Código:GE-FR-013
Vigente a partir de: 16/10/2024
Versión: 1

I N F O R M E F I N A L

AUDITORÍA AL PROCESO DE TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES (TICS)

Fecha: 25-07-2025

INFORME "FINAL TICS"

Tabla de contenido

1. Objetivo

Evaluar el cumplimiento normativo en la gestión e implementación de los sistemas de información y la infraestructura tecnológica de FORPO, con el propósito de identificar riesgos y recomendar acciones para la mejora.

2. Alcance

La auditoría se enfocará principalmente en la validación de criterios documentales y jurídicos, debido a la ausencia de personal auditor especializado en ingeniería de sistemas no se evaluarán aspectos técnicos relacionados con el proceso. El proceso auditoría se iniciará con un diagnóstico de la gestión e implementación de las políticas de seguridad digital y privacidad de la información, seguido de la revisión del cumplimiento normativo en relación con el Plan Estratégico de Tecnologías de la Información (PETI) y demás disposiciones TIC aplicables a la entidad. Esta evaluación se realizará conforme a los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

3. Justificación

En cumplimiento del Plan Anual de Auditorías programadas para el 2025, y conforme a las Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna emitidas por el Instituto de Auditores Internos (IIA), la Oficina de Control Interno llevó a cabo un diagnóstico sobre el cumplimiento normativo asociado al proceso de Tecnología de la Información y Comunicaciones (TICS). Esta actividad se enmarca dentro de las funciones de aseguramiento y constituye un paso fundamental para evaluar el estado actual de cumplimiento normativo de la entidad.

El objetivo principal es determinar el nivel de cumplimiento respecto a la normativa vigente en materia de gobierno digital, seguridad de la información, publicidad, interoperabilidad y transparencia, así como identificar oportunidades de mejora que fortalezcan la gestión tecnológica institucional y contribuyan al cumplimiento de los objetivos estratégicos de la entidad.

4. Criterios

- Norma técnica ISO 27001
- Norma Global de Auditoria Interna
- Constitución Política
- Ley 80 de 1993
- Ley 1150 de 1993
- Ley 1474 de 2011

- Ley 1712 de 2014
- Ley 2195 de 2022
- Decreto 1078 de 2015
- Decreto 1499 de 2017
- Caracterización del proceso
- Procedimientos e Instructivos
- Normograma Institucional
- Mapa de riesgos
- Plan de Acción y planes específicos
- Plan de tratamiento de Riesgos de Seguridad y Privacidad de la Información
- Plan de Seguridad y Privacidad de la Información

5. Desarrollo de la auditoría

El 14 de mayo de 2025 se dio apertura a la auditoría que se realizó al proceso de Tecnología de la Información y Comunicaciones (TICS). Durante la reunión inicial se presentó el plan de auditoría, en la misma reunión se presentó el equipo auditor designado y se formalizó el inicio de las actividades mediante la firma del acta de apertura, la carta de compromiso y el acta de representación.

Entre el 14 y el 21 de mayo se llevó a cabo la prueba de recorrido, utilizando la técnica de entrevista dirigida al personal de enlace asignado para atender el proceso de auditoría. Esta prueba tuvo como objetivo que el equipo auditor conociera los aspectos clave del proceso auditado, incluyendo sus actividades críticas, riesgos asociados y controles implementados.

Para la verificación de las acciones relacionadas con la gestión de Tecnología de la Información y Comunicaciones (TICS), se utilizaron como fuentes principales la Suite Visión Empresarial y el sitio Web Institucional.

En cumplimiento del Oficio No. 2025-302-01456-1 de fecha 28 de mayo de 2025 de la DIGEN, se decide por parte del grupo auditor incorporar a la Auditoria la revisión al desarrollo del ERP, para lo cual, se elaboró una encuesta de percepción dirigida a las diferentes subdirecciones y coordinaciones, del mismo surge informe ejecutivo de “Verificación a la Implementación del nuevo ERP en la entidad” y enviado a la Dirección General.

