MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
Fecha: 2025-12-11 16:37:53 Folios: 1
Radicado: 252209107
Tramite a: ANGELA JANETH CORTES HERNANDEZ
1.0.1. GIT de Seguridad y Privacidad de la Informació

Código TRD:1600

MEMORANDO

PARA: **ANGELA JANETH CORTÉS HERNÁNDEZ**
Coordinadora del GIT de Seguridad y Privacidad de la Información

DE: **JUAN DIEGO TORO BAUTISTA**
Jefe Oficina de Control Interno

ASUNTO: Informe Final Auditoría Interna al Proceso de Seguridad y Privacidad de la Información Vigencia 2025

FECHA: 11 de diciembre de 2025

Respetada ingeniera:

Se remite Informe Final de la Auditoría al Proceso de Seguridad y Privacidad de la Información, realizada por la Oficina de Control Interno en cumplimiento del Programa Anual de Auditoría Interna en la vigencia 2025.

Conforme el procedimiento de Auditoría Interna de Gestión, el plan de mejoramiento frente a los hallazgos detectados debe remitirse para validación dentro de los 10 días hábiles posteriores a este comunicado.

Cordialmente,

(Firmado electrónicamente)
JUAN DIEGO TORO BAUTISTA
Jefe Oficina de Control Interno

Anexo: Informe final Auditoría Proceso Seguridad y Privacidad de la Información.
Elaboró: Rafael Hernando Calle
Revisó: Juan Diego Toro – Jefe Oficina de Control Interno

REGISTRO DE FIRMAS ELECTRONICAS

252209107

Ministerio de Tecnología de la Información y las Comunicaciones
gestionado por: azsign.com.co

Id Acuerdo: 20251211-164105-b38f21-49140906

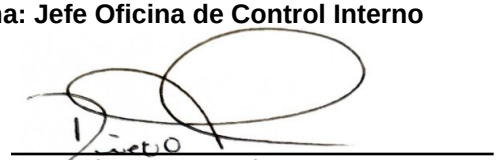
Estado: Finalizado

Creación: 2025-12-11 16:41:05

Finalización: 2025-12-11 16:58:39

Escanee el código para verificación

Firma: Jefe Oficina de Control Interno



Juan Diego Toro Bautista
79569758
jtorob@mintic.gov.co
Jefe de Oficina de Control Interno
Ministerio de Tecnologías de la Información y las Comunicaciones

REPORTE DE TRAZABILIDAD

252209107

Ministerio de Tecnología de la Información y las Comunicaciones
gestionado por: azsign.com.co

Id Acuerdo: 20251211-164105-b38f21-49140906

Estado: Finalizado

Creación: 2025-12-11 16:41:05

Finalización: 2025-12-11 16:58:39

Escanee el código para verificación

TRAMITE	PARTICIPANTE	ESTADO	ENVIO, LECTURA Y RESPUESTA
Firma	Juan Diego Toro Bautista jtorob@mintic.gov.co Jefe de Oficina de Control Interno Ministerio de Tecnologías de la Información y las	Aprobado	Env.: 2025-12-11 16:41:10 Lec.: 2025-12-11 16:58:28 Res.: 2025-12-11 16:58:39 IP Res.: 181.53.156.20 Canal: Email

Informe de Auditoría:
Proceso de Seguridad y Privacidad de la Información

Oficina de Control Interno

Diciembre 2025

Informe de Auditoría

TABLA DE CONTENIDO

1. INTRODUCCIÓN 3
2. OBJETIVOS DE LA AUDITORÍA 3
   2.1. OBJETIVO GENERAL 3
   2.2. OBJETIVOS ESPECÍFICOS 3
3. ALCANCE DE LA AUDITORÍA 3
4. CRITERIOS DE LA AUDITORÍA 4
5. EJECUCIÓN DE LA AUDITORÍA 5
   5.1. TÉCNICAS DE AUDITORÍA 5
   5.2. REUNIÓN DE APERTURA 5
   5.3. REUNIÓN DE CIERRE: 5
   5.4. COMUNICACIÓN DE OBSERVACIONES 6
6. RESULTADOS DE LA AUDITORÍA 6
7. TABLA DE HALLAZGOS IDENTIFICADOS 59
8. FORTALEZAS 68
9. CONCLUSIONES 68
10. RECOMENDACIONES 68
11. PLAZO MÁXIMO PARA ENVÍO DE PLANES DE MEJORAMIENTO: 69

Informe de Auditoría

1. INTRODUCCIÓN

La Oficina de Control Interno del Ministerio de Tecnologías de la Información y las Comunicaciones en desarrollo de su función constitucional y legal, y en cumplimiento de su Programa Anual de Auditoría Interna aprobado en el Comité Institucional de Coordinación de Control Interno - CICCI del 27-02-2025, desarrolló la auditoría al proceso de Seguridad y Privacidad de la Información para el periodo comprendido entre el 01-01-2024 al 30-09-2025. Se utilizarán en este informe las siguientes abreviaturas:

- **FUTIC:** Fondo Único de Tecnologías de la Información y las Comunicaciones.
- **MinTIC:** Ministerio de Tecnologías de la Información y las Comunicaciones.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información.
- **OCI:** Oficina de Control Interno.
- **SPI:** Seguridad y Privacidad de la Información.

2. OBJETIVOS DE LA AUDITORÍA

2.1. Objetivo General

Verificar la implementación y efectividad de una muestra seleccionada de los controles relacionados con Seguridad y Privacidad de la Información - SPI.

2.2. Objetivos Específicos

1. Validar el cumplimiento de las Resoluciones 500 de 2021 "*Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital*" y 2277 de 2025 "*Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia*".

2. Verificar el cumplimiento de las obligaciones de los contratos pertenecientes al proceso, incluyendo la adecuada supervisión de estos.

