Bogotá D.C, jueves 30 de mayo de 2024

PARA: Néstor Julián Rosas González
Subdirector de Gestión Corporativa

DE: Angélica Hernández Rodríguez
, Oficina de Control Interno

ASUNTO: Entrega Informe Definitivo Auditoria Proceso TIC

Respetado Doctor:

La Oficina de Control Interno en el rol de evaluación y seguimiento, hace entrega del Informe de Auditoría Interna al Proceso de Gestión TIC, resaltando que el informe preliminar se socializó en reunión de cierre el 23 de mayo de 2024 y se recibió respuesta por parte del equipo auditado el 28 de mayo 2024 (Radicado Orfeo 20242000052303).

Respecto a las conclusiones de la auditoría, se recomienda realizar la divulgación del informe y elaborar el plan de mejoramiento de acuerdo con los procedimientos vigentes. Cabe señalar que en caso de requerir la Oficina de Control Interno puede realizar asesoría metodológica para formular el plan de mejoramiento.

De conformidad con lo establecido en la Ley 1712 de 2014, Arts. 9, lit d) y 11, lit e), el informe en mención será publicado en la página web institucional, sección transparencia – Informes de Control Interno.

Cordialmente,

Angélica Hernández Rodríguez
Jefe Oficina Control Interno.

c/c. Blanca Andrea Sánchez Duarte – Directora General
Iván Dario Morales Caicedo - Subdirector para la Gestión del Centro de Bogotá
Daniela Jiménez – Subdirectora Artístico y Cultural
Yeimi Tatiana Osorio Galindo – Jefe Oficina Jurídica
Luz Mery Ponguta – Jefe Oficina Asesora de Planeación
*Comité Institucional de Coordinación de Control Interno

Documento 20241100053533 firmado electrónicamente por:

Angélica Hernández Rodríguez
Oficina de Control Interno
Fecha firma: 30-05-2024 12:39:40
Fecha firma: 30-05-2024 12:39:40

Aprobó:
Maria Janneth Romero - Contratista - Oficina de Control Interno

97e3752778895a1c3bed19dd5231fd570a6474b28a7995a3b507f5b75d9dca7f
Codigo de Verificación CV: 1c809

INFORME DE AUDITORÍA

Radicado: **20241100053543**
Fecha: 30-05-2024

FECHA DE EMISIÓN DEL INFORME	**Día:**	30	**Mes:**	05	**Año:**	2024

Proceso:	Gestión TIC.
Líder de Proceso / Responsable Operativo Auditado:	Néstor Julián Rosas González.
Objetivo de la Auditoría:	Verificar el diseño y ejecución de los controles que garantizan el cumplimiento de los requisitos internos y externos asociados a la gestión del proceso de Gestión TIC en cumplimiento de la misionalidad de la Entidad.
Alcance de la Auditoría:	Actividades realizadas entre el 01/01/2023 y el 31/12/2023 del Proceso de Gestión TIC, en el marco de la documentación vigente.
Criterios de la Auditoría:	Externa: • Constitución Política de Colombia 1991. • Decreto 1083 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública. • Decreto 1008 de 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones. • NTC-ISO 27001:2013. (ISO 27001:2022) • Modelo de Seguridad y Privacidad de la Información MSPI. Interna: • Guía metodológica de gestión de activos de información. (GT-GU-01 Versión 4). • Política Seguridad de la Información (GT-PO-01 Versión 3). • Política Tratamiento de datos personales (GT-PO-02 Versión 1). • Procedimiento Actualización del Plan Estratégico de Tecnologías de Información y Las Comunicaciones (GT-PD-01 Versión 1). • Procedimiento Gestión de soluciones y servicios de tecnología -Mesa de ayuda (GT-PD-02 Versión 3). • Procedimiento Gestión de soluciones y servicios de tecnologías y MTO. (GT-PD-03 Versión 2). • Procedimiento Asignación de cuentas (GT-PD-04 Versión 4). • Procedimiento Respaldo de la información (GT-PD-05 Versión 3). • Procedimiento Implementación de soluciones y servicios de Tecnología (GT-PD-06 Versión 2). • Procedimiento Operaciones del centro de datos (GT-PD-07 Versión 2).

	• Procedimiento Sistemas Operativos de Servidores – Estaciones (GT-PD-08 Versión 2). • Procedimiento Gestión de incidentes, amenazas y debilidades de seguridad (GT-PD-09 Versión 2). • Procedimiento Seguridad de redes (GT-PD-10 Versión 2). • Procedimiento Consulta, actualización, revocación y supresión de datos personales (GT-PD-11 Versión 2). • Procedimiento Registro y actualización base de datos personales ante la SIC (GT-PD-12 Versión 2). Y las demás normas vinculadas a la gestión evaluada.

Reunión de Apertura						**Ejecución de la Auditoría**				**Reunión de Cierre**					
Día	21	**Mes**	02	**Año**	2024	**Desde**	01/02/2024 D / M / A	**Hasta**	31/05/2024 D / M / A	**Día**	23	**Mes**	05	**Año**	24

Jefe Oficina de Control Interno	**Equipo Auditor**
ANGÉLICA HERNÁNDEZ RODRÍGUEZ	MARIA JANNETH ROMERO MARTÍNEZ LAURA JULIANA FANDIÑO CUBILLOS

DESARROLLO DE ACTIVIDADES:

La Oficina de Control Interno de conformidad con el Plan Anual de Auditorías Internas versión 1 aprobada en Comité Institucional de Coordinación de Control Interno (CICCI) – Comité Directivo, del 27 de diciembre de 2023 y sus posteriores modificaciones: Versión 2 aprobada el 21 de marzo del 2024 y versión 3 del 29 de abril de 2024; realizó la reunión de apertura de la Auditoria al Proceso de Gestión TIC el día 21 de febrero de 2024 y presentó el Plan de Auditoria, el cual fue aceptado en su totalidad por el equipo auditado. El cronograma se desarrolló entre el 01 de febrero y el 23 de mayo de 2024, como se relaciona a continuación:

INFORME DE AUDITORÍA

Radicado: **20241100053543**
Fecha: 30-05-2024

ITEM	ACTIVIDAD DE AUDITORIA	AUDITOR RESPONSABLE	CRONOGRAMA
			FEBRERO / MARZO / ABRIL / MAYO
1	PLANEACIÓN	Auditores OCI	
2	REUNIÓN DE APERTURA	Auditores OCI	
3	SOLICITUD DE INFORMACION TENIENDO EN CUENTA EL OBJETO Y ALCANCE DEFINIDOS	Auditores OCI	
4	DETERMINACIÓN DE LA MUESTRA DE AUDITORIA	Auditores OCI	
5	DISEÑO DE PAPELES DE TRABAJO y PRUEBAS DE AUDITORIA	Auditores OCI	
6	APLICACIÓN DE PRUEBAS DE AUDITORIA (Entrevistas, trabajo in situ, revisión documental)	Auditores OCI	
7	ANALISIS Y EVALUACION DE DATOS	Auditores OCI	
8	ELABORAR INFORME PRELIMINAR	Auditores OCI	
9	REUNION DE CIERRE - PRESENTACIÓN DE RESULTADOS (INFORME PRELIMINAR)	Auditores OCI	
10	ACTIVIDADES DE REVISIÓN	Auditores OCI	
11	PRESENTACIÓN DEL INFORME DEFINITIVO	Auditores OCI	

En reunión de cierre llevada a cabo el día 23 de mayo del año en curso, se presentó el informe preliminar de auditoría; frente al cual, el equipo auditado en cabeza del líder de proceso, manifestó que acepta de conformidad un hallazgo. En la respuesta dada por el proceso a través de radicado 20242000052303 de fecha 28/05/2024, se aceptaron 4 de los hallazgos expuestos (1, 2, 3, y 4). Una vez evaluada la respuesta del proceso auditado, se retira el hallazgo 5 (Ver cuadro resumen de hallazgos informe final).

FORTALEZAS:

- ✓ Disposición, cordialidad y apoyo del equipo de auditado para atender las entrevistas de auditoría y visitas in situ.
- ✓ La disposición del equipo auditado para implementar el esquema de auditoria remota a través de las herramientas tecnológicas brindadas por la entidad; la aplicación de listas de verificación, entrevistas y reuniones virtuales a través de Google Meet cuando fue necesario.
- ✓ La gestión adelantada frente a la formulación del PETI 2023, cuyo contenido y estructura atiende las recomendaciones de MINTIC[1].
- ✓ El ejercicio realizado frente a la validación del Catálogo de Servicios de TI; el cual, en términos generales se ajusta a los lineamientos establecidos por MINTIC[2].
- ✓ Si bien se presentan oportunidades de mejora en algunos temas evaluados, se resalta la experticia del equipo auditado y los avances evidenciados en la gestión del proceso que respalda la operación tecnológica de la entidad.

[1] G.ES.06 Guía Cómo Estructurar el Plan Estratégico de Tecnologías de la Información – PETI de MINTIC

[2] Guía MINTIC: ¿Cómo construir un Catálogo de Servicios de T.I.?

- ✓ La implementación por parte del proceso auditado, de varias de las recomendaciones realizadas en el desarrollo de la auditoria en la vigencia 2020, que coadyuvo al avance en el nivel de implementación del MSPI.
- ✓ La gestión adelantada para la implementación del Plan y Estrategia de transición de IPv4 a IPv6.
- ✓ La gestión adelantada por gestión de TICs en el desarrollo del aplicativo PANDORA en la FUGA.
- ✓ Articulación del equipo auditor y el equipo auditado en entrevistas, generando dentro del rol de evaluación de la OCI la oportunidad de desarrollar actividades de asesoría frente a lo evidenciado.

OPORTUNIDADES DE MEJORA Y OBSERVACIONES:

De acuerdo con las técnicas de auditoría aplicadas en el desarrollo del presente ejercicio, cuyos procedimientos se fundamentan en consultas, inspección, rastreo, procedimientos analíticos y confirmación; se definieron y articularon los criterios evaluados, sobre los cuales a continuación se presentan los aspectos más relevantes evidenciados por el equipo auditor:

1. Plan Estratégico de Tecnologías de Información - PETI

De acuerdo a la información del anexo 2 del radicado 20232900132263 aportado por el proceso auditado, se observa:

1.1. Formulación:

Presentación y aprobación ante el Comité Directivo: Se evidencia cumplimiento en la sesión del 30/01/2023 del Comité Directivo (Acta radicado Orfeo No. 20231200029023).

El acta señala que el PETI contiene adicionalmente los planes complementarios de:

- Plan de Seguridad y Privacidad de la Información;
- Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información;
- Plan de comunicaciones seguridad de la información;
- Cronograma de mantenimiento preventivo y correctivo de los dispositivos tecnológicos.

Se indica en el PETI que los anteriores planes administrados por el proceso TIC se integran a éste en cumplimiento del Decreto 612 de 2018.

De acuerdo a lo expuesto anteriormente, se verifica el plan operativo del PETI, observándo acciones en los componentes del Plan de Seguridad y Privacidad de la Información, Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – PTRSP, Plan de Comunicación de Seguridad y Privacidad de la Información e Infraestructura y Servicios Tecnológicos, en este último integrados al Cronograma de mantenimiento. La evaluación de su ejecución se desarrolla en el presente informe en el ítem 1.2.

En la sesión se aprobó el PETI 2023, sin comentarios sobre el documento presentado.

Contenido y estructura: Se valida el documento *Plan Estratégico Tecnologías de la Información PETI* de fecha enero 2023 aportado como evidencia, cuyo contenido se ajusta a los requerimientos establecidos en la guía técnica *G.ES.06 Guía Cómo Estructurar el Plan Estratégico de Tecnologías de la Información - PETI* de MINTIC en su versión 1.0., incluyendo los siguientes componentes:

- Estrategia de TI.
- Gobierno de TI.
- Análisis de información.
- Sistemas de Información.
- Gestión de servicios tecnológicos, apropiación y uso.

Se observa que se desagregan cada uno de los temas referidos en la guía y su desarrollo se ajusta a lo dispuesto en la misma.

Publicación en la página web: Conforme lo establecido en el Decreto 612 de 2018[3], se observa que se dio cumplimiento al plazo señalado para su publicación (31 de enero de cada año)[4].

1.2. Ejecución:

Se observa que las actividades del Plan Estratégico de Tecnologías de Información y Comunicaciones (PETI), se formulan en el documento *pn-ftpl-06_plan_de_accion_para_la_formulacion_seguimiento_y_monitoreo_planes_institucionales_y_estrategicos_v5_28092023*, en el cual se registran 8 acciones, así:

Ítem Act.	Actividad	Componente
1	Mantenimientos dispositivos tecnológicos.	Infraestructura y Servicios tecnológicos
2	Adquisición de licenciamiento para la entidad.	Infraestructura y Servicios Tecnológicos
3	Implementación política de Gobierno Digital.	Transformación Digital
4	Fortalecimiento sistema gestión documental ORFEO.	Desarrollo de SI apoyo
5	Implementación módulos Pandora.	Desarrollo de SI apoyo
6	Realizar medición MSPI de acuerdo a los controles mínimos de la norma y establecer un rango de Apropiación de acuerdo al resultado.	Plan de Seguridad y Privacidad de la Información

[3] Decreto 612 de 2018 por medio del cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del estado, Artículo 1. Adicionar al Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, los siguientes artículos: "2.2.22.3.14. Integración de los planes institucionales y estratégicos al Plan de Acción. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año: 10. Plan Estratégico de Tecnologías de la Información y las Comunicaciones -- PETI. PARÁGRAFO 1. … Cuando se trate de planes de duración superior a un (1) año, se integrarán al Plan de Acción las actividades que correspondan a la respectiva anualidad. (Subrayado fuera de texto).

[4] https://fu8ga.gov.co/transparencia-y-acceso-a-la-informacion-publica/planeacion-presupuesto-informes/plan-tecnologias-de-la-informacion?field_fecha_de_emision_value=All&term_node_tid_depth=285

7	• Proteger del Acceso no autorizado a la información. • Blindar a la entidad de Ataques Externos o internos. • Proteger los activos de información contra el Daño de la información. • Proteger a la entidad de un ataque de Denegación del servicio	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información - PTRSP
8	Realizar piezas de comunicación	Plan de Comunicación de Seguridad y Privacidad de la Información.

Fuente: *pn-ftpl-06_plan_de_accion_para_la_formulacion_seguimiento_y_monitoreo_planes_institucionales_y_estrategicos_v5_28092023*

El resultado de la evaluación de la ejecución del PETI se presentó por la OCI en los siguientes informes:

Informes Vinculados	Fecha de Presentación	Radicado Orfeo
Informe de Seguimiento y Recomendaciones orientadas al cumplimiento de las Metas Plan Desarrollo a cargo de la entidad a septiembre de 2023	30/11/2023	20231100123153
Informe Anual de Verificación, Recomendaciones, Seguimiento y Resultado sobre el Cumplimiento de las Normas en Materia de Derecho de Autor sobre Software 2023.	14/03/2024	20241100026783

Fuente: Expedientes 20231100310040001 y 20241100310040001 – Informes Oficina de Control Interno 2023 y 2024 respectivamente

Acción 1: *Mantenimientos dispositivos tecnológicos:*

Acción evaluada en los dos informes. Teniendo en cuenta que los resultados ya fueron socializados por la OCI, se presenta resumen de lo observado:

a. La ejecución del plan es monitoreada y controlada por el proceso auditado a través del *Cronograma y Seguimiento de Mantenimiento Infraestructura Física y de Tecnología de la Información (GTI-FT-98),* el cual incluye:

- Actividades preventivas: Verificación Antivirus, Mantenimiento Software Básico, Lector de Huellas, Lectores de barras y escáner, Equipos de cómputo (Preventivo - Fallas Incidencias mayores)
- Actividades correctivas: UPS y aire acondicionado, impresoras, dispositivos de Red, Servidores, equipos de Cómputo (Corrección fallas de acuerdo a requerimiento o necesidad del Servicio)
- Actividades predictivas; Software planta telefonía, software teléfonos, actualización software y Revisión de hardware y software de dispositivos TI red (Switches, Access Paint, firewall)

b. Conforme lo reportado por el proceso, el cronograma 2023 se ejecutó al 100%; sin embargo, en las evaluaciones realizadas por la OCI[5], se observaron oportunidades de mejora relacionadas con algunos productos entregables establecidos en el plan operativo:

- Los soportes que dan cuenta de la ejecución no permiten en todos los casos, identificar la fecha o periodo en que se ejecuta.

[5] Informe Anual de Verificación, Recomendaciones, Seguimiento y Resultado sobre el Cumplimiento de las Normas en Materia de Derecho de Autor sobre Software 2023. Páginas 10 a 12 (https://www.fuga.gov.co/transparencia-y-acceso-a-la-informacion-publica/planeacion-presupuesto-informes?field_fecha_de_emision_value=All&term_node_tid_depth=269)

- No se evidencia en algunas actividades, un soporte que identifique la gestión realizada para cada periodo establecido en el cronograma.
- En algunos casos no se evidencia la articulación entre el soporte y la acción.

Acción 2: *Adquisición de licenciamiento para la entidad*:

Acción evaluada en los dos informes relacionados; se presenta el resumen de lo observado:

a. Renovación y/o adquisición de licencias:

- Renovación de licencias Google (Contrato FUGA-107-2023 – Xertica Colombia S.A.S).
- Renovación de licencias Creative Cloud. (Contrato FUGA-104-2023 - Panamericana Librería y Papelería S.A).
- Renovación de Licenciamiento AutoCAD. (Contrato FUGA-105-2023 - Panamericana Librería y Papelería S.A).
- Renovación Licencias ENDPOINTS - SOPHOS - CIXH3CTAA. (Contrato FUGA-127-2023 – Insitel S.A).
- Renovación Licencias FIREWALL - SOPHOS, XG-210. (Contrato FUGA-127-2023 – Insitel S.A).
- Adquisición Licencias AWS CLOUD. (Contrato FUGA-127-2023 – Insitel S.A).
- Adquisición Licencia Power BI Pro. (Contrato FUGA-127-2023 – Insitel S.A).

b. Adición y prorroga de los contratos:

- FUGA-170-2021 (Renovación hosting página web)
- FUGA-48-2021 (Servicio de internet para las sedes de la Fundación - ETB)

Se recoge la observación realizada en el *Informe Anual de Verificación, Recomendaciones, Seguimiento y Resultado sobre el Cumplimiento de las Normas en Materia de Derecho de Autor sobre Software 2023*, relacionada con la articulación de la información registrada en los inventarios de TIC y de Recursos Físicos, de tal manera que la misma sea coherente y corresponda a la ejecución de las obligaciones contractuales del Contrato FUGA-127-2023: Licencia de SOPHOS ENDPOINT AGE[6].

Conforme lo anterior, si bien se evidenciaron oportunidades de mejora de forma, se da cumplimiento a la acción y los soportes corresponden a los productos entregables establecidos en el plan operativo.

Acción 3: *Implementación política de Gobierno Digital:*

[6] Informe Anual de Verificación, Recomendaciones, Seguimiento y Resultado sobre el Cumplimiento de las Normas en Materia de Derecho de Autor sobre Software 2023. Páginas 8 y 9 (https://www.fuga.gov.co/transparencia-y-acceso-a-la-informacion-publica/planeacion-presupuesto-informes?field_fecha_de_emision_value=All&term_node_tid_depth=269)

Acción evaluada en el primer informe relacionado en la tabla de *Informes Vinculados*, con ejecución al corte de III Trimestre de la vigencia[7]; resultado que se articula con la evaluación del IV Trimestre realizada en este ejercicio de auditoría, así:

La implementación de la política, conforme lo observado en la matriz *Medición Meta Política gobierno digital diciembre*, comprende:

- Medir y evaluar el PETI trimestralmente: Se cumple conforme lo observado en la ruta del servidor en el proyecto de inversión 7760[8] y en los soportes allegados como evidencia en la auditoría (Radicado Orfeo 20242900020873).

- Validar catálogos de servicios TI y medir los indicadores de proceso: La evidencia aportada corresponde a la gestión de monitoreo tanto a la matriz de riesgos como de los indicadores del proceso.

Frente a los indicadores se observan 4 formatos *Fichas Técnicas Indicador*, correspondientes a: i. Porcentaje de disponibilidad de la infraestructura tecnológica proporcionada por la entidad; ii. Porcentaje de implementación de controles asociados al Modelo de Sistema de Gestión de Seguridad de la información MSPI; iii. Porcentaje de mantenimiento de infraestructura tecnológica; y iv. Porcentaje de atención oportuna de requerimientos; el resultado de la medición al cierre de la vigencia muestra que los 3 primeros tienen una condición satisfactoria, en tanto que el indicador de atención oportuna de requerimientos tiene una condición normal en su medición.

Respecto a la validación de los catálogos de servicios TI, se observa la gestión adelanta a través de la *Plantilla Servicios de TI-Pred-fuga* aportada como evidencia, en la cual se identifican los siguientes servicios:

Nombre del servicio	Descripción
Mesa de ayuda	Aplica a las todas las áreas de la Fundación Gilberto Álzate Avendaño en temas relacionados con la solicitud de incidentes y/o requerimientos.
Correo Electrónico	Correo Electrónico.
Unidades de Red	Repositorio de información de cada una de los funcionarios de la Fundación Gilberto Álzate Avendaño para que sea consultada por los funcionarios. Esta información reside en discos que hacen parte de un sistema de almacenamiento en red tipo NAS (Network Access serve). El acceso a cada una de las carpetas se realiza a través perfiles de acceso de lectura o escritura.
Bases de datos	La información almacenada en las bases de datos es el pilar de los sistemas de información estos pueden ser de uso misional o administrativo dada su importancia se utilizan herramientas de administración, optimización donde se garantiza su respaldo y una continua operación para garantizar su operación.
Servidores	Los servidores configurados en los cuales residen bases de datos, aplicativos misionales y administrativos, para la correcta entrega de insumo para desempeñar las labores de los funcionarios de la entidad.

[7] Informe de Seguimiento y Recomendaciones orientadas al cumplimiento de las Metas Plan Desarrollo a cargo de la entidad a septiembre de 2023. Página 7 (https://www.fuga.gov.co/transparencia-y-acceso-a-la-informacion-publica/planeacion-presupuesto-informes?field_fecha_de_emision_value=All&term_node_tid_depth=265)

[8] \\192.168.0.34\Seg Proyectos de Inversion PDD-UNCSAB 2020-2024\2023\Sub_Corporativa\7760_Modernización_arquitectura_institucional\Meta_3_Política_Gobierno_Digital

Respaldo	Servicio de ejecución y almacenamiento para resguardar la información relevante de la entidad con fines de tener respaldo de la información.
Internet	El servicio de Internet facilita al usuario, a través de la red de la Fundación Gilberto Álzate, el envío y recepción de información desde y hacia fuera de la entidad, a través de un navegador.
Sistemas de Informació	Ofrecer al usuario la asesoría para el levantamiento de los requerimientos funcionales, técnicos y financieros hasta la puesta en marcha, velando que el desarrollo cumpla con las políticas establecidas por el Área de TIC de la Fundación Gilberto Álzate.
Servicio VPN	Servicio que permite la conexión segura y confiable a la red interna a través de internet.
Servicio RED	Servicio que permite la interacción de datos en las sedes con respecto a la infraestructura interna como servidores, switches y equipos de cómputo de la entidad.
Servicio de telefonía voz	Servicio que permite la interacción de la voz sobre dispositivos de RED dispuestos para ello.

Fuente: *Plantilla Servicios de TI-Pred-fuga*

La plantilla incluye hojas por cada servicio donde se identifican objetivo, características, alcance, canal de suministro, a quien va dirigido e indicador, lo cual se encuentra articulado con la guía de MINTIC *¿Cómo construir un Catálogo de Servicios de T.I.?*[9]

- Emitir fichas técnicas y/o justificaciones para EP relacionados con la adquisición de bienes tecnológicos: La evidencia corresponde a los estudios previos o justificaciones técnicas realizados en la gestión precontractual de los procesos:

No. de Contrato	Descripción	No. Expediente
FUGA-104-2023	Renovación de licencias Creative Cloud.	202313002000900120E
FUGA-105-2023	Renovación de Licenciamiento AutoCAD.	202313002000900121E
FUGA-107-2023	Renovación de licencias Google.	202313002000900109E
FUGA-127-2023	Renovación Licencias ENDPOINTS - SOPHOS - CIXH3CTAA, FIREWALL - SOPHOS, XG-210, AWS CLOUD y Power BI Pro	202313002000900110E

Fuente: Orfeo Dependencia 130 - Oficina Jurídica – Serie y subserie: Contratos – Año de Creación: 2023

- Elaborar informe relacionado con la implementación del plan de mantenimiento y administración de la infraestructura TIC: Se evidencian los informes presentados en los últimos tres trimestres de la vigencia, en los cuales se presentan los avances de la ejecución del *Cronograma y Seguimiento de Mantenimiento Infraestructura Física y de Tecnología de la Información (GTI-FT-98).* Es importante señalar que la matriz de medición aportada como evidencia tiene programada la presentación de 4 informes en la vigencia, uno cada trimestre; no obstante, no se evidencia el informe del I trimestre.

- Actualizar la documentación relacionada con Gestión TIC conforme con la realidad institucional y de acuerdo con las necesidades que se detecten e incluirlo en el SIG: De la verificación realizada a los documentos SIG publicados en la intranet y pagina web de la entidad, se observa que, en 2023 se actualizaron los siguientes:

[9] https://gobiernodigital.mintic.gov.co/692/articles-51982_recurso_4.pdf

Tipo de Documento	Nombre	Código	Versión	Fecha actualización
Política	Seguridad de la Información	GT-PO-01	3	20/11/2023
Procedimiento	Asignación de cuentas	GT-PD-04	4	16/08/2023
Procedimiento	Respaldo de la información	GT-PD-05	3	20/11/2023
Formato	Gestión de usuarios	GT-FT-15	3	27/12/2023

Fuente: http://intranet.fuga.gov.co/proceso-gestion-tic

Adicionalmente en las evidencias aportadas por el proceso se observa la actualización del normograma.

Conforme lo anterior, se evidencia que en términos generales se da cumplimiento a la acción y los soportes corresponden a los productos entregables establecidos en el plan operativo.

Acción 4: *Fortalecimiento sistema gestión documental ORFEO*:

Acción evaluada en el primer informe relacionado en la tabla de *Informes Vinculados*, con ejecución al corte de III Trimestre de la vigencia[10]; resultado que se articula con la evaluación del IV Trimestre realizada en este ejercicio de auditoría, así:

- Esta acción se ejecuta a través del Contrato FUGA-63-2023 Objeto: *Prestar los servicios profesionales a la Fundación Gilberto Alzate Avendaño en el mantenimiento y actualización de las herramientas informáticas del sistema de gestión documental*. En ejecución del contrato se presenta la gestión de los ajustes a los servicios web del API REST del SGDA, la implementación de los nuevos módulos, funcionalidades, servicios y actualización de Orfeo. (Expediente 2023130020009000007E)
- Circular Interna 13 de 2023 *"Implementación actualizaciones en Orfeo*", que incluye los ajustes en el Módulo de inventario documental, módulo de expedientes, servicio de notificaciones, presentación de firmas, anexos, ir a radicado padre, documentos firmados, revisiones, apertura en el navegador, teléfonos móviles, API - Interoperabilidad y Seguridad de implementación de Orfeo.
- Se evidencia en el módulo de inventario documental la gestión relacionada con el FUID.
- En el IV trimestre se aportan como evidencia correos electrónicos entre los cuales se observa la revisión técnica del Modelo de Requisitos SGDA – FUGA -2023, la gestión respecto al desarrollo de las Tablas de Control de Acceso, el Manual para generar actas de anulación en Gestión Documental y el desarrollo en la implementación de la hoja de control (documento Requisitos desarrollos de software historias de usuario); adicionalmente se incluyen: solicitud acceso ambiente de prueba SGDEA-Orfeo de la OAP, publicación de plantillas de respuesta a PQRS en Orfeo y publicación de formatos de Servicio al Ciudadano (Encuesta y aviso para peticiones anónimas en cartelera), con lo cual se documenta el producto entregable del plan operativo "*Soporte y actualización de la herramienta con relación a las posibles incidencias que se presenten sobre la herramienta*".
- No se identifica la gestión adelantada respecto a los "Reportes de TRD" los cuales hacen parte de los entregables registrado en *Plan operativo* del PETI.