Con base en los procedimientos establecidos en el programa de auditoría, el equipo analizó las evidencias y la documentación recopilada, elaborando el informe final obteniendo los siguientes resultados:

6. Hallazgos

Hallazgo No. 01 – Deficiencias en la gestión y control documental del proceso de Tecnología de la Información y Comunicaciones (TICS)

Condición:

Durante la auditoría al proceso de Tecnología de la Información y Comunicaciones (TICS), se evidenció la inexistencia, desactualización o falta de control documental sobre insumos clave que soportan la gestión técnica, operativa y estratégica del área. No se cuenta con el catálogo de servicios tecnológicos, inventario de información relevante, ni de la política de gobernanza de TI, los cuales fueron solicitados durante la auditoría sin respuesta formal.

El personal del grupo TIC que atendió la Auditoria informó que algunos documentos se encuentran en revisión por parte de la Oficina Asesora de Planeación. También el grupo auditor encontró que mediante Oficio No. 2025-302-00959-1 del 22 de abril de 2025 la Dirección General de la entidad solicitó formalmente la actualización de los documentos antes del 25 de abril de 2025 (fecha prorrogada previamente en dos ocasiones), se comprobó que los siguientes documentos no han sido actualizados ni parametrizados en la herramienta gerencial Suite Visión Empresarial (SVE) al día de finalización de la prueba de recorrido:

Documentos no actualizados:

- Manual del Sistema de Gestión de Seguridad de la Información (SGSI).
- Procedimientos de administración de plataformas TIC, gestión de incidentes, atención a requerimientos, control de cambios.
- Instructivos para el manejo de herramientas críticas.
- Protocolos de configuración y respaldo de bases de datos, protección de datos personales y uso de recursos tecnológicos.
- Catálogo de servicios TIC, inventario de información relevante y política institucional de gobernanza de TI.
- Los referidos en el Oficio No. 2025-302-00959-1 de fecha 22 de abril de 2025.

Criterio:

- Ley 1712 de 2014 – Transparencia y Acceso a la Información
- Ley 594 de 2000 – Gestión Documental
- Ley 1341 de 2009 y Ley 2108 de 2021 – Sociedad de la Información
- CONPES 3975 de 2019 – Política de Gobierno Digital
- Norma ISO 27001 – Controles
- Plan Estratégico Institucional-Objetivo Estratégico “Fortalecer el modelo de direccionamiento estratégico”.

- Modelo Operacional por Procesos (FORPO)
- Plan Estratégico de TI (PETI)
- Mapas de riesgo del proceso TI
- Principios de control interno (COSO – supervisión, evaluación, documentación)

Causa:

- Ausencia de un sistema formal de control documental en el proceso de TI.
- Falta de asignación clara de responsables para la actualización y custodia de los documentos.
- Escasa priorización del mantenimiento del sistema documental y del conocimiento institucional.

- Actualmente no existen controles efectivos que garanticen la generación, validación, publicación, actualización y trazabilidad de los documentos clave del proceso de TI.
- Desconocimiento institucional sobre los servicios TI ofrecidos, limitando la continuidad operativa
- Imposibilidad de aplicar controles adecuados de seguridad sobre la información y los sistemas.
- Incremento del riesgo de errores por uso de documentos obsoletos o inexistentes.
- Pérdida de eficiencia operativa y tiempo por ausencia de lineamientos técnicos claros.
- Posible riesgo digital, identificado por el proceso de Tecnología de la Información y Comunicaciones (TICS) en su mapa de riesgos. Así mismo, la materialización del riesgo estratégico “Posibilidad de pérdida reputacional por resultados en niveles deficientes de las metas y objetivos propuestos debido al incumplimiento de las actividades establecidas en los planes, programas y proyectos”, identificado en el mapa de riesgos de la Oficina Asesora de Planeación. Lo anterior hace referencia al objetivo Fortalecer el modelo de direccionamiento estratégico, actividad para el 2024 “Revisar y actualizar la estructura, los procesos y procedimientos de la entidad”.
- Posibilidad de riesgo “Perdida del conocimiento crítico”, teniendo en cuenta que en algunos casos no se encuentra documentada la información, esto implica que es más probable desconocer la operatividad del proceso lo que no permite brindar un soporte adecuado.

