INSTITUTO PARA LA ECONOMIA SOCIAL - IPES
COMUNICACIONES - INTERNAS
AL CONTESTAR POR FAVOR CITE:
Radicado: 10-817-2025-002334
Fecha: 29/07/2025 - 03:07 PM
Remitente: ANDRES MENDEZ JIMENEZ
Destinatario: WILFREDO GRAJALES ROSAS
No.Folios: 3 Anexos: 61

MEMORANDO

110301

Bogotá DC.,

PARA: WILFREDO GRAJALES ROSAS Director General

ADRIANA VILLAMIZAR NAVARRO, Subdirectora de Diseño y Análisis Estratégico

DE: ANDRÉS MÉNDEZ JIMÉNEZ, Asesor de Control Interno

ASUNTO: INFORME FINAL DE AUDITORÍA MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI) IPES 2024-2025

Respetado Director y Subdirectora:

En el marco del Sistema de Control Interno se ha de tener en cuenta lo establecido por la Ley 87 de 1993 en cuanto a quiénes son los responsables de la implementación de un sistema de control interno en las entidades del Estado:

"ARTÍCULO 6º. Responsabilidad del control interno. El establecimiento y desarrollo del Sistema de Control Interno en los organismos y entidades públicas, <u>será responsabilidad del representante legal o máximo directivo correspondiente</u>. No obstante, la aplicación de los métodos y procedimientos al igual que la calidad, eficiencia y eficacia del control interno, <u>también será de responsabilidad de los jefes de cada una de las distintas dependencias de las entidades y organismos".</u> Subrayado fuera de texto.

Aunado a lo anterior, se contempla en el Manual Operativo del Decreto 1499 de 2017, que articula los Sistemas Integrados de Gestión y de Control Interno, específicamente en la séptima dimensión del MIPG, el Control Interno, contempla cinco componentes de la estructura del MECI: 1) Ambiente de Control, 2) Evaluación del Riesgo, 3) Actividades de Control, 4) Información y Comunicación, y 5) Actividades de Monitoreo.

En este sentido la Asesoría de Control Interno, dentro del rol de evaluador independiente (tercera línea de defensa) y de acuerdo a lo dispuesto en el Plan Anual de Auditoria 2025, entregó a la Administración del IPES los resultados de la Auditoría Interna Regular al cumplimiento del **MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI) IPES 2024-2025** como habilitador de

Carrera 9 N° 10-59
PBX. (+57)
6014841930
Línea Gratuita
018000517621
www.ipes.gov.co

la Política de Gobierno Digital, en el marco del Modelo Integrado de Planeación y Gestión (MIPG), conforme a los lineamientos establecidos por el MinTIC, a través de la presentación del informe preliminar enviado a la Subdirección de Diseño y Análisis Estratégico- SDAE para réplica con los radicados que se detallan a continuación

Subdirección	Informe Preliminar		Réplica	
	N° Radicado	Fecha	N° Radicado	Fecha Réplica
SDAE	10-817-2025-002152	15-julio-2025	10-817-2025-002245	21-julio-2025

Por otra parte y siguiendo lo dispuesto a nivel del procedimiento de auditoria en el IPES, se llevó a cabo reunión de cierre de auditoría interna el lunes 28 de julio de 2025.

Es importante precisar que la Subdirección de Diseño y Análisis Estratégico, junto con los responsables del procedimiento auditado, deben suscribir un Plan de Mejoramiento relacionando la causa raíz de cada observación, las acciones de mejora que mitiguen la misma con tiempos y responsables, haciendo uso del Archivo Excel "PV01-FO-015 V2 PLAN DE MEJORAMIENTO AUDITORIAS INTERNAS" el cual se encuentra publicado en SIG MIPG, para lo cual se tendrá **8 días hábiles a partir de la fecha de radicación de este Informe Final.**

Con el fin de cumplir con el objetivo de la mejora continua de los procesos y conscientes de la importancia de formular acciones de mejora efectivas para la mitigación de riesgos del proceso, desde la Asesoría de Control Interno se propondrá sesión de acompañamiento particular con la Subdirección de Diseño y Análisis Estratégico, la cual si se considera necesaria por el proceso auditado será citada de manera acordada con el auditor y la(s) persona(s) asignada(s) por la Subdirección responsable.

Por lo que agradecemos a la SDAE, designar a los responsables de la formulación y seguimiento de acciones de mejora, quienes deberán aportar en el espacio propuesto de trabajo, un primer borrador para retroalimentación por parte del auditor responsable.

Posterior a ello, la Asesoría de Control Interno realizará seguimiento al cumplimiento del Plan de Mejoramiento con el fin de asegurar que hayan sido tomadas las acciones definidas por el auditado y corregidas las observaciones para ser subidas a través del sistema dispuesto.

Carrera 9 N° 10-59
PBX. (+57)
6014841930
Línea Gratuita
018000517621
www.ipes.gov.co

Por último, en el marco del Programa de Aseguramiento y Calidad - PAMC que comprende la estandarización del proceso de auditoría interna basada en riesgos en el IPES, de manera atenta les solicito comedidamente, que con los funcionarios responsables del proceso y/o procesos auditados, cada subdirector diligencie la Encuesta de Satisfacción que será remitida en los próximos días.

Cordialmente,

ANDRÉS MÉNDEZ JIMÉNEZ

Anexos: Informe Final Auditoría MSPI 2025 – Cincuenta y nueve (59) folios
Anexo 1. Papel de Trabajo MSPI - IPES 2025 VF.xlsx
Anexo 2. Mapas de Calor - Riesgos GIRT.xlsx

	NOMBRE, CARGO O CONTRATO	FIRMA	FECHA
Elaboró	Sergio Andrés Castro Londoño – CO1.PCCNTR.7734097 / GOOBI 306 de 2025		29-Julio-2025
Revisó Aprobó	Andrés Méndez Jiménez - Asesor de Control Interno		29-Julio-2025
Los arriba firmantes declaramos que hemos revisado el presente documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad, lo presentamos para firma del **Asesor de Control Interno** del Instituto para la Economía Social IPES			

Carrera 9 N° 10-59
PBX. (+57)
6014841930
Línea Gratuita
018000517621
www.ipes.gov.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.

Tipo de Auditoría	Especial		Regular	X	
Código Auditoría	N/A				
Fecha Auditoría	02 de mayo 2025 al 07 de julio de 2025				
Dependencia	Gestión de la Información y de los Recursos Tecnológicos				

Contenido

1. CONTEXTO Y JUSTIFICACIÓN 1
2.1 OBJETIVOS ESPECÍFICOS 5
3. ALCANCE 6
4. LIMITACIÓN AL ALCANCE 8
5. CONFORMACIÓN EQUIPO DE TRABAJO DE AUDITORÍA 8
6. FORTALEZAS 8
7. CONTEXTO AUDITORÍA 9
7.1. MARCO NORMATIVO 10
8. RESUMEN DE RESULTADOS DE LA AUDITORÍA 11
9. DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍA 26
10. PLAN DE MEJORAMIENTO 58
11. ANEXOS 59

1. CONTEXTO Y JUSTIFICACIÓN

Dentro de las competencias de la Asesoría de Control Interno enmarcadas en la Ley 87 de 1993 está evaluar la eficiencia, eficacia y economía de los controles, asesorando a la Dirección General en la:

a. Continuidad del Proceso Administrativo,
b. Revaluación de los planes establecidos
c. Introducción de los correctivos necesarios para el cumplimiento de las metas y objetivos previstos por la Entidad.

De acuerdo al Plan Anual de la vigencia 2025, la Asesoría de Control Interno programó trabajo a Auditoría Interna Regular y definió en su Alcance procesos y procedimientos que ejecuta la dependencia: Gestión de la Información y de los Recursos Tecnológicos

Este trabajo se llevó a cabo entre el 02 de mayo y el 07 de julio del 2025.

De acuerdo con el Plan Anual de Auditoría para la vigencia 2025, aprobado por el Comité Institucional de Coordinación de Control Interno en la cuarta sesión realizada el 9 de diciembre de 2024, la Asesoría de Control Interno programó la ejecución de una Auditoría Interna Regular sobre la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en el Instituto para la Economía Social (IPES). Esta auditoría se fundamenta en lo dispuesto por el Modelo Integrado de Planeación y Gestión (MIPG), específicamente en el habilitador denominado "Seguridad de la Información" establecido por la Política de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

El MSPI, definido por MinTIC, obliga a las entidades públicas de los órdenes nacional, territorial y distrital a adoptar medidas efectivas para garantizar la protección integral de los activos de información institucionales, asegurando el cumplimiento de los principios fundamentales de confidencialidad, integridad, disponibilidad y privacidad. En cumplimiento de estas obligaciones, el IPES debe seguir los lineamientos establecidos en la Resolución No. 500 de 2021 y la Resolución No. 002277 de 2025 del MinTIC, además de adherirse a las directrices contenidas en la Política de Gobierno Digital establecida en el Decreto 767 de 2022.

Estas normativas exigen que las entidades estructuren e implementen un modelo integral de gestión de la seguridad de la información basado en la identificación, análisis y gestión de riesgos, la implementación de controles técnicos y administrativos adecuados, la formalización de procedimientos internos, la ejecución oportuna de planes de acción y la aplicación de mecanismos efectivos de monitoreo y mejora continua. Dicho modelo debe alinearse con estándares internacionales ampliamente reconocidos, tales como las normas ISO/IEC 27001:2022 (Sistema de Gestión de Seguridad de la Información), ISO/IEC 27005:2022 (Gestión de Riesgos de Seguridad de la Información) e ISO 22301:2019 (Gestión de la Continuidad del Negocio), para lograr una gestión integral, coherente y eficaz de la seguridad informática, seguridad digital y ciberseguridad institucional.

En este contexto, y considerando las responsabilidades del IPES en la implementación progresiva del MSPI, se realizó una auditoría interna cuyo objetivo específico fue evaluar el cumplimiento de metas, productos y resultados establecidos en las fases del ciclo operativo del MSPI: diagnóstico, planificación, implementación, evaluación del desempeño y mejora continua. Además, se buscó verificar la existencia, pertinencia y eficacia de los productos, artefactos y documentos técnicos generados por el Instituto para cumplir con dicho modelo, identificando posibles brechas normativas, deficiencias técnicas o administrativas, riesgos emergentes y oportunidades de mejora que pudieran afectar la madurez del sistema de gestión de seguridad de la información.

Esta auditoría buscó fortalecer la gobernanza institucional, asegurar la trazabilidad y efectividad de las acciones implementadas, y consolidar una cultura institucional orientada a la gestión de riesgos tecnológicos, seguridad digital y protección integral de la información. Asimismo, dado que los sistemas de información misionales HEMI y GOOBI son críticos para los procesos estratégicos y operativos del IPES por procesar, almacenar

y transmitir información sensible sobre beneficiarios, contratistas y procesos administrativos y sociales, se evaluó el cumplimiento de los principios fundamentales de confidencialidad, integridad, disponibilidad y privacidad en dichos sistemas.

Adicionalmente, se analizó la existencia de vulnerabilidades técnicas o administrativas que pudieran comprometer la seguridad, la eficacia de los controles implementados, el tratamiento de los riesgos identificados y la capacidad de respuesta institucional ante amenazas emergentes. Finalmente, la auditoría permitió validar el cumplimiento normativo en la gestión de la seguridad de los sistemas HEMI y GOOBI, identificar brechas o fallos en los controles actuales, formular recomendaciones para fortalecer el MSPI y promover una cultura organizacional orientada a la protección de activos de información y a la resiliencia frente a incidentes de seguridad.

HEMI (HERRAMIENTA MISIONAL)

En el marco de la auditoría interna sobre la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), se validaron aspectos de seguridad y generalidades funcionales de la herramienta misional HEMI, plataforma tecnológica a través de la cual el Instituto para la Economía Social (IPES) soportó operativamente sus procesos estratégicos y misionales. Esta solución permitió el registro, gestión y análisis de la información asociada a la atención integral de los beneficiarios del Instituto, en alineación con los planes de desarrollo del Distrito y las políticas públicas del Gobierno Distrital.

Dada su criticidad operativa y su papel en el soporte de los procesos misionales del Instituto, el sistema HEMI fue objeto de revisión técnica y normativa conforme a los lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI), contemplados en la Resolución 500 de 2021 y la Resolución 002277 de 2025 del MinTIC, el Decreto 620 de 2020, el Marco de Interoperabilidad del Estado colombiano, y la normativa vigente en materia de protección de datos personales, particularmente la Ley 1581 de 2012 y sus decretos reglamentarios. Esta revisión también se basó en estándares internacionales como las normas ISO/IEC 27001:2022 (gestión de seguridad de la información), ISO/IEC 27005:2022 (gestión de riesgos) e ISO/IEC 22301:2019 (continuidad del negocio).

En este marco normativo, se recomienda reemplazar prácticas manuales de intercambio de información, como el cargue de archivos planos entre entidades, por mecanismos de interoperabilidad técnica en línea, seguros y auditables. El procesamiento manual puede llegar a incrementar riesgos asociados a la confidencialidad, integridad y disponibilidad de los datos (CID), debido a la posible exposición a errores humanos, falta de trazabilidad, ausencia de controles criptográficos y dificultad para garantizar la autenticidad de la información.

De acuerdo con la política de Gobierno Digital (Decreto 767 de 2022) y el Marco de Interoperabilidad del Estado, las entidades públicas están obligadas a adoptar soluciones que permitieran el intercambio automatizado, oportuno y seguro de datos. La interoperabilidad técnica no solo reduce la exposición a vulnerabilidades, sino que fortalece la gestión de riesgos tecnológicos, promoviendo la eficiencia operativa y contribuyendo al cumplimiento efectivo de los principios del MSPI.

Por tanto, en el análisis del sistema HEMI, se evaluó si los procesos actuales garantizaban la seguridad de la información bajo esquemas automatizados, y si se habían implementado mecanismos de interoperabilidad compatibles con los lineamientos del MinTIC y los estándares internacionales aplicables.

GOOBI ERP (SISTEMA ADMINISTRATIVO Y FINANCIERO):

En el marco de la auditoría interna sobre la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), se validaron aspectos de seguridad de la información y generalidades funcionales del sistema GOOBI GRP (Gestión de Recursos Públicos), solución tecnológica adoptada por el Instituto para la Economía Social – IPES para soportar la gestión administrativa y financiera de la entidad. Esta plataforma, especializada en el sector público bajo un enfoque ERP (Enterprise Resource Planning), integra transversalmente los procesos institucionales relacionados con la planeación, ejecución y control de los recursos públicos.

El sistema comprende los siguientes módulos funcionales: planeación institucional, control y ejecución del gasto, gestión de ingresos, administración de contratos, gestión financiera y presupuestal, gestión del talento humano, y control de bienes y activos.

Dada su criticidad operativa y su papel en el soporte de los procesos estratégicos del Instituto, el sistema GOOBI GRP fue objeto de revisión técnica y normativa conforme a los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI), establecidos en la Resolución 500 de 2021 y la Resolución 002277 de 2025 del MinTIC, el Decreto 620 de 2020, la normativa vigente en materia de protección de datos personales, el Marco de Interoperabilidad del Estado colombiano, y los estándares internacionales ISO/IEC 27001:2022, ISO/IEC 27005:2022 e ISO/IEC 22301:2019. Esta evaluación se enfocó en verificar el cumplimiento de los principios fundamentales de confidencialidad, integridad y disponibilidad (CID), esenciales para asegurar la seguridad, trazabilidad y confiabilidad de la información procesada en los sistemas administrativos y financieros del IPES.

2. OBJETIVO GENERAL

Realizar evaluación y emitir una opinión independiente sobre el adecuado diseño y ejecución de los controles establecidos para prevenir y mitigar los riesgos existentes en la ejecución de los procesos determinados en el alcance del trabajo realizado referente a: Evaluar la gestión realizada por el proceso Gestión de la Información y de los Recursos Tecnológicos del Instituto para la Economía Social - IPES, principalmente la implementación del **Modelo de Seguridad y Privacidad de la Información (MSPI)** como habilitador de la Política de Gobierno Digital, en el marco del Modelo Integrado de Planeación y Gestión (MIPG), conforme a los lineamientos establecidos por el MinTIC.

