Auditoría a Sistemas de Información y Módulos del SEA

Informe final de auditoría interna: **INF-AI-33-2026**

Fecha de emisión: 15/10/2026

Índice general

1. Introducción..... 2
2. Metodología. 3
3. Seguimiento a Plan de mejoramiento anterior..... 7
4. Antecedentes y contextualización Proyecto..... 8
5. Resultados de auditoría 11
6. Conclusiones..... 22

1. Introducción

Los Sistemas de Información de la Unidad de Planificación Rural Agropecuaria – UPRA constituyen un componente fundamental para el desarrollo de los procesos institucionales, al soportar la gestión, procesamiento, almacenamiento y disponibilidad de la información requerida para la prestación de servicios, la generación de productos institucionales y la toma de decisiones. Su adecuada gestión requiere la aplicación de prácticas que aseguren la calidad, confiabilidad, disponibilidad, integridad, seguridad y mantenibilidad de las soluciones tecnológicas durante las diferentes etapas de su ciclo de vida.

En este contexto, la gestión del ciclo de vida de los Sistemas de Información comprende actividades relacionadas con la identificación y entendimiento de requerimientos, análisis y diseño, desarrollo y mantenimiento, control de versiones, ejecución de pruebas, gestión de cambios, implementación en producción, documentación técnica y funcional, seguridad de las aplicaciones y seguimiento posterior a su puesta en operación. Estas actividades se articulan con los procedimientos y lineamientos institucionales definidos por la UPRA para la gestión de Sistemas de Información y Servicios Tecnológicos.

La presente auditoría tiene como propósito evaluar la aplicación de buenas prácticas durante el ciclo de vida de los Sistemas de Información institucionales, verificando el cumplimiento de los lineamientos técnicos y normativos aplicables, con el fin de contribuir a su calidad, confiabilidad, disponibilidad y mantenibilidad. La evaluación comprende las actividades ejecutadas durante el segundo semestre de 2025 y el primer semestre de 2026 y contempla, entre otros aspectos, la gestión de requerimientos, desarrollo, pruebas, administración de versiones, implementación, mantenimiento, documentación técnica, seguridad y trazabilidad de los cambios.

La auditoría constituye un instrumento para el fortalecimiento del control y el mejoramiento continuo de la gestión tecnológica institucional. En este sentido, los resultados obtenidos buscan proporcionar información objetiva sobre la aplicación de los controles y prácticas establecidas, así como identificar situaciones observadas, limitaciones y oportunidades de mejora que contribuyan a fortalecer la trazabilidad, seguridad, estandarización y gestión integral del ciclo de vida de los Sistemas de Información de la UPRA.

2. Metodología

2.1. Identificación

Aspecto evaluable (unidad auditable)	Sistemas de Información y Módulos SEA
Líder de proceso / jefe(s) de dependencia(s)	PAOLA ANDREA ZAMBRANO Jefe Oficina TIC JULIA EDITH ESPINDOLA GARCÍA Jefe Encargada Oficina TIC
Objetivo de la auditoría	Evaluar la aplicación de buenas prácticas durante el ciclo de vida de los Sistemas de Información institucionales, verificando el cumplimiento de los lineamientos técnicos y normativos aplicables, con el fin de contribuir a la calidad, confiabilidad, disponibilidad y mantenibilidad de los sistemas de información de la Unidad de Planificación Rural Agropecuaria (UPRA).
Alcance de la auditoría	La auditoría comprenderá la evaluación técnica del ciclo de vida de los Sistemas de Información institucionales, verificando la aplicación de buenas prácticas relacionadas con la gestión de requerimientos, diseño, desarrollo, pruebas, administración de versiones, implementación, mantenimiento, documentación técnica, seguridad de las aplicaciones y trazabilidad de los cambios, conforme a los lineamientos técnicos y normativos aplicables. La auditoría comprenderá las actividades ejecutadas entre el segundo semestre de 2025 y el primer semestre de 2026. Cuando sea necesario para establecer la trazabilidad de los desarrollos o validar la efectividad de los controles evaluados, podrán revisarse soportes y registros correspondientes a vigencias anteriores.
Reunión de apertura	Acta de Reunión de Apertura (Radicado # 2026-3-010391)
Ejecución de auditoría	Desde: julio 17 de 2026 Hasta: octubre 15 de 2026 Memorando de presentación de Auditoría (Rad # 2026-3-010132)
Reunión de cierre	octubre 15 de 2026
Líder de auditoría	Sandra Milena Ruano Reyes Asesora de Control Interno
Auditor	Paola Tatiana Mesa Dávila Contratista Control Interno

