AUDITORÍA A LOS CONTROLES DE SEGURIDAD INFORMÁTICA DEL APLICATIVO WEBSAFI EN EL SERVICIO GEOLÓGICO COLOMBIANO

Fecha del Informe: 30 de abril del 2026
Nombre Auditores: Crhistian Amador León - Alfredo José Flórez Otero
No. Informe: OCI-14-2026

1. OBJETIVO Y ALCANCE.

Objetivo: Evaluar la implementación, efectividad y cumplimiento de los controles de seguridad informática implementados en el sistema WEBSAFI, con el fin de verificar la protección de la información administrativa, financiera y de talento humano, así como la integridad de las transacciones, la disponibilidad del servicio y la seguridad de las integraciones con otros sistemas institucionales.

Alcance: Vigencia 2025 y primer trimestre de 2026. La verificación se ejecutó entre el 4 de marzo y el 15 de abril de 2026. En desarrollo de esta, se solicitó información al Grupo de Trabajo de Tecnologías de la Información de la Secretaria General, y comprendió la revisión de la documentación y los controles implementados. Con base en la información allegada, se realizó el análisis, contraste y validación de los soportes remitidos.

2. CRITERIOS DE AUDITORÍA / SEGUIMIENTO.

- **Ley 87 de 1993.** *"Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones".*
- **Decreto 648 de 2017** "*Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentaria Único del Sector de la Función Pública" y en cumplimiento del rol de enfoque hacia la prevención que le compete a las Oficina de Control Interno*".
- **Resolución No. 500 de 2021.** "*Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".*
- **Resolución 2277 de 2025:** "Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia"
- Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información emitido por MinTIC.
- MO-TEC-002 - Políticas de operación específicas de gestión de seguridad de la información
- Política General de Seguridad de la Información SGC.
- ISO/IEC 27001:2022 e ISO/IEC 27002:2022
- Demás normativa y documentación interna aplicable consultada en ISOLUCIÓN.

3. ANÁLISIS DE LA INFORMACIÓN

3.1. Metodología Aplicada

La metodología aplicada para la auditoría comprendió las siguientes actividades:

- Se comunicó el inicio de la auditoría mediante memorando interno radicado No. 2026-130-001642-3 del 06 de marzo de 2026, dirigido a la Coordinación del Grupo de Trabajo Tecnologías de Información, en el cual se informó el objetivo, alcance, cronograma y requerimientos de información.
- Se solicitó al Grupo de Trabajo de Tecnologías de la Información, la designación de los responsables encargados de atender el ejercicio de auditoría, así como la remisión de la información requerida dentro del plazo establecido.
- Se requirió información relacionada con:
  - La gestión del sistema WEBSAFI, incluyendo su registro dentro del inventario institucional de activos de información y su clasificación, así como la identificación del supervisor del contrato con el proveedor de la herramienta y los responsables TIC del sistema.
  - La gestión de accesos e identidades, incluyendo la matriz de roles y privilegios, el procedimiento de creación, modificación y eliminación de usuarios, el listado de usuarios activos, la relación de usuarios con privilegios administrativos, la evidencia de revisión de accesos privilegiados, las solicitudes tramitadas mediante mesa de ayuda y la autenticación contra Directorio Activo (en caso de aplicar).
  - La gestión de cambios y mantenimiento del sistema, incluyendo los procedimientos aplicables, el registro de cambios efectuados durante las vigencias 2025 y primer trimestre 2026, y la evidencia de los desarrollos realizados.
  - La ejecución de pruebas funcionales y no funcionales, las actas de aprobación previas al paso a producción y la evidencia de la separación de ambientes (desarrollo, pruebas y producción).
  - Los controles de seguridad de la información, incluyendo la protección de logs, la aplicación de la política de copias de respaldo, los controles criptográficos (cuando aplique) y los mecanismos de seguridad en las comunicaciones e integraciones con otros sistemas institucionales.
  - La gestión de operación e incidentes, incluyendo el registro de incidentes del sistema durante la vigencia 2025 y el procedimiento para su reporte y gestión.
  - La gestión contractual del servicio, incluyendo los informes de cumplimiento de los Acuerdos de Niveles de Servicio (ANS) y la evidencia de seguimiento del supervisor del contrato frente a los incidentes reportados.
- Se efectuó la revisión, análisis y contraste de la información según los soportes remitidos.
- La reunión de apertura se llevó a cabo el 11 de marzo de 2026, mediante la plataforma Meet de Google, en la cual se socializó el plan de trabajo, la metodología de verificación, los entregables previstos y el cronograma establecido.
- En el marco de la reunión de apertura de la auditoría, se acordó con el área auditada, la entrega progresiva de la información requerida, en atención a la imposibilidad de consolidarla en una sola remisión; en este sentido, se realizaron entregas parciales durante marzo de 2026, remitiendo inicialmente avances de la información, posteriormente un consolidado con la

mayoría de las respuestas requeridas y, finalmente, la totalidad de los soportes el 24 de marzo de 2026.

- El informe preliminar se envió al proceso para comentarios mediante radicado 2026-130-002468-3 del 20/04/2026, y remitido mediante correo electrónico del 24/04/2026. La respuesta fue recibida por la Oficina de Control Interno, mediante correo electrónico del 29/04/2026.

3.2. Desarrollo de la auditoría

La auditoría se desarrolló bajo un enfoque basado en riesgos, tomando como referencia las buenas prácticas contenidas en la ISO/IEC 27001:2022 y la guía ISO/IEC 27002:2022, lineamientos definidos por el Ministerio de Tecnologías de la Información en la política de Gobierno digital, y lineamientos y/o normativa interna. Para su ejecución, los controles evaluados fueron organizados en cinco dominios definidos para efectos del análisis, así:

(1) Gobierno del sistema,
(2) Gestión de accesos e identidades,
(3) Gestión de cambios,
(4) Seguridad de la información, y
(5) Gestión de operación e incidentes.

Esta clasificación corresponde a una agrupación metodológica adoptada para el ejercicio de auditoría, con el propósito de facilitar la evaluación integral de los controles implementados en el sistema.

Así mismo, los dominios definidos permitieron evaluar de manera articulada la implementación, efectividad y cumplimiento de los controles, así como su contribución a la protección de la información, la integridad de las transacciones, la disponibilidad del servicio y la seguridad de las integraciones con otros sistemas institucionales.

3.2.1. Gobierno del Sistema

En el marco del seguimiento realizado al sistema WEBSAFI, se evaluaron los aspectos relacionados con su identificación, responsabilidad y control dentro de la gestión institucional, con el propósito de verificar la existencia de lineamientos y mecanismos que permitan su adecuada administración.

En este sentido, se evidenció que el sistema WEBSAFI se encuentra en operación y soporta procesos administrativos y financieros de la entidad, así como su inclusión en instrumentos de gestión tecnológica como el catálogo de servicios institucional (*Soporte con el que cuenta la OCI desde la vigencia 2025*). No obstante, en la validación realizada frente a los mecanismos formales de gestión de activos de información, se identificó una debilidad en su registro y control, pues a la solicitud de la OCI del *"Registro del sistema WEBSAFI dentro del inventario institucional de activos de información, indicando su clasificación "*, se indicó por parte del área auditada que el aplicativo no se encuentra registrado en el sistema de inventario de activos, así:

Así mismo, en validación efectuada por la Oficina de Control Interno al inventario de activos de información publicado en el micrositio de transparencia de la entidad, no se evidenció la inclusión del referido sistema.

Lo anterior, incumple los siguientes criterios:

- El manual de operación "*MO-TEC-002 Políticas de operación específicas de gestión de seguridad de la información*" versión 1, el cual especifica en el numeral "*4.2.1 Política de gestión de activos"* que los activos de información deben ser debidamente identificados, clasificados, protegidos y gestionados durante todo su ciclo de vida, garantizando su adecuada administración y control.
- La Política General de Seguridad de la Información de la entidad vigente (versión 2 de enero de 2025) la cual indica que la entidad debe asegurar la protección de los activos de información, garantizando su confidencialidad, integridad y disponibilidad, mediante la implementación de controles y mecanismos de gestión adecuados. Así mismo se indica como objetivo del SGSI establecer, implementar, mantener y mejorar continuamente un modelo general de criterios, directrices, condiciones y pautas para proteger los activos de información digital del SGC
- El Modelo de Seguridad y Privacidad de la Información – MSPI establece como actividad fundamental la identificación, inventario, clasificación y publicación de los activos de información, con el fin de garantizar su adecuada protección y gestión dentro de la entidad.
- La ISO/IEC 27001:2022 y la ISO/IEC 27002:2022 establecen la necesidad de identificar y gestionar los activos de información como base para la implementación de controles de seguridad y la gestión de riesgos.

Riesgo: Posibilidad de que los sistemas de información institucionales no sean identificados, clasificados ni gestionados formalmente como activos de información, lo que puede generar deficiencias en la implementación de controles de seguridad, afectando la confidencialidad, integridad y disponibilidad de la información, así como el cumplimiento de los lineamientos del Modelo de Seguridad y Privacidad de la Información y la normativa aplicable.