2.1 OBJETIVOS ESPECÍFICOS

2.1.1. Analizar la herramienta **HEMI** del Instituto para la Economía Social (IPES) con el fin de identificar oportunidades de mejora en relación con los principios de confidencialidad, integridad y disponibilidad de la información, conforme a la norma ISO/IEC 27001:2022 y al Modelo de Seguridad y Privacidad de la Información (MSPI) definido por el MinTIC. Esta evaluación pretende identificar las posibles vulnerabilidades que puedan afectar los activos de información administrados por la plataforma, valorar la efectividad de los controles existentes y recomendar acciones orientadas a fortalecer el sistema de gestión de seguridad de la información institucional, en cumplimiento de las disposiciones de la Resolución 00500 de 2021 y la Resolución 002277 de 2025 del MinTIC.

2.1.2. Analizar la herramienta **GOOBI** del Instituto para la Economía Social (IPES) con el propósito de identificar oportunidades de mejora en torno a los principios de confidencialidad, integridad y disponibilidad (CIA) de la información, en concordancia con la norma ISO/IEC 27001:2022 y el Modelo de Seguridad y Privacidad de la Información (MSPI) definido por el MinTIC. Esta evaluación tiene como fin identificar posibles vulnerabilidades que puedan afectar la protección de los datos administrados por la plataforma, evaluar la efectividad de los controles de seguridad implementados (organizacionales, físicos y tecnológicos) y formular recomendaciones orientadas a fortalecer su gestión, de acuerdo con las mejores prácticas internacionales (ISO/IEC 27002 e ISO/IEC 27005) y lo dispuesto en la Resolución 00500 de 2021 y la Resolución 002277 de 2025 del MinTIC.

2.1.3. Verificar el grado de cumplimiento de las actividades orientadas a garantizar la continuidad de la seguridad de la información en el Instituto para la Economía Social – IPES, con base en los lineamientos establecidos en el procedimiento ***PA03-PD-009 V2 - Implementación de la Continuidad de la Seguridad de la Información***, las disposiciones de la *Resolución 00500 de 2021 y la Resolución 002277 de 2025 del MinTIC*, y las buenas prácticas definidas en la norma *ISO 22301:2019, relacionada con los Sistemas de Gestión de Continuidad del Negocio (SGCN)*. Esta verificación tiene como propósito evaluar la existencia y efectividad de los controles implementados para mitigar riesgos que puedan afectar la *disponibilidad, integridad y confidencialidad de la información*, así como su recuperación ante eventos disruptivos, garantizando la resiliencia operativa y el cumplimiento de los objetivos estratégicos del IPES.

2.1.4. Verificar el cumplimiento integral de las actividades ejecutadas por el proceso Gestión de la Información y de los Recursos Tecnológicos del IPES, en el marco de la gestión del ***Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – vigencia 2024***, con el propósito de identificar incidentes

de seguridad, vulnerabilidades no gestionadas y posibles escenarios de exposición a ciberataques que puedan comprometer la confidencialidad, integridad y disponibilidad de los activos de información de los diferentes procesos institucionales. Esta verificación se realizará conforme a los lineamientos establecidos en la *Resolución 500 de 2021 del MinTIC, la norma ISO/IEC 27005:2022 sobre gestión de riesgos de seguridad de la información y los principios definidos en el Modelo de Seguridad y Privacidad de la Información (MSPI)*, con el fin de evaluar la eficacia de los controles implementados y proponer acciones de mejora para fortalecer la postura de seguridad de la Entidad.

3. ALCANCE

El alcance se definió para el proceso Gestión de la Información y de los Recursos Tecnológicos, como responsable de la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), desde el periodo comprendido entre el 01 de enero 2024 al 31 de marzo 2025 en el Instituto para la Economía Social - IPES, teniendo en cuenta los manuales, instructivos y procedimientos del proceso, como la verificación de la seguridad de los sistemas de información HEMI – GOOBI.

El Alcance se determinó como resultado de un análisis de:

- Procesos críticos de relevancia según tamaño del Impacto de Riesgo.
- Nivel de Criticidad (*procesos sin identificación de riegos, carencia de controles, alta rotación de personal, cambio de funciones, procedimientos, eventos recientes, SDQS, etc*.)
- Exposición a eventos externos e internos del Instituto.
- Criterio profesional de los auditores aprobado por la Asesoría de Control Interno.
- Disponibilidad de recurso humano, técnico, financiero, etc.

En este contexto, la auditoría comprendió la verificación del cumplimiento de los procedimientos, manuales y planes relacionados con la seguridad de la información adoptados por el Instituto, los cuales se presentan a continuación. Esta validación tuvo como finalidad evaluar el grado de cumplimiento normativo y la coherencia con las directrices establecidas en la Resolución 00500 de 2021 y la Resolución 002277 de 2025 del MinTIC, en el marco del proceso de adopción e implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) por parte del Proceso de Gestión de la Información y de los Recursos Tecnológicos del IPES, correspondiente a la vigencia 2024 y al primer cuatrimestre de 2025:

Proceso GIRT
Gestión de la Información de los Recursos Tecnológicos

N°	CÓDIGO	DOCUMENTACIÓN VIGENTE	VERSIÓN	FECHA
1	PA03-MN-001	Manual del Sistema de Gestión de Seguridad y Privacidad de la Información	V5	04/02/2024
2	PA03-MN-002	Manual de Usuario Herramienta Misional (HEMI) 2024	V3	07/06/2024
3	PA03-MN-003	Manual Técnico Herramienta Misional (HEMI) 2024	V3	07/06/2024
4	PA03-MN-006	Manual Gestión (Creación, Eliminación O Modificación) de Cuentas de Usuario en el Directorio Activo 2024	V1	20/06/2024
5	PA03-PD-009	Implementación de la Continuidad de la Seguridad de la Información 2022	V2	29/11/2022
6	N/A	Resolucion No 025 de 2024 Actualización PETI 2024 PlanesTI	N/A	31/01/2024
7	PA03-DE-007	Plan Tratamiento de Riesgo Seguridad y Privacidad de la Informacion 2024	V7	28/01/2023
8	PA03-DE-006	Plan Estrategico de Tecnologias de Informacion PETI 2024-2028 – Actualización 2024	V7	28/01/2024
9	PA03-DE-006	Plan De Seguridad Y Privacidad De La Información 2024	V7	28/01/2024
10	PA03-DE-005	Plan Estrategico de Tecnologias de Informacion PETI 2024-2028 – Actualización 2025	V6	31/01/2025
11	PA03-DE-006	Plan De Seguridad Y Privacidad De La Información 2025	V8	31/01/2025
12	PA03-DE-008	Plan Tratamiento de Riesgo Seguridad y Privacidad de la Informacion 2025	V8	31/01/2025

4. LIMITACIÓN AL ALCANCE

Durante la ejecución de la auditoría no se presentaron retrasos en los requerimientos ni en las revisiones realizadas que afectaran la ejecución de esta.

5. CONFORMACIÓN EQUIPO DE TRABAJO DE AUDITORÍA

Asesor de Control Interno

Andrés Méndez Jiménez

Auditor(a) Responsable de la Auditoría MSPI

Sergio Andrés Castro Londoño
Ingeniero de Sistemas de Información, Especialista en Telecomunicaciones, Especialista en Inteligencia de Negocios (BI), Magíster en Tecnologías de la Información y las Comunicaciones (MTIC).

6. FORTALEZAS

- Se reconoce al proceso Gestión de la Información y de los Recursos Tecnológicos, el esfuerzo, la constancia y dedicación en adelantar actividades de adopción de lineamientos del modelo, alcanzando el **38.054%** de cumplimiento de las actividades del MSPI
- Se resalta la disposición, responsabilidad y compromiso de parte de los miembros del proceso de Gestión de la Información y de los Recursos Tecnológicos en la ejecución de las diferentes actividades propuestas, así como el acompañamiento en todas las reuniones realizadas para aclarar dudas e inquietudes frente a los requerimientos del auditoria MSPI.
- Se reconoce el compromiso, el sentido de pertenencia y el esfuerzo del equipo del Proceso de Gestión de la Información y de los Recursos Tecnológicos en la formulación y desarrollo de artefactos, planes estratégicos de tecnologías de la información y acciones orientadas al fortalecimiento de la seguridad de la información. Del mismo modo, se destacan los avances parciales alcanzados en la ejecución de estas iniciativas, reflejados en actividades encaminadas al cumplimiento de las metas y resultados definidos en el Anexo 1 de la Resolución 500 de 2021 y en las disposiciones de la Resolución 002277 de 2025 del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), dentro del proceso de adopción e implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) correspondiente a la vigencia 2024 y al primer cuatrimestre de 2025.

7. CONTEXTO AUDITORÍA

En cumplimiento del Plan Anual de Auditoría 2025 aprobado por el Comité Institucional de Coordinación de Control Interno-CICCI, la Asesoría de Control Interno del IPES programó una auditoría interna regular para evaluar la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI). Esta acción se enmarca en el habilitador "Seguridad de la Información" del Modelo Integrado de Planeación y Gestión (MIPG) y en lo dispuesto por la Política de Gobierno Digital del MinTIC.

El MSPI exige a las entidades públicas adoptar medidas que garanticen la protección de los activos de información bajo los principios de confidencialidad, integridad, disponibilidad y privacidad, conforme a las Resoluciones 500 de 2021 y 2277 de 2025 del MinTIC, el Decreto 767 de 2022 y estándares internacionales como las normas ISO/IEC 27001, 27005 y 22301.

La auditoría tuvo como objetivo evaluar el cumplimiento de metas, productos y resultados en cada fase del ciclo del MSPI (diagnóstico, planeación, implementación, evaluación del desempeño y mejora continua), verificando la eficacia de los artefactos técnicos y controles implementados, así como la identificación de riesgos, brechas normativas y oportunidades de mejora.

Se priorizó el análisis de los sistemas HEMI (herramienta misional) y GOOBI ERP (gestión administrativa y financiera), dada su relevancia en la administración de información sensible. En HEMI, se identificaron debilidades en materia de seguridad de la información que pueden llegar comprometer los principios de confidencialidad, integridad y disponibilidad (CID).

En GOOBI ERP se evidenció la ausencia de mecanismos seguros de interoperabilidad, situación que podría afectar la disponibilidad, trazabilidad y protección de la información, así como exponer a la entidad a riesgos de incumplimiento normativo y a posibles vulnerabilidades operativas.

Desde un enfoque técnico y jurídico, se concluyó que los procesos manuales y la falta de integración segura limitaban la eficacia del sistema de gestión de seguridad de la información. En este sentido, se recomendó avanzar hacia esquemas de interoperabilidad técnica automatizada con el apoyo de entidades como MinTIC y la Alta Consejería TIC, evaluando el uso de plataformas como X-Road u otras soluciones equivalentes, en coherencia con el MSPI y la norma ISO/IEC 27001:2022.

Finalmente, se realizaron pruebas de recorrido para validar las actividades ejecutadas por el Proceso de Gestión de la Información y de los Recursos Tecnológicos, en relación con el cumplimiento del procedimiento PA03-PD-009 Implementación de la Continuidad de la Seguridad de la Información V2 del 29/11/2022 y la ejecución del PA03-DE-007 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2024 V2 del 28/01/2023.

7.1. MARCO NORMATIVO

Se procedió a realizar un análisis de la normatividad externa asociada al Modelo de Seguridad y Privacidad de la Información (MSPI), llevada a cabo por el IPES:

Normatividad Auditoría MSPI 2025

N°	NORMATIVIDAD MSPI
1	Decreto No 767 2022 - Politica de Gobierno Digital
2	Decreto No 338 de 2022 - DAFP – MinTIC
3	Resolución No 500 del 2021 (MSPI)v1 – MinTIC (Anexo 1)
4	Resolución No 746 del 2022 (MSPI)v2 – MinTIC (Anexo 2)
5	Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas - V6 del Departamento Administrativo de la Función Pública
6	○ ISO/IEC 27001:2022 es la norma internacional más reconocida para la gestión de la seguridad de la información. Establece los requisitos para implementar, mantener y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información (SGSI) dentro de una organización, con el objetivo de proteger la confidencialidad, integridad y disponibilidad de la información. ○ ISO/IEC 27005:2022 es un estándar internacional que proporciona directrices para la gestión de riesgos de seguridad de la información, dentro del marco de un Sistema de Gestión de Seguridad de la Información (SGSI), conforme a la norma ISO/IEC 27001 ○ ISO/IEC 22301:2019 es la norma internacional que establece los requisitos para un Sistema de Gestión de la Continuidad del Negocio (SGCN). Su objetivo es garantizar que una organización pueda continuar operando durante y después de una interrupción, como desastres naturales, ciberataques, fallos tecnológicos o crisis sanitarias. (SGCN)
7	CONPES 3975 de 2019 - Política Nacional para la Transformación Digital e Inteligencia Artificial
8	CONPES 3854 de 2016 - Política Nacional de Seguridad Digital
9	CONPES 3995 de 2020 - Política Nacional de Confianza y Seguridad Digital
10	Ley 1712 de 2014 - Ley de transparencia y acceso a la información publica

N°	NORMATIVIDAD MSPI
11	Resolución No 02277 del 03 de Junio del 2025 MinTIC - MSPI 2025 - Lineamientos 2025: 1. Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información MSPI 2. Roles y Responsabilidades 3. Indicadores de Gestión de Seguridad de la Información 4. Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional 5. Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas

8. RESUMEN DE RESULTADOS DE LA AUDITORÍA

En el marco de la Auditoría Interna Regular sobre la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en el Instituto para la Economía Social (IPES), la cual fue realizada al proceso Gestión de la Información y de los Recursos Tecnológicos, se determinaron **5 observaciones** que se detallan de manera general con la posible incidencia en seguridad, operación, administrativa y disciplinaria:

Núm	Observación	Situación	Potencial impacto				
			Seguridad (CID)	Funcionamiento Operación	Administrativo	Disciplinario	Fiscal
1	Bajo avance en la implementación del MSPI y brechas significativas frente a los lineamientos normativos y estándares de seguridad de la información en el IPES, en concordancia con las disposiciones dadas en las Resoluciones 500 de 2021 y 2277 de 2025, el Decreto 767 de 2022, así como con los estándares internacionales ISO/IEC 27001, 27005 y 22301.	Durante la auditoría al Modelo de Seguridad y Privacidad de la Información (MSPI) en el Instituto para la Economía Social – IPES, se evidenció un avance global del **38.054%** en su ciclo de operación, con base en la evaluación realizada por la ACI mediante un instrumento de medición que adoptó las directrices del Anexo 1 de la Resolución 500 de 2021 del MinTIC, documentado en el papel de trabajo MSPI 2025. Este avance se concentró principalmente en las fases de diagnóstico y planificación. No obstante, se identificó una ausencia de progresos significativos en las fases de implementación, evaluación del desempeño y mejora continua, lo que evidenció el incumplimiento de las metas programadas para la vigencia 2024 – primer cuatrimestre de 2025 y limitó el logro de los resultados esperados para la adopción efectiva del modelo. Estas situaciones fueron detectadas durante la verificación de los 19	X	X	X		

		requerimientos establecidos en la solicitud de información formalizada mediante el Memorando No. 10-817-2025-001363. El diagnóstico realizado permitió identificar brechas relevantes en la adopción de los lineamientos normativos definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), en concordancia con las Resoluciones 500 de 2021 y 2277 de 2025, el Decreto 767 de 2022, así como con los estándares internacionales ISO/IEC 27001, 27005 y 22301. Las debilidades identificadas pudieron afectar la efectividad del Sistema de Gestión de Seguridad de la Información (SGSI) institucional y evidenciaron la necesidad de implementar medidas correctivas y acciones de mejora para garantizar el cumplimiento normativo, mitigar los riesgos de seguridad digital y fortalecer la capacidad operativa del Instituto frente a los desafíos del entorno tecnológico de ese momento.					