2.2. Criterios de Auditoría

- Guía para la Gestión Integral del Riesgo en Entidades Públicas, versión 7 – 2025.
- Guía para la Administración del Riesgo y el diseño de controles en entidades públicas, versión 6. noviembre de 2022.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas – Riesgos de Gestión, Corrupción y Seguridad Digital, versión 4. octubre de 2018.
- Política de Gobierno Digital – MinTIC.
- Modelo de Referencia de Arquitectura Empresarial – MRAE del Estado Colombiano – MinTIC.
- Modelo Integrado de Planeación y Gestión – MIPG
- Norma ISO/IEC 27001:2022.
- GIA-PR-001 Proceso Gestión de la Información Agropecuaria, versión 2 (2021-11-22).
- Anexo 10. Plan Estratégico de Tecnologías de la Información PETI 2026.pdf
- Procedimientos:
    - GIA-PD-004 – Procedimiento Ingeniería de Software, versión 4 del 26/11/2025.
    - GIA-GU-001 – Guía Metodológica de Referencia de Sistemas de Información, versión 2 del 17/12/2020.
    - GIA-PD-012 – Procedimiento de Arquitectura Empresarial, versión vigente.
    - GST-PD-007 – Procedimiento Gestión de Cambios de TI, versión 1 del 27/12/2023.
    - GST-IN-006 – Instructivo para la Ejecución de Pruebas en el Desarrollo Seguro de Software, versión 2 del 09/04/2026.
    - GST-MA-002 – Manual de Política de Seguridad de la Información, versión vigente durante el período auditado.
- Mapas de Riesgos:
    - GIA-RI-001 Mapa de Riesgos Proceso Gestión de la Información Agropecuaria, versión 6 (2025-07-28).
    - GST-RI-001 Mapa de Riesgos Proceso Gestión de Servicios Tecnológicos, versión 6 (2025-07-28).
- Formatos asociados e Indicadores del proceso
- Normatividad vigente aplicable a la entidad.

2.3. Muestreo y herramientas

Para la definición de la muestra se solicitó a la Oficina TIC la relación consolidada de los desarrollos, mantenimientos, mejoras, integraciones y migraciones realizados sobre los Sistemas de Información institucionales durante el segundo semestre de 2025 y el primer semestre de 2026, mediante la Solicitud N.° 1 de información, radicado SEA N.° 2026-3-010489, proceso 205465. La respuesta fue remitida por la Oficina TIC el 20 de agosto de 2026, mediante Memorando N.° 2026-3-011744, adjuntando el archivo denominado *"Muestra Solicitud de Información N.° 1 para la Auditoría a Sistemas de Información (2).xlsx"*.

Una vez revisada la información suministrada, se evidenció que esta correspondía principalmente a una relación general de Sistemas de Información y no permitía individualizar suficientemente las intervenciones ejecutadas durante el período auditado. De los nueve (9) registros reportados, en ocho (8) la fecha de inicio figuraba como "NA"; adicionalmente, no se encontraba diligenciada de manera suficiente la fecha de implementación o puesta en producción, salvo para el caso de SEA, ni se contaba con un alcance específico o descripción individualizada de cada desarrollo, mejora, mantenimiento, integración o migración. Estas limitaciones impidieron determinar con precisión variables necesarias para la selección de la muestra, tales como tipo de intervención, criticidad, complejidad, impacto, nivel de cambio y oportunidad de implementación. El memorando de respuesta señala que se remitió el Excel como relación consolidada de los desarrollos del período auditado.

En consecuencia, no fue posible conformar de manera completa y confiable el universo de intervenciones ni aplicar el instrumento institucional de cálculo de muestra EVI-FT-009, dado que su utilización requiere un universo previamente identificado y suficientemente caracterizado. Por esta razón, no se efectuó una selección estadística de muestra y se optó por realizar una prueba de recorrido dirigida sobre el proyecto "Actualización tecnológica y salida a producción de la nueva plataforma SEA / SEA.doc", teniendo en cuenta su ejecución dentro del período auditado, la disponibilidad de información, su relevancia técnica y la posibilidad de verificar de manera integrada las principales etapas del ciclo de vida del software.

La prueba de recorrido permitió evaluar, para el caso seleccionado, aspectos relacionados con requerimientos, desarrollo, control de versiones, pruebas, gestión de cambios, implementación, seguridad, documentación y estabilización. No obstante, debido a la limitación presentada en la conformación del universo, los resultados obtenidos corresponden exclusivamente al caso

SEA/SEA.doc y no pueden generalizarse al total de los Sistemas de Información institucionales.