3. ALCANCE DE LA AUDITORÍA

La auditoría al proceso de Seguridad y Privacidad de la Información comprende el periodo entre el 01-01-2024 al 30-09-2025.

4. CRITERIOS DE LA AUDITORÍA

Marco Jurídico y Normativo:

Leyes:

- Constitución Política de Colombia.
- **Ley 80 de 1993:** Por la cual se expide el Estatuto General de Contratación de la Administración Pública.
- **Ley 87 de 1993:** Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones.
- **Ley 1341 de 2009**: Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–.
- **Ley 1474 de 2011:** Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- **Ley 1978 de 2019:** Por la cual se moderniza el sector TIC, se distribuyen competencias, se crea un regulador único".

Decretos:

- **Decreto 0019 de 2012:** Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.
- **Decreto 1078 de 2015 (DUR-TIC):** "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".
- **Decreto 1082 de 2015**: Por medio del cual se expide el DUR del sector Administrativo de Planeación Nacional.
- **Decreto 1083 de 2015:** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.
- **Decreto 2106 de 2019:** "Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública".
- **Decreto 1064 de 2020:** Por el cual se modifica la estructura del MinTIC.

Resoluciones:

- **Resolución 500 de 2021**: "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital"
- **Resolución 2277 de 2025:** "Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia".

Otros:

- Manual de Contratación GCC-TIC-MA-006.
- Manual de Supervisión e interventoría GCC-TIC-MA-005.

- Procedimiento de Supervisión GCC-TIC-PR-004.
- Carta descriptiva del proceso SPI-TIC-CD-001.
- Mapa de riesgos de Gestión SPI-TIC-DI-012.
- Mapa de riesgos de SPI SPI-TIC-DI-001.
- Manual de Lineamientos de Seguridad para la Protección y Tratamiento de Datos Personales SPI-TIC-MA-002.
- Manual de políticas de SPI SPI-TIC-MA-001.
- Documento Maestro Lineamientos MSPI 2025.

5. EJECUCIÓN DE LA AUDITORÍA

5.1. Técnicas de Auditoría

Para el desarrollo de la auditoría se tuvieron en cuenta los siguientes procedimientos:

- **Consulta:** entrevistas, encuestas, cuestionarios.
- **Inspección:** estudio de documentos, registros y examen físico de recursos tangibles.
- **Revisión de comprobantes**: se realiza específicamente para probar la validez de la información documentada o registrada.
- **Rastreo:** se realiza específicamente para probar la integridad de información documentada o registrada.

5.2. Reunión de Apertura

Fecha: 21-10-2025.
Lugar: Reunión virtual (Teams).

Se realizó la apertura de la auditoría, donde se presentó al equipo auditor, se comunicaron los objetivos, alcance, cronograma e información relevante del plan de auditoría a ejecutar. Se aclararon los aspectos sobre la entrega de evidencias con la oportunidad y completitud de acuerdo con lo establecido en la Carta de Representación firmada por el proceso.

Asimismo, se designó a la ingeniera Angela Janeth Cortés Hernández, como la persona responsable de entregar la información requerida durante la auditoría y se estableció el procedimiento para solicitar dicha información.

5.3. Reunión de Cierre:

Fecha: 09-12-2025.
Lugar: Reunión virtual (Teams).

Se realizó el cierre de la auditoría, donde se presentaron los resultados obtenidos, así como las recomendaciones y fortalezas identificadas del proceso auditado.

5.4. Comunicación de Observaciones

Las observaciones preliminares se dieron a conocer oportunamente al auditado dentro del desarrollo de la auditoría, otorgando el plazo para que se presentaran los argumentos y soportes que permitieran desvirtuar las observaciones comunicadas y ejercer el derecho de contradicción y defensa.

Pese a lo anterior, una vez vencido el plazo inicial y dado que no se recibió ninguna respuesta, el equipo auditor se comunicó e indagó con el proceso informando que ya había finalizado este término; se otorgó un nuevo plazo extraordinario discrecional, sin embargo, vencido este segundo plazo, no se remitieron respuestas específicas, y, por lo tanto, se ratificaron las 22 observaciones preliminares como hallazgos en este informe final:

Observaciones comunicadas	Observaciones excluidas	Total hallazgos del informe final
22 OP - Observaciones preliminares-	Ninguna	22

Tabla 1. Comunicación de observaciones.

6. RESULTADOS DE LA AUDITORÍA

Como resultado de la verificación y análisis documental, se detectaron situaciones en los objetivos específicos de la auditoría. Cada hallazgo redactado contiene la técnica de auditoría utilizada, la situación encontrada, la evidencia que lo soporta y el criterio de auditoría incumplido.

El informe está estructurado conforme a los objetivos definidos en el plan de auditoría y en cada objetivo se encuentra un resumen de las actividades realizadas y los hallazgos identificados.

Como resultado de la revisión de cada objetivo de auditoría se identificaron hallazgos, los cuales corresponden a incumplimientos de un criterio de auditoría (Ley, Manual, Procedimiento, Obligación Contractual, anexos, y/o similares).

Asimismo, se presentan Alertas tempranas, las cuales son situaciones que no tienen un incumplimiento total del criterio evaluado, pero que, sin las adecuadas acciones preventivas (o correctivas), a futuro podrían convertirse en hallazgos potenciales. Para estas en particular, y aunque no es obligatorio de acuerdo con el procedimiento, se recomienda incluirlas dentro del Plan de mejoramiento.

Se presentan las actividades desarrolladas y los resultados obtenidos:

ESPECÍFICO 1. Validar el cumplimiento de las resoluciones *500 de 2021* "*Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital*" y *2277 de 2025* "*Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia*".