Recomendaciones:

- Incorporar el sistema WEBSAFI dentro del inventario institucional de activos de información, asegurando su adecuada identificación, clasificación y valoración conforme a los lineamientos del MSPI.

- Establecer o fortalecer los procedimientos y controles que garanticen la articulación entre los instrumentos de gestión tecnológica (como el catálogo de servicios) y el inventario de activos de información.
- Implementar mecanismos de revisión y actualización periódica del inventario de activos de información, que permitan asegurar la inclusión de todos los sistemas en operación.
- Definir responsables y puntos de control para garantizar la trazabilidad y actualización de la información asociada a los activos tecnológicos.

Comentario al Informe Preliminar por parte del proceso: "*Respuesta / Plan de mejora*"
*"Respecto a las observaciones relacionadas con el cumplimiento de las políticas y estándares de gestión de activos de información, se permite aclarar que el sistema de información **WebSAFI** fue desarrollado e implementado con anterioridad a la expedición de la normatividad mencionada, incluyendo el manual **MO-TEC-002**, la Política General de Seguridad de la Información (versión 2 – enero 2025), el **MSPI** y los lineamientos de la **ISO/IEC 27001:2022 y 27002:2022**.*

En ese sentido, al momento de su implementación inicial no se contaba con los lineamientos actuales que exigen la identificación, clasificación, inventario y gestión formal de los activos de información bajo el enfoque del SGSI.

*No obstante, la entidad reconoce la importancia de dar cumplimiento a la normatividad vigente y garantizar la adecuada gestión del activo de información correspondiente al sistema WebSAFI, alineado con los principios de **confidencialidad, integridad y disponibilidad**.*

*Por lo anterior, se solicita de manera respetuosa un **plazo prudente** para llevar a cabo las siguientes actividades:*

- *Identificación formal del sistema WebSAFI como activo de información.*
- *Inclusión en el inventario institucional de activos.*
- *Clasificación de la información conforme a los criterios definidos en el SGSI.*
- *Definición e implementación de controles de seguridad aplicables.*
- *Documentación dentro del Modelo de Seguridad y Privacidad de la Información (MSPI).*

Estas acciones permitirán asegurar el cumplimiento progresivo de los lineamientos establecidos en la normatividad vigente y fortalecer la gestión de seguridad de la información en la entidad".

Análisis OCI a la respuesta del proceso: En relación con la respuesta presentada por el proceso, en la cual se indica que el sistema WebSAFI fue implementado con anterioridad a

la expedición de la normatividad vigente en materia de gestión de activos de información, se precisa que dicha situación constituye un contexto válido respecto a su implementación inicial.

No obstante, se evidenció que los lineamientos en materia de seguridad de la información y gestión de activos no son completamente nuevos, toda vez que el Manual de Operación MO-TEC-002 corresponde a una actualización de un documento previo existente desde el año 2020, el cual ya contemplaba políticas específicas de seguridad de la información y gestión de activos. En este sentido, si bien la normativa actual ha fortalecido y actualizado dichos lineamientos, no puede considerarse que la entidad no contara con referentes previos en la materia.

Adicionalmente, el cumplimiento de los lineamientos vigentes establecidos en el Manual de Operación MO-TEC-002, la Política General de Seguridad de la Información, el Modelo de Seguridad y Privacidad de la Información – MSPI y las normas ISO/IEC 27001:2022 y 27002:2022 es de carácter obligatorio en el marco de la gestión actual de la entidad, independientemente de la fecha de implementación de los sistemas de información.

En este sentido, la situación expuesta por el proceso no desvirtúa la condición evidenciada por la Oficina de Control Interno, relacionada con la ausencia de registro, clasificación y gestión formal del sistema WebSAFI como activo de información.

No obstante, se valora positivamente que el proceso reconoce la situación identificada y propone acciones orientadas a la identificación, inclusión en el inventario, clasificación y gestión del sistema como activo de información, las cuales son coherentes con la no conformidad evidenciada.

Por lo anterior, se mantiene la no conformidad y se considera procedente el plan de mejora propuesto, el cual deberá ser objeto de seguimiento en el marco de los mecanismos definidos por la entidad.

Respuesta por parte del proceso: *"La propiedad de WEBSAFI es de Software House, es un servicio contratado, ¿debe estar en el inventario institucional de activos de información? ¿Hasta dónde va la propiedad?"*

Análisis OCI a la respuesta del proceso: En relación con la observación presentada por el proceso respecto a "*La propiedad de WEBSAFI es de Software House, es un servicio contratado, ¿debe estar en el inventario institucional de activos de información? ¿Hasta dónde va la propiedad?"*, se precisa que, independientemente de que el software sea provisto por un tercero bajo un modelo de servicio (SaaS), el sistema constituye un activo

de información de la entidad, en la medida en que soporta procesos institucionales y gestiona información propia de la organización.

De acuerdo con las definiciones institucionales establecidas en el Manual de Operación MO-TEC-002, un activo corresponde a cualquier información, recurso o elemento asociado a su tratamiento (tales como sistemas, infraestructuras, medios físicos, servicios o personas) que tenga valor para la organización, y cuya protección resulta necesaria para garantizar sus objetivos y operaciones; así mismo, un activo de información corresponde a todo elemento que contiene, procesa o soporta información que la entidad genere, obtenga, adquiera, transforme o controle en el ejercicio de sus funciones .

En este sentido, la clasificación de un activo de información no depende de su propiedad, sino de su uso y control en el desarrollo de las funciones institucionales. Así mismo, de acuerdo con los lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI y las buenas prácticas establecidas en la norma ISO/IEC 27001:2022 y su guía ISO/IEC 27002:2022, la gestión de activos de información incluye todos aquellos recursos tecnológicos y de información utilizados en la operación institucional, independientemente de su modalidad de adquisición.

En consecuencia, el sistema WEBSAFI, en tanto procesa y soporta información institucional, constituye un activo de información que debe ser gestionado e incluido en el inventario institucional. Por lo anterior, la observación presentada no desvirtúa la situación evidenciada, por lo cual se mantiene la no conformidad relacionada con la debilidad en la gestión de activos de información.

3.2.2. Gestión de Accesos e Identidades

En el marco del seguimiento realizado al sistema WEBSAFI, se evaluaron los controles relacionados con la gestión de accesos e identidades, con el propósito de verificar que el acceso al sistema se encuentre debidamente controlado, autorizado y restringido conforme a los perfiles y responsabilidades definidas, garantizando la protección de la información y la integridad de las operaciones.

Para ello, se analizaron los mecanismos implementados para la asignación, modificación y eliminación de usuarios, la gestión de roles y privilegios, la autenticación de usuarios, así como los controles asociados a la revisión periódica de accesos y la administración de privilegios.

En la verificación realizada, se identificaron las siguientes debilidades en la gestión de accesos e identidades del sistema WEBSAFI:

- La matriz de roles y privilegios suministrada no refleja de manera integral los perfiles funcionales definidos en el sistema, toda vez que contempla únicamente roles generales

(SUPER_ADMIN, ADMIN, USER_ADMIN, USER y CONSULTA), mientras que en la base de usuarios activos se identifican múltiples perfiles funcionales específicos, sin que se evidencie su correspondencia con los privilegios asignados.

- Los roles definidos en la matriz presentan una misma combinación base de permisos (insertar, editar, eliminar y consultar), diferenciándose principalmente en su descripción, lo que limita la verificación del principio de mínimo privilegio y la adecuada segregación de funciones.
- No se evidenció la existencia de un mecanismo formal de revisión periódica de accesos, especialmente de aquellos con privilegios elevados, toda vez que la información suministrada corresponde a la gestión operativa de solicitudes de usuarios y no a un ejercicio de validación periódica de los accesos otorgados.
- Si bien se evidenció la gestión de solicitudes de acceso a través de registros operativos de atención de requerimientos suministrados por el proceso, la información corresponde a la ejecución de actividades de creación, modificación y eliminación de usuarios, sin que se identifiquen controles formales de aprobación o validación independiente en la asignación de accesos, tales como registros de autorización por parte de responsables definidos, lo que limita la verificación de la adecuada autorización de los permisos otorgados

Riesgo: Posibilidad de asignación de accesos inadecuados, excesivos o no autorizados a los usuarios del sistema, así como de permanencia de privilegios innecesarios en el tiempo, lo que puede afectar la confidencialidad, integridad y disponibilidad de la información, así como la trazabilidad y control de las operaciones realizadas en el sistema, incrementando el riesgo de errores, uso indebido o fraude.

