INFORME DE AUDITORÍA INTERNA No.:1

FECHA DE EMISIÓN DEL INFORME	**Día:**	04	**Mes:**	04	**Año:**	2025

1. PROCESO:	Gestión de Infraestructura y Tecnologías de Información.
2. LÍDER DE PROCESO / JEFE(S) DEPENDENCIA(S):	Líder Estratégico: Director de Tecnología de la Información y las Comunicaciones. 1. Coordinador Grupo de Innovación, Desarrollo y Arquitectura de Aplicaciones, 2. Coordinador Grupo de Sistemas y Arquitectura de Tecnología 3. Coordinador Grupo Arquitectura de Datos 4. Coordinador Grupo de Proyectos de Tecnología 5. Coordinador del Grupo de Seguridad e Informática Forense.
3. OBJETIVO DE LA AUDITORÍA:	Verificar y evaluar de manera integral la gestión del proceso conforme a la normatividad legal vigente y lo establecido en los procedimientos internos aplicables en el marco del Sistema de Gestión Integrado, así como, el estado de los requisitos de la norma NTC ISO 27001:2022, con el fin de obtener información que permita identificar oportunidades de mejora para el proceso, el Sistema de Gestión Integrado, el Sistema de Control Interno y la Gestión Institucional.
4. ALCANCE DE LA AUDITORÍA:	Se realizó auditoría integral a la gestión del proceso, mediante prueba selectiva o muestreo de las actividades desarrolladas durante el periodo comprendido entre el 05 de julio de 2023 y el 21 de marzo de 2025, fecha de cierre del trabajo de campo de esta auditoría. Para su desarrollo se aplicó el Modelo Integrado de Planeación y Gestión- MIPG, la Guía de Auditoria para Entidades Públicas, y las directrices para la auditoría de los Sistemas de

	Gestión, contenidas en la Guía Técnica Colombiana ISO 19011:2018 y en la norma NTC ISO 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Así como, las directrices establecidas por el Ministerio de Tecnologías de la Información y las Comunicaciones y la documentación aplicable, en el marco del Sistema de Gestión Integrado. Fue necesario incorporar hechos que estuvieran por fuera del periodo de tiempo definido en el alcance de la auditoria.
5. CRITERIOS DE LA AUDITORÍA:	En desarrollo de esta auditoría se evaluaron y verificaron los siguientes aspectos: 1. El estado de la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI en la Entidad. 2. La gestión del contrato del gestor documental GEDESS, en sus etapas precontractual y contractual. 3. El estado de la implementación de la Norma Técnica Colombiana NTC 5854 Accesibilidad a Páginas WEB, que establece los requisitos de accesibilidad que son aplicables a la página Web de la Entidad. 4. Los requisitos de la Norma Técnica Colombiana Seguridad de la Información NTC ISO 27001:2022 4. CONTEXTO DE LA ORGANIZACIÓN. 4.1 Comprensión de la Organización y de su Contexto 4.2 Comprensión de las Necesidades y Expectativas de las Partes Interesadas (4.2.a.b.c) Nuevo requisito 4.3 Determinación del Alcance del Sistema de Gestión de Seguridad de la Información 4.4 Sistema de Gestión de Seguridad de la Información - Nuevo requisito 5. LIDERAZGO.

	5.1 Liderazgo y Compromiso 5.2 Política 5.3 Roles, Responsabilidades y Autoridades en la Organización - Nuevo requisito 6. PLANIFICACIÓN. 6.1 Acciones para abordar los riesgos y las oportunidades 6.2. Objetivos de seguridad de la información y planificación para alcanzarlos - Nuevo requisito 6.3 Planificación de los cambios - Nuevo requisito 7. APOYO. 7.1 Recursos 7.3 Toma de conciencia 7.4 Comunicación 7.5 Control de la documentación 8. OPERACIÓN. 8.1 Planificación y control de la operación 8.2 Evaluación de los riesgos para la Seguridad de la Información 8.3 Tratamiento de los Riesgos de la Seguridad de la Información 9. EVALUACIÓN DEL DESEMPEÑO. 9.1 Seguimiento, medición, análisis y evaluación 9.3 Revisión por la Dirección 10. MEJORA. 10.2 No Conformidades Y Acciones Correctivas. Así como, de los Controles del Anexo. 5. CONTROLES ORGANIZACIONALES. A.5.1 Políticas de seguridad de la información A.5.7 Inteligencia sobre amenazas. Nuevo requisito A.5.8 Seguridad de la información en la gestión de proyectos A.5.9 Inventario de información y otros activos asociados

	A.5.10 Uso aceptable de la información y otros activos asociados A.5.14 Transferencia de información A.5.15 Control de acceso A.5.20 Abordar la seguridad de la información en los acuerdos con los proveedores A.5.23 Seguridad de la información para el uso de servicios en la nube. Nuevo requisito Nuevo requisito. A.5.27 Aprender de los incidentes de seguridad de la información. A.5.29 Seguridad de la información durante la interrupción A.5.30 Preparación de las TIC para la continuidad de la actividad. Nuevo requisito 6. CONTROLES DE PERSONAS. A.6.6 Acuerdos de confidencialidad o no divulgación 7. CONTROLES FÍSICOS. A.7.4 Vigilancia de la seguridad física. Nuevo requisito A.7.9 Seguridad de los activos fuera de las instalaciones A.7.10 Medios de almacenamiento 8. CONTROLES TECNOLÓGICOS. A.8.1 Dispositivos de punto final de usuario A.8.4 Acceso al código fuente A.8.9 Gestión de la configuración. Nuevo requisito A.8.10 Borrado de información. Nuevo requisito A.8.11 Enmascaramiento de datos. Nuevo requisito A.8.12 Prevención de fugas de datos. Nuevo requisito A.8.13 Copia de seguridad de la información A.8.16 Actividades de seguimiento. Nuevo requisito A.8.23 Filtrado Web. Nuevo requisito A.8.24 Uso de la criptografía

	A.8.28 Codificación segura. Nuevo requisito A.8.29 Pruebas de seguridad en el desarrollo y la aceptación A.8.30 Desarrollo contratado externamente A.8.32 Gestión del cambio. 5. Se evaluó la conformidad de los requisitos: 7.3, 9.1, 10.1 y 10.3 de la Norma Técnica Colombiana de Calidad NTC ISO 9001:2015. 6. Se evaluó la conformidad de los requisitos: 7.3, 8.1 y 10.3., de la Norma Técnica Colombiana Ambiental NTC ISO 14001:2015.

Reunión de Apertura						**Ejecución de la Auditoría**				**Reunión de Cierre**					
Día	17	**Mes**	02	**Año**	2025	**Desde:**	10/02/2025 D / M / A	**Hasta:**	21/03/2025 D / M / A	Día	04	Mes	04	Año	2025

6. HALLAZGOS DE LA AUDITORÍA

6.1 ASPECTOS FUERTES DEL PROCESO:

No se identificaron aspectos fuertes.

6.2 OBSERVACIONES

En desarrollo de la auditoría el equipo auditor observó que:

Fortalecimiento del PETI para la Modernización Tecnológica.

1. El Plan Estratégico de Tecnologías de la Información (PETI) debe fortalecer su enfoque en la modernización de la infraestructura tecnológica de la Superintendencia de Sociedades, de la siguiente manera:

6.2 OBSERVACIONES

- Adquirir y actualizar el hardware esencial como switches core y de borde, servidores robustos, sistemas avanzados de control de acceso y la implementación de tecnología RFID (Radio Frequency Identification) para optimizar procesos.
- Estructurar proyectos estratégicos para la implementación de una ciberseguridad digital que proteja integralmente los activos de la entidad.
- Optimizar y hacer sostenible las aplicaciones integrales existentes.
- Desarrollar una plataforma tecnológica integral que permee todas las áreas de la Superintendencia.
- Considerar la incorporación estratégica de los más de 58 contratistas profesionales en diversas disciplinas especializadas, como analistas BI, desarrolladores Front End, especialistas en ciberseguridad y desarrolladores de fábrica de software, a través de estrategias que garanticen una efectiva transferencia de conocimiento y la sostenibilidad a largo plazo de los proyectos tecnológicos, superando la temporalidad de sus contratos.

Recursos de seguridad.

2. No existe continuidad en el contrato del Oficial de Seguridad de la Información, dado que la Entidad estuvo 2 meses sin Oficial, lo que afecta la mejora continua del proceso del Sistema de Gestión de Seguridad de la Información y la actualización a la Norma NTC ISO 27001:2022.

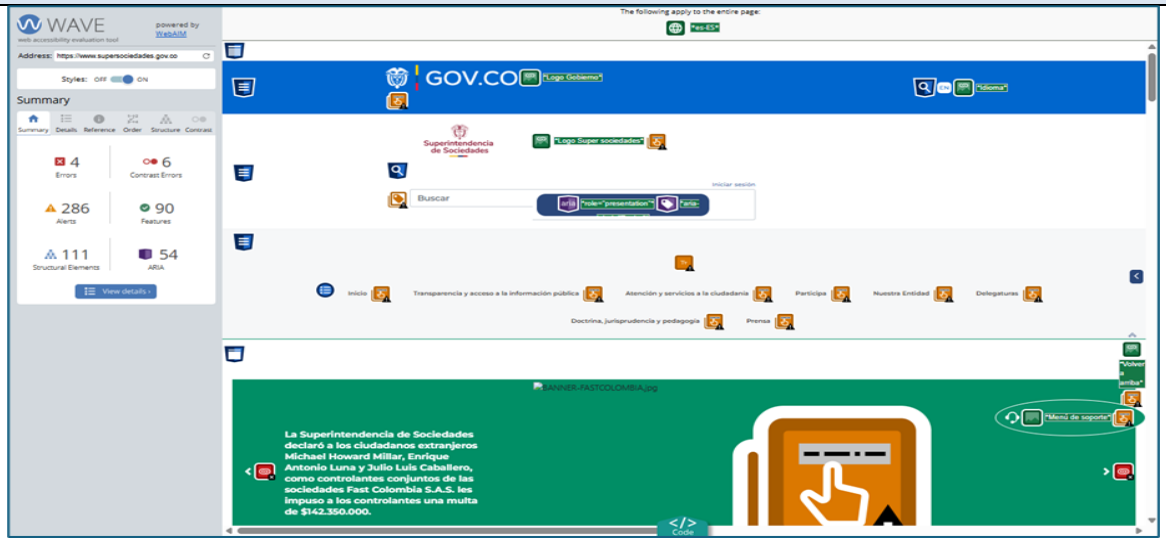
Actividades de Seguimiento.

3. Se observó que, aunque la Entidad dispone de herramientas para identificar situaciones anómalas, estas no se revisan de manera continua, sino solo durante el horario hábil. Esto podría retrasar la reacción frente a eventos de seguridad fuera de dicho horario, limitando la capacidad de respuesta rápida ante incidentes de seguridad.

Norma Técnica Colombiana NTC 5854 Accesibilidad a Páginas WEB.

4. Al verificar si la página de SuperSociedades está aplicando correctamente los principios y pautas de accesibilidad WCAG 2.1 en su página web, se utilizó el programa validador Web Accessibillity Evaluation Tool WAVE, con el fin de confirmar si la página cumple con los requisitos mínimos de accesibilidad, mostrando los siguientes resultados: Se observa un resumen de los hallazgos identificados en la página web de la Entidad: 4 errores, 6 errores de contraste y 286 alertas.

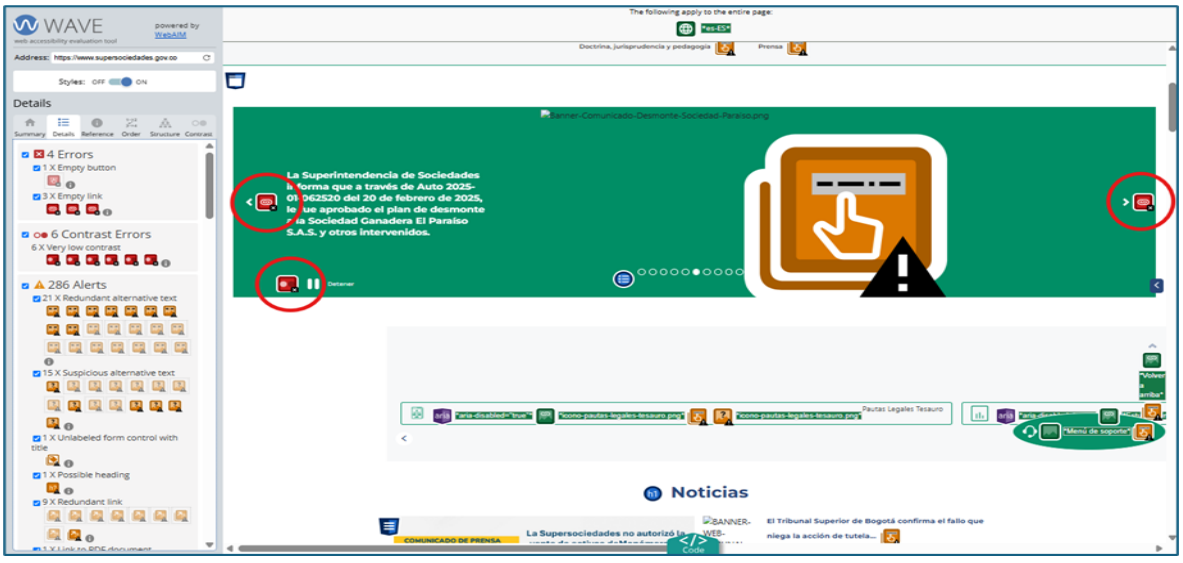
6.2 OBSERVACIONES



Fuente: https://wave.webaim.org/report#/https://www.supersociedades.gov.co

Dentro de los errores que se observaron están:

- Un botón vacío que no presenta texto ni tiene función específica en la página principal.
- Tres enlaces vacíos que no describen su función y puede generar confusión para parte de la población de usuarios como se muestra en la imagen.
- Seis errores de contraste, lo cual indica que las tonalidades no son aptas para que pueda ser percibido por todos los usuarios o que el tamaño o tipo de fuente es muy pequeña y no permita su visión óptima.



Fuente:https://wave.webaim.org/report#/https://www.supersociedades.gov.co

6.2 OBSERVACIONES

Con el reporte anterior, es posible verificar cuales son las pautas WCAG 2.1 que no se han cumplido y cuales requieren de ajustes. Dentro de las falencias más repetitivas que emitió dicho validador encontramos:

Características sensoriales y Contraste (mejorado) relacionadas con las pautas 1.3.3 y 1.4.6 respectivamente. La intención de estos criterios de conformidad es proporcionar suficiente contraste entre el texto y su fondo, para que pueda ser leído por todos los usuarios que navegan en la página web, por tanto, no se observa el cumplimiento de estas pautas.

La gestión contractual del gestor documental GEDESS, en sus etapas precontractual y contractual.

Orden de Compra 72658 de 2021:

Etapa precontractual.

5. Desde la planeación del proyecto, se observó deficiencia por parte de la Entidad en la designación de los supervisores, toda vez que, no fueron designados desde el inicio de la ejecución de la orden de compra los encargados de vigilar permanentemente el contrato, para realizar el respectivo seguimiento técnico y funcional frente a la puesta en producción de los módulos del nuevo gestor documental GeDeSS (Gestión documental, PQRS, apoyo judicial, notificaciones administrativas, grupo de sistemas y arquitectura de tecnologías, informática forense e innovación , desarrollo y arquitectura de aplicaciones)

Respuesta del Auditado:

"*No se acepta y se solicita el retiro de esta observación, teniendo en cuenta las razones que a continuación se exponen:*

En cumplimiento de lo establecido en el artículo 83 de la Ley 1474 de 2011, en los estudios previos que soportaron esta necesidad teniendo en cuenta el alto contenido tecnológico de este proyecto, se plantearon como encargados de ejercer las funciones de supervisión al Director de Tecnología y el Coordinador de Proyectos de Tecnología. Tal y como da cuenta la designación efectuada el 21 de julio de 2021; además por ser esta área la solicitante, quien justificó la necesidad y a cargo de quien se encontraba el proyecto de inversión 2018011000380 -Fortalecimiento interno de los procesos y de la infraestructura tecnológica de la Superintendencia de Sociedades a nivel nacional. Estas áreas se han mantenido como supervisores durante toda la ejecución del contrato.

Durante la ejecución del proyecto, en el año 2023, se evidenció por parte del Directora de Tecnología que era necesario involucrar a las áreas funcionales que iban a tener mayor uso del sistema para que revisaran las funcionalidades que venían siendo desarrolladas por el Proveedor, por lo cual se le solicitó al ordenador del gasto en el mes de enero de 2023 incluir a los Coordinadores de las

6.2 OBSERVACIONES

Áreas de Gestión Documental, Notificaciones, Apoyo Judicial y Relación Estado Ciudadano en la supervisión funcional del proyecto, razón por la cual el Ordenador del Gasto, designó los citados coordinadores como Supervisores a partir del 24 de enero de 2023.

Finalmente, en el año 2024 y teniendo en cuenta los diferentes componentes tecnológicos que involucraba el Gestor Documental y que se aproximaba el cierre del proyecto, se solicitó por parte de la Directora de Tecnología al ordenador del gasto que se involucrara a los Coordinadores de las Otras Áreas de Tecnología para que pudieran verificar y recibir los diferentes componentes del Gestor de acuerdo con su pericia técnica en la materia; por tal razón se procedió a designar el 9 de julio de 2024 por parte del ordenador del gasto a los coordinadores de las áreas:

Grupo de Sistemas y Arquitectura de Tecnologías, Grupo de Innovación, Desarrollo y Arquitectura de Aplicaciones, Grupo de Seguridad e Informática Forense y Grupo de Arquitectura de Datos.

Estas modificaciones fueron realizadas teniendo en cuenta la evolución y desarrollo del proyecto y considerando siempre la naturaleza de la ejecución. En proyectos tecnológicos, es una buena práctica garantizar la inclusión de los líderes técnicos y funcionales en la medida en que se van necesitando en cada fase para asegurar el éxito de su implementación.

En conclusión no existió deficiencia en la supervisión del contrato, por cuanto desde su inicio, durante toda su ejecución, hasta su finalización y actualmente en la etapa de liquidación, la supervisión correspondió a las necesidades del proyecto, de acuerdo a las competencias de las áreas, quienes se han encargado de vigilar permanentemente el contrato, para realizar el respectivo seguimiento técnico y funcional frente a la puesta en producción de los módulos del nuevo gestor documental GeDeSS., dando cumplimiento al artículo 83 de la Ley 1474 de 2011, vigilando y realizando permanentemente el seguimiento técnico, administrativo, financiero, contable, y jurídico a la correcta ejecución del objeto contratado.

En el siguiente enlace, se encuentran las notificaciones de designación de supervisión:02_Notificacion_Supervision"

Consideraciones de la OCI:

Al respecto, es necesario recordar que la supervisión en los contratos tiene por función ejercer el control y vigilancia sobre la ejecución contractual de los contratos vigilados y está dirigida a verificar el cumplimiento de las condiciones pactadas en los mismos. Como consecuencia de esto, la supervisión está facultada para impartir instrucciones al contratista y hacer recomendaciones encaminadas a lograr la correcta ejecución del objeto contratado.

En cuanto al caso en concreto, se debe resaltar que uno de los elementos más relevantes para la ejecución del contrato fue la elaboración de las Hojas de Usuario (HU), que fueron herramientas clave para capturar y comunicar los requisitos desde la perspectiva del usuario final.

6.2 OBSERVACIONES

Este elemento fue determinante desde las primeras etapas del proyecto, por lo que la designación de estos supervisores específicos debió considerarse desde el inicio y no un año y medio después de empezar la ejecución de la orden de compra, es decir en 2023.