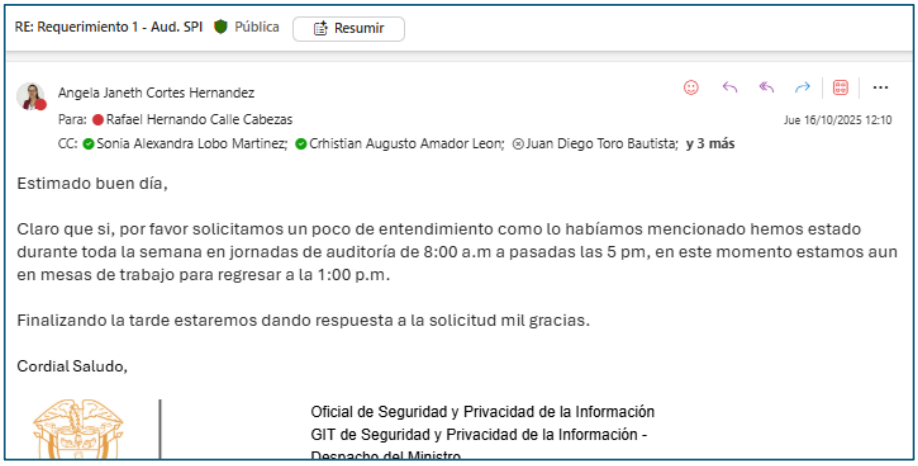
Para desarrollar este objetivo, se realizaron las siguientes solicitudes de información:

- **Requerimiento 1:** Realizado el 06-10-2025, solicitando la contextualización del proceso, incluyendo las líneas y enfoques del proceso, plan sectorial e institucional, plan de SPI, plan de riesgos, plan operativo, manual de políticas de SPI y las Resoluciones 500 de 2021 y 2227 de 2025:

Resolución (muestra)	Descripción (muestra)
Resolución 500 de 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
Resolución 2277 de 2025	Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia
Anexos	Documento Maestro Lineamientos MSPI 2025

Tabla 2. Resoluciones muestra.

La fecha programa de entrega de este requerimiento era el 08-10-2025, sin embargo, el proceso solicitó prórroga hasta el 21-10-2025, es decir, 8 días hábiles adicionales. Finalmente, se aceptó el suministro de la información en dos (2) entregas. La reunión de contextualización se realizó el 10-10-2025; la entrega de la información solicitada en la reunión de contextualización fue entrega solo hasta el 16-10-2025:


RE: Requerimiento 1 - Aud. SPI Pública Resumir

Angela Janeth Cortes Hernandez

Para: Rafael Hernando Calle Cabezas Jue 16/10/2025 12:10

CC: Sonia Alexandra Lobo Martinez; Crhistian Augusto Amador Leon; Juan Diego Toro Bautista; y 3 más

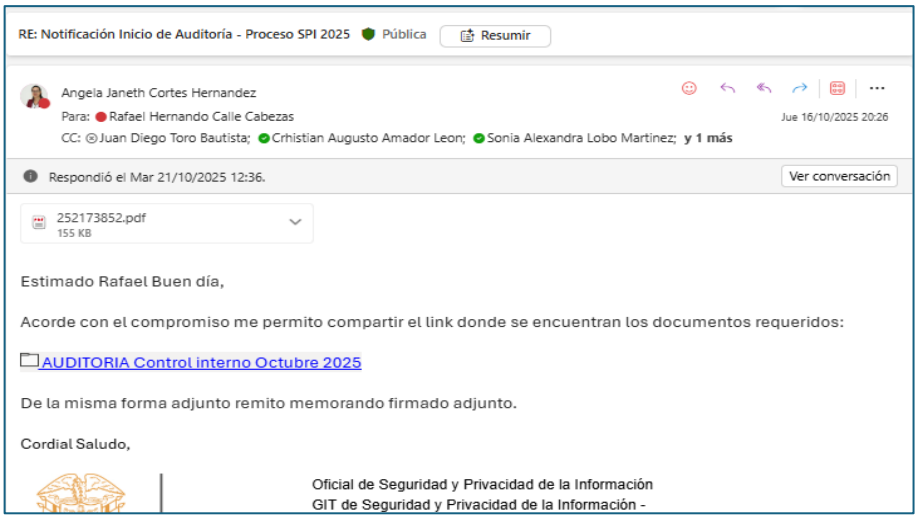
Estimado buen día,

Claro que si, por favor solicitamos un poco de entendimiento como lo habíamos mencionado hemos estado durante toda la semana en jornadas de auditoría de 8:00 a.m a pasadas las 5 pm, en este momento estamos aun en mesas de trabajo para regresar a la 1:00 p.m.

Finalizando la tarde estaremos dando respuesta a la solicitud mil gracias.

Cordial Saludo,

Oficial de Seguridad y Privacidad de la Información
GIT de Seguridad y Privacidad de la Información -
Despacho del Ministro


RE: Notificación Inicio de Auditoría - Proceso SPI 2025 Pública Resumir

Angela Janeth Cortes Hernandez
Para: Rafael Hernando Calle Cabezas
CC: Juan Diego Toro Bautista; Crhistian Augusto Amador Leon; Sonia Alexandra Lobo Martinez; y 1 más
Jue 16/10/2025 20:26

Respondió el Mar 21/10/2025 12:36. Ver conversación

252173852.pdf
155 KB

Estimado Rafael Buen día,

Acorde con el compromiso me permito compartir el link donde se encuentran los documentos requeridos:

AUDITORIA Control interno Octubre 2025

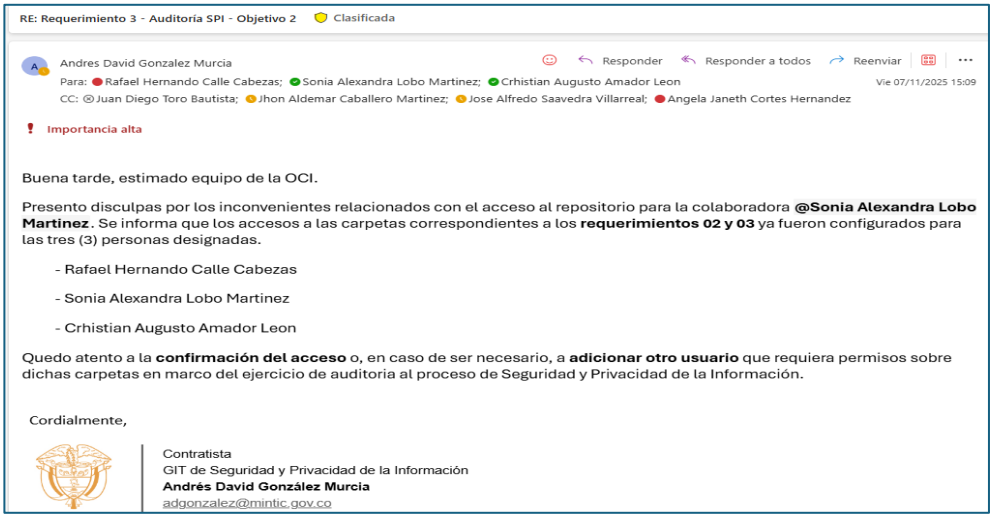
De la misma forma adjunto remito memorando firmado adjunto.

Cordial Saludo,

Oficial de Seguridad y Privacidad de la Información
GIT de Seguridad y Privacidad de la Información -

- **Requerimiento 2:** Realizado el 28-10-2025 en el cual se solicitó evidencias puntuales al cumplimiento de la Resolución 500 de 2021. Se otorgaron 4 días hábiles adicionales, es decir, hasta el 05-11-2025. Se precisa que las rutas de los repositorios donde el proceso suministró las evidencias a los requerimientos iniciales realizados fueron modificadas y el acceso de esta información para el equipo auditor fue impactado. La situación fue superada hasta el 07-11-2025.

- **Requerimiento 4:** Realizado el 05-11-2025 en el cual se solicitó evidencias puntuales al cumplimiento del Anexo 1 de la Resolución 500 de 2021 (actualizada con la Resolución 2277 de 2025) y el Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información.


RE: Requerimiento 3 - Auditoría SPI - Objetivo 2 Clasificada

Andres David Gonzalez Murcia
Responder Responder a todos Reenviar
Para: Rafael Hernando Calle Cabezas; Sonia Alexandra Lobo Martinez; Crhistian Augusto Amador Leon
CC: Juan Diego Toro Bautista; Jhon Aldemar Caballero Martinez; Jose Alfredo Saavedra Villarreal; Angela Janeth Cortes Hernandez
Vie 07/11/2025 15:09

Importancia alta

Buena tarde, estimado equipo de la OCI.

Presento disculpas por los inconvenientes relacionados con el acceso al repositorio para la colaboradora **@Sonia Alexandra Lobo Martinez**. Se informa que los accesos a las carpetas correspondientes a los **requerimientos 02 y 03** ya fueron configurados para las tres (3) personas designadas.

- Rafael Hernando Calle Cabezas
- Sonia Alexandra Lobo Martinez
- Crhistian Augusto Amador Leon

Quedo atento a la **confirmación del acceso** o, en caso de ser necesario, a **adicionar otro usuario** que requiera permisos sobre dichas carpetas en marco del ejercicio de auditoria al proceso de Seguridad y Privacidad de la Información.

Cordialmente,

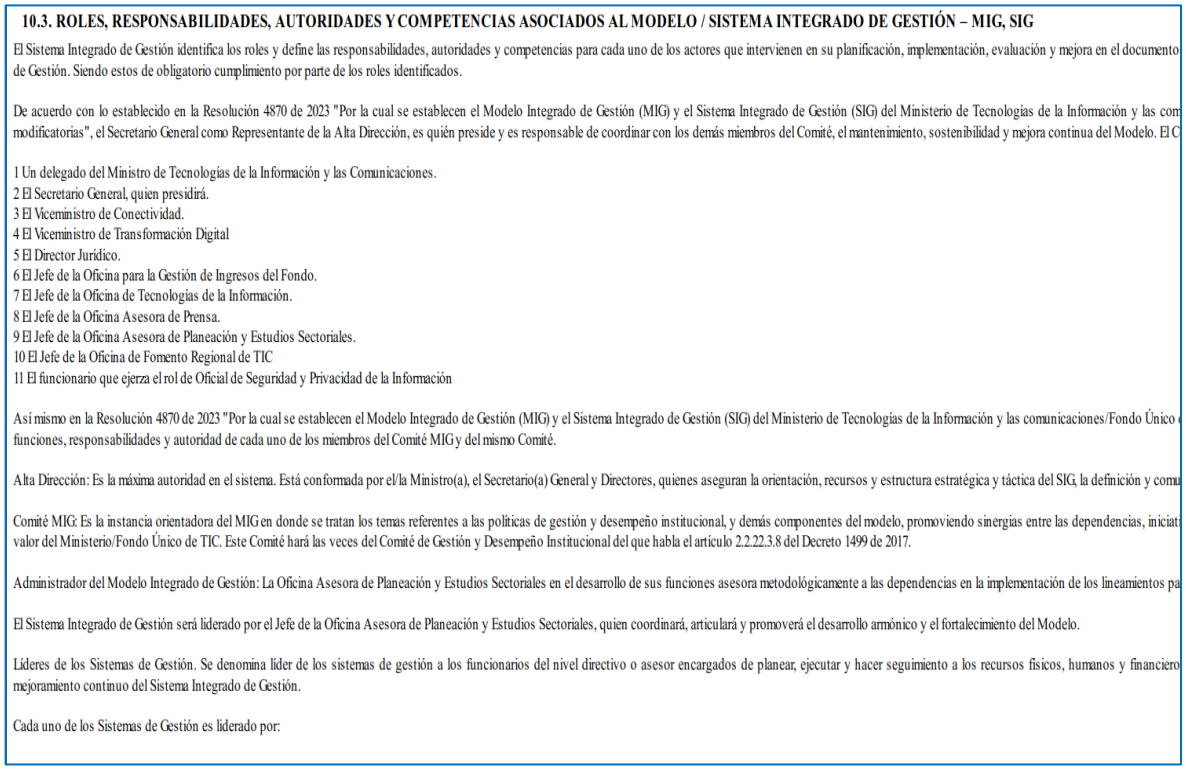
Contratista
GIT de Seguridad y Privacidad de la Información
Andrés David González Murcia
adgonzalez@mintic.gov.co