Recomendaciones

- Actualizar y fortalecer la matriz de roles y privilegios del sistema WEBSAFI, asegurando que refleje de manera completa los perfiles funcionales existentes y los permisos asociados a cada uno.
- Implementar controles que garanticen la aplicación del principio de mínimo privilegio y la adecuada segregación de funciones en la asignación de accesos.
- Definir e implementar un procedimiento formal de revisión periódica de accesos, incluyendo la validación de usuarios activos y privilegios administrativos, con la correspondiente evidencia de ejecución.
- Establecer mecanismos de aprobación y validación independiente en la gestión de accesos, evitando la concentración de funciones en un único usuario.

3.2.3. Gestión de Cambios

En el marco del seguimiento realizado al sistema WEBSAFI, se evaluaron los controles relacionados con la gestión de cambios, con el propósito de verificar que las modificaciones, desarrollos y actualizaciones del sistema se gestionen de manera controlada, autorizada y trazable, garantizando la estabilidad, integridad y disponibilidad del servicio. Para ello, se analizaron los mecanismos implementados para la solicitud, evaluación, aprobación, ejecución, pruebas y paso a producción de los cambios, así como la existencia de registros, evidencias y controles asociados a su gestión.

En desarrollo de la verificación realizada, se identificaron las siguientes debilidades en la gestión de cambios del sistema WEBSAFI:

- No se evidenció la existencia de un procedimiento formal documentado y aplicado para la gestión de actualizaciones y mantenimiento del sistema, toda vez que el proceso indicó que las actualizaciones se realizan a través de una herramienta denominada "Actualizador", la cual permite gestionar versiones de los módulos, sin que se definan formalmente las etapas, responsables, controles y criterios asociados al proceso de gestión de cambios.
- Si bien se evidenció la existencia de registros asociados a solicitudes y desarrollos a través de tickets y correos electrónicos, estos no corresponden a un registro integral, estructurado y centralizado de gestión de cambios, lo que limita la trazabilidad completa de los mismos desde su solicitud hasta su implementación en producción.
- Aunque en algunos casos se evidencian aprobaciones y validaciones funcionales, estas no obedecen a un esquema formal y estandarizado de aprobación previa al paso a producción, ni se identifican criterios definidos que aseguren que todos los cambios sean evaluados y autorizados antes de su implementación.
- No se evidenció de manera clara la implementación de controles formales que aseguren la adecuada gestión y promoción de cambios entre ambientes, ni mecanismos definidos que garanticen el control en el paso a producción.

Riesgo: Posibilidad de implementación de cambios no controlados, no autorizados o insuficientemente evaluados en el sistema WEBSAFI, lo que puede generar afectaciones en la estabilidad, disponibilidad, integridad y seguridad de la información, así como la materialización de incidentes operativos o fallas en el servicio.

Recomendaciones:

- Adoptar o adaptar el procedimiento PR-GGC-CSI-001 para la gestión de cambios del sistema WEBSAFI, considerando su modelo de operación bajo esquema SaaS.
- Definir e implementar un flujo formal de gestión de cambios que incluya solicitud, evaluación, aprobación, pruebas, implementación y cierre.
- Establecer un registro centralizado de cambios que permita garantizar la trazabilidad completa de los mismos.
- Definir lineamientos claros para la ejecución y documentación de pruebas funcionales y no funcionales.
- Implementar mecanismos de control que aseguren la validación y autorización previa de los cambios antes de su paso a producción.

Observación al Informe Preliminar por parte del proceso: "*En relación con las debilidades identificadas en la gestión de cambios del sistema* ***WEBSAFI****, se permite aclarar que actualmente sí se realiza un seguimiento integral de los cambios desde su solicitud hasta su salida a producción, mediante el uso de tickets y comunicaciones asociadas. Este proceso incluye la validación y aprobación final por parte del usuario final, quien emite el concepto de conformidad previo a la implementación en producción, constituyéndose este como el mecanismo de control actualmente establecido.*

No obstante, se reconoce que dicho proceso no se encuentra formalmente documentado bajo un procedimiento estructurado que defina de manera explícita las etapas, roles, responsables, criterios de aprobación, controles y mecanismos de trazabilidad, conforme a las buenas prácticas en gestión de cambios y a los lineamientos del Sistema de Gestión de Seguridad de la Información.

En este sentido, y en atención a las recomendaciones emitidas por el área de Control Interno, la entidad se compromete a fortalecer el proceso mediante las siguientes acciones:

- *Elaboración y formalización de un procedimiento documentado de gestión de cambios para el sistema WEBSAFI.*
- *Definición de las etapas del proceso (solicitud, análisis, aprobación, desarrollo, pruebas, paso a producción y cierre).*
- *Establecimiento de roles y responsabilidades claras.*
- *Implementación de un registro centralizado y estructurado que garantice la trazabilidad completa de los cambios.*
- *Definición de criterios formales de aprobación y control previo al paso a producción.*
- *Fortalecimiento de los controles de gestión de cambios entre ambientes.*

Estas acciones permitirán alinear el proceso con las mejores prácticas y asegurar una gestión de cambios más robusta, controlada y trazable, en cumplimiento de los lineamientos institucionales y normativos vigentes. …"

Análisis OCI a la respuesta del proceso: En relación con la respuesta presentada por el proceso frente a la gestión de cambios del sistema WEBSAFI, en la cual se indica que actualmente se realiza un seguimiento integral de los cambios mediante el uso de tickets y comunicaciones asociadas, se precisa que dicha información evidencia la existencia de prácticas operativas orientadas a la gestión de cambios, incluyendo solicitudes, validaciones y aprobaciones por parte de usuarios finales.

No obstante, la verificación realizada por la Oficina de Control Interno se enfocó en la existencia de un esquema formal, documentado y estructurado de gestión de cambios, que contemple de manera explícita las etapas del proceso, roles, responsables, criterios de aprobación, controles y mecanismos de trazabilidad, conforme a los lineamientos del Sistema de Gestión de Seguridad de la Información. Si bien se evidencian prácticas operativas soportadas en tickets, estas no corresponden a un proceso formalmente definido ni garantizan una trazabilidad integral, estandarizada y centralizada de los cambios desde su solicitud hasta su implementación en producción.

En este sentido y teniendo en cuenta que el proceso reconoce que no cuenta actualmente con un procedimiento documentado que defina de manera estructurada la gestión de cambios, se valora positivamente la propuesta de acciones orientadas a la formalización del procedimiento, definición de roles, establecimiento de controles y fortalecimiento de la trazabilidad, las cuales son coherentes con la no conformidad identificada.

Por lo anterior, la observación presentada no desvirtúa la situación evidenciada, por lo cual se mantiene la no conformidad, considerándose procedente el plan de mejora propuesto, el cual deberá ser objeto de seguimiento por parte de la entidad.

3.2.4. Seguridad de la información

En el marco del seguimiento realizado al sistema WEBSAFI, se evaluaron los controles técnicos asociados a la seguridad de la información, con el propósito de verificar que la información gestionada por el sistema se encuentre debidamente protegida en términos de confidencialidad, integridad, disponibilidad y trazabilidad, conforme a los lineamientos institucionales y las buenas prácticas en la materia.

Para ello, se analizaron los mecanismos implementados para la generación, almacenamiento y protección de registros de auditoría (logs), la gestión de copias de respaldo, el uso de controles criptográficos, así como la seguridad de las integraciones con otros sistemas institucionales y servicios de autenticación.

En desarrollo de la verificación realizada, y considerando la información adicional suministrada por el proceso al informe preliminar, se identificaron las siguientes debilidades en los controles de seguridad de la información del sistema WEBSAFI:

- Si bien el sistema cuenta con mecanismos de registro de eventos mediante herramientas como Graylog y almacenamiento en motores tipo Elasticsearch, no se evidenció la definición formal de criterios de retención, ni controles documentados que garanticen la integridad, protección contra alteración o eliminación indebida, control de acceso y trazabilidad de los registros de auditoría.
- Se evidenció la implementación de mecanismos técnicos para la gestión de respaldos mediante herramientas especializadas (como Oracle RMAN), incluyendo validaciones de integridad; no obstante, no se identificó documentación formal que establezca de manera estructurada la periodicidad, alcance, niveles de criticidad, tiempos de retención, ni la definición de pruebas de restauración debidamente planificadas, ejecutadas y documentadas.
- Si bien se evidenció la implementación de mecanismos de cifrado en tránsito mediante protocolos seguros, así como controles asociados al cifrado de respaldos, no se identificó la formalización, documentación ni articulación de estos controles dentro de un esquema definido de gestión criptográfica conforme a los lineamientos del Sistema de Gestión de Seguridad de la Información.
- Se informó la conexión del sistema con servicios como LDAP y otros sistemas institucionales; sin embargo, no se evidenció la definición ni documentación formal de controles de seguridad asociados a dichas integraciones, tales como mecanismos de autenticación segura, cifrado de la información, gestión de accesos y trazabilidad de las transacciones.