En consonancia con lo anterior, como parte del frente funcional, se contempló la entrega de Hojas de Usuario como entregable del año 2021, las cuales fueron recibidas con el compromiso de actualizarlas durante la vigencia 2022 de acuerdo con las observaciones documentadas.

La importancia de la vinculación de los supervisores radicaba en efectuar el seguimiento e impartir las instrucciones necesarias haciendo las recomendaciones encaminadas a lograr la correcta ejecución del objeto, como fue el caso de las Hojas de Usuario, entregables en los que era necesario vincular a las áreas de Gestión documental, PQRS, apoyo judicial, notificaciones administrativas.

Lo anterior se evidencia, en las inconsistencias identificadas entre los casos de prueba y las historias de usuario definidas para los flujos de radicación, en el que, los casos de prueba fueron publicados con las últimas modificaciones en versión 0.1 el 12 de abril de 2022 y que fueron devueltos con observaciones por la Entidad el 13 de abril de 2022 mediante correo electrónico, esto, de acuerdo con oficio 159-101304 con radicado 2022-01-274668 del 20 de abril de 2022. De igual manera, lo anterior se evidencia en el Oficio 159-234307 con radicado 2022-01-775566 del 28 de octubre de 2022.

De esta manera, se demuestra que la vinculación de estos supervisores era necesaria desde "Fase 1 Funcional" y no desde el 24 de enero de 2023 como lo manifiesta el auditado.

"Conforme a las consideraciones anteriores, se mantiene la observación".

Etapa contractual - ejecución.

6. Durante la ejecución de la orden de compra, se observó que mediante el oficio 2022-01-775566 del 28/10/2022 la supervisora del contrato solicitó la entrega del ítem wgo01--IT-SW-07-02 Instalación de Licencia o Suscripción Anual, o afines (ambientes preproductivos y productivos) bajo los términos establecidos por la supervisión a más tardar el día 25 de noviembre de 2022. Sin embargo, para la fecha de este requerimiento, la Entidad ya había efectuado el pago de $95.000.000 equivalente al 83% del valor del ítem a pesar de que no se había efectuado la validación del cumplimiento del ítem que comprende la correcta instalación y el adecuado funcionamiento de los productos adquiridos.

Respuesta del Auditado:

"*No se acepta y se solicita el retiro de esta observación, fundamentados en lo siguiente:*

6.2 OBSERVACIONES

En los informes de soporte del pago 02 se encuentran las evidencias del avance parcial de la actividad, por lo cual se procedió con el pago. Posterior a ello se suscitó el imprevisto de la nueva versión de CloudPak mencionada en la modificación No. 1, por lo cual se debió proceder con la repotenciación y reinstalación total de los ambientes. (Modificación No. 1)

En el siguiente link se encuentran los soportes del pago incluido el informe de supervisión correspondiente 2021-01-783844: Pago-2 y el radicado de respuesta del proveedor 2022-01-848418."

Consideraciones de la OCI:

Conforme a los seguimientos efectuados por la supervisión, se estableció a través del oficio 159-234307 con radicado 2022-01-775566 del 28/10/2022 que, con corte a esta fecha, no se había dado entrega formal por parte del contratista de los ambientes preproductivos y productivos a pesar de que los tiempos establecidos en el cronograma de la prórroga suscrita el 8 de julio de 2022 se encontraban vencidos.

Como consecuencia de lo anterior, la supervisión solicitó la entrega de los citados ambientes considerando adicionalmente lo siguiente:

De acuerdo con lo establecido en el numeral 4.2.3.1 del RFQ Instrumento de Agregación por Demanda CCE-116-IAD-2020, en cuanto a la instalación de licencias, se señala como responsabilidad del proveedor, realizar las tareas necesarias para garantizar la instalación y el funcionamiento de los productos adquiridos entregando los respectivos informes de instalación.

A su vez, este numeral del RFQ estableció como requisitos para la entrega e "Configuración de la infraestructura desde la capa de Sistema Operativo, RedHat OpenShift, Conectividad, Seguridad y todos los componentes CP4BA":

- Sistema desplegado en el entorno On Premises de Supersociedades
- Entrega del plan de pruebas completado
- Equipo técnico capacitado
- Entrega de manual de instalación y de administración

De acuerdo con esto, a fin de validar el cumplimiento de las obligaciones relacionadas con la instalación, el contratista debía evidenciar además de la correcta instalación, el adecuado funcionamiento de los productos adquiridos, por lo que la supervisión solicitó cumplir los siguientes requerimientos acorde a las fechas de entrega estipuladas en el oficio 159-234307:

1. Despliegue de parametrizaciones efectuadas en los ambientes de Dacartec a los ambientes de desarrollo y de pruebas OnPremise de la Entidad.

6.2 OBSERVACIONES

2. Entrega previa del plan de pruebas de funcionamiento, donde se contemplen la totalidad de los componentes de licenciamiento adquiridos por la Entidad. Este plan de pruebas debe discriminar el acceso y correcto funcionamiento de los componentes de licenciamiento previstos en la arquitectura y la oferta de Dacartec:

   - IBM Business Automation Workflow.
   - IBM FileNet Content Manager
   - IBM Operational Decision Manager
   - IBM Content Collector
   - IBM Enterprise Records
   - IBM Datacap
   - IBM Robotic Process Automation

3. En sesión de Teams, presentar la ejecución del plan de pruebas, por cada componente de licenciamiento. Para cada componente se deben establecer actividades de prueba que permitan como mínimo:

   - Presentación de los componentes y parametrizaciones desplegadas. En particular servicios web parametrizados a la fecha, así como flujos de radicación y producción documental.
   - Verificar acceso desde usuarios administradores de cada componente del CP4BA.
   - Prueba funcional de parametrización base de cada componente.

Adicionalmente la supervisión advirtió que estas pruebas no correspondían a validación funcional, sino a validación del funcionamiento efectivo de las licencias instaladas.

De esta manera, la supervisión solicitó la entrega oportuna del ítem wgo01--IT-SW-07-02 Instalación de Licencia o Suscripción Anual a más tardar el día 25 de noviembre de 2022.

De acuerdo con lo anterior, esta oficina observa que el ítem comprendía una serie de actividades que iban más allá de la simple instalación de las licencias, pues involucraba una serie de actividades conexas que debían tenerse en cuenta para validar su cumplimiento, como son: la entrega de los ambientes preproductivos y productivos, el despliegue de parametrizaciones y la entrega del plan de pruebas de funcionamiento en el que se contemplaran la totalidad de los componentes de licenciamiento adquiridos por la Entidad (entre otras). Sin embargo, la mayor parte del ítem fue pagado al proveedor el 30/12/2021 a pesar de que, con fundamento en el oficio 159-234307 del 28/10/2022, existían una serie de actividades que debían ser atendidas para que la supervisión validará el cumplimiento de las obligaciones asociadas a la instalación, pues el contratista debía evidenciar, no solo la correcta instalación, sino el adecuado funcionamiento de los productos adquiridos.

"Conforme a las consideraciones anteriores, se mantiene la observación".

6.2 OBSERVACIONES

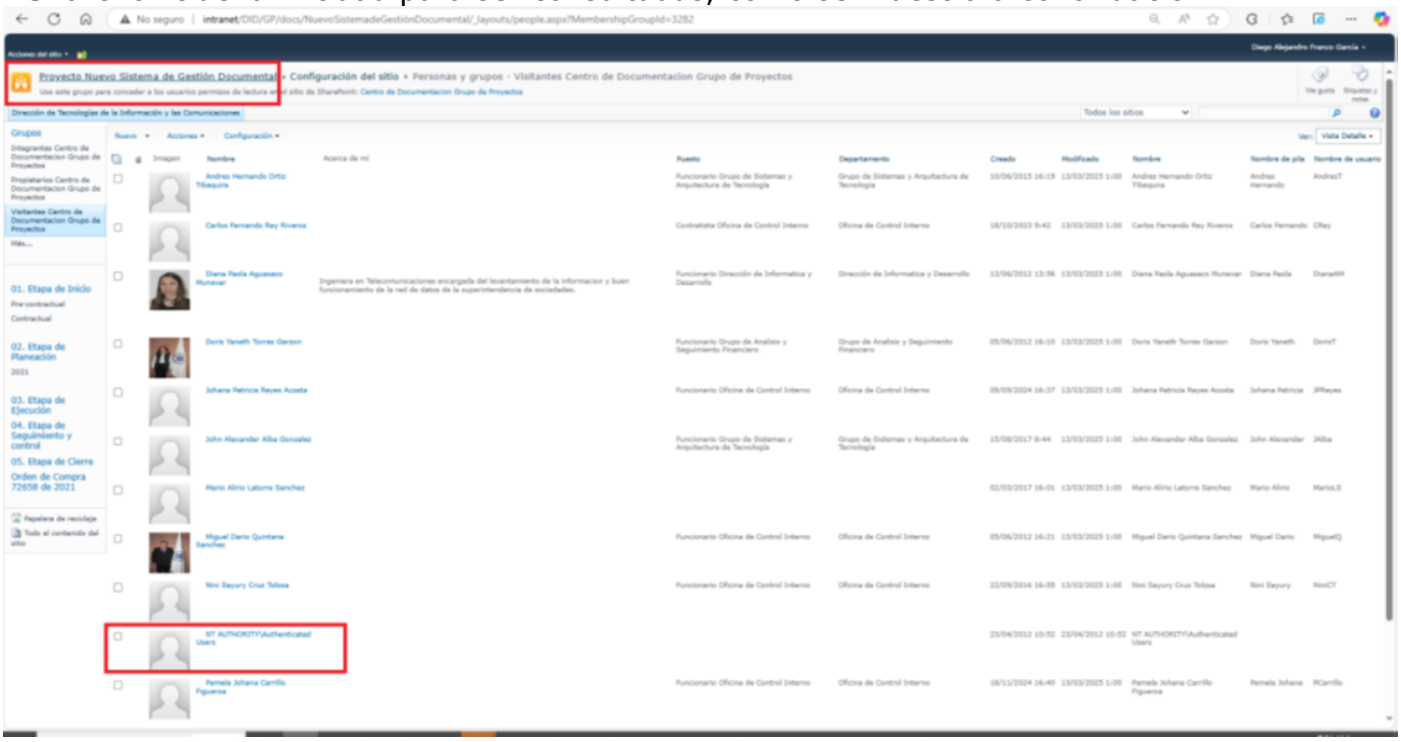
7. No fueron informados los riesgos en el Proyecto de SGDA de la Entidad, hoy GEDESS a los supervisores que ingresaban al proyecto sobre el desarrollo de su ejecución. Igualmente, no hay unificación de un modelo que identifique los riesgos, por lo que la comunicación de estos y su monitoreo deben estar documentados y, en consecuencia, es necesario realizar la comunicación de los riesgos del proyecto a los supervisores en sus distintas etapas.

Respuesta del Auditado:

Se acepta parcialmente esta observación, fundamentados en lo siguiente:

No todos los riesgos del proyecto se encuentran escritos bajo el modelo de seguimiento establecido, para lo cual se formulará el correspondiente plan de mejoramiento. Se resalta que se cuenta con un modelo y se efectuaban los seguimientos.
En cuanto al conocimiento y la gestión de los riesgos propios del proyecto son responsabilidad de todos y cada uno de los integrantes de la supervisión de acuerdo con las obligaciones en el manual de contratación y la Ley 1474 de 2011.

Las matrices de riesgos se encuentran en el repositorio de la orden de compra, y están en el SharePoint de la Entidad para ser consultadas, como se muestra a continuación:



Permiso para todos los de la Entidad.

6.2 OBSERVACIONES

Es preciso indicar al equipo auditor que durante la ejecución del proyecto se realizó seguimiento continuo con el proveedor y desde el año 2023 también con la Secretaría General, donde se analizaban y estudiaban por parte de todos los supervisores las diferentes situaciones que se iban presentando y por ello, como planes de contingencia para que la Entidad lograra tener el producto contratado, se realizaron las modificaciones cubriendo los imprevistos presentados.

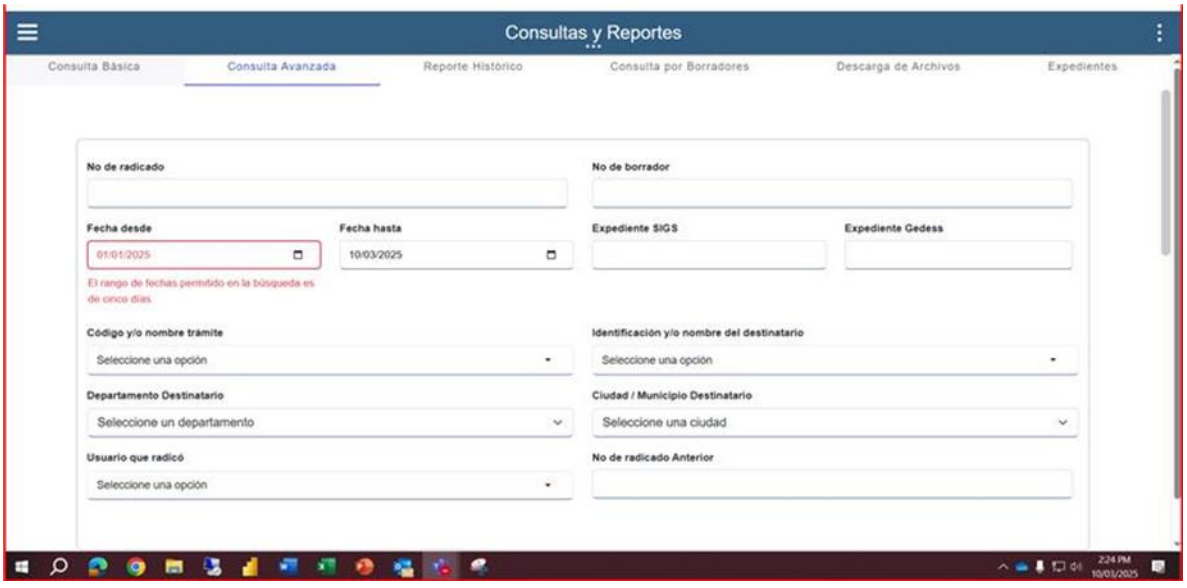
En el siguiente link se encuentran los soportes: 07_Seguimiento"

Consideraciones de la OCI:

De acuerdo con la respuesta del auditado, recibida por correo electrónico el 31 de marzo de 2025, aún no se evidencia el registro de socialización de los riesgos del proyecto, su contenido obedece a actividades referentes al seguimiento de la orden de compra y no al monitoreo de los riesgos del proyecto.

"Conforme a la consideración anterior, se mantiene la observación".

8. Se realizó la consulta frente a los documentos radicados en el proceso, para revisar cuantas radicaciones registraba el proceso, desde el 1 de enero hasta el 10 de marzo del año en curso así:



Es así como se observó lo siguiente:

- El rango de fecha de la consulta no puede ser mayor a 5 días, por lo que no es posible realizar la consulta de fechas anteriores.

6.2 OBSERVACIONES

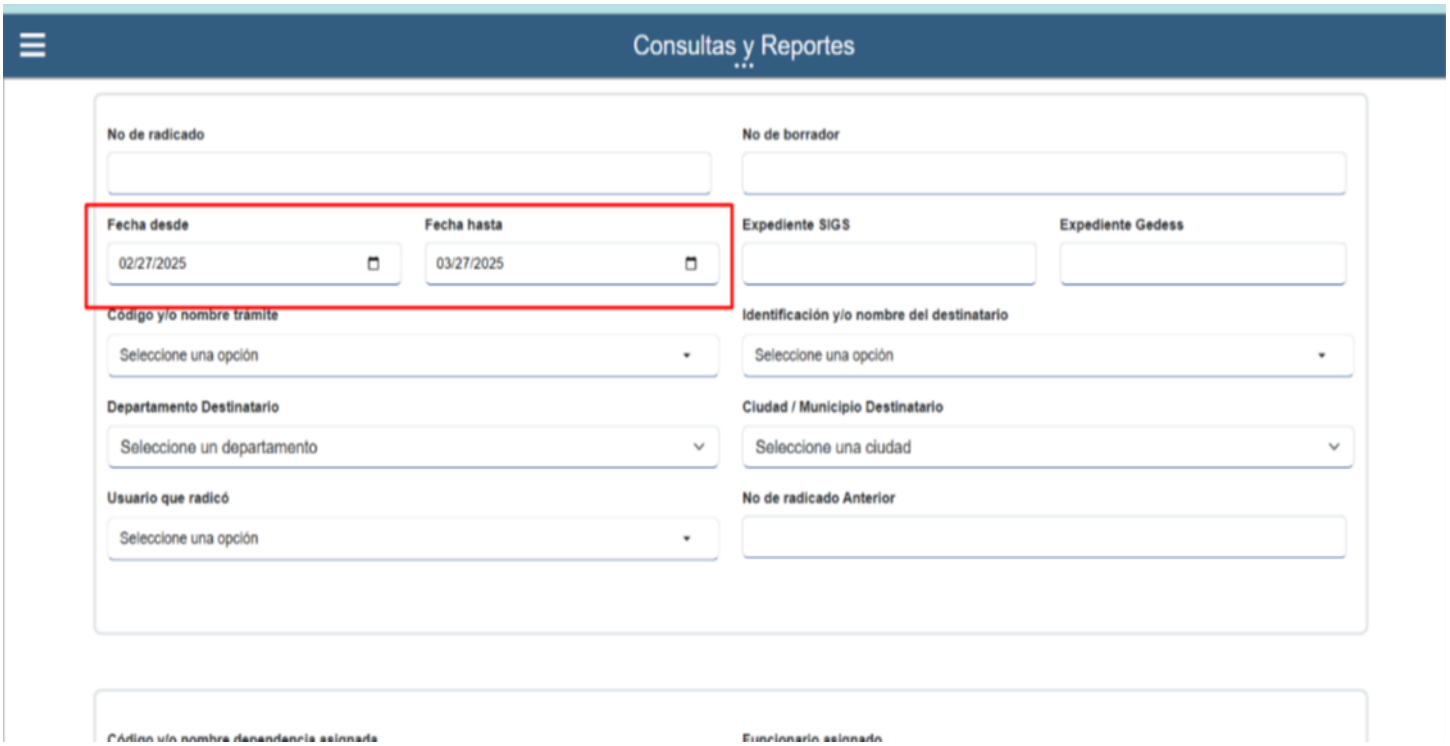
Respuesta del Auditado:

Pronunciamiento del Auditado (DTIC):

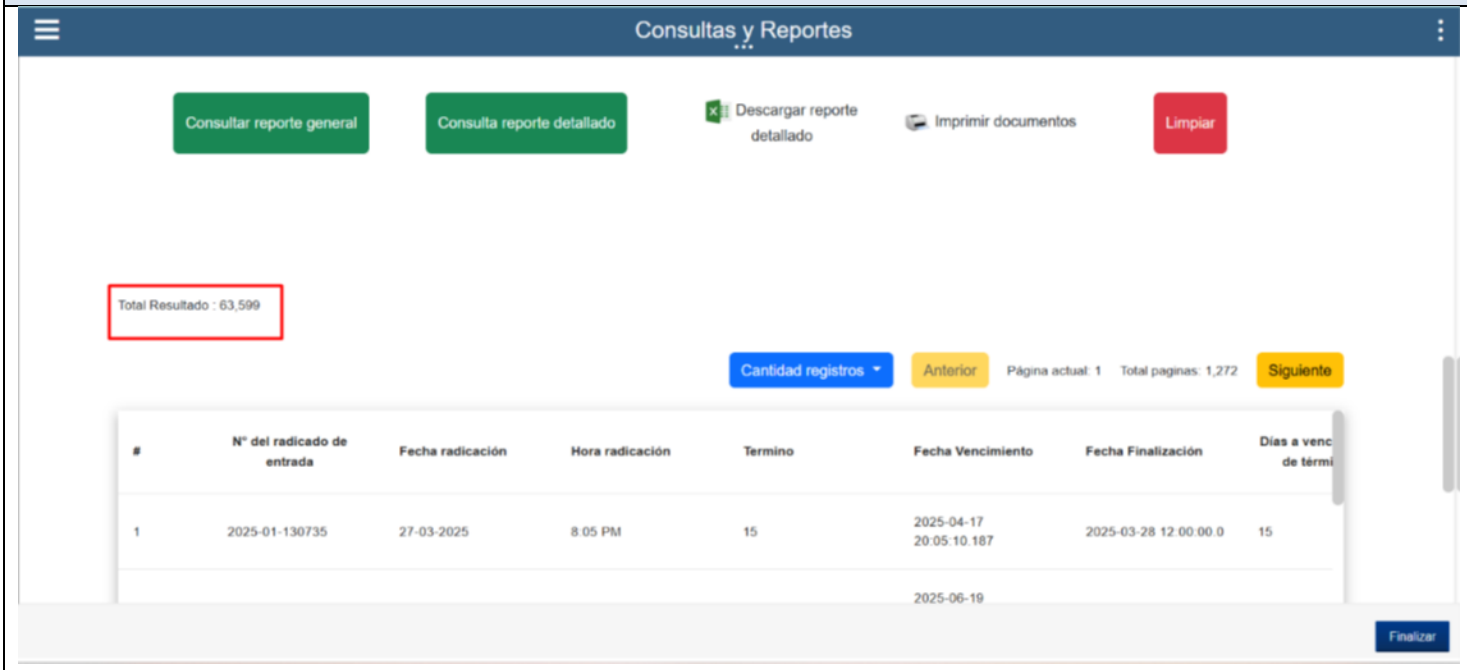
No se acepta y se solicita el retiro de esta observación por la siguiente razón:

En el momento de la prueba realizada se limitaba la consulta a un rango máximo de cinco días de búsqueda, sin embargo, si era posible consultar todo el periodo de tiempo deseado de 5 en 5 días. No quiere decir que la información anterior a los cinco días más recientes no se encontrara disponible para consulta.