Como resultado de la validación realizada se obtuvieron los siguientes hallazgos:

Hallazgo 1.1. No se encuentran establecidos los roles y responsabilidades asociados a la seguridad digital

Con el requerimiento 2.1.g se solicitaron los documentos donde se encuentren establecidos los "Roles y responsabilidades asociados a la seguridad digital", para lo cual el proceso remitió como evidencia "*el Manual del MIG donde se definen los roles y responsabilidades del MIG y el SIG en el capítulo 10.3. Roles, responsabilidades, autoridades y competencias asociados al Modelo / Sistema Integrado de Gestión – MIG, SIG*". Al validar este capítulo de este documento, la información que relaciona es:

- Cómo se integra el Comité MIG, en donde se identifica solo el "11 El funcionario que ejerza el rol de Oficial de Seguridad y Privacidad de la Información",
- Líderes de los sistemas de gestión,
- Responsabilidades de los Líderes de Procesos y de los Gestores MIG.



10.3. ROLES, RESPONSABILIDADES, AUTORIDADES Y COMPETENCIAS ASOCIADOS AL MODELO / SISTEMA INTEGRADO DE GESTIÓN – MIG, SIG

El Sistema Integrado de Gestión identifica los roles y define las responsabilidades, autoridades y competencias para cada uno de los actores que intervienen en su planificación, implementación, evaluación y mejora en el documento de Gestión. Siendo estos de obligatorio cumplimiento por parte de los roles identificados.

De acuerdo con lo establecido en la Resolución 4870 de 2023 "Por la cual se establecen el Modelo Integrado de Gestión (MIG) y el Sistema Integrado de Gestión (SIG) del Ministerio de Tecnologías de la Información y las com modificatorias", el Secretario General como Representante de la Alta Dirección, es quién preside y es responsable de coordinar con los demás miembros del Comité, el mantenimiento, sostenibilidad y mejora continua del Modelo. El C

1 Un delegado del Ministro de Tecnologías de la Información y las Comunicaciones.
2 El Secretario General, quien presidirá.
3 El Viceministro de Conectividad.
4 El Viceministro de Transformación Digital
5 El Director Jurídico.
6 El Jefe de la Oficina para la Gestión de Ingresos del Fondo.
7 El Jefe de la Oficina de Tecnologías de la Información.
8 El Jefe de la Oficina Asesora de Prensa.
9 El Jefe de la Oficina Asesora de Planeación y Estudios Sectoriales.
10 El Jefe de la Oficina de Fomento Regional de TIC
11 El funcionario que ejerza el rol de Oficial de Seguridad y Privacidad de la Información

Así mismo en la Resolución 4870 de 2023 "Por la cual se establecen el Modelo Integrado de Gestión (MIG) y el Sistema Integrado de Gestión (SIG) del Ministerio de Tecnologías de la Información y las comunicaciones/Fondo Único funciones, responsabilidades y autoridad de cada uno de los miembros del Comité MIG y del mismo Comité.

Alta Dirección: Es la máxima autoridad en el sistema. Está conformada por el/la Ministro(a), el Secretario(a) General y Directores, quienes aseguran la orientación, recursos y estructura estratégica y táctica del SIG, la definición y comu

Comité MIG: Es la instancia orientadora del MIG en donde se tratan los temas referentes a las políticas de gestión y desempeño institucional, y demás componentes del modelo, promoviendo sinergias entre las dependencias, iniciati valor del Ministerio/Fondo Único de TIC. Este Comité hará las veces del Comité de Gestión y Desempeño Institucional del que habla el artículo 2.2.22.3.8 del Decreto 1499 de 2017.

Administrador del Modelo Integrado de Gestión: La Oficina Asesora de Planeación y Estudios Sectoriales en el desarrollo de sus funciones asesora metodológicamente a las dependencias en la implementación de los lineamientos pa

El Sistema Integrado de Gestión será liderado por el Jefe de la Oficina Asesora de Planeación y Estudios Sectoriales, quien coordinará, articulará y promoverá el desarrollo armónico y el fortalecimiento del Modelo.

Líderes de los Sistemas de Gestión. Se denomina líder de los sistemas de gestión a los funcionarios del nivel directivo o asesor encargados de planear, ejecutar y hacer seguimiento a los recursos físicos, humanos y financiero mejoramiento continuo del Sistema Integrado de Gestión.

Cada uno de los Sistemas de Gestión es liderado por:

Sistema	Líder
Sistema de Gestión de Calidad	Jefe de la Oficina Asesora de Planeación y Estudios Sectoriales o quien haga sus veces.
Sistema de Gestión Ambiental	Subdirector Administrativo o quien haga sus veces
Sistemas de Seguridad y Privacidad de la Información	Oficial de Seguridad y Privacidad de la Información o quien haga sus veces.
Sistema de Gestión de Seguridad y Salud en el Trabajo	Subdirector de Gestión del Talento Humano o quien haga sus veces.
Estrategia Responsabilidad Social Institucional	Subdirector Administrativo o quien haga sus veces.