[10] Informe de Seguimiento y Recomendaciones orientadas al cumplimiento de las Metas Plan Desarrollo a cargo de la entidad a septiembre de 2023. Página 7. (https://www.fuga.gov.co/transparencia-y-acceso-a-la-informacion-publica/planeacion-presupuesto-informes?field_fecha_de_emision_value=All&term_node_tid_depth=265)

Acción 5: *Implementación módulos Pandora*:

Acción evaluada en el primer informe relacionado en la tabla de *Informes Vinculados*, con ejecución al corte de III Trimestre de la vigencia[11]; resultado que se articula con la evaluación del IV Trimestre realizada en este ejercicio de auditoría, así:

- Esta acción se ejecuta a través del Contrato FUGA-62-2023 Objeto: Prestar los servicios profesionales a la Oficina Asesora de Planeación de la Fundación Gilberto Alzate Avendaño, en el levantamiento de requerimientos, la implementación de desarrollos y la puesta en producción de las funcionalidades del Sistema de Información de Planeación y Gestión Pandora. (Expediente 20231300200090029E).
- Las evidencias aportadas corresponden a los informes presentados por el contratista en ejecución del contrato. En estos se observan: ajustes en formatos para la modificación de proyectos, CDP y CRP, avances en el módulo Plan Distrital de Desarrollo submódulo Plan Estratégico, módulo de indicadores, ajustes en el módulo de Evaluación y Control, mejoras en el módulo de seguimiento de proyectos y generación y programación de Backpus, entre otros.

Respecto al producto entregable del plan operativo *Mantener módulos Seguimiento proyectos de inversión, Control Interno, Indicadores y Sistema de gestió*n, si bien se identifican los soportes que dan cuenta del entregable: "*Mantener los tableros de control para seguimiento a presupuesto, proyectos de inversión":* No se observa la implementación de estos tableros de control para el módulo de Evaluación y Control (*Control interno*).

Acción 6: *Realizar medición MSPI de acuerdo a los controles mínimos de la norma y establecer un rango de Apropiación de acuerdo al resultado*.

La matriz *Instrumento medición 2023* aportada como evidencia, presenta una evaluación de efectividad de controles y avance del ciclo de funcionamiento del modelo de operación PHVA al cierre de la vigencia del 89%.

La evaluación de la ejecución reportada por el proceso auditado, será presentada de manera detallada en este informe de auditoría, en el componente 2. *Estado de implementación del Modelo de Seguridad y Privacidad de la Información -MSPI.*

Acción 7: *Proteger del Acceso no autorizado a la información; Blindar a la entidad de Ataques Externos o internos; Proteger los activos de información contra el Daño de la información; y Proteger a la entidad de un ataque de Denegación del servicio*[12].

[11] Informe de Seguimiento y Recomendaciones orientadas al cumplimiento de las Metas Plan Desarrollo a cargo de la entidad a septiembre de 2023. Página 7. (https://www.fuga.gov.co/transparencia-y-acceso-a-la-informacion-publica/planeacion-presupuesto-informes?field_fecha_de_emision_value=All&term_node_tid_depth=265)

[12] \\192.168.0.34\Seg Proyectos de Inversion PDD-UNCSAB 2020-2024\2023\Sub_Corporativa\7760_Modernización_arquitectura_institucional\Meta_3_Política_Gobierno_Digital\9_Septiembre: Gobierno digital

Acción evaluada en el primer informe relacionado en la tabla de *Informes Vinculados*, con ejecución al corte de III Trimestre de la vigencia[13]; resultado que se articula con la evaluación del IV Trimestre realizada en este ejercicio de auditoría, así:

- La evidencia presentada al corte de septiembre de 2023, corresponde a los paneles de seguridad de SOPHOS de los periodos comprendidos entre el 01/01/2023 al 28/03/2023, el 01/04/2023 al 30/06/2023, el 01/07/2023 al 31/07/2023 y el 01/08/2023 al 31/08/2023. No se aporta evidencia de la gestión realizada en el último trimestre de la vigencia.

- En los paneles de seguridad antes señalados se observa, entre otros reportes:

Reporte 1. Aplicaciones de alto riesgo:

01/01/2023 al 28/03/2023	01/04/2023 al 30/06/2023	01/07/2023 al 31/07/2023	01/08/2023 al 31/08/2023
Torrent Clients P2P	TOR Proxy	Torrent Clients P2P	TOR Proxy
TOR Proxy	Freegate Proxy	Ares P2P	Vuze P2P
VPN Lighter	Ares P2P	TOR Proxy	Torrent Clients P2P
Wireguard	Torrent Clients P2P	ISAKMP VPN	Ares P2P
Ares P2P	ISAKMP VPN	Vuze P2P	SkyVPN

Fuente: PETI\Proteger del Acceso no autorizado a la información\Security dashboard

La posición en la tabla en cada periodo, corresponde a las aplicaciones con mayor número de ataques y de bytes. Se destacan como aplicaciones recurrentes en los 4 reportes: Torrent Clients P2P, TOR Proxy y Ares P2P.

Reporte 7: Categorías Web bloqueadas:

01/01/2023 al 28/03/2023	01/04/2023 al 30/06/2023	01/07/2023 al 31/07/2023	01/08/2023 al 31/08/2023
Games	Games	Games	Games
Sexually Explicit	Gambling	Search Engines	Search Engines
Gambling	Search Engines	Gambling	Gambling
Search Engines	Sexually Explicit	Sexually Explicit	IPAddress
Uncategorized	Information Technology	Sin categoría	Video hosting

Fuente: PETI\Proteger del Acceso no autorizado a la información\Security dashboard

La posición en la tabla en cada periodo, corresponde a las categorías con mayor número de ataques. Se destacan como categorías recurrentes en los 4 reportes: Games, Search Engines, Gambling y Sexualidad Explicit.

septiembre.rar\Gobierno digital septiembre\Medir y evaluar el PETI trimestre II\Proteger del Acceso no autorizado a la información - archivo RAR, tamaño descomprimido 89.626.230 bytes

[13] Informe de Seguimiento y Recomendaciones orientadas al cumplimiento de las Metas Plan Desarrollo a cargo de la entidad a septiembre de 2023. Página 8. (https://www.fuga.gov.co/transparencia-y-acceso-a-la-informacion-publica/planeacion-presupuesto-informes?field_fecha_de_emision_value=All&term_node_tid_depth=265)

Reporte 8. Dominios Web bloqueados:

01/01/2023 al 28/03/2023	01/04/2023 al 30/06/2023	01/07/2023 al 31/07/2023	01/08/2023 al 31/08/2023
x-images2.bangbros.com	dynamicwindows.rushbet.co	onlinecheck.wildtangent.com	onlinecheck.wildtangent.com
ayce.gameloft.com	mobilecrush.king.com	mobilecrush.king.com	mobilecrush.king.com
dynamicwindows.rushbet.co	candycrush4.king.com	west-midas.codm.activision.com	content.garena.com
events.nordeus.com	onlinecheck.wildtangent.com	id.supercell.com	pgorelease.nianticlabs.com
onlinecheck.wildtangent.com	kofg.gcdn.netmarble.com	cdn.outfit7.com	duckduckgo.com

Fuente: PETI\Proteger del Acceso no autorizado a la información\Security dashboard

La posición en la tabla en cada periodo, corresponde a los dominios con mayor número de ataques. Se destacan como dominio recurrente en los 4 reportes: onlinecheck.wildtangent.com.

Reporte 15. Ataques de Intrusión:

Descripción	01/01/2023 al 28/03/2023	01/04/2023 al 30/06/2023	01/07/2023 al 31/07/2023	01/08/2023 al 31/08/2023
MALWARE-CNC User-Agent known malicious user-agent string - Mirai	686	413	172	81
MALWARE-CNC Mirai Botnet Attack Attempt	623	393	160	64
MALWARE-CNC Win.Trojan. ZeroAccess inbound connection	200	19	8	6
MALWARE-CNC Win.Trojan. ZeroAccess outbound connection	20	19	8	6
MALWARE-CNC Win.Trojan. AveMaria variant outbound connection	11	17	5	6

Fuente: PETI\Proteger del Acceso no autorizado a la información\Security dashboard

Los reportes evidenciados están vinculados con el producto establecido en el plan operativo: "*Gestionar y controlar los riesgos asociados a la matriz general de la entidad generando las capturas correspondientes o documentos asociados al adecuado tratamiento*". El seguimiento a la información que se genera en los reportes, se vincula con el control existente para el riesgo de *Seguridad Digital* relacionado con la *Perdida de la Integridad* y que afecta el activo "A*plicaciones de la organización";* en el control se precisa que el soporte es el informe exportado del sistema.

Acción 8: *Realizar piezas de comunicación*:

Acción evaluada en los dos informes relacionados en la tabla de *Informes Vinculados*; en el primero de ellos con la ejecución al corte de III Trimestre de la vigencia[14] y el segundo con la gestión al cierre de la misma[15], integrando los dos resultados, así:

[14] Informe de Seguimiento y Recomendaciones orientadas al cumplimiento de las Metas Plan Desarrollo a cargo de la entidad a septiembre de 2023. Página 8. (https://www.fuga.gov.co/transparencia-y-acceso-a-la-informacion-publica/planeacion-presupuesto-informes?field_fecha_de_emision_value=All&term_node_tid_depth=265)

[15] Informe Anual de Verificación, Recomendaciones, Seguimiento y Resultado sobre el Cumplimiento de las Normas en Materia de Derecho de Autor sobre Software 2023. Página 13 (https://www.fuga.gov.co/sites/default/files/2024-03/Informe%20Derechos%20de%20Autor%20Software%202023%20web.pdf)

La evidencia evaluada corresponde a:

- Pantallazos de la información publicada en la intranet en MIPG – Política de Seguridad Digital
- Presentaciones de la estrategia *"Ernestips*".
- Campaña Phishing – Falabella

En articulación con el resultado del informe de *Derechos de Autor – Software*, se destaca el ejercicio realizado para monitorear el comportamiento de los usuarios frente a ataques tipo phishing y se vincula a este ejercicio la conclusión del equipo TIC frente a la creación de conciencia de todos los colaboradores de la entidad en los temas relacionados con la seguridad de la información.

Conforme lo anterior, se cumple con los productos entregables establecidos en el plan operativo.

En términos generales se observa que la entidad formuló y ejecutó su PETI 2023 de conformidad con los lineamientos internos y externos establecidos; no obstante, teniendo en cuenta las situaciones observadas de manera general se recomienda:

- Documentar de manera integral la ejecución de cada una de las acciones establecidas en el PETI y vincular los soportes con los entregables señalados en el plan operativo del mismo (Acción 1, 3, 4, 5 y 7).
- Revisar el expediente 20231300200090011OE, correspondiente al contrato FUGA-127-2023, por cuanto en la consulta realizada se observó que el expediente indica que corresponde al contrato FUGA-352-2023.

2. Estado de implementación del Modelo de Seguridad y Privacidad de la Información -MSPI (Revisar diagnóstico - Riesgos)

Teniendo en cuenta la información aportada por el proceso auditado en el anexo del radicado 20232900132263 (Instrumento de Identificación de la Línea Base de Seguridad de MINTIC), que incluye el monitoreo con corte diciembre de 2023; se procedió a verificar y validar lo reportado, con el resultado que se presenta a continuación en las columnas de calificación y evaluación OCI:

2.1. Evaluación de Efectividad de Controles (ISO 27001:2013 Anexo A):

No.	Evaluación de Efectividad de controles					
	DOMINIO	Calificación Dic 2023 TIC	Calificación OCI	Calificación Objetivo	Evaluación de efectividad de control tic	Evaluación de efectividad de control - OCI
A.5	Políticas de seguridad de la información	100	80	100	**Optimizado**	Gestionado
A.6	Organización de la seguridad de la información	100	90	100	**Optimizado**	Optimizado
A.7	Seguridad de los recursos humanos	100	80	100	**Optimizado**	Gestionado
A.8	Gestión de activos	98	90	100	**Optimizado**	Optimizado
A.9	Control de acceso	100	82	100	**Optimizado**	Optimizado
A.10	Criptografía	80	80	100	**Gestionado**	Gestionado

A.11	Seguridad física y del entorno	100	77	100	**Optimizado**	Gestionado
A.12	Seguridad de las operaciones	89	66	100	**Optimizado**	Gestionado
A.13	Seguridad de las comunicaciones	88	77	100	**Optimizado**	Gestionado
A.14	Adquisición, desarrollo y mantenimiento de sistemas	96	50	100	**Optimizado**	Efectivo
A.15	Relaciones con los proveedores	70	60	100	**Gestionado**	Efectivo
A.16	Gestión de incidentes de seguridad de la información	80	60	100	**Gestionado**	Efectivo
A.17	Aspectos de seguridad de la información de la gestión de la continuidad del negocio	57	37	100	**Efectivo**	Repetible
A.18	Cumplimiento	94	93	100	**Optimizado**	Optimizado
	PROMEDIO EVALUACIÓN DE CONTROLES	**89**	**73**	100	**Optimizado**	**Gestionado**

Fuente: Instrumento de Identificación de la Línea Base de Seguridad de MINTIC (Corte diciembre 2023) y evaluación propia.

Si bien se observa que de manera general la evaluación se encuentra en clasificación de *Gestionado*[16] *Efectivo*[17] y *Optimizado*[18], es importante que se revise el criterio calificado como *Repetible*[19], de tal manera que se priorice la evaluación, documentación e implementación de los lineamientos, teniendo en cuenta que estos corresponden a los aspectos de seguridad de la información de la gestión de la continuidad del negocio (A.17).

La evaluación de cada uno de los controles de los dominios antes relacionados, puede ser consultada en el *Anexo Instrumento de medición MSPI diciembre 2023,* en los aspectos administrativos y técnicos, el cual hace parte integral del presente informe.

Conforme lo observado en dicho anexo, se presentan de manera general las siguientes observaciones:

Políticas de seguridad de la información (A.5): Si bien la entidad cuenta con el documento Políticas de Seguridad de la Información Código: GT-PO-01 Versión: 3, no se evidencian las directrices relacionadas con el manejo de las desviaciones y excepciones; adicionalmente, se observa en el control de cambios del documento, que no se realiza la revisión y actualización anual conforme lo establece el criterio.

Organización de la seguridad de la información (A.6): Frente la definición de roles y responsabilidades se observa que se definen de manera genérica y no incluyen todos los procesos. No se identifica el colaborador designado por la entidad como Oficial de Seguridad (Resolución Interna 219 de 2023), ni cuáles son sus responsabilidades específicas En la entrevista realizada el 16/05/2024 se indica que, si bien no hay una designación formal, las responsabilidades del oficial están inmersas en las obligaciones específicas del

[16] Instrumento de Identificación de la línea base de seguridad de MINTIC, hoja Escala de Evaluación: **Gestionado**: Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
[17] Instrumento de Identificación de la línea base de seguridad de MINTIC, hoja Escala de Evaluación: **Efectivo:** Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
[18] Instrumento de Identificación de la línea base de seguridad de MINTIC, hoja Escala de Evaluación: **Optimizado**: Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.
[19] Instrumento de Identificación de la línea base de seguridad de MINTIC, hoja Escala de Evaluación: **Repetible**: Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.

contratista de apoyo a las actividades del proceso de gestión TIC de la entidad, en lo relacionado con el componente tecnológico y la gestión del PETI.

De acuerdo al resultado de la verificación del cumplimiento normativo interno, el equipo auditor genera un hallazgo pues no se evidencia la designación del Oficial de Seguridad para la entidad. Este hallazgo se vincula en la tabla de hallazgos con la designación del Responsable de la Seguridad de la Información en la entidad.

Respecto al *Contacto con las autoridades* se observa que, si bien se tienen reportes GPLI con el registro de los incidentes presentados, estos no permiten identificar de manera clara su impacto, ni las acciones implementadas para solucionarlos conforme se establece en las *Políticas de Seguridad de la Información GT-PO-01* y el procedimiento *Gestión de Incidentes, Amenazas y Debilidades de Seguridad GT-PD-09*.

Si bien se identifica la implementación de controles respecto a los proyectos del proceso TIC, no se identifica cómo se integra la seguridad de la información en el ciclo de vida de los proyectos de procesos diferentes al auditado.

Seguridad de los recursos humanos (A.7): Se evidencia el cumplimiento de controles respecto a la investigación de antecedentes, términos y condiciones del empleo, responsabilidades de la dirección y capacitaciones en materia de seguridad de la información; sin embargo, no se evidencian acuerdos de confidencialidad en los que se establezca que después de terminada la relación laboral o contractual seguirán vigentes por un periodo, conforme lo señala el criterio.

Gestión de activos (A.8): Se observa que el inventario de activos publicado no se encuentra actualizado y no se identifican las directrices relacionadas con las restricciones de acceso que soportan los requisitos de protección para cada nivel de clasificación, el registro formal de los receptores autorizados de los activos, almacenamiento de los activos de TI de acuerdo con las especificaciones de los fabricantes y el marcado claro de todas las copias de medios para la atención del receptor autorizado, conforme se señala en el criterio A.8.2.3.

Respecto a la protección durante el transporte de medios que contienen información física, si bien se referencia el Contrato con TANDEM, no se identifican los lineamientos de conservación y seguridad de la información durante este proceso.

Control de acceso (A.9): No se identifican las directrices con las cuales se da cumplimiento a todos los criterios relacionados con el control de Requisitos del Negocio para el control de acceso que incluye la política de control de acceso y el acceso a redes y a servicios en la red.

Frente al control de Gestión de Acceso de usuarios, no se evidencia la implementación de todos los criterios vinculados al suministro de acceso de usuarios, gestión de derechos de acceso privilegiado, gestión de información de autenticación secreta de usuarios, revisión de los derechos de acceso de usuarios, retiro o ajuste de los derechos de acceso.

Respecto al control Responsabilidades de los Usuarios, no evidencia el cumplimiento de todos los criterios vinculados a la notificación de usuarios (uso de información de autenticación secreta).

Por último, en cuanto al Control de Acceso a Sistemas y Aplicaciones, en los temas relacionados con procedimientos de ingreso seguro, uso de programas utilitarios privilegiados y control de acceso a códigos fuente de programas, se observan criterios que no tienen lineamientos o directrices documentadas conforme la especificidad señalada en la norma.

Criptografía (A.10): Si bien se establecen en la política lineamientos generales sobre el uso de controles criptográficos, no se identifican directrices que permitan asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información conforme lo señala el control.

Seguridad física y del entorno (A.11): Se observa la implementación de los controles físicos de entrada; sin embargo no se identifican las directrices que permitan implementar integralmente los controles relacionados con el perímetro de seguridad física, seguridad de oficinas, recintos e instalaciones, protección contra amenazas externas y ambientales, trabajo en áreas seguras, prevención de la pérdida, daño, robo o compromiso de activos y la interrupción de las operaciones de la organización.

Seguridad de las operaciones (A.12): En los documentos revisados, no se identifican las directrices con las cuales se implementan los criterios relacionados con: a. los controles que permitan asegurar las operaciones en las instalaciones de procesamiento de información; b. que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos; c. la protección contra pérdida de datos; d. el registro de eventos y la generación de evidencias; e. la integridad de los sistemas operacionales, la prevención del aprovechamiento de vulnerabilidades técnicas; y f. la minimización del impacto de las actividades de auditoría sobre los sistemas operacionales.

Adicionalmente se evidenciaron oportunidades de mejora frente a la gestión documental reportada en el instrumento de medición que no permite verificar la implementación de los criterios evaluados, por cuanto se reportaron procedimientos y manuales sin precisar a cuáles se hace referencia (A.12.1.1, A.12.4.3. A.12.7.1, entre otros)

Seguridad de las comunicaciones (A.13): Frente a las directrices que permitan evaluar la implementación de los criterios relacionados con los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red y su incorporación en los acuerdos de servicios de red, vinculados a la seguridad de los servicios de red, no se identifica donde se encuentran documentadas las especificaciones señaladas en el control. También se evidencian oportunidades de mejora frente a la definición de directrices que permitan mantener la seguridad de la información transferida y la gestión documental que permita validar su implementación.

Adquisición, desarrollo y mantenimiento de sistemas (A.14): No se identifican directrices que permitan asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida, incluidos los requisitos para sistemas de información que prestan servicios en redes

públicas, que esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información y que se asegure la protección de los datos usados para pruebas. Se observan oportunidades de mejora frente a la documentación de la implementación de los criterios vinculados al control.

Relaciones con los proveedores (A.15): Respecto a la implementación de las directrices relacionadas al seguimiento y revisión de cumplimiento de los compromisos vinculados a la seguridad de la información con los proveedores y su periodicidad, no se identifican lineamientos específicos conforme los criterios definidos en el control; tampoco se identifica como se gestionan los cambios en el suministro de servicios por parte de los proveedores (mantenimiento y mejora de las políticas, procedimientos y controles de seguridad de la información existentes), de conformidad con la criticidad de la información, sistemas y procesos involucrados, los incidentes de seguridad de la información y la revaloración de los riesgos, lo anterior con el fin de mantener el nivel acordado de seguridad de la información y la prestación del servicio.

Gestión de incidentes de seguridad de la información (A.16): Si bien se observa en el procedimiento *Gestión de Incidentes, Amenazas y Debilidades de Seguridad* (GT-PD-09), directrices generales respecto a la respuesta a los incidentes de seguridad de la información, en el mismo no se define como se cumplen los criterios evaluados. No se evidencian planes de respuesta ni directrices vinculadas a los criterios establecidos para el control.

En la aplicación de la lista de verificación del 25/04/2024, se indica que no se tiene y se va a documentar en el procedimiento de incidentes.

De igual manera no se identifican las directrices relacionadas con la gestión de incidentes y la comunicación sobre eventos de seguridad y debilidades, que incluyen entre otros: a. responsabilidades y procedimientos; b. reporte de eventos de seguridad de la información; c. reporte de debilidades de seguridad de la información; d. evaluación de eventos de seguridad de la información y decisiones sobre ellos; e. aprendizaje obtenido de los incidentes de seguridad de la información; y f. recolección de evidencia.

Aspectos de seguridad de la información de la gestión de la continuidad del negocio (A.17): No se evidencian las directrices relacionadas con la planificación de la continuidad de la seguridad de la información. Tampoco se identifica la verificación, revisión y evaluación de la continuidad de la seguridad de la información, así como lineamientos específicos que permitan asegurar la disponibilidad de las instalaciones de procesamiento de la información (identificación de elementos redundantes, pruebas para asegurar que éstos reaccionen conforme lo esperado en una emergencia o falla).

Conforme lo anterior, en articulación con lo evidenciado en el control Gestión de Incidentes de Seguridad de la Información (A.16) y algunas situaciones presentadas en la vigencia auditada relacionada con caídas del servidor, interrupciones de suministro de red, entre otras, como se muestra en las siguientes tablas; se configura hallazgo por cuanto no se tiene una planificación integral para dar continuidad del negocio que garantice la seguridad de la información ante posibles incidentes o amenazas.

Sistema	Fecha	Situación reportada – Grupo WhatsApp
Orfeo	17/01/2023	No funciona ORFEO

Página web	27/01/2023	"… la página www.festivalcentro.gov.co no está viendo bien"
Página web e intranet	03/02/2023	Inconvenientes reportados por varios colaboradores en la página web e intranet
Orfeo	14/02/2023	Inconvenientes reportados por varios colaboradores en Orfeo Warning: file_put_contents(); Only 0 of 26705 bytes written, possibly out of free disk space in /var/www/html/orfeopg/vendor/illuminate/filesystem/Illuminate/Filesystem/Filesystem.php on line 70
Orfeo	07/03/2023	Inconvenientes reportados por varios colaboradores. No se puede firmar
Internet	27/04/2023	No hay internet en Casa Amarilla
Orfeo	07/06/2023	No se puede ingresar
Orfeo	14/06/2023	Inconvenientes en la radicación de Correspondencia
Orfeo	07/07/2023	Error general en el sistema
Orfeo	11/07/2023	Intermitencias en el servicio
Internet Orfeo	01/08/2023	Sistemas caídos
Internet, conectividad y demás aplicaciones	04/08/2023	"… ETB tiene una rotura en fibra en un tramo importante reportado desde ayer 10:40 pm. En este momento están enviando personal a sitio para resolver la falla, no hay tiempos asociados a la reparación"; servicios reestablecidos en la misma fecha
Plataforma Centro y Orfeo	04/08/2023	Plataformas fuera del aire
Orfeo	14/08/2023	Error de conexión a la BD
Correo electrónico	30/11/2023	"… incidencias a nivel de correo electrónico, al realizar el escalamiento al proveedor correspondiente, nos indican una falla mayor en varios de los servicios, esta incidencia está siendo atendida y el transcurso del día se normalizarán los servicios, la principal falla es intermitencia en el envío y recepción de correos"

Fuente: Grupo Institucional de WhatsApp

Sistema	Fecha	Situación reportada – GLPI
Orfeo	19/01/2023	Fallas en el sistema Orfeo
Orfeo	07/02/2023	Urgentes inconvenientes para el acceso a ORFEO
Redes	21/03/2023	Inconvenientes Ingreso a la red de la Fundación.
Pandora	23/05/2023	Solicitud revisión página Pandora
Orfeo	27/06/2023	Orfeo - Falla verificación con base de datos
Internet	20/06/2023	Fallas en la intranet y en su navegación
Orfeo	14/06/2023	Incidente Orfeo
Servidor	13/07/2023	Servidor sin servicio
Orfeo	07/07/2023	Falla en la traza de revisiones en el módulo histórico de borradores
Orfeo	05/07/2023	Orfeo caído
Servidor	18/08/2023	problemas para ingresar al servidor
Servidor	04/10/2023	Carpeta Servidor desaparecida
Correo	30/11/2023	Problemas con el correo institucional
Inter operatividad	15/11/2023	Inconvenientes de traslado de PQRSD a Bogotá te escucha
	05/12/2023	Caída de servicio Fundación Gilberto Alzate

Fuente: Reportes GLPI enero a diciembre de 2023

Adicionalmente en la ejecución de la Auditoria Proceso Transformación Cultural para la Revitalización del Centro, se presentó la siguiente situación, señalada por la OCI en el informe correspondiente (20231100104043):

> *"Durante el desarrollo de la auditoría se presentó una falla en el servidor institucional donde se consolidan las evidencias de las metas de los proyectos de inversión, lo que dificultó la verificación de los soportes que dan cuenta de la ejecución de actividades misionales. Esta situación género que la información ya validada tuviera que ser nuevamente cargada en diferentes fechas, lo que dificultó al equipo auditor asegurar la trazabilidad y reprocesos en las evaluaciones; conforme lo anterior, se recomienda que institucionalmente se asegure la integridad de la información de conformidad con los lineamientos del Modelo de Seguridad y Privacidad de la Información (ISO 27001: 2021 Anexo A. Numeral A.12.3 Copias de Respaldo). Adicionalmente y teniendo en cuenta que el procedimiento Respaldos de la Información Código GT-PD-05 Versión: 2 del proceso Gestión de Tecnologías de la Información, no precisa sobre cual copia de seguridad se debe hacer la restauración de los datos y si se incluyen las copias de seguridad incrementales posteriores, se recomienda revisar los lineamientos*".

Teniendo en cuenta la evaluación del Anexo 1 de la ISO 27011:2013 relacionada con la gestión de incidentes de seguridad de la información (A.16) y aspectos de seguridad de la información de la gestión de la continuidad del negocio (A.17), el equipo auditor genera un hallazgo por cuanto no se evidencia el Plan de Continuidad de Negocio que garantice la preservación de la disponibilidad y continuidad de los servicios que ofrece la entidad.

Cumplimiento (A.18): Frente a las revisiones de cumplimiento técnico, no se evidencian los informes de resultados y seguimientos realizados para asegurar que las brechas de seguridad fueron solucionadas.

De manera general, se observó que el procedimiento *Seguridad de redes* (GT-PD-10 Versión 2) refiere en la actividad 2 "*La solicitud para ello deberá ser gestionada según lo establecido en el Procedimiento de asignación de equipos y acceso a los sistemas de información, igualmente se capturan imágenes de pantalla*" (Subrayado fuera de texto); sin embargo, este procedimiento no está incluido en los documentos SIG del proceso publicados en intranet.

Conforme lo anterior, de manera general se recomienda:

- Ajustar el documento *Políticas de Seguridad de la Información* (GT-PO-01 Versión: 3), de tal manera que incluya las directrices con las cuales se da cumplimiento a los diferentes criterios señalados en cada control o justificar y documentar si no aplica.
- Documentar de manera integral la implementación de los criterios vinculados a todos los controles evaluados (Ver Anexo).
- Verificar los cambios en la versión actualizada de la ISO 27001:2022 y ajustar en los instrumentos de medición y documentos del proceso, en articulación con los lineamientos que sean emitidos por MINTIC o la Alta Consejería.