- Herramientas utilizadas durante la auditoría:
  - Sistema de Eficiencia Administrativa – SEA.
  - Azure DevOps.
  - SharePoint institucional.
  - Repositorios de código fuente y documentación técnica.
  - RFC y actas del Comité de Cambios.
  - Repositorio documental institucional.
  - Prueba de recorrido aplicada a SEA/SEA.doc.
  -

- Relación de planillas de trabajo utilizadas:
  - 05_Plani1Riesgos_20260609
  - 06_Plani2SIModulosSEA_20260609
  - 07_Plani3PruebaRecorrido_20260609

3. Seguimiento al plan de mejoramiento derivado de auditoría interna anterior

De acuerdo con el Plan Anual de Auditorias 2026, la auditoria a Sistemas de Información y Módulos SEA, no tiene un plan de mejoramiento anterior asociado al mismo objetivo para realizar seguimiento.

4. Antecedentes y Contextualización de los Sistemas de Información y Módulos SEA

La Unidad de Planificación Rural Agropecuaria – UPRA, en desarrollo de sus funciones institucionales, requiere del uso permanente de tecnologías de la información para soportar la gestión, procesamiento, análisis, almacenamiento, intercambio y disponibilidad de información asociada a sus procesos misionales, estratégicos y de apoyo. En este contexto, los Sistemas de Información constituyen un componente fundamental para la operación institucional, la generación de productos y servicios y la toma de decisiones basada en información.

La evolución tecnológica de la entidad ha implicado el desarrollo, mantenimiento y actualización progresiva de diferentes soluciones informáticas, así como la incorporación de herramientas para la gestión de requerimientos, control de versiones, pruebas, cambios e implementación en ambientes productivos. Estas actividades requieren la aplicación de prácticas que permitan asegurar la funcionalidad, disponibilidad, integridad, confidencialidad y mantenibilidad de los Sistemas de Información durante las diferentes etapas de su ciclo de vida.

Para orientar esta gestión, la UPRA cuenta con procedimientos y lineamientos institucionales asociados a ingeniería de software, arquitectura empresarial, gestión de cambios de TI, desarrollo seguro, documentación técnica y administración de los Sistemas de Información. De igual forma, utiliza herramientas como Azure DevOps, el Sistema de Eficiencia Administrativa – SEA, repositorios de código y espacios institucionales de almacenamiento y gestión documental, que soportan la planificación, ejecución y trazabilidad de las actividades de desarrollo y mantenimiento.

Dentro de este ecosistema tecnológico, el Sistema para la Eficiencia Administrativa – SEA constituye una de las soluciones institucionales utilizadas para soportar diferentes procesos administrativos y de gestión. Durante el período evaluado se adelantaron actividades relacionadas con su actualización tecnológica, mantenimiento, incorporación de funcionalidades, gestión de requerimientos y ajustes de seguridad, incluyendo la actualización y salida a producción de la plataforma SEA/SEA.doc, intervención seleccionada durante la auditoría para la ejecución de la prueba de recorrido.

En este contexto, la auditoría se orientó a evaluar la aplicación de buenas prácticas durante el ciclo de vida de los Sistemas de Información institucionales, considerando aspectos relacionados con la gestión de requerimientos, análisis y diseño, desarrollo, pruebas, control de versiones, gestión de cambios, implementación, mantenimiento, documentación y seguridad. La evaluación buscó determinar el nivel de aplicación de los lineamientos institucionales y la trazabilidad de los controles definidos para gestionar las intervenciones realizadas durante el segundo semestre de 2025 y el primer semestre de 2026.

No obstante, las limitaciones presentadas en la información suministrada para conformar de manera completa el universo de desarrollos e intervenciones impidieron extender la evaluación técnica al conjunto de los Sistemas de Información institucionales. En consecuencia, la prueba de recorrido se concentró en SEA/SEA.doc, cuyos resultados constituyen evidencia específica del caso evaluado y no pueden generalizarse al total de los Sistemas de Información de la UPRA.

Alineación Estratégica de Sistemas de Información



Nota: La información presentada fue tomada del documento "Anexo 10 – Plan Estratégico de Tecnologías de la Información – PETI 2023–2026", específicamente del numeral 1.1. Objetivo General del PETI, página 9; numeral 7.1.2. Modelo de Motivación Institucional y Tabla 5. Despliegue Estratégico de la UPRA, páginas 17 y 18; y numeral 7.3. Dominio de Sistemas de Información, página 34. Fuente: elaboración propia de la entidad.

5. Resultados de Auditoría 2026

5.1. Análisis de riesgos y controles

En el marco de la presente auditoría se realizó el análisis de los riesgos y controles asociados a los procesos de Gestión de la Información Agropecuaria (GIA) y Gestión de Servicios Tecnológicos (GST), relacionados con la gestión del ciclo de vida de los Sistemas de Información, particularmente frente a la gestión de requerimientos, capacidad y funcionalidad tecnológica, integridad de los sistemas, actualizaciones de seguridad y desarrollo seguro. Para el inicio del ejercicio auditor se tomaron como referencia los Mapas Institucionales de Riesgos de Gestión GIA-RI-001 y GST-RI-001, versión 6 del 28 de julio de 2025, vigentes para el período objeto de evaluación.