Está fue una medida temporal consensuada entre las supervisiones técnica y funcional en conjunto con el proveedor como parte de una medida de estabilización y para evitar la congestión del sistema. A fecha de hoy se realizaron mejoras de concurrencia y ya es posible consultar periodos de más de un mes, tal y como se muestra a continuación.



6.2 OBSERVACIONES



Es así como se puede verificar lo siguiente:

• El rango de fecha de la consulta SI puede ser mayor a 5 días, por lo que SI es posible realizar la consulta de fechas anteriores.

<u>Consideraciones de la OCI:</u>

Se acepta la aclaración realizada por el auditado, sin embargo, tal como lo manifiesta en la respuesta:

> *"(…) A fecha de **hoy** se realizaron mejoras de concurrencia y ya es posible consultar periodos de más de un mes, tal y como se muestra a continuación (…)",* es decir que la fecha de **hoy** esto es el día 31 de marzo de 2025 (negrillas fuera de texto). El 31 de marzo se realizó el ajuste y ya se había cerrado el trabajo de campo, por lo que fue posterior a la prueba.

"Conforme a las consideraciones anteriores, se mantiene la observación".

9. El Informe estado de ejecución del 21 de noviembre de 2024 radicado 2024-01-912988, señala lo siguiente:

> *"(…) Durante el proceso de estabilización se han presentado algunos incidentes, fallas o necesidades que no fueron visibles en periodos de pruebas que se han venido informando tanto a la Dirección de Tecnología de la entidad como al proveedor, a nivel general sobre las*

6.2 OBSERVACIONES

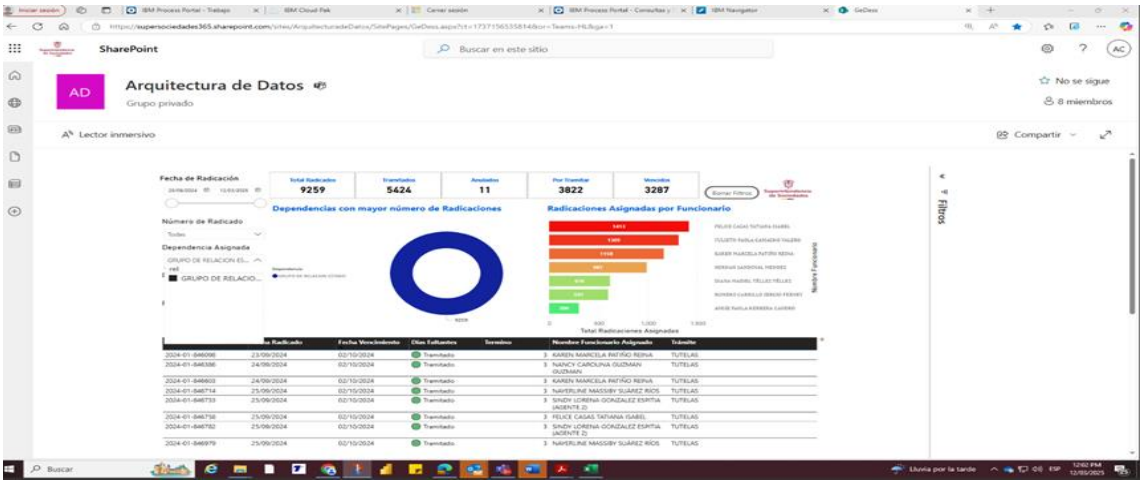
Historias de usuario se observa lo siguiente (…) en el numeral IV. ESTADO ACUAL DE EJECUCIÓN. i. Componente Funcional. A. Gestión Documental, en el numeral 7. Consultas y Reportes:

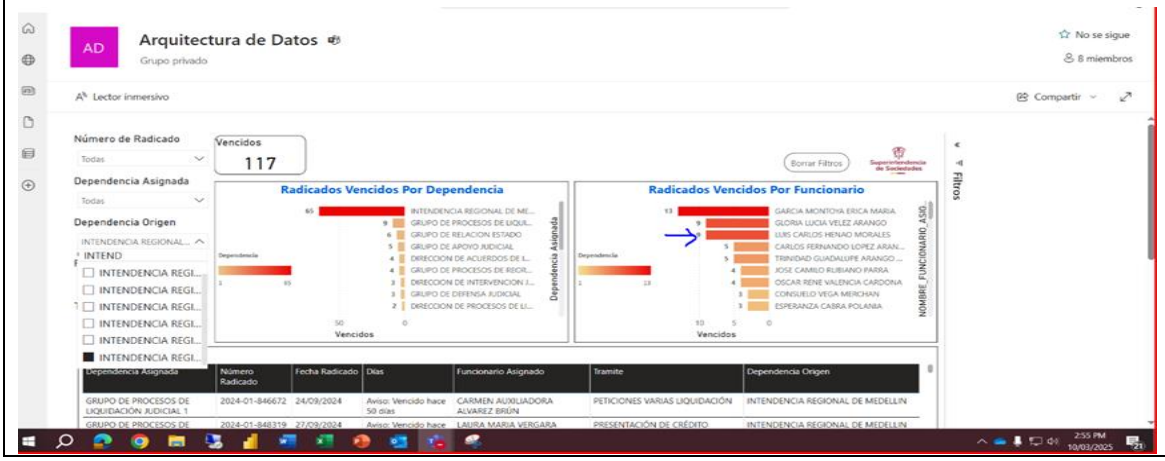
(...) **AJUSTE** **RESPUESTA** **OBSERVACIÓN.**

• No se evidencia lo que tiene pendiente por tramitar en las áreas con usuarios	Se está desarrollando un reporte así como un complemento para reporte a través de Power Bi	No Ajustado

(...)

El anterior ítem descrito, fue objeto de revisión por este equipo auditor y al realizar el trabajo de campo y revisar sus avances, se visualizó así:





6.2 OBSERVACIONES

Los reportes que muestran las imágenes tomadas los días 10 y 12 de marzo del año en curso, de dos grupos de trabajo de la Entidad, mostraron lo siguiente:

- Más de 3.000 documentos vencidos, por lo que se continuó con el trabajo de campo y se entrevistó a los funcionarios, los cuales manifestaron que el informe por Power Bi, no reflejaba la realidad del estado de los radicados en general, ni vencidos por dependencia, ni por funcionario. Es así, que el Tablero de Control por la aplicación Power Bi, no refleja el estado real de los documentos gestionados en la Entidad.
- Igualmente, los funcionarios están realizando registros de forma manual en archivos de Excel y realizando los filtros para dar trámite a las radicaciones que se encuentran ya tramitadas, pero no aparecen registradas.

Respuesta del auditado:

Pronunciamiento del Auditado (DTIC):
No se acepta y se solicita el retiro de esta observación, fundamentado en lo siguiente:

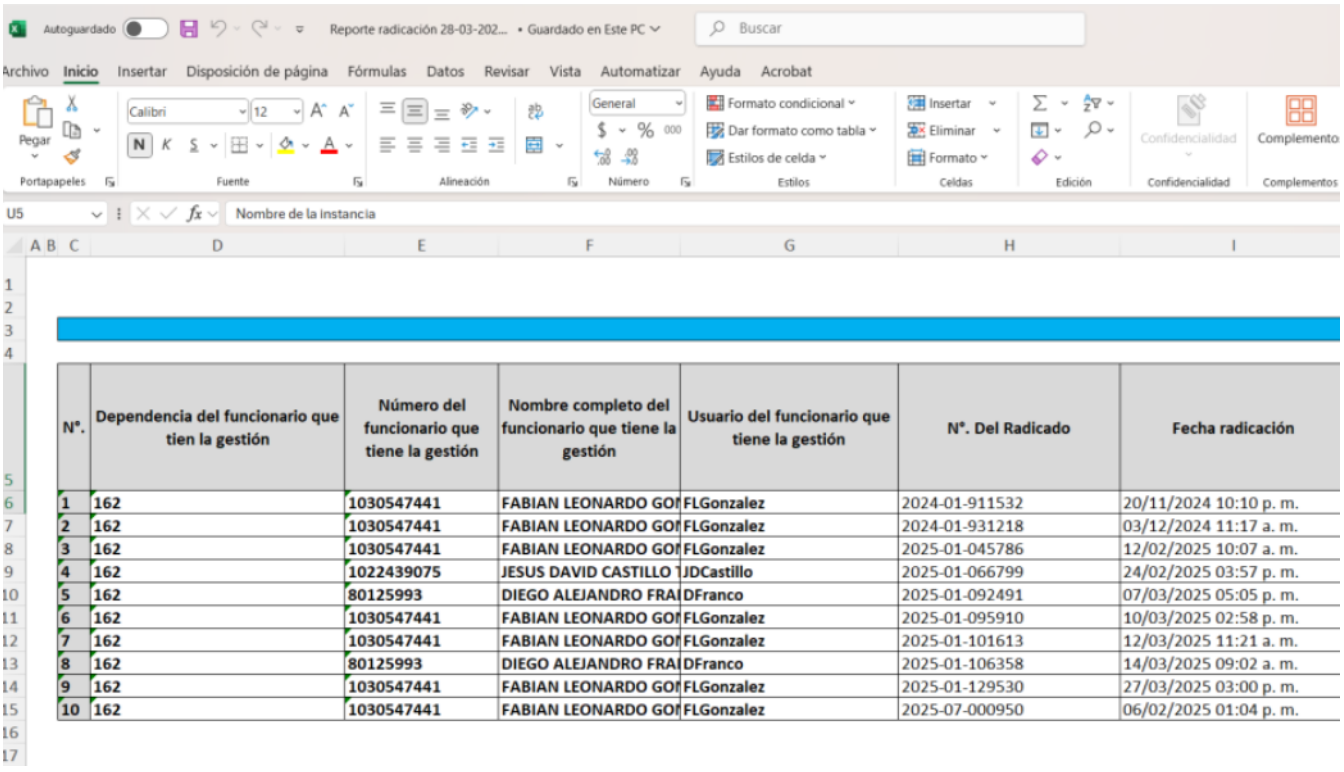
Para el momento de la prueba de Control Interno se encontraba identificado un síntoma presentado con la tabla de donde se obtiene la información para el tablero; algo normal en un sistema que se encuentra en estabilización, esto fue escalado y se está atendiendo por el proveedor bajo el caso 725 del GLPI de Dacartec. El tablero había funcionado correctamente. Con el uso del tablero se logró identificar algunos comportamientos no adecuados como que los radicados anulados contaban como vencidos, este síntoma, ya fue corregido. Otras novedades relacionadas continúan en revisión por los equipos técnicos.

Es de resaltar que el tablero muestra la información del usuario final al momento de dar trámite a las radicaciones, es decir, si los usuarios no cierran los flujos correctamente, esto puede visualizarse como vencidos y no cerrados, aun cuando ya se hayan trabajado. Estos temas ya han sido tratados en las diferentes socializaciones que se han impartido como uso y apropiación del conocimiento en las nuevas herramientas con las que cuenta la Entidad; socializaciones que se realizaron durante los meses de enero y febrero de 2025, y cuyas invitaciones fueron ampliamente difundidas a través del buzón institucional de la Entidad. En algunos casos se hicieron sesiones para toda la población de la Entidad y en otros se realizaron sesiones focalizadas por Delegaturas e intendencias regionales.

Capacitaciones_2025.pdf

Estas incidencias presentadas en el proceso de estabilización del sistema han sido punto de partida para encontrar oportunidades de mejora de GeDeSS. Como se muestra a continuación, el reporte por Dependencia ya está disponible:

6.2 OBSERVACIONES



N°.	Dependencia del funcionario que tien la gestión	Número del funcionario que tiene la gestión	Nombre completo del funcionario que tiene la gestión	Usuario del funcionario que tiene la gestión	N°. Del Radicado	Fecha radicación
1	162	1030547441	FABIAN LEONARDO GOI	FLGonzalez	2024-01-911532	20/11/2024 10:10 p. m.
2	162	1030547441	FABIAN LEONARDO GOI	FLGonzalez	2024-01-931218	03/12/2024 11:17 a. m.
3	162	1030547441	FABIAN LEONARDO GOI	FLGonzalez	2025-01-045786	12/02/2025 10:07 a. m.
4	162	1022439075	JESUS DAVID CASTILLO T	JDCastillo	2025-01-066799	24/02/2025 03:57 p. m.
5	162	80125993	DIEGO ALEJANDRO FRA	DFranco	2025-01-092491	07/03/2025 05:05 p. m.
6	162	1030547441	FABIAN LEONARDO GOI	FLGonzalez	2025-01-095910	10/03/2025 02:58 p. m.
7	162	1030547441	FABIAN LEONARDO GOI	FLGonzalez	2025-01-101613	12/03/2025 11:21 a. m.
8	162	80125993	DIEGO ALEJANDRO FRA	DFranco	2025-01-106358	14/03/2025 09:02 a. m.
9	162	1030547441	FABIAN LEONARDO GOI	FLGonzalez	2025-01-129530	27/03/2025 03:00 p. m.
10	162	1030547441	FABIAN LEONARDO GOI	FLGonzalez	2025-07-000950	06/02/2025 01:04 p. m.

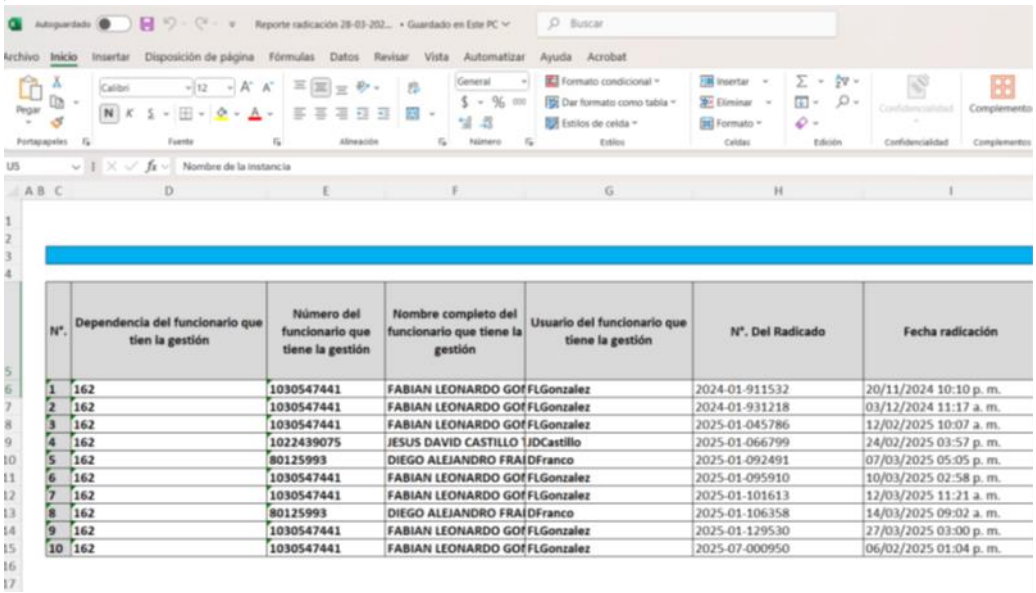
- *"Igualmente, los funcionarios están realizando registros de forma manual en archivos de Excel y realizando los filtros para dar trámite a las radicaciones que se encuentran ya tramitadas, pero no aparecen registradas."*

6.2 OBSERVACIONES

Respuesta del Auditado:

Esto es una medida de auto control efectuada por parte de los usuarios mientras se afianza el manejo del nuevo aplicativo y se estandariza la forma de llevar una gestión correcta de los radicados en GeDeSS y finaliza el periodo de estabilización de esta herramienta. No obstante, se reconoce que en este periodo de estabilización han surgido mejoras a los reportes entregados, lo cual es normal en esta etapa del proyecto.

Así mismo se reitera que desde el viernes 28 de marzo ya se encuentra el reporte por dependencia el cual apoya la gestión de los usuarios.



N°.	Dependencia del funcionario que tien la gestión	Número del funcionario que tiene la gestión	Nombre completo del funcionario que tiene la gestión	Usuario del funcionario que tiene la gestión	N°. Del Radicado	Fecha radicación
1	162	1030547441	FABIAN LEONARDO GOI	FLGonzalez	2024-01-911532	20/11/2024 10:10 p. m.
2	162	1030547441	FABIAN LEONARDO GOI	FLGonzalez	2024-01-931218	03/12/2024 11:17 a. m.
3	162	1030547441	FABIAN LEONARDO GOI	FLGonzalez	2025-01-045786	12/02/2025 10:07 a. m.
4	162	1022439075	JESUS DAVID CASTILLO	JDCastillo	2025-01-066799	24/02/2025 03:57 p. m.
5	162	80125993	DIEGO ALEJANDRO FRA	DFranco	2025-01-092491	07/03/2025 05:05 p. m.
6	162	1030547441	FABIAN LEONARDO GOI	FLGonzalez	2025-01-095910	10/03/2025 02:58 p. m.
7	162	1030547441	FABIAN LEONARDO GOI	FLGonzalez	2025-01-101613	12/03/2025 11:21 a. m.
8	162	80125993	DIEGO ALEJANDRO FRA	DFranco	2025-01-106358	14/03/2025 09:02 a. m.
9	162	1030547441	FABIAN LEONARDO GOI	FLGonzalez	2025-01-129530	27/03/2025 03:00 p. m.
10	162	1030547441	FABIAN LEONARDO GOI	FLGonzalez	2025-07-000950	06/02/2025 01:04 p. m.

6.2 OBSERVACIONES

Consideraciones de la OCI:

De acuerdo con la respuesta del auditado, menciona lo siguiente … *"(…) Para el momento de la prueba de Control Interno se encontraba identificado un síntoma presentado con la tabla de donde se obtiene la información para el tablero; algo normal en un sistema que se encuentra en estabilización, esto fue escalado y se está atendiendo por el proveedor bajo el caso 725 del GLPI de Dacartec. El tablero había funcionado correctamente. Con el uso del tablero se logró identificar algunos comportamientos no adecuados como que los radicados anulados contaban como vencidos, este síntoma, ya fue corregido. Otras novedades relacionadas continúan en revisión por los equipos técnicos (…)"*

Lo anterior obedece a que esta es una de las funciones que continúan en estabilización, no siendo aislado el esfuerzo del equipo de Tecnología por continuar con las acciones de mejoramiento, de lo que es objeto esta **Observación,** la cual se mantiene.