2	Debilidades en materia de seguridad de la información y gestión tecnológica de la herramienta HEMI, que pueden llegar comprometer los principios de confidencialidad, integridad y disponibilidad (CID).	Durante la auditoría realizada a la herramienta misional HEMI del Instituto para la Economía Social – IPES, se identificaron debilidades en la confidencialidad, integridad y disponibilidad de la información, las cuales pudieron comprometer la seguridad de la información institucional. En primer lugar, se evidenció la ausencia de mecanismos automatizados y seguros de interoperabilidad para el intercambio de información entre ANI/RNEC y el IPES, situación que contravenía el Marco de Interoperabilidad del Ministerio TIC y las disposiciones del Decreto 620 de 2020, particularmente en lo relacionado con la implementación de servicios ciudadanos digitales y del Modelo de Seguridad y Privacidad de la Información (MSPI). Esta limitación puede exponer a la entidad a posibles riesgos operacionales y de integridad de la información, derivados del uso de procesos manuales sin trazabilidad ni controles técnicos efectivos, con dependencia exclusiva de acuerdos de confidencialidad como único mecanismo de control jurídico sobre el tratamiento de información sensible, sin el acompañamiento de integraciones	X	X	X		

		técnicas que puedan garantizar la trazabilidad, integridad y seguridad de los datos sensibles en tránsito. Esta situación reflejó una débil alineación con los estándares internacionales en materia de ciberseguridad (ISO/IEC 27001:2022), continuidad del negocio (ISO 22301:2019), el Marco de Interoperabilidad del MinTIC y el MSPI, con la posibilidad de generar riesgos tecnológicos, operacionales, legales y reputacionales de alto impacto, que requieren atención prioritaria por parte de la entidad. Por lo anterior, **se recomienda** al proceso adelantar las gestiones pertinentes, tanto en el ámbito jurídico como técnico, ante la Secretaría General – Alcaldía Mayor de Bogotá, la Alta Consejería Distrital TIC, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y la Agencia Nacional Digital, con el fin de verificar la viabilidad normativa, técnica y operativa para establecer un intercambio seguro de información interinstitucional, ya sea mediante la implementación del componente de interoperabilidad X-Road o a través de otro mecanismo que garantice la confidencialidad, integridad, disponibilidad y trazabilidad					

		de la información, conforme al Modelo de Seguridad y Privacidad de la Información – MSPI y los lineamientos del marco de interoperabilidad del Estado colombiano. En segundo lugar, no se evidenció una infraestructura tecnológica con entornos redundantes que respaldaran la continuidad operativa frente a incidentes o fallas, lo que representó un incumplimiento frente a los lineamientos de la norma ISO/IEC 22301:2019 y del control A.5.29 de la ISO/IEC 27001:2022, afectando la resiliencia de los servicios misionales. A esto se sumó la carencia de mecanismos de autenticación multifactor (2FA), lo cual contravenía el control A.8.2 “Autenticación del usuario” de la norma ISO/IEC 27001:2022 y amplió la superficie de riesgo ante accesos no autorizados, suplantación o ataques de fuerza bruta. Finalmente, se identificaron debilidades en la comprensión y uso de los tableros de control y reportes del sistema HEMI, tanto a nivel directivo como funcional, debido a la baja interactividad y limitada funcionalidad dinámica de la herramienta. Estas limitaciones					

		dificultaron la consolidación, interpretación y aprovechamiento de los datos disponibles, impidiendo la realización de análisis objetivos sobre el desempeño, uso y eficiencia del sistema. En consecuencia, se vio comprometida la capacidad institucional para monitorear indicadores, identificar patrones de gestión y tomar decisiones informadas. Se recomienda optimizar los reportes de la herramienta, transformándolos en reportes dinámicos y de fácil comprensión, así como incorporar estadísticas visuales que faciliten la interpretación de los datos del sistema relacionados con actividades, metas y resultados esperados. Esto permitirá visualizar métricas e indicadores que fortalezcan el seguimiento, control y la toma de decisiones.					

3	Se identificaron debilidades a nivel operativo en la gestión de accesos del sistema, reflejado en la falta de sincronización con el Directorio Activo y la ausencia de mecanismos de autenticación multifactor (2FA/MFA), así como en la inexistencia de procesos de interoperabilidad para el intercambio de información con otros sistemas internos y externos. Asimismo, se evidenció que la información que reposa en la herramienta GOOBI carece de servidores redundantes, lo que incrementa el riesgo de interrupciones en la continuidad del negocio y puede afectar los principios de confidencialidad, integridad y disponibilidad (CID) de la información.	Durante la prueba de recorrido realizada el 25 de junio del presente año, se identificaron debilidades a nivel de la operación de GOOBI, relacionadas con la gestión de accesos, usuarios, interoperabilidad, continuidad operativa y análisis de información, que comprometen los principios de confidencialidad, integridad y disponibilidad. Se evidenció la ausencia de autenticación multifactor (2FA/MFA), una administración de usuarios no integrada con el Directorio Activo (AD), contraseñas gestionadas manualmente sin políticas de renovación, ni alertas de vencimiento, lo que limita el control centralizado y la trazabilidad de identidades. Asimismo, el sistema carece de mecanismos estandarizados de interoperabilidad con plataformas institucionales y externas, incumpliendo los lineamientos de la Política de Gobierno Digital y del Marco de Interoperabilidad. Se identificó la falta de un servidor espejo o soluciones de alta disponibilidad, lo que incrementa el riesgo de interrupción de servicios críticos. Adicionalmente, la herramienta no cuenta con tableros de control, reportes dinámicos ni métricas de satisfacción que permitan evaluar el desempeño, la usabilidad y la eficiencia	X	X	X		

		del sistema. Estas condiciones evidencian una brecha frente a las buenas prácticas establecidas en la ISO/IEC 27001:2022, la ISO 22301:2019 y el MSPI del MinTIC, exponiendo al Instituto para la Economía Social (IPES) a riesgos operacionales, tecnológicos, reputacionales y de incumplimiento normativo.					

4	Debilidades en el cumplimiento de las actividades del procedimiento PA03-PD-009 V2 para garantizar la continuidad de la seguridad de la información en el Instituto para la Economía Social – IPES.	Se identificaron debilidades críticas en la gestión de la continuidad de la seguridad de la información, especialmente frente a situaciones de contingencia que comprometen la operatividad institucional. Si bien se evidenció la activación del Plan de Continuidad del Negocio (PCN) tras un incidente de seguridad relacionado con un ataque tipo ransomware, detectado por la herramienta de monitoreo Darktrace Network y reportado en el Comité de Seguridad del 3 de marzo de 2025, no se encontró evidencia de una estrategia formal de continuidad de la seguridad de la información debidamente documentada, desplegada ni evaluada posterior a la contingencia, ni se presentó un informe técnico sobre la eficacia de los controles implementados durante el evento. Adicionalmente, los informes posteriores al comité documentaron amenazas perimetrales detectadas por el firewall Fortinet y alertas de seguridad generadas por soluciones como Kaspersky; sin embargo, no se materializaron riesgos sobre los activos evaluados ni impactos en los sistemas institucionales, lo que evidencia una respuesta institucional reactiva y no	X	X	X		

		preventiva, sin mecanismos formales de análisis post-incidente, pruebas de controles ni procesos de mejora continua. En la prueba de recorrido realizada al procedimiento PA03-PD-009 V2 se constató que el inventario de activos de información no ha sido actualizado para las vigencias 2024-2025, manteniéndose únicamente el correspondiente al año 2023. Esta situación limita la capacidad del Instituto para identificar riesgos actuales, establecer controles efectivos y garantizar los principios de confidencialidad, integridad y disponibilidad de la información, en contravía de los lineamientos de la norma ISO/IEC 27001:2022. Aunque en la réplica al informe preliminar el proceso manifestó haber publicado los activos de información con corte a 2025 en el enlace de transparencia, no se aportaron evidencias ni soportes, tanto en la prueba de recorrido como en la documentación de réplica, que acrediten la gestión realizada con cada proceso, área o dependencia en relación con la identificación, clasificación de activos y determinación de riesgos asociados a la seguridad					

		informática, de la información y digital durante las vigencias 2024 y 2025. Asimismo, aunque se cuenta con una matriz de riesgos de seguridad de la información, no se evidencian riesgos digitales actualizados ni una gestión integral que refleje las amenazas reales reportadas por el proceso en actas, informes o comités, observándose una falta de trazabilidad entre los incidentes detectados y la actualización de los planes de tratamiento, lo cual refleja una desconexión entre la operación diaria y la gestión estratégica de la seguridad de la información. También se evidenció la ausencia de nuevos controles técnicos implementados durante el período auditado, lo que imposibilita la evaluación de la efectividad de medidas preventivas y limita la capacidad institucional para demostrar avances en la mejora continua, exigida por la norma ISO/IEC 27001:2022 y el Modelo de Seguridad y Privacidad de la Información (MSPI). Finalmente, se observó la carencia de infraestructura redundante o servidores espejos que respalden el funcionamiento de sistemas críticos, vulnerabilidad que se materializó durante el reciente traslado de sede institucional, en el cual la falta de					

		mecanismos de alta disponibilidad impidió la continuidad de los servicios, afectando directamente la operatividad del Instituto durante el cierre de junio y la primera semana de julio de 2025, situación que contraviene lo dispuesto en la norma ISO 22301:2019 sobre Sistemas de Gestión de Continuidad del Negocio y en el procedimiento PA03-PD-009 V2 del IPES, que exigen validar y mantener capacidades de recuperación frente a eventos disruptivos.					

5	Se identificaron deficiencias en la ejecución del Plan de Gestión de Riesgos de Seguridad y Privacidad de la Información, específicamente en el seguimiento y monitoreo de los indicadores establecidos en el documento **PA03-DE-007-V7 – Plan de Tratamiento de Riesgo 2024**, lo que evidencia una gestión parcial e insuficiente de las actividades previstas para mitigar y controlar los riesgos identificados.	Se evidencian debilidades significativas en el proceso de identificación, clasificación, valoración y tratamiento de los riesgos de seguridad informática, seguridad de la información y seguridad digital en el Instituto para la Economía Social (IPES), derivadas de la gestión ineficiente, desactualizada y poco articulada de los activos de información institucionales para el periodo 2024-2025, insumo esencial según la Guía de Administración del Riesgo del DAFP. Durante la auditoría se constató que, a pesar de la existencia de actividades de sensibilización, no se realizó seguimiento a los planes de TI conforme al Decreto 612 de 2018 en el segundo semestre de 2024; tampoco se halló evidencia documental que respalde la aprobación formal de los mapas de riesgos correspondientes al tránsito entre las vigencias 2023 y 2024, ni la validación por parte de los comités competentes (CICCI y/o Comité de Gestión y Desempeño Institucional), lo cual representa un incumplimiento de la Política de Riesgos del IPES. Aunque se identificaron matrices de riesgo formuladas para 2024, no se	X	X	X		

		encontró el documento de aceptación de riesgos residuales ni el acto administrativo que formalice el Plan de Tratamiento de Riesgos, en contravía de la norma ISO/IEC 27001:2022 y el Modelo Integrado de Planeación y Gestión (MIPG). Si bien se publicó el informe de seguimiento en el portal institucional conforme a la Ley 1712 de 2014, la ausencia de riesgos materializados durante la vigencia impidió evaluar la efectividad de los controles implementados o proponer mejoras derivadas de incidentes o simulacros. Finalmente, se evidenció la falta de seguimiento a los indicadores del plan de tratamiento de riesgos, lo cual compromete la trazabilidad de las acciones, debilita la verificación del cumplimiento de los objetivos estratégicos del proceso y afecta negativamente la mejora continua del sistema de gestión de seguridad de la información del Instituto.					

9. DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍA

A continuación se presentarán las observaciones encontradas como resultado del ejercicio de auditoria las cuales se describirán de manera detallada:

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES
Nombre del Proceso: Gestión de la Información y de los Recursos Tecnológicos
Auditoría Modelo de Seguridad y Privacidad de la Información (MSPI) IPES 2024-2025
***Auditor:* Sergio Andrés Castro Londoño**
***Ver Anexo 1* - Papel de Trabajo MSPI - IPES 2025.xlsx**

OBSERVACIÓN NO.1

Bajo avance en la implementación del MSPI y brechas significativas frente a los lineamientos normativos y estándares de seguridad de la información en el IPES, en concordancia con las disposiciones dadas en las Resoluciones 500 de 2021 y 2277 de 2025, el Decreto 767 de 2022, así como con los estándares internacionales ISO/IEC 27001, 27005 y 22301.

Situación(es):

Durante la auditoría al Modelo de Seguridad y Privacidad de la Información (MSPI) en el Instituto para la Economía Social – IPES, se evidenció un avance global del **38.054%** en su ciclo de operación, concentrado principalmente en las fases de diagnóstico y planificación. Sin embargo, se observó una falta de progresos significativos en las fases de implementación, evaluación del desempeño y mejora continua, lo que evidencia el incumplimiento de las metas programadas para la vigencia 2024 – primer cuatrimestre de 2025 y limita el logro de los resultados esperados para la adopción efectiva del modelo.

Estas situaciones fueron detectadas durante la verificación de los 19 requerimientos establecidos en la solicitud de información formalizada mediante el Memorando No. 10-817-2025-001363. El diagnóstico realizado permitió identificar brechas en la adopción de los lineamientos normativos definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), en concordancia con las Resoluciones 500 de 2021 y 2277 de 2025, el Decreto 767 de 2022, así como con los estándares internacionales ISO/IEC 27001, 27005 y 22301.

Las debilidades encontradas afectan la efectividad del Sistema de Gestión de Seguridad de la Información (SGSI) institucional y evidencian la necesidad de implementar medidas correctivas y acciones de mejora para garantizar el cumplimiento normativo, mitigar riesgos de seguridad digital y fortalecer la capacidad operativa del Instituto frente a los desafíos del entorno tecnológico actual.

Como soporte de este análisis, se anexa el archivo *Papel de Trabajo MSPI - IPES 2025.xlsx*, que contiene el detalle de las observaciones derivadas del análisis de las evidencias documentales presentadas por el proceso auditado.

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES

Causa(s):

Se evidenciaron debilidades en los procesos de adopción e implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), en contravía de lo dispuesto en los *Artículos No. 3, 4, 5, 6 y 15 de la Resolución 500 de 2021 y lo establecido en la Resolución 002277 de 2025.* Esta situación podría estar relacionada con el presunto desconocimiento o la falta de comprensión técnica u omisión o falta de recursos para desarrollar las actividades (productos y entregables) , alcanzar las metas y resultados esperados, los cuales se encuentran establecidas en el ciclo de operación PHVA del MSPI, requeridos en cada fase del modelo, lo que limita su correcta ejecución.

Una de las principales causas identificadas corresponde a la débil articulación entre las áreas responsables de los activos de información, ya que no existe un proceso coordinado entre las dependencias de tecnología, gestión documental, talento humano, seguridad informática y procesos misionales para alimentar y mantener actualizado el inventario institucional. Esta situación se ve agravada por la ausencia de procedimientos documentados y sistemáticos que definan la periodicidad, los responsables, los validadores y los mecanismos de verificación necesarios para asegurar la calidad del inventario. Adicionalmente, se evidencian limitaciones en la asignación de recursos humanos y tecnológicos, reflejadas en la falta de personal técnico especializado y de herramientas que permitan automatizar o centralizar el levantamiento y control de activos. A esto se suma el desconocimiento o la baja capacitación del personal frente a los requerimientos normativos establecidos en el Modelo de Seguridad y Privacidad de la Información – MSPI, lo cual dificulta su adecuada implementación y sostenibilidad.

Consecuencia(s):

Posibles consecuencias o efectos de las situaciones observadas:

a) Riesgo de materialización de incidentes de seguridad por ausencia de controles implementados ISO 27001:2022 y procesos de evaluación, que pueden dejar expuestos los activos de información del IPES a ciberataques, accesos no autorizados, pérdida o modificación de datos críticos.
b) El estancamiento en la implementación de las fases del Modelo de Seguridad y Privacidad de la Información (MSPI) constituye un incumplimiento normativo que transgrede lo establecido en la Resolución 500 de 2021 y el Decreto 767 de 2022 emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Esta situación expone al Instituto a posibles hallazgos en auditorías externas, así como a eventuales requerimientos de entes de control o sanciones administrativas por inobservancia de las disposiciones legales en materia de seguridad de la información.
c) Pérdida de confianza institucional por la falta de un sistema robusto de seguridad de la información puede afectar la percepción de confianza de ciudadanos, beneficiarios, entidades distritales y órganos de control sobre la gestión de datos del IPES.
d) Debilidades en la continuidad operativa por la no implementación de la fase de mejora y evaluación del desempeño compromete la

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES

capacidad del IPES para reaccionar ante incidentes, recuperarse ante fallos y garantizar la disponibilidad de los servicios.

e) Desalineación con la Política de Gobierno Digital, por el bajo nivel de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

f) Falta de trazabilidad y evidencias sobre el cumplimiento de los procesos de implementación del MSPI, debido a la inexistencia de reportes y tableros de control, que permitan visualizar las métricas, indicadores y avances del MSPI, ante entes de control, en el cumplimiento efectivo de las acciones en seguridad y privacidad de la información.

Riesgo(s) Asociado(s):

Error humano y acceso inadecuado (eliminación, alteración, corrupción, mala gestión), por no adoptar los lineamientos generales del MSPI, según las disposiciones dadas en la Resolución No 500 del 2021 de MinTIC, con la posible afectación de la confidencialidad, integridad y disponibilidad de la información de acuerdo con:

a) Disponibilidad - Perdida de disponibilidad de la infraestructura que soporta los servicios y activos de información de TI.
b) Integridad - Perdida de Integridad de la información digital almacenada, procesada y manejada en los sistemas de información misional y administrativos.
c) Confidencialidad - Perdida de confidencialidad de: la información digital almacenada, procesada y manejada en los sistemas de información misional y administrativos; y la información del proceso PGSIRT.