Riesgo: Posibilidad de afectación a la confidencialidad, integridad, disponibilidad y trazabilidad de la información gestionada por el sistema WEBSAFI, debido a la falta de implementación, formalización y evidencia de cumplimiento de los controles de seguridad definidos en las políticas

del Sistema de Gestión de Seguridad de la Información, lo que puede generar debilidades en la gestión de eventos, respaldos, protección de la información y control de accesos, dificultando la detección oportuna de incidentes, la recuperación ante fallas y el cumplimiento de los lineamientos normativos aplicables.

Recomendaciones

- Formalizar, documentar y evidenciar la implementación de los lineamientos establecidos en el Manual MO-TEC-002 en relación con la gestión de registros de auditoría (logs), incluyendo criterios de retención, integridad, control de acceso y trazabilidad.
- Documentar y evidenciar el cumplimiento de la política de copias de respaldo definida en el MO-TEC-002, incluyendo la periodicidad, alcance, niveles de criticidad, tiempos de retención y la ejecución de pruebas de restauración.
- Formalizar y documentar los controles criptográficos implementados, asegurando su alineación con los lineamientos establecidos en el MO-TEC-002 y su aplicación conforme a la clasificación de la información y análisis de riesgos.
- Definir, documentar y evidenciar la implementación de controles de seguridad asociados a las integraciones del sistema (LDAP u otros), en cumplimiento de los lineamientos de seguridad en comunicaciones e interoperabilidad establecidos por la entidad.
- Asegurar la articulación y alineación de los controles técnicos implementados en el sistema WEBSAFI con las políticas y lineamientos definidos en el SGSI, garantizando su aplicación efectiva y trazable.

Observación al Informe Preliminar por parte del proceso: "*1. Gestión de backups: La base de datos de WebSafi utiliza Oracle RMAN, herramienta que garantiza la integridad mediante validaciones de bloques en cada ejecución. Para formalizar la trazabilidad solicitada:*

- *Validación Técnica: Se realiza una verificación de integridad (RESTORE VALIDATE) al finalizar cada respaldo, asegurando la recuperabilidad de la información.*
- *Evidencia Documental**:** A partir de mayo, se emite un Reporte Mensual de Gestión de Backups, el cual consolida los logs de ejecución y certificación de integridad.*

2. Controles Criptográficos y Acceso: En relación con los controles criptográficos asociados al cifrado de información a nivel de base de datos la entidad realizó el análisis de riesgos correspondiente y estableció:

• Aislamiento de Red: Los sistemas se encuentran desplegados en infraestructuras controladas, con acceso restringido mediante mecanismos de autenticación, segmentación de red, controles perimetrales y monitoreo continuo, lo que reduce significativamente la probabilidad de acceso no autorizado directo a los datos almacenados. Adicionalmente, se implementan controles compensatorios como el cifrado en tránsito (TLS/HTTPS), control de accesos basado en roles, gestión de privilegios, registro de eventos (logs) y mecanismos de respaldo controlado.

• Cifrado en Tránsito: Se ha formalizado el uso de Oracle Native Network Encryption (NNE) con

algoritmo AES256, asegurando que toda comunicación entre la aplicación y la base de datos sea cifrada de forma nativa.

• Cifrado en Reposo: Se integra el cifrado por contraseña en los respaldos de RMAN, garantizando la confidencialidad de los datos almacenados en medios externos sin requerir licenciamiento adicional."

Análisis OCI a la respuesta del proceso: En relación con la respuesta presentada por el proceso frente a los controles de seguridad de la información del sistema WEBSAFI, se precisa que la información aportada evidencia la existencia de mecanismos técnicos implementados, particularmente en lo relacionado con la gestión de copias de respaldo mediante herramientas como Oracle RMAN, así como la implementación de controles criptográficos como el cifrado en tránsito y el cifrado de respaldos. En este sentido, se reconoce que dichos controles contribuyen a la protección de la información en términos de confidencialidad e integridad, y representan avances frente a la situación inicialmente evidenciada.

No obstante, la verificación realizada por la Oficina de Control Interno no se limitó a la existencia de controles técnicos, sino a su formalización, documentación y alineación con los lineamientos definidos en el Sistema de Gestión de Seguridad de la Información – SGSI.

En este contexto, persisten debilidades relacionadas con la ausencia de documentación formal que establezca criterios de retención, integridad, control de acceso y trazabilidad de los registros de auditoría (logs), así como la falta de lineamientos estructurados para la gestión de copias de respaldo, incluyendo su periodicidad, alcance, niveles de criticidad y la ejecución de pruebas de restauración debidamente documentadas. Así mismo, no se evidenció documentación formal de los controles de seguridad asociados a las integraciones del sistema, ni su articulación dentro de un esquema definido de seguridad de la información.

En relación con los controles criptográficos, la información aportada permite evidenciar su implementación; no obstante, no se identificó su formalización ni documentación dentro del marco del SGSI, ni su alineación con la clasificación de la información y análisis de riesgos de la entidad. Por lo anterior, la respuesta presentada no desvirtúa la situación evidenciada en su totalidad, por lo cual se mantiene la no conformidad, con ajustes en su alcance, y se valora positivamente el fortalecimiento de los controles técnicos por parte del proceso.

3.2.5. Gestión de operación e incidentes.

En el marco de la revisión al contrato No. 128-2025 con fecha de inicio del 19 de febrero de 2025 y fecha de finalización del 31 de diciembre de 2025 suscrito con el proveedor SOFTWARE HOUSE S.A.S, cuyo objeto corresponde "Contratar el servicio de soporte técnico, administración y actualización de versiones del software ERP WEBSAFI (Enterprise Resource Planning)", se efectuó la revisión de los pagos realizados durante la vigencia 2025, así como de los soportes asociados a la ejecución del componente de soporte mensual, la bolsa de horas y los acuerdos de niveles de servicio (ANS).

Para tal efecto, se analizaron las facturas, órdenes de pago, informes de actividades, registros de solicitudes (tickets) y certificaciones de cumplimiento cargadas en SECOP, evidenciando lo siguiente:

Periodo	¿Tiene informe soporte?	¿Pago soporte?	Valor soporte	¿Bolsa de horas?	Horas bolsa	Valor bolsa	Total Bolsa en Pesos $	¿Soporte técnico bolsa?
Febrero	Si	Si	$ 5.394.270,00	No	0	$ 321.300,00	0	No
marzo	Si	Si	$ 17.980.900,00	No	0	$ 321.300,00	0	No
Abril	Si	Si	$ 17.980.900,00	SI	10	$ 321.300,00	3.213.000,00	Si
Mayo	Si	Si	$ 17.980.900,00	SI	102	$ 321.300,00	32.772.600,00	Si
Junio	Si	Si	$ 17.980.900,00	No	0	$ 321.300,00	0	No
Julio	Si	Si	$ 17.980.900,00	SI	20	$ 321.300,00	6.426.000,00	Si
Agosto	Si	Si	$ 17.980.900,00	No	0	$ 321.300,00	0	No
Septiembre	Si	Si	$ 17.980.900,00	SI	49	$ 321.300,00	15.743.700,00	Si
Octubre	Si	Si	$ 17.980.900,00	No	0	$ 321.300,00	0	No
Noviembre	Si	Si	$ 17.980.900,00	SI	53	$ 321.300,00	17.028.900,00	Si
Diciembre	Si	Si	$ 17.980.900,00					
		Total	**$ 185.203.270,00**	-	**234**	-	**$ 75.184.200,00**	-

De acuerdo con la revisión de los soportes, se evidenció lo siguiente:

- Bolsa de horas contratada: **234 horas**
- Bolsa de horas ejecutada: **234 horas**
- Valor total soporte: **$185.203.270**
- Valor total horas: **$75.184.200**
- Las horas ejecutadas corresponden a desarrollos, ajustes funcionales y mejoras del sistema.
- Cada ejecución cuenta con soporte técnico (tickets, descripción de actividades, horas reportadas y evidencia de implementación).
- Los pagos se realizaron conforme al valor hora definido contractualmente.

En este sentido, la ejecución de la bolsa de horas se considera adecuada y coherente con lo pactado contractualmente.