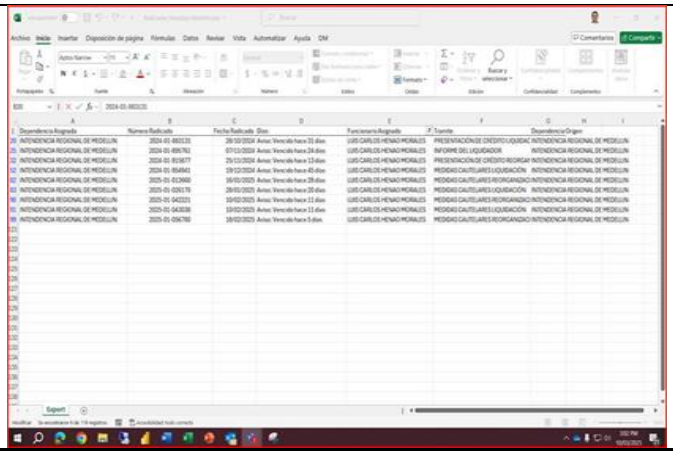
Ahora, en relación con los registros de forma manual, debe ser una situación objeto de revisión, puesto que, al ser indicada como una medida de autocontrol, se confirma que el aplicativo no es aún confiable para el usuario, ni para el proceso y que su funcionalidad presenta aún falencias, que continúan en estabilización.

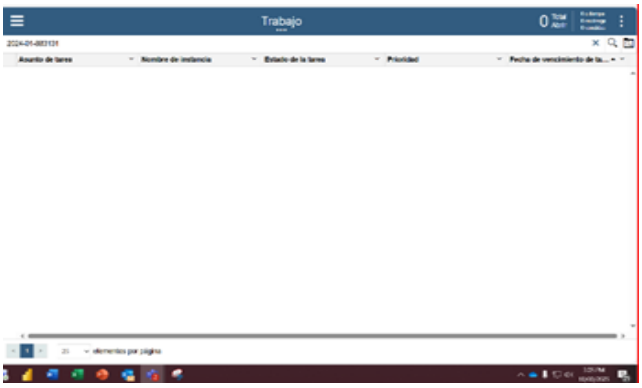
"Conforme a las consideraciones anteriores, se mantiene la observación".

10. Al revisar las radicaciones que aparecen vencidas, se observó lo siguiente:

- Un radicado (2024-01-883131-presentaciones de crédito…), se visualiza así, de acuerdo con las siguientes imágenes:

Filtro de funcionario con permisos especiales.





6.2 OBSERVACIONES

Bandeja de trabajo del funcionario que realiza el reparto

- Se encuentra vencido hace 31 días, y solo se visualiza en el tablero del funcionario con permisos especiales, pero en la bandeja de trabajo del funcionario que realiza el reparto no aparece.

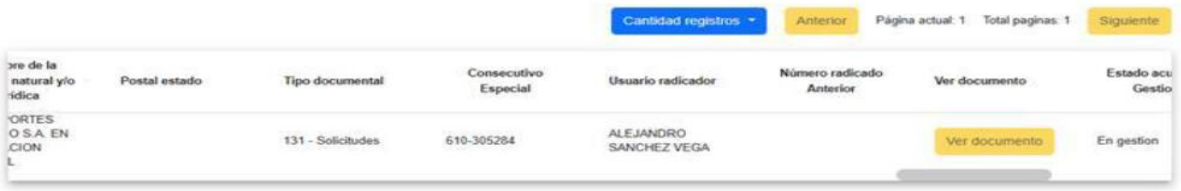
<u>Respuesta del Auditado</u>:

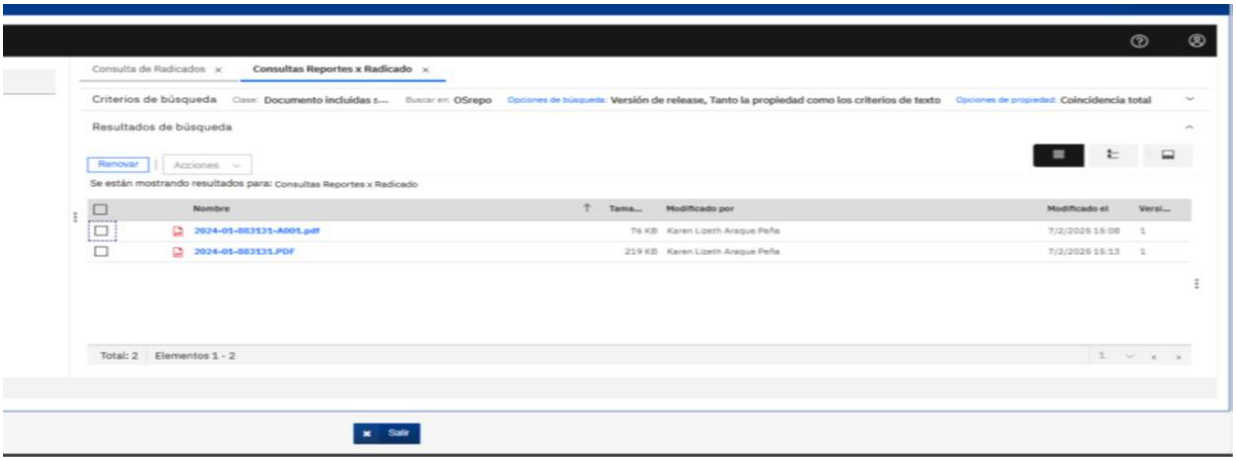
Pronunciamiento del Auditado (DTIC):

No se acepta y se solicita el retiro de esta observación, fundamentado en lo siguiente:

Se debe recordar que el Gestor Documental GeDeSS, cuenta con roles de seguridad igual que el gestor anterior Postal y las personas que no tienen permisos no lo pueden visualizar, con el fin de controlar el acceso al documento de acuerdo con su seguridad. Así mismo que una vez se cumple el flujo del proceso, el radicado ya no puede ser visualizado por el enrutador, si no queda en el flujo a la persona asignada.

Esta es la imagen de lo registrado en GeDeSS





6.2 OBSERVACIONES

Igualmente se solicita ajustar el informe de auditoría por cuanto la imagen presentada no corresponde al radicado enunciado.

Consideraciones de la OCI:

De acuerdo con el pronunciamiento del auditado, no se desconocen los roles de seguridad y de los que se asignan, por lo que se reitera la situación y se realiza la aclaración con el auditado, por otra parte, el radicado si corresponde al mencionado en el informe.

"Conforme a la consideración anterior, se mantiene la observación".

Etapa Precontractual.

11. Del análisis efectuado a la Orden de Compra, en su etapa precontractual, se evidencia falta de planeación, por cuanto la fecha de finalización del anterior soporte de IBM fue 31 de enero de 2024 y esta OC inició el 11 de marzo de 2024; por lo que durante este período (1 mes y 10 días), no se contó con soporte por parte de IBM. Esta situación es informada en el estudio previo de la OC, tal como se evidencia:

> Teniendo en cuenta lo anterior, y con el fin de garantizar la operación de la herramienta de cara a los usuarios internos y externos de la Entidad, se hace necesario contar con la suscripción y soporte para el licenciamiento IBM del sistema de gestor documental electrónico de la Superintendencia de Sociedades - GeDeSS, con lo cual se podrá contar con el soporte del fabricante necesario y permanente, durante doce (12) meses, en el evento en que sea requerido, periodo que incluye la finalización de la implementación bajo la Orden de Compra 72658 y el periodo inicial de la puesta en operación. Se hace necesario realizar la adquisición de la suscripción y soporte a la mayor brevedad, dado que la vigencia más reciente finalizó el pasado 31 de enero de acuerdo con el "Proof of Entitlement" No: 182103067 de IBM (Adjunto).

Respuesta del Auditado:

Pronunciamiento del Auditado (DTIC):
No se acepta y se solicita el retiro de esta observación, fundamentado en lo siguiente:

No corresponde a una falta de planeación toda vez que la supervisión tramitó con oportunidad el proceso como se evidencia en acta de Comité de contratación No. 07 del 2024, sin embargo, el proceso no se aprobó y se debió realizar un proceso nuevo que tomo el tiempo que se menciona. Así mismo se informa que no se presentó ningún evento critico durante el periodo que no se contó con la orden de compra de soporte.

Consideraciones de la OCI.

Luego de analizar la respuesta dada por el proceso auditado, se mantiene la observación, por cuanto de la documentación revisada y que conforma la orden de compra, se hace evidente que la Entidad estuvo por más de 1 mes sin tener soporte técnico por parte de IBM, tal como se mencionó en el estudio previo del proceso de contratación transcrito.

"Conforme a la consideración anterior, se mantiene la observación".

6.3 NO CONFORMIDAD	
DESCRIPCIÓN	**NORMATIVIDAD INCUMPLIDA**
1. Revisión por la dirección del SGSI. Se evidenció que durante el año 2024 no se realizó la revisión por la alta dirección del Sistema de Gestión de Seguridad de la Información (SGSI), omitiendo la evaluación de los puntos clave de entrada y salida que se deben abordar en dicha revisión, actividad que se debe ejecutar por lo menos una vez al año. Lo anterior, para asegurar su conveniencia, adecuación, eficacia y alineación del sistema SGSI con la Planeación estratégica de la Entidad. Lo anterior, incumple lo dispuesto en el requisito 9.3 Revisión por la dirección de la Norma NTC ISO 27001:2022	Requisito 9.3 Revisión por la dirección de la Norma NTC ISO 27001:2022
2. Tratamiento de riesgos de seguridad de la información. Se evidencia que no existe un plan documentado para el tratamiento de riesgos de seguridad de la información. Esto implica que los riesgos, especialmente aquellos clasificados como Extremos, Altos o Moderados, que exceden el nivel de riesgo aceptable para la entidad, no están siendo documentados. La ausencia de este plan impide determinar los aspectos aceptables de la seguridad de la información. Lo anterior, incumple lo dispuesto en el requisito 8.3 Tratamiento de los Riesgos de la Seguridad de la Información de la Norma NTC ISO 27001:2022	Requisito 8.3 Tratamiento de los Riesgos de la Seguridad de la Información de la Norma NTC ISO 27001:2022
3. Liderazgo y Compromiso. El equipo auditor evidenció que en las caracterizaciones de cada uno de los procesos del Sistema de Gestión Integrado (SGI), no se visualiza la actualización de los requisitos a la Norma NTC ISO 27001:2022, a excepción del proceso de Gestión de Infraestructura y Tecnologías de Información. La DTIC no cuenta con un CIO (Director de la Información) estable y disponible para la gestión de los sistemas de tecnología y toma de decisiones. Lo anterior, incumple lo dispuesto en el requisito 5.1 Liderazgo y Compromiso del Sistema de Gestión de Seguridad de la Información de la NTC ISO 27001:2022	Requisito 5.1 Liderazgo y Compromiso del Sistema de Gestión de Seguridad de la Información de la NTC ISO 27001:2022

4. Política. El equipo auditor evidenció una inconsistencia entre los objetivos de la POLÍTICA DE GESTIÓN INTEGRAL publicados en la Intranet y los objetivos establecidos en los siguientes documentos del SGI. • GC-MO-001 Documento de modelos del SGI Versión 008 • GC-PO-001 Documento de políticas versión 016 Así mismo, en el siguiente documento GC-PO-001 DOCUMENTO DE POLITICAS DEL SGI Versión 016, no especifica la siguiente política: Política Nacional para la Transformación Digital e Inteligencia Artificial. Lo anterior, incumple lo dispuesto en el requisito 5.2 Política del Sistema de Gestión de Seguridad de la Información de la NTC ISO 27001:2022.	Requisito 5.2 Política del Sistema de Gestión de Seguridad de la Información de la NTC ISO 27001:2022

5. Control de la documentación. El equipo auditor evidenció que los siguientes documentos del Sistema de Gestión Integral, no se encuentran alineados a la ISO 27001:2022: GC-MO-001 Documento de Modelos SGI, Versión 008 GC-M-001 Manual de Operaciones y del SGI, versión: 017 GC-I-002 Instructivo para la Gestión de Riesgos de Seguridad de la Información, versión 001 GC-PO-001 Documento de Políticas del SGI, versión: 016 Así mismo, en el proceso de Gestión de Infraestructura y Tecnologías de Información, 9 de los 23 formatos se encuentran con el logo de la Entidad desactualizado: GINT-F-005_Analisis Impacto GINT-F-004_Plan Pruebas GINT-F-007_Bitacora Acceso Centro Computo GINT-F-008_Procesos Base de Datos línea Comandos GINT-F-010_Concepto técnico Equipo GINT-F-011_Solicitud Respaldo información GINT-F-015_Plan Capacidad GINT-F-021_Formato Historia Usuarios GINT-F-026_Aceptación Condiciones Como Usuario Lo anterior, incumple lo dispuesto en el requisito 7.5 Control de la documentación del Sistema de Gestión de Seguridad de la Información de la NTC ISO 27001:2022 **Pronunciamiento del Auditado (DTIC)**: No se evidencia incumplimiento del numeral 5.1 "Política de Seguridad de la Información", ya que las políticas han sido debidamente definidas, aprobadas y revisadas en los intervalos planificados, según lo establecido en los documentos mencionados, y han sido debidamente divulgadas. Se solicita aclarar el informe de auditoría en el sentido de que la No Conformidad hace referencia al numeral 5.1 y no al 5.2. **<u>Consideraciones de la OCI:</u>** El día 1 de abril del 2025 se recibió correo por parte de la Coordinadora del Grupo de Seguridad e Informática Forense, donde indica que la No Conformidad es aceptada. Así las cosas y con fundamento en lo expuesto anteriormente la No Conformidad No. 5, se mantiene. **Por lo anterior se mantiene la No Conformidad.**	Requisito 7.5 Control de la documentación del Sistema de Gestión de Seguridad de la Información de la NTC ISO 27001:2022

6. Ausencia de evidencias que respaldan las actividades de control de los riesgos identificados en el proceso. En el reporte de monitoreo correspondiente al segundo semestre de la vigencia 2024, no se identificó que el responsable realizara el cargue de las evidencias que soportan las actividades de control para los siguientes riesgos: "SGSI-GINT-002-R003 Pérdida de disponibilidad del centro de cómputo Por daño en las instalaciones donde se encuentra alojada la plataforma computacional, el procesamiento, bases de datos, comunicaciones, respaldo de información y las seguridades físicas y ambientales ocasionando Pérdida de servicios", identificado como un riesgo de seguridad digital. "SGSI-GINT-006-R008 Pérdida de disponibilidad Por falta de mantenimiento ocasionando Pérdida total de servicios", no se observó cargue de las evidencias que soportan las actividades de control que se llevaron a cabo, identificado como un riesgo de seguridad de la información. Lo anterior, no permite determinar si los controles establecidos mitigan los riesgos definidos para el proceso, Lo anterior, incumple lo dispuesto en el requisito 8.3 Tratamiento de los Riesgos de la Seguridad de la Información de la Norma NTC ISO 27001:2022 **Respuesta del auditado:** **Pronunciamiento del Auditado (DTIC):** No se acepta y se solicita el retiro de esta No Conformidad, sustentado en lo siguiente: En relación con la No Conformidad reportada sobre la ausencia de evidencias en el monitoreo del segundo semestre de 2024, respetuosamente queremos manifestar que no estamos de acuerdo con esta No Conformidad, dado que, conforme a los registros existentes en el software ITS, las evidencias que soportan las actividades de control para los riesgos SGSI-GINT-002-R003 y SGSI-GINT-006-R008 fueron debidamente cargadas el día 14/01/2025.	Requisito 8.3 Tratamiento de los Riesgos de la Seguridad de la Información de la Norma NTC ISO 27001:2022

Solicitamos atentamente que el equipo auditor evalúe la evidencia registrada y, en consecuencia, proceda con la eliminación de la No Conformidad, considerando que se ha cumplido con lo dispuesto en el requisito 8.3 Tratamiento de los Riesgos de la Seguridad de la Información de la norma NTC ISO 27001:2022. **<u>Consideraciones de la OCI:</u>** La Guía de Administración de Riesgos de la Entidad definió los tiempos en los que los dueños de proceso deben realizar el reporte de monitoreo a los riesgos, para el caso específico de los riesgos de seguridad de la información determinó que el reporte se debe hacer de manera semestral y dentro de los ocho (8) días hábiles siguientes a los cortes de junio y diciembre, ahora bien, como parte de sus actividades como segunda línea de defensa, la Oficina Asesora de Planeación, por medio de correo electrónico institucional, el pasado lunes 9 de diciembre definió las fechas en las que se debía hacer el reporte, indicando que el plazo máximo era el 08 de enero de 2025, así las cosas, la Oficina de Control Interno evidenció lo siguiente: El 27 de diciembre uno de los funcionarios de la DTIC realizó un reporte indicando "Se realizan pruebas de funcionamiento plantas eléctricas pero la evidencia se enviará en el mes de enero de 2026, ya que los funcionarios responsables están de vacaciones", reporte que, si bien está dentro de los tiempos definidos, no cuenta con evidencia que soporte dichas actividades, por tanto, no hay evidencia de la aplicación del control. El 14 de enero efectivamente la DTIC realizó el reporte respectivo del monitoreo a los riesgos, no obstante, este reporte no se efectuó en los tiempos definidos por la Oficina Asesora de Planeación. Así las cosas y con base en lo expuesto anteriormente la No Conformidad No. 6 se mantiene **Por lo anterior se mantiene la No Conformidad.**	

7. Reincidencia plan de mejoramiento No. 1016. Las acciones propuestas en el plan de mejoramiento No. 1016 para eliminar la causa raíz de la No Conformidad No. 10, identificada en la auditoría realizada al proceso en la vigencia 2023, referente al cumplimiento de la Guía de Indicadores de Gestión GC-G-001, no fueron efectivas, debido a que se evidenció lo siguiente: Los Indicadores definidos para la vigencia 2025, no se encuentran publicados en la Página Web de la Entidad. Imprecisiones en la información registrada en el formato GC-F-006 Datos indicadores procesos, específicamente en el indicador "*Gestión soporte tecnológico*", toda vez que en la hoja "*Reg_Gestión Soporte Tecnológico*" en la celda F11 "*Total T1"*, determinan que el total de N° de Ticket de solicitudes registradas fue de 4.138, no obstante, en el campo observaciones, el responsable del reporte indica *"En el primer trimestre se recibieron 4.189 solicitudes (…)"*. Lo anterior, incumple el requisito del numeral 10.2 No Conformidad y Acción Correctiva de la NTC ISO 27001:2022	Requisito 10.2 No Conformidad y Acción Correctiva de la NTC ISO 27001:2022
8. Declaración de aplicabilidad. La Oficina de Control Interno, realizó entrevista al Oficial de Seguridad de la Información, evidenciando que la declaración prevista en el criterio 6.3.1, numeral 1.4 aún no se encuentra formalizada en el sistema de gestión. Lo anterior, incumple el requisito del numeral 6.1 Acciones para tratar riesgos y oportunidades de la Norma NTC ISO 27001:2022	Requisito 6.1 Acciones para abordar riesgos de la NTC ISO 27001:2022

9. Políticas específicas de Seguridad de la Información. Se evidenció que las políticas y modelos de seguridad de la información establecidas por la Entidad en los documentos GC-PO-001 Documento de Políticas del SGI y GC-MO-001 Documento de Modelos se encuentran desactualizados. No se ha realizado la revisión de las políticas a la luz de la norma ISO 27001:2022 y sus nuevos requisitos. En los documentos se hace referencia a las plataformas que actualmente ya no están operando y en otros casos, no involucra herramientas o servicios con los que en estos momentos cuenta la Entidad. Adicionalmente, falta comunicar con regularidad a todos los servidores públicos y contratistas las actualizaciones que surjan. Lo anterior incumple el control A.5.1 Políticas de seguridad de la información, de la Norma NTC ISO 27001:2022.	Control A.5.1 Políticas de seguridad de la información, de la Norma NTC ISO 27001:2022.
10. Seguridad de la información en la gestión de proyectos. Se evidenció que, en la gestión de proyectos, no se identifican los riesgos relacionados con la seguridad de la información en etapas diferentes a la de "ejecución", ni se redactan los riesgos conforme a los lineamientos establecidos en la Guía GINT-G-016 de Gestión de Proyectos. Esta deficiencia podría dar lugar a vulnerabilidades no mitigadas desde las primeras fases del proyecto y a lo largo de todo su ciclo de vida. Lo anterior, incumple el control A.5.8 Seguridad de la información en la gestión de proyectos, de la Norma NTC ISO 27001:2022.	Control A.5.8 Seguridad de la información en la gestión de proyectos, de la Norma NTC ISO 27001:2022.
11. Inventario de información y otros activos asociados. Se evidenció que no se actualizó el Inventario de Activos para todos los procesos de la Entidad, considerando los nuevos campos exigidos por la Ley 1712. Si bien, se completó la actualización de ocho (8) procesos, aún falta incorporar los campos correspondientes a la Ley 1712 para los dieciocho (18) procesos restantes, información que está documentada en el Aplicativo de Riesgos y Auditoría. Lo anterior, incumple el control A.5.9 Inventario de información y otros activos asociados, de la Norma NTC ISO 27001:2022.	Control A.5.9 Inventario de información y otros activos asociados, de la Norma NTC ISO 27001:2022.