- Revisar las evidencias que se presentan como soporte de los criterios evaluados en el instrumento de medición y ajustar teniendo en cuenta la documentación vigente y la realidad institucional.
- Revisar y articular con los lineamientos internos de acuerdo a la NIST y revisar lo dispuesto en la guía Roles y Responsabilidades del MSPI de MINTIC.
- En los reportes de incidentes GLPI, incluir información relacionada con su impacto y las acciones implementadas para solucionarlos, con el fin de analizar, evaluar y estandarizar los temas que se reportan, generando estadísticas para facilitar la toma de decisiones.
- Documentar las herramientas del Sistema de Gestión Documental de manera articulada con el sistema de seguridad de la información, asegurando que brindan lineamientos claros sobre la conservación y seguridad de la información en los procesos de transporte físico contratados con terceros, teniendo en cuenta la realidad institucional.
- De acuerdo con los resultados de los reportes de Sophos, permitir los bloqueos específicos de acuerdo a las alertas con mayor incidencia.
- Respecto al diseño y aplicación de seguridad física a oficinas, recintos e instalaciones (A.11.1.3) y teniendo en cuenta que el Protocolo Seguridad Tesorerías ya no está vigente, se recomienda generar directrices sobre la seguridad de las instalaciones que sean necesarias (Data Center).
- Teniendo en cuenta que no se evidenció un plan de emergencias institucional que vincule el tratamiento para los equipos tecnológicos, la protección de la información en un evento natural o un accidente y el respaldo de esta información en un lugar fuera de la entidad; se recomienda documentar estos lineamientos de acuerdo a la NIST.
- Revisar y actualizar los documentos SIG, de conformidad con los ajustes que surjan a partir de las observaciones realizadas por el equipo auditor.

Por último y en articulación con lo expuesto por el proceso auditado en su *Informe Seguridad de la Información – FUGA Modelo MSPI MINTIC*, aportado por el proceso auditado al corte de diciembre de 2023, se recoge la siguiente recomendación:

- *"Frente a la continuidad del negocio se deben documentar planes DRP Y BCP para darle alcance a estos aspectos, la entidad debe tener claro cómo actuar en caso de emergencia, una vez se documente lo anterior el índice a nivel de controles tendrá un incremento*"

2.2. Avance ciclo de funcionamiento del modelo de operación (PHVA):

COMPONENTE	% de Avance Actual Entidad	% Avance Evaluación OCI	% Avance Esperado
Planificación	40%	34%	40%
Implementación	16%	14%	20%
Evaluación de desempeño	17%	16%	20%
Mejora continua	14%	16%	20%
TOTAL	**87%**	**79%**	**100%**

Fuente: Instrumento de Identificación de la Línea Base de Seguridad de MINTIC (Corte diciembre 2023) y evaluación propia.

La evaluación específica realizada a cada uno de los controles de los dominios puede ser consultada en la hoja PHVA del Anexo Instrumento de medición MSPI diciembre 2023, el cual hace parte integral del presente informe.

Planificación:

- En el documento *Políticas de Seguridad de la Información* (GT-PO-01 Versión: 3), no se evidencia en el alcance la identificación del contexto interno, externo, gestión de riesgos y la identificación de las partes interesadas.
- No se evidencia la Declaración de Aplicabilidad de la entidad.
- La evaluación de este componente incluye aspectos validados en el componente de Efectividad (Controles administrativos y técnicos), vinculados a la revisión anual de la política de seguridad de la información, desviaciones y excepciones sin identificar y activos de información no actualizados, expuestos en el ítem 2.1.

Implementación:

- No se evidencia una estrategia de planificación y control operacional.
- Respecto a la Implementación del plan de tratamiento de riesgos, no se identifica la gestión vinculada a las fases de desarrollo de proyectos y ciclo de vida del tratamiento de riesgos.
- Si bien se evidencia un indicador general de implementación del MSPI, no se identifican indicadores de medición específicos que permitan medir la eficiencia y eficacia de los componentes de implementación del modelo, tal como señala en la *Guía - Indicadores Gestión de Seguridad de la Información* de MINTIC[20] y lo dispuesto en la Resolución 500 de 2021 de MinTIC *"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital"* Anexo 1 *Modelo de Seguridad y Privacidad de la Información* - 11.5 Guía - Indicadores Gestión de Seguridad de la Información.

Evaluación de Desempeño:

- Se evidencia el seguimiento, evaluación y análisis del plan de tratamiento de riesgos; sin embargo, no se identifica la gestión vinculada a las fases de desarrollo de proyectos y ciclo de vida del tratamiento de riesgos, en especial en aquellos proyectos que no se vinculan directamente al proceso auditado.

Mejora Continua:

- Si bien se realizan seguimientos y se presentan al Comité Directivo en el marco del avance del MSPI realizado en el instrumento de medición de MinTIC, no se evidencia el análisis sobre el resultado presentado.

  En la entrevista realizada el 16/05/2024 el proceso señala que el plan se encuentra en el PETI en la sección 11.1 Plan de Seguridad y Privacidad de la Información y su seguimiento se realiza a través de la evaluación

[20] Guía - Indicadores Gestión de Seguridad de la Información de MINTIC: https://gobiernodigital.mintic.gov.co/692/articles-237905_maestro_mspi.pdf

del PHVA, se indica adicionalmente que teniendo en cuenta el nivel de especificidad de cada uno de los criterios de los 114 controles señalados en el instrumento, la mejora se prioriza de conformidad con las situaciones que se van presentando de acuerdo a los dominios del MSPI en la entidad.

Conforme lo anterior, se recomienda:

- Establecer, aprobar y socializar la Declaración de Aplicabilidad de la entidad, de tal manera que ésta permita identificar y priorizar los controles que son más relevantes y efectivos de conformidad con las recomendaciones de la norma NTC/ISO 27001:2013.
- Revisar los controles vinculados al componente de implementación y gestionar los aspectos relacionados con la estrategia de planificación y control operación, plan de tratamiento de riesgos e indicadores de gestión del MSPI.

De acuerdo al Informe Seguridad de la Información – FUGA Modelo MSPI MINTIC, aportado por el proceso auditado al corte de diciembre de 2023, se recogen las siguientes recomendaciones realizadas por la 1ª. línea:

- *"El profesional a cargo debe construir un documento que contenga un plan para evaluar el desempeño y eficacia del MSPI a través de instrumentos que permita determinar la efectividad de la implantación del MSPI. Esto permitirá llegar al 20% esperado actualmente se encuentra en un nivel relacionado al 17%.*
- *Frente a la mejora continua se debe generar un documento que indique los resultados consolidados del componente evaluación de desempeño y de igual forma se debe generar una comunicación de los resultados y plan para subsanar los hallazgos y oportunidades de mejora. Dicho lo anterior y con el adecuado soporte la entidad obtendrá un avance en su calificación".*

2.3. Nivel de madurez modelo seguridad y privacidad de la información:

		NIVEL DE CUMPLIMIENTO TIC	CONTEO DE VALORES IGUAL A MENOR TIC	TOTAL DE CALIFICACIONES DE CUMPLIMIENTO TIC	NIVEL DE CUMPLIMIENTO OCI	CONTEO DE VALORES IGUAL A MENOR OCI	TOTAL DE CALIFICACIONES DE CUMPLIMIENTO OCI
NIVELES DE MADUREZ DEL MSPI	Inicial	SUFICIENTE	0	10	SUFICIENTE	0	10
	Repetible	SUFICIENTE	0	21	SUFICIENTE	1	20
	Definido	SUFICIENTE	1	42	SUFICIENTE	9	33
	Administrado	SUFICIENTE	5	59	SUFICIENTE	16	43
	Optimizado	SUFICIENTE	14	60	CRÍTICO	39	21

Fuente: Instrumento de Identificación de la Línea Base de Seguridad de MINTIC (Corte diciembre 2023) y evaluación propia.

El nivel de madurez se calcula de manera automática en el *Instrumento de Identificación de la Línea Base de Seguridad* de MINTIC, de acuerdo al resultado de la evaluación realizada en los aspectos administrativos, técnicos y PHVA.

Teniendo en cuenta que el *Modelo de Seguridad de la Información* de MinTIC, señala que el nivel Optimizado corresponde a que la seguridad de la información presenta un valor agregado para la entidad; se observa que en términos generales cuenta con:

- Directrices para llevar a cabo la identificación de activos y gestión de riesgos relacionados con la seguridad y privacidad de la información.
- Controles alineados con la preservación de la confidencialidad, integridad y disponibilidad de la información.
- Procesos básicos de gestión de seguridad y privacidad de la información.
- Se tiene documentado, estandarizado y aprobado por la Dirección el MSPI
- Se realizan monitoreos respecto a la efectividad de los controles del modelo, los cuales se verifican a través de auditorías al proceso de Gestión TIC.

No obstante, se observan oportunidades de mejora relacionadas con retroalimentar cualitativamente el MSPI, por lo que la evaluación en el nivel Optimizado se califica en CRITICO.

Conforme lo anterior, algunos de los aspectos relacionados con una evaluación menor en este nivel, expuestos de manera detallada en el ítem 2.1. y en la matriz anexa a este informe, que genera la calificación como critica, son:

- Inventario de activos de información desactualizados y debilidades en su diligenciamiento.
- No todas las directrices que requieren cumplir con el criterio de estar establecidas, se encuentran documentadas.
- Se evidencian debilidades en la definición del alcance de la política de seguridad de la información.
- No se evidencian Planes de Continuidad del Negocio.
- Se evidencian debilidades en la definición de los roles de seguridad y privacidad de la información.

2.4. Calificación frente a mejores prácticas en Ciberseguridad (NIST)

MODELO FRAMEWORK CIBERSEGURIDAD NIST			
Etiquetas de fila	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF	CALIFICACIÓN OCI
IDENTIFICAR	87	100	71
DETECTAR	83	100	70
RESPONDER	83	100	64
RECUPERAR	53	100	33
PROTEGER	93	100	74

Fuente: Instrumento de Identificación de la Línea Base de Seguridad de MINTIC (Corte diciembre 2023) y evaluación propia.

Si bien para el cálculo de este componente se tienen en cuenta las evaluaciones realizadas sobre los aspectos administrativos, técnicos y PHV ya expuestas en los ítems anteriores, se identifican adicionalmente las siguientes situaciones sobre las funciones de CSF:

Identificar:

- No se identifica como se comunica a las partes interesadas la infraestructura critica de la entidad.

- No se identifican las amenazas internas y externas y no se evidencia donde se encuentran documentadas.
- No se identifican los impactos potenciales en la entidad y su probabilidad.

Detectar:
- No se identifica como se establece y gestiona una línea base de las operaciones de red, los flujos de datos esperados para usuarios y sistemas, la determinación del impacto de los eventos y no se observan umbrales de alerta de los incidentes.
- No se evidencia como se comparte con las partes autorizadas la efectividad de las tecnologías de protección en la entidad.
- No es claro cómo se identifican los eventos de ciberseguridad en la entidad y se determinan las medidas de protección, tampoco se evidencia como se verifica la efectividad de estas medidas.

Responder:
- No se evidencian planes de respuesta a incidentes.
- No se identifican estrategias de respuesta.

Recuperar:
- No se evidencia si las actividades de restauración son coordinadas con las partes interesadas internas y externas.
- No se identifican planes de recuperación.
- No se identifican estrategias de recuperación.

Proteger:
- No se identifican procesos de protección.

Teniendo en cuenta que la entidad no tiene establecidos planes que le permitan gestionar la recuperación de su información, de conformidad con los criterios señalados en el componente de las mejores prácticas en Ciberseguridad del Anexo A de la ISO 27011:2013 relacionada con la gestión de incidentes de seguridad de la información (A.16), y aunado a lo evidenciado en la auditoria la Proceso de Gestión documental, donde se identificó que la entidad no tenía definida una Política de Preservación Digital que le permita garantizar la preservación y aseguramiento de los documentos y que el Plan de Preservación Digital no se articulaba con los riesgos documentales que pudieran afectar la perdurabilidad y accesibilidad de los documentos, su seguridad, integridad, autenticidad, confidencialidad, trazabilidad y disponibilidad en el tiempo; el equipo auditor genera un hallazgo.

Conforme lo anterior, se recomienda:

- Revisar los criterios en cada una de las funciones de ciberseguridad e implementar los criterios que se encuentren vinculados a los aspectos observados anteriormente.
- Teniendo en cuenta que el aspecto con menor calificación corresponde al de *Recuperar* (33) es importante que se revisen e implementen las acciones pertinentes para dar cumplimiento integral a los criterios

establecidos en la ISO 27001:2013, principalmente en los temas relacionados con los planes de recuperación.

En articulación con lo expuesto por el proceso auditado en su *Informe Seguridad de la Información – FUGA Modelo MSPI MINTIC*, aportado por el proceso auditado al corte de diciembre de 2023, se recoge la siguiente recomendación:

- *"… el eslabón más débil frente a esta calificación se encuentra en el término "Recuperar" el cual se debe fortalecer con Los planes de recuperación y los procesos son mejorados incorporando las lecciones aprendidas para actividades futuras: 1) Los planes de recuperación incorporan las lecciones aprendidas. 2) Estrategias de recuperación actualizadas.*"

3. Derechos de Autor - Software

Teniendo en cuenta el resultado del informe presentado el 14/03/2024 (Orfeo 20241100026783)[21], y el reporte cargado a la Dirección Nacional de Derechos de Autor, se evidencia que la entidad de manera general:

- Mantiene el control en términos de número y responsables, de los equipos de cómputo de la entidad, En este sentido se reportaron 121 equipos para el 2023, información validada y coherente con el inventario de Recursos Físicos.
- Se han establecido lineamientos y se dispone de controles para garantizar que el software instalado en los equipos este debidamente licenciado. Lo anterior articulado con lo evidenciado en el ítem 1.2. del presente informe, específicamente en la evaluación de la Acción 2: *Adquisición de licenciamiento para la entidad* del PETI. No obstante, se evidenciaron oportunidades de mejora relacionadas con la información registrada en los inventarios de software tanto de TIC como de Recursos Físicos.
- Se tienen implementados lineamientos tanto en la *Política de Seguridad de la Información* como en el *Instructivo para la disposición final de residuos de aparatos eléctricos y electrónicos* (RAEE) relacionados con el destino final del software dado de baja en la entidad y en términos generales se evidencia que se dan cumplimiento a los mismos.

Oportunidades de mejora evidenciadas:

- Se evidencian diferencias entre la información registrada en el inventario de TIC y las Hoja de Vida de los dispositivos tecnológicos, la mayoría de ellas relacionadas con números de placas y de series, versiones de software o aplicaciones originadas en su mayoría por las actualizaciones automáticas de los equipos, diferencias en los datos registrados frente a los procesadores, memoria, disco duro y placa de monitores, entre otros; lo anterior en articulación con lo evidenciado en la visita in situ del 06/03/2024,
- La información publicada en la página web, vinculada a la 7 Datos Abiertos, 7.1. Instrumentos de Gestión de la Información, 7.1.1. Registro Activos de Información, respecto al inventario de Activos Hardware y Activos Software no se encuentra actualizada.

[21] https://www.fuga.gov.co/sites/default/files/2024-03/Informe%20Derechos%20de%20Autor%20Software%202023%20web.pdf

- Se evidencian diferencias en la información de software registrada en el inventario de TIC, frente al inventario de Recursos Físicos.
- La ejecución de *Cronograma de Mantenimiento de la Infraestructura Tecnológica*, no se encuentra documentado de manera integral o los soportes allegados no permiten validar la gestión reportada. Lo anterior en articulación también con lo expuesto en el presente informe en el numeral 1.2 Ejecución, específicamente en el aparte Acción 1*: Mantenimientos dispositivos tecnológicos* del PETI.

Recomendaciones Generales:

- Actualizar y articular el inventario de hardware con las hojas de vida de los dispositivos.
- Articular la información registrada en los inventarios de TIC y Recursos Físicos relacionados con Software/Licencias.
- Actualizar la información publicada en la página web de la entidad relacionada con los activos de información hardware y software.
- Documentar de manera integral la ejecución de las actividades del Cronograma de Mantenimiento de la Infraestructura tecnológica, específicamente en aquellas vinculadas a garantizar el mantenimiento de los equipos y del software de la entidad.
- Documentar en la Política de Seguridad de la Información los lineamientos relacionados con los derechos de propiedad intelectual, uso de software patentado, cumplimiento de derechos de propiedad intelectual, control sobre inventario de software instalado, entre otros, definidos en la ISO/IEC 27001:2013 - Anexo A – Ítem A.18.1.2.
- Si bien se evidencia la gestión realizada por el equipo TIC frente a realizar campañas de sensibilización del tema de Seguridad de la Información, se recomienda incluir en el PIC actividades específicas del tema de derechos de autor – software.
- Institucionalmente, participar de manera activa en las sensibilizaciones realizadas por el equipo TIC y desarrollar de manera integral los ejercicios propuestos.

4. Gestión contractual:

La Oficina de Control Interno realizó el seguimiento a los procesos contractuales suscritos bajo las distintas modalidades de selección, los cuales se encuentran publicados en el Sistema Electrónico para la Contratación Pública SECOP II https://www.colombiacompra.gov.co/secop-ii, así como la información publicada en el sistema de información de gestión documental ORFEO.

En suma, para la selección de la muestra se usó como insumo la relación de los contratistas y contratos que actualmente se encuentran vinculados al proceso de Gestión TIC, compuesta por:

- PANDORA: Convenio 1629-2021
- PANDORA: FUGA-62-2023
- ORFEO: FUGA-63-2023
- HOSTING: FUGA-170-2021 Gopher Group S.A.S.
- Adquisición De Licenciamiento Tecnológico: FUGA 127 de 2023.

4.1. PANDORA

✓ Convenio Interadministrativo

Teniendo en cuenta que la verificación de la gestión contractual relacionada con la adquisición o desarrollo de nuevos sistemas de información, es objeto de evaluación en el presente ejercicio de auditoría en el componente del Modelo de Seguridad y Privacidad de la Información y que el aplicativo PANDORA si bien corresponde a un convenio interadministrativo suscrito en el 2021, para el periodo del alcance aún se encuentra en desarrollo, se incluye en la muestra con el fin de evaluar la implementación de los controles del Anexo A ISO 27001-2013, evaluados en el numeral 2 del presente informe.

FUGA 1629 de 2021	
Tipo de proceso	Convenio Interadministrativo
Secop	1629-2021 https://community.secop.gov.co/Directory/CompanyProfiles/DynamicMyCompanyProfile/ViewProfile?companyCode=702066127&prevCtxUrl=https%3a%2f%2fwww.secop.gov.co%3a443%2fCO1ContractsManagement%2fTendering%2fSalesContractManagement%2fIndex&prevCtxLbl=Administraci%c3%b3n+de+contratos
Expediente Orfeo	20211300200090223E
Objeto	Aunar esfuerzos técnicos, tecnológicos y administrativos, para el desarrollo de la plataforma para la gestión de la planeación y gestión institucional – PANDORA, entre el Instituto Distrital de las Artes y la Fundación Gilberto Alzate Avendaño, dentro de un propósito de colaboración armónica entre entidades.
Asociados	**Fundación Gilberto Alzate Avendaño – FUGA** **Instituto Distrital De Las Artes – IDARTES**
Valor inicial	El presente convenio no se define con un valor monetizado dada la modalidad en la que se celebra el mismo, y que no genera erogaciones para las partes, siendo claro que ninguna de estas aporta recursos soportados presupuestalmente que vayan a ingresar al presupuesto de la otra entidad.
Fecha de suscripción del contrato	18 de agosto de 2021
Fecha de acta de inicio	12 de julio de 2019
Fecha de terminación inicial	30 de mayo de 2024
Supervisor	Por parte del Instituto Distrital De Las Artes - IDARTES a través de el/la Jefe de la Oficina Asesora De Planeación Y Tecnologías De La Información, y Por parte de la Fundación Gilberto Alzate Avendaño – FUGA a través de el/la Jefe De La Oficina Asesora De Planeación.

* Elaboración OCI fuente Orfeo

El 10 de agosto de 2021 se determinaron los estudios previos definitivos, Radicado 20211200069913, por tanto, mediante acto de justificación de contratación directa, Radicado 20212000071123, se demostró la celebración del convenio interadministrativo mediante la modalidad de contratación directa.

En los estudios previos se determinó que, para certificar la ejecución y el cumplimiento de los proyectos de inversión a cargo de la FUGA, es preciso la articulación con otras entidades, por lo cual, era necesario la implementación de mecanismos que garantizaran el acceso y transparencia en las acciones de la entidad, a través de canales de comunicación y el uso de las TIC. Para ello la entidad tuvo que actualizar la infraestructura tecnológica para asegurar la información, su almacenamiento y comunicación eficiente entre las dependencias.

Es así como la implementación del sistema de información PANDORA le permitió a la Fuga recolectar, consolidar, analizar información, ejercer el control, seguimiento y evaluación de la gestión institucional.

Igualmente, se estableció que el convenio marco no compromete recursos económicos de las partes para su ejecución y cumplimiento, toda vez que el mismo se desarrolla con las capacidades instaladas de las entidades intervinientes. En materia de infraestructura tecnológica se identificó que la Fuga debía implementar:

- Servidor de aplicaciones con RAM entre 16 y 32 GB y espacio en disco de 300GB o más.
- Servidor Linux CentOS 7 con Docker y Docker-Compose Instalado.
- Base de datos mariadb (Se recomienda que sea en un servidor independiente al servidor de aplicaciones)
- Instalar: composer, git, node.
- Licenciamiento Bitbucket. - En cuanto al ciclo de vida del Sistema de Información.

Ahora bien, se estimó cuales riesgos previsibles podrían afectar el equilibrio de la ejecución del contrato, en cumplimiento del artículo 4° de la Ley 1150 de 2007, así como el artículo 2.2.1.1.1.6.4., y numeral 6 del artículo 2.2.1.1.2.1.1., del Decreto 1082 de 2015:

Que puede pasar	Consecuencia	Controles	Monitoreo
Fallas en la plataforma tecnológica de las entidades involucradas.	Incumplimiento o retraso de las obligaciones, actividades del cronograma de trabajo del convenio	Reprogramación de actividades de acuerdo al cronograma inicialmente establecido	Verificando que el personal no sea incapacitado
Pérdida de la información almacenada	Se produce pérdida de la información de la entidad por fallas.	Adelantar las respectivas copias de seguridad de la información.	Verificando que se realicen las copias de seguridad
Filtración de la información.	Se produce hurto de información de la entidad.	Incluir una cláusula de confidencialidad en el contrato.	Verificando que se realicen los protocolos de seguridad

* Elaboración OCI fuente Orfeo

Conforme lo anterior, se observa que se incluyen dentro de los riesgos previsibles, riesgos tecnológicos asociados al cumplimiento del contrato; lo anterior teniendo en cuenta lo señalado en el *Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación de Colombia Compra Eficiente (M-ICR-*

01) [22]*.* Se observa adicionalmente que las situaciones vinculadas a estos, están articuladas con los tres aspectos relevantes en la gestión de la información y que corresponden a la confidencialidad, la integridad y disponibilidad.

Teniendo en cuenta que este proceso contractual está vinculado con la ejecución del proyecto PY05 del PETI (Implementación módulos Pandora: Demoras y pérdida de información en procesos misionales, transversales y estratégicos), no se evidencia de manera clara como se integran los riesgos de seguridad de la información identificados, con la ejecución del mismo (ISO 27001:2014 Control A.6.1.5.).

El contrato fue firmado el 17 de agosto de 2021 y aprobado en Secop el 18 de agosto de 2021, en la misma fecha se comunicó la supervisión del contrato Radicado 20211300072543 y Acta de inicio Radicado 20211200076303 de 27 de agosto de 2021.

En el contrato se pactó la creación de un comité técnico de seguimiento con la finalidad garantizar la ejecución del cumplimiento de las actividades y gestiones establecidas en los planes de trabajo, está conformado por:

- IDARTES: La Directora General o su delegado (a), o el (la) supervisor(a) de convenio, El /La Jefe de la Oficina Asesora de Planeación y Tecnologías de la Información.
- FUGA: La Subdirectora de Gestión Corporativa o su delegado. La Jefe de la Oficina Asesora de Planeación o su delegado y un representante del área de tecnología de la información.

En ese orden, en las cláusulas del convenio se estableció que el comité debía sesionar de manera ordinaria cada tres meses, y de manera extraordinaria cuando fuera convocado por el secretario técnico, profesional de planta o contratista del IDARTES.

A continuación, se relaciona la muestra aleatoria y los resultados de la revisión de las reuniones del comité desde el año 2021-2023:

Se realizaron 9 reuniones en 2021, 39 en el 2022, 26 en el 2023 y hasta la fecha 2 del 2024:

- 30 de agosto de 2021. Radicado 20211200081573. Fecha 13-09-2021.

En el contrato se estableció que en la primera reunión técnica se debían desarrollar los siguientes temas:

- ✓ La metodología de desarrollo de software que se tendrá como referencia para la ejecución de las actividades del Convenio.
- ✓ Mecanismos para el levantamiento de requerimientos. SI
- ✓ Mecanismos para el control de cambios.

[22] Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación de Colombia Compra Eficiente (M-ICR-01). Numeral 2 Identificar y clasificar los Riesgos. Tipo: Riesgos Tecnológicos: son los derivados de fallas en los sistemas de comunicación de voz y de datos, suspensión de servicios públicos, nuevos desarrollos tecnológicos o estándares que deben
ser tenidos en cuenta para la ejecución del contrato, obsolescencia tecnológica.

- ✓ Atributos de Calidad de Software.
- ✓ Características mínimas de los documentos técnicos generados en cada fase del proceso de desarrollo e implementación del sistema Pandora, teniendo en cuenta la Guía de Dominio de Sistemas de Información de la Política de Gobierno Digital.
- ✓ Buenas prácticas y criterios de aceptación mínimos en términos de seguridad que deben cumplir los desarrollos.
- ✓ Plan de pruebas funcionales y no funcionales. SI
- ✓ Matriz de responsabilidades en cada fase del desarrollo.

De acuerdo a lo observado en el acta de la sesión, solo se mencionó el tema de los mecanismos para el levantamiento de requerimientos y el plan de pruebas. Conforme lo anterior, se verificó el acta correspondiente a la segunda sesión de la mesa técnica, llevada a cabo el 02/09/2021 (Orfeo 20211200081583), en la cual se hace la presentación de la propuesta de trabajo para la implementación del aplicativo, evidenciándose que se incluyen los temas relacionados con la metodología de arquitectura, identificación de requerimientos; sin embargo no se identifican de manera clara lo relacionado con mecanismos para el control de cambios, atributos de calidad de Software, características mínimas de los documentos técnicos, criterios de seguridad a implementar, plan de pruebas y matriz de responsabilidades en cada fase del desarrollo de la aplicación.

- 16 de septiembre de 2021. Radicado 20211200086413. Fecha: 29-09-2022
- 4 de noviembre de 2021. Radicado 20211200099323. Fecha: 10-11-2022.
- 2 de diciembre de 2021. Radicado 20211200109603 Fecha: 09-12-2021.
- 4 de febrero de 2022. Radicado 20221200055063. Fecha: 15-06-2022.
- 1 de abril de 2022. Radicado 20221200055123. Fecha: 15-06-2022. No fue firmado por SCRD y Catastro.
- 6 de mayo de 2022. Radicado 20221200087163. Fecha 14-09-2022.
- 25 de mayo de 2022. Radicado 20221200087183. Fecha 14-09-2022.
- 1 de junio de 2022. Radicado 20221200087203. Fecha 14-09-2022.
- 1 de julio de 2022. Radicado 20221200087513. Fecha 15-09-2022. No fue firmado por IDARTES.
- 15 de julio de 2022. Radicado 20221200087583. Fecha 15-09-2022.
- 26 de agosto de 2022. Radicado 20221200087673. Fecha 15-09-2022.
- 7 de octubre de 2022. Radicado 20221200118093. Fecha 16-12-2022.
- 28 de octubre de 2022. Radicado 20221200118133. Fecha 16-12-2022.
- 18 de noviembre de 2022. Radicado 20231200021553. Fecha 13-02-2023.
- 23 de diciembre de 2022. Radicado 20231200021623. Fecha 13-02-2023.
- 20 de enero de 2023. Radicado 20231200080823. Fecha 31-07-2023.
- 3 de marzo de 2023. Radicado 20231200080853. Fecha 31-07-2023.
- 28 de abril de 2023. Radicado 20231200080883. Fecha 31-07-2023.
- 30 de junio de 2023. Radicado 20231200080923. Fecha 31-07-2023.
- 21 de julio de 2023. Radicado 20231200080953. Fecha 31-07-2023.
- 25 de agosto de 2023. Radicado 20231200120403. Fecha 23-11-2023.
- 29 de septiembre de 2023. Radicado 20231200120453. Fecha 23-11-2023.
- 3 de noviembre de 2023 Radicado 20241200017543. Fecha 15-02-2024

- 15 de diciembre de 2023 Radicado 20241200017573 Fecha 15-02-2024
- 12 de enero de 2024. Radicado 20241200017583 Fecha 15-02-2024.
- 23 de febrero de 2024. Radicado 20241200027443. Fecha 16-03-2024.

Finalmente, se determinó la creación del Comité de Desarrollo de Software que debe sesionar de manera ordinaria cada mes, y de manera extraordinaria cuando sea convocado por el Secretario Técnico, sin embargo no se evidenció la existencia del mismo.

En entrevista realizada el 16/05/2024 se indica que, todas las actas de implementación de PANDORA se encuentran en la ruta \\192.168.0.34\Gestion del Conocimiento\2022\PANDORA\Actas Convenio IDARTES_FUGA; sin embargo, de la revisión realizada se evidenció que corresponden al comité técnico y no al Comité de Desarrollo de Software.