Probabilidad de Compartir información de aplicativos y sistemas de información con entidades externas permitiendo acceso a código e información

Estos son errores que causamos y el acceso inadecuado puede provocar accidentes como alteración o eliminación. Esto es algo que puede resultar perjudicial al considerar cuestiones de cumplimiento y protección de datos. Es importante controlar el acceso al contenido internamente, no solo externamente, para prevenir errores humanos y violaciones de cumplimiento."…

Riesgo(s) Identificado(s) en el ejercicio de auditoria:

Exposición a incidentes de seguridad y brechas de confidencialidad, integridad y disponibilidad de la información institucional debido a la falta de implementación y evaluación de controles críticos del MSPI, lo que podría resultar en pérdidas de datos sensibles, interrupciones operativas y sanciones regulatorias.

Normatividad o Criterio:

- MSPI MinTIC - 29/07/2016
- Decreto 767 de 2022 - Política de Gobierno Digital
- Decreto 338 de 2022 - Seguridad Digital MinTIC
- Resolución No 500 del 2021 (MSPI)v1 – MinTIC

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES

- Anexo 1 - Resolución No 500 de 2021 (MSPI)
- Resolución No 746 del 2022 (MSPI)v2 – MinTIC
- Anexo 2 - Resolución No 746 de 2022 (MSPI)
- Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas - MNGRSI (Anexo 4 - DAFP)
- SO 27001:2022
- ISO 27005:2022
- ISO 22301:2019
- Resolución No 02277 del 03 de junio del 2025 MinTIC - MSPI 2025 - Lineamientos 2025:
  a) Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información MSPI
  b) Roles y Responsabilidades
  c) Indicadores de Gestión de Seguridad de la Información
  d) Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional
  e) Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas

Connotación:

Probabilidad de impacto negativo por las posibles vulnerabilidades que puedan afectar los principios CID de la seguridad informática, seguridad de la información, seguridad digital del Instituto, con la posible incidencia operativa, administrativa, disciplinaria y/o fiscal.

Recomendación

Se recomienda a la al proceso Gestión de la Información y de los Recursos Tecnológicos del Instituto para la Economía Social – IPES adoptar e implementar de manera prioritaria un plan de acción integral para avanzar en las fases de implementación, evaluación del desempeño y mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI), con base en los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) en las Resoluciones 500 de 2021 y 2277 de 2025, el Decreto 767 de 2022, y los estándares internacionales ISO/IEC 27001:2022, 27005:2022 y 22301:2022.

Valoración Comentarios del Auditado

Mediante Memorando con radicado número 10-817-2025-002245 del 21 de julio del 2025, la Subdirección de Diseño y Análisis Estratégico-SDAE, manifiesta lo siguiente**:**

a) Se anexa informes técnicos derivados de pruebas de vulnerabilidades sobre el sitio web institucional.
b) En el ajuste de la resolución 492 del 2021 que está en revisión por parte del área jurídica, se encuentra un parágrafo de los roles a cumplir sobre el esquema de los roles de seguridad de la información en lo correspondiente a la parte directiva, al grupo operativo, al grupo técnico y al grupo de seguridad de la información.

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES
c) De conformidad a la información publicada en la página web de la entidad en la sección de Transparencia numeral 7.1.1 Registro de activos de información, se encuentra la información correspondiente, la información presento cambios emitidos para su correspondiente publicación, por lo anterior para realizar la subsanación en tiempo se enviará el documento actualizado al área de comunicaciones para su modificar la fecha *d) La identificación, evaluación y gestión de riesgos de seguridad de los activos de información del IPES y de los servicios de TI, tanto para la vigencia 2024 y especialmente la de 2025, se encuentran referidos en la matriz de riesgos de la gestión del proceso, que se encuentran publicadas por ley de transparencia en el siguiente link:* ***https://www.ipes.gov.co/index.php/4-3-plan-de-accion/mapa-de-riesgos-de-procesos*** *e) Dos (2) charlas realizadas en 2024, 2025 en ciberseguridad con temas generales de seguridad informática, de información y digital.* *f) El documento correspondiente la fase de Planeación, implementación y pruebas de funcionamiento, el cual se encuentra registrado en el reporte y en los archivos cargados en el portal del MinTIC. Tal como se evidencia en el micrositio de dicha entidad, así como las actividades realizadas a cada fase, se anexa captura de pantalla donde se indica que el IPES cumple con los lineamientos establecidos en materia de migración a IPv6.* *g) La observación no se acepta puesto que estamos en el cumplimiento base de la ISO 270001, en la cual se cumple con los requerimientos base los cuales se vinculan en el Plan Estratégico de Tecnologías de la Información, los cuales son aprobados en comité institucional de gestión y desempeño tal y como la dicta la norma, además la entidad no se encuentra certificada en ISO 270001 del 2022 y en la cual se está implementando y la entidad se encuentra dentro de los tiempos de migración.* *h) Implementación del plan de tratamiento de riesgos 2024: La identificación, evaluación y gestión de riesgos de seguridad de los activos de información del IPES y de los servicios de TI, tanto para la vigencia 2024 y especialmente la de 2025, se encuentran referidos en la matriz de riesgos de la gestión del proceso, que se encuentran publicadas por ley de transparencia en el siguientes link: https://www.ipes.gov.co/index.php/4-3-plan-de-accion/mapa-de-riesgos-de-procesos* *i) Plan de transición IPV6 – Documento Planeación e implementación IPV6.* *j) En el año 2024 se hizo reporte a la Alta Consejería de la Tics, como se muestra en el soporte, del Instrumento de autodiagnóstico del MSPI - junio 2024 y Gap de Protección de Datos Personales – junio 2024, para dar cumplimiento al seguimiento a la implementación del Habilitador de Seguridad y Privacidad de la Información de la Política de Seguridad Digital y los lineamientos en protección de datos personales que realiza la Oficina Consejería Distrital de TIC.* *k) El Plan Estratégico de Tecnologías de la Información, ha tenido seguimiento tanto en el año 2022, como en el año 2025, tal y como se muestran los soportes, los seguimientos son a través de indicadores que nos muestran la gestión dentro del mismo plan por lo cual su evaluación esta implícita dentro del mismo reporte. como evidencia se adjunta el seguimiento más reciente.*

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES

Análisis de la ACI:

Revisados los soportes aportados por el proceso en respuesta a la observación del informe preliminar, la Asesoría de Control Interno concluye lo siguiente:

a) Se reconoce la existencia de informes técnicos derivados de pruebas de vulnerabilidades sobre el sitio web institucional y valora la postura proactiva del proceso de Gestión de la Información de los Recursos Tecnológicos (GRTI) en la identificación de amenazas y vulnerabilidades mediante escaneos, migraciones tecnológicas, actualizaciones de manuales y medidas de protección perimetral. Sin embargo, se evidencia una limitada formalización documental y trazabilidad de los resultados de los análisis técnicos efectuados, así como la ausencia de una Oficina TIC formalmente estructurada y de la certificación ISO/IEC 27001:2022, lo que genera una brecha en la adopción sistemática de controles administrativos y técnicos que permitan una gestión integral y estandarizada de la seguridad de la información, incrementando el riesgo de que las acciones implementadas carezcan de un marco formal de auditoría, evaluación periódica y mejora continua del SGSI. Asimismo, se identifica que, aunque existen esfuerzos en protección perimetral y copias de seguridad, no se cuenta con un plan documentado y probado de respuesta a incidentes de ciberseguridad (con simulacros o escenarios controlados), ni con informes formales y periódicos de vulnerabilidades y pruebas de penetración que respalden los controles aplicados en cada entorno tecnológico, por lo que se recomienda estructurar un procedimiento formal para la gestión de vulnerabilidades alineado con normas internacionales como ISO/IEC 27001:2022, implementar un plan anual de pruebas de vulnerabilidad y penetración, diseñar y ejecutar un plan de respuesta a incidentes de ciberseguridad con ejercicios de simulación, avanzar en la formalización de la Oficina TIC y del SGSI orientado a la certificación, y generar informes técnicos periódicos que documenten hallazgos, riesgos y planes de mejora derivados de los análisis de seguridad realizados. **Por tal razón y conforme con los soportes presentados por el proceso auditado en la réplica, la observación cambia a estado no cumplido a estado parcial.**

b) De acuerdo con los soportes presentados por el proceso, se evidencia la proyección de un borrador del documento PA03-FO-020 V5 - Plantilla Resolución 492 Ajustes 18-12-2024, que contiene roles y responsabilidades en materia de seguridad y privacidad de la información. Sin embargo, dicho borrador no corresponde a un documento oficial del Instituto. **Por tal razón, la observación se mantiene.**

c) De acuerdo con los soportes presentados por el proceso, se confirma la publicación de los activos de información con corte a 2025 en el enlace de transparencia del Instituto. Sin embargo, durante la prueba de recorrido se presentaron únicamente los activos de información correspondientes a la vigencia 2023, sin acreditar la gestión realizada con cada proceso, área o dependencia respecto a la identificación, clasificación de activos y determinación de riesgos asociados a la seguridad informática, de la información y digital durante las vigencias 2024 y 2025. **Por tal razón, la observación se mantiene.**

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES
d) De acuerdo con los soportes aportados por el proceso, no se encontró evidencia documental que respalde la actualización, aprobación y formalización de los mapas de riesgos de gestión para el tránsito entre las vigencias 2023 y 2024. Aunque en el repositorio institucional (Suite Visión) se identificó el mapa de riesgos de 2023 y se presentó el acta del Comité de Seguridad del 12 de diciembre de 2023, donde se discutieron lineamientos para 2024, no se hallaron documentos que acrediten la validación ni la aprobación formal de los nuevos mapas de riesgos por parte de los comités competentes (CICCI y/o de Gestión y Desempeño Institucional), lo que representa una omisión frente a la gestión integral del riesgo y a los lineamientos de la Política de Riesgos del IPES. Si bien se realizaron actividades generales de sensibilización en seguridad de la información y ciberseguridad, no existe evidencia de aprobación formal de los riesgos actualizados ni de los controles definidos para su mitigación, lo que limita la eficacia del aseguramiento institucional. Además, aunque se identificaron matrices de riesgos para 2024, no se evidenció el documento de aceptación de riesgos residuales ni el acto administrativo o técnico que apruebe formalmente el Plan de Tratamiento de Riesgos, tal como lo exigen la norma ISO/IEC 27001:2022 y el Modelo Integrado de Planeación y Gestión (MIPG). **Por tal razón la observación se mantiene.**
e) De acuerdo con las evidencias aportadas por el proceso, se reconocen las capacitaciones de ciberseguridad realizadas durante la vigencia 2024; sin embargo, no se evidencia el diseño de un plan de comunicaciones que contemple la sensibilización y capacitación sobre la adopción e implementación del MSPI en el Instituto. Tampoco se observa la planeación ni socialización de documentos oficializados relacionados con políticas específicas de seguridad, planes estratégicos de seguridad 2025 y procedimientos de seguridad del IPES, en los que se definan el alcance del programa, roles y responsabilidades de quienes lo diseñan, desarrollan, implementan y mejoran, así como el material y las metas a cumplir. No se identifican audiencias objetivo, cursos obligatorios para el personal, temáticas por sesión o curso, métodos de capacitación, frecuencia de las actividades o escenarios en los que se requieran (como reinducciones o formación para personal nuevo). Además, no se presentan evidencias de documentación de cada actividad (incluyendo evaluaciones), ni de procesos de evaluación y actualización del material desarrollado. **Por tal razón, la observación se mantiene.**
f) De acuerdo con los soportes presentados por el proceso, se evidencia el reporte de cumplimiento del IPES en el micrositio del MinTIC – Trazabilidad, correspondiente al proceso de diagnóstico, planeación, implementación del protocolo IPV6, el cual se encuentra debidamente registrado tanto en el reporte como en los archivos cargados en el portal del MinTIC. **Por tal razón, se retira la observación.**
g) De acuerdo con la réplica, la cual no acepta la observación argumentando que se está cumpliendo con la ISO 27001 mediante los requerimientos base vinculados en el Plan Estratégico de Tecnologías de la Información, y considerando que la entidad no se encuentra certificada en la ISO/IEC 27001:2022, se aclara que la evaluación no se centra en el PETI, sino en el documento correspondiente a la fase de implementación del MSPI.

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES
Este documento debe establecer la estrategia de planificación y control operacional sobre cómo se desarrollará el modelo, así como contar con la revisión y aprobación de la Alta Dirección. La ausencia de este documento constituye un posible incumplimiento de lo dispuesto en el artículo 15 (Control de las actividades incluidas en la estrategia de seguridad digital y gestión de riesgos) de la Resolución No. 500 de 2021 del MinTIC, así como de las disposiciones de la Resolución 002277 de 2025 del MSPI, alineadas con la ISO/IEC 27001:2022. **Por lo tanto la observación se mantiene.**
h) De acuerdo con el PA03-DE-007-V7 “Plan Tratamiento de Riesgo Seguridad y Privacidad de la Información 2024”, se observaron debilidades en la identificación, clasificación y valoración de riesgos derivadas de deficiencias en la gestión, actualización y control de los activos de información (insumo base del análisis de riesgos) para 2024–2025. Esto impide una valoración exhaustiva de los riesgos que pueden afectar sistemas, datos sensibles e infraestructuras críticas del IPES y limita la definición de estrategias de mitigación adecuadas, incrementando la exposición a incidentes de seguridad. Asimismo, no existe evidencia documental de la actualización, validación, aprobación y formalización de los mapas de riesgos en el tránsito 2023–2024 por los comités competentes (CICCI y/o Comité de Gestión y Desempeño Institucional); tampoco se acreditan la aceptación de riesgos residuales ni el acto administrativo/técnico que apruebe formalmente el Plan de Tratamiento de Riesgos, como exigen la ISO/IEC 27001:2022 y el MIPG. **Por tal razón, la observación se mantiene.**
i) De acuerdo con los soportes presentados por el proceso, se evidencia el reporte de cumplimiento del IPES en el micrositio del MinTIC – Trazabilidad, correspondiente al proceso de transición del protocolo IPV6, el cual se encuentra debidamente registrado tanto en el reporte como en los archivos cargados en el portal del MinTIC. **Por tal razón, se retira la observación .**
j) De acuerdo con los soportes presentados por el proceso, en el año 2024 se efectuó el reporte a la Alta Consejería de TIC del Instrumento de Autodiagnóstico del MSPI y del Gap de Protección de Datos Personales, en cumplimiento de los lineamientos establecidos en la Política de Seguridad Digital y en las disposiciones normativas relacionadas con la protección de datos personales. No obstante, dichos reportes corresponden únicamente a ejercicios de autodiagnóstico y no evidencian la existencia de un Plan de Ejecución de Auditorías formalmente definido, que garantice el seguimiento y control mediante revisiones periódicas de los procesos de adopción e implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en el IPES, conforme a las obligaciones establecidas en las resoluciones 500 de 2021, 002277 de 2025 del MinTIC y a las mejores prácticas en gestión de la seguridad de la información (ISO 27001:2022). Estas observaciones deben ser validadas y aprobadas por parte de la Alta Dirección. **Por tal razón, la observación se mantiene.**
k) De acuerdo con lo señalado en la réplica respecto a la presentación del PETI y el monitoreo de sus indicadores, no se evidencian procesos de mejora continua en la adopción de los lineamientos para la implementación del Modelo de Seguridad y Privacidad de la

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES

Información (MSPI) en el IPES. Esta situación refleja una debilidad en el componente de evaluación del desempeño, el cual debería permitir la obtención de resultados, la preparación de acciones correctivas y la generación de estrategias que fortalezcan el nivel de madurez y responsabilidad institucional en materia de seguridad de la información, en concordancia con lo dispuesto en las resoluciones 500 de 2021, 002277 de 2025 del MinTIC y a las mejores prácticas en gestión de la seguridad de la información (ISO 27001:2022). **Por tal razón, la observación se mantiene.**