Observación – Debilidades en la aplicación y seguimiento de los ANS

De acuerdo con lo establecido en el contrato No. 128-2025, se definieron acuerdos de niveles de servicio (ANS) con tiempos máximos de atención según la criticidad de los requerimientos, los cuales se detallan a continuación:

Nivel de Criticidad	Tiempo Máximo de Solución	ANS	Descripción	Descuento sobre valor al Mes
BAJA	24 HORAS	85%	Solicitud anticipada de un requerimiento por vencimiento en algún proceso, a saber. Programación de capacitación. Solicitud de un nuevo requerimiento o funcionalidad (Consulta, mejora, modificación, actualización) Solicitudes para hacer presentaciones y/o demostraciones.	Para valores mayores o iguales a 90 y menores a 95: 5%. Para valores mayores o iguales a 80 menores a y 90: 10%. Para valores mayores o iguales a 70 y menores a 80: 15%
MEDIA	12 HORAS	90%	Próximo vencimiento para entrega de información a Entidades de control. Programación reunión extraordinaria. Programación visita Solicitud de revisión de un proceso determinado, previo análisis efectuado por el usuario.	Para valores mayores o iguales a 90 y menores a 95: 5%. Para valores mayores o iguales a 80 menores a y 90: 10%. Para valores mayores o iguales a 70 y menores a 80: 15%
ALTA	4 HORAS	95%	Próximo vencimiento liquidación nómina y seguridad social. Inconsistencias con información de nómina y seguridad social Comisiones: Procesos de programación y legalización. Gestión de contabilidad e inventarios Conocimiento Geocientífica Consulta general de operación del sistema Asistencia / Respuesta por conexión remita. Contingencia por causa externa (falla de energía eléctrica, daño en servidor) Falla técnica en impresión de informes. Falla técnica en comunicaciones (Servidor correo). Asistencia / respuesta por conexión remota. Restitución de copias de seguridad	Para valores mayores o iguales a 90 y menores a 95: 5%. Para valores mayores o iguales a 80 menores a y 90: 10%. Para valores mayores o iguales a 70 y menores a 80: 15%

A partir de la revisión de los informes de soporte mensual, se evidenció que la entidad cuenta con información operativa suficiente para validar los ANS, incluyendo prioridad de los requerimientos, fechas de solicitud, atención y solución, así como horas asociadas a su gestión.

No obstante, del análisis consolidado de las solicitudes registradas durante la vigencia 2025, se identificaron las siguientes situaciones:

- Se evidencian casos puntuales en los cuales los tiempos de atención superan los establecidos contractualmente, sin que se identifique su análisis o tratamiento.

INFORME DE SOLICITUDES SERVICIO GEOLOGICO COLOMBIANO MES DE MARZO DE 2025													
Ticket	No. Solicitud	Clasificador	Prioridad	Fecha solicitud	Funcionario/ contratista solicitante	Módulo	Descripción funcionalidad	Estado	Fecha Diagnostico / Primera Atención	Fecha Solución	Detalle de la solución	HORAS ANS	HORAS CALCULADAS
39505	3	Soporte o Pregunta	Media	2025-03-03 09:51	Diana Marcela Lopez	Inventario	Buenos días me podran por favor ayduar con la siguiente corrección de mi cuenta de cobro la cual tiene fecha de terminación 11 de febrero pero en realidad es por todo el mes muchas gracias	Cerrado	2025-03-05 - 10:35	2025-03-05 - 10:35	Buenos días Diego, Contrato: 215-2024 Verificando la plataforma identificamos que registro la novedad de porroga y adición con fecha de terminación 11 de febrero de 2025. Atendiendo su solicitud, se verifico la fecha de la novedad siendo correcta 28 de febrero de 2025. Por favor verificar.	12	40min
39574	17	Soporte o Pregunta	Media	2025-03-06 16:39	Luz Angela Linares	Nómina	Buenas tardes Se realizó la validación de la planilla de seguridad social de febrero presentando inconsistencias para: 1. 30284840 - FANNY SALAZAR SANCHEZ: Debe reportarse en una sola línea con la novedad de incapacidad todo el mes. Dado que no se pueden reportar 28 días, se solicita poner 30 días laborados con un IBC de 1.489.234 2: 10292974 WILSON ALEXANDER TORRES TONGUINO: Presenta la inconsistencia: "El número de días reportados para la novedad IRL no coincide con la cantidad de días reportados entre la fecha inicial y la fecha final de la novedad" Se solicita modificar los días de VST deben ser 22 y los de accidente de trabajo 8. Los IBC están correctos	Cerrado	2025-03-07 - 11:28	2025-03-14 - 17:28	Buenos días, Luz Angela Se verifican ambos casos y se valida días correctos, verificar planilla nuevamente. 1. 30284840 - FANNY SALAZAR SANCHEZ: Debe reportarse en una sola línea con la novedad de incapacidad todo el mes. Dado que no se pueden reportar 28 días, se solicita poner 30 días laborados con un IBC de 1.489.234 2: 10292974 WILSON ALEXANDER TORRES TONGUINO: Presenta la inconsistencia: Buenas tardes Luz Angela, Adjuntamos Resumen de Autoliquidación Mensual 2-2025 conciliado. Por favor verificar.	12	4,5
39584	20	Soporte o Pregunta	Media	2025-03-10 14:54	Diuliano Yuri Rodriguez Suarez	Control de Comisiones	Buenas tardes tres Software House evidenciamos, que el aplicativo "control de comisiones", no bloquea a los contratistas, que no tienen contrato y deja programar la comision; tenemos un caso de la comision 10 de PGN, que la radicaron el 27 de febrero, y en especial a la comisionada "Natalia Toro" le programaron una comision para el dia 11 de marzo; pero el contrato quedo activo el dia 03 de marzo. nos podrian ayudar a tener este bloqueo, que los contratistas que no tengan un contrato activo, no aparezca para programar ninguna comision ni en PGN ni en SGR.	Cerrado	2025-03-11 - 08:14	2025-03-14 - 18:40	Buenos días, Atendiedo su solicitud, se implementaron las siguientes validaciones para la programación de contratista: El sistema valida que la fecha de regreso de la comisión sea menor mínimo 3 días Vs a la fecha final del contrato (parametrizable en control comisiones) Que el contratista tenga contrato activo en RVC El sistema generara la validación correspondiente y NO permitira continuar con la programación. Adjuntamos Imagen ejemplo de la funcionalidad. Quedamos atentos a sus comentarios.	12	3

- Se evidencian inconsistencias en la aplicación de la categoría “No aplica ANS”, sin que se identifiquen criterios definidos, estandarizados y documentados que sustenten su asignación, lo que afecta la consistencia y comparabilidad en la clasificación de los requerimientos.
- Se identifican requerimientos que, por su naturaleza funcional o por corresponder a incidentes del sistema, cumplen con características para ser gestionados bajo ANS; no obstante, fueron clasificados fuera de su alcance, lo que limita la adecuada medición, seguimiento y control del cumplimiento de los niveles de servicio.

INFORME DE SOLICITUDES SERVICIO GEOLOGICO COLOMBIANO MES DE AGOSTO DE 2026												
Ticket	No. Solicitud	Clasificador	Prioridad	Fecha solicitud	Funcionario/ contratista solicitante	Módulo	Descripción funcionalidad	Estado	Fecha Diagnostico / Primera Atención	Fecha Solución	Detalle de la solución	HORAS ANS	HORAS CALCULADAS
40482	1	Soporte o Pregunta	No Aplica ANS	2026-08-01 09:17	Diana Marcela Lopez	Inventario	buenos días Ingeniera se informa que en el cierre se encontraron las siguientes diferencias * Solo subió la interfase de 1 ingresos del PGN se envia evidencia fotográfica	Cerrado	2026-08-12 - 23:29	2026-08-12 - 23:29	Buenas tardes Diana Se encuentra verificada la conciliación de inventarios JULIO 2026 Adjunto Boletines. La forma de generar los boletines es: No debe seleccionar nada en Grupo Origen	No Aplica ANS	No Aplica ANS

- No se evidenció la consolidación de indicadores, reportes periódicos ni mecanismos formales de seguimiento al cumplimiento de los ANS.
- Se evidencian inconsistencias en la clasificación de la criticidad de los requerimientos, particularmente en periodos en los cuales la totalidad de las solicitudes se registran bajo una única categoría (Media), sin presencia de requerimientos clasificados como Alta o Baja, lo que no resulta consistente con la dinámica operativa esperada de un sistema ERP, que normalmente involucra incidentes de diversa criticidad.

Periodo	Informe de Solicitudes	Baja	Media	Alta	N/A
Febrero	24	1	18	1	4
marzo	62	7	46	1	8
Abril	72	2	67	0	3
Mayo	74	1	69	3	1
Junio	110	5	95	2	8
Julio	81	1	72	3	5
Agosto	79	6	65	1	7
Septiembre	83	0	83	0	0
Octubre	180	0	180	0	0
Noviembre	105	0	105	0	0
Diciembre	114	0	114	0	0

Se recomienda fortalecer la gestión de los acuerdos de niveles de servicio (ANS), mediante:

- La definición de criterios claros y documentados para la clasificación de requerimientos según su criticidad
- La estandarización de los criterios para determinar cuándo un requerimiento se encuentra dentro o fuera del alcance de ANS
- La implementación de mecanismos de seguimiento, control e indicadores que permitan evaluar el cumplimiento del servicio
- El fortalecimiento de la trazabilidad entre solicitudes, desarrollos y uso de la bolsa de horas

Observación al Informe Preliminar por parte del proceso: "*Aclaración frente al incumplimiento de ANS*"

"En relación con la observación sobre el presunto incumplimiento de los Acuerdos de Nivel de Servicio (ANS), es importante precisar que, si bien en la imagen presentada se evidencian tiempos que podrían interpretarse como fuera de los acuerdos establecidos, el análisis realizado no contempla el contexto completo de la gestión de los tickets ni la dinámica operativa del proceso.

