desactivación.

Al respecto el proceso indicó que *"(...) es importante precisar que una parte de los usuarios proviene del sistema anterior (SICSES), el cual no contaba con mecanismos de auditoría completos, por lo que no se dispone de información histórica de nombres completos de los usuarios ni de la fecha de inactivación. En la matriz que se adjunta se tienen registros con campos en blanco, que indican que fueron creados durante el proceso de migración para que el usuario tuviera acceso al sistema ADA una vez se implementó oficialmente (1 de septiembre de 2025)*", sin embargo, el registrar las fechas de creación y desactivación de usuarios no es un requisito administrativo menor, sino un control clave y fundamental de seguridad de la información. Su ausencia le impacta a la Entidad en 3 aspectos:

i. Incumplimiento de estándares internacionales.
ii. Debilitamiento del control de accesos.
iii. Incremento significativo del riesgo operativo, legal y reputacional.

i). Las fechas de creación y desactivación permiten controlar el ciclo de vida de las cuentas/usuarios, asegurando que los accesos estén alineados con una necesidad real, siendo importante para:

- Trazabilidad y auditoría: evidenciar quién tuvo qué acceso y en qué periodo ante auditorías o incidentes o eventos de seguridad de la información.
- Control de accesos: evitar cuentas activas innecesarias o "huérfanas", sobre todo de eventos de migración como los sucedidos.
- Reducción de riesgos de seguridad: minimizar accesos no autorizados y abuso de privilegios.

ii). No mantener estas fechas implica incumplimientos en marcos de control y buenas prácticas ampliamente adoptados:

- ISO/IEC 27001: Exige un proceso formal y auditable de alta y baja de usuarios, y su trazabilidad y log.
- COBIT 2019 – DSS05.04: Requiere evidencia del manejo oportuno y autorizado de identidades.
- NIST SP 800-53: Demanda controlar y revisar el ciclo de vida completo de las cuentas.

iii). La falta de este registro incrementa riesgos importantes que deben ser tratados con prioridad:

- Accesos no autorizados por cuentas de usuarios que ya no deberían estar activas.
- Falta de trazabilidad, dificultando la investigación de incidentes.
- Hallazgos de auditoría y no conformidades con impacto reputacional y legal.

Es requerido implementar y mantener estos registros los cuales permiten demostrar control, reducir riesgos y fortalecer la postura de la gobernanza de la seguridad en la Entidad, de forma tangible y auditable.

**CRITERIO**:

- Ley 87 de 1993: Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado.
- Resolución 2023120002585 de 2023: "Por la cual se adoptaron y aprobaron el Marco Estratégico Institucional 2023 - 2026 "Super - Visión Efectiva", el Plan Estratégico Institucional 2023 -2026 y el Plan de Acción Anual Institucional 2023, de la Superintendencia de la Economía Solidaria".
- Plan Estratégico de Tecnologías de la Información – PETI.
- Circular Básica Contable y Financiera, incluyendo los anexos técnicos.
- ISO/IEC 27001:2022. Controles A.8.31 – Separación de los entornos de desarrollo, prueba y producción, A.5.3 – Segregación de funciones, A.5.18 - Derechos de acceso
- COBIT 2019. Segregación de ambientes. BAI03 – Gestionar la identificación y el desarrollo de soluciones. DSS01 – Gestionar operaciones. APO01 - Segregación de usuarios / roles.
- NIST SP 800 (principalmente SP 800-53 Rev. 5)

Igualmente, existen las directrices del Sistema de Control Interno, en donde define los principios de calidad de la información (exactitud, completitud, oportunidad) y de Responsabilidad del custodio del activo.

**CAUSAS**:

- Falta de definición formal de roles, perfiles y responsabilidades en el sistema ADA.
- Ausencia de un modelo de control de accesos basado en el principio de mínimo privilegio.
- Debilidades en la gestión del ciclo de vida de usuarios, acentuadas por el proceso de migración desde SICSES sin controles compensatorios.
- Inexistencia o insuficiencia de procedimientos documentados y evidencias sobre

segregación de ambientes.
- Uso de prácticas operativas informales para resolver necesidades técnicas, como asignar roles administrativos o accesos a producción por conveniencia.