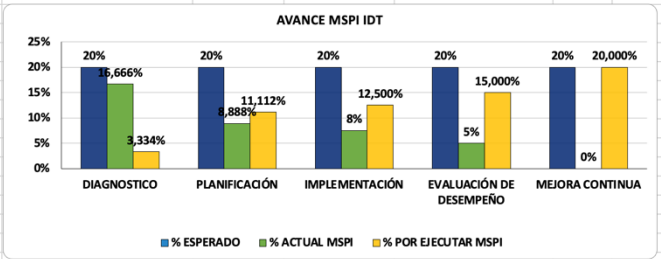
Como resultado de las anteriores situaciones presentadas, se comparte el análisis estadístico de los 19 requerimientos del MSPI en el siguiente gráfico el cual se encuentra de manera detallada su análisis y valoración en el ANEXO No 1:

ALCALDÍA MAYOR DE BOGOTÁ D.C. — INSTITUTO PARA LA ECONOMÍA SOCIAL

CICLOS	FASES MSPI		CUMPLE	META	% ESPERADO	% ACTUAL MSPI
1	DIAGNOSTICO	1.1	SI	20%	6,667%	6,667%
		1.2	SI		6,667%	6,667%
		1.3	PARCIAL		6,667%	3,333%
2	PLANIFICACION	2.1	NO	20%	2,222%	0,000%
		2.2	PARCIAL		2,222%	1,111%
		2.3	PARCIAL		2,222%	1,111%
		2.4	PARCIAL		2,222%	1,111%
		2.5	PARCIAL		2,222%	1,111%
		2.6	NO		2,222%	0,000%
		2.7	PARCIAL		2,222%	1,111%
		2.8	PARCIAL		2,222%	1,111%
		2.9	SI		2,222%	2,222%
3	IMPLEMENTACIÓN	3.1	NO	20%	5%	0,000%
		3.2	NO		5%	0,000%
		3.3	PARCIAL		5%	2,500%
		3.4	SI		5%	5,000%
4	EVALUACION DE DESEMPEÑO	4.1	PARCIAL	20%	10%	5,000%
		4.2	NO		10%	0,000%
5	MEJORA CONTINUA	5.1	NO	20%	20%	0,000%
RESULTADOS MSPI				100%	100,00%	38,054%

ESTADISTICAS FINAL
MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN MSPI

FASES MSPI	% ESPERADO	% ACTUAL MSPI	% POR EJECUTAR MSPI
DIAGNOSTICO	20%	16,666%	3,334%
PLANIFICACIÓN	20%	8,888%	11,112%
IMPLEMENTACIÓN	20%	8%	12,500%
EVALUACIÓN DE DESEMPEÑO	20%	5%	15,000%
MEJORA CONTINUA	20%	0%	20,000%
RESULTADOS MSPI	100%	38,054%	61,946%



ALCALDÍA MAYOR DE BOGOTÁ D.C. — INSTITUTO PARA LA ECONOMÍA SOCIAL

FASES MSPI	MSPI	CUMPLE	META	% ESPERADO	% FINAL EJECUTADO	% PENDIENTE POR EJECUTAR	MSPI	ACTIVIDADES MSPI	CUMPLIO	CUMPLIO PARCIAL	NO CUMPLIO
DIAGNOSTICO	1.1	SI	20%	6,667%	6,667%	0,000%	1.1	1	X		
	1.2	SI		6,667%	6,667%	0,000%	1.2	2	X		
	1.3	PARCIAL		6,667%	3,333%	-3,334%	1.3	3		X	
PLANIFICACION	2.1	NO	20%	2,222%	0,000%	-2,222%	2.1	4			X
	2.2	PARCIAL		2,222%	1,111%	-1,111%	2.2	5		X	
	2.3	PARCIAL		2,222%	1,111%	-1,111%	2.3	6		X	
	2.4	PARCIAL		2,222%	1,111%	-1,111%	2.4	7		X	
	2.5	PARCIAL		2,222%	1,111%	-1,111%	2.5	8		X	
	2.6	NO		2,222%	0,000%	-2,222%	2.6	9			X
	2.7	PARCIAL		2,222%	1,111%	-1,111%	2.7	10		X	
	2.8	PARCIAL		2,222%	1,111%	-1,111%	2.8	11		X	
	2.9	SI		2,222%	2,222%	0,000%	2.9	12	X		
IMPLEMENTACIÓN	3.1	NO	20%	5%	0,000%	-5,000%	3.1	13			X
	3.2	NO		5%	0,000%	-5,000%	3.2	14			X
	3.3	PARCIAL		5%	2,500%	-2,500%	3.3	15		X	
	3.4	SI		5%	5,000%	0,000%	3.4	16	X		
EVALUACION DE DESEMPEÑO	4.1	PARCIAL	20%	10%	5,000%	-5,000%	4.1	17		X	
	4.2	NO		10%	0,000%	-10,000%	4.2	18			X
MEJORA	5.1	NO	20%	20%	0,000%	-20,000%	5.1	19			X
RESULTADOS MSPI			100%	100,00%	38,054%	-61,94%		19	4	9	6

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES
NOTA El anexo en mención enmarca el Papel de Trabajo MSPI - IPES 2025.xlsx, que contiene el detalle de las observaciones derivadas del análisis de las evidencias documentales presentadas por el proceso auditado.

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES
Nombre del Proceso: Gestión de la Información y de los Recursos Tecnológicos
PA03-MN-002 MANUAL DE USUARIO HERRAMIENTA MISIONAL (HEMI) V3 Fecha: 07/06/2024 **PA03-MN-003 MANUAL TÉCNICO HERRAMIENTA MISIONAL (HEMI) V3 Fecha: 07/06/2024**
***Auditor:* Sergio Andrés Castro Londoño**

OBSERVACIÓN NO.2

Debilidades en materia de seguridad de la información y gestión tecnológica de la herramienta HEMI, que pueden llegar comprometer los principios de confidencialidad, integridad y disponibilidad (CID).

Situación(es):

Durante la prueba de recorrido realizada el 25 de junio de 2025 sobre la herramienta misional HEMI, se identificaron múltiples debilidades en materia de seguridad de la información y gestión tecnológica, que comprometen los principios de confidencialidad, integridad, disponibilidad y continuidad del negocio. Entre ellas, se evidenció una alta dependencia de acuerdos de confidencialidad jurídicos como única medida de protección para el intercambio de información sensible, sin integraciones técnicas seguras que garanticen trazabilidad, autenticación robusta, cifrado o controles de acceso auditables; además, se constató la ausencia de mecanismos de autenticación multifactor (2FA), exponiendo el sistema a riesgos de suplantación e intrusión, en contravía de los lineamientos establecidos en la norma ISO/IEC 27001:2022 y el Modelo de Seguridad y Privacidad de la Información (MSPI). Adicionalmente, HEMI no cuenta con infraestructura de respaldo ni esquemas de alta disponibilidad que permitan asegurar la continuidad operativa, situación evidenciada durante la interrupción total del servicio generada por el traslado del centro de datos en junio–julio de 2025, lo cual incumple la norma ISO 22301:2019 y el procedimiento PA03-PD-009 V2. A esto se suma la limitada capacidad del sistema para generar reportes dinámicos y tableros de control comprensibles, afectando la apropiación funcional, la toma de decisiones basada en evidencia y el seguimiento efectivo a los procesos misionales. Estas situaciones observadas, debilita la postura de ciberseguridad institucional del IPES, expone a la entidad a riesgos operacionales, reputacionales y de incumplimiento normativo, y puede ser objeto de observaciones por parte de entes de control.Las principales situaciones observadas de la prueba de recorrido fueron las siguientes:

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES

a) Dependencia de acuerdos de confidencialidad como mecanismo para el intercambio de información entre entidades públicas.

De acuerdo con los compromisos de confidencialidad, no divulgación y reserva de la información sensible constituidos por el IPES, se identificaron acuerdos de confidencialidad para el tratamiento de información pública clasificada, información pública reservada, información privada, además de información técnica, financiera, estratégica y cualquier información relacionada con las operaciones presentes y futuras del IPES con las siguientes entidades:

- Acuerdo de confidencialidad DNP-IPES, el cual no presenta fecha y firma del representante legal del DNP.
- Acuerdo de confidencialidad suscrito entre la Secretaría General – Alcaldía Mayor de Bogotá D.C. y el IPES, mediante el cual se permite acceder a la información contenida en la base de datos del Archivo Nacional de Identificación (ANI), administrado por la Registraduría Nacional del Estado Civil (RNEC). Este acceso se realiza mediante intercambio de archivos planos conforme al protocolo establecido con la Secretaría General.

Sin embargo, es necesario atender las siguientes recomendaciones, como los análisis técnicos y jurídicos de seguridad de la información sobre acuerdos de confidencialidad y procesos de interoperabilidad:

La consulta, acceso, descarga, procesamiento y posterior carga de bases de datos provenientes de otras entidades públicas implican un tratamiento complejo de información que requiere medidas robustas de seguridad. Generalmente, dichos procesos están respaldados por acuerdos de confidencialidad entre entidades públicas, los cuales definen las responsabilidades y compromisos de seguridad y protección de datos personales.

Sin embargo, es necesario evaluar si estos acuerdos por sí solos garantizan adecuadamente la seguridad desde los principios básicos de confidencialidad, integridad y disponibilidad (CID).

Desde el marco legal colombiano, la protección y seguridad de la información está regulada principalmente por:

- Ley 1581 de 2012 (Ley de Protección de Datos Personales), que establece obligaciones jurídicas para quienes tratan datos personales.
- Ley 1712 de 2014 (Ley de Transparencia y del Derecho de Acceso a la Información Pública).
- Ley 1273 de 2009 (Delitos informáticos), que protege penalmente la información almacenada en sistemas de información.
- Decreto 1074 de 2015, especialmente el capítulo 25 sobre gestión de seguridad y privacidad.
- ISO/IEC 27001:2022, como estándar internacional reconocido por Colombia para la gestión de seguridad de la información.

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES

Los acuerdos de confidencialidad firmados entre entidades públicas generalmente cubren:

- Compromiso explícito de confidencialidad frente al tratamiento de datos.
- Obligaciones legales específicas en caso de incumplimiento (responsabilidad administrativa, disciplinaria o penal).
- Especificación de las responsabilidades frente al tratamiento, procesamiento y almacenamiento seguro.

Sin embargo, aunque estos acuerdos establecen responsabilidades jurídicas, por sí solos no garantizan técnicamente la seguridad efectiva en la operación diaria. Dichos acuerdos deben complementarse obligatoriamente con medidas técnicas específicas para materializar los compromisos adquiridos.

Análisis técnico desde la triada CID:

A continuación, se evalúan los riesgos técnicos de seguridad según los principios fundamentales de la seguridad de la información (CID):

✓ <u>Confidencialidad</u>

El intercambio manual de información entre entidades, aun cuando esté respaldado por acuerdos de confidencialidad, implica riesgos significativos desde la perspectiva de seguridad de la información, al exponer los datos a accesos no autorizados por la manipulación manual y almacenamiento intermedio, posibles filtraciones debido a errores humanos o incidentes internos, así como al uso inadecuado de canales no seguros o a la falta de mecanismos adecuados de cifrado. En consecuencia, desde el punto de vista técnico, estos acuerdos son insuficientes para garantizar la confidencialidad, integridad y disponibilidad de los datos, si no se complementan con controles técnicos específicos tales como cifrado robusto de información, controles estrictos de acceso, autenticación multifactor y auditorías periódicas que permitan identificar oportunamente vulnerabilidades o brechas de seguridad.

✓ <u>Integridad</u>

Actualmente, el procesamiento manual de información incrementa significativamente el riesgo de alteraciones accidentales o deliberadas en los datos, especialmente durante la carga manual de archivos planos provenientes de otras entidades hacia los sistemas propios. Esta situación se ve agravada por la debilidad o ausencia de mecanismos efectivos de validación y controles técnicos de integridad, así como por la inexistencia de procesos automatizados que permitan verificar la autenticidad e integridad de la información. Por tanto, desde el punto de vista técnico y considerando la integridad de la información, es necesario considerar implementar controles automatizados robustos, tales como mecanismos de hashing, checksum o firmas digitales, orientados a garantizar que los archivos planos descargados no sean objeto de manipulación indebida antes o durante su incorporación a los sistemas internos de la entidad.

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES

- ✓ Disponibilidad

  El procesamiento manual de información representa un riesgo significativo para la disponibilidad de los datos, ya que puede afectar la continuidad operacional del sistema al generar retrasos, errores, inconsistencias o incluso la denegación parcial del servicio debido a fallas humanas durante la carga de información. Entre los riesgos identificados se encuentran los retrasos operacionales derivados de errores en la manipulación manual, interrupciones del servicio o pérdida temporal de acceso a datos críticos, y una mayor dificultad para la recuperación ante incidentes. Desde una perspectiva técnica, resulta fundamental avanzar hacia esquemas de interoperabilidad automática mediante la implementación de mecanismos que aseguren la disponibilidad y continuidad del servicio en tiempo real, minimizando la dependencia de procesos manuales y mejorando la eficiencia operativa.

La ausencia de interoperabilidad técnica automatizada para el intercambio de información puede incrementar las vulnerabilidades de seguridad informática:

- Mayor exposición al error humano.
- Mayor dependencia del manejo manual de información sensible.
- Incremento en la posibilidad de incidentes por fugas, pérdida o alteración de datos.
- Dificultad para mantener trazabilidad, auditoría técnica y control permanente.

Por lo tanto, un proceso manual genera un entorno inseguro desde la perspectiva técnica, afectando directamente la seguridad operativa y los principios CID.

Conclusiones generales

Desde un enfoque jurídico y técnico, aunque los acuerdos de confidencialidad brindan un marco legal importante, resultan insuficientes para garantizar plenamente los principios de confidencialidad, integridad y disponibilidad (CID) si no se complementan con mecanismos técnicos robustos. Técnicamente, el tratamiento manual de la información incrementa exponencialmente los riesgos operativos y las vulnerabilidades de seguridad informática, en contraste con los procesos automáticos basados en interoperabilidad. En este sentido, la adopción de un modelo de interoperabilidad técnica automática constituye una buena práctica en materia de seguridad digital e informática, alineada con la normativa vigente y con los estándares internacionales, al contribuir significativamente a la reducción de riesgos asociados a la triada CID.

Recomendación

Se recomienda que el Instituto estructure e implemente un plan integral de interoperabilidad técnica segura, orientado a eliminar la dependencia de procesos manuales en el acceso, procesamiento y carga de bases de datos provenientes de otras entidades públicas, así como en el intercambio de información entre la herramienta misional HEMI y otros sistemas institucionales y externos. Este plan debe incluir el establecimiento de acercamientos institucionales con la Alta Consejería Distrital TIC, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y la Agencia Nacional Digital, con el fin de validar la viabilidad técnica, normativa y operativa de adoptar

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES

mecanismos de interoperabilidad confiables. Particularmente, se recomienda evaluar soluciones como la plataforma X-Road u otras equivalentes, que permitan el intercambio automatizado, auditable y seguro de datos entre entidades, bajo esquemas de integración basados en servicios web seguros (REST/SOAP con autenticación robusta), uso de canales cifrados (TLS/SSL), trazabilidad mediante registros de auditoría, y controles de acceso basados en roles (RBAC). Asimismo, los acuerdos de confidencialidad actualmente suscritos deben ser complementados con medidas técnicas que garanticen la seguridad efectiva en la operación diaria, incluyendo la implementación de autenticación multifactor (MFA) y mecanismos de validación de integridad de los datos. Estas acciones deben alinearse con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y los controles establecidos en la norma ISO/IEC 27001:2022, particularmente en lo relacionado con la interoperabilidad, la gestión de accesos y la protección de la información en tránsito y en reposo.

Este tipo de iniciativas contribuye a optimizar los procesos institucionales, fortalecer la trazabilidad en el uso de la información y asegurar el cumplimiento de las buenas prácticas en materia de seguridad y gobierno digital, conforme a lo establecido en el Decreto 767 de 2022 y el Decreto 620 de 2020 del MinTIC. Este último, de carácter normativo y obligatorio para las entidades públicas y los particulares que ejercen funciones administrativas, establece que los Servicios Ciudadanos Digitales: interoperabilidad, autenticación digital y carpeta ciudadana digital deben ser implementados conforme a los lineamientos definidos en la política de gobierno digital, con el fin de garantizar la prestación eficiente, segura y transparente de los servicios públicos mediante el uso de las tecnologías de la información.

b) Ausencia de infraestructura de respaldo y continuidad operativa

HEMI no dispone de servidores espejo, esquemas de alta disponibilidad ni medidas técnicas que permitan la conmutación automática en caso de fallos. Esto representa un riesgo crítico para la resiliencia operativa, ya que ante eventos como fallas técnicas, traslados o actualizaciones, el servicio se interrumpe sin contar con entornos redundantes que respalden la continuidad.