Durante la ejecución de la auditoría se evidenció que dichos mapas fueron posteriormente actualizados y formalizados en el SEA, el 20 de agosto de 2026 para GST-RI-001 y el 25 de agosto de 2026 para GIA-RI-001, fechas posteriores al inicio de la auditoría el 17 de julio de 2026.

Así mismo se evidenció que la Oficina TIC cuenta con planes de mejoramiento vigentes relacionados con la gestión de riesgos, en los cuales ya se encuentran contempladas acciones orientadas al tratamiento de situaciones previamente identificadas. Por esta razón, y con el fin de evitar la duplicidad de observaciones y acciones de mejora, no se consideró pertinente reiterar en la presente auditoría situaciones que ya se encuentran incorporadas y en seguimiento mediante los respectivos planes de mejoramiento. En particular, el estado de los riesgos relacionados con el alcance de la presente auditoría se encuentra gestionado de la siguiente manera:

- Los riesgos R1 y R6 del proceso Gestión de la Información Agropecuaria – GIA se encuentran incluidos en el Plan de Mejoramiento derivado de la auditoría al proceso GIA, radicado N.° 2026-3-013347 del 23 de septiembre de 2026.

- El riesgo R9 del proceso Gestión de Servicios Tecnológicos – GST se encuentra incluido en el Plan de Mejoramiento derivado de la auditoría al proceso GST, radicado N.° 2026-3-012378 del 1 de septiembre de 2026.

En consecuencia, el análisis efectuado permitió establecer que los riesgos identificados fueron actualizados. No obstante, debido al corto período

transcurrido desde la actualización de los mapas de riesgos y la implementación de los controles modificados, no fue posible evaluar durante el presente ejercicio su efectividad sostenida. Por tanto, la valoración de dicha efectividad deberá efectuarse en seguimientos posteriores, una vez exista un período suficiente de operación y evidencia que permita verificar la adecuada implementación y funcionamiento de los controles.

5.2 Metodología y lineamientos para el desarrollo y mantenimiento de Sistemas de Información.

Se verificó que la UPRA dispone de un marco metodológico para la gestión del ciclo de vida de los Sistemas de Información, soportado principalmente en el GIA-PD-004 – Procedimiento de Ingeniería de Software, versión 4 del 26 de noviembre de 2025, la GIA-GU-001 – Guía Metodológica de Referencia de Sistemas de Información, versión 2, y el GST-IN-006 – Instructivo para la Ejecución de Pruebas en el Desarrollo Seguro de Software, versión 2 del 9 de abril de 2026. Estos documentos establecen lineamientos relacionados con la planeación, gestión de requerimientos, análisis y diseño, desarrollo, pruebas, despliegue, mantenimiento y seguridad durante el ciclo de vida del software.

Mediante la prueba de recorrido aplicada al proyecto "Actualización tecnológica y salida a producción de la nueva plataforma SEA / SEA.doc", se evidenció la aplicación práctica del procedimiento de Ingeniería de Software y el uso de la metodología ágil Scrum, apoyada en Azure DevOps para la estructuración de épicas, features, historias de usuario, criterios de aceptación, tareas y sprints. Asimismo, se verificó el uso de repositorios, ramas y commits para el control de versiones, así como la ejecución progresiva de pruebas antes de la presentación de los desarrollos al usuario.

No obstante, se identificó que el GIA-PD-004 referencia un Instructivo DevOps y un Instructivo de versionamiento de código que no se encuentran formalmente institucionalizados, generando una brecha entre la documentación formal y las prácticas operativas implementadas. Si bien en el caso evaluado no se evidenció ausencia de metodología ni aplicación discrecional de estas prácticas, su falta de formalización limita la estandarización, continuidad y trazabilidad institucional.

5.3 Gestión y trazabilidad de requerimientos y cambios.

Se verificó que la UPRA cuenta con lineamientos formalmente establecidos para la gestión de requerimientos y cambios, principalmente a través del GIA-PD-004 – Procedimiento de Ingeniería de Software y del GST-PD-007 – Procedimiento Gestión de Cambios de TI. Para el caso evaluado, se evidenció que las necesidades de desarrollo son registradas inicialmente en SEA y sometidas a análisis de viabilidad, considerando aspectos como recursos, perfiles requeridos, tiempos estimados y riesgos asociados.

Durante la prueba de recorrido de SEA/SEA.doc se observó que los requerimientos son estructurados en Azure DevOps mediante épicas, features e historias de usuario con criterios de aceptación, y son revisados con los usuarios antes de su aprobación y paso a desarrollo. Asimismo, fue posible establecer trazabilidad entre la solicitud inicial, las historias de usuario, las tareas de análisis y desarrollo, las actividades de prueba y la posterior gestión del cambio.