Responsabilidades de los Líderes de Procesos. Se denomina líder de proceso, de conformidad con el Modelo de Operación por Procesos aprobado mediante Acta de comité MIG N° 25 de septiembre de 2018, funcionario del nivel directivo o asesor, responsables de continuo del Sistema Integrado de Gestión y son sus responsabilidades las siguientes:

a) Dar cumplimiento a las políticas, manuales, programas y demás documentos que orienten el desarrollo de los diferentes sistemas de gestión para garantizar su fortalecimiento y sostenibilidad.
b) Fomentar dentro de sus procesos la apropiación del Modelo Integrado de Gestión de la Entidad.
c) Asegurar la documentación de su proceso, socializar y promover su mejoramiento continuo.
d) Planificar la ejecución de sus procesos teniendo en cuenta los cambios en el contexto interno y externo, los riesgos identificados y las necesidades y expectativas de los diferentes grupos de valor.
e) Identificar y gestionar los riesgos y peligros que afecten su proceso en la entidad de manera articulada, con el fin de mitigarlos y potenciar el cumplimiento de los objetivos definidos en la planeación estratégica.
f) Identificar y gestionar las acciones de mejora generadas en los diferentes niveles en el marco de los procesos.
g) Participar en las actividades definidas por los líderes de los Sistemas de Gestión para la sostenibilidad del Modelo Integrado de Gestión.
h) Apoyar y participar en la formulación de los Planes de Continuidad de la Operación, planes de Emergencias y Simulacros.
i) Revisar, actualizar y aprobar los activos de información identificados para el proceso.
j) Realizar seguimiento control y medición del proceso a su cargo.
k) Apoyar la realización de la revisión por la Dirección del Sistema Integrado de Gestión.
l) Preparar y atender las auditorías internas y externas del SIG relacionadas con su proceso.
m) Promover la gestión del conocimiento y la innovación al interior de su proceso.
n) Establecer el profesional, para el cumplimiento de las responsabilidades como gestor del proceso en la dependencia.

Gestores MIG. son los enlaces responsables de agilizar la gestión de las dimensiones, componentes y requisitos solicitados sobre el MIG. Serán designados por el líder de cada dependencia, grupo interno de trabajo, programa o proyecto. Sus responsabilidades son:

Gestores MIG. son los enlaces responsables de agilizar la gestión de las dimensiones, componentes y requisitos solicitados sobre el MIG. Serán designados por el líder de cada dependencia, grupo interno de trabajo, programa o proyecto. Sus responsabilidades son:

a. Apoyar en sus procesos la apropiación del Modelo Integrado de Gestión y sus atributos de calidad.
b. Gestionar el diseño, creación, implementación y socialización de la documentación de los procesos en el marco del SIG.
c. Promover en sus procesos la identificación y actualización del contexto interno y externo, así como las necesidades y expectativas de los grupos de valor.
d. Apoyar a los líderes de procesos en la correcta gestión del riesgo: identificación, evaluación y seguimiento a controles, definición y seguimiento de planes de tratamiento e identificación y tratamiento de materializaciones.
e. Apoyar la identificación y gestión de las acciones de mejora generadas en los procesos, promoviendo su mejoramiento continuo.
f. Apoyar las estrategias definidas por los líderes de los sistemas de gestión para el fortalecimiento del SIG en la entidad y difundir al interior de sus procesos sus políticas, objetivos y directrices.
g. Participar activamente en las reuniones y sensibilizaciones programadas en el marco del Sistema Integrado de Gestión.
h. Apoyar la preparación y atención de las auditorías internas y externas del SIG.
i. Promover la gestión del conocimiento e innovación al interior del proceso, incluyendo la identificación y documentación de buenas prácticas y lecciones aprendidas.
j. Apoyar la preparación y el envío de la información requerida para la revisión por la Dirección.
k. Apoyar la identificación y actualización de los activos de información identificados en su proceso.
l. Apoyar en la planificación y desarrollo de la continuidad de la operación del Ministerio/Fondo Único de TIC.

Deberes de los colaboradores del Ministerio/Fondo Único de TIC con respecto al MIG. En relación con el MIG se establecen los siguientes deberes de los colaboradores del Ministerio/Fondo Único de TIC:

Aplicar dentro de su gestión los lineamientos del MIG y dar estricto cumplimiento a sus dimensiones.
Apoyar, a través del conocimiento técnico y el soporte administrativo requerido, las acciones de actualización y mejora de las dimensiones que conforman el MIG.
Participar en las jornadas de sensibilización, apropiación y fomento de las dimensiones del MIG y el SIG adelantadas por la Entidad.

Por lo anterior, se identifica que el documento entregado como evidencia no tiene establecidos los roles y responsabilidades asociados a la seguridad digital, conllevando al incumplimiento de lo indicado en el “Documento Maestro Lineamientos MSPI” que establece:

- *7. Fase 1: Planificación: “Documento de roles y responsabilidades asociadas a la **seguridad y privacidad de la Información**”.*
- *7.2.2. Política de seguridad y privacidad de la información: Se deben asignar los roles y responsabilidades que se identifiquen.*
- *7.2.3. Roles y responsabilidades: Salidas: Roles y responsabilidades en seguridad de la información **de las diferentes áreas o procesos de la entidad**.*
- *Anexo A.5.2 Roles y responsabilidades en **la seguridad de la información.** Control: Las políticas para seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.*
- *Documento “Lineamientos de Roles y Responsabilidades”.* (Énfasis fuera de texto)

Hallazgo 1.2. Incumplimiento del artículo 9 de la Resolución 500 de 2021.