De hecho, durante el traslado del centro de datos a la nueva sede institucional (junio–julio de 2025), se reportó una interrupción total del servicio debido a la inexistencia de una infraestructura de respaldo, vulnerando así los principios de continuidad del negocio definidos en la norma ISO 22301:2019 y el procedimiento PA03-PD-009 V2 – Implementación de la Continuidad de la Seguridad de la Información.

Esta omisión también incumple las disposiciones del artículo 17 de la Ley 1581 de 2012 y el Decreto 1377 de 2013, las cuales exigen implementar medidas técnicas y administrativas que garanticen la disponibilidad y recuperación de la información.

c) Ausencia del 2FA de autenticación

La herramienta HEMI, no implementa autenticación multifactor (MFA/2FA), lo cual representa una debilidad crítica en la protección de cuentas frente a amenazas como phishing, suplantación, fuerza bruta o robo de credenciales.

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES

Estas condiciones vulneran los controles de autenticación y gestión de accesos definidos en la *ISO/IEC 27001:2022 - Dominio A.8.Controles tecnológicos – A.8.2 – Autenticación del usuario* y contradicen los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC, en lo relativo a la implementación de controles técnicos proporcionales al nivel de riesgo.

d) Limitaciones en análisis e informes de gestión

Se identifican debilidades en la comprensión y uso de los tableros de control y reportes del sistema HEMI, tanto a nivel directivo como funcional, debido a la baja interactividad y escasa funcionalidad dinámica de la herramienta.

Estas limitaciones dificultan la consolidación, interpretación y aprovechamiento de los datos disponibles, impidiendo la realización de análisis objetivos sobre el desempeño, uso y eficiencia del sistema. En consecuencia, se ve comprometida la capacidad institucional para monitorear indicadores, identificar patrones de gestión y tomar decisiones informadas.

Esta situación incide negativamente en la gestión estratégica y constituye un obstáculo para el mejoramiento continuo de los procesos misionales y administrativos, al no contar con herramientas de análisis adecuadas ni con una apropiación funcional suficiente por parte de los equipos responsables.

Se recomienda fortalecer las capacidades funcionales del sistema HEMI en materia de visualización de datos y facilitar espacios de formación orientados a mejorar la comprensión y el uso efectivo de los tableros, promoviendo una cultura institucional basada en el análisis de datos y la toma de decisiones basada en evidencia.

Causa(s):

Ausencia de infraestructura de respaldo y debilidades en los controles implementados para el seguimiento de la seguridad de la información en la herramienta HEMI, lo que incrementa significativamente el riesgo de inconsistencias, errores operativos y alteraciones en la información registrada.

Consecuencia(s):

Las debilidades identificadas comprometen los principios fundamentales de la seguridad de la información: confidencialidad, integridad y disponibilidad (CID), generando riesgos significativos sobre los activos de información institucional. Esta situación puede derivar en accesos no autorizados, alteración o pérdida de datos críticos y la interrupción de servicios esenciales. Además, podría dar lugar a observaciones o reportes desfavorables por parte de los entes de control, afectando la imagen institucional y el cumplimiento normativo del IPES.

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES

Riesgo(s) Asociado(s):

Error humano y acceso inadecuado (eliminación, alteración, corrupción, mala gestión), en realizar procesos manuales de análisis y procesamiento de bases de datos externas, que luego son depuradas y cargarlas en HEMI, con la posible afectación de la confidencialidad, integridad y disponibilidad de la información de acuerdo con:

a) *Disponibilidad - Perdida de disponibilidad de la infraestructura que soporta los servicios y activos de información de TI, debido a la ausencia de servidores de dominio espejo que mantenga y garantice la continuidad del negocio de las operaciones que se realizan en HEMI sin interrupciones.*
b) *Integridad - Perdida de Integridad de la información digital almacenada, procesada y manejada en los sistemas de información misional y administrativos.*
c) *Confidencialidad - Perdida de confidencialidad de: la información digital almacenada, procesada y manejada en los sistemas de información misional y administrativos; y la información del proceso PGSIRT*

Normatividad o Criterio:

- PA03-PD-009 V2 – Implementación de la Continuidad de la Seguridad de la Información.
- ISO 22301:2019 – Sistema de Gestión de la Continuidad del Negocio
- **ISO/IEC 27001:2022 Gestión de la Seguridad de la Información (CID)**
- Resolución No 500 del 2021 (MSPI)v1 - MinTIC
- Anexo 1 - Resolución No 500 de 2021de MinTIC (MSPI)
- Resolución No 746 del 2022 (MSPI)v1 - MinTIC
- Resolución 002277 de 2025 de MinTIC (MSPI)
- Decreto 620 de 2020 de MinTIC (Servicios Ciudadanos Digitales - Interoperabilidad)
- Ley 1581 de 2012 establece el régimen general de protección de datos personales, esta ley también regula el tratamiento de los datos sensibles
- Ley 1266 de 2008, sobre protección de datos personales, establece lineamientos para la seguridad de la información, y el 2FA puede ser una herramienta para cumplir con estos requisitos.
- Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Artículo 3 de la Resolución 460 de 2022 del MinTIC, de acuerdo con lo siguiente:

  “3.2 Confianza pública y gestión ética de los datos: La calidad de los datos que integran la infraestructura de datos del Estado, y su modelo de Gobernanza deben propender por la creación de un escenario de confianza para la generación, acceso, intercambio y reutilización de datos (…)

  “3.3 Estandarización e interoperabilidad: La infraestructura de datos del Estado debe operar bajo criterios de estandarización a través de todo su ciclo de gestión. Así, la estandarización debe aplicarse sobre los datos en sí mismos y en los metadatos. La aplicación de este

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES

principio debe caracterizarse por una baja dependencia de esquemas complejos, facilitando la interoperabilidad y el lenguaje común de intercambio entre sistemas de información (…)

"3.4 Fácil búsqueda, accesibilidad: interoperabilidad y reutilización: Los datos que integran la infraestructura de datos del Estado se deben caracterizar por ser accesibles, interoperables, reusables y de fácil búsqueda. Estos deben ser de fácil búsqueda y acceso, interoperables y dispuestos para su reutilización..."

Connotación:

Probabilidad de impacto negativo en el funcionamiento y operación de HEMI, por las posibles vulnerabilidades que puedan afectar los principios CID de la seguridad informática, seguridad de la información, seguridad digital del Instituto, con la posible incidencia administrativa, disciplinaria y/o fiscal.

Recomendación(es)

Con el fin de mitigar los riesgos asociados al acceso, procesamiento y carga manual de bases de datos provenientes de otras entidades públicas, se recomienda al Instituto gestionar acercamientos institucionales con la Alta Consejería Distrital TIC, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y la Agencia Nacional Digital, con el propósito de validar la viabilidad técnica, normativa y operativa de implementar mecanismos de interoperabilidad que permitan el intercambio seguro, automatizado y en línea de información interinstitucional. En este contexto, se sugiere evaluar la adopción de plataformas tecnológicas como X-Road o soluciones equivalentes, que habiliten procesos de integración de datos con trazabilidad, autenticación robusta y cifrado, fortaleciendo los principios de confidencialidad, integridad y disponibilidad. Esta medida debe armonizarse con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y los controles establecidos en la norma ISO/IEC 27001:2022, promoviendo una infraestructura tecnológica más segura, eficiente y alineada con las exigencias del entorno digital del sector público.

También se recomienda implementar el mecanismo de autenticación multifactor (MFA/2FA) en los sistemas institucionales, dado que la ausencia de esta medida representa una debilidad crítica en la protección de cuentas de usuario frente a amenazas comunes como el phishing, la suplantación de identidad, los ataques de fuerza bruta o el robo de credenciales. La adopción de este control contribuiría a fortalecer significativamente la seguridad de acceso a los sistemas de información del Instituto, en cumplimiento de los principios de confidencialidad, integridad y disponibilidad establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI) y en concordancia con los lineamientos de la norma ISO/IEC 27001:2022.

Asimismo, se recomienda parametrizar y ajustar la herramienta HEMI incorporando funcionalidades específicas que garanticen el cumplimiento de las disposiciones establecidas en el Decreto 315 de

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES

2024, particularmente en lo relacionado con los protocolos institucionales del IPES, así como con los principios de seguridad y privacidad de la información.

Valoración Comentarios del Auditado

Mediante Memorando con radicado número 10-817-2025-002245 del 21 de julio del 2025, la Subdirección de Diseño y Análisis Estratégico-SDAE, manifiesta lo siguiente**:**

a) El proceso auditado informa que HEMI se integra con el Directorio Activo, por lo que la centralización de la gestión y la periodicidad en la seguridad de contraseñas dependen de este. La herramienta incorpora validaciones para la detección de errores, mantiene registros de logs de acciones por usuario y cuenta con una consulta asociada al log de auditoría.

b) HEMI es interoperable de por sí. Las funcionalidades de interoperabilidad responden a un proceso de identificación de una necesidad o requerimiento y su correspondiente gestión administrativa y técnica interna y con la otra parte que interopera. No se puede calificar el cumplimiento como PARCIAL sustentando en las observaciones ACI cuando el sistema interopera o a interoperado con diferentes sistemas y cuando las características de interoperabilidad no implican que el sistema cumpla o no cumpla con las funcionalidades requeridas.

c) Sobre el ejemplo mencionado de la Registraduría esto no implica que HEMI no cumpla con las funcionalidades requeridas, que es lo que se pregunta. Se anexa Acuerdo de Confidencialidad relacionado con el intercambio de información con el ANI de la RNEC el cual opera mediante intercambio de archivos planos atendiendo el protocolo establecido con la Secretaría General de la Alcaldía.

Análisis de la ACI:

Revisados los soportes aportados por el proceso en respuesta a la observación del informe preliminar, la Asesoría de Control Interno concluye lo siguiente:

a) Respecto al punto a), se logró validar de acuerdo con los soportes aportados, que la herramienta HEMI se integra con el Directorio Activo, por lo que la centralización de la gestión y la periodicidad en la seguridad de contraseñas dependen de este. La herramienta incorpora validaciones para la detección de errores, mantiene registros de logs de acciones por usuario y cuenta con una consulta asociada al log de auditoría. **Por tal razón, se elimina la observación**.

b) Respecto al punto b) y c) y en base a los soportes presentados, estos son, acuerdos de confidencialidad ANI – RNEC, se constató una alta dependencia de acuerdos de confidencialidad suscritos en el ámbito jurídico como única medida de protección para el intercambio de datos, lo cual, si bien establece compromisos formales entre las partes, no representa una garantía técnica efectiva de seguridad, ni permite una trazabilidad adecuada sobre los flujos de información sensible. Estos acuerdos deben ser necesariamente complementados con integraciones técnicas seguras, autenticación robusta, cifrado de datos y controles de acceso auditables, que materialicen los compromisos jurídicos en la operación diaria. Dichos acuerdos deben complementarse obligatoriamente con medidas técnicas específicas para materializar los compromisos adquiridos, toda vez, que el

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES
tratamiento manual de la información incrementa exponencialmente los riesgos operativos y las vulnerabilidades de seguridad informática, en contraste con los procesos automáticos basados en interoperabilidad. En este sentido, la adopción de un modelo de interoperabilidad técnica automática constituye una buena práctica en materia de seguridad digital e informática, alineada con la normativa vigente y con los estándares internacionales, al contribuir significativamente a la reducción de riesgos asociados a la triada CID. ***Por tal razón se recomienda al proceso,*** *adelantar las gestiones pertinentes, tanto en el ámbito jurídico como técnico, ante la Secretaría General – Alcaldía Mayor de Bogotá, la Alta Consejería Distrital TIC, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y la Agencia Nacional Digital, con el fin de verificar la viabilidad normativa, técnica y operativa para establecer un intercambio seguro de información interinstitucional, ya sea mediante la implementación del componente de interoperabilidad X-Road o a través de otro mecanismo que garantice la confidencialidad, integridad, disponibilidad y trazabilidad de la información, conforme al Modelo de Seguridad y Privacidad de la Información – MSPI y los lineamientos del marco de interoperabilidad del Estado colombiano.*

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES
Nombre del Proceso: Gestión de la Información y de los Recursos Tecnológicos
Herramienta GOOBI – Validación de la siguiente normativa aplicable: ○ **MSPI Res 500 de 2021, 002277 de 2025 de MinTIC** ○ **ISO 27001:2022; ISO 22301:2019** ○ **PA03-PD-009 V2 Implementación de la Continuidad de la Seguridad de la Información**
Auditor: **Sergio Andrés Castro Londoño**

OBSERVACIÓN NO.3

Se identificaron debilidades en la gestión de accesos del sistema, reflejadas en la falta de sincronización con el Directorio Activo y la ausencia de mecanismos de autenticación multifactor (2FA/MFA), así como en la inexistencia de procesos de interoperabilidad para el intercambio de información con otros sistemas internos y externos. Asimismo, se evidenció que, a nivel de la operación, la herramienta GOOBI carece de servidores redundantes, lo que incrementa el riesgo de interrupciones en la continuidad del negocio y puede afectar los principios de confidencialidad, integridad y disponibilidad (CID) de la información.

Situación(es):

Durante la prueba de recorrido realizada el 25 de junio del presente año, se identificaron debilidades en la operación de la herramienta GOOBI, relacionadas con la gestión de accesos, usuarios, interoperabilidad, continuidad operativa y análisis de información, que comprometen los principios de confidencialidad, integridad y disponibilidad. Se evidenció la ausencia de autenticación multifactor (2FA/MFA), una administración de usuarios no integrada con el Directorio Activo (AD), contraseñas gestionadas manualmente sin políticas de renovación, ni alertas de vencimiento, lo

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES

que limita el control centralizado y la trazabilidad de identidades. Asimismo, el sistema carece de mecanismos estandarizados de interoperabilidad con plataformas institucionales y externas, incumpliendo los lineamientos de la Política de Gobierno Digital y del Marco de Interoperabilidad. Se identificó la falta de un servidor espejo o soluciones de alta disponibilidad, lo que incrementa el riesgo de interrupción de servicios críticos. Adicionalmente, la herramienta no cuenta con tableros de control, reportes dinámicos ni métricas de satisfacción que permitan evaluar el desempeño, la usabilidad y la eficiencia del sistema. Estas condiciones evidencian una brecha frente a las buenas prácticas establecidas en la ISO/IEC 27001:2022, la ISO 22301:2019 y el MSPI del MinTIC, exponiendo al Instituto para la Economía Social (IPES) a riesgos operacionales, tecnológicos, reputacionales y de incumplimiento normativo.

A continuación, se detallan las siguientes situaciones observadas:

a) Gestión de acceso y credenciales

- El acceso a la herramienta GOOBI se encuentra restringido a la red institucional o mediante conexión VPN, previa configuración en el firewall y creación de usuarios en el Directorio Activo (AD) con autorización del jefe inmediato. Sin embargo, se evidenció que la gestión de contraseñas es manual y se realiza únicamente en el primer ingreso del usuario, sin políticas de renovación periódica, alertas de vencimiento ni funcionalidades para su administración interna. Adicionalmente, no se han implementado recordatorios automáticos ni se cuenta con solicitudes documentadas de parametrización para fortalecer esta funcionalidad por parte de las áreas usuarias o del equipo TIC, lo que representa una debilidad en los controles de autenticación y gestión de credenciales, contraviniendo las buenas prácticas establecidas en la ISO/IEC 27001:2022 (control A.8.2 – Autenticación del usuario).

b) Gestión de usuarios

- No se observó la existencia de una sincronización automática con el Directorio Activo (AD), lo que debilita los controles de acceso y la administración del ciclo de vida de los usuarios.

- Se observó que la creación y administración de usuarios en la ERP GOOBI se realiza directamente desde la base de datos Oracle, sin integrarse con el Directorio Activo institucional, aunque se justifique por razones de seguridad, control y auditoría, representa una debilidad en términos de buenas prácticas de ciberseguridad. Esta configuración limita la trazabilidad centralizada, dificulta la implementación de autenticación multifactor (2FA), aumenta el riesgo de cuentas huérfanas o accesos no autorizados y se aleja de los lineamientos establecidos en la ISO/IEC 27001:2022 y el Modelo de Seguridad y Privacidad de la Información (MSPI). La gestión centralizada de usuarios mediante el Directorio Activo permite una administración más segura, coherente y alineada con los estándares de seguridad de la información en entidades públicas.