12. Uso aceptable de la información y otros activos asociados. Se evidenció la falta de control para evitar que funcionarios o contratistas se conecten a redes inalámbricas personales o desconocidas desde los equipos de trabajo asignados por la Entidad. Esto les permite acceder a correos electrónicos personales, redes sociales y otras plataformas no relacionadas con el entorno laboral. Lo anterior, incumple el control A.5.10 Uso aceptable de la información y otros activos asociados, de la Norma NTC ISO 27001:2022.	Control A.5.10 Uso aceptable de la información y otros activos asociados, de la Norma NTC ISO 27001:2022.
13. Control de acceso. Se evidenció que el formato utilizado como control físico para registrar los usuarios que acceden al Data Center ubicado en el área de la DTIC, denominado GINT-F-007 "Bitácora de Acceso al Centro de Cómputo", no incluye de manera permanente la fecha y hora de salida de quien ingresa. Además, en el Data Center Forense, el sistema de reconocimiento facial y biométrico, que se emplea como uno de los controles físicos de acceso, no está funcionando. Lo anterior, incumple el control A.5.15 Control de acceso, de la Norma NTC ISO 27001:2022.	Control A.5.15 Control de acceso, de la Norma NTC ISO 27001:2022.
14. Abordar la seguridad de la información dentro de los acuerdos con proveedores. Se evidenció la necesidad de fortalecer los controles existentes para definir de manera clara y detallada los requisitos de seguridad que deben cumplirse con cada proveedor. Esto incluye la implementación de medidas que garanticen la protección de los activos de información compartidos y el adecuado manejo que se le debe dar a la información, asegurando que todos los proveedores cumplan con las normativas y estándares de seguridad establecidos por la Entidad, así como con las disposiciones de la Norma NTC ISO 27001:2022. Lo anterior, incumple el control A.5.20 Abordar la seguridad de la información dentro de los acuerdos con proveedores, de la Norma NTC ISO 27001:2022.	Control A.5.20 Abordar la seguridad de la información dentro de los acuerdos con proveedores, de la Norma NTC ISO 27001:2022.

15. Aprender de los incidentes de seguridad de la información. Se evidenció que, aunque la Entidad dispone de un procedimiento documentado, una política y un modelo que establece el plan de respuesta a incidentes para preparar a la Superintendencia de Sociedades en el manejo de incidentes de seguridad y ciberseguridad relacionados con los activos de información, y aunque se estipula que dichos incidentes deben ser documentados en el formato GINT-F-024 Bitácora de Eventos e Incidentes de Seguridad, con el fin de llevar un registro histórico que sirva de base para la medición de los indicadores de gestión y para la toma de acciones y lecciones aprendidas, desde el 2024 no se están registrando las lecciones aprendidas en los casos que corresponda. Lo anterior, incumple el control A.5.27 Aprender de los incidentes de seguridad de la información, de la Norma NTC ISO 27001:2022.	Control A.5.27 Aprender de los incidentes de seguridad de la información, de la Norma NTC ISO 27001:2022.
16. Continuidad del Negocio. Se evidenció que, aunque la Entidad cuenta con un procedimiento documentado, una política y un modelo que establecen y definen un conjunto de actividades, roles y responsabilidades para garantizar la continuidad de la plataforma tecnológica en caso de un evento de desastre, interrupción mayor o contingencia, y que, además, se han realizado pruebas de alta disponibilidad sobre componentes de infraestructura, el procedimiento describe plataformas que ya no están operativas, omitiendo aquellas que actualmente forman parte de la infraestructura tecnológica. Esta situación podría generar confusión y afectar la efectividad del plan ante un incidente real. Adicionalmente, la Entidad no cuenta con un BIA (Análisis de Impacto al Negocio), que es fundamental para identificar y evaluar los posibles impactos que tendría la entidad en caso de un desastre, lo cual constituye el primer paso en la planificación de continuidad del negocio. La ausencia de un BIA adecuado podría limitar la capacidad de la Entidad para priorizar las acciones de recuperación y mitigar los riesgos de manera eficaz. Lo anterior, incumple el control A.5.30 Preparación de las TIC para la continuidad de Negocio, de la Norma NTC ISO 27001:2022.	Control A.5.30 Preparación de las TIC para la continuidad de Negocio, de la Norma NTC ISO 27001:2022.

17. Acceso al Código Fuente. Se evidenció que no se encuentra restringido el acceso al código fuente ubicado en el repositorio Azure Devops, al identificar que existen nueve (9) ingenieros analistas de requerimiento o especialistas BPM de la fábrica de software interna, que actualmente tienen acceso al código fuente. Únicamente deben tener acceso a este código los ingenieros desarrolladores. Cabe precisar que este acceso está restringido a usuarios que no ejecutan roles dentro del Grupo de Innovación, Desarrollo y Arquitectura de Aplicaciones. Lo anterior, incumple el control A.8.4 Acceso al Código Fuente, de la Norma NTC ISO 27001:2022.	Control A.8.4 Acceso al Código Fuente, de la Norma NTC ISO 27001:2022.
18. Gestión de la Configuración. Se evidenció que, aunque la Entidad cuenta con la "Guía de Recomendaciones de Seguridad de Infraestructura Tecnológica" (GINT-G-004), que establece los lineamientos básicos de seguridad y configuración para la infraestructura tecnológica, esta no está completamente alineada con los requisitos de la Norma NTC ISO 27001:2022. En particular, la guía no incluye la totalidad de las configuraciones de seguridad aplicables a hardware, software y servicios que soportan las aplicaciones y servicios tecnológicos. Adicionalmente, carece de directrices claras sobre las acciones o estrategias necesarias para realizar el monitoreo adecuado de las configuraciones de seguridad, así como los procedimientos y plazos para respaldar dichas configuraciones. Esta falta de exhaustividad y formalización de procesos puede generar vulnerabilidades, ya que no se cuenta con un enfoque integral para garantizar la seguridad y la disponibilidad de las configuraciones a lo largo del tiempo. Lo anterior, incumple el control A.8.9. Gestión de la Configuración, de la Norma NTC ISO 27001:2022.	Control A.8.9 Gestión de la Configuración, de la Norma NTC ISO 27001:2022.

19. Pruebas de seguridad en el desarrollo de software y aceptación. Se evidenció que el documento GINT-MT-001 "Metodología de Desarrollo de Software", que describe la metodología utilizada en la Entidad basada en SCRUM-Agile y DevOps, está desactualizado en relación con la plataforma tecnológica utilizada. Además, no incluye directrices claras sobre las pruebas de seguridad que deben realizarse tanto para las nuevas aplicaciones como en el mantenimiento de las existentes. La falta de una definición específica sobre el proceso de pruebas de seguridad en el ciclo de desarrollo y mantenimiento de aplicaciones impide garantizar la ejecución adecuada de este control en dichos procesos. Lo anterior, incumple el control A.8.29 Pruebas de seguridad en el desarrollo y aceptación, de la Norma NTC ISO 27001:2022.	Control A.8.29 Pruebas de seguridad en el desarrollo y aceptación, de la Norma NTC ISO 27001:2022.
20. Desarrollo externalizado. Se evidenció que no se definen ni acuerdan de manera clara y completa, los requisitos y expectativas en términos de seguridad para el desarrollo de software tercerizado. Además, no se realizan pruebas de seguridad a las aplicaciones desarrolladas por terceros, lo que aumenta el riesgo de que se introduzcan vulnerabilidades en el entorno de producción. La falta de una definición precisa de los requisitos de seguridad y la ausencia de pruebas de seguridad, en los desarrollos tercerizados comprometen la integridad y la protección de la información y los sistemas. Lo anterior, incumple el control A.8.30 Desarrollo externalizado, de la Norma NTC ISO 27001:2022.	Control A.8.30 Desarrollo externalizado, de la Norma NTC ISO 27001:2022.

21. Gestión del cambio. Se evidenció que la Entidad dispone de un procedimiento documentado, GINF-PR-006 Cambios al ambiente productivo, versión 10, actualizado el 14 de febrero de 2025, el cual en su nueva versión establece que se debe: "Validar que se han cumplido las directrices contenidas en el documento GINT-MT-001 Metodología de desarrollo de software. Para ello, el gestor del cambio ya sea funcionario o contratista asignado, debe elaborar un resumen de las directrices de seguridad de la información, calidad o administrativas que se aplicaron en el cambio realizado". Este resumen debe documentarse en el formato GINT-F-003 Solicitud de Cambios del Ambiente Productivo-RFC. Sin embargo, esta actividad aún no ha sido implementada. No se han cerrado los RFC correspondientes al 2025 ni se han elaborado las actas respectivas. Adicionalmente, en los casos de reuniones de aprobación para los cambios de emergencia, no se suscriben actas de reunión, a pesar de que el procedimiento no exime de esta obligación. La falta de implementación de estas acciones compromete el control adecuado de los cambios y la trazabilidad de las decisiones relacionadas con el ambiente productivo. Lo anterior, incumple el control A.8.32 Gestión del cambio, de la Norma NTC ISO 27001:2022.	Control A.8.32 Gestión del cambio, de la Norma NTC ISO 27001:2022.
22. Sistema de Gestión Ambiental. No se está asegurando que los funcionarios de los grupos de la Dirección de Tecnología implementen acciones tendientes a asegurar el cumplimiento de las políticas ambientales. Lo anterior, se evidenció que la separación de residuos no es la adecuada en el punto ecológico, también se evidenció que en oficinas en que no se encontraban funcionarios y tenían luz natural, estaban las luces prendidas. Por lo anterior, es necesario fortalecer las acciones tendientes a generar conciencia en los funcionarios para que contribuyan con el mejoramiento del Sistema de Gestión ambiental de la Entidad. Por lo anterior, se incumple el requisito 7.3 Toma de Conciencia, de la Norma NTC ISO 14001:2015 Sistema de Gestión Ambiental.	Requisito 7.3 Toma de Conciencia, de la Norma NTC ISO 14001:2015, Sistema de Gestión Ambiental.

23. Falta de cumplimiento en accesibilidad web según la NTC 5854 y Resolución 1519 de 2020. Se evidenció que la página web de la Superintendencia de Sociedades no cumple con varios criterios de accesibilidad establecidos en la Norma Técnica Colombiana NTC 5854 y en el anexo 1 de la Resolución 1519 de 2020. Específicamente, se identificaron fallas en la implementación de las pautas 1.3.3, 1.3.4 y 1.4.6, relacionadas con el contraste insuficiente en algunas secciones y la falta de adaptabilidad en dispositivos móviles, lo que afecta la accesibilidad al portal. Así mismo, se encontraron deficiencias en los criterios 3.3.1, 3.3.2, 3.3.3, que impiden el correcto ingreso de información, limitando la interacción y el acceso de los ciudadanos a los servicios ofrecidos en línea. Lo anterior, impacta negativamente la experiencia de los usuarios, especialmente aquellos con discapacidades visuales o dificultades para la navegación, generando barreras en el acceso a la información y los servicios digitales de la entidad. Lo anterior, incumple el requisito del numeral 1.3.3, 1.3.4 y 1.4.6, 3.3.1, 3.3.2, 3.3.3 de la Norma NTC ISO 5854:2011	Requisito del numeral 1.3.3, 1.3.4 y 1.4.6, 3.3.1, 3.3.2, 3.3.3 de la Norma NTC ISO 5854:2011

24. Garantías Orden de Compra No. 72658 de 2021 – Acta de terminación. No se han cumplido los tiempos establecidos en la garantía acordada por el contratista en el acta de terminación de la orden de compra 72658 de 2021, tal como se evidencia en los soportes documentales aportados. Lo anterior incumple el Manual de Contratación; Numeral 5.5.3; acápite V. **Respuesta del auditado:** **Pronunciamiento del Auditado (DTIC):** No se acepta y se solicita el retiro de esta No Conformidad, sustentado en lo siguiente: El acta de terminación estableció los siguientes ANS- tiempos de recibo, atención y resolución de requerimientos por garantía: *Recepción de requerimientos 5 x 8, atención de lunes a viernes de 8 am a 5 pm.* *Bajo: Fallo en ortografía, texto o evento leve que no afecta el uso cotidiano del sistema.* *Atención: 2 horas corrientes* *Resolución: 72 horas corrientes* *Medio: Fallo que no impide la utilización del sistema, pero sí afecta al usuario cotidiano y normal del mismo, estableciendo un punto alterno de operación.* *Atención: 2 horas corrientes Resolución: 48 horas corrientes* *Alto: Fallo que impida el uso total o parcial de la herramienta.* *Atención: 1 hora corriente* *Resolución: 8 horas corrientes* *Nota: Los fallos que se escalen al fabricante (IBM) tendrán tiempos de atención y resolución conforme con el acuerdo de nivel de servicios que tenga la Supersociedades con el mismo.* Los tiempos de atención y los ANS son los establecidos en el IAD Software por catálogo CCE-139-IAD-2020 en el cual en el detalle en la de los ANS y Fichas técnicas indica lo siguiente: "*Para aquellos incidentes que no puedan ser solucionados por el Proveedor y que requieran ser escalados al fabricante para que actualice o*	Manual de Contratación; Numeral 5.5.3; acápite V

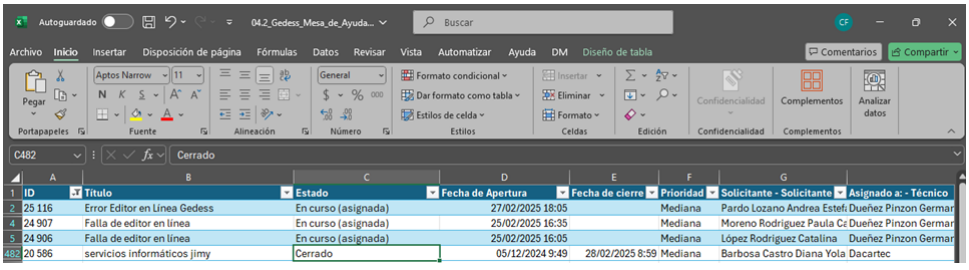
modifique el código de algún Producto, en los casos que se requiera realizar pruebas en un ambiente parecido al del cliente, el tiempo de solución se extenderá con base en el tiempo de respuesta del fabricante al proveedor o la ejecución de las respectivas pruebas. Esto no aplica en caso de inadecuada instalación y configuración de los Productos por parte del Proveedor."

Adicional a lo anteriormente expuesto, la supervisión designada respetuosamente manifiesta que se presentan incidentes técnicos imprevistos de alta complejidad que incluso requieren intervención de equipos conjuntos, que toman mayores tiempos de resolución, y que, por demás, su solución no es únicamente responsabilidad del proveedor, sino que involucra personal de la Superintendencia e incluso se escalan hasta el fabricante. Sin que en estos mayores tiempos se deje de efectuar seguimiento por parte de la supervisión.

Consideraciones de la OCI:

Revisada la documentación aportada en su momento por el proceso, se evidencia que en el Excel que se envió al equipo auditor durante la visita de campo, las incidencias mencionadas no tienen fecha de cierre; y la incidencia 20586 tiene fecha de apertura 05/12/2024 y cierre el 28/02/2025, por lo que no cumple con los tiempos fijados por el proveedor.

Esta situación se evidencia a continuación:



ID	Titulo	Estado	Fecha de Apertura	Fecha de cierre	Prioridad	Solicitante - Solicitante	Asignado a: - Técnico
25 116	Error Editor en Línea Gedess	En curso (asignada)	27/02/2025 18:05		Mediana	Pardo Lozano Andrea Estef	Dueñez Pinzon Germar
24 907	Falla de editor en línea	En curso (asignada)	25/02/2025 16:35		Mediana	Moreno Rodriguez Paula Ca	Dueñez Pinzon Germar
24 906	Falla de editor en línea	En curso (asignada)	25/02/2025 16:05		Mediana	López Rodriguez Catalina	Dueñez Pinzon Germar
20 586	servicios informáticos jimy	Cerrado	05/12/2024 9:49	28/02/2025 8:59	Mediana	Barbosa Castro Diana Yola	Dacartec

Se retira la observación y se deja la no conformidad

Por lo anterior se mantiene la No Conformidad.

25. Informes de supervisión. La supervisión de la OC 125780 no tiene establecida la entrega de informes periódicos por parte del proveedor, que permita hacer seguimiento a los casos de soporte escalados a IBM y los tiempos de atención a estos. Lo anterior, incumple el Manual de Contratación; Numeral 5.5.3; acápite V. **Respuesta del auditado:** **Pronunciamiento del Auditado (DTIC):** No se acepta y se solicita el retiro de esta observación, fundamentado en lo siguiente: La interacción (gestión de los casos) con el fabricante IBM lo tiene directamente el proveedor Dacartec, con quien la Superintendencia de Sociedades suscribió la orden de compra 125780. Esto toda vez que es quien tiene la experticia y el conocimiento pleno de todos y cada uno de los componentes técnicos que conforman la solución GeDeSS para la extracción de logs y todo tipo de evidencia que pueda ser solicitada por el laboratorio del fabricante para la atención de los casos. Adicionalmente, las evidencias del soporte recibido fueron remitidas a Control Interno. En el paquete remitido se da cuenta y ejemplo de casos escalados al fabricante y del apoyo y acompañamiento que se brindó por parte de este durante la puesta en operación, esto con VPCs adicionales como medida de mitigación durante la primera parte de la fase de estabilización. Esto gracias al soporte de fabricante con que se cuenta gracias a la orden de compra 125780.  Pendientes Auditoría GeDeSS Diego Alejandro Franco García Para Carlos Fernando Rey Riveros CC Jeny Shirley Diaz Gonzalez; Miguel Dario Quintana Sanchez Responder Responder a todos Reenviar lunes 17/03/2025 1:26 p. m. 1. 125780.zip 786 KB 2. FormExcel.zip 133 KB 3. PlanCapacitación.zip 14 KB Buen día Carlos, De acuerdo con nuestra reunión, remito evidencias solicitadas: 1. Evidencias de soporte al licenciamiento, orden de compra 125780 Es preciso tener en cuenta que durante la ejecución de la orden de compra 72658 también se hacia seguimiento a los casos que se escalaban al fabricante IBM a través de esta OC. Se adjuntan correos de evidencia de gestiones realizadas en el marco de la orden de compra, entre ellas el apoyo a la puesta en operación por parte de IBM y el incremento temporal a la cantidad de licencias de cara la misma puesta en operación. (1. 125780.zip)	Incumplimiento del Manual de Contratación; Numeral 5.5.3; acápite V.