Respecto de la salida a producción, se verificó la utilización de un RFC registrado en SEA, con identificación de la infraestructura involucrada, actividades previstas, plan de pruebas, tiempos y responsables. El cambio fue presentado y aprobado por el Comité de Cambios, ejecutado dentro de una ventana de mantenimiento y posteriormente presentado para formalizar su cierre.

5.4 Desarrollo, control de versiones, pruebas e implementación en producción.

Se verificó que la UPRA cuenta con lineamientos para el desarrollo, control de versiones, pruebas e implementación de software, principalmente mediante el GIA-PD-004 – Procedimiento de Ingeniería de Software, la GIA-GU-001 – Guía Metodológica de Referencia de Sistemas de Información, el GST-PD-007 – Procedimiento Gestión de Cambios de TI y el GST-IN-006 – Instructivo para la Ejecución de Pruebas en el Desarrollo Seguro de Software. La GIA-GU-001 establece, entre otros aspectos, el uso de repositorios Git, líneas base, ramas para ambientes de prueba, control de versiones de artefactos desplegados y ejecución de pruebas antes del paso a las etapas posteriores.

En la prueba de recorrido aplicada a SEA/SEA.doc se evidenció que las historias de usuario se desagregan en actividades técnicas asignadas a los responsables, que el código fuente se administra mediante repositorios, ramas y commits y

que existe versionamiento para los ambientes de prueba y producción.

Asimismo, los desarrollos son desplegados inicialmente en ambiente de pruebas, donde son validados frente a las historias de usuario y criterios de aceptación; los errores identificados son nuevamente asignados al desarrollador para su corrección y posteriormente las funcionalidades son presentadas al usuario para su validación.

Para la implementación en producción se evidenció la utilización de RFC, su registro y gestión mediante SEA, la definición de infraestructura, actividades, pruebas, responsables y ventana de mantenimiento, así como su presentación y aprobación ante el Comité de Cambios. Igualmente, se observaron mecanismos de reversa o rollback y actividades posteriores de estabilización.

No obstante, en materia de desarrollo seguro se identificaron debilidades en la trazabilidad técnica de las pruebas de seguridad. El GST-IN-006 establece que los resultados de las pruebas deben documentarse como parte del RFC y ser presentados al Comité de Cambios antes de autorizar el paso a producción.

Además, para las verificaciones técnicas exige documentar hallazgos, acciones correctivas, re-pruebas y evidencias asociadas. GST-IN-006 GST-IN-006(1) Los soportes complementarios aportados posteriormente a la presentación de resultados preliminares mediante memorando No. 2026-3-013831 permitieron evidenciar la atención efectiva de un hallazgo puntual de seguridad, pero no demostraron la operación integral y sistemática de este control conforme a lo definido en el instructivo.

5.5 Documentación y los lineamientos de seguridad aplicables a los Sistemas de Información.

Se verificó que la UPRA cuenta con lineamientos institucionales para la documentación técnica y funcional y para la seguridad de los Sistemas de Información, principalmente a través del GIA-PD-004 – Procedimiento de Ingeniería de Software, la GIA-GU-001 – Guía Metodológica de Referencia de Sistemas de Información, el GST-IN-006 – Instructivo para la Ejecución de Pruebas en el Desarrollo Seguro de Software y demás documentos institucionales asociados a seguridad y gestión de accesos.

En la prueba de recorrido aplicada a SEA/SEA.doc se evidenció documentación asociada al diseño y a la base de datos, incluyendo esquemas, diccionarios de datos, descripción de tablas y campos y generación de documentación técnica en formato HTML. Asimismo, se indicó que los manuales o guías de usuario se actualizan cuando los cambios realizados sobre los módulos así lo requieren, aunque se observó que la entidad se encuentra en transición hacia herramientas que permitan mantener esta documentación de forma más dinámica.

Respecto de la gestión de accesos, para el caso evaluado se verificó que SEA administra roles, perfiles, permisos y usuarios, y que los permisos adicionales deben ser solicitados por responsables autorizados, quedando trazabilidad mediante incidencias.

No obstante, el GST-MA-005 – Manual para la Gestión de Cuentas de Usuario suministrado corresponde a la versión 3 del 26 de agosto de 2026, posterior al período auditado y a la salida a producción evaluada, por lo cual esta versión no fue utilizada retroactivamente como criterio del caso.