Como se evidencia en los casos analizados (Solicitudes #39505, #39574 y #39584), existe un seguimiento continuo y detallado desde la creación del ticket hasta su cierre, incluyendo:

- *Registro de la solicitud inicial por parte del usuario.*
- *Validación y análisis técnico por parte del equipo de soporte.*
- *Interacción constante con el usuario para ajustes, validaciones y confirmaciones.*
- *Implementación de soluciones y ajustes en el sistema.*
- *Confirmación final por parte del usuario antes del cierre del ticket.*

*Es importante resaltar que, dada la experiencia y conocimiento funcional de la entidad, en muchos casos se realiza una **validación previa con el usuario**, en la cual se identifica si la situación reportada corresponde a un error del sistema o a inconsistencias derivadas del uso del mismo. En múltiples ocasiones, se trata de **errores operativos de los funcionarios**, los cuales son corregidos mediante acompañamiento y orientación, sin afectar la estabilidad ni el funcionamiento del sistema.*

Adicionalmente, algunos casos requieren iteraciones, validaciones externas (como operadores de información), o conciliaciones funcionales, lo cual extiende los tiempos de atención, pero garantiza una solución correcta y validada.

*Siempre **la gestión realizada asegura la calidad de la solución, la continuidad del servicio y la satisfacción del usuario**, lo cual se evidencia en la aprobación final de cada ticket por parte del solicitante.*

No obstante, en atención a las observaciones de Control Interno, la entidad reconoce la oportunidad de mejora en:

- *La formalización de los ANS considerando la complejidad real de los casos.*
- *La clasificación adecuada de los tickets según su criticidad y tipo (incidente, requerimiento, ajuste funcional).*
- *El fortalecimiento de los mecanismos de medición y control de tiempos.*

Estas acciones permitirán alinear de manera más precisa los indicadores de cumplimiento con la realidad operativa del sistema WEBSAFI".

Análisis OCI a la respuesta del proceso: En relación con la respuesta presentada por el proceso frente al presunto incumplimiento de los Acuerdos de Niveles de Servicio (ANS), se precisa que la información aportada evidencia la existencia de actividades operativas orientadas a la gestión de los requerimientos, incluyendo el registro de solicitudes, análisis técnico, interacción con los usuarios, implementación de soluciones y validación para el cierre de los tickets.

No obstante, el análisis realizado por la Oficina de Control Interno no se limitó a la gestión operativa de los casos, sino a la verificación del cumplimiento de los tiempos y condiciones establecidos contractualmente para los ANS, los cuales definen criterios objetivos de medición basados en niveles de criticidad y tiempos máximos de atención.

En este sentido, si bien factores como iteraciones, validaciones funcionales, acompañamiento a usuarios o conciliaciones externas hacen parte de la dinámica operativa del servicio, estos no eximen del cumplimiento, medición y control de los ANS definidos, ni sustituyen la necesidad de contar con mecanismos formales que permitan su seguimiento, análisis y gestión ante desviaciones.

Así mismo, no se evidenció el análisis formal de los casos en los cuales los tiempos de atención superan los establecidos contractualmente, ni la existencia de mecanismos estructurados que permitan gestionar dichas desviaciones, lo cual limita la trazabilidad y control del cumplimiento de los ANS. Pese a lo anterior, se valora positivamente que el proceso reconoce la necesidad de fortalecer la formalización de los ANS, la adecuada clasificación de los requerimientos y los mecanismos de medición y control de tiempos, aspectos que son coherentes con la observación realizada.

Por lo anterior, la respuesta presentada no desvirtúa la situación evidenciada, por lo cual se mantiene la observación, considerándose procedente el plan de mejora propuesto por el proceso.

Observación al Informe Preliminar por parte del proceso: ***"Aclaración sobre la clasificación "No aplica ANS"***

En relación con la observación sobre inconsistencias en la aplicación de la categoría ***"No aplica ANS"****, es importante precisar que, en el contexto operativo del sistema* ***WEBSAFI****, no todos los requerimientos gestionados a través de la mesa de ayuda corresponden a incidentes o solicitudes que deban estar sujetos a Acuerdos de Nivel de Servicio (ANS).*

Dado el conocimiento técnico y funcional del contratista, así como la dinámica del servicio, existen solicitudes que corresponden a:

- *Consultas funcionales.*
- *Acompañamiento al usuario.*
- *Ajustes menores o validaciones operativas.*
- *Correcciones derivadas del uso inadecuado del sistema.*

Este tipo de requerimientos, por su naturaleza, no impactan la disponibilidad, continuidad ni la integridad del sistema, y por tanto no requieren ser gestionados bajo ANS, ya que no constituyen incidentes críticos ni solicitudes formales de desarrollo.

No obstante, se reconoce que actualmente la asignación de la categoría ***"No aplica ANS"*** *se realiza con base en el criterio técnico y la experiencia del equipo de soporte, lo que puede generar variaciones en su aplicación al no contar con criterios formalmente documentados y estandarizados.*

En este sentido, y atendiendo la observación de Control Interno, se adoptarán las siguientes acciones de mejora:

- *Definir y documentar criterios claros para la clasificación de tickets bajo ANS y "No aplica ANS".*
- *Establecer tipologías de requerimientos (incidente, requerimiento, consulta, mejora, etc.).*
- *Implementar lineamientos que permitan una clasificación homogénea y consistente.*
- *Fortalecer los mecanismos de seguimiento y medición de los ANS, garantizando su correcta aplicación.*

De esta manera, se busca mantener la flexibilidad operativa necesaria para atender oportunamente las necesidades del servicio, sin afectar la correcta medición, control y trazabilidad de los niveles de atención".

Análisis OCI a la respuesta del proceso: En relación con la respuesta presentada por el proceso frente a la clasificación de requerimientos bajo la categoría "*No aplica ANS*", se precisa que la información aportada permite evidenciar que, en efecto, existen tipologías de solicitudes que, por su naturaleza, no corresponden a incidentes o requerimientos sujetos a Acuerdos de Niveles de Servicio (ANS), tales como consultas funcionales, acompañamiento a usuarios o validaciones operativas.

No obstante, la verificación realizada por la Oficina de Control Interno no se centró en la existencia de dichas tipologías, sino en la ausencia de criterios formales, documentados y estandarizados para su clasificación, lo cual impacta la consistencia, trazabilidad y comparabilidad en la gestión de los requerimientos. En este sentido, el hecho de que la asignación de la categoría “No aplica ANS” se realice con base en el criterio técnico y la experiencia del equipo de soporte, sin lineamientos definidos, genera riesgo de subjetividad en la clasificación, lo que puede afectar la adecuada medición y control del cumplimiento de los ANS.

Así mismo, el proceso reconoce la inexistencia de criterios formalmente documentados y estandarizados para dicha clasificación, lo cual confirma la situación evidenciada por la Oficina de Control Interno. Pese a lo anterior, se valora positivamente la definición de acciones orientadas a establecer tipologías de requerimientos, documentar criterios de clasificación y fortalecer los mecanismos de seguimiento y medición, las cuales son coherentes con la observación realizada.

Por lo anterior, la respuesta presentada no desvirtúa la situación evidenciada, por lo cual se mantiene la observación, considerándose procedente el plan de mejora propuesto por el proceso.

3.3. Evaluación del proceso contractual SGC-CD-414-2026

En el marco de la auditoría realizada, se incluyó la revisión jurídica del proceso contractual SGC-CD-414-2026 (contrato No. 379-2026) con fecha de inicio del 20 de enero de 2026 y fecha de finalización del 31 de diciembre de 2026 suscrito con el proveedor SOFTWARE HOUSE S.A.S, cuyo objeto corresponde a la contratación del servicio de soporte técnico, administración y actualización de versiones del software ERP WEBSAFI. De acuerdo con el análisis efectuado, no se identificaron observaciones en relación con el cumplimiento de los requisitos legales y procedimentales asociados al proceso contractual, evidenciándose lo siguiente:

- La contratación se adelantó mediante la modalidad de contratación directa por la causal de no pluralidad de oferentes, contando con el certificado de exclusividad del proveedor, así como con el acto administrativo de justificación debidamente expedido por la Entidad.
- El proveedor aportó la totalidad de los documentos requeridos para la suscripción del contrato, los cuales se encuentran cargados en la plataforma SECOP II.
- Las garantías contractuales fueron constituidas conforme a lo establecido en los estudios previos, en cuanto a montos y vigencias, y cuentan con aprobación en SECOP II.
- Se evidenció la expedición y publicación del Certificado de Disponibilidad Presupuestal (CDP) y del Registro Presupuestal (RP).
- Las cuentas de cobro correspondientes a los meses de enero y febrero de 2026 fueron creadas y aprobadas en SECOP II, previa verificación de los soportes exigidos, incluyendo recibo a satisfacción, factura electrónica, acreditación del pago de aportes al sistema de seguridad social y evidencias de ejecución de actividades, por parte del supervisor del contrato.
- El supervisor del contrato se encuentra debidamente designado y registrado en SECOP II.
- Se evidenció la disponibilidad de los documentos del proceso contractual, tales como estudios previos, matriz de riesgos, análisis del sector, acto administrativo de justificación,

certificado de exclusividad y documentación del proveedor, los cuales se encuentran publicados en SECOP II.