**CONSECUENCIAS O EFECTOS**:

- Alto riesgo de accesos no autorizados, cambios accidentales o indebidos y uso inapropiado de privilegios.
- Debilitamiento del control interno y de la gobernanza de TI, por incumplimiento de segregación de funciones y de mínimo privilegio.
- Mayor probabilidad de caídas del servicio, pérdida o alteración de información y afectación a la continuidad operativa.
- Pérdida de trazabilidad y responsabilidad sobre acciones realizadas en el sistema.
- Hallazgos y no conformidades frente a auditorías internas, externas y marcos de buenas prácticas.
- Incremento del riesgo operativo, legal y reputacional para la Entidad.

**RECOMENDACIONES DEL EQUIPO AUDITOR.**

- Definir, documentar y aprobar un modelo formal de roles y perfiles, alineado con funciones reales y principio de mínimo privilegio.
- Reducir y controlar estrictamente los usuarios con privilegios administrativos, asegurando su justificación, aprobación y monitoreo.
- Implementar y evidenciar la segregación efectiva de ambientes (Desarrollo, Pruebas y Producción), restringiendo accesos a producción.
- Retirar accesos de desarrolladores al ambiente productivo, aplicando gestión formal de cambios y accesos excepcionales.
- Completar y mantener actualizada la información de usuarios, incluyendo fechas de creación, desactivación, roles, autenticación y dependencia.
- Realizar revisiones periódicas de usuarios y accesos, especialmente posteriores a migraciones o cambios relevantes.
- Fortalecer los procedimientos de gestión de usuarios y de aplicaciones, asegurando su aplicación y evidencia.
- Restringir el ambiente de producción a roles exclusivamente operativos, aplicar segregación de funciones y realizar una gestión formal de cambios y accesos excepcionales solo con aprobación y registro.

## 4.3. Alcance 3. Verificar el cumplimiento de los controles de los riesgos identificados y valorados del proceso a evaluar; así mismo, proponer identificación de riesgos y controles respectivos

**CONDICIÓN.**

**Hallazgo 5. El software ADA no contó con una matriz de riesgos y controles para su desarrollo.**

Con el requerimiento del numeral 17 se solicitaron los Riesgos y controles asociados al desarrollo de software, sin embargo, se remitió un solo riesgo proyectado en una matriz del mapa de riesgos. La OCI reiteró este requerimiento solicitando todas las versiones de las matrices y la evidencia de ejecución de los controles durante enero 2025 hasta febrero de 2026, y para lo cual el proceso respondió que:

> *"Durante las vigencias 2024 y 2025 (...) no se contaba con una matriz de riesgos formalmente aprobada. En este sentido, el primer mapa de riesgos de seguridad y privacidad de la información fue aprobado el 28 de enero de 2026; (...) se precisa que no se cuenta con registros asociados a vigencias anteriores, en razón a que la matriz de riesgos y sus respectivos controles no se encontraban definidos ni en operación antes de su aprobación en el año 2026; (...) no aplicaban matrices de riesgos ni controles asociados en el marco solicitado.".*