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES

c) Ausencia de autenticación multifactor (MFA)

- En la operación GOOBI GRP, no cuenta con mecanismos de autenticación de doble factor (2FA/MFA) en ambientes locales (on-premise), lo que representa una brecha de seguridad al no añadir una capa adicional de protección frente a accesos no autorizados, robo de credenciales o ataques de fuerza bruta.

  Estas condiciones vulneran los controles de autenticación y gestión de accesos definidos en la *ISO/IEC 27001:2022 - Dominio A.8.Controles tecnológicos – A.8.2 – Autenticación del usuario* y contradicen los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC, en lo relativo a la implementación de controles técnicos proporcionales al nivel de riesgo.

d) Interoperabilidad limitada

- En el ámbito de la interoperabilidad, se identificó que el sistema GOOBI GRP carece de mecanismos estandarizados para integrarse en línea con otros sistemas institucionales o del ecosistema digital del sector público, como Bogotá te Escucha (PQRDS), BOGDATA, SICAPITAL y SECOP. No se evidenció la implementación de protocolos técnicos seguros, tales como Web Services (WS), APIs RESTful, X-Road, EDI, SFTP/FTPS o Enterprise Service Bus (ESB), los cuales son esenciales para garantizar un intercambio de datos confiable, eficiente, trazable y alineado con los principios de confidencialidad, integridad y disponibilidad (CID).
  La ausencia de estos mecanismos limita la eficiencia operativa, restringe la automatización de procesos interplataforma, dificulta la trazabilidad de la información intercambiada, aumenta los riesgos de seguridad al depender de canales no controlados y obstaculiza la articulación institucional y sectorial necesaria para una toma de decisiones oportuna y basada en datos consistentes.
  Esta situación incumple los lineamientos de la Política de Gobierno Digital, el Marco de Interoperabilidad del Estado Colombiano y las disposiciones técnicas del MinTIC y la Agencia Nacional Digital, que obligan a las entidades públicas a implementar mecanismos interoperables seguros y auditables. En consecuencia, se compromete la gestión integral de la información pública, generando riesgos como duplicidad de registros, esfuerzos administrativos innecesarios, errores en la toma de decisiones, indisponibilidad oportuna de datos y pérdida de confianza ciudadana.
  Lo anterior, configura un riesgo de incumplimiento normativo frente a la Ley 1581 de 2012, el Decreto 1377 de 2013, el Decreto 620 de 2020, el Decreto 767 de 2022 y los estándares internacionales de seguridad de la información, como la norma ISO/IEC 27001:2022, con una posible afectación a la continuidad del servicio, la transparencia institucional y la legitimidad de la administración digital.

e) Riesgo crítico de continuidad operativa

- Se verificó la ausencia de un servidor espejo o mecanismos de alta disponibilidad para respaldar el servidor principal que aloja la base de datos de GOOBI. Esta condición impide

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES

implementar procesos de conmutación automática ante fallas (failover), elevando el riesgo de interrupción de servicios críticos y afectando directamente la operación institucional.

f) Limitaciones en análisis e informes de gestión

- La herramienta en la actualidad no permite generar reportes dinámicos y parametrizados comprensibles para la toma de decisiones, tampoco cuenta con dashboard (tableros de control), que permitan visualizar metas, resultados, métricas, estadísticas, entre otros indicadores de medición, lo cual impide realizar análisis objetivos de desempeño, uso o eficiencia del sistema.

g) Ausencia de métricas de satisfacción

- No existe un módulo o sistema estructurado para evaluar la satisfacción del usuario funcional. Las valoraciones se recopilan informalmente, sin consolidación de indicadores de usabilidad, eficiencia o mejora continua.

h) Ausencia de manual de usuario en línea

- La herramienta no cuenta con un manual de usuario en línea para consulta o descarga, ni se evidencian soportes que acrediten su oficialización, implementación o los procesos de uso y apropiación mediante actividades de sensibilización con los usuarios funcionales del Instituto.

Conclusión técnica:

Estas deficiencias vulneran principios esenciales de seguridad de la información relacionados con la confidencialidad, integridad y disponibilidad, establecidos en la ISO/IEC 27001:2022, la ISO 22301:2019 sobre continuidad del negocio y el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC. La falta de controles robustos en la gestión y administración de usuarios mediante el Directorio Activo, la ausencia de mecanismos de interoperabilidad, y la inexistencia de un servidor espejo o soluciones de alta disponibilidad para respaldar el servidor principal que aloja la base de datos de GOOBI, exponen al IPES a riesgos operacionales, tecnológicos, reputacionales y de incumplimiento normativo.

Causa(s):

Las debilidades identificadas en la operación de la herramienta GOOBI tienen como causas principales la ausencia de una arquitectura tecnológica robusta, la falta de implementación de controles de seguridad alineados con estándares internacionales (como la ISO 27001 e ISO 22301), la carencia de mecanismos automatizados de autenticación, trazabilidad y respaldo, y una gestión limitada por parte del área TIC en cuanto a la documentación técnica, interoperabilidad y mejora continua del sistema.

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES

Consecuencia(s):

Estas situaciones han derivado en consecuencias significativas, como un aumento en el riesgo de accesos no autorizados, exposición a ciberataques, vulnerabilidad ante fallas operativas, dificultad para garantizar la continuidad del negocio, baja trazabilidad de las acciones de los usuarios, y restricciones para cumplir con los principios de seguridad de la información, lo cual compromete la eficiencia institucional, la integridad de los datos y la confianza de los usuarios internos y externos en los sistemas del IPES.

Riesgo(s) Asociado(s):

1. ***Error humano y acceso inadecuado (eliminación, alteración, corrupción, mala gestión),*** por no implementar los lineamientos del MSPI y las directrices de la Resolución No 500 del 2021 de MinTIC, con la posible afectación de la seguridad CID del Instituto:

   a) Disponibilidad - Perdida de disponibilidad de la infraestructura que soporta los servicios y activos de información de TI.
   b) Integridad - Perdida de Integridad de la información digital almacenada, procesada y manejada en los sistemas de información misional y administrativos.
   c) Confidencialidad - Perdida de confidencialidad de: la información digital almacenada, procesada y manejada en los sistemas de información misional y administrativos; y la información del proceso PGSIRT…"

Normatividad o Criterio:

- PA03-PD-009 V2 – Implementación de la Continuidad de la Seguridad de la Información.
- ISO 22301:2019 – Sistema de Gestión de la Continuidad del Negocio
- **ISO/IEC 27001:2022 Gestión de la Seguridad de la Información (CID)**
- Resolución No 500 del 2021 (MSPI)v1 - MinTIC
- Anexo 1 - Resolución No 500 de 2021de MinTIC (MSPI)
- Resolución No 746 del 2022 (MSPI)v1 - MinTIC
- Resolución 002277 de 2025 de MinTIC (MSPI)
- Decreto 620 de 2020 de MinTIC (Servicios Ciudadanos Digitales - Interoperabilidad)
- Ley 1581 de 2012 establece el régimen general de protección de datos personales, esta ley también regula el tratamiento de los datos sensibles
- Ley 1266 de 2008, sobre protección de datos personales, establece lineamientos para la seguridad de la información, y el 2FA puede ser una herramienta para cumplir con estos requisitos.
- Ley 1273 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Artículo 3 de la Resolución 460 de 2022 del MinTIC, de acuerdo con lo siguiente:

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES

"3.2 Confianza pública y gestión ética de los datos: La calidad de los datos que integran la infraestructura de datos del Estado, y su modelo de Gobernanza deben propender por la creación de un escenario de confianza para la generación, acceso, intercambio y reutilización de datos (…)

"3.3 Estandarización e interoperabilidad: La infraestructura de datos del Estado debe operar bajo criterios de estandarización a través de todo su ciclo de gestión. Así, la estandarización debe aplicarse sobre los datos en sí mismos y en los metadatos. La aplicación de este principio debe caracterizarse por una baja dependencia de esquemas complejos, facilitando la interoperabilidad y el lenguaje común de intercambio entre sistemas de información (…)

"3.4 Fácil búsqueda, accesibilidad: interoperabilidad y reutilización: Los datos que integran la infraestructura de datos del Estado se deben caracterizar por ser accesibles, interoperables, reusables y de fácil búsqueda. Estos deben ser de fácil búsqueda y acceso, interoperables y dispuestos para su reutilización..."

Connotación:

Probabilidad de impacto negativo en el funcionamiento y operación de GOOBI, por las posibles vulnerabilidades que puedan afectar los principios CID de la seguridad informática, seguridad de la información, seguridad digital del Instituto, con la posible incidencia administrativa, disciplinaria y/o fiscal.

Recomendación

Se recomienda al Instituto implementar medidas técnicas y organizacionales para cerrar estas brechas, priorizando la incorporación de autenticación MFA, mecanismos de alta disponibilidad, trazabilidad integral, sincronización con el Directorio Activo y documentación técnica actualizada, en concordancia con los lineamientos del MSPI y las buenas prácticas internacionales.

Adicionalmente, se recomienda la definición de requerimientos funcionales por parte de los usuarios que hacen uso de la herramienta GOOBI vencimiento del sistema

Valoración Comentarios del Auditado

Mediante Memorando con radicado número 10-817-2025-002245 del 21 de julio del 2025, la Subdirección de Diseño y Análisis Estratégico-SDAE, manifiesta lo siguiente**:**

a) La ERP GOOBI cuenta con una base de conocimientos que permite identificar el error en las operaciones que realizan los funcionarios y documentar las causas y las acciones a tomar.
b) La plataforma ERP GOOBI cuenta con la trazabilidad y el registro detallado de todas las transacciones realizadas por los usuarios en el sistema de información. No obstante, conforme a las políticas internas definidas por la entidad al momento de la configuración del

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES

sistema, no se autorizó el acceso a estas consultas por parte de los funcionarios, restringiendo su visualización únicamente a los administradores del sistema.

c) Se cuenta con un manual de usuario cuya fecha de elaboración corresponde al 21 de noviembre de 2017. No obstante, en el marco de la vigencia 2025 y a través del contratista GOOBI S.A.S., se tiene previsto realizar la actualización del documento funcional, con el objetivo de reflejar los cambios introducidos en la plataforma, tanto en lo referente a la actualización de componentes como al despliegue de nuevas versiones y funcionalidades.

Análisis de la ACI:

Revisados los soportes aportados por el proceso en respuesta a la observación del informe preliminar, la Asesoría de Control Interno concluye lo siguiente:

Respecto al punto a) y b), se logró validar de acuerdo con los soportes aportados, que la herramienta GOOBI cuenta con una base de conocimiento que permite identificar el error en operaciones y mantiene la trazabilidad y registro de transacciones realizadas por el usuario a documentos. **Por tal razón, se elimina la observación a y b de las situaciones observadas en el presente informe.**

Respecto al punto c), se observa que, si bien en los soportes aportados por el proceso se incluye el manual de usuario de GOOBI en formato .docx, no se evidencian soportes que acrediten su oficialización, implementación ni los procesos de uso y apropiación mediante actividades de sensibilización con los usuarios funcionales del Instituto. Asimismo, se reitera que la observación señala la ausencia de un manual en línea que pueda ser consultado y/o descargado directamente desde la herramienta GOOBI. **En consecuencia, la observación se mantiene.**

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES

Nombre del Proceso: Gestión de la Información y de los Recursos Tecnológicos

PA03-PD-009 V2 Implementación de la Continuidad de la Seguridad de la Información

Auditor: **Sergio Andrés Castro Londoño**

OBSERVACIÓN NO.4

Debilidades en el cumplimiento de las actividades del procedimiento **PA03-PD-009 V2** para garantizar la continuidad de la seguridad de la información en el Instituto para la Economía Social – IPES

Situación(es):

En la revisión del procedimiento PA03-PD-009 V2 se identificaron debilidades críticas en la gestión de la continuidad de la seguridad de la información, particularmente ante escenarios de contingencia que pueden afectar la operatividad institucional. Si bien se verificó la activación del Plan de Continuidad del Negocio (PCN) tras un incidente de seguridad por ataque tipo ransomware,

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES

detectado por la herramienta Darktrace Network y reportado en el Comité de Seguridad del 3 de marzo de 2025, no se materializaron riesgos ni impactos sobre los activos evaluados o sistemas institucionales. No obstante, se evidenció una respuesta institucional más reactiva que preventiva, con ausencia de análisis post-incidente, validación de controles y procesos de mejora continua.

Se constató que el inventario de activos de información no ha sido actualizado para las vigencias 2024-2025, manteniéndose únicamente el correspondiente al año 2023. Esta situación limita la capacidad del Instituto para identificar riesgos vigentes, aplicar controles efectivos y garantizar los principios de confidencialidad, integridad y disponibilidad de la información, en contravía de la norma ISO/IEC 27001:2022. Aunque en la réplica al informe preliminar el proceso manifestó haber publicado los activos con corte a 2025 en el enlace de transparencia del Instituto, no se presentaron evidencias ni soportes en la prueba de recorrido efectuada el pasado 2 de julio del año que discurre, que acrediten la gestión con cada proceso, área o dependencia en relación con la identificación, clasificación de activos y determinación de riesgos de seguridad informática, de la información y digital para las vigencias 2024 y 2025.

Asimismo, aunque se cuenta con una matriz de riesgos de seguridad de la información, no se evidencian riesgos digitales actualizados ni una gestión integral que incorpore las amenazas reales documentadas en actas, informes o comités, lo que refleja una falta de trazabilidad entre los incidentes detectados y la actualización de los planes de tratamiento. Esto denota una desconexión entre la operación diaria y la gestión estratégica de la seguridad de la información.

De igual manera, no se identificaron nuevos controles técnicos implementados durante el período auditado, lo que impide evaluar la efectividad de las medidas preventivas y limita la capacidad institucional para demostrar avances en la mejora continua, conforme a la norma ISO/IEC 27001:2022 y al Modelo de Seguridad y Privacidad de la Información (MSPI).

Finalmente, se evidenció la ausencia de infraestructura redundante o servidores espejos que respalden los sistemas críticos, una vulnerabilidad que se materializó durante el traslado de sede institucional. La carencia de mecanismos de alta disponibilidad interrumpió la continuidad de los servicios, afectando la operatividad del Instituto durante el cierre de junio y la primera semana de julio de 2025, en contravención de lo dispuesto en la norma ISO 22301:2019 sobre Sistemas de Gestión de Continuidad del Negocio y en el procedimiento PA03-PD-009 V2, que exige validar y mantener capacidades de recuperación frente a eventos disruptivos.

Causa(s):

Las debilidades identificadas en la continuidad de la seguridad de la información en el IPES tienen como causa principal la ausencia de una estrategia formal y documentada para la implementación efectiva del Plan de Continuidad de la Seguridad de la Información, así como la falta de actualización del inventario de activos de información y de gestión integral de riesgos de seguridad digital. Adicionalmente, la no implementación de controles técnicos nuevos ni de infraestructura redundante, como servidores espejo, evidencia un bajo nivel de alineación con los estándares internacionales ISO/IEC 27001:2022 e ISO 22301:2019 y los lineamientos del MSPI.

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES

Consecuencia(s):

Como consecuencia, el Instituto enfrenta una alta exposición a riesgos operativos y de disponibilidad, lo que compromete la capacidad institucional para responder y recuperarse ante incidentes críticos, afectando la prestación continua de los servicios misionales, debilitando la protección de la información crítica y generando posibles hallazgos en auditorías externas, sanciones legales y pérdida de confianza por parte de los ciudadanos y entes de control.

Riesgo(s) Asociado(s):

Obsolescencia y degradación del hardware y software del Instituto, por no mantener actualizado anualmente el inventario de activos de información de la Entidad, de acuerdo con los procesos de identificación de los datos, recursos humanos, documentación, propiedad intelectual, servicios, infraestructura tecnológica del IPES, construcción y/o actualización de los catálogos de la Arquitectura TI: Catálogo de componentes de información, Catálogo de sistemas de información, Catálogo de servicios de TI, Catálogo de elementos de infraestructura on-premise y cloud, Catálogo de servicios de seguridad ,entre estos referidos por la seguridad permitral y de operaciones, como también el inventario de aplicaciones y software instalados en los equipos de cómputo del Instituto, según las bases de datos y el inventario que reporta bienes y servicios de la entidad.