✓ **Contratos de prestación de servicios**

FUGA 62 de 2023	
Tipo de proceso	Contratación Directa
No. de proceso	https://www.secop.gov.co/CO1ContractsManagement/Tendering/ProcurementContractEdit/View?docUniqueIdentifier=CO1.PCCNTR.4518839&prevCtxUrl=https%3a%2f%2fwww.secop.gov.co%3a443%2fCO1ContractsManagement%2fTendering%2fProcurementContractManagement%2fIndex&prevCtxLbl=Contratos+
Expediente Orfeo	20231300200090029E
Objeto	Prestar los servicios profesionales a la Oficina Asesora de Planeación de la Fundación Gilberto Alzate Avendaño en la elaboración de documentación, construcción y puesta en producción de la plataforma Pandora en la entidad.
Contratista	**Andrés Felipe Malaver Malaver**
Valor inicial	$ 50.013.000
Aprobación de la póliza	02 de febrero de 2023. Radicado 20231300017133
Fecha de suscripción del contrato	31 de enero de 2023
Fecha de acta de inicio	02 de febrero de 2023. Radicado 20231200017593
Fecha de terminación inicial	01 de diciembre de 2023
Fecha de terminación final	5 de enero de 2024
Prorroga	$5.668.140
Modificaciones	1
Comunicación de Supervisión Contrato	02 de febrero de 2023, Radicado 20231300017153
Supervisor	Luis Fernando Mejía Castro

* Elaboración OCI fuente Orfeo

Etapa pre contractual

Revisado el expediente en el aplicativo de gestión documental ORFEO, se observa que se encuentra el diligenciamiento del formato “GJ-FT-24 Hoja de ruta”, de conformidad con el numeral 2 del título I, sección I “Aspectos Generales Procesos Competitivos y Contratación Directa”, del Procedimiento contractual. Código GJ-PD-01.

El contrato en Secop fue firmado y aprobado el 31 de enero de 2023, asimismo se publicaron los documentos requeridos para la suscripción y ejecución del contrato.

En la plataforma Secop II, se cargaron todos los documentos del proceso, tanto los pre contractuales, como los de la ejecución del contrato.

Se evidenció que la plantilla del documento del acta de inicio no tiene número de radicado ni fecha en la primera hoja.

Etapa Contractual

Se realizó verificación a los siguientes pagos:

No. Pago	Período de cobro	Radicado
1	02 de febrero al 28 de febrero de 2023	20231200003714 Fecha 01-03-2023
3	1 de abril al 30 de abril de 2023	20231200009764 Fecha 05-05-2023
7	01 de agosto al 31 de agosto de 2023	20231200019254 Fecha 04-09-2023
9	01 de octubre al 31 de octubre de 2023	20231200025254 Fecha 03-11-2023
11	01 de diciembre al 31 de diciembre de 2023	20231200030324 Fecha 28-12-2023

* Elaboración OCI fuente Orfeo

Los informes 1 y 4 no indican número del informe y fecha.

Sin perjuicio de lo anterior, de los pagos revisados se logró establecer que las evidencias y documentos cargados por el contratista cumplen con las obligaciones establecidas en el contrato, asimismo se constató de los informes de supervisión.

Mediante comunicación del 5 de abril Radicado 20231200037723 el contratista solicitó la cesión o terminación anticipada del contrato a partir del 15 de abril. No obstante, el 12 de abril Radicado 20231200039613 el supervisor solicitó a la Oficina Jurídica la interrupción del trámite de liquidación del contrato, puesto que el contratista manifiesto su interés de continuar prestando sus servicios a la FUGA.

Radicado 20231200113533 de 8 de noviembre se adelantó la adición y prórroga del contrato hasta el 5 de enero de 2024. La modificación se realizó el 17 de noviembre Radicado 2023130011709. La plantilla del documento no tiene número de radicado ni fecha.

Radicado 20241200008563 de 22 de enero de 2024 se diligenció paz y salvo por desvinculación.

4.2. ORFEO

FUGA 63 de 2023	
Tipo de proceso	Contratación Directa
No. de proceso	FUGA-CD-63-2023 https://www.secop.gov.co/CO1ContractsManagement/Tendering/ProcurementContractEdit/View?docUniqueIdentifier=CO1.PCCNTR.4522920&prevCtxUrl=https%3a%2f%2fwww.secop.gov.co%3a443%2fCO1ContractsManagement%2fTendering%2fProcurementContractManagement%2fIndex&prevCtxLbl=Contratos+
Expediente Orfeo	202313002000900007E
Objeto	Prestar los servicios profesionales a la Fundación Gilberto Alzate Avendaño en el mantenimiento y actualización de las herramientas informáticas del sistema de gestión documental.
Contratista	**IDELBER SÁNCHEZ**
Valor inicial	$ 47.907.000
Valor prorroga	$2.235.6600
Aprobación de la póliza	2 de febrero de 2022. Radicado 20231300017273
Adición y Prorroga	1
Fecha de suscripción del contrato	31 de enero de 2023
Fecha de acta de inicio	2 de febrero de 2022. Radicado **20232900017393**
Fecha de terminación inicial	15 de diciembre de 2023
Fecha de terminación final	10 de enero de 2023
Anticipo	N/A
Modificaciones	N/A
Comunicación de Supervisión Contrato	03 de febrero de 2023. Radicado 20232000018013
Supervisor	Gala Margarita Forero Yanquen
Apoyo a la supervisión	Edwin Gustavo Díaz Méndez – Contratista Líder TIC

* Elaboración OCI fuente Orfeo

Etapa pre contractual

En los Estudios previos Radicado 20232000013813, se identificó que se requiere contar con los servicios de un profesional que apoye a la Subdirección de Gestión Corporativa en el acompañamiento y soporte de las herramientas y/o aplicaciones relacionadas con gestión documental, por el término del plazo establecido, el cual se estima es el estrictamente necesario y suficiente para lograr el cumplimiento de los programas, planes y proyectos de la entidad, en consonancia con el principio de anualidad presupuestal.

En cumplimiento del artículo 4° de la Ley 1150 de 2007, así como el artículo 2.2.1.1.1.6.3., y numeral 6 del artículo 2.2.1.1.2.1.1., del Decreto 1082 de 2015, se estableció entre otros, como riesgo previsible que puede afectar la ejecución y el cumplimiento del contrato:

Que puede pasar	Consecuencia	Controles	Monitoreo
El diseño del software propuesto por el contratista no cumpla con los requerimientos solicitados por gestión documental	Realizar nuevamente el diseño del software, de acuerdo a los requerimientos	Definir claramente los requisitos para el diseño del software	Informes de actividades del contratista.

* Elaboración OCI fuente Orfeo

Conforme lo anterior, se observa que no se incluyen dentro de los riesgos previsibles, riesgos tecnológicos asociados al cumplimiento del contrato; lo anterior teniendo en cuenta lo señalado en el *Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación de Colombia Compra Eficiente (M-ICR-01)*[23] ; adicionalmente y aunado a lo ya expuesto, se observa que en las obligaciones generales del contratista[24] solo se hace referencia, en materia de seguridad de la información, a la confidencialidad.

Revisado el expediente en el aplicativo de gestión documental ORFEO, se observa que se encuentra el diligenciamiento del formato “GJ-FT-24 Hoja de ruta”, de conformidad con el numeral 2 del título I, sección I “Aspectos Generales Procesos Competitivos y Contratación Directa”, del Procedimiento contractual. Código GJ-PD-01.

El contrato en Secop fue firmado y aprobado el 31 de enero de 2023, asimismo se publicaron los documentos requeridos para la suscripción y ejecución del contrato.

La plantilla del documento de acta de inicio no cuenta con radicado Orfeo ni fecha.

Etapa Contractual

Se realizó verificación a los siguientes pagos:

No. Pago	Período de cobro	Radicado
1	02 de febrero al 28 de febrero de 2023	20232900005644 Fecha 09-03-2023
4	1 de mayo al 31 de mayo de 2023	20232900018284 Fecha 28-08-2023
7	01 de agosto al 31 de agosto de 2023	20231200019254 Fecha 20-10-2023
10	01 de noviembre al 30 de noviembre de 2023	20242900001724 Fecha 12-02-2024

[23] Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación de Colombia Compra Eficiente (M-ICR-01). Numeral 2 Identificar y clasificar los Riesgos. Tipo: Riesgos Tecnológicos: son los derivados de fallas en los sistemas de comunicación de voz y de datos, suspensión de servicios públicos, nuevos desarrollos tecnológicos o estándares que deben ser tenidos en cuenta para la ejecución del contrato, obsolescencia tecnológica.

[24] Estudios Previos Contrato FUGA-63-2023: 2.8. Obligaciones Generales del Contratista: 3. Guardar reserva con respecto de la información que llegase a conocer con ocasión de la ejecución del contrato, al igual que no compartir ningún tipo de información que repose en los computadores de la entidad con ningún propósito.

La forma de pago del contrato establece *"2. **Pagos intermedios: Mensualidades vencidas**, cada una por valor de CUATRO MILLONES SETECIENTOS NOVENTA MIL SETECIENTOS PESOS ($4.790.700 M/CTE)"* Negrilla fuera de texto. En ese sentido, se evidencia que el pago No. 4 fue radicado en el mes de agosto., el pago No 7. en octubre y el pago No. 10 en febrero de 2024.

El 20 de septiembre se solicitó adición y prórroga del contrato Radicado 20232000096613. CDP 686 de 21 de septiembre Radicado 20232500096943.

Mediante Radicado 20232300109473 del 31 de octubre se modificó el contrato y se prorrogó hasta el 15 de diciembre, teniendo en cuenta los requerimientos definidos para el proceso de Gestión Documental, en relación a la elaboración e implementación del Modelo del Sistema de Gestión de Documento Electrónico - SGDEA y la tabla de control de acceso, actividades que son acompañadas por el contratista y que se encuentran programadas en los planes estratégicos del PINAR y de MIPG para el 15 de diciembre de 2023.

La minuta de modificación se realizó el 7 de noviembre Radicado 20231300111973.

Finalmente, de los pagos revisados se evidenció que el contratista cumplió con las obligaciones contractuales.

4.3. ALOJAMIENTO WEB. HOSTING

FUGA 170 de 2021	
Tipo de proceso	Mínima Cuantía
No. de proceso	FUGA-PMC-155-2021
Expediente Orfeo	202113002000900128E
Objeto	Renovación hosting página web
Contratista	GOPHER GROUP S.A.S
Representante Legal	Ana María Ruge Diez
Valor inicial	$14.259.289
Adiciones	N/A
Fecha de suscripción del contrato	9 de agosto de 2021
Fecha aprobación de la póliza	18 de agosto de 2021
Fecha de acta de inicio	18 de agosto de 2021
Fecha de terminación inicial	2 de enero de 2024 Nota: Teniendo en cuenta que el tiempo de suscripción de la licencia es de veintiocho (28) meses y quince (15) días calendario; que en el plazo de ejecución se habían definido ocho (8) días calendario adicionales, para que el contratista realizara la fase de instalación, migración y puesta en funcionamiento entre el actual hosting y el entrante y que el contratista que resultó adjudicatario del proceso de selección y con quien se celebró el contrato es el mismo con el que se contaba con el servicio, este término (8 días calendario) no se requirió, quedando en definitiva como plazo de ejecución del contrato veintiocho (28) meses y quince (15) días calendario.
Fecha prorroga 1	2 de febrero 2024

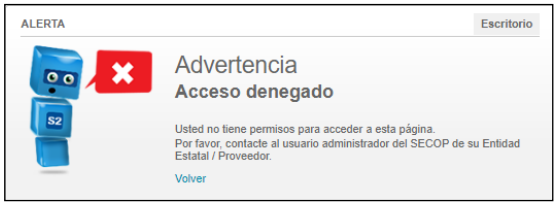
Fecha prorroga 2	2 de abril 2024
Anticipo	N/A
Plazo inicial	14 de mayo de 2023
Modificación 1	$539.858
Modificación 2	$1.136.155
Modificación 3	$4.990.794
Supervisor inicial	Édgar Leonardo Barbosa Trujillo Radicado 20242000040503
Apoyo a la supervisión	Edwin Gustavo Díaz Méndez John Fredy Salinas Arévalo

* Elaboración OCI fuente Orfeo

Etapa Precontractual

Revisado el expediente en el aplicativo de gestión documental Orfeo; se observa que no se encuentra el diligenciamiento del formato “GJ-FT-07 Hoja de Ruta Mínima Cuantía”, de conformidad con el Procedimiento contractual. Código GJ-PD-01 V15.

No fue posible la revisión del proceso en Secop II:



En los estudios previos Radicado 20212000063693 se analizó el estudio de mercado con el fin de identificar los precios del servicio tecnológico que se requería, conforme con lo dispuesto en el artículo 25-7 y 25-121 de la Ley 80 de 1993, la Ley 1150 de 2007 y el Decreto 1082 de 2015; por tanto, se hizo necesario adelantar el proceso de selección correspondiente a la renovación del hosting de la página web bajo la modalidad de Mínima Cuantía.

Se determinó que la Fuga contaba con un proceso denominado *“Gestión Tecnológica de la Información”,* que sirve de apoyo a las dependencias administrativas y misionales. Por tanto, con el rubro de *“Servicios de suministro de infraestructura de hosting y de tecnología de la información (TI)”,* se buscó adquirir el servicio de hosting para acceder al manejo de los equipos con los que cuenta la entidad.

Es así como, se necesitó de un servicio de alojamiento web (hosting), que permitiera mantener en línea y de forma ininterrumpida el portal www.fuga.gov.co, herramienta para publicar los contenidos de las actividades que se realizan en la entidad. La importancia de contar con este servicio radicó en que es allí donde se almacenan los archivos que permiten al público en general visualizar lo publicado vía internet.

Para tal efecto, se tuvieron en cuenta empresas del sector objeto de la contratación, específicamente se invitó a cotizar a GOPHER GROUP y CLOUD COLOMBIA.

En cumplimiento del artículo 4° de la Ley 1150 de 2007, así como el artículo 2.2.1.1.1.6.3., y numeral 6 del artículo 2.2.1.1.2.1.1., del Decreto 1082 de 2015, se estableció como riesgo previsible que puede afectar la ejecución y el cumplimiento del contrato:

Que puede pasar	Consecuencia	Controles	Monitoreo
Que el contratista no inicie la prestación del servido de alojamiento (hosting) objeto del presente proceso	Retraso en el desarrollo y ejecución de las diferentes actividades programadas	El supervisor del contrato requerirá constantemente al contratista para que este inicie la prestación de los servicios contratados, en el tiempo y con las especificaciones establecidas	Verificando que el contratista cumpla con las especificaciones y los tiempos establecidos, para dar inicio a la ejecución
Posible pérdida de Información en el empalme o la migración que realice el contratista .	Pérdida de la información y datos sensibles de la Fundación	El supervisor del contrato verificará el cumplimiento del protocolo que debe adelantar el contratista para el empalme, migración e implementación del nuevo hosting.	Verificando que el Contratista cumpla con el protocolo para el empalme, migración e implementación del nuevo hosting

* Elaboración OCI fuente Orfeo

Conforme lo anterior, se observa que se incluyen dentro de los riesgos previsibles, un riesgo tecnológico asociado al cumplimiento del contrato; lo anterior teniendo en cuenta lo señalado en el *Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación de Colombia Compra Eficiente (M-ICR-01).* Se observa adicionalmente que la situación vinculada a éste, está articulada con la integridad en la gestión de la información.

Mediante acta del 2 de febrero de 2011 Radicado 20212000065933 se designaron a los miembros del comité evaluador para la verificación de requisitos mínimos habilitantes de índole jurídico, técnico y económico. En el mismo radicado se adjuntaron los documentos referentes al informe de evaluación preliminar.

Una vez verificada la oferta presentada por GOPHER GROUP S.A.S., y realizada la evaluación económica, técnica y jurídica, se estableció que cumplía con lo establecido en la invitación, por tanto se dio traslado para observaciones hasta el día 04 de agosto de 2021, sin embargo no se presentaron observaciones a la misma.

En virtud de lo anterior, por medio de comunicación de 9 de agosto el Representante Legal de GOPHER GROUP S.A.S. aceptó la Oferta del Proceso de Selección de Mínima Cuantía No. FUGA-PMC-155-2021. Radicado 20211300069193.

En la aceptación de la oferta se estableció la suma de $14.259.289, teniendo en cuenta los ítems contratados. Igualmente, se definieron los valores correspondientes para cada vigencia:

Vigencia	Valor mensual	Meses	Valor por vigencia
Vigencia 2021	$481.883	4 meses y 15 días calendario	$2.168.471
Vigencia 2022	$496.339	12 meses	$5.956.068
Vigencia 2023	$511.229	12 meses	$6.134.750
Valor total			$14.259.289

Etapa Contractual

Se realizó verificación a los siguientes pagos:

No. Pago	Período de cobro	Radicado
1	18 de agosto al 17 de septiembre de 2021	20212000021444 Fecha 20-10-2021
4	18 de noviembre al 17 de diciembre de 2021	20212300016464 Fecha 19-08-2021
7	01 de febrero al 28 de febrero de 2022	20222900011064 Fecha 16-05-2022
10	01 de mayo al 31 de mayo de 2022	20222900025374 Fecha 16-09-2022
14,15,16	01 de septiembre de 2022 al 30 de noviembre de 2022	20222300117273 Fecha 15-12-2022
18, 19, 20, 21	01 de enero al 30 de abril de 2022	20232900010634 Fecha 26-05-2023
26 y 27	01 de septiembre de 2023 al 30 de octubre de 2023	20232900026654 Fecha 17-11-2023
28 y 29	01 de noviembre de 2023 al 30 de diciembre de 2023	20242300040233 Fecha 22-04-2024

La Fuga se comprometió a realizar un primer pago con la entrega de la instalación, migración y puesta en funcionamiento del portal web, lo cual se cumplió y se constató con las evidencias aportadas.

Así mismo, en el Pago No.1 la plantilla del documento del informe del contratista no cuenta con radicado ni fecha, y no fue firmado por el contratista.

Pago No. 4. La fecha 19 de agosto de 2021 de radicación del informe de supervisión, no guarda relación con el periodo 18 de noviembre al 17 de diciembre de 2021, puesto que es un mes que antecede al que se pretende cobrar. La plantilla del documento del informe de contratista no cuenta con radicado ni fecha, asimismo no fue firmado con el contratista.

CONTRATO No. FUGA-170-2021

Radicado: **20212300016464**
Fecha: 19-08-2021

1. INFORMACIÓN GENERAL

Nº DE CONTRATO Y FECHA DE SUSCRIPCIÓN	FUGA-170-2021 05 de AGOSTO de 2021
NOMBREO RAZÓN SOCIAL DEL CONTRATISTA	GOPHER GROUP S A S
Nº DE IDENTIFICACIÓN	900.425.485-8
PERIODO QUE ABARCA EL PRESENTE PAGO	DEL 18 DE NOVIEMBRE AL 17 DE DICIEMBRE DE 2021
OBJETO DEL CONTRATO	RENOVACIÓN HOSTING PÁGINA WEB.

Pago No. 7. La plantilla del documento del informe de supervisión no cuenta con radicado, asimismo el informe del contratista no cuenta con radicado ni fecha, tampoco fue firmado.

Pago No. 10. La plantilla del documento del informe de supervisión no cuenta con radicado, asimismo la del informe del contratista no cuenta con radicado ni fecha, tampoco fue firmado.

Pagos No. 14. 15. 16. La plantilla del documento del informe de supervisión no cuenta con radicado, asimismo la del informe del contratista no cuenta con radicado ni fecha.

Pagos No. 18, 19, 20, 21. La plantilla del informe del contratista no cuenta con radicado ni fecha.

Pagos No. 26 y 27. La plantilla del documento del informe de supervisión no cuenta con radicado. El informe del contratista indica que corresponde a los pagos 26, 27 y 28. La plantilla no cuenta con radicado ni fecha, tampoco está firmado.

Pagos No. 28 y 29 la factura tiene fecha de 12 de enero de 2024. La plantilla del documento del informe de contratista no cuenta con radicado ni fecha, y no fue firmado. No se evidencia el soporte del cargue en Secop II.

La forma de pago del contrato establece *"La Fundación se compromete a pagar el valor de la aceptación de oferta, en pagos mensuales o por fracción de mes, de acuerdo a los servicios efectivamente prestado; el primero será tramitado tan pronto el contratista realice la instalación, migración y puesta en funcionamiento del portal web (que cumpla con las características descritas en la ficha técnica); para cada uno de los pagos el contratista deberá radicar la factura, presentar la certificación de pago de aportes a Seguridad Social y Parafiscales, del contrato."*

En virtud de lo anterior, es claro que los pagos no se realizaron de forma mensual de acuerdo a los servicios prestados, según lo establecido en los estudios previos y en la aceptación de la oferta.

Por consiguiente, se genera incumplimiento en el numeral 16.3 del Manual de supervisión e Interventoría, código GJ-MN-02 Versión 3, que establece que el Supervisor, deberá cumplir a cabalidad con las funciones de tipo administrativo, técnicas, jurídicas, financieras y contables, so pena de la imposición de las sanciones legales, reglamentarias y contractuales correspondientes.[25]. Lo que constituye un hallazgo.

Ahora bien, se solicitó adición y prórroga del contrato Radicado 20232000055623 y 20232900068383, teniendo en cuenta que el servicio de hosting es indispensable para la comunicación constante entre la Fuga y los ciudadanos; por lo cual, se adiciona por el término de un (1) mes. Modificación No. 1 otrosi Radicado 20231300077463.

Radicado 20242300009083 solicitud de adición y prórroga. Radicado 20241300010383 Modificación No.2, dado que es necesario mantener la continuidad del servicio de hosting que actualmente tiene contratado la entidad, pues por medio de este se puede asegurar que el sitio web de la entidad esté disponible las 24 horas del día, los 7 días de la semana, y de esta manera se pueda mantener los servidores en funcionamiento. Se realizó por el término de dos (2) meses.

Modificación No. 3 Radicado 20242900027213 se adicionó la suma de cuatro millones novecientos noventa mil setecientos noventa y cuatro pesos ($4.990.794) m/cte., respaldados por medio del Certificado de Disponibilidad Presupuestal No. 366 (BogData 546894) del 7 de marzo de 2024. Radicado 20241300027883 minuta de modificación.

4.4. Adquisición De Licenciamiento Tecnológico

FUGA 127 de 2023	
Tipo de proceso	Subasta Inversa
No. de proceso	FUGA-SASI-112-2023 https://www.secop.gov.co/CO1ContractsManagement/Tendering/ProcurementContractEdit/View?docUniqueIdentifier=CO1.PCCNTR.5395421&prevCtxUrl=https%3a%2f%2fwww.secop.gov.co%3a443%2fCO1ContractsManagement%2fTendering%2fProcurementContractManagement%2fIndex&prevCtxLbl=Contratos+
Expediente Orfeo	20231300200090011OE
Objeto	Adquisición de licenciamiento tecnológico para la Fundación Gilberto Alzate Avendaño
Contratista	INGENIERÍA DE SISTEMAS TELEMÁTICOS (INSITEL S.A.).
Valor inicial	$ 69.818.133
Aprobación de la póliza	29 de septiembre de 2023. Radicado 20231300017273
Fecha de suscripción del contrato	21 de septiembre de 2023
Fecha de acta de inicio	21 de septiembre de 2023
Fecha de terminación inicial	12 de enero de 2024

[25] https://www.fuga.gov.co/sites/default/files/2022-05/gj-mn-02_manual_de_supervision_e_interventoria_v322122021_0.pdf

Fecha de terminación final	10 de enero de 2023
Comunicación de Supervisión Contrato	03 de febrero de 2023. Radicado 20232000018013
Supervisor	Andrea Isabel Casas Bohórquez
Apoyo a la supervisión	Edwin Gustavo Díaz Méndez – Contratista Líder TIC

* Elaboración OCI fuente Orfeo

Etapa pre contractual

El contrato en Secop II fue firmado y aprobado el 31 de enero de 2023; sin embargo, el equipo auditor no pudo verificar los documentos pre contractuales en la plataforma, solo se evidencia el cargue del contrato y el único pago.

En ese orden, revisado el expediente en el aplicativo de gestión documental ORFEO, se observa que se encuentra el diligenciamiento del formato “GJ-FT-24 Hoja de ruta”, de conformidad con el Procedimiento contractual. Código GJ-PD-01.

En estudios previos se determinó que la Fuga cuenta con infraestructura tecnológica que requiere ser respaldada y soportada, por lo cual se hace necesaria la renovación del software, siendo el caso específico la renovación del antivirus, firewall y servicios de almacenamiento en la nube, así como la articulación de diferentes componentes de red y servicios tecnológicos internos emergentes que requieren un licenciamiento especifico como lo es Power Bi Pro, permitiendo con esto una adecuada interacción entre el hardware y software.

Por lo tanto, la Fuga requirió para su funcionamiento, además de la renovación las licencias con las que cuenta, una licencia Power BI Pro, la cual permite leer, interactuar y generar analítica de datos mediante informes y paneles de información asociada a las actividades de planeación del aplicativo Pandora, el cual se encuentra en este momento instalado en la infraestructura tecnológica de la Fundación. El poder contar con esta licencia permite tener una amplia variedad de consultas que se pueden utilizar para el análisis de datos, no solo para analizar con mayor detalle los datos históricos, sino también para poder pronosticar eventos y comportamientos futuros, de acuerdo a los datos que se evalúen. Esto brinda la posibilidad de realizar análisis hipotéticos, la creación de informes claros con un diseño atractivo, llevando poco tiempo y estando disponibles de inmediato.

Se estableció que de no cumplir con lo estipulado se estaría aumentando el riesgo de materializar amenazas como:

- Pérdida de conectividad por daño o bloqueo en la operación lógica interna del hardware asociado.
- Inadecuada gestión de los datos, lo que conllevaría a situaciones de retraso.
- Pérdida de interacciones entre las aplicaciones.
- Pérdida de conectividad entre las sedes de la entidad, generando un deterioro en la ejecución de los procesos de la Fundación.

ACTIVIDAD:	FECHA Y HORA:	LUGAR:
Publicación acto administrativo de apertura y pliego de condiciones definitivo.	Jueves 17 de agosto de 2023.	SECOP II (www.colombiacompra.gov.co)
Presentación de observaciones a los pliegos de condiciones definitivo.	Miércoles 23 de agosto de 2023.	SECOP II (www.colombiacompra.gov.co)
Respuesta a las observaciones al pliego de condiciones definitivo.	Lunes 28 de agosto de 2023.	SECOP II (www.colombiacompra.gov.co)
Plazo máximo para expedir adendas.	Hasta el día hábil anterior al cierre.	SECOP II (www.colombiacompra.gov.co)
Cierre del proceso, plazo máximo de presentación de ofertas.	Jueves 31 de agosto de 2023 a las 10:00 a.m.	SECOP II (www.colombiacompra.gov.co)
Publicación del informe de verificación o evaluación.	Martes 05 de septiembre	SECOP II (www.colombiacompra.gov.co)
Presentación de observaciones al informe de verificación o evaluación /Término para subsanar.	Hasta el martes 12 de septiembre de 2023.	SECOP II (www.colombiacompra.gov.co)
Audiencia pública de subasta inversa	Lunes 18 de septiembre de 2023 a las 11:00 a.m.	SECOP II (www.colombiacompra.gov.co)
Publicación acto administrativo de adjudicación o de declaratoria de desierta.	Dentro de los dos (2) días hábiles siguientes a la fecha de expedición del documento.	SECOP II (www.colombiacompra.gov.co)
Firma del contrato.	Dentro de los dos (2) días hábiles siguientes a la adjudicación.	SECOP II (www.colombiacompra.gov.co)
Expedición del registro presupuestal.	Dentro del día hábil siguiente a la suscripción del contrato.	SECOP II (www.colombiacompra.gov.co)
Entrega de las garantías de ejecución del contrato	Dentro de los tres (3) días siguientes a la suscripción	SECOP II (www.colombiacompra.gov.co)

Ahora bien, fue competencia de la Subdirección de Gestión Corporativa realizar la contratación de la renovación de las licencias con las que cuenta la entidad, por medio de un proceso de selección (subasta inversa), por lo que se adelantó un estudio de mercado con el fin de identificar los precios de las licencias requeridas, relacionadas en la ficha técnica. Se tuvo en cuenta empresas del sector objeto de la contratación y se invitó a cotizar a 17 empresas del sector tecnológico, recibiendo respuesta únicamente por parte de INSITEL S.A., y PC TRONIC.

El plazo de la entrega de las licencias requeridas deberá ser realizado de acuerdo al siguiente cronograma:

- ENDPOINTS - SOPHOS - CIXH3CTAA (RENOVACIÓN): 15 de diciembre de 2023.
- FIREWALL - SOPHOS - XG-210 (RENOVACIÓN): 15 de diciembre de 2023.
- AWS CLOUD: 30 de noviembre de 2023.
- Power BI Pro: 30 de septiembre de 2023.