Evidencia:

- Oficio No. 2025-302-00959-1 del 22 de abril de 2025
- Correo electrónico del 27 de mayo de 2025 sin respuesta formal
- Mapas de riesgo del proceso TI y OFPLA.
- Entrevistas al personal TIC y matriz “prueba de recorrido”
- Revisión de la herramienta Suite Visión Empresarial (SVE)

Conclusión del auditor:

La inexistencia y falta de actualización de documentos estratégicos, técnicos y operativos del proceso de TI representa una debilidad significativa en la gestión del conocimiento, la seguridad de la información desconociendo el cumplimiento normativo, que en caso de reiterarse puede poner en riesgo la continuidad y trazabilidad institucional.

Recomendaciones:

1. Asignar responsables definidos por cada documento, con trazabilidad, cronograma de actualización y cumplimiento.
2. Coordinar con la Oficina de Planeación revisiones periódicas e internas sobre la vigencia y suficiencia de la documentación.

Hallazgo 02– Ausencia de implementación de estrategias, y/o servicios digitales de Interoperabilidad.

Condición:

Durante la auditoría al proceso de Tecnología de la Información y Comunicaciones (TICS), se evidenció que la entidad no ha implementado, diseñado y/o actualizado políticas, estrategias y directrices de Interoperabilidad.

Criterio:

1. Decreto 620 de 2020 – Servicios Ciudadanos Digitales
2. CONPES 3975 de 2019 – Política de Gobierno Digital
3. CONPES 4144 de 2025- Política Nacional de Inteligencia Artificial
4. Plan Estratégico Institucional – Objetivo estratégico “Fortalecer la infraestructura tecnológica”.
5. Control ISO 27001

Causa:

- Falta de integración o lineamiento con el marco normativo.
- Falta de suficiencia en los recursos técnicos y presupuestales,
- Ausencia de planificación y controles para la adopción e implementación de herramientas de interoperabilidad. No se evidencia un control formal que garantice la planificación, seguimiento y evaluación del avance en la implementación de estrategias y/o herramientas de Interoperabilidad. No se han definido responsables, ni cronogramas, ni mecanismos para monitorear el cumplimiento de esta obligación normativa.

Efecto:

- Limitación en el intercambio seguro y eficiente de información con otras entidades.
- Afectación en la calidad y oportunidad de los servicios digitales.

Evidencia:

- Correo del Ministerio de Defensa Nacional “Oficio No. 2025-302-00959-1 del 22 de abril de 2025”
- Matriz de Excel recopilación de información de personal del GrupoTIC en prueba de recorrido
- Mapa de riesgos del proceso de TI

Conclusión del auditor:

La ausencia de implementación de herramientas y estrategias de interoperabilidad evidencia una brecha significativa en el cumplimiento de la normatividad vigente y en el avance hacia la transformación digital institucional. Esta situación limita la capacidad del establecimiento para integrarse con otras entidades del Estado y ofrecer servicios más seguros, ágiles y eficientes. Adicionalmente, esta deficiencia representa una posible materialización del riesgo digital identificado por el proceso en su mapa de riesgos, afectando la seguridad, continuidad y eficiencia operativa de la entidad.

Recomendaciones:

1. Fortalecer capacidades técnicas y presupuestales. La entidad debe evaluar y asignar los recursos necesarios (humanos, tecnológicos y financieros) para garantizar la implementación efectiva de soluciones de interoperabilidad, incluyendo la capacitación del personal del Grupo TIC.
2. Diseñar e implementar una estrategia institucional de interoperabilidad formal alineada con el marco normativo vigente, entre otros (Decreto 620 de 2020, CONPES 3975 de 2019, CONPES 4144 de 2025).
3. Establecer herramientas de control que permita hacer seguimiento al avance de la estrategia de interoperabilidad, incluyendo indicadores de cumplimiento, revisión periódica de los resultados, identificación de brechas y medidas correctivas, garantizando así una mejora continua del proceso.

