

	FORMATO	CÓDIGO:	F-OCI-006
	INFORME DE AUDITORÍA	VERSIÓN:	3
		CLASIFICACIÓN DE LA INFORMACIÓN:	Pública

AUDITORÍA A LOS CONTROLES DE SEGURIDAD INFORMÁTICA DEL SISTEMA DE INFORMACIÓN FONDO ESPECIALIZADO DE INFORMACIÓN DE HIDROCARBUROS – FEIH

1. INFORMACIÓN GENERAL DE LA AUDITORÍA

Tabla 1. Información general

Tipo de informe	Preliminar		Final	X
No. Informe	OCI-32-2026			
Fecha del informe	30 de septiembre de 2026			
Objetivo	Evaluar la implementación, operación y efectividad de los controles de seguridad informática asociados al Sistema de Información Fondo Especializado de Información de Hidrocarburos (FEIH), así como la integridad de las transacciones, la disponibilidad del servicio y la seguridad de las integraciones con otros sistemas institucionales			
Alcance	Revisión de los controles de seguridad informática asociados al FEIH, considerando su operación, administración, soporte, mantenimiento y, cuando aplique, desarrollo o evolución, así como las integraciones y componentes tecnológicos directamente relacionados con el sistema. La verificación consideró las actuaciones y evidencias correspondientes al período comprendido entre el 1 de enero de 2025 y el 31 de julio de 2026, sin perjuicio de consultar antecedentes o documentación previa cuando resultó necesario para comprender el diseño y funcionamiento de los controles. La identificación de sistemas o componentes relacionados, incluido el Banco de Información Petrolera (BIP), no implicó su incorporación automática al alcance y dependió de la relación funcional o técnica determinada con el FEIH.			
Periodo ejecución de	12 de agosto al 25 de septiembre de 2026			
Equipo Auditor	Crhistian Augusto Amador León			
Documentación analizada	- Documentación técnica, funcional y operativa específica del FEIH, incluyendo documentación de arquitectura, infraestructura, componentes, integraciones, operación y administración. - Información disponible en Azure DevOps relacionada con el desarrollo, control de versiones, cambios, pruebas, liberaciones y despliegues del FEIH. - Inventario institucional de sistemas de información e inventario de activos de información relacionados con el FEIH. - Información y evidencias relacionadas con usuarios, roles, perfiles y privilegios del FEIH.			

	FORMATO	CÓDIGO:	F-OCI-006
	INFORME DE AUDITORÍA	VERSIÓN:	3
		CLASIFICACIÓN DE LA INFORMACIÓN:	Pública

	• Información y evidencias relacionadas con copias de respaldo y recuperación, registros de eventos y trazabilidad, incidentes tecnológicos y de seguridad de la información, soporte y disponibilidad del FEIH. • Registros y evidencias provenientes de Mesa de Ayuda – iTop, Harmony Endpoint y OpenNMS, relacionados con los controles objeto de evaluación. • MO-TEC-002 – Políticas de operación específicas de gestión de seguridad de la información. • PR-TEC-GAU-001 – Gestión de Accesos a Usuarios. • PR-GGC-CSI-001 – Gestión de Cambios de Sistemas de Información. • PR-TEC-004 – Gestión de Incidentes Tecnológicos. • PR-TEC-PLA-005 – Gestión de Incidentes de Seguridad de la Información y Datos Personales. • GU-TEC-INF-001 – Guía de Pruebas para Sistemas de Información. • IN-TEC-004 – Gestión de Incidentes, Requerimientos y Aplicaciones Tecnológicas – Aplicativo ITOP (Rol Analista), cuando resultó aplicable. • Procedimientos institucionales aplicables a la gestión de copias de respaldo y recuperación. • PR-TEC-INF-001 vigente durante el período evaluado, en los aspectos aplicables al desarrollo y gestión tecnológica del FEIH. • Respuestas y soportes suministrados por la DGI en atención a las solicitudes de información efectuadas por la OCI durante la ejecución de la auditoría.
--	---

2. DESARROLLO DE LA AUDITORÍA

2.1 Metodología

Mediante memorando No. 2026-130-004835-3 del 12 de agosto de 2026, la Oficina de Control Interno comunicó el inicio de la auditoría a la Dirección de Gestión de Información, remitió el Plan de Auditoría y el Formulario de Identificación y Levantamiento de Información del Sistema de Información Fondo Especializado de Información de Hidrocarburos – FEIH, solicitando su diligenciamiento y la entrega de los respectivos soportes y evidencias a más tardar el 19 de agosto de 2026.

El formulario tuvo como propósito consolidar la información general del FEIH e identificar su modalidad de desarrollo y la documentación específica, técnica, funcional, contractual y operativa disponible, como insumo para la ejecución de la auditoría.

	FORMATO	CÓDIGO:	F-OCI-006
	INFORME DE AUDITORÍA	VERSIÓN:	3
		CLASIFICACIÓN DE LA INFORMACIÓN:	Pública

Mediante radicado No. 2026-720-004972-3 del 19 de agosto de 2026, la Dirección de Gestión de Información remitió respuesta a la solicitud inicial, designó como enlace de la auditoría al Coordinador del Grupo de Sistemas de Información Geocientífica y puso a disposición de la OCI el formulario diligenciado y los soportes técnicos, funcionales, operativos y de gestión relacionados con el FEIH. Frente al acceso requerido para la ejecución de las pruebas, la DGI informó que el FEIH no dispone de un rol específico de auditoría o solo lectura. Adicionalmente, se habilitó al auditor acceso de lectura al proyecto “SGC - FONDO ESPECIALIZADO DE INFORMACIÓN” en Azure DevOps, para la consulta de la documentación e información disponible en dicha plataforma.