El 28 de julio de 2023 se determinaron los estudios previos definitivos, Radicado 20232000080113, por tanto mediante Resolución No. 153 de 2023, Radicado 20232000001535, se ordena la apertura del proceso de selección FUGA-SASI-112-2023 y se planteó el cronograma a seguir:

En cumplimiento del artículo 4° de la Ley 1150 de 2007, así como el artículo 2.2.1.1.1.6.3., y numeral 6 del artículo 2.2.1.1.2.1.1., del Decreto 1082 de 2015, se estableció entre otros, como riesgo previsible que puede afectar la ejecución y el cumplimiento del contrato:

Que puede pasar	Consecuencia	Controles	Monitoreo
Que el licenciamiento adquirido tenga modificaciones en sus condiciones y no sea susceptible de actualizaciones.	Retraso en el desarrollo de las actividades programadas, en la medida que no se podría suplir la necesidad, por cambio de políticas en el uso de las licencias adquiridas.	El supervisor del contrato efectuará un constante seguimiento al contratista, con el fin de confirmar que este brinde soporte en las actualizaciones que se puedan presentar	Verificando que el contratista efectúe el acompañamiento correspondiente, para la actualización de las licencias adquiridas.
Que las licencias presenten obsolescencia en su funcionamiento	Incompatibilidad entre las licencias suministradas por el contratista y los equipos tecnológicos con los que cuenta la Fundación	Atención y soporte por parte del contratista, para el cambio y/o la actualización de las licencias que sean requeridas.	Validando el correcto funcionamiento de las licencias adquiridas por la Fundación.

* Elaboración OCI fuente Orfeo

Conforme lo anterior, se observa que se incluyen dentro de los riesgos previsibles, riesgos tecnológicos asociados al cumplimiento del contrato; lo anterior teniendo en cuenta lo señalado en el *Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación de Colombia Compra Eficiente (M-ICR-01)*[26]; adicionalmente, se observa que en las obligaciones generales del contratista[27] se hace referencia, en materia de seguridad de la información, a la confidencialidad.

En virtud de lo indicado, se verificó el cumplimiento de los plazos, a saber:

Radicado 20232000089733 de 30 de agosto de 2023. Respuesta observación extemporánea.

Radicado 20231300090003 31 de agosto de 2023 se realizó la Verificación y evaluación preliminar de jurídica.

Radicado 20232000091073 de 04 de septiembre 2023 se designó al comité evaluador.

Radicado 20232000091963 de 05 de septiembre se realizó la Evaluación Preliminar de la verificación de requisitos habilitantes y evaluación preliminar. La plantilla del documento no indica radicado Orfeo ni fecha.

Sin perjuicio de lo anterior, fue modificado mediante una adenda, Radicado 20232000094523 13 de septiembre de 2022, pues la Subdirección de Gestión Corporativa solicitó modificar el cronograma del proceso

[26] Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación de Colombia Compra Eficiente (M-ICR-01). Numeral 2 Identificar y clasificar los Riesgos. Tipo: Riesgos Tecnológicos: son los derivados de fallas en los sistemas de comunicación de voz y de datos, suspensión de servicios públicos, nuevos desarrollos tecnológicos o estándares que deben
ser tenidos en cuenta para la ejecución del contrato, obsolescencia tecnológica.

[27] Estudios Previos Contrato FUGA-127-2023: 2.2.1. Obligaciones Generales del Contratista: 9. Guardar reserva con respecto de la información que llegase a conocer con ocasión de la ejecución del contrato, al igual que no compartir ningún tipo de información que repose en los computadores de la entidad con ningún propósito.

para la celebración de la apertura del sobre económico y la publicación de la lista de participantes (La plantilla del documento no indica radicado Orfeo ni fecha), así:

ACTIVIDAD	FECHA Y HORA	LUGAR
Apertura del sobre económico	Lunes 18 de septiembre 11:30 am	SECOP II www.colombiacompra.gov.co
Audiencia pública de subasta inversa electrónica	Lunes 18 de septiembre 11:30 am	Google Meets (Servicio de video-comunicación). meet.google.com/yog-dnkq-pqa O marca el: Más números de teléfono: https://tel.meet/yog-dnkq-pqa?pin=6796873233805
Publicación acto administrativo de adjudicación o de declaratoria de desierta.	Dentro de los dos (2) días hábiles siguientes a la celebración de la Audiencia de Subasta Inversa	SECOP II www.colombiacompra.gov.co
Firma del contrato	Dentro de los DOS (02) días hábiles siguiente a la adjudicación	SECOP II www.colombiacompra.gov.co
Expedición del Registro Presupuestal	Dentro del día hábil siguiente a la suscripción del contrato	Fundación Gilberto Alzate - FUGA
Entrega de garantías	Dentro de los dos (2) días hábiles siguientes a la suscripción del contrato	Fundación Gilberto Alzate – FUGA

* Elaboración OCI fuente Orfeo

Radicado 20231300094583 13 de septiembre 2023 se efectuó la Evaluación definitiva del proceso.

Radicado 20231300095423 de 18 de septiembre 2023 se realizó la evaluación económica y recomendación de adjudicación.

Cumplidas las fechas establecidas en el cronograma, se realizó audiencia subasta inversa electrónica en la que se adjudicó. a INGENIERÍA DE SISTEMAS TELEMÁTICOS - INSITEL S.A. Radicado 20231300095693. En ese orden, se profiere Resolución No. 179 de 2023 mediante la cual se adjudicó el proceso de selección abreviada de subasta inversa No. FUGA-SASI-112-2023. Radicado 20232000001795.

El contrato se realizó el 21 de septiembre 20231300097053. La póliza se aprobó el 29 de septiembre. Radicado 20231300099203. En la misma fecha se comunicó la supervisión del contrato. Acta de inicio Radicado 20232700100483 de 3 de octubre de 2023.

Etapa Contractual

No se encuentran cargados en Secop II los documentos de inicio de la ejecución del contrato, acta de inicio, CRP y la comunicación de designación al supervisor.

Se realizó la verificación del único pago establecido:

No. Pago	Período de cobro	Radicado
1	Diciembre de 2023	20232700030974 Fecha 29-12-2023

Factura electrónica generada el 12 de diciembre de 2023 en la cual se describe lo siguiente:

No. Pago	Descripción	Uni	Cant	V.Unit	Valor Total
0030001000008	CENTRAL INTERCEPT X ENDPONINT ADVANCED START AND END DATES: 12/21/2023 ?12/20/2026 (REPLACING EXISTING LICENSE D555255498 FOR109 CIXA-CU12/21/2020 ?12/20/2023 CENTRAL INTERCETP X ADVANCED? 100 ?199 USERS? RENEWAL	UN	1.00	27,468,000.00	27,468,000.00
0030001000014	RENOVACIÓN DE XSTREAM PROTECTION PARA XG 210 PARA 12 MESES		1.00	6,199,185.00	6,199,185.00
0030001000014	RENOVACIÓN DE WEBSERVER PROTECTION PARA XG 210 PARA 12 MESES		1.00	1,566,100.00	1,566,100.00
0030001000014	RENOVACIÓN DE EMAIL PROTECTION PARA XG 210 PARA 12 MESES		1.00	1,567,500.00	1,567,500.00
0030001000014	RENOVACIÓN DE SANDSTORM PARA XG 210 PARA 12 MESES		1.00	2,351,415.00	2,351,415.00
0030001000014	RENOVACIÓN DE SANDSTORM PARA XG 210 PARA 12 MESES		1.00	2,137,650.00	2,137,650.00
0030001000001	AWS CAPACIDAD 1TB PARA 3 MÁQUINAS VIRTUALES AMAZON SIMPLE STORAGE SERVICE (S3)	UN	1.00	15,704,150.00	15,704,150.00
0030004000032	LEER, INTERACTUAR Y GENERAR ANALÍTICA DE DATOS MEDIANTE INFORMES Y PÁNELES DE INFORMACIÓN ASOCIADA A LAS ACTIVIDADES DE PLANEACIÓN DEL APLICATIVO PANDORA	UN	1.00	1,676,700.00	1,676,700.00
				TOTAL BRUTO	58,670,700.00
				IVA	11,147,433.00
				TOTAL A PAGAR	69.818.133,00

* Elaboración OCI fuente Orfeo

En virtud de lo anterior y de lo estipulado en el cronograma relacionado en los estudios previos, y en el contrato se realizaron las siguientes entregas:

- Acta de entrega de 6 de diciembre:
  - Suministro de Renovación de licencia por doce (12) meses Xstream Protection, Webserver Protection, Email Protection, Sandstorm y Enhanced support para Sophos Firewall XG 210 al cliente Fundación Gilberto Alzate Avendaño. se adjunta pdf de confirmación de renovación de licencia.

- Suministro de renovación de licencia por treinta y seis (36) meses de Central Intercept X Endpoint Advanced para 109 dispositivos al cliente Fundación Gilberto Alzate Avendaño. se adjunta pdf de confirmación de renovación de licencia.

- Acta de entrega de 9 de noviembre:
  - Suministro de una (1) licencia por treinta y seis (36) meses de Amazon Simple Storage Service con capacidad de 1 TB para 3 máquinas virtuales al cliente Fundación Gilberto Alzate Avendaño – FUGA. se entrega acceso de cuenta.

- Acta de entrega de 2 de noviembre:
  - Suministro de una (1) licencia por veinticuatro (24) meses de Microsoft Power BI Pro al cliente Fundación Gilberto Alzate Avendaño – FUGA. No se evidenció en la factura. Se entrega acceso de cuenta administrador a Edwin Diaz.

Para demostrar el pago a seguridad el revisor fiscal, adjuntó certificación, en el que consta el pago por concepto de los aportes correspondientes al sistema de salud, pensión, riesgos profesionales, cajas de compensación familiar, Instituto Colombiano de Bienestar familiar-ICBF y Servicio Nacional de Aprendizaje-SENA, del mes de diciembre.

En conclusión, teniendo en cuenta lo evidenciado en la evaluación del contrato FUGA- 63-2023 se recomienda que para la solicitud de adiciones y prórrogas previamente se asegure que el supervisor realice el seguimiento adecuado del contrato, asegurando que la cuenta de cobro respectiva cuente con la radicación de los informes del contratista y el cumplimiento de las obligaciones.

En ese sentido, es importante fortalecer la gestión del supervisor con el fin de revisar que la factura o cuenta de cobro presentada por el contratista corresponda con los conceptos a pagar en el periodo respectivo, de acuerdo con lo pactado en el contrato, ya que en algunos contratos se presentaron cuentas de cobros de manera conjunta y no como se estableció en el clausulado de condiciones generales.

Finalmente, se observan oportunidades de mejora en las actividades de supervisión en Secop II, por tanto se requiere implementar criterios y controles para todos los procesos, por lo cual se sugiere que se verifiquen los documentos de ejecución pre contractual y contractual que deban ser cargados en la plataforma de acuerdo con lo requerido en el contrato.

5. MIPG:

De conformidad con la información dispuesta en la página web de la entidad (https://fuga.gov.co/transparencia-y-acceso-a-la-informacion-publica/planeacion-presupuesto-informes?field_fecha_de_emision_value=All&term_node_tid_depth=287), se observa el documento Seguimiento 31122023 Plan de Acción MIPG V28 2023; sobre el cual se realizaron las verificaciones correspondientes a las actividades cuya responsabilidad de ejecución corresponde al proceso auditado, o éste participa en conjunto con otros procesos en su implementación:

5.1. Producto ID 593: Registro de uso de datos abiertos que generen Publicaciones o aplicaciones por la ciudadanía

FUENTE	Gobierno Digital Direccionamiento y Planeación
LINEAMIENTO	Gestión con valores para el resultado Direccionamiento Estratégico y planeación
VARIABLES	TIC para Gobierno Abierto - Indicadores de resultado Componente TIC para Gobierno abierto
ATRIBUTOS DEL PRODUCTO	O por otros actores o grupos de interés (academia, centros de investigación, medios de comunicación, empresas, entre otros) con soportes
FRECUENCIA	ANUAL
IMPLEMENTACION (I) SOSTENIBILIDAD (S)	 S
AÑO	2023
FECHA	15/12/2023
AREA RESPONSABLE	CORPORATIVA -SISTEMAS
SI=100% P= 80% con observaciones	 100
EVIDENCIA	Se realiza informe dando alcance al registro de uso de datos de la entidad https://drive.google.com/drive/u/1/folders/1tpIvr1cQSuVg48ruPSojP2hlsAlaGUl1
CALIFICACIÓN OCI	100
OBSERVACIÓN OCI	De la consulta realizada al drive referenciado se observa: Informe registro de uso de datos abiertos que generen publicaciones o aplicaciones por la ciudadanía, el cual incluye las capturas de pantalla tomadas a partir de usuario que tiene la entidad asignada. Registro uso de datos: donde se identifican niveles en la entidad para la toma decisiones basadas en datos, las fases del ciclo de vida del dato que se gestionaron en la entidad y lo relacionado con Datos maestros.

Fuente: Seguimiento 31122023 Plan de Acción MIPG V28 2023

5.2. Producto ID 722: Sistema de Gestión de Documento Electrónico (ORFEO)

FUENTE	Gestión Documental Control Interno
LINEAMIENTO	5 Información y Comunicación 7 Control Interno
VARIABLES	Tecnológica Información y Comunicación/ Responsabilidades de la Alta dirección y Comité Institucional de Coordinación de Control Interno (línea estratégica)
ATRIBUTOS DEL PRODUCTO	Elaborar y diseñar el Modelo de requisitos para la Gestión de Documentos Electrónicos de Archivo que permita que los documentos de la fundación cuenten con la integridad, autenticidad, inalterabilidad, disponibilidad, preservación y metadatos.
FRECUENCIA	ANUAL

IMPLEMENTACION (I) SOSTENIBILIDAD (S)	I
AÑO	2023
FECHA	30/12/2023
AREA RESPONSABLE	CORPORATIVA- DOCUMENTAL Y SISTEMAS
SI=100% P= 80% con observaciones	100
EVIDENCIA	Se han realizado mesas técnicas entre los proceso de Tecnologías de la Información y Gestión Documental para la elaboración y diseño del Modelo de Gestión de Documento Electrónico Acta de reunión 8 de septiembre de 2023 bajo radicado No 20232300100993. Acta de reunión del 25 de octubre de 2023 bajo radicado No 20232300120033 Acta de reunión 9 de noviembre bajo radicado (pendiente) Se presenta para aprobación ante Comité Interno de Archivo en sesión del 30/11/2023 https://orfeo.fuga.gov.co/centroAyuda/ Acta de reunión con radicado 20232300100993 y 20232300120033
CALIFICACIÓN OCI	80
OBSERVACIÓN OCI	En la sesión del 30/11/2024 (20232300133583) se observa la presentación de los grupos de requisitos que se consideran aplicar en el Modelo de la entidad; sin embargo, no se evidencia de manera clara cuál es el modelo elaborado y diseñado presentado.

Fuente: Seguimiento 31122023 Plan de Acción MIPG V28 2023

5.3. Producto ID 780: Acto administrativo de aprobación de Registro de Activos de Información actualizados

FUENTE	Transparencia y Acceso a la Información
LINEAMIENTO	5 información y Comunicación
VARIABLES	Instrumentos gestión de la información
ATRIBUTOS DEL PRODUCTO	Incluido el inventario de activos de seguridad y privacidad de la información; con la información publicada en la sección de Transparencia de la Web oficial
FRECUENCIA	ANUAL
IMPLEMENTACION (I) SOSTENIBILIDAD (S)	S
AÑO	2023
FECHA	15/09/2023
AREA RESPONSABLE	CORPORATIVA- DOCUMENTAL- SISTEMAS
SI=100% P= 80% con observaciones	100
EVIDENCIA	"Resolución No. 174 de 2023 “Por la cual se adoptan los Instrumentos de la Gestión de Información Pública en la Fundación Gilberto Alzate Avendaño y se deroga la Resolución No. 0096 de 2017.”
CALIFICACIÓN OCI	80
OBSERVACIÓN OCI	EL Registro de activos de información no se encuentra actualizado. El publicado tiene fecha 01/08/2021

Fuente: Seguimiento 31122023 Plan de Acción MIPG V28 2023

5.4. Producto ID 781: Inventario de activos de información relevante (interna y Externa) actualizado periódicamente de acuerdo a los lineamientos de la guía metodológica activos información fuga vigente. (Componente comunicaciones interna MECI)

FUENTE	Transparencia y Acceso a la Información Seguridad Digital
LINEAMIENTO	5 información y Comunicación
VARIABLES	Instrumentos gestión de la información
ATRIBUTOS DEL PRODUCTO	con las siguientes tipologías (documental, seguridad digital, colección de arte, biblioteca, etc), publicadas en los sitios web oficiales
FRECUENCIA	ANUAL
IMPLEMENTACION (I) SOSTENIBILIDAD (S)	 S
AÑO	2023
FECHA	15/12/2023
AREA RESPONSABLE	CORPORATIVA- DOCUMENTAL- SISTEMAS Y COMUNICACIONES
SI=100% P= 80% con observaciones	 100
EVIDENCIA	Los datos se encuentran publicados en datos abierto y en la página web, para la fecha de reporte se está gestionando una baja de elementos es por ello que no se actualiza al corte dado que muchos de estos elementos cambiaran su destino. Resolución No. 174 de 2023 “Por la cual se adoptan los Instrumentos de la Gestión de Información Pública en la Fundación Gilberto Alzate Avendaño y se deroga la Resolución No. 0096 de 2017.” El Inventario de activos de información relevante se encuentra actualizado https://datosabiertos.bogota.gov.co/dataset?organization=fundacion-gilberto-alzate-avendano https://fuga.gov.co/search/node?keys=activos https://www.fuga.gov.co/transparencia-y-acceso-a-la-informacion-publica/datos-abiertos?field_fecha_de_emision_value=All&term_node_tid_depth=325
CALIFICACIÓN OCI	80
OBSERVACIÓN OCI	Si bien se observan las tipologías definidas (inventarios de hardware y software, bases de datos y obras de arte); no se encuentran actualizados, son inventarios al corte del 2021

Fuente: Seguimiento 31122023 Plan de Acción MIPG V28 2023

5.5. Producto ID 956: Sistema de Gestión de Seguridad de la Información SGSI

FUENTE	Direccionamiento y Planeación Seguridad Digital
LINEAMIENTO	2 Direccionamiento Estratégico y Planeación
VARIABLES	FURAG- Alistamiento para la implementación del Sistema de Gestión de Seguridad de la Información
ATRIBUTOS DEL PRODUCTO	Formalizado mediante acto administrativo y formulado: - A partir de las necesidades identificadas - Con la definición del alcance

	- Con la definición de objetivos específicos de seguridad de la información - Roles y responsabilidades específicos - Con la integración de campañas de comunicación y concientización en temas de seguridad de la información para cada uno de los distintos roles dentro de la entidad () - Con ejercicios de simulación de incidentes de seguridad digital al interior de la entidad, incluyendo campañas de phishing, smishing, entre otros - Estableciendo convenios o acuerdos con otras entidades en temas relacionados con la defensa y seguridad digital.
FRECUENCIA	EVENTUAL POR NECESIDAD NORMATIVA
IMPLEMENTACION (I) SOSTENIBILIDAD (S)	I
AÑO	2023
FECHA	30/11/2023
AREA RESPONSABLE	CORPORATIVA- SISTEMAS
SI=100% P= 80% con observaciones	100
EVIDENCIA	Se relaciona la resolución, política actualizada y la campaña phishing realizada en la entidad. http://intranet.fuga.gov.co/sites/default/files/gt-po-01_politicas_seguridad_de_la_informacion_v3_20112023.pdf https://fuga.gov.co/transparencia-y-acceso-a-la-informacion-publica/normograma/resolucion-219-de-2023
CALIFICACIÓN OCI	80
OBSERVACIÓN OCI	No se evidencian convenios o acuerdos con otras entidades en temas relacionados con la defensa y seguridad digital.

Fuente: Seguimiento 31122023 Plan de Acción MIPG V28 2023

5.6. Producto ID 970: Integrar y o actualizar clausulados en los procesos contractuales

FUENTE	Seguridad Digital
LINEAMIENTO	3 Gestión con valores para el resultado
VARIABLES	FURAG- Alistamiento para la implementación del Sistema de Gestión de Seguridad de la Información
ATRIBUTOS DEL PRODUCTO	relacionados con el cumplimiento de las políticas de ciberseguridad internas, por parte de los proveedores y contratistas de la entidad
FRECUENCIA	ANUAL
IMPLEMENTACION (I) SOSTENIBILIDAD (S)	S
AÑO	2023
FECHA	30/11/2023
AREA RESPONSABLE	CORPORATIVA- SISTEMAS JURIDICA
SI=100% P= 80% con observaciones	100
EVIDENCIA	Se actualizó el formato GJ-FT-13 Estudios Previos Tipo Prestación De Servicios y/o Apoyo a la Gestión. Que garantiza la inclusión de clausulados en los procesos contractuales relacionados con el cumplimiento de las políticas de ciberseguridad internas, por parte de los proveedores y contratista de la entidad. Se procedió a actualizar el apartado No. 2.8 Obligaciones generales del contratista.

	*Actualización en la intranet https://intranet.fuga.gov.co/proceso-gestion-juridica
CALIFICACIÓN OCI	80
OBSERVACIÓN OCI	La gestión reportada corresponde a la actualización realizada en febrero de 2024. En la vigencia 2023 no se tenían incluidas políticas de ciberseguridad internas incluidas dentro de los procesos contractuales con proveedores internos y externos. No se ejecutó en el plazo establecido.

Fuente: Seguimiento 31122023 Plan de Acción MIPG V28 2023

Conforme lo anterior se observa que, de los 6 productos evaluados los cuales fueron reportados con una calificación de cumplimiento del 100%; desde la verificación de la OCI, en 5 de ellos el soporte que da cuenta de su ejecución no permite identificar la implementación integral de los atributos de los productos por lo que no se puede evaluar como 100% su ejecución. Esta situación generó que en el Plan MIPG 2024 (Versión 30) no se incluyeran los productos que no tuvieron una implementación integral.

De acuerdo a lo anteriormente expuesto se recomienda incluir en el plan 2024 los productos que no fueron ejecutados de manera integral y asegurar su cumplimiento conforme los atributos identificados.

6. Gestión de Riesgos:

6.1. Implementación del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información:

Se realiza la validación frente a lo dispuesto en el documento *Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas – Anexo Técnico* (Anexo 4 – DAFP) de MinTIC[28], en articulación con lo dispuesto la Resolución 500 de 2021 de MinTIC, "*Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital*."

Fase 1. Planificación (*Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas* del DAFP pasos 1, 2 y 3):

- *Contexto interno y externo de la entidad pública*: Como se mencionó en la evaluación del MSPI no se identifica:
  - En el alcance de las Políticas de Seguridad de la Información GT-PO-01 la definición del contexto interno, externo y del proceso para la gestión del riesgo conforme se establece en la ISO 3001:2009 numeral 5.3;

[28] Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas – Anexo Técnico (Anexo 4 – DAFP) de MINTIC Numeral 1.3. Alcance del documento: Este documento complementa y profundiza lo expuesto en la **Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas**, emitida conjuntamente entre el Departamento Administrativo de la Función Pública y la Secretaría de Transparencia de la Presidencia de la República, específicamente en las secciones de Análisis del contexto (con un enfoque hacia el entorno digital), identificación de activos, catálogos de amenazas y vulnerabilidades para el análisis de riesgos de seguridad de la información, controles para la mitigación de los riesgos de seguridad de la información, el reporte de riesgos de seguridad de la información y otros aspectos adicionales para llevar a cabo una gestión del riesgo de seguridad de la información adecuada.

- Las partes interesadas pertinentes y los requisitos de las mismas (legales, reglamentarios y las obligaciones contractuales);
- Los procesos para manejar desviaciones y excepciones;
- Los roles y responsabilidades respecto al **MSPI**, se definen de manera genérica y no se evidencia lo relacionado con la Oficina Jurídica y Talento Humano;
- Los registros de activos de información publicados se encuentran desactualizados;
- No se tiene definida la Declaración de Aplicabilidad por lo que no es posible identificar los controles a omitir en la evaluación de riesgos;

Respecto al contexto externo no se evidencian entre otros factores, la cantidad de ciudadanos a los cuales la entidad brinda servicios a través del entorno digital como trámites a través de la página web y los aspectos externos que pueden verse afectados con los riesgos de seguridad de la información, tales como el ambiente social, económico y factores ambientales que tengan alguna relación con las operaciones asociadas a la entidad, señalados en el MNGRSI.

En la entrevista realizada al proceso el 16/05/2024 se indica que esta gestión se realizó a través de la caracterización de los grupos de interés que realizo la Oficina Asesora de Planeación, adicionalmente se toman en cuenta los temas relevantes evidenciados a través de los reportes de PQRS. Respecto a los aspectos externos señalan que se hizo sobre aquellos que fueron identificados cuando se incluyeron en el mapa de riesgos.

De acuerdo a lo expuesto por el proceso se realizó la verificación del documento referenciado (*Caracterización de ciudadanía y grupos de valor* – Mayo 2023)[29], se identifica la población que podría verse afectada con el acceso a servicios de manera virtual a través de la página web, teniendo como medición el total de la población encuestada. No se identifica la cantidad de ciudadanos que pueden verse afectados en los aspectos externos vinculados a los ambientes social, económico y ambiental.

- *Alcance para aplicar la gestión de riesgos de seguridad de la información*: No se identifican los criterios diferenciales del MSPI para vincular los procesos con la gestión de riesgos de seguridad de la información.

  De acuerdo a lo indicado por el proceso en la entrevista del 16/05/2024, los procesos vinculados a la gestión de riesgos de seguridad de la información fueron identificados a través de mesas de trabajo realizadas con la Oficina Asesora de Planeación, en trabajo articulado con cada uno de los procesos de la entidad, dentro de los cuales integraron a su gestión de riesgos los de seguridad de la información los procesos de Servicio al Ciudadano, Gestión Financiera, Talento Humano y en el proceso Misional, la Subdirección Artística y Cultural; sin embargo, si bien se aclara la metodología aplicada, no se evidencia los criterios diferenciales aplicados.

- *Alineación o creación de la política de gestión de riesgo de seguridad de la información*: Se observa que la entidad estableció una política de gestión de riesgo integral a través del documento *Política de administración del riesgo GM-PO-01*, en la cual se incluye el compromiso en la gestión de los riesgos de

[29] https://fuga.gov.co/sites/default/files/2023-04/caracterizacion-ciudadania-grupos-valorfuga-v3-29052023.pdf

seguridad de la información; se evidencia que el documento está diseñado conforme lo indica la *Guía de administración del riesgo de gestión* del DAFP.

- *Definición de roles y responsabilidades respecto al **MNGRSI***: La entidad además de definir los roles y responsabilidades establecidas en la "*Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad de la información. Diseño de Controles en Entidades Públicas*" del DAFP, debe designar un responsable de seguridad digital[30], con responsabilidades definidas que deberá cumplir respecto a la gestión del riesgo de seguridad de la información[31].

  En la Resolución Interna 219 de 2023 por la cual se adopta el modelo de seguridad de la información en la entidad y los expedientes de los contratos de los profesionales vinculados al proceso auditado, no se evidencia la designación del *Responsable de Seguridad Digital* ni obligaciones relacionadas a las responsabilidades especificas señaladas en el MNGRSI referenciadas en la nota de pagina 31. En la entrevista realizada el 16/05/2024 se indica que no se encuentra designado oficialmente el *Responsable de Seguridad Digital*, que esta gestión se articula con la gestión del Oficial de Seguridad, sobre lo cual como ya se señaló en el ítem 2.1. Control A.6 del presente informe, tampoco se encuentra designado.

Conforme lo anterior, se genera un hallazgo vinculado a los roles y responsabilidades frente al MNGRSI, el cual se articulará con el identificado por incumplimiento de lo establecido en la Resolución Interna 219 de 2023 frente a la designación del Oficial de Seguridad en la tabla de Hallazgos.

- *Definición de recursos para la Gestión de riesgos de seguridad de la información*[32]: Si bien se observa a través del proyecto de inversión **7760 Modernización de la Arquitectura Institucional de la FUGA**, específicamente en la meta proyecto 3. *Implementar el 90% de la Política de Gobierno Digital*, la destinación para el periodo auditado (2023) de un presupuesto final de 182 Millones ejecutado al 100% al cierre de la vigencia de acuerdo a lo reportado en SEGPLAN, para el desarrollo de las actividades de: medición y evaluación del PETI, validación de los catálogos de servicios TI y medición de los indicadores

[30] Modelo Nacional de Gestión de Riesgo de Seguridad de la Información (MNGRSI) - 3.1.4 Definición de roles y responsabilidades: Responsable de Seguridad Digital: Cada entidad pública **debe designar un responsable de Seguridad Digital** que también es el responsable de **la Seguridad de la Información**, el cual debe pertenecer a un área que haga parte de la Alta Dirección o Línea Estratégica, como lo establece el Manual Operativo del MIPG en el numeral 3.2.1.4 Política de Seguridad de la información.