Hallazgo No. 03 – Debilidades en los controles de seguridad informática por gestión parcial de soluciones de protección:

Durante la ejecución de la auditoría al proceso de Tecnología de la Información y Comunicaciones (TICS), se identificó que en varios equipos de cómputo institucionales aparece el mensaje: “Ha expirado la protección del antivirus”. Esta situación persiste desde el cierre de la vigencia 2024 y continúa vigente en 2025, afectando la protección activa de los equipos frente a amenazas cibernéticas. Cabe destacar que el servicio de firewall se encuentra activo, en funcionamiento y contratado hasta diciembre de 2025.

Criterio:

- Norma ISO 27001, (protección contra malware y gestión de la seguridad en redes).
- Política de Seguridad de la Información.
- Mapa de riesgos del proceso de TICS – Riesgo digital: “Ataque Cibernético”.

Causa:

- Falta de gestión oportuna por parte de los intervinientes en el proceso para la renovación o adquisición del antivirus.

- Ausencia de controles que garanticen la continuidad del licenciamiento del software de seguridad.
- Debilidad en el propósito del control proyectado en el mapa de riesgos del proceso “Asegurar que la información sensible y crítica esté protegida contra accesos no autorizados”.

Efecto:

- Exposición directa de los equipos institucionales a amenazas como virus, spyware, ransomware y/o accesos no autorizados.
- Riesgo de pérdida o secuestro de información sensible para la entidad.
- Posibilidad de interrupción de servicios por daños a la infraestructura tecnológica.
- Posibilidad de materialización de riesgo digital “Ataque cibernético” identificado en el mapa de riesgos del proceso.

Evidencia:

- Capturas de pantalla de los mensajes de advertencia en equipos institucionales.
- Mapa de Riesgos del proceso de TI.

Conclusión del auditor:

La expiración de las licencias antivirus en los equipos institucionales representa una vulnerabilidad en la protección frente amenazas cibernéticas, exponiendo la infraestructura tecnológica y la información sensible a posibles ataques, pérdida o manipulación no autorizada. Esta situación refleja una deficiencia en la gestión y control de la seguridad de la información, incumpliendo los requisitos normativos y políticas internas de la entidad. La ausencia de controles preventivos y mecanismos de alerta oportuna ponen en riesgo de interrupciones en los servicios tecnológicos y compromete la continuidad operativa de la entidad.

Recomendaciones:

1. Gestionar de forma inmediata la renovación de las licencias de antivirus, garantizando cobertura institucional.
2. Establecer un plan de contingencia de protección tecnológica, que incluya protocolos de reacción frente a incidentes cibernéticos.
3. Implementar un control automático de monitoreo de licencias para prevenir vencimientos.

Hallazgo 04– Deficiencias en la Implementación de la Infraestructura Tecnológica ERP.

Condición:

En cumplimiento del Oficio No. 2025-302-01456-1 de fecha 28 de mayo de 2025, se solicitó a la Oficina

de Control Interno (OCI) por parte de la DIGEN realizar la verificación del estado de implementación del nuevo Sistema de Planificación de Recursos Empresariales (ERP), derivado del Contrato Interadministrativo No.066-5-2024. La Oficina de Control Interno ante la solicitud relacionada y la ausencia de personal especializado en ingeniería de sistemas que permitiera realizar un seguimiento aplicado y técnico, decidió elaborar y aplicar una encuesta a las dependencias con el objetivo de evaluar la satisfacción en el nivel de implementación del sistema (ERP). Adicionalmente se realizó verificación en la plataforma transaccional de contratación “SECOP II, que permitiera acercar más al grupo auditor a la ejecución del contrato.