Una vez revisada la información inicialmente suministrada y efectuadas las verificaciones disponibles, el 14 de septiembre de 2026 la OCI remitió una solicitud complementaria de información orientada a completar las validaciones pendientes, relacionada con componentes transversales e integraciones, disponibilidad y balanceo, protección de credenciales, roles y privilegios, gestión de usuarios, cambios y liberaciones, copias de respaldo y recuperación, incidentes y disponibilidad del FEIH. La DGI remitió respuesta y soportes complementarios el 16 de septiembre de 2026.

Posteriormente, el 21 de septiembre de 2026, se efectuaron precisiones adicionales relacionadas con los soportes de incidentes asociados al FEIH, las pruebas aleatorias de recuperación y calidad de la información y la definición de permisos o privilegios de los roles del sistema. Como resultado, la DGI remitió información y evidencias complementarias para su incorporación a las pruebas de auditoría. La información suministrada fue complementada con las verificaciones efectuadas por la OCI sobre las fuentes y mecanismos disponibles, incluyendo el FEIH, Azure DevOps, inventarios institucionales, documentación técnica y funcional, información de usuarios, roles y privilegios, registros de respaldo, Mesa de Ayuda – iTop, Harmony Endpoint, OpenNMS y demás soportes asociados a los controles evaluados.

Durante el desarrollo de la auditoría se efectuó la revisión documental, el análisis de la información y de las evidencias suministradas por la Dirección de Gestión de Información (DGI), así como consultas y verificaciones sobre las fuentes de información a las cuales se dispuso de acceso durante la ejecución del ejercicio auditor.

La evaluación se desarrolló mediante pruebas orientadas a verificar los controles asociados a la identificación e inventario del FEIH; arquitectura, infraestructura e integraciones; gestión de accesos, roles y privilegios; desarrollo, gestión de cambios, pruebas y liberaciones; copias de respaldo y recuperación; registros

	FORMATO	CÓDIGO:	F-OCI-006
	INFORME DE AUDITORÍA	VERSIÓN:	3
		CLASIFICACIÓN DE LA INFORMACIÓN:	Pública

de eventos y trazabilidad; gestión de incidentes; y operación, soporte y disponibilidad.

Como insumo inicial se analizó el Formulario de Identificación y Levantamiento de Información del FEIH y los soportes suministrados por la DGI, complementando su revisión con la información disponible en Azure DevOps, los inventarios institucionales y demás evidencias técnicas, funcionales y operativas relacionadas con los controles objeto de evaluación. El formulario mencionado fue diseñado para consolidar la información general del sistema, su modalidad de desarrollo y la documentación específica disponible para la ejecución de la auditoría.

Para los aspectos que requirieron una validación específica se aplicaron pruebas selectivas, entre ellas la revisión de muestras relacionadas con la gestión de accesos de usuarios, liberaciones efectuadas en ambiente de producción, copias de respaldo e incidentes asociados al FEIH. Asimismo, se revisaron registros y reportes provenientes de las herramientas institucionales utilizadas para la gestión y monitoreo de los controles evaluados.

Una vez analizada la información inicialmente suministrada y efectuadas las verificaciones disponibles, la OCI solicitó información complementaria para concluir las pruebas que requerían evidencia adicional, relacionada con componentes transversales, disponibilidad y balanceo, protección de credenciales, roles y privilegios, gestión de usuarios, cambios y liberaciones, copias de respaldo y recuperación, incidentes y disponibilidad del FEIH.

Las respuestas y soportes complementarios recibidos fueron contrastados con la documentación institucional aplicable y con las demás evidencias disponibles, con el fin de determinar el grado de implementación y operación de los controles evaluados durante el período objeto de auditoría.

2.2 Resultados de la Auditoría

Como resultado de las pruebas realizadas y del análisis de la información y evidencias suministradas, a continuación, se presentan los principales resultados obtenidos frente a los controles de seguridad informática evaluados en el FEIH, de acuerdo con los aspectos definidos en el alcance de la auditoría.

2.2.1 Identificación general e inventario del FEIH

El Sistema de Información Fondo Especializado de Información de Hidrocarburos – FEIH se encuentra en producción desde el 21 de octubre de 2024 y

	FORMATO	CÓDIGO:	F-OCI-006
	INFORME DE AUDITORÍA	VERSIÓN:	3
		CLASIFICACIÓN DE LA INFORMACIÓN:	Pública

corresponde a un desarrollo interno de la Entidad, administrado por la Dirección de Gestión de Información (DGI).

Durante la auditoría se verificó su registro en los instrumentos institucionales correspondientes, encontrándose que en el Catálogo de Sistemas de Información se encuentra identificado como SIS-17 y en el inventario de activos de información como ORA0045, registrado como activo crítico y con valoración institucional de confidencialidad, integridad y disponibilidad.

De acuerdo con la información suministrada, se encuentran identificados los responsables asociados a la gestión funcional y técnica del FEIH. Asimismo, se verificó la existencia del proyecto "SGC - FONDO ESPECIALIZADO DE INFORMACIÓN" en Azure DevOps, utilizado para gestionar información relacionada con el desarrollo y evolución del sistema. Durante la auditoría, la DGI habilitó acceso de lectura a dicho proyecto para la consulta de la información disponible.

Con base en las verificaciones efectuadas, se evidenció que el FEIH se encuentra identificado en los instrumentos institucionales consultados y cuenta con responsables definidos para su gestión. Para este aspecto no se identificaron situaciones que requieran la formulación de observaciones o recomendaciones.