3. NO CONFORMIDADES

De acuerdo con los resultados obtenidos, fueron identificadas las siguientes 4 no conformidades, para que sea definido un plan de mejoramiento de acuerdo con el procedimiento vigente *"PR-PSG-ADM-001 planes de mejoramiento continuo"*, así:

ID	Descripción de la No Conformidad	Criterio
1	**Debilidad en la gestión de activos de información – Sistema WEBSAFI** En el marco de la verificación realizada, se evidenció que el sistema de información WEBSAFI no se encuentra registrado dentro del inventario institucional de activos de información, de acuerdo con lo informado por el área responsable. Así mismo, en validación efectuada por la Oficina de Control Interno al inventario de activos de información publicado en el micrositio de transparencia de la entidad, no se evidenció la inclusión del referido sistema. Lo anterior evidencia una debilidad en la gestión de activos de información, en tanto no se garantiza su adecuada identificación, clasificación y control, en contravía de lo establecido en las políticas internas de seguridad de la información, los lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI, y las buenas prácticas definidas en estándares internacionales como ISO 27001 e ISO 27002.	**Manual de Operación MO-TEC-002** - Políticas de operación específicas de gestión de seguridad de la información versión1 del 27 de enero de 2026 - 4.2.1. Política de gestión de activos. (…) *El SGC, como propietario de los activos de información, debe mantener un inventario actualizado con todos los activos institucionales, identificados, clasificados y protegidos según su valor, criticidad, sensibilidad, nivel de reserva y funcionalidad. (…)* *(…) El proceso de clasificación y etiquetado se realizará de acuerdo con lo establecido en el Procedimiento de Identificación, Clasificación y Etiquetado de Activos de Información Digitales (PR-GGC-003).* Así mismo, la Política General de Seguridad de la Información versión 2 de enero de 2025 dispone que la entidad establece la necesidad de garantizar la protección de los activos de información, asegurando su confidencialidad, integridad y disponibilidad mediante la implementación de controles adecuados. En concordancia, el Modelo de Seguridad y Privacidad de la Información – MSPI dispone que los activos de información deben ser identificados, inventariados, clasificados y publicados como parte

ID	Descripción de la No Conformidad	Criterio
		fundamental de la gestión de seguridad de la información. De igual forma, la ISO/IEC 27001:2022 y la ISO/IEC 27002:2022 establecen la necesidad de identificar y gestionar los activos de información como base para la implementación de controles de seguridad y la gestión de riesgos. (A.5.9 Inventario de activos - A.5.12 Clasificación de la información).
2	**Debilidades en la gestión de accesos e identidades - Sistema WEBSAFI** En el marco de la verificación realizada a la gestión de accesos e identidades del sistema WEBSAFI, se evidenciaron debilidades relacionadas con la definición, asignación, control y seguimiento de los accesos otorgados a los usuarios, así: • La matriz de roles y privilegios suministrada no refleja de manera integral los perfiles funcionales definidos en el sistema, toda vez que contempla únicamente roles generales (SUPER_ADMIN, ADMIN, USER_ADMIN, USER y CONSULTA), mientras que en la base de usuarios activos se identifican múltiples perfiles funcionales específicos, sin que se evidencie su correspondencia con los privilegios asignados. • Los roles definidos en la matriz presentan una misma combinación base de permisos (insertar, editar, eliminar y consultar), diferenciándose principalmente en su descripción, lo que limita la verificación del principio de mínimo privilegio y la adecuada segregación de funciones. • Así mismo, frente a la solicitud de evidencia de revisión periódica de accesos privilegiados, el proceso remitió información correspondiente a	**Manual de Operación MO-TEC-002** - **MO-TEC-002 -** Políticas de operación específicas de gestión de seguridad de la información – 4.3.1. Política de control de Acceso, versión 1 del 27 de enero de 2026. *"Los cambios que impliquen la creación, modificación, bloqueo, desactivación, activación y eliminación de cuentas de usuario, roles o privilegios serán atendidos por medio de una solicitud formal por parte del jefe inmediato o supervisor de contrato al Grupo de Tecnologías de Información en la mesa de ayuda… conservando registro de las autorizaciones y los privilegios otorgados."* *"...esta debe estar acorde a los perfiles de acceso estipulados, los cuales se deben mantener en una matriz de roles y privilegios estandarizados, configurados y asignados.".* *"El SGC a través del grupo designado, debe verificar periódicamente y ratificar los accesos y todas las autorizaciones sobre sus recursos tecnológicos, sistemas de información y plataformas (…)"* *"El SGC a través del grupo designado, debe revisar y controlar los derechos de acceso privilegiado con regularidad, para verificar*

ID	Descripción de la No Conformidad	Criterio
	la gestión operativa de solicitudes de creación, modificación y eliminación de usuarios; no obstante, no se evidenció la existencia de mecanismos formales orientados a la validación periódica de los accesos otorgados, especialmente aquellos con privilegios elevados. • Si bien se evidenció la gestión de solicitudes de acceso a través de registros operativos de atención de requerimientos suministrados por el proceso, no se identificó evidencia de mecanismos de aprobación o validación independiente en la asignación de accesos, tales como registros de autorización por parte de responsables definidos o evidencias de aprobación previa, lo que limita la verificación de la adecuada autorización de los permisos otorgados. Lo anterior, teniendo en cuenta que no se garantiza que los accesos otorgados sean adecuados, autorizados y controlados conforme a las funciones de los usuarios, afectando la aplicación del principio de mínimo privilegio, la segregación de funciones y la trazabilidad de los accesos.	*si son acordes con los deberes asociados a los roles y perfiles definidos por el SGC."* **PR-TEC-GAU-001** – Procedimiento de Gestión de Usuarios, versión 1 del 15 de enero de 2020. "Todos los roles se crearán según la Matriz de Roles y Perfiles definida por el SGC…" "Para proceder a ejecutar la solicitud, se debe contar con la aprobación del director y/o jefe del Área. En caso contrario, la solicitud será finalizada…" En concordancia, el Modelo de Seguridad y Privacidad de la Información – MSPI establece la implementación de controles para la gestión de accesos, incluyendo la definición de roles, la asignación controlada de permisos, la segregación de funciones y la revisión periódica de los accesos otorgados. De igual forma, la ISO/IEC 27001:2022 y la ISO/IEC 27002:2022 establecen la necesidad de implementar controles de acceso basados en roles, aplicar el principio de menor privilegio, garantizar la adecuada segregación de funciones y realizar revisiones periódicas de los derechos de acceso para asegurar su pertinencia y vigencia (A.5.15, A.5.16 y A.5.18).
3	**Debilidades en la gestión de cambios del sistema WEBSAFI** En el marco de la verificación realizada a la gestión de cambios del sistema WEBSAFI, se evidenciaron debilidades relacionadas con la formalización, control, trazabilidad y estandarización del proceso de gestión de cambios:	**PR-GGC-CSI-001 -** Procedimiento de Gestión de Cambios de Sistemas de Información, versión 1 del 20 de diciembre de 2019. "Administrar y controlar los cambios… utilizando herramientas comunes para registrar, evaluar, aprobar, seguir y cerrar

ID	Descripción de la No Conformidad	Criterio
	• No se evidenció la aplicación del procedimiento institucional de gestión de cambios, toda vez que las actualizaciones del sistema se realizan a través de una herramienta denominada "Actualizador", sin que se observe la adopción de los lineamientos definidos en dicho procedimiento, particularmente en lo relacionado con la definición estructurada de las etapas del proceso, los responsables, los controles asociados y los criterios para la aprobación y paso a producción de los cambios. • Se evidenció la existencia de solicitudes, desarrollos y atenciones de requerimientos a través de tickets y comunicaciones, estos no corresponden a un registro integral y centralizado de gestión de cambios, lo que limita la trazabilidad completa de los mismos. • Aunque en algunos casos se evidencian aprobaciones y validaciones funcionales, no se identificó la existencia de un esquema formal y estandarizado que garantice que todos los cambios sean evaluados, aprobados y autorizados antes de su implementación en producción. • No se evidenció la ejecución estructurada y documentada de pruebas no funcionales, ni la existencia de lineamientos definidos para su realización, lo que limita la verificación de la calidad y seguridad de los cambios implementados. • Si bien el sistema WEBSAFI opera bajo un modelo de software como servicio (SaaS), en el cual el desarrollo y despliegue técnico de los cambios es realizado por un tercero, no se evidenció la adopción o adaptación del	todos los cambios que se presentan en ambiente productivo." "Esta fase comprende la solicitud del cambio diligenciando el formato de Requerimiento de Cambios…" "El Comité de cambios… realizará la aprobación o rechazo del cambio…" "La aprobación… se realizará por consenso… quedando registro de ello…" "Para paso a producción… el cambio deberá haber sido probado." "Toda la documentación… deberá ser almacenada en el repositorio del cambio…" De igual forma, la ISO/IEC 27001:2022 establece en su Anexo A los siguientes controles aplicables: • A.8.32 – Gestión de cambios, el cual dispone que los cambios en los sistemas de información deben ser controlados mediante procesos que incluyan su evaluación, aprobación, pruebas e implementación. • A.5.36 – Cumplimiento de políticas y normas, que señala la obligación de asegurar el cumplimiento de los procedimientos internos definidos por la organización. En concordancia, el Modelo de Seguridad y Privacidad de la Información – MSPI establece la necesidad de implementar, evaluar y mejorar continuamente los controles de seguridad digital, bajo un enfoque basado en riesgos y el ciclo PHVA, asegurando que los cambios en los sistemas de información sean gestionados