[31] MNGRSI - 3.1.4 Definición de roles y responsabilidades: Responsable de Seguridad Digital: •Actualizar el procedimiento para la Identificación y Valoración de Activos de la Entidad, de acuerdo a los criterios de seguridad de la información (Confidencialidad, integridad y disponibilidad). •Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad de la información (Identificación, Análisis, Evaluación y Tratamiento). •Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad de la información y en la recomendación de controles para mitigar los riesgos. •Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos. •Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad de la información.

[32] Modelo Nacional de Gestión de Riesgo de Seguridad de la Información (MNGRSI) - 3.1.5 Definición de recursos para la Gestión de riesgos de seguridad de la información: La entidad pública debe disponer los recursos suficientes para el desarrollo de la gestión de riesgos de seguridad de la información, (capital, tiempo, personal, procesos, sistemas y tecnologías), con el fin de apoyar a los responsables en la implementación de controles y seguimiento de los riesgos de seguridad de la información.

del proceso, la emisión de fichas técnicas y/justificaciones para los estudios previos relacionados con la adquisición de bienes tecnológicos, la elaboración de informes relacionados con la implementación del plan de mantenimiento y administración de la infraestructura TIC y la actualización de la documentación relacionada con el proceso; no es posible identificar de manera específica, los recursos asignados para el desarrollo de la gestión de riesgos de seguridad de la información conforme lo señala el MNGRSI, relacionados con:

- Personal capacitado e idóneo para la gestión del riesgo de seguridad de la información.
- Recursos económicos para la implementación de controles para la mitigación de riesgos (con base al análisis de riesgo realizado, teniendo en cuenta el alcance de la política de riesgos de la entidad en cuanto a seguridad de la información), que permita ser incluido dentro de la gestión presupuestal y eficiencia del gasto público de la entidad.
- Recursos para los aspectos de mejora continua, monitoreo y auditorías

Sobre este aspecto el proceso en entrevista realizada el 16/05/2024 señala que se tiene un proyecto que tiene recursos asignados de manera general y su ejecución frente a la gestión de riesgos está enmarcado en la renovación de licencias para el periodo del alcance de la auditoria.

- *Identificación de activos de información*[33]: Conforme lo señalado en el MNGRSI se validan en los Inventarios de Activos de información publicados en la página web de la entidad, el desarrollo de los pasos para la identificación y valoración de activos, en los formatos *GT-FT-10* en los cuales se realiza el registro de los activos identificados en la entidad, observándose que el formato integra los primeros 5 pasos correspondientes a: Paso 1. Listar los activos por cada proceso; Paso 2. Identificar el dueño de los activos; Paso 3. Clasificar los activos; Paso 4. Clasificar la Información; y Paso 5. Determinar la criticidad del activo. No se evidencia la implementación del paso 6. Identificar si existen infraestructuras Criticas Cibernéticas.

  Teniendo en cuenta que los inventarios más recientes publicados en la página web son:

  - Inventario de Activos de Información Gestión Documental
  - GT-FT-10 Activos de Información Hardware 2021
  - GT-FT-10 Activos de Información Obras de Arte 2021

[33] Modelo Nacional de Gestión de Riesgo de Seguridad de la Información (MNGRSI) - 3.1.6 Identificación de activos de información: Un activo de información es cualquier elemento que participe en el tratamiento de información que tenga valor para la organización, sin embargo, en el contexto de seguridad de la información son activos elementos tales como: hardware, software, aplicaciones de la entidad pública, servicios Web, redes, información digital, personal, ubicación, organización, Tecnologías de la Información -TI- o Tecnologías de la Operación -TO-) que utiliza la organización para su funcionamiento.
Es necesario que la entidad pública identifique los activos de información y documente un inventario de activos, así podrá saber lo que se debe proteger para garantizar tanto su funcionamiento interno (BackOffice) como su funcionamiento de cara al ciudadano (Front Office), aumentando así su confianza en el uso del entorno digital para interactuar con el Estado.
La identificación y valoración de activos debe ser realizada por la **Primera Línea de Defensa – Líderes de Proceso**, en cada proceso donde aplique la gestión del riesgo de seguridad de la información, siendo debidamente orientados por el responsable de seguridad digital o de seguridad de la información de la entidad pública.

- GT-FT-10 Activos de Información Bases de Datos 2021
- GT-FT-10 Activos de Información Software 2021
- GT-FT-10 Activos de Información Biblioteca 2021

Se seleccionó aleatoriamente el inventario **Activos de Información Software,** para verificar la implementación de los criterios establecidos en el MNGRSI y el documento interno que se articula con la *Guía metodológica de gestión de activos de información GT-GU-01,* con el siguiente resultado:

GT-FT-10 Activos de Información Software: El documento publicado tiene fecha de elaboración y revisión del 1 agosto del 2021.

Paso 1 Listar los activos por cada proceso: De acuerdo al MNGRSI cada proceso debe listar los activos, indicando algún consecutivo, nombre y descripción breve de cada uno. Se observa que todos los activos registrados corresponden a licencias, de las cuales las siguientes no se encuentran en el inventario al corte de diciembre de 2023 conforme se evidenció en el informe de Derechos de autor Software presentados a ese corte:

- Licencia G Suite Basic un año para 150 usuarios (Correo electrónico)
- Licencias Office Estándar 2016 Olp NL Gov para windows
- Licencias Office Home and business 9999-778-307-271
- Licencia Office Home and business 2019 todos los idiomas en línea para 69 usuarios
- Licencias project 2016 Olp NL Gov Prjct 2016 /076-0
- Licencias windows 10
- Licencias Winsvrstdcore 2016 Olp Gov Corelic 9em-00
- Licencias workspace business standard anual para 5 usuarios
- Licencias workspace business starter anual para 145 usuarios
- Licencias cal para escritorio remoto de usuario para 100 usuarios
- Windows 10 single-instalada portátil de placa 3414

El inventario no incluye licencias de LINUX, MAC, PROMOX, MACO OS, WIN 10 PRO, SOPHOS, MICROSOFT POWER BI PRO entre otras (Ver informe Derechos de Autor Software numeral 2).

Se evidencia que el inventario publicado, en el campo *Nombre del Activo de Información*, relaciona 104 activos con el nombre LICENCIA, que corresponde también a lo registrado en el campo *Descripción del Activo de Información* no permite identificar el activo al que se hace referencia.

No se evidencia que la información registrada se encuentre identificada con un número consecutivo que permita identificar el activo dentro del inventario.

Se observa que todos los activos están vinculados al proceso Gestión TIC y no se evidencian registros relacionados con los aplicativos propios o tercerizados que se encuentran instalados en la entidad. Ejemplo: Humano, Contar, Vsummer, Pandora, Orfeo. De acuerdo a lo observado en auditorías a los

procesos vinculados a estos aplicativos, se evidenciaron situaciones que pueden generar eventos de riesgos para la entidad, tales como:

Aplicativo HUMANO: Auditoria al proceso de Gestión de Talento Humano (20221100102483): Se evidenció un funcionario con dos usuarios activos en el aplicativo, todos los roles tenían acceso a todos los menús del sistema, se definieron roles de Administrador, para varios usuarios del sistema, algunos de los cuales se encontraban en estado Inactivos como usuarios, sobre lo cual la OCI se pronunció en los siguientes términos:

> *"Conforme lo anteriormente señalado y teniendo en cuenta que en desarrollo de esta auditoria sólo se validaron algunos aspectos relacionados con los usuarios y los roles asignados, tales como Gestión Acceso de Usuarios – registro y cancelación registro de usuarios (ISO 27001:2013 – A..9.2.1) Suministro de Acceso de Usuarios (ISO 27001:2013 – A.9.2.2), Gestión de derechos de acceso privilegiado (ISO 27001:2013 – A.9.2.3); es importante que se verifique en el sistema de información implementado (Humano), el cumplimiento de los criterios establecidos en la ISO 27001: 2013 vinculados a la seguridad de la información, tanto en su componente administrativo como técnico*"

Aplicativo PANDORA: Auditoría Proceso Transformación Cultural para la Revitalización del Centro (20231100103963): De lo observado en el ejercicio de auditoria se generó la siguiente recomendación:

> *"Ajustar de considerarse pertinente, la parametrización del aplicativo PANDORA, de tal manera que se asegure que la información no se modifique durante y después de los cierres periódicos establecidos. Es decir, que el reporte de información con un corte específico coincida y que los ajustes que se realicen posterior a esa fecha no se vean reflejados hacia atrás, sino que se articulen con el periodo en el cual se está realizando efectivamente el ajuste o reprogramación".*

Auditoria Proceso Gestión Financiera (20231100133283): Si bien no se evidenciaron debilidades frente al aplicativo Vsummer, se identificó el incumplimiento de lo dispuesto en los controles de acceso de usuarios y acceso a sistemas y aplicaciones de la entidad por cuanto se observó que solamente hasta el 24/03/2023 se gestionó la deshabilitación del usuario de un exfuncionario de la entidad retirado en el 2021 en el sistema SAP BogData. (ISO 27001-2022, Anexo A Gestión de Acceso de Usuarios (A.9.2) y Control de Acceso a Sistemas y Aplicaciones (A.9.4)

Paso 2: Identificar el dueño de los activos: De acuerdo a lo observado en el inventario, en el campo de Cargo o Rol del Dueño del activo se registra en cada activo que el dueño es la Fundación Gilberto Álzate Avendaño; sin embargo, lo que señala el MNGRSI es que el dueño del activo es el líder del proceso o el jefe de una de las áreas pertenecientes al proceso.

Adicionalmente en el inventario se observa que el cargo o rol del custodio para todos los registros es: "Responsable Designado Mediante Inventario Expedido por Recursos Físicos" y el área del Custodio es "Sistemas"

Paso 3. Clasificar los activos: Para el caso del inventario evaluado, este se identifica como Inventario de Información Software; sin embargo, como se mencionó anteriormente solo se registran los activos relacionados con las licencias de la entidad.

En este paso se observa que se incluye en el formato el medio de conservación, evidenciándose para todos los casos la clasificación en análogo, lo cual es coherente con la tipología referenciada.

Paso 4. Clasificar la Información[34]: En el inventario evaluado se observa que se registra lo pertinente a:

- Ley 1712 de 2014 respecto a la Información Reservada, indicando para cada uno de los activos que no aplica.
- Ley 1581 de 2012 respecto a Contenido de Datos Personales, registrando que no contienen datos personales y que corresponde a un tipo de dato público; se observa en el comentario de ayuda la siguiente tipología de referencia: Tipo de Dato: Información pública clasificada (Dato privado o semiprivado), Información pública reservada, Documento privado, Dato sensible, Información interna, Documento en construcción, Dato abierto, Dato público, N/A. Adicionalmente se incluye otro campo de "Otras normas que apliquen" diligenciadas en N/A para todos los activos.

Conforme lo anterior, se observa que de manera general se incluyen los criterios establecidos en el MNGRSI.

Paso 5. Determinar la criticidad del activo (Valoración del Activo)[35]: En el documento *Guía metodológica de gestión de activos de información GT-GU-01*, se observa en los ítems 3.2.3 al 3.2.6 el establecimiento de los requerimientos específicos para determinar la criticidad de los activos; sin embargo, no se evidencia el criterio con el cual se determina si "*se gestionara los riesgos en todos los activos del inventario o solo en aquellos que tengan un nivel de criticidad alto*" (Nota del ítem 3.2.8). El documento fue aprobado por la Subdirección de Gestión Corporativa que hace parte de la línea estratégica de la entidad.

El inventario evaluado registra para cada uno de los activos una valoración de criticidad tanto en Confidencialidad, Integridad y Disponibilidad de "Media"; sin embargo, respecto a la confidencialidad esta

[34] Modelo Nacional de Gestión de Riesgo de Seguridad de la Información (MNGRSI) 3.1.6 Identificación de activos de información: Paso 4: **Nota:** Al realizar la identificación del contexto externo, la entidad pública debería tener plenamente identificados los aspectos regulatorios y normativos con los que deberá cumplir, las leyes enunciadas (1712 de 2014 y 1581 de 2012) pueden ser de cumplimiento para la mayoría de las entidades públicas sin embargo es tarea de la entidad pública determinar si hay más o menos aspectos regulatorios para tener en cuenta respecto a la información. El **área jurídica** de la entidad debe colaborar en esta tarea específica.

[35] Modelo Nacional de Gestión de Riesgo de Seguridad de la Información (MNGRSI) 3.1.6 Identificación de activos de información: Paso 5: En este paso la entidad pública debe definir las escalas (que significa criticidad ALTA, MEDIA y BAJA) para valorar los activos respecto a la confidencialidad, integridad y disponibilidad e identificar su nivel de importancia o criticidad para el proceso. Para definir estas escalas puede tomar como referencia la Guía de Gestión de Activos del Modelo de Seguridad y Privacidad de la Información (MSPI) , estas escalas deberán ser definidas y documentadas en un procedimiento de gestión de activos que debe ser aprobado por parte de la línea estratégica de la entidad pública.

evaluación no es coherente con la tipificación del tipo de dato con el que se evaluó el activo por cuanto todos los activos se clasifican con tipo de dato *Publico*, lo cual lo ubica en una tipificación para el valor de Confidencialidad de criticidad "Baja" de acuerdo a la escala establecida en la *Guía metodológica de gestión de activos de información* GT-GU-01.

De igual manera se observa que la integridad si bien se evalúa con una criticidad "Media", en el esquema se identifica esta clasificación como *Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal a nivel medio, de pérdida económica o de imagen en la FUGA, o afectar la operación del proceso* (subrayado fuera de texto); sin embargo, considerando que en la mayoría de los casos se trata de licencias distribuidas en toda la entidad, la perdida de exactitud y completitud puede afectar no solo un proceso sino la operación de varios de los procesos de la Fundación, por lo que la criticidad de la integridad estaría ubicada en un valor de "Alta". Situación similar se observa en la evaluación de la Disponibilidad.

Ahora bien, teniendo en cuenta que el nivel de criticidad general en el inventario se evalúa en "Media" y considerando que las tres propiedades evaluadas se encuentran también clasificadas en ese nivel (Confidencialidad, integridad y disponibilidad), se evidencia que la valoración es coherente con lo dispuesto en el ítem 3.2.8 de la *Guía metodológica de gestión de activos de información* GT-GU-01; sin embargo, de acuerdo a las observaciones indicadas en el párrafo anterior la valoración se presentaría en el nivel "Alta" de criticidad general.

Paso 6. Identificar si existen Infraestructuras Críticas Cibernéticas -ICC: Si bien en la *Guía metodológica de gestión de activos de información* GT-GU-01 se observa en el ítem 3.2.9 *Identificar Infraestructura Crítica Cibernética (ICC) (Paso 6*)[36], la referencia para determinar si se tiene ICC, no se identifica el resultado del ejercicio referenciado. No es posible determinar si se llevó a cabo o no la identificación de Infraestructuras Críticas Cibernéticas – ICC en la entidad. En la entrevista realizada el 16/05/2024 al proceso se señala que se hizo una valoración de criticidad, pero no se tiene documentas las ICC.

Sin embargo, se aporta como evidencia el formato de la Alta Consejería TIC de *Identificación de Activos de Información*, en el cual se observa un ejercicio realizado para determinar el ICC, con la aclaración dada por el proceso, de que los registrados fueron agrupados para incluir la mayor parte de ellos, como se muestra a continuación:

PROCESO / GRUPO	PROCEDIMIENTO	NOMBRE DEL ACTIVO DE INFORMACIÓN	DESCRIPCIÓN DEL ACTIVO DE INFORMACIÓN
Gestión TIC	N/A	Switches de comunicación interna sedes	Switches de comunicación interna sedes
Gestión TIC	N/A	Sistemas de información	Software gestión planeación Software gestión documental

[36] Guía metodológica de gestión de activos de información GT-GU-01 Ítem 3.2.9 Identificar Infraestructura Crítica Cibernética (ICC) (Paso 6): De acuerdo a la tabla 9 si la FUGA determina que tiene ICC si el activo es afectado por 1 o más de los siguientes criterios, de ser afirmativa la respuesta el activo será considerado infraestructura crítica cibernética.

			Software de biblioteca Gestión de casos Gestión contable financiero recursos físicos Comunicaciones
Gestión TIC	N/A	Sistemas de información	Sistemas operativos windows 2008 r2 grand stream, Linux hp oneview/virtualizador proxmox firewall Sophos.
Gestión TIC	N/A	Hojas electrónicas formularios datos ciudadanos	Bases de datos ciudadanos administradas por los diferentes procesos de la entidad y registradas en la SIC
Gestión Comunicaciones	N/A	Publicación WEB	Documentos generados por la entidad sujetos de publicación para datos abiertos y link de transparencia

Fuente: Matriz de Identificación Activos Críticos

Conforme lo observado, en la matriz aportada solo los dos últimos relacionados tienen evaluación de ICC respecto al Impacto Social (Daño, pérdida o deterioro). Sobre los demás activos se registra en el formato que no tienen impacto social, económico o ambiental pero no se registra si se consideran con infraestructura crítica.

Adicionalmente, si bien se hace referencia a activos críticos, se evidencia que, de los activos relacionados, el primero se encuentra en un nivel de criticidad bajo y los restantes en medio, por lo que no se identifica el criterio de valoración del activo que los incluyen dentro de este ejercicio de identificación. Lo anterior aunado a que no se evidencia que se haya establecido el criterio para determinar en la entidad, los activos a gestionar como riesgo como ya se mencionó anteriormente.

Por último, si bien la verificación detallada se realiza sobre la muestra seleccionada del Inventario de Software, de una revisión general a los demás inventarios se evidencia:

GT-FT-10 Activos de información Hardware 2021:

- El inventario se encuentra desactualizado. Se registran 254 activos, lo cual no es coherente con la información al corte de diciembre de 2023 aportada como evidencia para el seguimiento de Derechos de Autor Software, donde se registra un total de 121 activos; desactualización que incide en el número de activos bajo la responsabilidad de los procesos. Ejemplo: El proceso de Evaluación Independiente de la Gestión tiene registrados 4 portátiles, cuando solo son 3 los asignados.
- En todos los registros, se indica en el campo cargo o rol del dueño del activo y custodio del activo, la Fundación Gilberto Álzate Avendaño.
- Se evidencian 43 activos con un nivel de criticidad alta, observándose que los criterios de confidencialidad, completitud y disponibilidad se catalogan en este mismo nivel (alta), donde se incluyen licencias, aires acondicionados, gabinetes de pared entre otros.

GT-FT-10 Activos de Información Bases de Datos 2021:

- El inventario se encuentra desactualizado, la base de datos más reciente registrada es de la vigencia 2022.
- En el inventario se evidencia el registro de bases de datos en los procesos de Gestión Jurídica, Gestión TIC, Planeación, Servicio al Ciudadano y Transformación Cultural para la revitalización del Centro; sin embargo, se observan entre otras, las siguientes situaciones: TIC no incluye las bases de datos de los reportes de GPLI aportados en desarrollo de la presente auditoria, ni la base de datos de Hojas de Vida Equipos aportado en el seguimiento a Derechos de Autor – Software. En planeación no se observa la base de datos de MIPG ni de Riesgos. En Comunicaciones se tiene una base de datos relacionada con el Seguimiento Estrategia de Comunicaciones, aportada en el desarrollo del Seguimiento a metas, no incluida en el inventario.
- Se observa que todos los activos se clasifican como información reservada sin embargo se evidencia que la base de datos Plan Anual de Adquisiciones 2021, Normograma 2022, Ganadores convocatorias, Participantes Convocatorias entre otros; es información que se encuentra disponible en la página web de la entidad. También se indica que todas las bases tienen tipo de *Dato Sensible*[37]; sin embargo, en las anteriormente señaladas no se identifica la característica en la información registrada que lo califica en esa tipología.
- Todos los activos relacionados en este inventario se clasifican con un nivel de criticidad Alta, catalogando los tres criterios a evaluar en ese nivel (Confidencialidad, Integridad y Disponibilidad).

GT-FT-10 Activos de Información Obras de Arte 2021:

- El inventario corresponde a un total de 354 activos identificados bajo la tipología de Otros, con una clasificación en tipo de datos como *Datos Públicos*[38] y un nivel de criticidad Baja, catalogando los tres criterios a evaluar en ese nivel (Confidencialidad, Integridad y Disponibilidad).
- La última actualización del inventario corresponde al 01/08/2021.
- En todos los registros, se indica en el campo cargo o rol del dueño del activo la Fundación Gilberto Álzate Avendaño.

GT-FT-10 Activos de Información Biblioteca 2021:

- El inventario publicado no se encuentra en el formato GT-FT-10.
- En todos los registros, se indica en el campo cargo o rol del dueño del activo y custodio del activo, la Fundación Gilberto Álzate Avendaño.

[37] Ley 1581 de 2012 Artículo 5°. Datos sensibles. Para los propósitos de la presente ley, se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

[38] Guía metodológica de gestión de activos de información Código: GT-GU-01 Dato público: Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas

- Se evidencia el registro de 9.902 activos clasificados como tipo de dato Publico y un nivel de criticidad Baja, catalogando los tres criterios a evaluar en ese nivel (Confidencialidad, Integridad y Disponibilidad).

Inventario de Activos de Información Gestión Documental:

- El inventario publicado no se encuentra en el formato GT-FT-10, observándose que en el paso 1 se identifica la dependencia y no el proceso, como se establece en el formato y como se registra en los demás inventarios revisados.
- Se evidencia el registro de 146 activos de los cuales solo uno (Actas del Comité de Dirección) se identifica en el nivel de criticidad Alta, catalogando los tres criterios a evaluar en ese nivel (Confidencialidad, Integridad y Disponibilidad).
- Se evidencian activos sobre los cuales se evalúa por lo menos dos propiedades en **Alta** por lo que se debía clasificar con un nivel de criticidad **Alta**[39]; sin embargo, se registra este nivel en media. (Actas Comités de Dirección, Comité mediador de convivencia, de Resolución de Conflictos, Prioritario de salud ocupacional, consecutivo de comunicaciones oficiales, historias laborales, nómina y novedades de nómina, entre otros).
- Se observan activos identificados con información reservada clasificada, con tipo de datos sensibles, pero con una evaluación de criticidad respecto a su confidencialidad e integridad en bajo, lo que la ubica en un nivel general de criticidad Media. Ejemplos: Acciones constitucionales de Acción de cumplimiento, de tutela y populares, así como el activo Comprobantes de pago de nómina con información reservada con un nivel de criticidad Baja, entre otros.
- Se observan campos en la Descripción del Activo de Información el registro de “Falta” (Datos del aplicativo del manejo de inventarios y devolutivos, Declaraciones tributarias, listado de apropiaciones presupuestales, plan de mantenimiento, Plan de verificación a la aplicación de la TRD.
- Se evidencia que se registra en algunos los campos Dueño del Activo, el cargo o Rol del Dueño del activo al Director General, sin embargo se registra en el área del dueño del activo una diferente, igual situación se presenta en el campo de Custodio del activo. Ejemplo:

[39] Guía para la Gestión y clasificación de activos de información de Mintic: 6.1. Definición Criticidad: Es un cálculo automático que determina el valor general del activo, de acuerdo con la clasificación de la Información: * Alta. Activos de información en los cuales la clasificación de la información en dos o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta. * Media. Activos de información en los cuales la clasificación de la información es alta en una de sus propiedades (confidencialidad, integridad, y disponibilidad) o al menos una de ellas es de nivel medio. * Baja. Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

DEPENDENCIA Paso 1	Nombre del Activo de Información Paso 1	Dueño del activo Paso 2		Custodio del activo Paso 2	
		Cargo o Rol del Dueño del activo	Área del Dueño del Activo	Cargo o Rol del Custodio	Area del Custodio
Oficina Jurídica	ACCIONES CONSTITUCIONALES / Acción De Cumplimiento	Director General	130 - Oficina Jurídica	Jefe Oficina Jurídica	Archivo Central
Oficina Jurídica	ACCIONES CONSTITUCIONALES / Acciones De Tutela	Director General	130 - Oficina Jurídica	Jefe Oficina Jurídica	Archivo Central
Oficina Jurídica	ACCIONES CONSTITUCIONALES / Acciones Populares	Director General	130 - Oficina Jurídica	Jefe Oficina Jurídica	Archivo Central
Direccion General	ACTAS / Acta De Informe De Gestión	Director General	100 - Dirección General	Director (a) General	Archivo Central
Direccion General	ACTAS / Actas Comité De Coordinación Del Plan Institucional De La Gestión Ambiental PIGA	Director General	120 - Oficina Asesora de Planeación	Jefe Oficina de Asesora de Planeación	Archivo Central
Direccion General	ACTAS / Actas Comité De Coordinación Del Sistema Integrado De Gestión	Director General	120 - Oficina Asesora de Planeación	Jefe Oficina de Asesora de Planeación	Archivo Central
Direccion General	ACTAS / Actas Comité De Dirección	Director General	100 - Dirección General	Director (a) General	Archivo Central

Fuente: Inventario de Activos de Información Gestión Documental:

En términos generales se observa:

- No se observa donde se ha documentado y aprobado la definición de si se gestionará los riesgos en todos los activos del inventario o solo en aquellos que tengan un nivel de criticidad Alto[40].
- Los inventarios de activos publicados se encuentran desactualizados.
- El diligenciamiento de los campos no se articula con las alertas de ayudas dispuestas en el formato por lo que se evidenciaron registros en algunos campos que no son coherentes con lo solicitado (Dueño de la Información, Custodio de la Información, Descripción del Activo de Información, entre otros).
- No se incluyen en los inventarios los aplicativos propios o tercerizados implementados en la entidad.
- No se evidencia la identificación de activos de información relacionados con servicios, componentes de red, personas, instalaciones conforme se señala en el MNGRSI (Ver Tabla 1. Tipología de Activos del MNGRSI)
- La evaluación de los niveles de criticidad no corresponde en todos los casos a los criterios con los cuales se debe clasificar (Guía metodológica de gestión de activos de información GT-GU-01).

[40] Modelo Nacional de Gestión de Riesgo de Seguridad de la Información (MNGRSI) 3.1.6 Identificación de activos de información: Importante: La entidad pública puede decidir si realiza la gestión de riesgos en todos los activos identificados en este punto o si desea hacerlo a los activos más críticos. Esta decisión debe estar debidamente formalizada en el procedimiento de gestión de activos que solicita el **Modelo de Seguridad de la Información**. Adicionalmente, debe quedar explicita en la Política de Administración de Riesgos de la entidad pública, debidamente aprobada por el Comité Institucional de Coordinación de Control Interno.

Conforme lo anterior se recomienda:

- Documentar los criterios diferenciales del MSPI a través de los cuales se identifican los procesos vinculados a la gestión de riesgos.
- Documentar la evaluación de las infraestructuras criticas cibernéticas en la entidad.
- Definir y aprobar los criterios para determinar los activos de información que serán incluidos en la gestión de riesgos (Criticidad Alta, Media, Baja).
- Actualizar los inventarios publicados, en los cuales se identifique de manera correcta cada uno de los campos obligatorios, los cuales deberán cumplir con la característica propia y la definición de lo requerido.
- Revisar la clasificación de la criticidad de los activos conforme la realidad institucional.
- Indicar como complemento en la identificación de los activos, nemónicos para complementar su identificación de dentro de los inventarios conforme lo sugiere el MNGRSI.

Fase 2. Ejecución: Esta fase se evalúa sobre la implementación de los planes de tratamiento, gestión que se desarrolla en el ítem 5. 2.

Fase 2 Monitoreo y revisión:

Se evidencia la implementación de las tres líneas de defensa en la gestión de riegos de la entidad, definiendo para cada una de ellas sus responsabilidades específicas[41].

Registro y reporte de incidentes de seguridad de la información: Se evidencia a través de los reportes GLPI, el registro de las situaciones presentadas en la entidad relacionada con el proceso; sin embargo, los mismos presentan oportunidades de mejora relacionadas con la identificación de los eventos registrados, categorización de los mismos y la gestión realizada para solucionar los casos reportados.

Reporte de la gestión del riesgo de seguridad de la información al interior de la entidad pública: No se evidencia el reporte con la periodicidad indicada a la Alta Dirección y al Comité Institucional de Coordinación de Control Interno y partes interesadas, de: 1. Listado de activos críticos TI/TO y listado de ICC. 2. Reporte de criticidad/impacto de la organización. 3. Reporte de evolución de riesgos y modificación del riesgo. 4. Cantidad de riesgos por fuera de la tolerancia del riesgo identificado de acuerdo con la periodicidad de evaluación realizada. 5. Impacto económico que podría presentarse frente a la materialización del riesgo.