2.2.2 Arquitectura, infraestructura e integraciones

Durante la auditoría se revisó la documentación técnica relacionada con la arquitectura e infraestructura del FEIH, evidenciándose la separación de los ambientes de desarrollo, pruebas y producción, así como la identificación de los principales componentes tecnológicos que soportan su funcionamiento.

Respecto de las integraciones, se verificó la información correspondiente a los componentes de Autorización y Exportación de PDF, así como las integraciones con Metabase y Objetos Geográficos. Los soportes revisados permitieron identificar su función dentro de la operación del FEIH y los mecanismos utilizados para su comunicación con otros componentes.

En relación con la infraestructura tecnológica, se evidenció el uso de OpenNMS para el monitoreo de los componentes asociados al FEIH. La información suministrada permitió verificar la existencia de mecanismos de seguimiento sobre su disponibilidad, sin que durante esta prueba se identificaran situaciones que requirieran la formulación de observaciones.

Para la integración con Objetos Geográficos, la DGI informó que las credenciales utilizadas para su funcionamiento se encuentran almacenadas en un archivo de

	FORMATO	CÓDIGO:	F-OCI-006
	INFORME DE AUDITORÍA	VERSIÓN:	3
		CLASIFICACIÓN DE LA INFORMACIÓN:	Pública

configuración denominado config.ini y que actualmente no se utiliza un mecanismo alternativo para su almacenamiento. Como medida de protección, se suministró evidencia de los permisos configurados sobre la carpeta en la cual se encuentra dicho archivo.

Con base en la evidencia revisada, no se identificaron elementos suficientes para generar observaciones frente a este aspecto; no obstante, teniendo en cuenta los lineamientos institucionales orientados a la protección de los activos de información frente a accesos no autorizados y a la aplicación del principio de mínimo privilegio, se considera pertinente fortalecer preventivamente las medidas de protección aplicadas a estas credenciales, para lo cual se formula la recomendación especificada en el numeral 4 del presente informe.

2.2.3 Gestión de accesos, roles y privilegios

Durante la auditoría se revisaron los mecanismos establecidos para la gestión de accesos al FEIH, incluyendo la creación y habilitación de usuarios, la asignación de roles y la definición de los permisos asociados. De acuerdo con la información suministrada por la DGI, el registro y autenticación de usuarios se realiza mediante un componente transversal utilizado por diferentes aplicaciones de la Entidad. Para el acceso específico al FEIH, la DGI informó que los usuarios externos deben estar asociados a una compañía operadora y que su autorización es gestionada por usuarios con rol de Administrador Técnico o Administrador Funcional. Una vez validada la autorización, se habilita el acceso y se asigna el rol correspondiente de acuerdo con las funciones que desempeñará el usuario en la plataforma.

Respecto de la definición de privilegios, se verificó la matriz Módulo-Rol-Permiso, en la cual se encuentran relacionados los roles del FEIH, los módulos disponibles y los permisos asociados para consultar, crear, editar o eliminar información. Esta evidencia permitió identificar los privilegios definidos para los diferentes roles y su relación con las funcionalidades del sistema.

Como prueba selectiva, se revisaron los tres casos más recientes de creación y/o autorización de usuarios externos reportados dentro del período evaluado. Los soportes permitieron verificar el usuario, la fecha de solicitud, el rol Compañía asignado y la fecha de atención o ejecución. No obstante, en la evidencia suministrada no fue posible identificar de manera completa, para cada uno de los casos seleccionados, la trazabilidad de quién realizó la solicitud y quién efectuó la aprobación correspondiente.

Teniendo en cuenta que la DGI tiene establecido un mecanismo de autorización para el acceso de usuarios externos al FEIH, y con el propósito de fortalecer la

	FORMATO	CÓDIGO:	F-OCI-006
	INFORME DE AUDITORÍA	VERSIÓN:	3
		CLASIFICACIÓN DE LA INFORMACIÓN:	Pública

trazabilidad de estas autorizaciones, se formula la recomendación correspondiente mencionada en el numeral 4 del presente informe.

2.2.4 Desarrollo, gestión de cambios, pruebas y liberaciones

El FEIH corresponde a un desarrollo interno de la Entidad cuya gestión de requerimientos, código fuente, cambios, versiones y despliegues se realiza mediante Azure DevOps. Durante la auditoría se verificó la existencia de ambientes diferenciados de desarrollo, pruebas y producción, así como la utilización de esta herramienta para mantener la trazabilidad de los desarrollos y liberaciones efectuadas sobre el sistema.

Como prueba selectiva se revisaron dos liberaciones efectuadas durante el período evaluado: API Release-52, asociada al artefacto 20260729.1 del 29 de julio de 2026, y APP Release-47, asociada al artefacto 20260714.1 del 14 de julio de 2026. En las muestras se evidenció información relacionada con los elementos de trabajo y cambios asociados, los artefactos generados y su posterior implementación en producción. Para la Release-52 se observó, adicionalmente, el registro de un primer intento de implementación con error y una ejecución posterior satisfactoria, conservándose la trazabilidad de ambas ejecuciones en Azure DevOps.