Pese a lo anterior, un desarrollo de un sistema de información o software interno en una Entidad sí requiere definir una matriz de riesgos, tanto desde la perspectiva de seguridad de la información como de gobernanza y control de TI, dado que:

i. Todo desarrollo de software interno introduce nuevos activos de información, procesos y expone nuevos riesgos, por lo que debe realizarse una identificación, análisis y tratamiento de riesgos (activos, amenazas, vulnerabilidades, impacto y tratamiento). Este requisito está explícito en los principales marcos normativos y de buenas prácticas:

   a. ISO/IEC 27001 - Gestión de riesgos de seguridad de la información (Cláusula 6.1.2, Cláusula 8.2, Controles A.8.25 y A.8.26). Estos lineamientos de esta norma requieren que los riesgos de seguridad sean considerados durante todo el ciclo de vida del desarrollo, desde el diseño, desarrollo, pruebas, hasta la puesta en producción.
   b. COBIT - Gestión del riesgo y desarrollo de soluciones. Exige identificar, analizar y responder a los riesgos relacionados con soluciones tecnológicas, incluyendo desarrollos internos, como parte del gobierno TI.
   c. NIST SP 800 - Ciclo de vida del sistema. En Algunos de sus controles explica que todo sistema desarrollado debe contar con una evaluación formal de riesgos, especialmente antes de entrar en operación.

ii. El impacto en la Entidad de no haber definido una matriz de riesgos y controles desde el diseño y desarrollo del software ADA son:

   a. Riesgos de seguridad no identificados, como vulnerabilidades en el diseño, autenticación o manejo de información.
   b. Incumplimiento normativo, generando hallazgos o no conformidades frente a estándares como ISO 27001, COBIT o NIST.
   c. Pérdida de trazabilidad, dificultando la investigación de incidentes y la justificación de decisiones técnicas.
   d. Impactos legales y reputacionales, derivados de fallas en la

confidencialidad, integridad o disponibilidad de la información.

**CRITERIO**:

- ISO/IEC 27001:2022. Cláusula 6.1.2 – Evaluación de riesgos de seguridad de la información. A.5.4 – Responsabilidades de gestión de riesgos. A.8.25 – Ciclo de vida de desarrollo seguro.
- COBIT 2019. APO12 – Manage Risk. BAI03 – Gestionar la identificación y el desarrollo de soluciones.
- NIST SP 800. (Principalmente NIST SP 800 53 Rev. 5). RA 3 – Evaluación de riesgos. RA 5 – Monitoreo y escaneo de vulnerabilidades. SA 3 – Ciclo de vida del desarrollo del sistema.
- Ley 87 de 1993: Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado.
- Resolución 2023120002585 de 2023: "Por la cual se adoptaron y aprobaron el Marco Estratégico Institucional 2023 - 2026 "Super - Visión Efectiva", el Plan Estratégico Institucional 2023 -2026 y el Plan de Acción Anual Institucional 2023, de la Superintendencia de la Economía Solidaria".
- Plan Estratégico de Tecnologías de la Información – PETI.
- Circular Básica Contable y Financiera, incluyendo los anexos técnicos.

Igualmente, existen las directrices del Sistema de Control Interno, en donde define los principios de calidad de la información (exactitud, completitud, oportunidad) y de Responsabilidad del custodio del activo.

**CAUSAS**:

- Ausencia de un enfoque preventivo de gestión de riesgos durante el diseño y desarrollo del software ADA.
- Falta de lineamientos institucionales aplicados que exigieran la elaboración y aprobación de una matriz de riesgos desde el inicio del proyecto.
- Priorización del desarrollo técnico sin integrar controles de gobernanza, riesgo y cumplimiento.
- Definición tardía de la matriz de riesgos (a partir de enero de 2026), cuando el software ya se encontraba desarrollado y en operación.

**CONSECUENCIAS O EFECTOS**:

- Riesgos de seguridad, operativos y tecnológicos no identificados ni tratados oportunamente durante el ciclo de vida del software.
- Debilitamiento del control interno y de la gobernanza de TI, al no contar con controles definidos y ejecutados durante el desarrollo.
- Incumplimiento de buenas prácticas y estándares internacionales, generando potenciales hallazgos y no conformidades.
- Dificultades para justificar decisiones técnicas y para analizar incidentes o fallas ocurridas con anterioridad.

- Incremento del riesgo operativo, legal y reputacional para la Entidad.