Error humano y acceso inadecuado (eliminación, alteración, corrupción, mala gestión), por no implementar los lineamientos del MSPI y las directrices del Articulo No.6 - Resolución No 500 del 2021 de MinTIC, con la posible afectación de la seguridad CID del Instituto:

a) *Disponibilidad - Perdida de disponibilidad de la infraestructura que soporta los servicios y activos de información de TI.*
b) *Integridad - Perdida de Integridad de la información digital almacenada, procesada y manejada en los sistemas de información misional y administrativos.*
c) *Confidencialidad - Perdida de confidencialidad de: la información digital almacenada, procesada y manejada en los sistemas de información misional y administrativos; y la información del proceso PGSIRT…"*

Normatividad o Criterio:

- PA03-PD-009 V2 Implementación de la Continuidad de la Seguridad de la Información
- La norma ISO 22301:2019 es el estándar internacional para Sistemas de Gestión de Continuidad de Negocio (SGCN)
- Ley 1712 de 2014 - Ley de transparencia y acceso a la información publica
- Resolución No 500 del 2021 de MinTIC (MSPI)
- Resolución No 002277 de 2025 de MinTIC (MSPI)
- ISO/IEC 27001:2022.

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES

Connotación:

Debilidades en la capacidad para mantener la continuidad operativa del negocio y garantizar la seguridad de la información, lo que puede generar vulnerabilidades que pueden comprometer los principios de confidencialidad, integridad y disponibilidad (CID) de la seguridad informática y digital del Instituto, con posibles repercusiones de carácter administrativo, disciplinario y/o fiscal.

Recomendación

- Diseñar e implementar un Plan de Continuidad de la Seguridad de la Información alineado con el PCN institucional, que incluya análisis de impacto (BIA), escenarios de contingencia, procedimientos de recuperación, responsables y recursos críticos.
- Actualizar el inventario de activos de información corte 2025, presentando los soportes y evidencias correspondientes de las gestiones realizadas con los procesos, áreas y/o dependencias en la vigencia 2024 y 2025.
- Identificar los riesgos asociados con seguridad informática, seguridad de la información y seguridad digital teniendo en cuenta los activos de información actualizados corte 2025.
- Rediseñar la matriz de riesgos para reflejar las amenazas reales documentadas y actualizar los planes de tratamiento en consecuencia.
- Integrar el plan dentro del SGSI del IPES, con un enfoque de mejora continua.
- Implementar infraestructura redundante (servidores espejos, failover automático) que garantice la continuidad operativa.
- Realizar simulacros y pruebas periódicas de contingencia que permitan validar la efectividad de los controles y ajustar la estrategia según los resultados obtenidos.

Valoración Comentarios del Auditado

Mediante Memorando con radicado número 10-817-2025-002245 del 21 de julio del 2025, la Subdirección de Diseño y Análisis Estratégico-SDAE, manifiesta lo siguiente**:**

"Los activos de información reportados en el marco de esta auditoría tienen vigencia 2023, por ende, no se logra validar o evaluar si los controles aún preservan las propiedades de seguridad de la información.(…)"

- **Replica GIRT**

Se cuenta con un documentos de activos de información, publicado en el año 2025 en la url https://www.ipes.gov.co/index.php/7-1-instrumentos-de-gestion-de-la-informacion/7-1-1-registro-de-activos-de-informacion

Análisis de la ACI:

Desde la Asesoría de Control Interno se observa que, aunque el proceso manifestó haber publicado los activos de información con corte a 2025 en el enlace del botón de transparencia IPES (ver aquí),

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍAOBSERVACIONES
durante la prueba de recorrido realizada el 2 de julio de 2025 no se presentaron evidencias ni soportes que acrediten la gestión con cada proceso, área o dependencia en lo relacionado con la identificación, clasificación de activos de información y determinación de riesgos de seguridad informática, de la información y digital correspondientes a las vigencias 2024 y 2025. Esta situación refleja un incumplimiento parcial de las actividades definidas en el procedimiento PA03-PD-009 V2, las cuales son esenciales para garantizar la continuidad de la seguridad de la información en el Instituto para la Economía Social – IPES. **Por lo anterior, la observación se mantiene.**

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍA OBSERVACIONES
Nombre del Proceso: Gestión de la Información y de los Recursos Tecnológicos
PA03-DE-007-V7 Plan Tratamiento de Riesgo Seguridad y Privacidad de la Información 2024
***Auditor:* Sergio Andrés Castro Londoño**

OBSERVACIÓN NO.5

Se identificaron deficiencias en la ejecución del Plan de Gestión de Riesgos de Seguridad y Privacidad de la Información, específicamente en el seguimiento y monitoreo de los indicadores establecidos en el documento **PA03-DE-007-V7 – Plan de Tratamiento de Riesgo 2024**, lo que evidencia una gestión parcial e insuficiente de las actividades previstas para mitigar y controlar los riesgos identificados.

Situación(es):

Las debilidades en los procesos de identificación, clasificación y valoración de riesgos de seguridad de la Información en el Instituto para la Economía Social (IPES) son el resultado de deficiencias en la gestión, actualización y control de los activos de información, los cuales son el insumo para su correcta estructuración. La debilidad se presenta en una gestión eficiente de los procesos realizados por la entidad, específicamente en la identificación, clasificación y actualización de activos de información para el periodo 2024-2025, dificulta la correcta identificación de los riesgos y su evaluación adecuada. Esto impide realizar un análisis exhaustivo de los riesgos que podrían comprometer la seguridad de los sistemas, datos sensibles e infraestructuras críticas del Instituto, afectando la capacidad para implementar estrategias de mitigación apropiadas. Como consecuencia, estas deficiencias elevan la exposición del IPES a incidentes de seguridad, como ataques cibernéticos, acceso no autorizado a la información y la pérdida de integridad de los datos.

(*Definición de Activos de Información según la Guía de Administración del Riesgo y Diseño de Controles en Entidades Públicas-DAFP:*

"Un activo es cualquier elemento que tenga valor para la organización, sin embargo, en el contexto de seguridad digital, son activos elementos tales como:

- *Aplicaciones de la organización*

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍA OBSERVACIONES

- *Servicios web*
- *Redes*
- *Información física o digital*
- *Tecnologías de información TI*
- *Tecnologías de operación TO que utiliza la organización para funcionar en el entorno digital " (…))*

En consecuencia de lo anterior, durante la prueba de recorrido realizada en el marco de la auditoría, se evidenciaron debilidades críticas en la implementación y seguimiento del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2024 (PA03-DE-007-V7), las cuales comprometen el cumplimiento de los lineamientos normativos y técnicos establecidos por el marco institucional.

En primer lugar, se verificó que no se realizó seguimiento a los planes de TI definidos en el marco del Decreto 612 de 2018 durante el tercer y cuarto trimestre de 2024, incumpliendo con las obligaciones de monitoreo y gestión de riesgos establecidas para las entidades públicas.

Adicionalmente, no se encontró evidencia documental que respalde la actualización, aprobación y formalización de los mapas de riesgos de gestión correspondientes al tránsito entre las vigencias 2023 y 2024. Aunque en el repositorio institucional (Suite Visión) se identificó el mapa de riesgos correspondiente a 2023 y se suministró por parte del proceso el acta del Comité de Seguridad del 12 de diciembre de 2023, en la que se discutieron lineamientos para 2024, no se hallaron documentos que acrediten la validación ni la aprobación formal de los nuevos mapas de riesgos por parte de los comités competentes (CICCI y/o de Gestión y Desempeño Institucional), situación que representa una omisión en la gestión integral del riesgo y los lineamientos dados a través de la Política de Riesgos IPES.

Si bien se realizaron actividades generales de sensibilización en materia de seguridad de la información y ciberseguridad, no se encontró evidencia de la aprobación formal de los riesgos actualizados ni de los controles definidos para su mitigación, lo que limita la eficacia del proceso de aseguramiento institucional.

Asimismo, aunque se identificaron matrices de riesgos formuladas para 2024, no se evidenció el documento de aceptación de riesgos residuales ni el acto administrativo o técnico que apruebe formalmente el Plan de Tratamiento de Riesgos, tal como lo exigen la norma ISO/IEC 27001:2022 y el Modelo Integrado de Planeación y Gestión (MIPG).

Por otra parte, se verificó la publicación del informe de seguimiento de riesgos en el portal institucional, cumpliendo con las disposiciones de la Ley 1712 de 2014 sobre transparencia y acceso a la información pública. No obstante, al no haberse reportado riesgos materializados durante la vigencia 2024, no fue posible realizar una evaluación objetiva de la efectividad de los controles implementados, ni identificar oportunidades de mejora derivadas de incidentes o simulacros.

Finalmente, se constató la ausencia de seguimiento y monitoreo a los indicadores asociados al plan de tratamiento de riesgos, lo que afecta directamente la trazabilidad de las acciones, dificulta

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍA OBSERVACIONES

la verificación del cumplimiento de los objetivos estratégicos del proceso y debilita la capacidad de mejora continua del sistema de gestión de seguridad de la información del Instituto.

Causa(s):

Las debilidades identificadas en el cumplimiento del Plan de Tratamiento de Riesgos 2024 tienen como causas principales la ausencia de seguimiento efectivo a los planes de TI conforme al Decreto 612 de 2018, la falta de actualización y aprobación formal de los mapas de riesgos entre las vigencias 2023 y 2024, la inexistencia de un documento de aceptación de riesgos residuales, y la carencia de monitoreo sobre los indicadores de gestión del riesgo. Estas omisiones responden, en parte, a la falta de articulación entre las áreas responsables, la ausencia de formalización documental en el marco del MIPG y una limitada cultura de control en materia de seguridad de la información.

Consecuencia(s):

Como consecuencia, se afecta la trazabilidad y efectividad del sistema de gestión del riesgo, se limita la capacidad del Instituto para anticipar, mitigar y responder a amenazas reales sobre los activos de información, y se incumplen los requisitos establecidos por la norma ISO/IEC 27001:2022, comprometiendo la mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI), y elevando la exposición institucional a eventos de ciberseguridad no gestionados.

Riesgo(s) Identificado(s):

Debilidad en el proceso de identificación, clasificación, valoración y tratamiento de riesgos de seguridad informática, seguridad de la información y seguridad digital del Instituto, teniendo en cuenta los activos de información actualizados anualmente de los procesos, áreas y/o dependencias del Instituto.

Normatividad o Criterio:

- PA03-DE-007-V7 Plan Tratamiento de Riesgo Seguridad y Privacidad de la Información 2024.
- Decreto 767 de 2022 - Política de Gobierno Digital
- Decreto 338 de 2022 - Seguridad Digital MinTIC
- Resolución No. 500 de 2021 de MinTIC – MSPI
- Resolución No. 002277 de 2025 de MinTIC – MSPI
- ISO 27001:2022
- ISO 22301:2019
- Guía para la Administración del Riesgo y Diseño de Controles en Entidades Públicas- V6 del Departamento Administrativo de la Función Pública
- PE01-DE-010-Política de Administración del Riesgo IPES Versión 9
-

DESCRIPCIÓN DE LOS RESULTADOS DE AUDITORÍA OBSERVACIONES

Connotación:

Debilidades en los procesos de gestión, administración y tratamiento de riesgos de seguridad, con ocasión a generar posibles vulnerabilidades que puedan afectar los principios CID de la seguridad informática, seguridad de la información, seguridad digital del Instituto, con la posible incidencia administrativa, disciplinaria y/o fiscal.

Recomendación

Realizar seguimiento periódico a los planes estratégicos de TI, conforme a las disposiciones normativas y a las buenas prácticas de gestión establecidas en los marcos de referencia, incluyendo los lineamientos del Decreto 1078 de 2015 (Compilatorio TIC) y los instrumentos de Gobierno Digital expedidos por el MinTIC. Así mismo, como parte del fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI) y de los procesos de tecnología, se sugiere al IPES adoptar mecanismos de control por medio de los cuales se asegure el seguimiento a los planes de TI, incluyendo su integración con los informes de seguimiento del Plan de Acción institucional. Esta actividad deberá incluirse en el Plan de Mejoramiento del SGSI y del proceso de TI, con el fin de garantizar su cumplimiento y trazabilidad.

Valoración Comentarios del Auditado

Revisadas las observaciones de la réplica a través del radicado número 10-817-2025-002245 del 21 de julio del 2025, la Subdirección de Diseño y Análisis Estratégico-SDAE, el proceso auditado reconoce la importancia de realizar un seguimiento periódico a los planes estratégicos de TI, en cumplimiento de las disposiciones normativas y las buenas prácticas de gestión definidas en los marcos de referencia, incluyendo los lineamientos del Decreto 1078 de 2015 (Compilatorio TIC) y los instrumentos de Gobierno Digital expedidos por el MinTIC. Asimismo, como parte del fortalecimiento del Sistema de Gestión de Seguridad de la Información (SGSI) y de los procesos tecnológicos, se adoptarán los lineamientos del MSPI y la norma ISO/IEC 27001:2022, los cuales quedarán integrados al SGSI para garantizar su trazabilidad y seguimiento.

Análisis de la ACI:

Desde la Asesoría de Control Interno se acepta las observaciones presentadas por el proceso auditado, considerando que se reconoce la importancia del seguimiento periódico a los planes estratégicos de TI, en alineación con las disposiciones normativas y las buenas prácticas de gestión, incluyendo los lineamientos del Decreto 1078 de 2015 (Compilatorio TIC) y los instrumentos de Gobierno Digital del MinTIC. Así mismo, se valora la adopción de los lineamientos del MSPI y la norma ISO/IEC 27001:2022, integrándolos al Sistema de Gestión de Seguridad de la Información (SGSI) para fortalecer su trazabilidad y seguimiento**. Por tal razón, la observación se mantiene.**

10. PLAN DE MEJORAMIENTO

La *Subdirección de Diseño y Análisis Estratégico-SDAE* a través del equipo de trabajo de Sistemas , suscribirá un Plan de Mejoramiento con las acciones a seguir en cada una de las observaciones presentadas, y enviarlo a esta Asesoría dentro de los ocho (8) días hábiles siguientes al recibo del Informe de Cierre del trabajo.

La Asesoría de Control Interno-ACI realizará seguimiento al cumplimiento del Plan de Mejoramiento con el fin de asegurar que hayan sido tomadas las acciones definidas por el auditado y corregidos los hallazgos u observaciones.

A continuación se relacionan las observaciones para la suscripción del plan de mejoramiento, teniendo en cuenta que cada observación puede tener más de un área como responsable, sin embargo dado que las mismas tienen un componente técnico y operativo la SDAE/Sistemas tendrá la responsabilidad directa de suscribir acciones de acuerdo a su competencia para lograr subsanar cada una de las situaciones encontrada:

Relación de observaciones y responsables suscripción plan de mejoramiento

N°	OBSERVACIÓN	CONSTRUCCIÓN PLAN DE MEJORAMIENTO SDAE
1	Bajo avance en la implementación del MSPI y brechas significativas frente a los lineamientos normativos y estándares de seguridad de la información en el IPES, en concordancia con las disposiciones dadas en las Resoluciones 500 de 2021 y 2277 de 2025, el Decreto 767 de 2022, así como con los estándares internacionales ISO/IEC 27001, 27005 y 22301.	X
2	Debilidades de seguridad de la información y ausencia de mecanismos seguros y automatizados de intercambio en información en línea entre sistemas internos y externos en la herramienta HEMI, que pueden llegar comprometer los principios de confidencialidad, integridad y disponibilidad (CID).	X
3	Se identificaron debilidades en la gestión de accesos del sistema, reflejadas en la falta de sincronización con el Directorio Activo y la ausencia de mecanismos de autenticación multifactor (2FA/MFA), así como en la inexistencia de procesos de interoperabilidad para el intercambio de información con otros sistemas internos y externos. Asimismo, se evidenció que en la operación GOOBI carece de servidores redundantes, lo que incrementa el riesgo de	X

N°	OBSERVACIÓN	CONSTRUCCIÓN PLAN DE MEJORAMIENTO SDAE
	interrupciones en la continuidad del negocio y puede afectar los principios de confidencialidad, integridad y disponibilidad (CID) de la información.	
4	Debilidades en el cumplimiento de las actividades del procedimiento PA03-PD-009 V2 para garantizar la continuidad de la seguridad de la información en el Instituto para la Economía Social – IPES.	X
5	Se identificaron deficiencias en la ejecución del Plan de Gestión de Riesgos de Seguridad y Privacidad de la Información, específicamente en el seguimiento y monitoreo de los indicadores establecidos en el documento **PA03-DE-007-V7 – Plan de Tratamiento de Riesgo 2024**, lo que evidencia una gestión parcial e insuficiente de las actividades previstas para mitigar y controlar los riesgos identificados.	X
	TOTALES	**5**

Nota: La anterior asignación podrá ser susceptible de cambio durante el ejercicio de suscripción del plan de mejoramiento.

11. ANEXOS

Anexo 1. Papel de Trabajo MSPI - IPES 2025 VF.xlsx
Anexo 2. Mapas de Calor - Riesgos GIRT.xlsx