Frente a las pruebas previas al paso a producción, la DGI informó que realiza validaciones funcionales y técnicas y aportó evidencia de una comunicación mediante la cual se informó la finalización satisfactoria de las pruebas y se autorizó continuar con el despliegue; también manifestó que actualmente no cuenta con un formato o conjunto de casos de prueba formalmente documentado y estandarizado en el que se registren de manera detallada los escenarios ejecutados, los resultados obtenidos y el cierre de cada prueba. Se resalta que en los soportes suministrados para las liberaciones evaluadas, no fue posible para la oficina de Control Interno identificar de manera detallada los casos o escenarios de prueba ejecutados y sus respectivos resultados. Al respecto, el procedimiento “PR-TEC-INF-001 – Implementación Sistemas de Información”, versión 7, contempla la realización de pruebas funcionales y no funcionales, el seguimiento a sus resultados y la conservación del soporte correspondiente; a su vez, la guía “GU-TEC-INF-001 – Pruebas para Sistemas de Información”, versión 3, establece el registro de los escenarios y casos de prueba, su ejecución, resultados, cierre y aprobación.

En relación con la gestión de cambios, se evidenció que Azure DevOps permite conservar trazabilidad técnica de los desarrollos y despliegues del FEIH. La DGI informó que los cambios, ajustes, correcciones y nuevas funcionalidades del

	FORMATO	CÓDIGO:	F-OCI-006
	INFORME DE AUDITORÍA	VERSIÓN:	3
		CLASIFICACIÓN DE LA INFORMACIÓN:	Pública

sistema se gestionan directamente mediante esta herramienta y no mediante el formato Requerimiento de Cambios de Tecnologías de Información – F-TEC-021 (código anterior F-GGC-CSI-001, referenciado en el procedimiento vigente). Al respecto, el procedimiento *PR-GGC-CSI-001* – Gestión de Cambios de Sistemas de Información establece tratamientos diferenciados para la gestión de cambios y, en su numeral 5.7.4, contempla que, cuando se trate de proyectos, los cambios pueden documentarse como parte del proyecto y no necesariamente requieren la gestión de un RFC (Requerimiento de Cambio) hasta la finalización de la etapa de estabilización. Con la evidencia suministrada no fue posible establecer si las liberaciones evaluadas se encontraban cobijadas por esta condición o correspondían a cambios posteriores a dicha etapa.

En consecuencia, aunque se evidenciaron mecanismos para la gestión técnica, trazabilidad y despliegue de los desarrollos del FEIH, se identificó una No Conformidad relacionada con el registro y trazabilidad de las pruebas, la cual se presenta en el numeral 3 del presente informe. Adicionalmente, frente a la gestión de cambios, se identificó un aspecto susceptible de fortalecimiento, para el cual se formula la recomendación correspondiente en el numeral 4 de este informe.

2.2.5 Copias de respaldo y recuperación

Durante la auditoría se revisó el esquema de copias de respaldo establecido para la base de datos de producción del FEIH, identificada como DB_FEIH_PROD. De acuerdo con la información suministrada, esta cuenta con respaldos completos (FULL), diferenciales (DIFF) y del registro de transacciones (LOG), almacenados en la ruta definida para las copias de seguridad de la base de datos.

Para verificar la operación del esquema informado, se revisó una muestra correspondiente a julio de 2026. La evidencia suministrada permitió identificar la ejecución de respaldos FULL con periodicidad semanal, respaldos diferenciales durante los demás días de la semana y respaldos del registro de transacciones durante el período evaluado, así como su almacenamiento en la ruta definida para DB_FEIH_PROD. En forma adicional, se verificó lo relacionado con las pruebas de recuperación y calidad de la información; se encontró que el procedimiento *PR-GGC-AMR-001- Gestión de Almacenamiento Masivo y Respaldo de la Información Institucional*, establece que el responsable de las copias de seguridad, junto con el líder de seguridad, debe realizar trimestralmente estas pruebas de manera aleatoria y conservar el registro correspondiente. Frente a este aspecto, la DGI informó que DB_FEIH_PROD no fue seleccionada dentro de las muestras aleatorias ejecutadas durante el período comprendido entre el 1 de enero de 2025 y el 31 de julio de 2026. Teniendo en cuenta que el procedimiento institucional establece que la selección para las

	FORMATO	CÓDIGO:	F-OCI-006
	INFORME DE AUDITORÍA	VERSIÓN:	3
		CLASIFICACIÓN DE LA INFORMACIÓN:	Pública

pruebas de recuperación y calidad se realiza de manera aleatoria, la ausencia de DB_FEIH_PROD dentro de las muestras efectuadas durante el período evaluado no constituye, por sí misma, un incumplimiento del procedimiento.

Con base en las verificaciones realizadas, se evidenció la operación del esquema de copias de respaldo informado para DB_FEIH_PROD. No obstante, teniendo en cuenta que durante el período evaluado esta base de datos no fue objeto de pruebas de recuperación y calidad, se considera pertinente formular una recomendación orientada a fortalecer la validación de su capacidad de recuperación.

2.2.6 Registros de eventos y trazabilidad

Durante la auditoría se verificaron los mecanismos disponibles en el FEIH para el registro y trazabilidad de las operaciones realizadas por los usuarios, con el propósito de establecer si el sistema conserva información que permita identificar las acciones efectuadas y asociarlas con los usuarios que las ejecutan.

A partir de las verificaciones realizadas sobre los registros disponibles, se evidenció que el FEIH conserva información relacionada con las operaciones efectuadas en el sistema, incluyendo la identificación del usuario asociado a la actividad registrada. Estos registros permiten mantener trazabilidad sobre las acciones ejecutadas en las funcionalidades verificadas.

Como parte de las pruebas efectuadas, se consultaron registros correspondientes a operaciones realizadas en el FEIH, evidenciándose información que permite relacionar las actividades ejecutadas con el usuario correspondiente y efectuar su consulta posterior.