En materia de seguridad, se evidenció que Servicios Tecnológicos realiza análisis sobre los ambientes de prueba y comunica hallazgos técnicos para su tratamiento antes o durante los pasos a producción. Sin embargo, durante la prueba de recorrido no se contó inicialmente con la totalidad de las evidencias que permitieran reconstruir de manera completa la ejecución, tratamiento y cierre de las pruebas de seguridad. Los soportes complementarios posteriormente aportados permitieron demostrar la atención de un hallazgo técnico puntual, pero no acreditaron el cumplimiento integral y sistemático de las actividades previstas en el GST-IN-006, particularmente en lo relacionado con la documentación y asociación de las evidencias de las pruebas al RFC y su revisión antes del paso a producción.

5.6 Prueba de recorrido sobre la actualización tecnológica y salida a producción de la nueva plataforma SEA / SEA.doc, desde el requerimiento hasta su implementación en producción.

Para verificar la aplicación de los controles definidos durante el ciclo de vida de los Sistemas de Información, se tenía previsto seleccionar una muestra de desarrollos ejecutados durante el segundo semestre de 2025 y el primer semestre de 2026 y efectuar pruebas de recorrido desde la identificación del

requerimiento hasta su implementación y estabilización en producción.

Adicionalmente, en la respuesta remitida mediante Memorando N.° 2026-3-011744 del 20 de agosto de 2026, la Oficina TIC informó como herramientas para la gestión del ciclo de desarrollo Azure DevOps, SEA y SharePoint, proporcionando las respectivas rutas de acceso. Sin embargo, durante la ejecución de la auditoría se evidenció que la Asesoría de Control Interno no contaba con permisos para acceder directamente a Azure DevOps ni al repositorio de SharePoint suministrado, situación que impidió efectuar de manera autónoma la consulta y contraste de las evidencias asociadas a requerimientos, historias de usuario, tareas, repositorios de código, versiones y documentación del desarrollo. Esta limitación hizo necesario realizar la verificación mediante una sesión asistida con el equipo de Sistemas de Información, quienes presentaron las evidencias disponibles directamente en las herramientas.

Durante la prueba de recorrido se verificaron aspectos relacionados con la identificación y refinamiento de requerimientos, estructuración de historias de usuario, criterios de aceptación, asignación de tareas, desarrollo, administración de repositorios y versiones, ejecución de pruebas funcionales, presentación de funcionalidades al usuario, gestión de errores, aprobación de cambios, RFC, Comité de Cambios, implementación en producción, mecanismos de reversa, documentación técnica, gestión de accesos y actividades posteriores de estabilización. La evidencia presentada permitió reconstruir razonablemente el ciclo de vida del caso evaluado desde el requerimiento hasta su implementación en producción.

Asimismo, se evidenció que las funcionalidades desarrolladas son sometidas progresivamente a pruebas en ambientes previos a producción y presentadas a los usuarios para su validación, permitiendo identificar ajustes antes de finalizar el desarrollo. Los errores detectados son registrados y nuevamente asignados al desarrollador para su atención.

No obstante, durante el recorrido se identificaron debilidades en la trazabilidad de algunas evidencias de seguridad y en la formalización de determinados lineamientos operativos, aspectos desarrollados en las observaciones correspondientes del presente informe.

5.7 Cumplimiento de TRD

En el marco de la presente auditoría se contempló la revisión de los repositorios documentales, rutas de almacenamiento y soportes asociados al ciclo de vida de los Sistemas de Información, con el propósito de verificar la conservación, organización y disponibilidad de las evidencias generadas durante las etapas de requerimiento, desarrollo, pruebas, control de versiones, gestión de cambios, implementación y documentación técnica, de conformidad con las Tablas de Retención Documental – TRD aplicables al proceso.

No obstante, la revisión presentó limitaciones, debido a que la Asesoría de Control Interno no contó con acceso directo a los repositorios informados por la Oficina TIC. En particular, las rutas suministradas para Azure DevOps y SharePoint no pudieron ser consultadas directamente por el equipo auditor por restricciones de acceso. En consecuencia, la verificación se efectuó principalmente mediante la visualización asistida de información durante la prueba de recorrido aplicada a SEA/SEA.doc, en la cual el equipo de Sistemas de Información presentó algunos de los soportes disponibles en las herramientas institucionales.

Durante dicha revisión se observaron documentos y registros asociados a requerimientos, historias de usuario, documentación de bases de datos, diccionarios de datos, documentación técnica generada en formato HTML, manuales o guías de usuario y otras evidencias relacionadas con el proceso de desarrollo. Sin embargo, dadas las restricciones de acceso señaladas, no fue posible realizar una verificación integral e independiente sobre la totalidad de los repositorios y soportes documentales asociados al ciclo de vida de los Sistemas de Información.