Con el requerimiento 2.5.d se solicitó indicar cómo son las clasificaciones de los incidentes de seguridad digital y remitir las evidencias de los reportes o comunicados al CSIRT Gobierno, para lo cual el proceso indicó que:

> "*Se carga en el repositorio el documento de Procedimiento de Gestión de Incidentes de Seguridad y Privacidad de la Información (SPI-TIC-PR-001). En este documento se establece que toda vez que se identifique un incidente de Seguridad Digital* ***grave*** *o* ***muy grave*** *el Oficial de Seguridad y Privacidad de la Información o quien este delegue será el encargado para convocar y reportar el incidente a entes externos entre ellos el CSIRT Gobierno y el ColCERT.*
> *Ahora bien,* ***durante el periodo a evaluar no se han presentado incidentes*** *de Seguridad Digital graves o muy graves que requieran realizar el reporte al CSIRT Gobierno." (Énfasis fuera de texto)*

Al validar las respuestas y evidencias suministradas, se identificó:

Caso 1. No se encuentra documentado cómo están catalogados los incidentes Graves o Muy Graves.

Al validar el procedimiento suministrado (Procedimiento de Gestión de Incidentes de Seguridad y Privacidad de la Información - SPI-TIC-PR-001), no se identifica cómo se clasifican o catalogan los incidentes de seguridad Graves o Muy Graves, y en general las demás clasificaciones.

Lo anterior, en contravía de lo definido en la Resolución 500 de 2021 en el artículo "9. Gestión de incidentes de seguridad digital" en el numeral 3 y del anexo “Lineamientos de Gestión de incidentes de seguridad de la información y seguridad digital” del Documento maestro de lineamientos del MSPI que indican respectivamente:

> "*3. Una vez identificado el incidente de seguridad digital se deberá reportar ante el CSIRT de Gobierno,* ***los incidentes catalogados*** *como Muy Grave y Grave por la entidad, para el respectivo apoyo y coordinación en la gestión de estos a través del formato de reporte establecido por el CSIRT Gobierno, el cual estará disponible por los canales de comunicación del CSIRT Gobierno*". (Énfasis fuera de texto).
> “*Garantizar que los incidentes de seguridad de la información y de seguridad digital (Ciberseguridad) se documenten de manera consistente, utilizando la taxonomía establecida por el COLCERT y estándares apropiados* ***para la categorización, clasificación*** *e intercambio de información producto de la gestión de incidentes*” (Énfasis fuera de texto).

Es importante precisar que es necesario poder contar con un criterio o juicio claro de cómo catalogar los incidentes (Menor, Mayor, Grave, Muy grave, etc.) definidos en la Entidad.

Caso 2: Los incidentes Menos graves o menores no se están comunicando al CSIRT Gobierno.

El proceso indicó que:

> "*Se carga en el repositorio el documento de Procedimiento de Gestión de Incidentes de Seguridad y Privacidad de la Información (SPI-TIC-PR-001). En este documento se establece que toda vez que se identifique un incidente de Seguridad Digital* ***grave*** *o* ***muy grave*** *el Oficial de Seguridad y Privacidad de la Información o quien este delegue será el encargado para convocar y* ***reportar el incidente a entes externos entre ellos el CSIRT Gobierno y*** *el ColCERT. Ahora bien,* ***durante el periodo a evaluar no se han presentado incidentes*** *de Seguridad Digital graves o muy graves que requieran realizar el reporte al CSIRT Gobierno". (Énfasis fuera de texto)*

Con lo anterior, se confirma que solo los incidentes Graves o Muy graves se reportan al CSIRT Gobierno, situación que está en contravía de lo definido en la Resolución 500 de 2021 en el artículo "9. Gestión de incidentes de seguridad digital" que indica en el numeral 4:

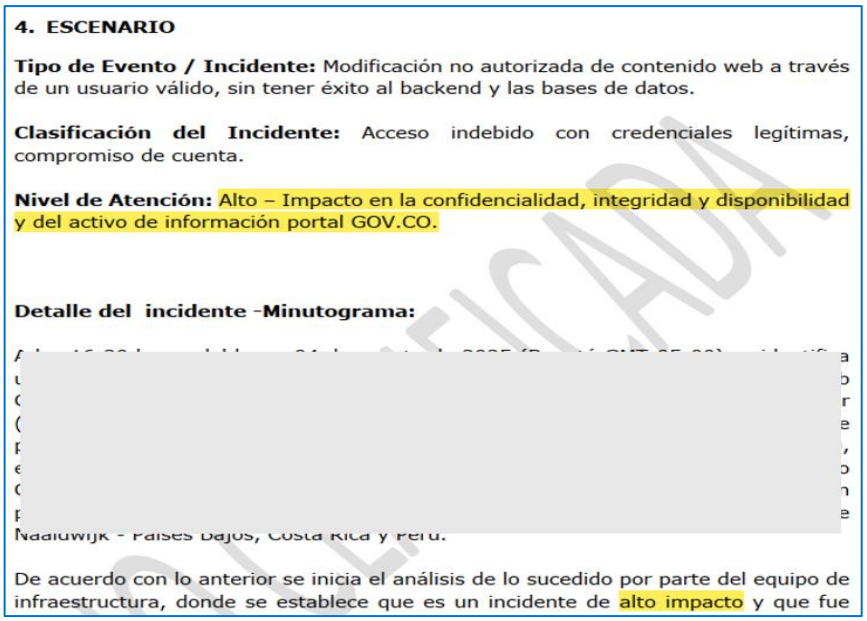
> "*4. Los incidentes catalogados por el responsable de seguridad digital de la entidad,* ***como Menos Grave y Menor, deben ser comunicados al CSIRT Gobierno*** *en el formulario establecido una vez sea gestionado, con el fin de poder llevar una estadística de los incidentes y conocer las tipologías de estos*". (Énfasis fuera de texto).