RE: Pendientes Auditoría GeDeSS

Diego Alejandro Franco García
Para Carlos Fernando Rey Riveros
CC Jeny Shirley Diaz Gonzalez

Responder | Responder a todos | Reenviar
jueves 20/03/2025 4:18 p. m.

TS017536690.pdf
519 KB

Buena tarde Carlos,

Adjunto el reporte completo de interacciones del caso desde la apertura hasta el cierre del caso.

Cordialmente,

Superintendencia de Sociedades

Coordinador Grupo de Proyectos de Tecnología
Diego Alejandro Franco García
DFranco@supersociedades.gov.co
Teléfono: (601) 2201000 Ext 4182
Av. El Dorado No. 51-80, Bogotá, Colombia
www.supersociedades.gov.co

Los tiempos de atención y los ANS son los establecidos en el IAD Software por catálogo CCE-139-IAD-2020 en el cual en el detalle en la de los ANS y Fichas técnicas indica lo siguiente: "*Para aquellos incidentes que no puedan ser solucionados por el Proveedor y que requieran ser escalados al fabricante para que actualice o modifique el código de algún Producto, en los casos que se requiera realizar pruebas en un ambiente parecido al del cliente, el tiempo de solución se extenderá con base en el tiempo de respuesta del fabricante al proveedor o la ejecución de las respectivas pruebas. Esto no aplica en caso de inadecuada instalación y configuración de los Productos por parte del Proveedor.*"

Consideraciones de la OCI:

En prueba de campo, entrevista desarrollada con el Coordinador del Grupo de Proyectos, en relación con la ejecución del soporte técnico de la OC 125780, se le preguntó específicamente sobre si la Entidad tiene una relación o lleva un control sobre los casos que Dacartec ha escalado a IBM, como una medida de control sobre la ejecución técnica de la orden de compra.
Al respecto contestó que el control que llevan son informes de seguimiento que se piden a Dacartec, sin embargo, al ser preguntado por los informes de seguimiento que se tienen a la fecha, manifestó que en noviembre o diciembre de 2024 él solicitó a Dacartec una relación de los casos que estaban en estudio de IBM, sin embargo, esta información nunca fue remitida. De igual manera señala que no está estipulado que se deban presentar informes con periodicidades definidas.
La información remitida por el auditado detalla el seguimiento de algunos casos específicos, sin embargo, no se trata de actividades periódicas de seguimiento que adelante el proceso.

Lo anterior reitera que desde el proceso auditado y desde el inicio de las garantías, no se lleva un control detallado de la prestación del servicio contratado y por tanto se elimina la Observación y se mantiene la No Conformidad. **Por lo anterior se mantiene la No Conformidad.**	

Orden de Compra 72658 del 2021 **Etapa precontractual.** **26. Análisis costo-beneficio.** La Entidad no realizó un análisis de costo-beneficio completo que comparara la modernización del sistema de gestión documental POST@L con la adquisición del nuevo gestor documental (GeDeSS), lo cual se evidencia en el Estudio Previo, en el que no se identifica ningún apartado, cuadro o referencia que contemple dicha comparación. Además, en las conclusiones del documento no se menciona la posibilidad de modernizar el sistema actual ni se presentan escenarios de mejora. Esto incumple los artículos 25 y 29 de la Ley 80 de 1993, así como el artículo 2.2.1.1.2.1.1 del Decreto 1082 de 2015. Respuesta del auditado: *"No se acepta y se solicita el retiro de esta No Conformidad, sustentado en lo siguiente:* *Si se contó con un análisis previo a la conformación y formulación del proyecto con el apoyo del contrato de servicios profesionales 081 de 2020, suscrito con el Ingeniero John Alexander Pulido Chaparro, que permitió la formulación de la planeación del proyecto, identificando entre otros aspectos el alcance y objetivos, mediante la aplicación de un ejercicio de arquitectura empresarial, con el cual se documentó la arquitectura actual, así como la arquitectura objetivo del nuevo sistema, incluyendo los riesgos asociados y el portafolio de proyectos necesarios para la actualización y migración del sistema actual a un sistema de gestión documentos electrónicos de archivo. Así mismo, se elaboró la matriz del modelo de requerimientos para el nuevo sistema y se aplicó el diagnóstico al sistema POST@L sobre el cumplimiento de dichos requisitos.* *Así mismo para el primer semestre de la vigencia 2021, se suscribió el contrato de servicios profesionales 096 de 2021 con el Ingeniero Pulido Chaparro, mediante el cual se prestó la asesoría para la elaboración de los estudios de selección del software que cumpliera con la arquitectura objetivo-establecida, así como los estudios técnicos y de mercado.*	Artículos 25 y 29 de la Ley 80 de 1993, así como el artículo 2.2.1.1.2.1.1 del Decreto 1082 de 2015.

Igualmente, en la vigencia 2019, la Entidad desarrolló el diseño de su arquitectura empresarial TO-BE, en el marco del contrato 058 de 2019 suscrito con CINTEL, en donde se estableció la siguiente línea de acción frente al sistema de gestión documental POSTAL: "Se propone la modernización de ésta aplicación reemplazando sus funcionalidades con otra solución, en el entendido que este sistema de gestión documental actualmente no posee las capacidades funcionales y de arquitectura para formar parte del ecosistema del Sistema de Gestión Documental Electrónico Archivo y las directrices del Archivo General
de la Nación, y se han detectado también brechas de seguridad.

CINTEL - DOCUMENTO ACTUALIZADO DEL DISEÑO ARQUITECTURAL DE SISTEMAS DE INFORMACION"

Consideraciones de la OCI:

El análisis de costo-beneficio es una herramienta fundamental en la planeación de cualquier contratación pública, especialmente cuando se busca reemplazar un sistema tecnológico existente con una nueva solución. Su propósito es determinar si la inversión es justificable, si los beneficios superan los costos y cuál es la mejor alternativa en términos de eficiencia, impacto y sostenibilidad financiera.

En este caso, el estudio previo que dio origen al proceso de contratación de la OC 72658 de 2021, si bien es cierto que incluyó el análisis técnico y operativo de la nueva solución, debió incluir una comparación en términos de costos entre mantener y actualizar Post@l versus adquirir e implementar una nueva solución, lo que habría permitido reafirmar decisión de manera más objetiva y justificada.

El análisis de costo-beneficio permite evaluar cuál de las alternativas posibles representa un mejor retorno para la entidad pública, considerando no solo el costo inicial sino también los gastos futuros, la escalabilidad, la interoperabilidad y los riesgos asociados. De acuerdo con esto, un análisis costo-beneficio completo, hubiera permitido conocer detalladamente si la opción escogida era adecuada en términos de costo, funcionalidad y sostenibilidad, minimizando riesgos ya que permitiría identificar posibles problemas financieros, técnicos y operativos, reduciendo el riesgo de fallos en la implementación.

El estudio previo de la Orden de Compra para justificar la necesidad del nuevo gestor documental se basó principalmente en el desarrollo de una arquitectura empresarial planteada en el marco del contrato 058 de 2019 suscrito con CINTEL. Si bien entre los entregables de este contrato se estableció modernizar la arquitectura empresarial de la Entidad, no se incluyó una comparación entre Post@l y una nueva solución en términos de costos de operación, mantenimiento, obsolescencia, etc. En la respuesta del auditado se hace referencia a los contratos suscritos con John Alexander Pulido Chaparro, que contribuyeron a la formulación de la planeación del proyecto. Sin embargo, en los productos de este contrato no se evidencia un análisis en términos de costos de reemplazar la solución anterior con un nuevo gestor documental. En cuanto a la comparación entre post@l y la nueva solución, el estudio previo menciona brevemente que "*El costo de la hora para implementar nuevas funcionalidades en el sistema POSTAL para 2021 asciende a $162.628, valor que es superior al comparativo efectuado con el Instrumento de Agregación por Demanda para Software por Catálogo definido por Colombia Compra Eficiente, donde el valor de la hora de parametrización tiene un costo de $130.000*". Sin embargo, no se hizo referencia a los costos de Actualizar y mantener Post@l (con costos de modernización, soporte y mantenimiento) y su comparación con adquirir e implementar un nuevo sistema (con costos de licenciamiento, implementación y capacitación). Así las cosas, mencionar las limitaciones técnicas de Post@l sin un análisis cuantitativo en términos de costos no es suficiente y debió establecerse en el estudio previo un análisis que mostrara cuánto costaría corregir esas limitaciones versus la adquisición de un sistema. **Por lo anterior se mantiene la No Conformidad.**	

27. Cálculo de la información a migrar de Post@l al nuevo gestor documental (GeDeSS) La Entidad no efectuó de manera adecuada el cálculo de la información a migrar de POST@L al nuevo gestor documental (GeDeSS) lo que se evidencia en el estudio previo, en la modificación 1, en la justificación de la modificación 4 y en la modificación 5. En estos documentos se estableció que, el tamaño de la información objeto de migración fue calculada inicialmente en 30GB (el proveedor otorgó 30GB adicionales para un total de 60GB) cuando el tamaño de la información total a migrar fue de 686GB, es decir, un incremento del 2186% frente a la estimación inicial de 30GB efectuado por la Entidad. Esto incumple los artículos 25 y 29 de la Ley 80 de 1993, así como el artículo 2.2.1.1.2.1.1 del Decreto 1082 de 2015. Respuesta del auditado: "*No se acepta y se solicita el retiro de esta No Conformidad, sustentado en lo siguiente:* *(Esta también como observación). Inicialmente se había planificado no hacer migración y arrancar el archivo documental del nuevo SGDEA desde cero o con metada mínima (60GB), sin embargo, dada la necesidad identificada ya con el desarrollo del proyecto de conservar la trazabilidad de los paquetes documentales (por ejemplo, citar un radicado anterior migrado), se vio la necesidad de migrar toda la data y su correspondiente auditoría. Este sustento está en las modificaciones 4 y 5.* *Todos los documentos de solicitud de modificaciones fueron sustentados técnica y jurídicamente por la Dirección de Tecnología y presentados en su debido momento a los miembros del Comité de Contratación de la Entidad quienes los revisaron y recomendaron al ordenador del gasto proceder con tales modificaciones, como se puede observar en la carpeta contractual de esta orden de compra y en las actas correspondientes del Comité de Contratación, es necesario también resaltar que uno de los miembros del Comité de Contratación que tenía voz pero no voto, es la Jefe de la Oficina de Control Interno de la Entidad. Adicionalmente, en aquellos casos donde se solicitó aclaraciones tanto por los miembros del Comité de Contratación como por el Ordenador del Gasto fueron resueltas por la Dirección de Tecnología.*	Artículos 25 y 29 de la Ley 80 de 1993, así como el artículo 2.2.1.1.2.1.1 del Decreto 1082 de 2015.

Como se puede observar, de acuerdo con lo solicitado por la Dirección de Tecnología, era una necesidad de la Entidad la cual se tramitó para garantizar el buen servicio dado que si no se contrataba: *<u>Modificación No. 5:</u>* *"() … 2.4 Perjuicios institucionales de no otorgar la adición* *Conllevaría al incumplimiento de los lineamientos del Archivo Central de la Nación frente al Sistema de Gestión Documental afectando en forma directa el acceso de información desde la perspectiva de la transparencia, la protección de datos y la regulación anti-trámites.* *De acuerdo con la Guía de Implementación del SGDEA del AGN, mediante la cual Se debe tener en cuenta que, sumado al enfoque tecnológico, las herramientas implementadas deben estar acorde con las exigencias de la normatividad vigente, las políticas institucionales, alineadas con los sistemas de gestión y deben obedecer a una adecuada planificación, coordinación y control de la información con el fin de garantizar su integridad, autenticidad y disponibilidad a lo largo del tiempo.* *Traería consigo el incumplimiento del plan estratégico institucional para la actual vigencia fiscal.* *Conllevaría a la materialización de los siguientes riesgos por la no migración completa de la información de todas las tablas de la base de datos del sistema Post@l:* *Pérdida de datos críticos: Si no se migra toda la información de manera adecuada, es posible que se pierdan datos esenciales para el funcionamiento y consulta de la información.* *Falta de integridad de la información: La información que no se migra correctamente podría sufrir daños o cambios en su integridad, lo que afectaría la confianza en los datos almacenados perdiendo su nivel probatorio.* *Inconsistencia en la información: Si solo se migra parte de la información, puede haber inconsistencias entre los datos almacenados en el sistema anterior y el nuevo, lo que puede dificultar la consulta de la información.* *Dificultades en la recuperación de información: La información no migrada correctamente puede ser difícil de encontrar o recuperar, lo que puede generar confusión y retrasos en la realización de las actividades del talento humano de la Entidad.* *Problemas de seguridad: Si no se migra adecuadamente la información relacionada en términos de políticas de seguridad,*	

puede tener consecuencias legales y de reputacionales para la Entidad. *Costos adicionales: Si es necesario volver a realizar la migración o corregir* *errores debido a una migración incompleta, esto puede generar costos* *adicionales y consumo de recursos que podrían haberse evitado con una* *migración completa y exitosa.* *Insatisfacción del personal y usuarios: Si los usuarios no encuentran la* *información que necesitan o experimentan problemas con el nuevo sistema debido a una migración incompleta, esto puede generar insatisfacción y resistencia al cambio.* *Resultaría imposible poner en operación el nuevo Sistema de Gestión Documental Electrónica de Archivo de la Superintendencia de Sociedades, generando un impacto negativo en los grupos de interés de la Superintendencia de Sociedades, e implicaría la ejecución de planes de acción que podrían generar reprocesos y demoras adicionales en la finalización del proyecto dado el avance significativo que a la fecha ya se cuenta."… ()* *Link a los documentos de las modificaciones: 01_Modificatorios"* **<u>Consideraciones de la OCI:</u>** Respecto de la información a migrar al nuevo sistema de gestión documental de la Entidad es necesario considerar: Las estimaciones iniciales no fueron las adecuadas: esto tiene sustento en la etapa inicial de la Orden de Compra, esto es, en el año 2021, pues se estimó migrar 60GB de información desde el sistema Post@l, lo cual resultó ser insuficiente, ya que en ese momento la base de datos ya contaba con 375 tablas y aproximadamente 500GB de información. En las modificaciones se refleja el incremento de Gigas adicionales ya que se presentó un aumento del 1043% (frente a los 60GB iniciales). Dentro de las principales causas se tiene que no se identificaron inicialmente todas las tablas que debían migrarse pues solo se seleccionaron 11 de las 375 tablas existentes, no se consideraron adecuadamente los archivos anexos y logs del sistema Post@l, que aumentaban significativamente el tamaño real de los datos y se desconocían particularidades técnicas del sistema Post@l, como el	

manejo de roles y permisos en backend, lo cual también afectó el diseño de la migración y debió ser evaluado desde el levantamiento de requerimientos. De esta manera, en el estudio previo no se incluyó un análisis técnico detallado del volumen total de datos ni una proyección de crecimiento real y tampoco se evidenció un análisis de riesgos ni alternativas de migración parcial o fases. Ahora, frente a la respuesta del auditado respecto de la observación 7, si bien es cierto justifica la adición a la Orden de Compra derivada del aumento de las gigas a migrar, esto no desvirtúa que la planeación en este aspecto no fue suficiente. Los oficios mencionados por el auditado, aunque sustenten técnicamente las modificaciones al contrato en cuanto a la migración de información, son documentos producidos posteriormente a la planeación inicial, lo que no desvirtúa el hecho de que la estimación inicial no fuera la adecuada. Adicionalmente, el listado de riesgos institucionales por no realizar una migración completa (pérdida de datos, fallas de integridad, incumplimiento de lineamientos del AGN, etc.) confirma la criticidad del proceso de migración. Por lo tanto, el hecho de que en la planeación inicial solo se hayan considerado 60GB y que no se hubieran identificado todas las tablas a migrar, refleja una falla estructural en el levantamiento de requerimientos. Si bien el auditado señala que se verificaron los precios del mercado y que el proveedor ofreció precios favorables, esto es irrelevante frente al punto central del hallazgo, que se centra en la estimación adecuada de la información a migrar desde la etapa de planeación. El principio de planeación no solo exige verificar precios razonables, sino determinar correctamente el objeto y el alcance de lo que se va a contratar. Finalmente, frente a este pronunciamiento por parte del auditado, este no desvirtúa el hallazgo de la OCI, pues, si bien las modificaciones se justificaron posteriormente y fueron acompañadas de la documentación técnica y decisiones del comité de contratación, esto no elimina el hecho de que la estimación inicial de la información a migrar no fue la adecuada y que no se identificaron oportunamente todas las tablas a migrar desde post@l. En cuanto al argumento presentado por el auditado para la no conformidad, el propio auditado reconoce que "*Inicialmente se había planificado no hacer migración y arrancar el archivo documental del nuevo SGDEA desde cero o con metadata mínima (60GB)…*", punto que cobra vital relevancia por cuanto:	

Muestra que, la etapa de planeación inicial, carece de un análisis integral de los procesos archivísticos y funcionales requeridos por la Entidad. Migrar desde cero afecta principios fundamentales de trazabilidad documental, integridad y continuidad del archivo exigidos por el AGN. Omitir la necesidad de migrar la información histórica en un SGDEA es, desde el punto de vista archivístico, una omisión crítica que debía preverse desde el estudio previo, no durante la ejecución del contrato. Si bien es cierto que en las justificaciones de las modificaciones 4 y 5 se justificó ampliamente la necesidad de migrar toda la base de datos y sus beneficios, esto no desvirtúa la necesidad de haber planeado este aspecto de manera correcta desde el inicio del proyecto, es decir, la información que era necesaria migrar al nuevo gestor documental. Las consecuencias mencionadas de no migrar la información por el auditado, aunque válidas, reafirman porqué se debió prever desde el inicio pues, de no hacer la migración completa, se pone en riesgo la integridad, disponibilidad y trazabilidad de la información, vulnerando los lineamientos del AGN y dificultando la operación del nuevo sistema y en consecuencia, generando costos, retrasos y reprocesos. Sin embargo, lo anterior no justifica la falencia en el cálculo de la información a migrar en la etapa de planeación, sino que, refuerza el argumento de que era un aspecto crítico que debía estar incluido desde el estudio previo de manera adecuada. Finalmente, ante el argumento relacionado con el Comité de Contratación de la Entidad, el hecho de que las modificaciones hayan sido aprobadas por dicho comité y que la Jefe de la Oficina de Control Interno haya asistido con voz, pero sin voto, no es óbice para que en la etapa de estructuración de la Orden de Compra se hubiera realizado una planeación técnica completa con la información razonable a migrar. La OCI o el Comité no sustituyen la obligación legal que tienen las áreas técnicas de estimar adecuadamente los requerimientos desde el principio, incluyendo la cantidad y tipo de datos a migrar. **Por lo anterior se mantiene la No Conformidad.**	

28. Etapa contractual - ejecución. Modificaciones como consecuencia de la indebida planeación. La Entidad no efectuó una planeación adecuada del proyecto, lo que se reflejó en la necesidad de realizar modificaciones a la orden de compra lo que generó prorrogas que extendieron la ejecución de la orden de compra e implicó la adición de recursos para la ejecución del proyecto. Esto incumple los artículos 25 y 29 de la Ley 80 de 1993, así como el artículo 2.2.1.1.2.1.1 del Decreto 1082 de 2015. Al respecto, se incumplen las normas citadas al no tener en cuenta aspectos como: a. Modificación No. 4 del 29/06/2023: i. Gestión del cambio se observa una planeación deficiente por cuanto no se calculó de manera efectiva el número de capacitaciones necesarias y de usuarios a los que iban dirigidas. Tuvo un impacto de 2 meses y un valor de $148.000.000. ii. No se contempló la integración de los servicios con 4-72, servicios utilizados por la Entidad con anterioridad a la contratación del nuevo gestor documental lo que tuvo un impacto de 2 meses y un costo adicional de $62.400.000. Se debe tener en cuenta que el Operador Postal Oficial o Concesionario de Correo es la persona jurídica habilitada por el Ministerio de Tecnologías de la Información y las Comunicaciones que, mediante contrato de concesión, prestará el servicio postal de correo, y mediante habilitación, los servicios de Mensajería Expresa y Servicios Postales de Pago a nivel nacional e internacional. El Operador Postal Oficial en Colombia es Servicios Postales Nacionales S.A. 4-72, concesionario hasta el año 2024. iii. Se adicionó el ítem wgo01--IT-SW-11-01 soporte técnico reactivo lo que evidencia una falta de planeación pues fue un servicio que debió ser contemplado desde el principio ya que está destinado a cubrir servicios de atención y resolución de problemas técnicos que surgen inesperadamente en el gestor documental de la Entidad, garantizando que cualquier interrupción o fallo sea atendido y solucionado de manera eficiente para restablecer las operaciones normales. Su impacto fue de $96.000.000. Lo anterior incumple los Artículos 25 y 29 de la Ley 80 de 1993, así como el artículo 2.2.1.1.2.1.1 del Decreto 1082 de 2015.	Artículos 25 y 29 de la Ley 80 de 1993, así como el artículo 2.2.1.1.2.1.1 del Decreto 1082 de 2015.