Adicionalmente, de acuerdo con la información reportada por Gestión Documental, la transferencia documental primaria correspondiente a las vigencias 2020, 2021, 2022 y 2023 fue legalizada el 12 de septiembre de 2025, sin compromisos pendientes. Por su parte, la transferencia correspondiente a la vigencia 2024 se encuentra aún en proceso de formalización.

En este contexto, si bien se evidenció la existencia de soportes documentales asociados al caso evaluado, las limitaciones de acceso a los repositorios y el estado de formalización de la transferencia documental de la vigencia 2024 restringieron la posibilidad de emitir una conclusión integral sobre el cumplimiento de las TRD para la totalidad de los Sistemas de Información objeto de auditoría.

5.8 Observaciones

5.8.1 Observación N°1. Debilidades en la formalización de los lineamientos operativos para DevOps y versionamiento de código referenciados en el procedimiento GIA-PD-004 – Ingeniería de Software.

Realizada la revisión del procedimiento GIA-PD-004 – Ingeniería de Software y la prueba de recorrido aplicada al proyecto "Actualización tecnológica y salida a producción de la nueva plataforma SEA / SEA.doc", se evidenció que el procedimiento referencia como documentos de apoyo un Instructivo DevOps y un Instructivo de versionamiento de código; sin embargo, dichos documentos no se encuentran formalmente institucionalizados dentro del Sistema de Gestión.

Durante la prueba de recorrido se verificó que la Oficina TIC aplica en la práctica mecanismos estructurados para la gestión de requerimientos, tareas, ramas, commits y versiones mediante Azure DevOps y repositorios de código, observándose que cada desarrollador trabaja sobre ramas específicas y registra los cambios realizados.

No obstante, la ausencia de formalización de los instructivos referenciados evidencia una debilidad en la estandarización documental de las prácticas operativas asociadas al desarrollo y control de versiones, lo cual puede afectar la continuidad, uniformidad y trazabilidad de estas actividades ante cambios de personal, herramientas o responsabilidades.

Criterio:

- GIA-PD-004 – Procedimiento Ingeniería de Software, versión 4 del 26/11/2025.
- GIA-GU-001 – Guía Metodológica de Referencia de Sistemas de Información.
- Modelo de Referencia de Arquitectura Empresarial – MRAE (MinTIC).
- ISO/IEC/IEEE 12207 – Procesos del ciclo de vida del software.

Recomendación:

Se recomienda formalizar, aprobar e institucionalizar los lineamientos operativos para la gestión DevOps y el versionamiento de código referenciados en el procedimiento GIA-PD-004, estableciendo como mínimo criterios para la administración de repositorios, estrategia y manejo de ramas, commits, versiones, revisiones y aprobaciones de código, liberaciones y paso entre

ambientes, así como responsables y evidencias requeridas, con el fin de fortalecer la estandarización, trazabilidad y continuidad de las prácticas actualmente implementadas.

5.8.2 Observación N°2. Debilidades en la trazabilidad técnica de las pruebas de seguridad definidas en el GST-IN-006 – Pruebas de Desarrollo Seguro.

Realizada la verificación de las evidencias presentadas durante la prueba de recorrido del proyecto "Actualización tecnológica y salida a producción de la nueva plataforma SEA / SEA.doc", se evidenció que la UPRA cuenta con el GST-IN-006 – Pruebas de Desarrollo Seguro, versión 2 del 09/04/2026, mediante el cual se establecen lineamientos para la ejecución de pruebas de seguridad sobre desarrollos y mejoras significativas de los Sistemas de Información.

Durante el recorrido se evidenció que Servicios Tecnológicos realiza análisis técnicos sobre los ambientes de prueba y comunica resultados asociados a aspectos de seguridad, incluyendo hallazgos relacionados con configuraciones y encabezados de seguridad, frente a los cuales se realizan ajustes antes de su paso a producción.

No obstante, no se contó con la totalidad de los soportes técnicos que permitieran verificar de manera integral la ejecución, resultado y cierre de las pruebas definidas en el GST-IN-006, particularmente la identificación de vulnerabilidades o debilidades técnicas, las acciones de corrección implementadas y la validación posterior que demuestre su resolución antes de la liberación a producción.

Criterio:

- GST-IN-006 – Instructivo de Pruebas de Desarrollo Seguro, versión 2 del 09/04/2026.
- GIA-PD-004 – Procedimiento Ingeniería de Software, versión 4 del 26/11/2025.
- GST-PD-007 – Procedimiento Gestión de Cambios de TI.
- ISO/IEC 27001:2022 – controles relacionados con ciclo de desarrollo seguro, pruebas de seguridad durante el desarrollo y aceptación, y gestión de cambios.