De acuerdo con la evidencia revisada, se identificó que el FEIH dispone de mecanismos de registro que permiten mantener trazabilidad sobre las operaciones verificadas y apoyar el seguimiento de las actividades realizadas por los usuarios.

Con base en las verificaciones efectuadas, no se identificaron situaciones que requieran la formulación de observaciones o recomendaciones para el tema evaluado.

2.2.7 Gestión de incidentes

Durante la auditoría se revisó la información relacionada con la gestión de incidentes asociados al FEIH, considerando los registros disponibles en la Mesa

	FORMATO	CÓDIGO:	F-OCI-006
	INFORME DE AUDITORÍA	VERSIÓN:	3
		CLASIFICACIÓN DE LA INFORMACIÓN:	Pública

de Ayuda y la información suministrada por la DGI frente a eventos de seguridad relacionados con el sistema.

En la revisión de los registros de la Mesa de Ayuda se identificaron casos asociados a la operación y soporte del FEIH, relacionados, entre otros aspectos, con solicitudes de restablecimiento de contraseñas, credenciales y actividades de soporte tecnológico. Estos registros evidencian la utilización del mecanismo institucional dispuesto para la atención y seguimiento de este tipo de situaciones.

Adicionalmente, frente a posibles incidentes de seguridad de la información, la DGI informó que realizó la validación correspondiente y que no se identificaron incidentes de seguridad asociados al FEIH durante el período evaluado. Asimismo, se efectuaron verificaciones sobre los registros disponibles en la herramienta de seguridad de los servidores, sin identificarse eventos que hubieran sido clasificados como incidentes de seguridad relacionados con el sistema.

De acuerdo con las verificaciones realizadas, se evidenció la existencia de mecanismos para el registro y atención de incidentes tecnológicos relacionados con el FEIH y no se identificaron situaciones que requieran la formulación de observaciones o recomendaciones para este aspecto.

2.2.8 Operación, soporte y disponibilidad

Durante la auditoría se revisaron los mecanismos utilizados para el seguimiento de la operación, soporte y disponibilidad del FEIH, incluyendo la información suministrada por la DGI y los registros disponibles en las herramientas institucionales de monitoreo y soporte.

Frente al monitoreo de la infraestructura tecnológica, se evidenció el uso de OpenNMS para efectuar seguimiento a componentes asociados al FEIH, incluyendo servidores, aplicación, base de datos y servicios relacionados. De acuerdo con la información suministrada por la DGI, este monitoreo permite identificar eventos de indisponibilidad y realizar seguimiento a la operación de los componentes tecnológicos del sistema.

Como parte de las pruebas realizadas, se revisó el reporte de disponibilidad de los componentes monitoreados, en el cual se observaron porcentajes de disponibilidad superiores al 99,99 % para el período reportado. Asimismo, se verificaron registros asociados a la atención de requerimientos y situaciones operativas del FEIH mediante la Mesa de Ayuda, como mecanismo institucional para su gestión y seguimiento.

	FORMATO	CÓDIGO:	F-OCI-006
	INFORME DE AUDITORÍA	VERSIÓN:	3
		CLASIFICACIÓN DE LA INFORMACIÓN:	Pública

De acuerdo con la información revisada, no se identificaron eventos que evidenciaran una afectación permanente de la operación del FEIH durante el período evaluado. No obstante, los porcentajes de disponibilidad corresponden a los componentes tecnológicos monitoreados y, por tanto, no se interpretaron como una medición directa de la disponibilidad funcional del sistema para el usuario final.

Con base en las verificaciones efectuadas, se evidenciaron mecanismos para el monitoreo y soporte de la operación del FEIH y no se identificaron situaciones que requieran la formulación de observaciones o recomendaciones para este aspecto.

3. ANÁLISIS DE LAS OBSERVACIONES PRESENTADAS AL INFORME PRELIMINAR

Mediante memorando No. 2026-130-005676-3, la Oficina de Control Interno remitió a la Dirección de Gestión de Información el Informe Preliminar de la Auditoría a los Controles de Seguridad Informática del Sistema de Información Fondo Especializado de Información de Hidrocarburos – FEIH, para su conocimiento y presentación de las observaciones que considerara pertinentes.

Mediante memorando con radicado No. 2026-700-005830-3 del 28 de septiembre de 2026, la Dirección de Gestión de Información remitió los comentarios y observaciones recopilados por el equipo de desarrollo del Grupo de Sistemas de Información Geocientífica, los cuales fueron analizados por la Oficina de Control Interno para determinar su incidencia sobre los resultados presentados en el Informe Preliminar.

Una vez efectuado el análisis, se evidenció que la DGI manifestó la aceptación de las recomendaciones relacionadas con la protección de las credenciales utilizadas por la integración con Objetos Geográficos, la trazabilidad de los accesos de usuarios externos, el registro de las pruebas, la articulación de la gestión de cambios y la inclusión de la base de datos DB_FEIH_PROD en futuras muestras de pruebas de recuperación. Frente a la No Conformidad relacionada con el registro y trazabilidad de las pruebas y a la recomendación sobre mecanismos de redundancia o continuidad, la DGI solicitó reconsiderar los resultados presentados, aspectos que se analizan a continuación:

- **Observación No. 1.** No Conformidad relacionada con el registro y trazabilidad de las pruebas.
La Dirección de Gestión de Información indicó: *“Solicitamos respetuosamente que este hallazgo sea reclasificado como una*