Reporte de la gestión del riesgo de seguridad de la información a autoridades o entidades especiales: De la información consultada y la aportada por el proceso en desarrollo de la auditoria, no se identifica la gestión realizada en cumplimiento de esta actividad relacionada en el ítem 3.3.3 del MNGRSI (Información por consolidar para generar el reporte de información y reportes relacionados con Infraestructuras Criticas Cibernéticas si aplican).

[41] Guía metodológica de gestión de activos de información. GT-GU-01

Auditorías Internas y Externas: Si bien en la vigencia auditada no se realizó el ejercicio de evaluación sobre la gestión de riesgos de seguridad de la información, la catalogación como unidad auditable estaba definida para la vigencia 2024, lo cual es coherente con el desarrollo del presente ejercicio.

Medición del Desempeño: Como ya se ha venido mencionando, si bien la entidad utiliza medidas de desempeño (indicadores) vinculados directamente con la implementación del MSPI, no se evidencian indicadores de medición de gestión y cumplimiento específicos, tal como se señala en la Guía de indicadores de gestión para la seguridad de la información de MinTIC.

Conforme lo anterior se recomienda de manera general revisar los criterios definidos para esta fase del MNGRSI e implementar las acciones que permitan garantizar su aplicación integral.

6.2. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información:

El plan se encuentra en el aparte XI. Planes administrados por el proceso Gestión Tecnológica, numeral 11.2 del Plan Estratégico tecnologías de la Información GT-FTPL-01

En el documento se definen las medidas de seguridad identificadas para desarrollar el plan de tratamiento en la entidad, así:

• Fase 1: Análisis de la información

Actividad	Evidencia	Observación OCI
Aplicar las políticas de tratamiento de riesgos.	Mapa de Riesgos Institucional	Sin observaciones
Determinar los controles (se desprenden de las medidas) aplicados en la FUGA en su matriz de riesgos.	Mapa de Riesgos Institucional	Sin observaciones
Determinar los riesgos que van a ser incluidos en el Plan de Tratamiento de Riesgos.	Mapa de Riesgos Institucional	Se evidencian riesgos de seguridad de la información identificados no solo en el proceso de Gestión TIC, sino o vinculados a los procesos de Servicio al Ciudadano, Gestión Financiera, Talento Humano y Transformación Cultural para la Revitalización del Centro.

• Fase 2: Desarrollo de los proyectos

En esta fase se realizarán las actividades que permitan la estructuración de las medidas[42].

Actividad	Evidencia	Observación OCI

[42] Durante la entrevista realizada el 16/05/2024 el proceso aclara que con medida se hace referencia a controles o actividades.

Determinar el nombre de la medida.	Mapa de Riesgos Institucional	Sobre esta gestión el equipo auditado señala en la entrevista del 16/05/2024 que no se documenta, pero se articula con los controles del MSPI, se identifica el control a aplicar y su relevancia y se va desarrollando de acuerdo a los criterios que se vinculan a estos. Se hace cuando se materializa. Como se trabaja con generalidades se va gestionando agrupando por controles.
Definir los responsables de cada medida	Mapa de Riesgos Institucional	
Establecer el objetivo de cada medida	Mapa de Riesgos Institucional	
Elaborar la justificación de la medida.	Mapa de Riesgos Institucional	
Definir las actividades a realizar para el desarrollo de la medida.	Mapa de Riesgos Institucional	

De la verificación realizada a los formatos de *Fichas de Riesgos* (GM-FT-09) diligenciados para los riesgos de seguridad de la información identificados, y teniendo en cuenta la aclaración realizada por el proceso, se observa que en la descripción de los controles se señala el responsable, el objetivo, la justificación y las actividades a desarrollar. Sin embargo, teniendo en cuenta que la fase corresponde es al desarrollo de proyectos, no se identifican cuáles son los proyectos sobre los cuales se estructuran las medidas y como se articulan estos a la gestión de riesgo institucional.

• Fase 3: Ciclo de vida del tratamiento de riesgos

Actividad	Evidencia	Observación OCI
Definir las actividades a realizar por cada uno de los elementos del ciclo de vida del Plan de Tratamiento de Riesgos.	Mapa de Riesgos Institucional	En la entrevista realizada el 16/05/2024 el proceso señala que se hace en el ejercicio de actualización de los riesgos en cada vigencia.

De lo evidenciado en las *Fichas de Riesgos* (GM-FT-09, no se identifican las actividades vinculadas a ciclo de vida del plan.

El Plan también señala actividades a realizar por la FUGA orientadas a controlar las siguientes posibles acciones:

- Proteger del Acceso no autorizado a la información.
- Blindar a la entidad de Ataques Externos o internos.
- Proteger los activos de información contra el Daño de la información.
- Proteger a la entidad de un ataque de Denegación del servicio.

La evidencia de la ejecución de las actividades antes referencias se evaluó en el aparte 1.2. Acción 7 del presente ejercicio.

Conforme lo expuesto, si bien el proceso realiza las precisiones respecto a la ejecución de las fases 2 y 3 del plan, no se identifica la articulación de las fases con las actividades especificas establecidas para cada una de ellas y no se evidencian soportes que den cuenta de su ejecución.

6.3. Mapa de Riesgos Institucional – Riesgos de Seguridad de la Información:

Verificado el Mapa de Riesgos Institucional vigente, se observa que el proceso de Gestión TIC, identificó los siguientes riesgos dentro del proceso:

RIESGO	CAUSA RAIZ ¿Porqué?	ZONA DE RIESGO INHERENTE	CONTROLES	ZONA DE RIESGO RESIDUAL
Riesgo de Gestión: 1. *Posibilidad de pérdida reputacional por la interrupción en la prestación del servicio tecnológicos ocasionada por la baja disponibilidad de recursos del proceso	Ocasionada por la baja disponibilidad de recursos del proceso	**Alto**	El profesional apoyo líder TIC trimestralmente verifica por medio de la plataforma Prometheus la disponibilidad de los servicios tecnológicos que ofrece el proceso, con el fin de mitigar y atender posibles interrupciones o fallas que puedan generar impacto en la medición y el uso de los sistemas de información. En caso de encontrar inconsistencias a nivel de servicio se debe justificar técnicamente en el informe, los motivos de la caída del servicio y ajustar en caso de ser necesario los criterios técnicos para establecer el servicio de acuerdo al equipo de trabajo disponible. Como soporte del control se genera un informe tomando captura de los servicios controlados.	**Moderado**
Riesgo de Seguridad Digital: 2. Pérdida de la confidencialidad Activo: Información Digital	Ausencia de identificación y autenticación de usuarios	**Moderado**	Control 1: El profesional de apoyo líder de gestión de tecnologías revisa que el profesional de apoyo de tecnologías realice la desactivación de las cuentas del personal cuando se retira y entregan la paz y salvo, con el fin de salvaguardar la información y como o establece el procedimiento GT-PD-04. En caso de no estar desactivadas las cuentas, el profesional de apoyo líder tecnologías procede a desactivarlas, como soporte se dejan los registros de paz y salvo firmados. Control 2: El Profesional apoyo de Gestión Tecnológica revisa que el correo de solicitud de creación de cuentas contenga el número de contrato, en caso de que sea contratista; en caso de ser funcionario, acta de posesión; en caso de no estar en la solicitud se devuelve al área que genera la solicitud por correo electrónico. Como soporte queda la solicitud y los correos electrónicos	**Moderado**
3. **Riesgo de Seguridad Digital:** Pérdida de la confidencialidad Activo: Recursos e información de la entidad	Permitir el acceso de personal externo a recursos e información no autorizados de la entidad	**Moderado**	El profesional de apoyo líder de gestión de tecnologías, trimestralmente revisa las evidencias de las actividades programadas en el Cronograma y Seguimiento de Mantenimiento Infraestructura de Tecnología de la Información, controlado por el profesional de apoyo de tecnología, en caso de encontrar inconsistencias, se solicitan los ajustes y explicación técnica por medio de correo electrónico.	**Moderado**

4. **Riesgo de Seguridad Digital:** Pérdida de la disponibilidad Activo: Equipos- hardware	Incumplimiento a los planes de mantenimiento a los equipos tecnológicos, de suministro o soporte energético.	**Moderado**	El profesional apoyo líder TIC revisa el informe entregado por el profesional de apoyo TIC estableciendo el cumplimiento de las actividades realizadas frente al cronograma de actividades de mantenimiento; en caso de no estar ejecutadas en tiempo y forma, se envía un correo solicitando la ejecución y reprogramación de la actividad.	**Moderado**
5. **Riesgo de Seguridad Digital:** Pérdida de la integridad Activo: Aplicaciones de la organización	Manipulación de información por externos	**Alto**	El profesional líder de gestión de tecnologías "mensualmente" revisa el Firewall para detectar posibles fallas o amenazas; en caso de encontrar inconsistencia, debe identificar, controlar y aplicar políticas para mitigar amenazas o debilidades en la red, que puedan afectar su adecuado funcionamiento, como soporte se deja el informe exportado del sistema. En caso de que se presente algún incidente, este debe ser reportado de acuerdo al procedimiento Gestión de incidentes, amenazas y debilidades de seguridad GT-PD-09	**Alto**

Fuente: Mapa de riesgos institucional 2023.

Dentro de la herramienta ficha de riesgos, se observa el análisis de objetivos anidando un objetivo estratégico al objetivo del proceso que además usa la metodología SMART para su formulación, se identifica además la relación ente factores de riesgo y clasificación del riesgo.

La redacción de los riesgos está basada en responder las preguntas ¿qué?, ¿cómo? Y ¿por qué? Identificando de manera clara el impacto, causa inmediata y la causa raíz.

En el Análisis y Evaluación de los riesgos se evidencia la calificación del impacto y la probabilidad siguiendo la metodología DAFP.

Se observa monitoreo de primera y segunda línea de defensa dando cumplimiento a lo establecido en la política de administración del riesgo y se hace referencia a los lineamientos brindados.

Ahora bien, teniendo en cuenta las características propias de los riesgos identificados como de seguridad digital, se verifica también en el formato *Ficha de Riesgos* GM-FT-09, lo dispuesto en la *Guía para la Administración del Riesgo y el diseño de controles en entidades Públicas* Versión 6 del DAFP, así:
Identificación del riesgo:

En la matriz se evidencia la identificación del activo a gestionar, el riesgo, la descripción del riesgo (aspecto asociado a la criticidad: confidencialidad, disponibilidad e integridad), tipo, amenaza[43], causa/vulnerabilidad[44] y consecuencia.

[43] Documento Maestro del Modelo de Seguridad y Privacidad de la Información MinTIC. Octubre 20210. Definiciones: Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
[44] Documento Maestro del Modelo de Seguridad y Privacidad de la Información MinTIC. Octubre 20210. Definiciones: Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000)

Si bien en el desarrollo de la entrevista del 16/05/2024 el proceso auditado señala que se gestiona el riesgo a grupos de activos identificados en los inventarios, articulando este ejercicio el resultado de la priorización de activos identificados en la *Matriz Identificación de Activos Críticos* de la Alta Consejería aportada como evidencia, y teniendo en cuenta las situaciones observadas en el ítem 5.1. Implementación del MNGRSI, del presente informe, se evidencia:

- No se identifica en esta fase, la articulación del riesgo con el dueño del activo identificado en el inventario.
- Si bien la guía señala que "*para cada riesgo se debe asociar el grupo de activos o activos específicos del proceso para conjuntamente analizar las posibles amenazas y vulnerabilidades que podrían causar su materialización"*, al no contar con una directriz para gestionar los riesgos (Criticidad alta o todos los activos identificados) como ya se ha venido mencionado y al estar agrupados en temas generales que no se encuentran articulados de manera integral entre el inventario y lo registrado en la *Matriz Identificación de Activos Críticos*, no es posible evaluar el activo a gestionar, lo anterior teniendo en cuenta que no todos tienen el mismo tratamiento:

Matriz Riesgos Institucional		Matriz de Identificación de Activos Críticos	
Riesgo	Activo	Tipo de Activo	Valor del Activo para el proceso
Perdida de Confidencialidad	Información Digital	No se identifican activos vinculados con la descripción del riesgo asociado.	
Perdida de Confidencialidad	Recursos e información de la entidad	No se identifican activos vinculados con la descripción del riesgo asociado.	
Pérdida de la disponibilidad	Equipos- hardware	Hardware / Infraestructura TIC • Switches de comunicación interna sedes. • Sistemas operativos Windows 2008 R2 Grand Stream, Linux, HP, oneview/virtualizador. Proxmox Firewall Sophos.	Confidencialidad: Sin clasificar. Integridad y disponibilidad: Baja Valor del Activo: Sin evaluar
Pérdida de la integridad	Aplicaciones de la organización	Software / Aplicaciones • Software gestión planeación • Software gestión documental • Software de biblioteca • Gestión de casos • Gestión contable • Financiero • Recursos físicos • Comunicaciones	Confidencialidad, Integridad y Disponibilidad en Media Valor del Activo: Sin evaluar
No se evidencia riesgos identificados en la matriz vinculados a esta tipología de activos		Datos / Información • Bases de datos ciudadanos administradas por los diferentes procesos de la entidad y registradas en la SIC.	Confidencialidad, Integridad y Disponibilidad en Media Valor del Activo: Sin evaluar

	• Documentos generados por la entidad sujetos de publicación para datos abiertos y link de transparencia	

- No se evidencia para todos los riesgos identificados, la articulación entre la amenaza, la vulnerabilidad (causa) y la consecuencia.
- No se identifica la metodología empleada en el análisis de causas, por lo cual no es posible evaluar que la causa identificada corresponda a la causa raíz.
- No se articulan los activos registrados en los inventarios de Bases de Datos y Activos de Información de Gestión Documental evaluados con nivel de criticidad Alto con la administración de riesgos institucional.

Valoración del Riesgo:

Se observa la implementación de la metodología establecida de manera general para todos los riesgos (Frecuencia), afectación económica, entre otras.

No obstante, como se señaló en el ítem 5.1. Implementación del MNGRSI, no se identifica como se llega a la medición registrada respecto a la afectación económica y al número de veces que se realiza la actividad al año. Tampoco se evidencia el análisis frente a la variable de presupuesto y ambiental que hacen parte también de la gestión de valoración de los riesgos[45].

Controles asociados a la seguridad de la información:
Si bien se evidencia en los campos Evaluación del riesgo - Valoración de los controles, la descripción del control o controles para cada riesgo, su evaluación (riesgo residual) y plan de acción, no se identifica para todos los casos, como se articulan estos con la fase de identificación; tampoco se identifican planes de contingencias asociados, considerando que estos están relacionados con los planes de continuidad del negocio y no a los planes de acción identificados.

La especificidad de cada uno de las anteriores observaciones, se presenta en la evaluación realizada a cada uno de los riesgos, así:

Riesgo 1: Riesgo de Gestión:

- Se evidencia identificación del riesgo con una causa y un control de tipo preventivo, siguiendo los lineamientos de la Guía DAFP; sin embargo, la causa no identifica el tipo de recursos al que se hace

[45] Guía para la Administración del Riesgo y el diseño de controles en entidades Públicas Versión 6 del DAFP: 6.3. Valoración del riesgo: Importante: La variable de presupuesto es la consideración de presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal. La variable ambiental estará también alienada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital. Esta variable puede no ser utilizar en la mayoría de los casos, pero debe tenerse en cuenta, ya que en alguna eventualidad puede existe afectación ambiental.

referencia (Humano, económico, tecnológico, entre otros), lo cual puede afectar la categorización del riesgo. Lo anterior en razón a que puede ser una vulnerabilidad cuya amenaza se materializaría con la interrupción de los servicios tecnológicos, por lo que puede ser considerado como un riesgo de Seguridad de la Información.

- No se identifica la articulación entre el riesgo, el tipo y la clasificación del riesgo, teniendo en cuenta que la descripción del riesgo identifica situaciones relacionadas directamente con seguridad digital.

Riesgo	Tipo	Clasificación
Posibilidad de pérdida reputacional por la interrupción en la prestación del servicio tecnológicos ocasionada por la baja disponibilidad de recursos del proceso.	Riesgo de Gestión	Usuarios, productos y prácticas

- No se identifica la metodología empleada en el análisis de causas, por lo cual no es posible evaluar que la causa identificada corresponda a la causa raíz.
- Se evidencia el registro de 600 número de veces que se realiza en promedio la actividad del año, precisando que se hace la medición sobre 50 solicitudes en promedio por 12 meses del año; no obstante, no se referencia la fuente de la información registrada que permita validar el cálculo[46].
- Frente a la valoración del criterio de impacto (Afectación económica) se reporta en 80 "*Entre 50 y 100 SMLMV: El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos*; sin embargo, no se identifica las variables con las cuales se hace el cálculo.
- Se observa que, de acuerdo a la evaluación realizada por el proceso, éste se ubica en una zona de riesgo inherente alta y residual moderado con un plan de acción de Reducir y la definición de una actividad; no obstante, al identificarse debilidades frente a la valoración de los criterios de análisis descritas anteriormente, no es posible evaluar la zona de riesgo inherente real conforme la realidad institucional.
- Respecto a la descripción del control se observa que este se aplica trimestralmente; sin embargo, de acuerdo a la posible ocurrencia del riesgo, la frecuencia del control no sería oportuna en relación con impacto de que se presenten interrupciones en la prestación de los servicios tecnológicos de la entidad.
- En la herramienta en el campo de gestión eventos se registra que no se materialización el riesgo; sin embargo, de lo observado en el ítem 2.1 Controles A.16 y A.17 se evidencia el reporte de interrupciones en la página web de la entidad y en la página de Festival Centro, registradas en enero, febrero y agosto.

Riesgo 2 de Seguridad Digital:

- Se identifican dos amenazas (Acceso no autorizado y Cambios no controlados) y una causa o vulnerabilidad (Ausencia de identificación y autenticación de usuarios); sin embargo, estas no se articulan de manera integral. No se identifica como los cambios no controlados explotan la vulnerabilidad identificada.

[46] Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6: Probabilidad: se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año. (Subrayado fuera de texto)

- Se identifica una consecuencia; sin embargo, teniendo en cuenta la descripción del riesgo y de acuerdo al MNGRSI no se evidencia como se articula ésta con la vulnerabilidad y la amenaza identificados.
- En este riesgo la generalidad del activo de información vinculado (Información digital) no permite hacer la individualización de la causa ya que no todos sistemas de información o la información digital en la entidad tienen un proceso de autenticación de usuarios igual, así como tampoco se observa que se incluya en el inventario la gestión de autenticación de aplicaciones que si bien no son propias de la entidad si impactan sobre la información digital de la misma (SAP y SDQS); situación que también genera debilidades en el control identificado por cuanto solo se hace referencia a la habilitación y des habilitaciones de las cuentas institucionales pero no al control mismo de autenticación e identificación, debilidades ya expuestas en el ítem 2.1 Control A.9.
- No se identifica la metodología empleada en el análisis de causas, por lo cual no es posible evaluar que la causa identificada corresponda a la causa raíz.
- Respecto a la evaluación de la probabilidad, se observa que se identifica un total de 260 número de veces que se realiza la actividad al año, calculado sobre el total de número de colaboradores de la entidad multiplicado por 2 (Ingreso y egreso); considerando que este cálculo se realiza en la identificación de los riesgos para el 2023, tomando como referencia la gestión 2022, el valor es aproximado es equivalente a la gestión de ingreso y retiros de los contratistas (224); sin embargo, es importante considerar que los funcionarios de planta no tienen este mismo comportamiento por cuanto no todos ellos tienen esta rotación en el año.
- Frente a la valoración del criterio de impacto (Afectación económica) se reporta en 80 "*Entre 50 y 100 SMLMV: El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos"*; sin embargo, no se identifica las variables con las cuales se hace el cálculo.
- Se observa que en la fase de análisis de riesgo éste se ubica en la zona moderada del riesgo inherente y un nivel de riesgo residual también en moderado, con un plan de tratamiento de Reducir. Se vinculan a este plan dos acciones con plazo de ejecución al 31/01/2023; si bien se reporta su ejecución, esta se llevó a cabo en septiembre del 2022, tal como se evidencia en el control de cambios del procedimiento que se referencia en el plan de acción.
- No se observa la implementación de un plan de contingencia.
- En la *Evaluación del riesgo – Valoración de los controles* se identifican dos controles, uno preventivo y otro detectivo.
- Se reporta en el seguimiento de 1ª. y 2ª. línea de defensa que el riesgo no se materializó en la vigencia auditada. El control se refiere a solo el acceso a los sistemas propios o tercerizados de la entidad; sin embargo, como se expuso en el ítem 5.1, en el desarrollo de la auditoria de Gestión Financiera se identificó la amenaza que podría haber explotado la vulnerabilidad relacionada con el riesgo, que si bien no estaba controlada directamente por TIC si estaba dentro de la gestión institucional.

Riesgo 3 de Seguridad Digital:

- Se identifican tres amenazas (Pirata informático, intruso ilegal, presencia de software malicioso o virus informático) vinculadas al riesgo y una causa o vulnerabilidad (permitir el acceso de personal externo a

recursos e información no autorizados de la entidad). La redacción de la causa o vulnerabilidad no es clara[47].

- Se identifica una consecuencia (Usuarios, productos y prácticas); vinculada directamente con el riesgo (Perdida de disponibilidad).
- No se identifica la metodología empleada en el análisis de causas, por lo cual no es posible evaluar que la causa identificada corresponda a la causa raíz.
- Se observa que en la fase de análisis de riesgo éste se ubica en la zona moderada del riesgo inherente y un nivel de riesgo residual también en moderado, con un plan de tratamiento de Reducir, que identifica una acción a ejecutar relacionada con la actualización del procedimiento de Gestión de Soluciones y servicios tecnología y MTO, la cual se implementó en el 2022.
- Respecto a la evaluación de la probabilidad, se observa que se identifica un total de 495 número de veces que se realiza la actividad al año, calculado sobre 365 días del año * cada usuario que navegue en internet; sin embargo, no se identifica la fuente de información sobre la cual se está realizando este cálculo por lo que no es posible validar la información registrada.
- Frente a la valoración del criterio de impacto (Afectación económica) se reporta en 80 "*Entre 50 y 100 SMLMV: El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos"*; sin embargo, no se identifican las variables con las cuales se hace el cálculo.
- En la *Evaluación del riesgo – Valoración de los controles* se identifica un control correctivo; sin embargo, en la descripción del control se observa que tiene una periodicidad de aplicación trimestral, por lo cual la oportunidad de la frecuencia del control no sería relevante en relación al impacto de que se presenten accesos de personal externo a recursos de información no autorizados.
- No se observa la implementación de un plan de contingencia.
- Se reporta el seguimiento de 1ª. y 2ª. línea de defensa que el riesgo no se materializó.

Riesgo 4 de Seguridad Digital:

- Se identifican dos amenazas (Pirata informático, presencia de software malicioso o virus informático) vinculadas al riesgo y una causa o vulnerabilidad (Incumplimiento a los planes de mantenimiento a los equipos tecnológicos, de suministro o soporte energético).
- Se identifica una consecuencia (Usuarios, productos y prácticas).
- No se identifica la metodología empleada en el análisis de causas, por lo cual no es posible evaluar que la causa identificada corresponda a la causa raíz.
- Se observa que en la fase de análisis de riesgo éste se ubica en la zona moderada del riesgo inherente y un nivel de riesgo residual también en moderado, con un plan de tratamiento de Reducir, que identifica una acción a ejecutar relacionada con la actualización del procedimiento de Gestión de Soluciones y servicios tecnología y MTO, la cual se implementó en el 2022.
- Respecto a la evaluación de la probabilidad, se observa que se identifica un total de 86 número de veces que se realiza la actividad al año; sin embargo, no se idéntica como se efectúa el cálculo ni la fuente de información que permita validar la información registrada.

[47] Documento Maestro del Modelo de Seguridad y Privacidad de la Información de MinTIC: Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

- Frente a la valoración del criterio de impacto (Afectación económica) se reporta en 80 "*Entre 50 y 100 SMLMV: El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos"*; sin embargo, no se identifican las variables con las cuales se hace el cálculo.
- En la *Evaluación del riesgo – Valoración de los controles* se identifica un control preventivo.
- No se observa la implementación de un plan de contingencia.
- Se reporta el seguimiento de 1ª. y 2ª. línea de defensa que el riesgo no se materializo.
  Teniendo en cuenta lo descrito en los ítems 2.1. Controles A.16 y A.17, se recomienda revisar las amenazas identificadas que podrían explotar la vulnerabilidad del riesgo.

Riesgo 5 de Seguridad Digital:

- Se identifican dos amenazas vinculadas al riesgo (Acceso no autorizado y Cambios no controlados) y una causa o vulnerabilidad (Manipulación de información por externos), las cuales se articulan con la propiedad de exactitud y completitud que define el factor de riesgo asociado con la Integridad.
- Se identifica una consecuencia (Fallas tecnológicas); sin embargo, no se identifica la articulación de ésta con las amenazas y vulnerabilidad.
- No se identifica la metodología empleada en el análisis de causas, por lo cual no es posible evaluar que la causa identificada corresponda a la causa raíz.
- Se observa que en la fase de análisis de riesgo éste se ubica en la zona alta del riesgo inherente y un nivel de riesgo residual también en alto, con un plan de tratamiento de Reducir, que identifica una acción a ejecutar relacionada con la actualización del procedimiento de Seguridad de Redes, la cual se implementó en el 2022.
- Respecto a la evaluación de la probabilidad, se observa que se identifica un total de 47.450 número de veces que se realiza la actividad al año; sin embargo, si bien se evidencia la operación matemática que la genera (365*130) no se identifica como se efectúa el cálculo ni la fuente de información que permita validar la información registrada.
- Frente a la valoración del criterio de impacto (Afectación económica) se reporta en 80 "*Entre 50 y 100 SMLMV: El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos"*; sin embargo, no se identifica las variables con las cuales se hace el cálculo.
- En la *Evaluación del riesgo – Valoración de los controles* se identifica un control preventivo.
- No se observa la implementación de un plan de contingencia.
- Se reporta el seguimiento de 1ª. y 2ª. línea de defensa que el riesgo no se materializo.

Adicionalmente se observa lo siguiente sobre riesgos de Seguridad de la Información identificados por procesos diferentes al evaluado:

RIESGO	CAUSA RAIZ ¿Porqué?	ZONA DE RIESGO INHERENTE	CONTROLES	ZONA DE RIESGO RESIDUAL

1. Riesgo de Seguridad de la Información: Pérdida de la confidencialidad Activo: Información Confidencial del Historial laboral Proceso: Gestión de Talento Humano	Inadecuada gestión en el acceso a los sistemas de información	**Moderado**	Control 1: El profesional especializado de talento humano o el subdirector de corporativa envían correo a mesa de ayuda para gestionar el rol de las personas que requieren acceso al expediente de historias laborales en Orfeo. Control 2: El ingeniero encargado de Orfeo, da acceso al expediente de historias laborales únicamente a los roles enviados por la subdirectora corporativa o el profesional especializado de talento humano, por tanto, el sistema Orfeo automáticamente no deja ingresar a los usuarios que no estén autorizados al expediente de historias laborales.	**Moderado**
2. Riesgo de Seguridad de la Información: Pérdida de la disponibilidad Activo: Información de PQRSD. Proceso: Servicio al Ciudadano	Acceso restringido a las aplicaciones desarrolladas por la Secretaría General y que la Fuga tiene con interoperabilidad (SDQS) Falta de comunicación oficial	**Alto**	El Profesional de Apoyo de Servicio al Ciudadano revisa semanalmente cuales peticiones están pendientes por dar respuesta y envía por medio de correo electrónico alertas a los lideres de procesos y/o responsable de dar la respuesta. Si se evidencia peticiones por fuera de los tiempos establecidos en la ley, se remitirá por correo electrónico el caso al profesional de Control Interno Disciplinario para que sea evaluado	**Alto**
3. Riesgo de Seguridad Digital: Pérdida de la integridad. Activo: Información almacenada en el drive o correo electrónico. Proceso: Transformación cultural para la revitalización del centro	Almacenamiento de información institucional en medios diferentes a Orfeo y sistemas de información institucionales. (Correo y drive)	**Alto**	El profesional de apoyo TIC genera backup periódicos, para el resguardo de la información misional. Como evidencia están los backup en el servidor de la entidad	**Alto**
4. Riesgo de Seguridad Digital: Pérdida de la disponibilidad: Activo: Token de pagos Proceso: Gestión Financiera	Por pérdida o robo	**Moderado**	El tesorero revisa y aplica la guía de seguridad para la tesorería de la FUGA en caso de pérdida o robo del token, por lo menos dos veces al año se presentará un informe ejecutivo que dé cuenta de la ejecución de los criterios descritos en la guía con sus respectivas evidencias, el cual será socializado en el Comité de Seguimiento y Control Financiero o Comité de Inversiones.	**Moderado**

Riesgo 1:

- Activo identificado en el inventario de activos de información de gestión documental. El nivel de criticidad de este activo se registra como Media; sin embargo, las propiedades de confidencialidad e integridad son evaluadas como Alta, por lo cual el nivel debía registrarse en Alta.
- Se identifica una amenaza vinculada al riesgo (Acceso no autorizado a la información confidencial de la historia laboral o datos reservados del trabajador) y una causa o vulnerabilidad (Inadecuada gestión en el acceso a los sistemas de información), las cuales se articulan con el factor de riesgo asociado con la confidencialidad.
- Se identifica una consecuencia (Divulgación de información no autorizada); sin embargo, no se identifica la articulación de ésta con las amenazas y vulnerabilidad.