Respuesta del auditado:

Pronunciamiento del Auditado (DTIC):

"No se acepta y se solicita el retiro de esta No Conformidad, sustentado en lo siguiente:

(Está también como observación). Cada proyecto tiene una dinámica diferente y las modificaciones surgen de imprevistos y/o materialización de riesgos no previsibles que se van presentando a medida que se ejecuta un proyecto, los cuales como se ha reiterado anteriormente fueron sustentados técnica y jurídicamente por la Dirección de Tecnología y presentados en su debido momento a los miembros del Comité de Contratación de la Entidad quienes los revisaron y recomendaron al ordenador del gasto proceder con tales modificaciones, como se puede observar en la carpeta contractual de esta orden de compra y en las actas correspondientes del Comité de Contratación, es necesario también resaltar que uno de los miembros del Comité de Contratación que tenía voz pero no voto, es la Jefe de la Oficina de Control Interno de la Entidad. Adicionalmente, en aquellos casos donde se solicitó aclaraciones tanto por los miembros del Comité de Contratación como por el Ordenador del Gasto fueron resueltas por la Dirección de Tecnología.

Se solicita al equipo auditor tener en cuenta el detalle en el acta de terminación con radicado 2024-01-938742 del 09 de diciembre de 2024 Numeral 2., se detallan cada una de las modificaciones en cuanto a:

Razones que la originaron (Fundamentos)
Logros alcanzados (Resultados)

Link a los documentos de las modificaciones: 01_Modificatorios"

<u>Consideraciones de la OCI:</u>

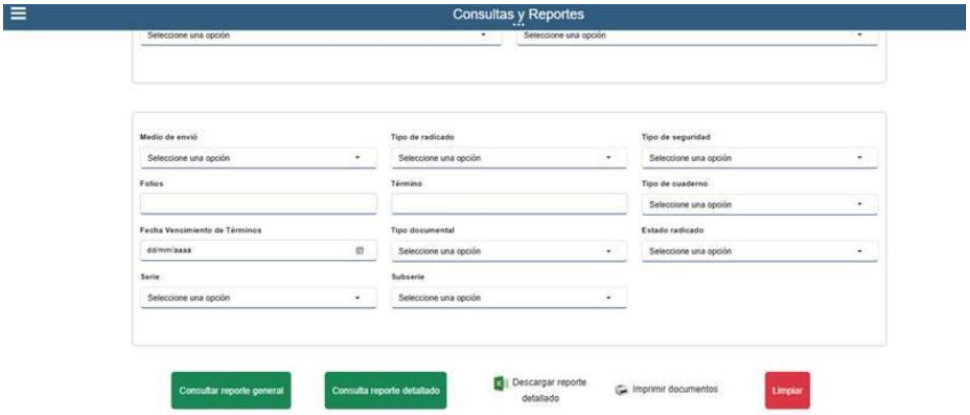
De acuerdo con las aclaraciones expuestas por la Coordinadora del Grupo de Gestión Documental, la modificación N°1 no hace parte de los elementos que evidencian la no conformidad. Sin embargo, al subsistir los aspectos que estructuran la No conformidad, que se reflejan en la modificación Nº 4, se mantiene la No Conformidad de acuerdo con lo siguiente:

En cuanto a la gestión del cambio, de acuerdo con la solicitud de modificación Nº 4 se evidencia que, el plan de capacitaciones

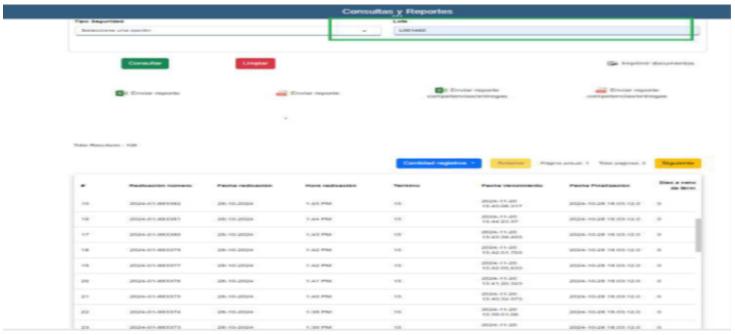
inicialmente diseñado resultó insuficiente frente a las necesidades reales de la Entidad. Las capacitaciones debían segmentarse de acuerdo con los procesos funcionales específicos que incorporaría el nuevo sistema (radicación, OPE, PQRS, producción documental, notificaciones, expedientes, etc.), las áreas misionales y de apoyo de la Entidad tienen diferencias significativas en sus necesidades de capacitación, lo que hizo inviable una capacitación genérica y transversal y el plan de trabajo original no contempló la complejidad funcional total del sistema GeDeSS, que resultó ser más demandante de lo previsto inicialmente en cuanto a tiempo, número de sesiones y profundidad del conocimiento requerido. De esta manera, aunque la Entidad implementó estrategias de gestión del cambio y justificó técnicamente la necesidad de ampliar las capacitaciones mediante la Modificación No. 4, la estrategia inicial fue deficiente y subestimó las condiciones reales del entorno organizacional y la complejidad del sistema de gestión documental entrante. Respecto de los servicios de 4-72, el proyecto no incluyó desde su fase de estructuración ni en los documentos de planeación (estudio previo, requerimientos técnicos y RFQ) la obligación de integrar el sistema GeDeSS con los servicios de mensajería certificada del operador postal oficial Servicios Postales Nacionales S.A. - 4-72, a pesar de que la gestión de notificaciones físicas es una función esencial en los procedimientos administrativos de la Entidad. Esta omisión generó la necesidad de realizar una modificación posterior (Modificación No. 4), lo cual representa una falla en la identificación oportuna de requerimientos funcionales críticos, que debieron haberse definido y cuantificado desde el estudio previo y el análisis técnico-jurídico del proyecto. De acuerdo con la solicitud de modificación Nº 4 se establece claramente que "*Revisada por la supervisión el alcance original de la orden es evidente que no estaba incluida la integración con el proveedor del servicio de correspondencia*". De igual manera el Acta de Terminación radicado 2024-01-938742 del 09/12/2024, en el numeral 2 detalla que la Modificación 4 incorporó requerimientos no previstos inicialmente, entre ellos la integración con el operador postal, lo cual prolongó la ejecución del contrato y generó ajustes técnicos posteriores. Adicional a lo anterior, La Ley 1369 de 2009 establece el marco legal para la prestación de servicios postales en Colombia, definiendo al Operador Postal Oficial y sus responsabilidades.	

Esta ley en su artículo 3º define el operador de servicios postales como "*la persona jurídica, habilitada por el Ministerio de Tecnologías de la Información y las Comunicaciones de Tecnologías de la Información y las Comunicaciones que ofrece al público en general servicios postales, a través de una red postal*". Respecto de la obligatoriedad del uso del Operador Postal por parte de la Entidades estatales, el artículo 15 de la Ley 1369 de 2009 señala que "*El Operador Postal Oficial o Concesionario de Correo será el único autorizado para prestar los servicios de correo a las entidades definidas como integrantes de la Rama Ejecutiva, Legislativa y Judicial del Poder Público*", lo cual ha sido ratificado por la Agencia Nacional de Contratación Pública Colombia Compra Eficiente en Concepto C–092 de 2023 en cual establece: "*La Subdirección de Gestión Contractual se permite informar que analizadas las normas contenidas en la Ley 1369 de 2009, es claro que las entidades integrantes de la Rama Ejecutiva, Legislativa y Judicial del Poder Público les asiste el deber legal de contratar los servicios servicio de postal universal y de servicios de correo prestados con exclusividad por el Operador Postal Oficial - Servicios Postales Nacionales SAS, de conformidad con lo dispuesto en el artículo 15 de la citada norma*". Así las cosas, la incorporación de la integración con 4-72 en la Modificación Nº 4 confirma que este aspecto no fue tenido en cuenta durante la etapa de planeación inicial del proyecto, constituyéndose en una falla estructural en la definición del objeto contractual. Respecto de la respuesta del auditado, la necesidad de integrar el sistema GeDeSS con el Operador Postal Oficial (4-72) no puede considerarse un riesgo sobreviniente ni un evento imprevisto. Esta necesidad era previsible, recurrente y jurídicamente exigible, teniendo en cuenta que: Desde antes de iniciar el proyecto, la Entidad ya utilizaba el servicio de 4-72 para notificaciones físicas de actos administrativos. La Ley 1369 de 2009 establece que el único operador habilitado para notificaciones postales oficiales es 4-72, hecho normativo y operativo que debió ser considerado desde la planeación. Los procedimientos administrativos, sancionatorios y de comunicaciones oficiales exigen trazabilidad postal certificada, lo cual es un requisito funcional esencial y no accesorio del SGDEA.	

Si bien se justificó adecuadamente la incorporación de los servicios de 4-72 y se hubieren producido documentos de soporte (como memorandos técnicos y presentaciones de los supervisores), estos fueron elaborados después de iniciada la ejecución contractual, cuando ya se había evidenciado la omisión. Tales justificaciones no validan la suficiencia de la planeación original, sino que confirman que fue necesario ajustar la Orden de Compra por fallas en el levantamiento de requerimientos. Sumado a esto, si el servicio de integración postal se identificó como crítico durante la segunda prórroga, esto refuerza el argumento de que debió preverse en la etapa de diseño, no en medio de la ejecución. En cuanto a la adición del ítem wgo01--IT-SW-11-01, el soporte técnico reactivo es una necesidad esencial y no un evento excepcional, ya que hace referencia a la atención de incidentes y fallos en la operación diaria de un sistema, especialmente durante etapas críticas como el despliegue, puesta en producción y estabilización del sistema. Esto no es un evento imprevisto, sino una necesidad esperada y recurrente en cualquier proyecto tecnológico de envergadura como la implementación de un Sistema de Gestión Documental Electrónico de Archivo (SGDEA). La adición del ítem wgo01--IT-SW-11-01 en etapa de estabilización no puede justificarse como un imprevisto. Al contrario, confirma que la Entidad no contempló en la etapa de planeación un componente básico. Esto representa una no conformidad sustancial, pues el soporte reactivo es parte estructural del ciclo de vida de un sistema, especialmente en ambientes críticos, donde fallas pueden afectar el cumplimiento normativo frente al Archivo General de la Nación, la trazabilidad, la integridad de la información y la continuidad de la operación institucional. Finalmente, como ya ha sido mencionado, el argumento relacionado con el Comité de Contratación de la Entidad, el hecho de que las modificaciones hayan sido aprobadas por dicho comité y que la Jefe de la Oficina de Control Interno haya asistido con voz, pero sin voto, no es óbice para que en la etapa de estructuración de la Orden de Compra se hubiera realizado una planeación técnica completa. La OCI o el Comité no sustituyen la obligación legal que tienen las áreas técnicas de estimar adecuadamente los requerimientos desde el principio. **Por lo anterior se mantiene la No Conformidad.**	

29. Generación de informes por GeDeSS. El gestor documental de la Entidad no permite la generación de informes y reportes en formatos como PDF, Excel o archivo plano, tal como se evidenció en el trabajo de campo llevado a cabo el 13 de marzo de 2025 y el informe de PQRS que genera la Entidad. Lo anterior incumple el numeral 4.2.3.2 del RFQ Instrumento de Agregación por Demanda CCE-116-IAD-2020 Catálogo de Productos IBM. **Respuesta del auditado:** **Pronunciamiento del Auditado (DTIC):** No se acepta y se solicita el retiro de esta No Conformidad, sustentado en lo siguiente: En la reunión del día 13 de marzo, celebrada por Teams con la Coordinadora de Gestión Documental no se envió correo electrónico alguno, fue solamente una charla explicativa respecto a las necesidades del cambio del gestor, y sus fundamentos. En dicha conversación no se habló de reportes ni de exportar en diferentes extensiones como: pdf, Excel, cosa que el gestor documental si hace. Se socializó sobre el tablero de Power Bi, se mostró como exportarlo a Excel. Se compartieron estadísticas de radicación, se mostró el procedimiento de cómo se radica en Webmaster, se habló de temas de gestión del cambio, errores de usuario y apropiación de la herramienta. Lo anterior puede ser verificado en la grabación de la aplicación Teams  	Numeral 4.2.3.2 del RFQ Instrumento de Agregación por Demanda CCE-116-IAD-2020 Catálogo de Productos IBM

Consideraciones de la OCI: De acuerdo a la respuesta del auditado, es necesario tener en cuenta que el aplicativo no ofrece la funcionalidad de exportar reportes que soporten los informes tales como PQRS y el que genera la Entidad de Radicados Vencidos. Igualmente, la obligación contractual relevante se encuentra establecida en el numeral 4.2.3.2 del *RFQ del Instrumento de Agregación por Demanda CCE-116-IAD-2020*. Este numeral exige que la solución de Gestión Documental cumpla, entre otros, con la generación de reportes en múltiples formatos. En particular, se estipula que el sistema (SGDEA) debe proveer herramientas para generar informes configurables y permitir su exportación al menos en formatos PDF, Excel y archivos planos. Es decir, desde el pliego de requisitos funcionales, era mandatorio que la plataforma ofreciera la posibilidad de extraer información y reportes en dichos formatos estándar para facilitar su análisis y seguimiento. **Por lo anterior se mantiene la No Conformidad.**	

30. Masivos. El Gestor Documental no permite elaborar documentos masivos. La elaboración de este tipo de archivo está limitada por el número de "marcadores" y por ende no es posible la emisión de masivos. Esto se evidenció en el trabajo de campo del 12 de marzo de 2025 en diferentes grupos de trabajo. Lo anterior, incumple el numeral 4.2.3.2 del RFQ Instrumento de Agregación por Demanda CCE-116-IAD-2020 Catálogo de Productos IBM. **Respuesta del auditado:** **Pronunciamiento del Auditado (DTIC):** No se acepta y se solicita el retiro de esta No Conformidad, sustentado en lo siguiente: A la fecha se han realizado un total de 2.501 lotes masivos, con 122.230 documentos, algunos de ellos con hasta 43 marcadores. Si de pronto existe algún grupo que necesite hacer este masivo con más marcadores con gusto realizaremos acompañamiento adicional a las capacitaciones que se han hecho, ya que también hace parte del aprendizaje y mejoramiento continuo.  **<u>Consideraciones de la OCI:</u>** En atención a lo anterior, es importante reforzar las acciones que generen respuesta efectiva para la realización de comunicaciones masivas, como es la generación de los oficios de requerimiento a las sociedades obligadas a presentar estados financieros y sus anexos, por lo que en trabajo de campo se constató que la Entidad tiene planes de contingencia para evitar retrasos en sus procesos, el nuevo Gestor Documental de la Entidad debe permitir la generación de este tipo de documentos. **Por lo anterior se mantiene la No Conformidad.**	Numeral 4.2.3.2 del RFQ Instrumento de Agregación por Demanda CCE-116-IAD-2020 Catálogo de Productos IBM.

31. Presuntos incumplimientos. La Entidad no adelantó el proceso sancionatorio correspondiente por los "presuntos incumplimientos" reiterados del contratista, sin que esto lo exonerara de ejecutar las obligaciones a su cargo en virtud de la suscripción del Instrumento de Agregación de Demanda y de la Orden de Compra. Esto se evidencia en varios oficios: 2022-01-775566 del 28/10/2022, 2022-01-643041 del 31/08/2022, 2023-01-075619 del 14/02/2023, 2023-01-132287 del 14/03/2023, 2023-01-146936 del 23/03/2023, 2023-01-175722 del 04/04/2023, 2023-01-269279 del 20/04/2023, 2023-01-326114 del 26/04/2023, 2023-01-394174 del 05/05/2023. Lo anterior, incumple los artículos 84 y 86 de la Ley 1474 de 2011 y la cláusula 20 del Instrumento de Agregación de Demanda para la adquisición de Software por Catálogo que requieran las entidades estatales CCE-139-IAD-2020. **Respuesta del auditado:** **Pronunciamiento del Auditado (DTIC):** "*No se acepta y se solicita el retiro de esta No Conformidad, sustentado en lo siguiente:* *Para cada requerimiento realizado por la supervisión con el fin de hacer seguimiento y gestión a la Orden de Compra, se presentó respuesta del proveedor de acuerdo con lo requerido, las necesidades y el estado de proyecto como se evidencia en el siguiente cuadro:*	Artículo 84 y 86 de la Ley 1474 de 2011 y en la cláusula 20 del Instrumento de Agregación de Demanda para la adquisición de Software por Catálogo que requieran las entidades estatales CCE-139-IAD-2020.

Requerimiento Supersociedades	Respuesta Dacartec
2022-01-775566	2022-01-848418
2022-01-643041	2022-01-691162
2023-01-075619	2023-01-209277
2023-01-132287	2023-01-209277
2023-01-146936	2023-01-209277
2023-01-175722	2023-01-209277
2023-01-269279	Corresponde al informe de ejecución corte 10 de marzo de 2023 por parte de los supervisores.
2023-01-326114	2023-01-449561
2023-01-394174	2023-01-449588

Cuadro de requerimientos y respuestas de la entidad y el proveedor.