Recomendación:

Se recomienda fortalecer la ejecución, registro y trazabilidad técnica de las pruebas de desarrollo seguro establecidas en el GST-IN-006, definiendo mecanismos que permitan asociar a cada desarrollo o cambio las pruebas ejecutadas, resultados obtenidos, vulnerabilidades o debilidades identificadas, acciones de corrección implementadas y evidencias de re-prueba o validación posterior, asegurando que los hallazgos de seguridad sean atendidos y cerrados antes de la liberación a producción y que dicha información quede vinculada al requerimiento, RFC o registro de cambio correspondiente.

Posterior a la presentación de resultados preliminares llevada a cabo el 30 de septiembre, mediante el Memorando N.° 2026-3-013831 del 5 de octubre de 2026, la Oficina TIC remitió tres soportes documentales relacionados con la gestión de hallazgos de seguridad y los ajustes efectuados en ambiente productivo: la trazabilidad de comunicaciones sobre los hallazgos identificados y su atención, la solicitud de cambio para la implementación de los ajustes en producción y el acta del Comité de Cambios en la que consta su revisión y aprobación.

La Asesoría de Control Interno, una vez revisados los soportes remitidos, concluye que si bien los soportes remitidos permiten evidenciar que se identificaron hallazgos de seguridad, se gestionó un cambio mediante RFC, se aprobaron ajustes en Comité de Cambios y posteriormente se obtuvo un resultado técnico satisfactorio sobre los encabezados de seguridad de SEA, no se acredita el cumplimiento integral de lo establecido en el numeral 3.6 – Prueba 6: Prevención de Vulnerabilidades Técnicas en Entornos Productivos del GST-IN-006.

En particular, no se evidenció que la totalidad de las verificaciones técnicas previstas en dicha prueba hubieran sido ejecutadas, documentadas y anexadas al RFC antes de la autorización del paso a producción, ni que existiera una trazabilidad completa entre vulnerabilidades identificadas, plan de mitigación, evidencias técnicas de cada verificación y validación de cierre. El instructivo exige expresamente que estas evidencias formen parte del RFC y sean presentadas al Comité de Cambios. GST-IN-006.

Por tanto, los nuevos soportes demuestran la corrección y efectividad de una situación técnica puntual, pero no permiten acreditar la eliminación de la causa raíz asociada a la debilidad en la trazabilidad y conservación sistemática de las evidencias de pruebas de desarrollo seguro, ni demostrar la efectividad

sostenida del control definido en el GST-IN-006. En consecuencia, no procede el cierre de la Observación N.° 2.

5.9 Oportunidades de mejora

Las oportunidades de mejora generadas por la Asesoría de Control Interno en sus informes tienen como fin la mejora de los aspectos evaluados, por lo que se espera sean consideradas por los responsables como un instrumento que contribuya a la realización de ajustes que se requieran, previos a posibles pronunciamientos de organismos externos de control.

A continuación, se enuncian las oportunidades de mejora derivadas del ejercicio de auditoria realizado:

5.9.1 Integración de la trazabilidad entre herramientas: Fortalecer la relación entre los registros generados en SEA, Azure DevOps, repositorios de código, SharePoint y RFC, mediante identificadores comunes o referencias cruzadas que permitan reconstruir de forma más ágil e integral el ciclo de vida de cada desarrollo.

5.9.2 Actualización de documentación técnica y funcional: Definir criterios para determinar qué documentación técnica y funcional debe revisarse o actualizarse en cada cambio o liberación, incorporando esta verificación como parte del cierre del desarrollo o del RFC, con el fin de mantenerla alineada con las versiones puestas en producción.

5.9.3 Revisión periódica de accesos: Fortalecer la gestión de accesos mediante revisiones periódicas de roles, perfiles y permisos, especialmente ante cambios de cargo, terminación de contratos, nuevas funcionalidades o modificaciones de los sistemas, dejando evidencia de las revisiones y ajustes realizados.

6. Conclusiones

La auditoría presentó limitaciones en el suministro y acceso a la información, lo que impidió conformar de manera completa el universo de desarrollos e intervenciones y, por tanto, no permitió cumplir integralmente con el alcance definido, orientado a evaluar técnicamente el ciclo de vida de los Sistemas de Información institucionales durante el segundo semestre de 2025 y el primer semestre de 2026.

En consecuencia, la evaluación se concentró en la prueba de recorrido de SEA/SEA.doc, donde se evidenció la aplicación y trazabilidad de las principales etapas del ciclo de vida del software. No obstante, estos resultados no pueden generalizarse al total de los Sistemas de Información institucionales, motivo por el cual se genera una alerta por las limitaciones recurrentes en el acceso, disponibilidad y suficiencia de la información requerida para el ejercicio de auditoría.

Es prioritario fortalecer el control interno sobre todos los productos asociados a los Sistemas de Información institucionales y su ciclo de vida que permitan evidenciar y hacer la trazabilidad del uso de los recursos asignados.