	FORMATO	CÓDIGO:	F-OCI-006
	INFORME DE AUDITORÍA	VERSIÓN:	3
		CLASIFICACIÓN DE LA INFORMACIÓN:	Pública

recomendación orientada a continuar y fortalecer las prácticas dentro de la plataforma Azure DevOps. Durante el periodo evaluado, las actividades de estabilización del sistema en producción se ejecutaron con extrema premura debido a la urgencia derivada de la operación sin descuidar los procesos de pruebas y aceptación por el correo institucional. La gestión del ciclo de vida de la aplicación está enmarcada en la metodología (plantilla de pruebas) y en la herramienta Azure DevOps y actualmente contamos con un procedimiento actualizado y un instructivo codificado que se alinea completamente con las buenas prácticas. Por lo tanto, la DGI asume el compromiso de estructurar un plan de mejoramiento enfocado en la documentación futura dentro de esta herramienta, justificando la trazabilidad de las pruebas directamente en los flujos de Azure DevOps, haciendo innecesaria la tipificación de este evento como una No Conformidad.

Adicionalmente, como acción de mejora sobre la información relacionada con la documentación institucional PR-TEC-INF-001 disponible en el SIGI, al respecto, se precisa que, a la fecha, el Grupo de Sistemas de Información Geocientífica, con el acompañamiento del Grupo de Planeación, se encuentra próximo a finalizar el proceso de actualización documental del procedimiento PR-TEC-INF-001, el cual pasará a denominarse "Gestión tecnológica del ciclo de vida de aplicaciones y sistemas de información". Como evidencia del avance de este proceso como respuesta al inicio de la auditoría se dispuso la carpeta que contiene el correo electrónico asociado a la actualización documental, así como la versión del procedimiento objeto de actualización. Una vez culminado el proceso de revisión y aprobación correspondiente, la actualización será incorporada al Sistema Integrado de Gestión Institucional – SIGI, de acuerdo con el procedimiento institucional establecido (planteada para antes del 31 de octubre del año en curso).

Asimismo, se remite URL de PDF publicado recientemente (posterior al inicio de la presente auditoría) en el SIGI sobre el instructivo de Elaboración de pruebas en el DevOps, Código: IN-TEC-005 que a la fecha mejora el mecanismo de elaboración y evidencia de pruebas en el desarrollo de sistemas y aplicaciones, teniendo en cuenta que las mismas se ejecutan y reportan en el DevOps".

Análisis de la Oficina de Control Interno: La Oficina de Control Interno reconoce las precisiones presentadas por la Dirección de Gestión de Información, así como las gestiones adelantadas para fortalecer la documentación institucional y la trazabilidad de las pruebas de los sistemas de información mediante Azure DevOps. De igual manera, se reconoce que la actualización de los instrumentos relacionados con esta actividad, venía

	FORMATO	CÓDIGO:	F-OCI-006
	INFORME DE AUDITORÍA	VERSIÓN:	3
		CLASIFICACIÓN DE LA INFORMACIÓN:	Pública

siendo gestionada por la DGI con anterioridad al desarrollo de la presente auditoría.

Se precisa que la situación identificada durante la auditoría no estuvo relacionada con la ausencia de pruebas previas al paso a producción, pues para las liberaciones evaluadas se evidenció la realización de validaciones funcionales y técnicas y se contó con una comunicación mediante la cual se informó la conformidad con los resultados y se autorizó continuar con el despliegue. No obstante, ante la solicitud específica de la OCI de remitir para las liberaciones seleccionadas los casos o escenarios ejecutados, sus resultados y la evidencia de cierre o aprobación, la DGI manifestó que *“actualmente, no se cuenta con un formato o conjunto de casos de prueba formalmente documentado y estandarizado en el que se registren de manera detallada los escenarios ejecutados, los resultados obtenidos y el cierre de cada prueba”*.

Asimismo, de los soportes suministrados durante la auditoría se evidenció la trazabilidad de los elementos de trabajo, cambios, artefactos y liberaciones gestionados mediante Azure DevOps, así como la comunicación de conformidad antes mencionada; sin embargo, para las liberaciones seleccionadas no fue posible identificar de manera detallada los casos o escenarios de prueba ejecutados y sus respectivos resultados, elementos requeridos por los lineamientos institucionales aplicables durante el período evaluado.

Frente a los soportes remitidos con las observaciones al Informe Preliminar, la OCI evidenció las gestiones adelantadas para la actualización del procedimiento *PR-TEC-INF-001* y la expedición del instructivo *IN-TEC-005 – Elaboración de pruebas* en Azure DevOps, este último publicado en el SIGI con posterioridad al período objeto de evaluación, cuyo corte correspondió al 31 de julio de 2026. Estos instrumentos fortalecen la definición y trazabilidad de las pruebas mediante Azure DevOps; no obstante, su actualización y expedición no modifican la situación evidenciada para las liberaciones objeto de la muestra ni los criterios institucionales que resultaban aplicables durante el período auditado.

En este sentido, la OCI a pesar de valorar las actuaciones adelantadas por la DGI para fortalecer la gestión y documentación de las pruebas, las cuales guardan relación con el aspecto identificado durante la auditoría, se mantiene la No Conformidad relacionada con el registro y trazabilidad de las pruebas en este informe final.