Los resultados evidencian que el ERP no ha sido implementado exitosamente, presentándose errores, paralizaciones y trabajo manual en procesos que requieren una atención permanente. Cabe resaltar que del Diagnostico solo participaron algunas coordinaciones como FACON, CRECA, TESOR, TAHUM, OCOIN con las cuales se trabajó, se tomó una muestra e identificó la falta de pruebas formales en la implementación, falta de capacitación y cronogramas validados. En cuanto a CODIN Y OJURI respondieron que no requerían un módulo en el ERP.

Los resultados de los análisis obtenidos a partir de las respuestas recolectadas de las coordinaciones evidencian que el ERP no ha sido implementado exitosamente.

Criterio:

1. ISO 27001, especialmente controles sobre gestión de cambios, continuidad del negocio y seguridad de la información.
2. Contrato Interadministrativo No. 066-5-2024 que regula la adquisición e implementación del ERP.

Causa:

- Poca planificación y gestión integral del proyecto de implementación del ERP, particularmente en lo relacionado con la definición de cronogramas detallados y la realización de pruebas formales de funcionamiento.
- Escasa interacción en los espacios de articulación y coordinación entre el proveedor y los líderes de proceso de las diferentes dependencias, lo que ha limitado la alineación de expectativas y ha impactado negativamente en la efectividad de la implementación.
- Baja presencia del desarrollador y ausencia de personal idóneo designado por este para acompañar técnicamente el proceso de implementación del ERP, lo que limitó el soporte especializado durante etapas críticas del desarrollo y afectó la capacidad de respuesta ante los diferentes incidentes.
- Falta de comunicación fluida y continúa para la resolución oportuna de incidencias y retroalimentación de usuarios.

Efecto:

- Riesgo elevado de interrupción en procesos administrativos, financieros y logísticos, afectando la operatividad institucional.
- Potencial generación de información inconsistente o incompleta que afecta la toma de decisiones.
- El incumplimiento contractual puede generar afectaciones en la ejecución oportuna y eficiente del objeto contractual, lo que puede comprometer el cumplimiento de los fines del ejercicio de la entidad.

Evidencia:

- Requerimiento DIGEN 2025-302-01456-1 de fecha 28 de mayo de 2025.
- Informe remitido a la DIGEN mediante Oficio No. 2025-104-01569-I.
- Informe de supervisión del 12 de junio de 2025 del contrato interadministrativo 066-5-2024

Conclusión del auditor:

El grupo auditor evidenció en el informe de supervisión del 12 de junio de 2025 realizado al contrato Interadministrativo No. 066-5-2024 la supervisión del contrato concluyó que: “*a fecha 31 de mayo no se cumplió con lo relacionado en el cronograma de la tercera prorroga (…)”* Como resultado de este incumplimiento, no se dio concepto favorable a una cuarta prórroga solicitada por el contratista. El supervisor del contrato finaliza esta acción anexando oficio remisorio a la Oficina Asesora Jurídica para iniciar proceso de incumplimiento contra la empresa contratista.

La implementación del ERP presenta deficiencias significativas que impactan negativamente la eficiencia operativa y la continuidad de los procesos de la entidad. La ausencia de controles formales para la planificación, pruebas, capacitación y monitoreo, sumada a la falta de comunicación efectiva entre el proveedor y las dependencias, lo que refleja una gestión inadecuada del proyecto tecnológico situación que genera un riesgo operacional considerable y pone a prueba la confiabilidad del sistema y la información que produce. Se requiere implementar controles robustos que fortalezcan la comunicación interinstitucional y aseguren la participación activa de todas las áreas involucradas ante procesos similares a futuro.

Recomendación:

- Mantener el uso del actual sistema (ERP INFORPO) como plataforma base para la continuidad operativa de los procesos misionales y administrativos de la entidad, mientras el nuevo ERP no se encuentre plenamente implementado y validado en ambiente de producción.

- Establecer una matriz de riesgos operacionales específica para los proyectos de alto impacto institucional, desde la etapa precontractual (fase de planeación), que permita identificar, valorar y mitigar oportunamente los riesgos críticos en la operación. Esta matriz debe contemplar acciones de contingencia ante posibles eventos que comprometan la continuidad operativa y el cumplimiento de los objetivos del proyecto.