- No se identifica la metodología empleada en el análisis de causas, por lo cual no es posible evaluar que la causa identificada corresponda a la causa raíz.
- Se observa que en la fase de análisis de riesgo éste se ubica en la zona moderada del riesgo inherente y un nivel de riesgo residual también en moderada, con un plan de tratamiento de Reducir, que identifica dos acciones a ejecutar por cada control, relacionada con la actualización del procedimiento de Vinculación.
- Respecto a la evaluación de la probabilidad, se observa que se identifica un total de 32 número de veces que se realiza la actividad al año; sin embargo, no se identifica como se efectúa el cálculo ni la fuente de información que permita validar la información registrada.
- Frente a la valoración del criterio de impacto (Afectación económica) se reporta en 80 "*Entre 50 y 100 SMLMV: El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos*" sin embargo, no se identifica las variables con las cuales se hace el cálculo.
- En la Evaluación del riesgo – Valoración de los controles se identifican dos controles preventivos, vinculados con el riesgo.
- No se observa la implementación de un plan de contingencia.
- Se reporta en el seguimiento de 1ª. y 2ª. línea de defensa que el riesgo no se materializo.

Se observa en el mismo inventario de activos de la información de gestión documental, que se identifican más activos con nivel de criticidad alta (nómina y actas de comités) vinculadas al proceso de Gestión de Talento Humano, que no se encuentran gestionados como riesgos.

Riesgo 2:

- No se identifica este activo en los inventarios de información publicados por la entidad.
- Se identifican dos amenazas vinculadas al riesgo (Cambio de objetos dentro de la integración de los sistemas que afecten la interoperabilidad y Afectación de Orfeo) y dos causas o vulnerabilidades (Acceso restringido a las aplicaciones desarrolladas por la Secretaría General y que la Fuga tiene con interoperabilidad (SDQS) y Falta de comunicación oficial), las cuales se articulan con el factor de riesgo asociado con la disponibilidad. Sin embargo, no se evidencia como se articulan las vulnerabilidades con las amenazas.
- Se identifica una consecuencia (Incumplimiento normativo).
- No se identifica la metodología empleada en el análisis de causas, por lo cual no es posible evaluar que la causa identificada corresponda a la causa raíz.
- Se observa que en la fase de análisis de riesgo éste se ubica en la zona alto del riesgo inherente y un nivel de riesgo residual también en alto, con un plan de tratamiento de Reducir, que identifica una acción a ejecutar, relacionada con capacitación a los colaboradores de la entidad respecto a los tiempos de respuesta de las peticiones; sin embargo, esta acción si bien se vincula con el control, no se articula con el riesgo.
- Respecto a la evaluación de la probabilidad, se observa que se identifica un total de 2.500 número de veces que se realiza la actividad al año; sin embargo, no se identifica como se efectúa el cálculo ni la fuente de información que permita validar la información registrada.

- Frente a la valoración del criterio de impacto (Afectación económica) se reporta en 500 "*Entre 100 y 500 SMLMV: El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal"*; sin embargo, no se identifica las variables con las cuales se hace el cálculo.
- En la Evaluación del riesgo – Valoración de los controles se identifica un control preventivo; sin embargo, este no se articula con la amenazas y vulnerabilidades identificadas.
- No se observa la implementación de un plan de contingencia.
- Se reporta en el seguimiento de 1ª. y 2ª. línea de defensa que el riesgo no se materializo.

Adicionalmente se observa en el inventario de Bases de Datos, que se identifican más activos con nivel de criticidad alta (Encuestas Satisfacción - Oferta Artística, Cultural y Académica FUGA) del proceso de Servicio al Ciudadano, que no se encuentran gestionados como riesgos.

Riesgo 3:

- Si bien se identifican varios activos de información en el inventario de bases de datos vinculados al proceso, no es posible identificar la articulación de éstos con la especificación misma relacionada con el medio de almacenamiento señalado en el riesgo (Drive o correo electrónico).
- Se identifico la falta de Disponibilidad como amenaza; sin embargo, según la Guía corresponde a un posible riesgo.
- La causa o vulnerabilidad que no se articula con la descripción del riesgo.
- No se identifica la articulación de la amenaza y la vulnerabilidad con el factor de riesgo asociado con la integridad.
- Se evidencia una consecuencia (falta de disponibilidad de información); sin embargo, se observa que esta es la misma amenaza identificada (Falta de disponibilidad).
- No se identifica la metodología empleada en el análisis de causas, por lo cual no es posible evaluar que la causa identificada corresponda a la causa raíz.
- Se observa que en la fase de análisis de riesgo éste se ubica en la zona alto del riesgo inherente y un nivel de riesgo residual también en alto, con un plan de tratamiento de Reducir, que identifica una acción a ejecutar, relacionada con solicitar por correo electrónico a mesa de ayuda, generar una cuenta de correo electrónico para cada subdirección misional donde se resguarde la información.
- Respecto a la evaluación de la probabilidad, se observa que se identifica un total de 63 número de veces que se realiza la actividad al año; sin embargo, no se identifica como se efectúa el cálculo ni la fuente de información que permita validar la información registrada.
- Frente a la valoración del criterio de impacto (Afectación económica) se reporta en 101 "*Entre 100 y 500 SMLMV: El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal."*; sin embargo, no se identifica las variables con las cuales se hace el cálculo.
- En la Evaluación del riesgo – Valoración de los controles se identifica un control preventivo.
- No se observa la implementación de un plan de contingencia.
- Se reporta en el seguimiento de 1ª. y 2ª. línea de defensa que el riesgo no se materializo.

Riesgo 4: (Eliminado en la actualización del mapa de riesgos del 2024).

Conforme lo expuesto anteriormente se recomienda:

- Identificar los dueños de los activos de información desde el inventario, de tal manera que se establezcan responsabilidades directas en la gestión del riesgo.
- Si bien es posible agrupar activos, es importante definir claramente la directriz para evaluar los riesgos frente a los activos identificados, de tal manera que se puedan gestionar de acuerdo a las particularidades de cada uno de ellos.
- Revisar y si es pertinente ajustar las amenazas y vulnerabilidades identificadas de tal manera que estas se articulen entre si y con el factor de riesgo asociado, para lo cual se debe tener como referencia la *Guía para la Administración del riesgo y el diseño de controles en entidades públicas* Versión 6 del DAFP y el *Modelo Nacional de Gestión de Riesgos de Seguridad de la Información en entidades Públicas*, de MinTIC, tanto para su articulación como para su definición.
- Documentar el análisis de causas de tal manera que sea posible revisar si la identificación de la causa raíz registrada en la matriz de riesgos es adecuada.
- En la valoración de afectación económica o reputacional y probabilidad se recomienda incluir la fuente de información, de tal manera que se posible hacer la evaluación objetiva correspondiente.
- Incluir dentro de la valoración del riesgo los factores relacionados con las variables de presupuestales y ambientales.
- Teniendo en cuenta que no se evidencian planes de contingencias asociados con los planes de continuidad del negocio para los riesgos identificados, se recomienda su documentación.
- Si bien todos los riesgos se integran en la Matriz Consolidadas de Riesgos, se recomienda, por las particularidades propias de los riesgos de seguridad de la información ya señaladas en este ítem, definir una estructura conforme la Figura 26. Formato mapa de riesgos seguridad de la información, dispuesta en la Guía *para la Administración del riesgo y el diseño de controles en entidades públicas* Versión 6 del DAFP

7. Indicadores:

Se validó la información dispuesta en la Matriz consolidada de indicadores año 2023 aportada por el proceso, observándose 4 indicadores formulados, con el respectivo seguimiento:

Nombre del Indicador	Fórmula	Tipo	Meta	Resultado 2023
1. Porcentaje de disponibilidad de la infraestructura tecnológica proporcionada por la entidad	(Número de horas totales monitoreadas por periodo - Número de horas paradas por mantenimiento monitoreadas por periodo/Número de horas totales monitoreadas por periodo) * 100	Calidad	90%	93%
2. Porcentaje de implementación de controles asociados al Modelo de Sistema de Gestión de	(Promedio porcentual de Evaluación de Efectividad de controles / Calificación objetivo según el MSPI)	Eficacia	85%	89%

Seguridad de la información MSPI				
3. Porcentaje de mantenimiento de infraestructura tecnológica	(N° de actividades ejecutadas en el periodo / Total de actividades de mantenimiento de infraestructura tecnológica programadas en el periodo) x 100%	Eficacia	90%	100%
4. Porcentaje de atención oportuna de requerimientos	(N° Requerimientos atendidos en el tiempo establecido (2 días) / N° Requerimientos solicitados) x 100	Eficacia	90%	81%

Conforme lo registrado en las Fichas Técnicas de cada uno de los indicadores, se observa:

Indicador 1: En el análisis de datos se presenta con condición satisfactoria el I, II y IV trimestre, en el III trimestre en condición normal por cuanto las horas dispuestas excedieron el indicador programado; en términos generales se observa que el rango de aceptación satisfactorio tiene un comportamiento justificado en el análisis, por encima de lo esperado (93% de 90% previsto). La evidencia aportada en el https://drive.google.com/drive/folders/1XzaTLsG682IFoKB4h4iOfDEcdbAkeLEu corresponde a los Informes Disponibilidad Infraestructura, gestionados a través de Prometheus en el I y II trimestre de la vigencia.

Indicador 2: En los datos de medición se registra un resultado final de 89% frente a una meta de 85% programada, ubicándose en una condición satisfactoria. Este indicador tiene una frecuencia de medición anual, observándose que en términos generales el rango de aceptación tiene un comportamiento por encima de lo esperado, lo cual se encuentra justificado en el análisis. Es importante señalar que de acuerdo a la verificación realizada por la OCI este porcentaje de implementación alcanza el 73%.

Indicador 3: En los datos de medición se registra un resultado final de 100% frente a una meta de 90% programada, ubicándose en una condición satisfactoria. Este indicador tiene una frecuencia de medición semestral, observándose que en términos generales el rango de aceptación tiene un comportamiento por encima de lo esperado. Si bien el drive aportado como evidencia en la hoja de vida del indicador (https://drive.google.com/drive/u/1/folders/1xRgTq8DYVdsg8MU5g_QRwoYdBq33i4tu) solo incluye la gestión del primer semestre, el resultado de la evaluación integral de la ejecución de las variables del indicador se observa en la Acción 1 del PETI desarrollada en el ítem 1.2 del presente informe, ejecución que es coherente con la medición aquí registrada.
Indicador 4: En el análisis del indicador se presenta con condición normal total, con un resultado de 81% frene a la meta programada del 90%. En el análisis de datos se señala en términos generales los meses en los cuales no se alcanza la condición satisfactoria; sin embargo, no es posible identificar de manera clara los problemas técnicos que ocasionaron la resolución en tiempos mayores al previsto (2 días). La evidencia aportada en el drive (https://drive.google.com/drive/u/1/folders/1YHorE_Hrpk1eOXytM95GDhcDF6tCLmjB) solo da cuenta de la gestión del primer semestre de la vigencia.

En términos generales se recomienda:
- En la formulación de los indicadores del 2024 revisar la meta de conformidad con el resultado del 2023.
- Documentar de manera integral la medición reportada. (Indicador 1, 3 y 4)

- Teniendo en cuenta que los indicadores son los mismos de la vigencia 2022, se recomienda en la formulación del 2024 en el evento de mantenerlos, incluir la línea base teniendo en cuenta los resultados presentados.
- Hacer las autoevaluaciones con objetividad teniendo en cuenta las oportunidades de mejora evidenciadas por la OCI.

8. Planes de Mejoramiento vinculados al Proceso:

Plan de Mejoramiento Institucional:

Se verificó el plan de mejoramiento institucional cargado en la plataforma SIVICOF de la Contraloría de Bogotá y en la plataforma interna PANDORA, identificando que el proceso auditado no tiene hallazgos y acciones correctiva abiertas bajo su responsabilidad.

Plan de Mejoramiento por Procesos:

De la verificación realizada por la OCI en el seguimiento realizado en diciembre a la gestión de los Planes de Mejoramiento por Procesos reportada a través del aplicativo interno PANDORA, se evidencio que el proceso auditado en un ejercicio de autoevaluación identificó un riesgo materializado por perdida de información debido a un disco duro dañado de un servidor, señalando como causa raíz el no tener lineamientos para realizar controles y monitoreos de salud regulares sobre los medios de almacenamiento.

Frente a este hallazgo se formuló la actividad de actualizar el procedimiento de respaldos incluyendo un punto de control de realizar un seguimiento mensual para evidenciar el monitoreo continuo de la salud de los medios de almacenamiento de la entidad; actividad que fue evaluada y clasificada por la OCI en estado cerrada conforme se evidencia en el informe presentado el 21/12/2023 (20231100133053).

Respecto a la efectividad del plan de mejoramiento suscrito a partir de los resultados de la auditoría realizada en el 2020 (20201100013513), se observa que para los 4 hallazgos identificados se suscribieron 4 actividades:

Hallazgo 1: Cumplimiento parcial de los lineamientos establecidos en el PETI expuestos en los numerales 1.1, 2.7 y 2.8 del presente informe.
Para este hallazgo se implementaron 2 acciones relacionadas con estructuración de matriz con los planes, seguimientos y capacitaciones; de acuerdo a lo observado en el desarrollo de esta auditoría, si bien la mayoría se encuentran subsanadas por lo que se evalúo como inicialmente Cerrada con Baja Efectividad, aún se presentan algunas debilidades, expuestas en el ítem 1 del presente informe.

Hallazgo 2: No se identifican en la Política de Administración de Riesgo de la entidad (CEM-PO-01) Versión 2, los criterios establecidos en los numerales 4.1.2, 4.1.4, 4.1.6 y 4.1.7 del anexo 4 Lineamientos para la Gestión de Riesgos de Seguridad Digital en entidades Púbicas de MINTIC. • El Mapa de Riesgos de la entidad no integra en su totalidad los riesgos identificados por el Proceso en el Plan de Tratamiento de

Riesgos y no cumple con todos los aspectos identificados para este tipo de riesgos en el Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP.

Para este hallazgo se implementaron 2 acciones relacionadas con el ajuste de la política y de los instrumentos de gestión de riesgos; si bien en términos generales esta fue efectiva por cuanto la política actualizada incluye los lineamientos del DAFP relacionada con los riesgos de seguridad de la información y la ficha de riesgos adopta una metodología específica para este tipo de riesgos, se evidencia que la matriz consolidada no permite identificar las características especiales de los riesgos vinculados a la seguridad de la información por lo que se evalúo inicialmente con Cerrada con Baja Efectividad.

Sobre este particular la OCI presento la siguiente alerta en la evaluación realizada en noviembre de 2022 a la ejecución de los planes de mejoramiento:

> *Hallazgo 2: Si bien la actividad se ejecutó en los procesos antes señalados y que la gestión, tal como lo indica la 2a. Línea de defensa, se llevó a cabo de manera extemporánea; se presenta una alerta de materialización de eventos no deseados de seguridad de la información en otros procesos que si bien manejan bases de datos, software, información, hardware, entre otros (de acuerdo a lo registrado en los inventarios de activos de información vigentes publicados - https://fuga.gov.co/transparencia-y-acceso-a-la-informacion-publica/datos-abiertos?field_fecha_de_emision_value=All&term_node_tid_depth=112); aun no tienen identificados en sus mapas de riesgos este tipo de eventos (Recursos Físicos, Planeación, Gestión de las Comunicaciones, entre otros).*

Conforme lo evidenciado en el desarrollo del presente ejercicio, se evidencia la subsanación de las situaciones que originaron el hallazgo.

Hallazgo 3: No se encuentran publicados los siguientes documentos: • Plan de mantenimiento de servicios Tecnológicos vigencia 2020 • Anexo 1 del Plan de Mantenimiento Infraestructura Tecnológica (Cronograma de mantenimiento Infraestructura Física) de la vigencia 2019 El documento publicado Políticas de Seguridad de la Información se encuentra desactualizado.

Para este hallazgo se implementaron 2 acciones relacionadas con estructuración de matriz con los planes, seguimientos y capacitaciones; de acuerdo a lo observado en el desarrollo de esta auditoría, estas fueron efectivas.

Hallazgo 4: De conformidad con el resultado de la evaluación realizada al nivel de madurez del modelo de seguridad y privacidad de la información (MSPI), se observó que no se implementaron los plazos establecidos por MINTIC y Gobierno en Línea; lo anterior teniendo en cuenta que los siguientes criterios presentan debilidades respecto al cumplimiento de los requisitos establecidos para cada uno de ellos. (Calificación por debajo de 40) • A 10: Criptografía • A 14: Adquisición, desarrollo y mantenimientos de sistemas • A 17: Aspectos de seguridad de la información de la gestión de continuidad del negocio De igual forma se observaron controles cuyos requisitos se cumplen con una calificación entre 40 y 70 puntos: • A.5: Políticas de Seguridad de la Información • A 6: Organización de la seguridad de la información • A.7: Seguridad de los recursos Humanos • A 8: Gestión de Activos • A 9: Control de Acceso • A 11: Seguridad

Física y del Entorno • A 12: Seguridad de las operaciones • A 13: Seguridad de las comunicaciones • A 16: Gestión de Incidentes de Seguridad de la Información.

Para este hallazgo se implementaron 2 acciones relacionadas con estructuración de matriz con los planes, seguimientos y capacitaciones; de acuerdo a lo observado en el desarrollo de esta auditoría, si bien se evidencia un avance importante en el nivel de madurez identificado (Auditoria 2020: 58%; Auditoria 2023: 73%), se observa que aún se mantienen algunas debilidades relacionadas con la implementación de los controles ya señalados en el ítem 2 del presente informe.

Teniendo en cuenta que los hallazgos 1 y 4 no ha sido subsanados de manera integral, en los seguimientos realizados a la ejecución de los planes de mejoramiento realizadas en marzo del 2021 y noviembre de 2022, las acciones vinculadas el riesgo se evaluaron como Cerradas con Baja Efectividad, con las siguientes alertas:

> *Hallazgos 1, 3 y 4: Se observa que la acción establecida no subsana lo evidenciado en la auditoria al proceso de Gestión de Tecnologías. De la verificación realizada al Formato Acción Correctiva y de Mejora, se evidencia que se unificaron los hallazgos 1, 3 y 4; sin embargo, la acción formulada corresponde a una situación general pero no ataca la situación particular de cada uno de los hallazgos planteados. Se evidencia adicionalmente que si bien se integran dos metodologías (Lluvia de ideas y Porqués); en el desarrollo de la técnica 2 no se evidencia la secuencia o efecto cascada de la respuesta a los porqués, lo que no permite identificar de manera clara cual es punto final del cuestionamiento realizado que facilite la identificación de la causa raíz.*
>
> *La causa determinada corresponde a una debilidad de equipo de trabajo; sin embargo, la acción propuesta corresponde a una actividad metodológica.*

Adicionalmente la OCI presento las siguientes recomendaciones iniciales cuando fueron formuladas las acciones:

- Fortalecer los criterios para validar la coherencia metodológica y la aplicación de las técnicas en la formulación de las acciones correctivas o de mejora llevado a cabo por la 2a. Línea de defensa; de conformidad con lo establecido en la actividad 3 del procedimiento Plan de Mejoramiento (GM-PD-01) Versión 3.
- Revisar y de considerarse pertinente separar los análisis de causa de los 3 hallazgos consolidados en esta actividad, lo anterior teniendo en cuenta el contexto del informe de auditoría que origino las no conformidades

Conforme lo anterior, de manera general se recomienda atender las recomendaciones expuestas en los informes tanto de seguimiento como de auditoría, de tal manera que se garantice la efectividad de las acciones implementadas en el proceso de mejora continua.

Eliminación de Hallazgos Informe Preliminar:

De conformidad con la respuesta del equipo auditado al informe preliminar radicada el 28/05/2024 Orfeo 20242000052303, se validó la evidencia complementaria aportada, con la cual se subsanaron las situaciones que dieron origen al hallazgo 5:

5	Manual de Contratación FUGA código GJ-MN-01 Versión 16.	Debilidades en la etapa precontractual publicación en Secop II del contrato FUGA-127-2023 (Orfeo) y FUGA-SASI-112-2023 (Secop II), incumpliendo lo establecido en el Manual de contratación 5.3.1 y en el Decreto 1082 de 2015. Artículo 2.2.1.1.1.7.1

De acuerdo al resultado de la evaluación expuesta en los ítems desarrollados en el presente informe, se configuran los siguientes hallazgos:

DESCRIPCIÓN DE HALLAZGOS		
No.	**Requisito**	**Descripción hallazgo**
1	• Resolución Interna 219 de 2023 “Por la cual se adopta el modelo de seguridad de información” • Modelo Nacional de Gestión de Riesgo de Seguridad de la Información (MNGRSI) - 3.1.4	Incumplimiento de lo establecido en el artículo 5 *Instancias* de la Resolución Interna 219 de 2023, por cuanto no se evidencia la designación del Oficial de Seguridad. Tampoco se identifica la designación del responsable de Seguridad Digital en la entidad conforme se establece en el MNGRSI.

2	• Decreto 1078 de 2015. por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Título 17 lineamientos generales en el uso y operación de los servicios ciudadanos digitales. Artículos 2.2.17.1.6 y 2.2.17.5.6 • Modelo Integrado de planeación y gestión, 3ª. Dimensión: Gestión con valores para resultados. 3.2.1.3 Política Gobierno Digital y 3.2.1.4 Política de Seguridad Digital • Decreto 1072 de 2015, por medio del cual se expide el Decreto Único Reglamentario del Sector Trabajo Artículo 2.2.4.6.4. • Ley 1523 de 2012, Por la cual se adopta la política nacional de gestión del riesgo de desastres y se establece el Sistema Nacional de Gestión del Riesgo de Desastres. Artículo 2°. • ISO 27031 – DE198-13 Tecnología de la Información, Técnica de Seguridad, Directrices para la continuidad del negocio.	No se cuenta con un Plan de Continuidad de Negocio que garantice la preservación, disponibilidad y continuidad de los servicios que ofrece la entidad, de acuerdo a lo observado en la evaluación del Anexo A de la ISO 27001:2013 relacionada con la gestión de incidentes de seguridad de la información (A.16) y aspectos de seguridad de la información de la gestión de la continuidad del negocio (A.17).
3	Modelo de Seguridad y Privacidad de la Información. Componente Ciberseguridad ISO 27001:2013.	La entidad no cuenta con un Plan de Recuperación ante desastres de tecnología que le permita garantizar la recuperación de la información y el mantenimiento del servicio tecnológicos, en cumplimiento de las mejores prácticas del NIST (National Institute of Standards and Technology) y lo dispuesto en la ISO 27001:2013 aplicables en el tema de Ciberseguridad.
4	Manual de supervisión e interventoría Código: GJ-MN-02 Versión 3.	Debilidades en la supervisión del contrato FUGA-170-2021 (Orfeo) y FUGA-PMC-155-2021 (Secop II), incumpliendo lo establecido en el Manual de supervisión e interventoría y lo estipulado en la cláusula No 5 del contrato *"Forma de Pago*"

RECOMENDACIONES GENERALES:

- Analizar las oportunidades de mejora y recomendaciones presentadas en este informe e implementar las mejoras que se consideren pertinentes.
- Actualizar la documentación acorde con la realidad institucional y las sugerencias hechas por la OCI in situ, en desarrollo del presente ejercicio de auditoría.

- Revisar y ajustar el normograma del proceso, de tal manera que se asegure su actualización permanente y la incorporación de todas las normas que le impactan.
- Documentar de manera integral la ejecución del PETI, conforme los productos entregables definidos en el Plan.
- Documentar de manera integral la implementación de los criterios vinculados a los controles del MSPI.
- Identificar los criterios aplicables a la entidad, de acuerdo a su realidad institucional y definir la Declaración de Aplicabilidad.
- Revisar y priorizar la implementación de los controles vinculados al nivel de madurez Optimizado.
- Revisar los criterios vinculados a los aspectos de Ciberseguridad relacionados con la función de Recuperar e implementar todos los criterios vinculados que permitan garantizar una gestión acertada sobre este aspecto, vinculado específicamente a Planes de Recuperación, mejoras y comunicaciones.
- Los responsables de la supervisión de los contratos deben revisar los informes y la evidencia suministrada por los contratistas, de tal forma que tenga coherencia la información con la documentación cargada tanto en Orfeo como en Secop II.
- Cumplir con lo establecido en Convenio Fuga-1629- 2021 aplicativo PANDORA para llevar a cabo las citaciones a las sesiones del Comité de Desarrollo de Software.
- Se recomienda para el *Instrumento de medición MSPI diciembre 2023* especificar de forma ordenada las evidencias aportadas que facilite la revisión por parte de la OCI.
- Se recomienda cargar en Secop II los documentos que reposan en Orfeo para toda la gestión contractual.
- En términos generales se recomienda revisar las observaciones específicas que realizó el equipo auditor en el presente informe y en auditorias pasadas, para así realizar los ajustes o correcciones que se consideren pertinentes.
- Documentar la ejecución de MIPG de manera integral, asegurando la articulación entre el % de cumplimiento reportado y la evidencia que da cuenta de lo ejecutado.
- Revisar y ajustar la gestión de riesgos de acuerdo a las situaciones evidenciadas en el ítem 5 del presente informe.
- Asegurar la implementación integral de los controles asociados a los riesgos del proceso, de tal manera que se minimice la probabilidad de su materialización.
- Revisar y ajustar los riesgos siguiendo los lineamientos establecidos y las recomendaciones dadas por la OCI.
- Revisar los resultados de esta auditoría en conjunto con los diferentes procesos que interactúan con Gestión de Tecnologías, apropiando el concepto de gestión por procesos para lograr una coordinación armónica que permita mejorar la gestión institucional.
- Se sugiere hacer una revisión de roles y responsabilidades para asegurar la segregación efectiva de controles y funciones en el proceso.
- Conforme lo evidenciado en el desarrollo de la auditoria se recomienda, de acuerdo a la magnitud e impacto de la seguridad de la información, revisar la asignación de recursos que permitan el cumplimiento de todos los criterios evaluados y la implementación integral del Modelo de Seguridad de la Información y los sistemas articulados a este.

INFORME DE AUDITORÍA	Radicado: **20241100053543** Fecha: 30-05-2024

FICHA TÉCNICA:

Herramientas Utilizadas:

- Lista de Verificación
- Actas de Reunión
- https://www.fuga.gov.co/transparencia
- https://intranet.fuga.gov.co/node/23

Muestra:

- Se tomaron muestras aleatorias de procesos de contratación vinculados a la gestión TIC, evaluados en el ítem 3.
- De acuerdo a los inventarios de activos de información publicados en la página web se hizo una muestra aleatoria para validar la gestión realizada en el ítem 53.1 del presente informe,
- Se verifico en los mensajes dispuestos en el WhatsApp institucional y se seleccionaron de manera aleatoria aquellos vinculados al reporte de fallas en los sistemas de información de la entidad.
- De los reportes GPLI aportados como evidencia se evaluaron como muestra aquellos en los cuales fue posible identificar situaciones vinculadas a fallas en los servicios tecnológicos presentados en la entidad.

CONCLUSIONES DE AUDITORÍA:

En el desarrollo de la auditoria se presentan oportunidades de mejora en términos de eficacia y eficiencia en la gestión del proceso.

ANEXOS: Archivo Excel instrumento medición dic2023

Este documento corresponde a los resultados del Informe Preliminar presentado y aprobado mediante acta radicada con el No. 20241100050933 de fecha 23/05/2024 con el Líder del Proceso y el equipo auditado.

MARÍA JANNETH ROMERO MARTÍNEZ LAURA JULIANA FANDIÑO CUBILLOS
EQUIPO AUDITOR
ANGELICA HERNÁNDEZ RODRÍGUEZ
JEFE OFICINA DE CONTROL INTERNO

El Documento 20241100053543 fue firmado electrónicamente por:

Laura Juliana Fandiño Cubillos **Contratista**,
Oficina de Control Interno ,
ID: 1016004056,
lfandino@fuga.gov.co,
Fecha de Firma: 30-05-2024 12:23:35

Maria Janneth Romero **Contratista**,
Oficina de Control Interno ,
ID: 51841680,
mromero@fuga.gov.co,
Fecha de Firma: 30-05-2024 12:17:31

Angélica Hernández Rodríguez ,
Oficina de Control Interno ,
ID: 1016009105,
ahernandez@fuga.gov.co,
Fecha de Firma: 30-05-2024 12:37:43

51c96f33fef7e358f9599bc0083826671acfdaef73bd78b4a9e0a91b5ef9b203
Codigo de Verificación CV: 55aff