- **Observación No. 2. Recomendación relacionada con mecanismos de redundancia o continuidad**

	FORMATO	CÓDIGO:	F-OCI-006
	INFORME DE AUDITORÍA	VERSIÓN:	3
		CLASIFICACIÓN DE LA INFORMACIÓN:	Pública

La Dirección de Gestión de Información manifestó: *“Nos permitimos objetar esta recomendación y solicitamos respetuosamente desestimar esta recomendación, dado que la implementación de componentes de redundancia tecnológica, como un balanceador de carga, genera costos elevados que no son necesarios ni proporcionales a las características operativas del sistema. Como se informó, el FEIH es una plataforma de acceso restringido, solo para actores específicos, y no requiere una infraestructura de concurrencia masiva. Las estadísticas de tráfico y los monitoreos de OpenNMS demuestran un funcionamiento óptimo (una disponibilidad del 100% sin caídas durante 576 días y un 99.998% global), evidenciando que la arquitectura actual posee la estabilidad requerida para soportar la operación sin necesidad de incurrir en inversiones adicionales”.*

Análisis de la Oficina de Control Interno: La Oficina de Control Interno analizó las consideraciones presentadas por la Dirección de Gestión de Información frente a las características de operación del FEIH y la conveniencia de implementar mecanismos adicionales de redundancia tecnológica.

Al respecto, durante la auditoría se evidenció la existencia de mecanismos para el monitoreo y soporte de la operación del FEIH, así como porcentajes de disponibilidad superiores al 99,99 % en los componentes tecnológicos monitoreados. De igual manera, durante el período evaluado no se identificaron eventos que evidenciaran una afectación permanente de la operación del sistema. Teniendo en cuenta que la recomendación incluida en el Informe Preliminar fue formulada con carácter preventivo y no se derivó de un incumplimiento o de una afectación evidenciada en la disponibilidad del FEIH durante el período evaluado, y considerando las precisiones efectuadas por la DGI respecto de las características operativas y necesidades actuales del sistema, la Oficina de Control Interno considera procedente acoger la observación presentada por la DGI. En consecuencia, se retira del informe final la recomendación relacionada con la evaluación de mecanismos adicionales de redundancia o continuidad de los componentes tecnológicos del FEIH.

4. SOLICITUD DE CORRECCIONES O ACCIONES CORRECTIVAS

A continuación, se presenta una No Conformidad establecida en esta auditoría, con el objeto de que sean implementada la respectiva corrección o acción correctiva, según el procedimiento vigente (PR-PSG-ADM-001 Planes de Mejoramiento Continuo):

	FORMATO	CÓDIGO:	F-OCI-006
	INFORME DE AUDITORÍA	VERSIÓN:	3
		CLASIFICACIÓN DE LA INFORMACIÓN:	Pública

Tabla 2 – No conformidades

No.	PROCESO	DESCRIPCIÓN DE LA NO CONFORMIDAD	CRITERIO QUE INCUMPLIÓ
1	Gestión de Tecnologías de la Información y las Comunicaciones Grupo de Trabajo Servicios y Divulgación de Información Geocientífica y Museal de la Dirección de Gestión de Información Grupo de Trabajo Sistemas de Información Geocientífica	En las liberaciones evaluadas se evidenció que la DGI realiza pruebas funcionales y técnicas previamente al paso a producción; sin embargo, la dependencia informó que actualmente no cuenta con un formato o conjunto de casos de prueba formalmente documentado y estandarizado en el que se registren de manera detallada los escenarios ejecutados, los resultados obtenidos y el cierre de cada prueba. Asimismo, de los soportes suministrados para las liberaciones evaluadas no fue posible identificar de manera detallada los casos o escenarios de prueba ejecutados y sus respectivos resultados.	<u>PR-TEC-INF-001- Implementación Sistemas de Información, versión 7, actividad 14</u>: “Realice pruebas, funcionales y no funcionales”. El procedimiento también establece que el Supervisor debe realizar seguimiento a los resultados y señala como registro el “<i>Soporte de los resultados de las pruebas</i>”. GU-TEC-INF-001 – Pruebas para Sistemas de Información, versión 3: establece que el diseño de pruebas comprende la definición de los casos de prueba con su resultado esperado y su registro en la herramienta estándar de la Entidad; asimismo, establece la ejecución y registro de los resultados y el cierre de las pruebas con su correspondiente aprobación.

5. RECOMENDACIONES

Tabla 3 - Recomendaciones por proceso

No.	PROCESO	RECOMENDACIÓN
1	Gestión de Tecnologías de la Información y las Comunicaciones Grupo de Trabajo Servicios y Divulgación de Información Geocientífica y Museal de la Dirección de Gestión de Información Grupo de Trabajo Sistemas de Información Geocientífica	Evaluar el fortalecimiento de las medidas de protección aplicadas a las credenciales utilizadas por la integración del FEIH con Objetos Geográficos, de manera que se garantice su acceso únicamente por los usuarios o componentes autorizados, de acuerdo con los lineamientos institucionales de seguridad de la información.