**RECOMENDACIONES DEL EQUIPO AUDITOR.**

- Definir, documentar y aprobar una matriz de riesgos y controles específica para el desarrollo de software, aplicable desde la etapa de diseño.
- Integrar la gestión de riesgos como actividad obligatoria en el ciclo de vida de los proyectos tecnológicos.
- Fortalecer el riesgo actualmente definido, asegurando la ejecución efectiva y documentada de los controles.
- Extender la gestión de riesgos y controles no solo al desarrollo, sino también a los ambientes de pruebas y producción.
- Establecer mecanismos de seguimiento periódico y actualización de la matriz de riesgos durante la vida útil del software.
- Fortalecer el riesgo actual y mejorar la ejecución del control asociado, no solo al desarrollo del software, sino en los ambientes de pruebas y producción.

**CONCLUSIONES**

1. Se verificó la funcionalidad del software ADA de acuerdo con el desarrollo de software y los cronogramas definidos, sin embargo, se identificaron deficiencias y debilidades en cuanto a la planeación, aprobación y seguimiento del cronograma, en la información propia de sus actividades, y en los soportes de ejecución de las actividades de este. Adicionalmente, el procedimiento y los formatos establecidos para llevar a cabo el desarrollo de sus funcionalidades presentan aspectos a mejorar, dado que el procedimiento no cuenta con la definición de todos los formatos que se utilizan y los formatos incurren en el no diligenciamiento completa de la información o contienen información incoherente.

2. Con la información y evidencias suministradas no fue posible validar la satisfacción en el uso del software ADA dado que la Entidad no ha realizado encuestas, y que la gran mayoría de usuarios son externos. Asimismo, dado el reducido porcentaje de usuarios de la Entidad con roles exclusivos de administración, jefe, desarrollador, realizar esta encuesta interna por parte de la OCI tendrían un conflicto de intereses, dado que son gestores que promueven el software. Por otra parte, el proceso indicó que, aunque el único canal para recibir incidentes de funcionamiento son las PQRSD, desde enero 2025 a febrero 2026 no se ha recibido ninguna por parte de los 5900 usuarios aproximadamente. A este aspecto, por temas de tiempos de auditoría, no se realizará esta comprobación de esta información.

3. En la validación realizada no se encuentra definido en la Entidad un procedimiento para gestión de incidentes de los sistemas de información. De la misma manera, no se identificó una segregación de usuarios, segregación de ambientes para el desarrollo de software y existen debilidades en cuanto al control y administración de usuarios del software ADA.

4. El desarrollo del software ADA no contó con una matriz de riesgos y controles para su desarrollo implicando posibles riesgos e impactos en la Entidad.

## 5. PLAN DE MEJORAMIENTO

Se requiere la definición y suscripción del respectivo plan de mejoramiento. La etapa inicial de FORMULACIÓN ha sido diligencia por la oficina de control interno, quien, como valor agregado, ha incluido recomendaciones para cada hallazgo, sin embargo, las propias que proponga el auditado junto con las acá recomendadas, deben ser consensuadas, hasta su respectiva definición.

Por lo anterior, se remitirá dentro de los 5 días siguientes, desde la OCI, el formato FT-COIN-008, con la formulación del plan de mejoramiento, para lo pertinente, otorgándose el termino de hasta 5 días hábiles para su trámite.

Atentamente,

**JORGE HERNANDO PEDRAZA VARGAS**
Jefe Oficina de Control Interno

Elaboró: Rafael Hernando Calle Cabezas - Contratista, Líder de la Auditoría.

### HISTORIAL DE CAMBIOS

| VERSIÓN | FECHA | RAZÓN DE LA ACTUALIZACIÓN |
|---|---|---|
| 0 | Noviembre 2020 | Primera versión del documento. |
| 1 | Octubre 2023 | Actualización Logos institucionales. |
| 2 | Marzo 2025 | Actualización del procedimiento de acuerdo a la actualización de la Guía de Auditoría Basada en Riesgos SES. |