ID	Descripción de la No Conformidad	Criterio
	procedimiento institucional de gestión de cambios por parte de la Entidad, ni mecanismos que permitan asegurar el control, validación y autorización de los cambios que impactan su operación. Lo anterior evidencia debilidades en la gestión de cambios, en tanto no se garantiza que los cambios implementados en el sistema sean gestionados bajo un proceso formal, controlado y trazable, lo que puede afectar la estabilidad, seguridad e integridad del sistema de información.	de manera controlada, trazable y verificable.
4	**Debilidades en la implementación de controles de seguridad de la información en el sistema WEBSAFI** En el marco de la verificación realizada a los controles de seguridad de la información asociados al sistema WEBSAFI, se evidenciaron debilidades relacionadas con la gestión de registros de auditoría (logs), copias de respaldo, uso de controles criptográficos y control sobre la información gestionada a través del sistema, así: • Si bien el sistema cuenta con mecanismos de registro de eventos mediante el uso de herramientas como Graylog y almacenamiento en motores tipo Elasticsearch, se observó que parte de los registros (logs) son gestionados bajo esquemas de retención temporal, susceptibles de eliminación, sin que se evidencie la definición formal de criterios de retención, mecanismos de protección contra alteración o eliminación indebida, ni controles documentados que garanticen su integridad y trazabilidad. • En relación con las copias de respaldo, se evidenció la existencia de mecanismos técnicos de generación de respaldos a nivel de infraestructura; no obstante, no se identificó documentación formal que establezca	**Manual de Operación MO-TEC-002** - **MO-TEC-002 -** Políticas de operación específicas de gestión de seguridad de la información – 4.3.1. Política de control de Acceso, versión 1 del 27 de enero de 2026 4.3.1. Política de control de acceso “Los cambios que impliquen la creación, modificación, bloqueo, desactivación, activación y eliminación de cuentas de usuario, roles o privilegios serán atendidos por medio de una solicitud formal (…) conservando registro de las autorizaciones y los privilegios otorgados.” “El SGC (…) debe verificar periódicamente y ratificar los accesos y todas las autorizaciones sobre sus recursos tecnológicos, sistemas de información y plataformas (…)” 4.6.2. Política de copias de respaldo “Se debe llevar un registro de la información a respaldar, la periodicidad de la ejecución de las copias de respaldo, el nivel de clasificación de la información respaldada y el período de retención de las copias de respaldo.” 4.6.3. Política de registro de eventos

ID	Descripción de la No Conformidad	Criterio
	la periodicidad, alcance, niveles de criticidad, tiempos de retención, ni evidencia de pruebas de restauración debidamente planificadas, ejecutadas y documentadas, lo que limita la verificación de la efectividad de dichos controles. • En relación con el uso de controles criptográficos, si bien se evidenció la implementación de mecanismos de cifrado en tránsito mediante protocolos seguros, así como controles asociados al cifrado de respaldos, no se identificó la formalización, documentación ni articulación de estos controles dentro de un esquema definido de gestión criptográfica conforme a los lineamientos del Sistema de Gestión de Seguridad de la Información, ni su alineación con la clasificación de la información y el análisis de riesgos de la entidad. • Si bien se informó la integración del sistema con servicios como LDAP para autenticación de usuarios, no se evidenció la definición ni documentación formal de controles de seguridad asociados a dichas integraciones, tales como mecanismos de autenticación segura, cifrado de la información, gestión de accesos y trazabilidad de las transacciones. Lo anterior evidencia debilidades en la implementación, formalización y documentación de los controles de seguridad de la información, en tanto no se garantiza de manera integral su aplicación conforme a los lineamientos definidos en el Sistema de Gestión de Seguridad de la Información, afectando la trazabilidad, verificación y control de los mecanismos de	"Establecer los lineamientos para generar, preservar la integridad, no repudio, la confidencialidad y la disponibilidad de los registros de auditoría (logs) (…)" 4.4.1. Política sobre el uso de controles criptográficos "El cifrado debe aplicarse a todos los dispositivos, medios y sistemas que almacenen o procesen información clasificada como reservada, confidencial o de uso interno. (…)" En concordancia, la ISO/IEC 27001:2022 establece en su Anexo A controles relacionados con la protección de la información, tales como: • A.8.15 – Registro de eventos, orientado a la generación y conservación de logs. • A.8.13 – Copias de respaldo, relacionado con la protección y recuperación de la información. • A.8.24 – Uso de criptografía, para la protección de la confidencialidad e integridad de la información. Así mismo, el Modelo de Seguridad y Privacidad de la Información – MSPI establece la necesidad de implementar controles de seguridad digital orientados a la protección de los activos de información, así como la evaluación de la efectividad de dichos controles bajo un enfoque basado en riesgos y el ciclo PHVA.

ID	Descripción de la No Conformidad	Criterio
	protección de la información gestionada por el sistema WEBSAFI.	

4. CONCLUSIONES.

- Como resultado del seguimiento realizado a los controles de seguridad informática del sistema WEBSAFI, se concluye que la entidad cuenta con mecanismos operativos para la gestión del sistema y la prestación del servicio; sin embargo, se evidencian debilidades en la formalización, documentación, control y evaluación de los controles implementados, lo que limita la demostración de su efectividad conforme a los lineamientos institucionales y las buenas prácticas en seguridad de la información.
- En particular, se identificaron debilidades en la gestión de activos de información, toda vez que el sistema WEBSAFI no se encuentra debidamente registrado en el inventario institucional, lo que afecta su identificación, clasificación y control dentro del Sistema de Gestión de Seguridad de la Información.
- Así mismo, se evidenciaron debilidades en la gestión de accesos e identidades, relacionadas con la definición de roles y privilegios, la ausencia de mecanismos formales de revisión periódica de accesos y la falta de evidencia de controles de aprobación en la asignación de permisos, lo que puede afectar la adecuada restricción y control de los accesos al sistema.
- En cuanto a la gestión de cambios, se evidenció que, aunque existen mecanismos operativos para la atención de requerimientos y desarrollos, no se observa la adopción del procedimiento institucional definido para tal fin, ni la existencia de un proceso formal, estructurado y trazable que garantice el control integral de los cambios implementados en el sistema, especialmente considerando su operación bajo un modelo de software como servicio (SaaS).
- De igual forma, en relación con los controles de seguridad de la información, se identificaron debilidades en la gestión de logs, copias de respaldo, formalización y documentación de controles criptográficos y seguridad de las integraciones, evidenciando la ausencia de lineamientos formales y documentación que permitan garantizar la integridad, disponibilidad, confidencialidad y trazabilidad de la información gestionada por el sistema.
- En cuanto a la ejecución de la bolsa de horas, se evidenció coherencia entre las horas contratadas y ejecutadas, así como la existencia de soportes asociados a su uso; no obstante, se identifican oportunidades de mejora en la articulación entre las solicitudes atendidas, su clasificación bajo ANS y la trazabilidad de los desarrollos realizados, con el fin de fortalecer el control integral sobre la ejecución del servicio.

En términos generales, si bien el sistema WEBSAFI se encuentra en operación y cuenta con mecanismos técnicos y operativos que soportan su funcionamiento, se evidencian debilidades en la formalización, estandarización e integración de los controles de seguridad de la información, lo que limita la capacidad de la Entidad para demostrar su efectividad, trazabilidad y cumplimiento frente a los lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI y las buenas prácticas internacionales.

Así mismo, se identificaron oportunidades de mejora en la gestión contractual del servicio, particularmente en la aplicación y seguimiento de los acuerdos de niveles de servicio (ANS), lo que puede afectar la medición objetiva del desempeño del proveedor y la toma de decisiones basada en información verificable.

Elaboró: Crhistian Augusto Amador León – Alfredo José Flórez Otero - Contratistas Oficina de Control Interno

Revisó y Aprobó: Erika Marcela Huari Mateus - Jefe Oficina de Control Interno