	FORMATO	CÓDIGO:	F-OCI-006
	INFORME DE AUDITORÍA	VERSIÓN:	3
		CLASIFICACIÓN DE LA INFORMACIÓN:	Pública

No.	PROCESO	RECOMENDACIÓN
2	Gestión de Tecnologías de la Información y las Comunicaciones Grupo de Trabajo Servicios y Divulgación de Información Geocientífica y Museal de la Dirección de Gestión de Información Grupo de Trabajo Sistemas de Información Geocientífica	Fortalecer la trazabilidad de la gestión de accesos de los usuarios externos del FEIH, procurando que para cada autorización se conserve evidencia que permita identificar la solicitud, la aprobación correspondiente, el rol asignado y la ejecución del acceso.
3	Gestión de Tecnologías de la Información y las Comunicaciones Grupo de Trabajo Servicios y Divulgación de Información Geocientífica y Museal de la Dirección de Gestión de Información Grupo de Trabajo Sistemas de Información Geocientífica	Fortalecer el registro de las pruebas realizadas a los desarrollos y cambios del FEIH, de manera que en la herramienta definida se conserve la trazabilidad de los escenarios o casos ejecutados, los resultados obtenidos, las incidencias identificadas cuando corresponda y su cierre y aprobación, de acuerdo con los lineamientos institucionales aplicables.
4	Gestión de Tecnologías de la Información y las Comunicaciones Grupo de Trabajo Servicios y Divulgación de Información Geocientífica y Museal de la Dirección de Gestión de Información Grupo de Trabajo Sistemas de Información Geocientífica	Fortalecer la articulación de la gestión de cambios del FEIH realizada mediante Azure DevOps con el procedimiento institucional vigente, de manera que se encuentre claramente identificada la condición bajo la cual se gestionan los cambios y, cuando corresponda, su clasificación y tratamiento como cambios estándar, normales o de emergencia, conservando la evidencia respectiva.

	FORMATO	CÓDIGO:	F-OCI-006
	INFORME DE AUDITORÍA	VERSIÓN:	3
		CLASIFICACIÓN DE LA INFORMACIÓN:	Pública

No.	PROCESO	RECOMENDACIÓN
5	Gestión de Tecnologías de la Información y las Comunicaciones Grupo de Trabajo Servicios y Divulgación de Información Geocientífica y Museal de la Dirección de Gestión de Información Grupo de Trabajo Sistemas de Información Geocientífica	Considerar la inclusión de la base de datos DB_FEIH_PROD dentro de futuras muestras de las pruebas de recuperación y calidad de la información, con el fin de validar su capacidad de restauración y conservar evidencia de los resultados obtenidos.

6. FORTALEZAS

- Trazabilidad del desarrollo y las liberaciones. Se evidenció el uso de Azure DevOps para la gestión técnica del desarrollo y evolución del FEIH, permitiendo mantener trazabilidad entre elementos de trabajo, cambios asociados, artefactos, versiones, liberaciones y despliegues efectuados sobre el sistema.
- Separación de ambientes tecnológicos. Se evidenció la disposición de ambientes diferenciados de desarrollo, pruebas y producción, lo cual contribuye a separar las actividades de construcción y validación de aquellas realizadas sobre el ambiente productivo.
- Monitoreo de los componentes tecnológicos. Se evidenció el uso de OpenNMS para el seguimiento de componentes asociados al FEIH, incluyendo servidores, aplicación, base de datos y servicios relacionados, como mecanismo para identificar eventos de indisponibilidad y apoyar el seguimiento de la operación.
- Esquema de copias de respaldo. Se evidenció la operación de un esquema de respaldo para la base de datos de producción DB_FEIH_PROD, mediante copias completas, diferenciales y del registro de transacciones, cuya ejecución fue verificada selectivamente durante la auditoría.

7. CONCLUSIONES.

- Con base en las pruebas realizadas y en la información y evidencias suministradas, se evidenció que el FEIH cuenta con controles y mecanismos para soportar su operación, administración y seguridad, entre los que se encuentran la separación de ambientes de desarrollo, pruebas y producción, la trazabilidad técnica de los desarrollos y liberaciones mediante Azure

	FORMATO	CÓDIGO:	F-OCI-006
	INFORME DE AUDITORÍA	VERSIÓN:	3
		CLASIFICACIÓN DE LA INFORMACIÓN:	Pública

DevOps, el monitoreo de componentes tecnológicos, la ejecución de copias de respaldo y el registro de operaciones realizadas por los usuarios.

- En relación con el desarrollo y evolución del sistema, se evidenció que Azure DevOps permite mantener trazabilidad sobre elementos de trabajo, cambios, artefactos, liberaciones y despliegues efectuados en producción. No obstante, se identificó una No Conformidad relacionada con el registro y trazabilidad de las pruebas, toda vez que, aunque se realizan pruebas funcionales y técnicas antes del paso a producción, para las liberaciones evaluadas no fue posible identificar de manera detallada los casos o escenarios de prueba ejecutados y sus respectivos resultados, de acuerdo con los lineamientos institucionales aplicables durante el período evaluado.
- Frente a la gestión de cambios, se evidenció la utilización de Azure DevOps como mecanismo para documentar técnicamente los desarrollos y liberaciones del FEIH. Sin embargo, se identificó la necesidad de fortalecer su articulación con el procedimiento institucional de gestión de cambios, particularmente en cuanto a la identificación de la condición bajo la cual se gestionan los cambios y, cuando corresponda, su clasificación y tratamiento de acuerdo con dicho procedimiento.
- En los demás aspectos evaluados, relacionados con la identificación e inventario del sistema, arquitectura, infraestructura e integraciones, gestión de accesos, roles y privilegios, copias de respaldo y recuperación, registros de eventos y trazabilidad, gestión de incidentes, y operación, soporte y disponibilidad, no se identificaron situaciones que dieran lugar a No Conformidades. No obstante, se formularon recomendaciones de carácter preventivo y de fortalecimiento frente a algunos de los controles evaluados.
- En términos generales, los resultados obtenidos evidencian la implementación de controles tecnológicos para soportar la operación del FEIH. No obstante, se identificó la necesidad de fortalecer el registro y trazabilidad de las pruebas, así como otros aspectos de carácter preventivo señalados en las recomendaciones del presente informe.

8. APROBACIÓN

 Erika Marcela Huari Mateus	 Crhistian Augusto Amador León
Jefe de Oficina de Control Interno	Auditor Interno trabajo