De lo anterior, se concluye que: *La supervisión designada ha actuado en cumplimiento a lo establecido en el artículo 84 de la Ley 1474 de 2011 que establece: "La supervisión e interventoría contractual implica el seguimiento al ejercicio del cumplimiento obligacional por la entidad contratante sobre las obligaciones a cargo del contratista.* *Los interventores y supervisores están facultados para solicitar informes, aclaraciones y explicaciones sobre el desarrollo de la ejecución contractual, y serán responsables por mantener informada a la entidad contratante de los hechos o circunstancias que puedan constituir actos de corrupción tipificados como conductas punibles, o que puedan poner o pongan en riesgo el cumplimiento del contrato, o cuando tal incumplimiento se presente."* *El artículo 25 de la Ley 80 de 1993 (principio de economía), en su numeral 4 indica: Los trámites se adelantarán con austeridad de tiempo, medios y gastos y se impedirán las dilaciones y los retardos en la ejecución del contrato.* *No solo mediante el desarrollo de Procesos Administrativos Sancionatorios la administración puede conminar y apremiar al contratista al cumplimiento de sus obligaciones, para lo cual puede desarrollar mesas de trabajo, solicitudes escritas y seguimiento a estas. Por cuanto, el tiempo promedio para adelantar un PAS para la imposición de multas es de aproximadamente 4 semanas desde el momento en que se presenta el informe por parte de la supervisión; la imposición de multas solo procede mientras se halle pendiente por parte del contratista el cumplimiento de obligaciones que dieron origen a la actuación administrativa, por lo cual, una vez el contratista se pone al día la administración no debe continuar con el desarrollo del PAS.* *Frente a situaciones de retrasos, la supervisión requería al contratista y este atendía los aspectos solicitados y contratados. Es decir, de acuerdo con los informes de la supervisión, para los pagos, las modificaciones y los solicitados por el Ordenador del Gasto, se manifestaba el cumplimiento de las obligaciones de DACARTEC S.A. razón por la cual, si se había superado la mora o el retraso, no era posible iniciar el proceso sancionatorio para multar al contratista.*	

Una vez finalizado el contrato a la fecha no existe informe de la supervisión que establezca el incumplimiento del contrato. Lo anterior no quiere decir que en el evento de determinarse un incumplimiento no se proceda a iniciar el proceso sancionatorio establecido en el artículo 86 de la Ley 1474 de 2011, aplicando la cláusula penal pecuniaria de acuerdo con lo acordado en la Orden de Compra y lo señalado en la Ley 80 de 1993, Ley 1150 de 2007, Ley 1474 de 2011, cumpliendo el debido proceso y los principios de la contratación".

Consideraciones de la OCI:

El principio de legalidad impone a las autoridades el deber de actuar conforme a la ley, lo cual incluye sancionar las conductas contrarias al ordenamiento. La Constitución Política establece que los servidores públicos responden por omisión o extralimitación en el ejercicio de sus funciones[1]. En desarrollo de este mandato, la Corte Constitucional ha sido enfática en que no puede invocarse la buena fe para eludir la aplicación de sanciones. La jurisprudencia ha señalado que "so pretexto de la vigencia de (la buena fe), no puede hacerse nugatorio el deber de sancionar los actos contrarios a la Constitución y a la Ley"[2].

En un Estado de Derecho, cuando la ley faculta a las autoridades para sancionar, estas pueden y deben exigir el cumplimiento de las prestaciones a su cargo, de ahí que la potestad sancionatoria administrativa no es meramente discrecional, sino una obligación jurídica cuando se configuran sus presupuestos, en garantía del interés general y los principios que rigen la función administrativa[3].

Así las cosas, todas las personas en la contratación estatal (incluidos los contratistas) deben responder por sus acciones y omisiones antijurídicas, de modo que el incumplimiento de un contratista exige una reacción sancionatoria de la entidad, so pena de comprometer la responsabilidad del funcionario por inacción.

La Corte Constitucional ha avalado el régimen sancionatorio en contratación estatal, resaltando que las sanciones contractuales buscan proteger la finalidad del contrato y los recursos públicos. La Corte ha señalado que, ante un posible incumplimiento a cargo del contratista, "la entidad pública lo citará a audiencia para debatir lo ocurrido", tras lo cual decidirá motivadamente imponer la multa, sanción o declaratoria de incumplimiento correspondiente,

[1] Constitución Política de Colombia, 1991, artículo 6

[2] Sentencia T-460 de 1992

[3] Constitución Política de Colombia, 1991, artículo 209

Estatuto General de Contratación de la Administración Pública, Ley 80 de 1993, artículo 26.

garantizando el debido proceso. Ello demuestra que, evidenciada una falta contractual, la entidad debe activar el procedimiento sancionatorio[4].

Así mismo, ha sostenido que el deber de sancionar comporta aplicar castigos razonables y proporcionales a la gravedad de la falta, reafirmando que la discrecionalidad en la imposición de sanciones está limitada por la ley y los principios de razonabilidad. En suma, para la Corte la facultad sancionatoria tiene un fundamento obligatorio en el principio de legalidad: la administración está obligada a hacer cumplir la Constitución y la ley, incluso mediante sanciones, cuando se presenten incumplimientos contractuales que vulneren el interés colectivo.

De igual manera, el Consejo de Estado ha reforzado la idea de que las entidades no pueden renunciar a sus facultades sancionatorias frente a incumplimientos. La Sala de Consulta y Servicio Civil conceptuó que la administración no debe prescindir de sus privilegios unilaterales para obligar a los contratistas a cumplir las obligaciones asumidas en el contrato[5]. Es decir, ante incumplimientos la entidad tiene el deber de ejercer sus potestades sancionatorias (imponer multas, declarar incumplido el contrato, hacer efectiva la cláusula penal, etc.), pues estas herramientas existen para asegurar la ejecución del contrato conforme a los fines estatales. La Sala enfatizó que dichas facultades exorbitantes (consagradas en los arts. 14 de la Ley 80/93, 17 de la Ley 1150/07 y 86 de la Ley 1474/11) son instrumentos al servicio del interés público y no mera opción discrecional.

En efecto, el Estatuto Anticorrupción (Ley 1474 de 2011) introdujo un procedimiento sancionatorio precisamente porque el Estado debe poder contar con instrumentos efectivos para apremiar el cumplimiento del contrato, como para sancionar al contratista incumplido y proteger el interés público de los efectos nocivos de los incumplimientos. De esta manera, una vez detectado un incumplimiento, la entidad tiene el deber jurídico de iniciar el Proceso Administrativo Sancionatorio (PAS) correspondiente. La inactividad estatal frente a faltas contractuales constituye una vulneración al principio de legalidad de la función pública e implica dejar de usar herramientas diseñadas para preservar la buena ejecución contractual.

Ahora bien, en la Orden de Compra No. 72658 de 2021 (bajo el Instrumento de Agregación de Demanda CCE-116-IAD-2020), el

[4] Sentencia C-499 de 2015

[5] Consejo de Estado Sala de Consulta y Servicio Civil, 11001-03-06-000-2015-00102-00

proveedor asumió obligaciones técnicas y cronogramas específicos para la implementación del sistema de gestión documental en la Entidad. Entre otras obligaciones, el contratista debía instalar y poner en funcionamiento los productos adquiridos en la infraestructura de la entidad, entregando informes de instalación, así como proveer ambientes de pruebas y producción operativos en plazos determinados. Para diciembre de 2022, la supervisión advirtió que no se habían entregado los ambientes preproductivo ni productivo en los términos pactados, habiéndose incluso vencido los plazos de la prórroga suscrita el 8 de julio de 2022. Conforme al oficio con radicado 2022-01-775566 la Entidad exigió formalmente al proveedor la entrega del ambiente de pruebas (preproducción) en un plazo de 5 días hábiles y del ambiente de producción en máximo 20 días, recordándole que dichos hitos ya estaban vencidos conforme al cronograma acordado Este requerimiento se fundamentó en que, pese a que la entidad proporcionó oportunamente la infraestructura necesaria, el proveedor no cumplió con la instalación completa del sistema en las fechas previstas, contrariando lo estipulado en el anexo técnico del instrumento de agregación (numeral 4.2.3.1). De igual manera, durante el primer trimestre de 2023 la supervisión documentó múltiples dilaciones e incumplimientos parciales en diversas entregas funcionales. Mediante oficios con Radicados 2023-01-132287 y 2023-01-146936, se requirió al contratista informes detallados y justificativos sobre por qué no se habían realizado a tiempo las sesiones de socialización, pruebas y liberación de varios módulos clave (radicación de documentos, expedientes, firma digital, notificaciones, consultas, roles, etc.) conforme al cronograma pactado. De esta manera la supervisión señaló la omisión del proveedor en el cumplimiento del cronograma, insistiendo en la necesidad de un plan de trabajo actualizado con fechas reales de entrega para poder cumplir con la fecha límite prevista. Incluso, se dejó constancia de que tales solicitudes ya habían sido reiteradas en comités de supervisión sin respuesta satisfactoria del contratista. En conclusión, a partir del análisis del Informe de supervisión de 16 de diciembre de 2022 y los oficios relacionados (Radicados 2022-01-775566, 2023-01-132287, 2023-01-146936, 2023-01-269279, entre otros), queda demostrado que el proveedor presentaba fallas reiterativas en la ejecución de lo contratado.	

La evidencia recopilada por la supervisión registro atrasos en la entrega de ambientes, faltas al cronograma, incumplimiento de entregables técnicos y cancelación injustificada de actividades pactadas. Ante la justificación de que no era procedente iniciar el PAS ya que el proveedor "se ponía" al día con sus obligaciones subsanando eventualmente los retrasos, de modo que una vez superado el presunto incumplimiento y no habría razón para sancionar, se recalca que, el cumplimiento tardío o subsanación posterior no elimina el incumplimiento incurrido ni la potestad sancionatoria de la Entidad. Las medidas sancionatorias en contratación (multas, clausula penal, etc.) existen precisamente para enfrentar al contratista renuente o moroso, incentivándolo a cumplir mediante una consecuencia jurídica adversa. Como ha señalado el Consejo de Estado, la multa contractual es un mecanismo coercitivo ante la tardanza o el incumplimiento parcial del contratista para compelerlo a que se ponga al día con sus obligaciones[6]. Es decir, si el contratista se retaso y luego se puso al día, ello confirma hubo una mora que la sanción buscaba corregir, más no significa que la sanción pierda su fundamento. **Por lo anterior se mantiene la No Conformidad.**	

7. CONCLUSIONES DE LA AUDITORÍA

De la evaluación realizada al proceso Gestión de Infraestructura y Tecnología de la Información, el equipo auditor concluye lo siguiente:

1. Se recomienda generar más conciencia de las Políticas de seguridad de la Información y utilizar los diferentes medios de comunicación (Intranet, Página Web, Correo institucional, fondos de pantalla), dado que se realizó una encuesta a 13 funcionarios de la DTIC y se encontró que el 52% respondió correctamente y el 48% de forma incorrecta... Así mismo, el 77% de los funcionarios indicaron no haber recibido capacitación de las Políticas del Sistema de Gestión de la Información.
2. El avance de la implementación del modelo de seguridad y privacidad de la información (MSPI) – ISO 27001:2022, es el siguiente: En los controles del Anexo A, muestran un avance de

[6] Consejo de Estado Sala de Consulta y Servicio Civil, 11001-03-06-000-2013-00384-00

7. CONCLUSIONES DE LA AUDITORÍA

efectividad del 82% en su gestión y para el ciclo de funcionamiento del modelo de operación PHVA se encuentra en un 66%, esto indica que la Superintendencia de Sociedades aplica los lineamientos del MSPI y se encuentra en proceso de mejora continua.

3. La página Web de la Superintendencia de Sociedades presenta deficiencias en la implementación de los criterios de accesibilidad establecidos en la NTC 5854 y la Resolución 1519 de 2020, lo que limita la usabilidad y el acceso a la información por parte de la ciudadanía, especialmente para personas con discapacidad.

Asimismo, el incumplimiento de los estándares de publicación y divulgación de información afecta la transparencia y disponibilidad de los contenidos oficiales, lo que puede generar dificultades en la consulta y el acceso a información clave para los usuarios.

Es fundamental que la Entidad adopte medidas correctivas para garantizar el cumplimiento de la normativa vigente, promoviendo una plataforma digital accesible, inclusiva y alineada con los principios de accesibilidad y gobierno digital.

4. El proceso de contratación de la Orden de Compra 72658 se adelantó adecuadamente.

5. El flujo de notificaciones administrativas de GeDeSS refleja los pasos clave que se detallan en el procedimiento ATC-PR-005_Notifiaciones administrativas que reposa en el SGI.

6. El proyecto de modernización del gestor documental de la Entidad se encuentra alineado con la Política Nacional para la Transformación Digital de la que trata el documento CONPES 3975 de 2019.

7. La orden de compra 72658 del 2021 termino el día 30 de septiembre, celebrando un informe de ejecución del 21 de noviembre de 2024 bajo el radicado 2024-01-912-988 y el Acta de terminación del 9 de diciembre de 2024 mediante radicado 2024-938742.

8. Si bien es cierto que se retira la observación número 6, es recomendable recordar que, el que la mutabilidad de los contratos estatales sea posible no significa que pueda llevarse a cabo por la mera voluntad de las partes o de la entidad contratante; por el contrario, la modificación del contrato debe ser excepcional en virtud de los principios de planeación y seguridad jurídica.

9. Es necesario en un tiempo razonable y especifico revisar y optimizar las acciones necesarias que propendan por el adecuado funcionamiento de la totalidad de los requerimientos funcionales y no funcionales contenidos en el documento RFQ Instrumento de Agregación por Demanda CCE-116-IAD-2020 Catálogo de Productos IBM que hace parte de la Orden de Compra No. 72658 del 2021.

10. Dada la complejidad y extensión del proyecto de GeDeSS, se requiere realizar una auditoría especial por parte de un grupo interdisciplinario de auditores que cuente con profesionales que verifiquen y evalúen técnicamente la ejecución del proyecto, el aspecto legal y el desarrollo financiero de la orden de compra 72658 del año 2021. De igual manera, esta auditoría especial requiere un término de ejecución mayor al de la presente auditoría y el grupo de auditores debe

7. CONCLUSIONES DE LA AUDITORÍA

ser diferente del equipo actual que actúa de manera imparcial en la verificación y evaluación del proyecto.

11. Se evaluó la conformidad de los requisitos 7.3, 9.1, 10.1 y 10.3 del Sistema de Gestión de la Calidad, Norma NTC – ISO 9001:2015 y se declara conforme.

12. Se evaluó la conformidad de los requisitos 4.1, 4.2, 4.3, 4.4, 5.3, 6.2, 6.3, 7.1, 7.3, 7.4, 8.1, 8.2. Así como los Controles del Anexo A: A.5.7, A.5.14, A.5.23, A.5.29, A.6.6, A.7.4, A.7.9, A.7.10, A.8.1, A.8.10, A.8.11, A.8.12, A.8.13, A.8.23, A.8.24, A.8.28, de la norma NTC ISO 27001:2022, encontrándose conformes. No obstante, se identificaron ocho (8) no conformidades que corresponden a los requisitos 5.1 Liderazgo y Compromiso, 5.2 Política, 6.1 Acciones para abordar los riesgos y las oportunidades, 7.5 Control de la documentación, 9.3 Revisión por la dirección, 8.3 Tratamiento de los Riesgos de la Seguridad de la Información, 10.2 No Conformidades y Acciones Correctivas; Trece (13) no conformidades que corresponden a los Controles A.5.1 Políticas de seguridad de la información, A.5.8 Seguridad de la información en la gestión de proyectos, A.5.9 Inventario de información y otros activos asociados, A.5.10 Uso aceptable de la información y otros activos asociados, A.5.15 Control de acceso, A.5.20 Abordar la seguridad de la información dentro de los acuerdos con proveedores, A.5.27 Aprender de los incidentes de seguridad de la información, A.5.30 Preparación de las TIC para la continuidad de negocio, A.8.4 Acceso al Código Fuente, A.8.9 Gestión de la Configuración, A.8.29 Pruebas de seguridad en el desarrollo y aceptación, A.8.30 Desarrollo externalizado, A.8.32 Gestión del cambio y una (1) observación que refiere al control A.8.16 Actividades de seguimiento, los cuales requieren la estructuración de acciones de mejora.

Con respecto al Control A.5.7 Gestión de Inteligencia de Amenazas, si bien la Entidad dispone de un firewall de nueva generación que realiza inteligencia de amenazas, facilitando su revisión, identificación e incluso la generación de acciones de mitigación. Asimismo, cuenta con herramientas como Microsoft Defender para la detección de nuevas vulnerabilidades y el Analyzer para la correlación de eventos en la red. Herramientas que permiten obtener información relevante, contextual y reveladora, lo que contribuye a la mitigación de amenazas y a una mejor toma de decisiones. Sin embargo, se debe considerar la consolidación de la gestión de todas estas herramientas y se documenten las fuentes de amenazas tanto internas como externas, manera que permita la toma decisiones más informadas para mitigar posibles ataques.

13. Se evaluó la conformidad de los requisitos 7.3, 8.1 y 10.3, de la norma NTC ISO 14001:2015, Sistema de Gestión Ambiental, encontrándose una No conformidad en el numeral 7.3. Toma de conciencia, el requisito 8.1. Control Operacional, no es aplicable al proceso y el requisito 10.3. Mejora Continua es conforme, porque no hay hallazgos reincidentes.

14. El Programa de Auditoria fue modificado así:

7. CONCLUSIONES DE LA AUDITORÍA

- Se prorrogo el trabajo de campo hasta el día 21 de marzo de 2025, como consecuencia de realizar la entrevista realizada al ordenador del gasto de la OC 72658 de 2021, por lo que la fecha para la elaboración del informe preliminar fue establecida para el 25 marzo.
- La comunicación de resultados se llevó a cabo los días 26 y 27 de marzo, por la extensión del informe preliminar de auditoría.
- Mediante radicado No. 2025-01-131387 del 28 de marzo de 2025, la DTIC solicito la ampliación del término para presentar observaciones y evidencias al informe preliminar de auditoría hasta el 1 de abril de 2025.
- Mediante radicado No 2025-01-134879 del 31 de marzo de 2025, la DTIC presento la respuesta al Informe de auditoría Interna.
- El 4 de marzo de 2025, se realizó la reunión de cierre de la Auditoría al Proceso de Gestión de Infraestructura y Tecnologías de Información y queda el informe en firme.

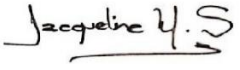
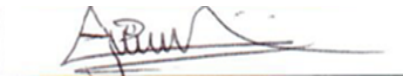
15. En atención a la solicitud del 31 de marzo de 2025 de la Dirección de Tecnología de la Información y las Comunicaciones (DTIC) referente al informe de auditoría preliminar N. 1, el equipo auditor, tras la evaluación de las evidencias presentadas, ha decidido mantener algunas observaciones y no conformidades previamente identificadas, mientras que otras han sido eliminadas, constituyendo el conjunto de resultados definitivos que integran el presente informe de auditoría.

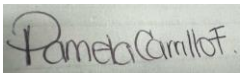
16. Atendiendo la solicitud del 31 de marzo de 2025 de la Dirección de Tecnología de la Información y las Comunicaciones (DTIC) sobre las observaciones y no conformidades, se programó la Reunión de Cierre de Auditoría para el día 4 de marzo de 2025, reunión en la cual se presenta el informe final de auditoría que contiene los hallazgos, las respuestas del auditado y las consideraciones de la OCI respecto de estas.

En conclusión, se identificaron once (11) Observaciones y treinta y una (31) No conformidades, que requieren la estructuración de acciones preventivas y correctivas que permitan garantizar el aseguramiento y mejora continua del proceso y la madurez del Sistema de Gestión Integrado, el Sistema de Control Interno y la Gestión Institucional.

Para constancia se firma en Bogotá D.C., a los 4 días del mes de abril del año 2025

8. RESPONSABLES INFORME DE AUDITORÍA

Nombre Completo	Responsabilidad	Firma
Jacqueline Murillo Sánchez	Jefe Oficina de Control Interno	
Miguel Darío Quintana Sánchez	Auditor Líder	

8. RESPONSABLES INFORME DE AUDITORÍA		
Nombre Completo	**Responsabilidad**	**Firma**
Rocío Pedrozo Ulloa	Auditor	
Nini Sayury Cruz Toloza	Auditor	
Victor Romero Ballesteros	Auditor	
Diana Paola Aguasaco Munevar	Auditor	
Pamela Johana Carrillo Figueroa	Auditor	
Johana Patricia Reyes Acosta	Auditor	
Doris Yaneth Torres Garzon	Auditor	El funcionario se encuentra en vacaciones
Carlos Fernando Rey Riveros	Auditor	

9. ANEXOS
Las listas de verificación, muestras evaluadas, papeles de trabajo y evidencias del trabajo auditor, se adjuntan en el aplicativo de Riesgos y Auditoria.