- De acuerdo con el informe de 12 de junio de 2025 de la supervisión, iniciar por parte del área jurídica o dar continuidad al procedimiento correspondiente por el presunto incumplimiento de CODALTEC en la ejecución del contrato Interadministrativo No. 066-5-2024, con celeridad., adoptando medidas pertinentes enfocadas a prevenir posibles afectaciones a la entidad.

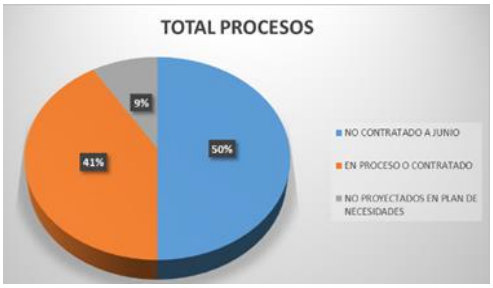
7. Revisión Procesos de Contratación (Vigencia 2025)-TICS

La auditoría revisó el plan de necesidades del Grupo TICS planteado para la vigencia 2025 y se contrasto con la plataforma del SECOP II en lo relacionado con la información o procesos de contratación iniciados con corte al mes de junio. Durante el análisis del plan de necesidades para la vigencia 2025 del Grupo TICS, se identificaron un total de 31 contratos programados hasta el mes de junio, los cuales se encuentran así:

- 17 procesos no han iniciado el trámite de contratación, lo que indica que aún están pendientes de iniciar los procedimientos correspondientes para cumplir lo programado en el plan de necesidades de la vigencia 2025.
- 14 procesos ya iniciaron el proceso de contratación, lo cual muestra que ya están en marcha conforme al plan inicial.
- De otro lado, hay 3 procesos adicionales que no se encontraban inicialmente en el plan de necesidades, pero se ha evidenciado según el registro del SECOP II que se encuentran subidos y presentan actividad.

Representación Grafica

CRITERIO	PROCESOS
NO CONTRATADO A JUNIO	17
EN PROCESO O CONTRATADO	14
NO PROYECTADOS EN PLAN DE NECESIDADES	3



7.1 Observaciones y Consideraciones:

- Se recomienda a las áreas responsables de los procesos contractuales fortalecer la coordinación y comunicación interinstitucional, con el fin de agilizar las etapas previas a la publicación de los procesos en la plataforma SECOP II. Esto incluye la oportuna elaboración de los documentos previos y los necesarios en la publicación de las herramientas dispuestas por Colombia Compra Eficiente. Esta recomendación busca evitar retrasos en la ejecución del Plan de Necesidades 2025, garantizar el cumplimiento de los cronogramas establecidos y permitir una continuidad en los procesos de la entidad, sin que se generen traumatismos.
- Implementar mecanismos que garanticen mayor agilidad en el cargue y publicación oportuna de los procesos contractuales en la plataforma SECOP II. Esto incluye la optimización de los tiempos de revisión documental, la priorización de los procesos conforme al cronograma del Plan de Necesidades 2025, y el fortalecimiento de los procedimientos internos que permitan reducir los tiempos entre la recepción del requerimiento y la publicación del proceso. El cumplimiento de esta recomendación contribuirá a una ejecución más eficiente y oportuna de los recursos, así como al logro de los objetivos institucionales establecidos para la vigencia propuesta.

8. Conclusiones Generales

- Los resultados del informe preliminar fueron presentados y debidamente socializados con el coordinador del proceso, y remitido a través del correo institucional el 10 de julio de 2025, con el fin de que se formularan las observaciones correspondientes y se allegaran las evidencias relacionadas con los hallazgos identificados. No obstante, a la fecha, el equipo auditor no ha recibido respuesta por parte del coordinador del proceso auditado; en consecuencia, y conforme a los procedimientos establecidos, el informe queda en firme.

- Las deficiencias encontradas en el proceso TIC son de carácter estratégico, no meramente técnicos. Estas situaciones afectan la continuidad operativa, la seguridad institucional, el cumplimiento de la normativa y la calidad del servicio a usuarios internos y externos.

- La gestión TIC presenta algunas debilidades estructurales que se deben corregir oportunamente evitando comprometer la misionalidad institucional. Estos hallazgos deben ser abordados en conjunto el área técnica con la Alta Dirección como asuntos prioritarios de gobierno organizacional.

- Gestión Documental Inadecuada en el Proceso de TICS. La falta de control sobre los documentos clave del proceso de TICS, como el manual del SGSI, procedimientos operativos y catálogos de servicios, pone en riesgo la continuidad de los servicios tecnológicos. La ausencia de un procedimiento formal para su actualización y gestión limita la capacidad de la entidad para garantizar la seguridad de la información y la toma de decisiones fundamentadas.

- La ausencia de implementación de herramientas y estrategias de interoperabilidad pude afectar la eficiencia, transparencia y capacidad de interactuar con otras entidades.

- La expiración de las licencias antivirus en varios equipos institucionales expone a la entidad a ciberataques, lo que compromete la seguridad de la información y puede generar interrupciones críticas en la operación de la infraestructura tecnológica.

- La implementación del ERP presenta fallas significativas como errores técnicos por parte del contratista, falta de pruebas, capacitación insuficiente y limitaciones en la comunicación con las dependencias clave. Esto ha generado interrupciones en los procesos administrativos, financieros y logísticos, comprometiendo la operatividad de la entidad.

9. Recomendación General

- Fortalecer la gestión estratégica y operativa de los procesos tecnológicos mediante la definición clara de roles y responsabilidades, la actualización oportuna de la documentación institucional, la implementación de mecanismos de control y seguimiento en proyectos claves como la interoperabilidad y el funcionamiento del ERP, así como el aseguramiento continuo de la infraestructura de ciberseguridad, garantizando la alineación con la normativa vigente y la Política de Gobierno Digital.

- Implementar matriz de riesgos en los procesos TIC de alto impacto para la entidad con el fin de establecer medidas de contingencia y/o mitigación sobre posibles eventos adversos que puedan afectar la operatividad.

- Revisión y fortalecimiento del Mapa de Riesgos TIC que permita incrementar la efectividad de los controles.

- Implementar nuevos controles efectivos con el fin de atacar la probabilidad de ocurrencias.

- Implementar un sistema de indicadores de gestión que permita medir de manera sistemática y objetiva los avances en la formulación, desarrollo y ejecución de políticas y proyectos de Tecnologías de la Información y las Comunicaciones (TIC) dentro de la entidad, con el fin de fortalecer la toma de decisiones, garantizar el cumplimiento de metas institucionales y fomentar la mejora continua.

- Implementar indicadores como mecanismos de control que permitan identificar oportunamente errores, fallas o desviaciones en la operación y funcionamiento de los sistemas, con el objetivo de facilitar una gestión proactiva, garantizar la continuidad del servicio y promover la mejora continua en los procesos tecnológicos.

10. Anexos

- Oficio No. 2025-302-00959-1 del 22 de abril de 2025
- Correo electrónico del 27 de mayo de 2025 sin respuesta formal
- Mapas de riesgo del proceso TI y OFPLA.
- Entrevistas al personal TIC y matriz de “prueba de recorrido”
- Capturas de pantalla de los mensajes de advertencia en equipos institucionales.
- Requerimiento DIGEN 2025-302-01456-1 de fecha 28 de mayo de 2025.
- Informe remitido a la DIGEN mediante Oficio No. 2025-104-01569-I.
- Informe de supervisión del 12 de junio de 2025 del contrato interadministrativo 066-5-2024

Grupo Auditor

Elaborado por:

Adm. Emp. Carol Liliana Reina Díaz

Abogado. Robinson Carranza Romero

Revisado y Aprobado por:
Contador Público. Juan Jairo Gil Rodríguez
Jefe Oficina de Control Interno