Asimismo, en el Procedimiento de Gestión de Incidentes de SPI no se identifica, dentro de las actividades, el reporte ante el CSIRT Gobierno de los incidentes Menos Grave y Menor por parte de la Entidad

Caso 3: Se identificaron incidentes Graves o Muy graves no reportados de acuerdo con la clasificación.

El proceso indicó que "*(...) durante el periodo a evaluar no se han presentado incidentes de Seguridad Digital graves o muy graves que requieran realizar el reporte al CSIRT Gobierno*", sin embargo, con las evidencias del punto del requerimiento 2.5.e se remitieron varios documentos y casos que implicaron una gestión operativa de seguridad digital y de SPI, con un compromiso en la integridad, confidencialidad o disponibilidad de la información en la Entidad.

Como ejemplo, se presenta el caso de “GOV.CO” donde se expone el incidente y se cataloga con un Nivel de Atención como “*Alto – Impacto en la confidencialidad, integridad y disponibilidad y del activo de información portal GOV.CO*”, implicando hasta la presentación del caso a la Fiscalía General de la Nación.



4. ESCENARIO

Tipo de Evento / Incidente: Modificación no autorizada de contenido web a través de un usuario válido, sin tener éxito al backend y las bases de datos.

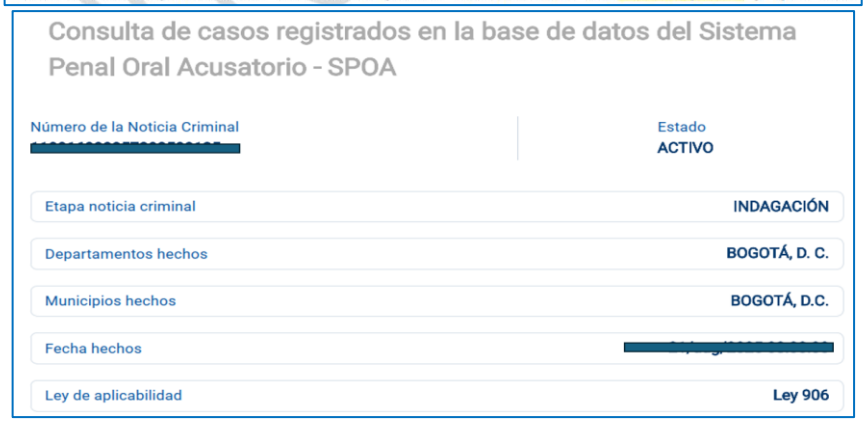
Clasificación del Incidente: Acceso indebido con credenciales legítimas, compromiso de cuenta.

Nivel de Atención: Alto – Impacto en la confidencialidad, integridad y disponibilidad y del activo de información portal GOV.CO.

Detalle del incidente -Minutograma:

[redacted]

De acuerdo con lo anterior se inicia el análisis de lo sucedido por parte del equipo de infraestructura, donde se establece que es un incidente de alto impacto y que fue



Consulta de casos registrados en la base de datos del Sistema Penal Oral Acusatorio - SPOA

Número de la Noticia Criminal	Estado
[redacted]	ACTIVO

Etapa noticia criminal	INDAGACIÓN
Departamentos hechos	BOGOTÁ, D. C.
Municipios hechos	BOGOTÁ, D.C.
Fecha hechos	[redacted]
Ley de aplicabilidad	Ley 906

Caso 4: No se identifican los planes de mejoramiento a los incidentes ni los seguimientos a estos.

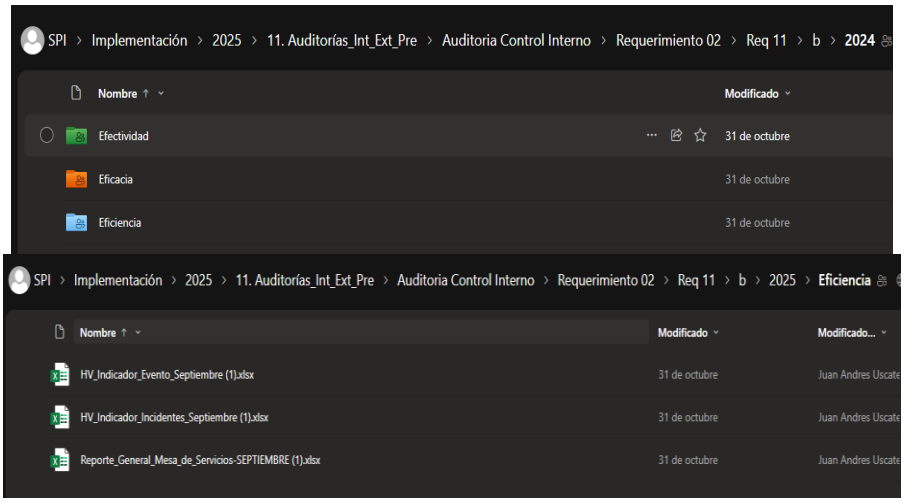
Se solicitó con el requerimiento 2.5.e el suministro de los “Planes de mejoramiento derivados de incidentes y la evidencia de seguimiento”, para lo cual el proceso respondió que: “*En el repositorio se cargan carpeta con la evidencia de seguimiento de los casos reportados*”.

Al validar los soportes suministrados: i) No se identificaron los planes de mejoramiento definidos, ii) Ni acciones de seguimiento de estos casos de incidentes presentados, situación que incumple la Resolución 500 de 2021 en el artículo "9. Gestión de incidentes de seguridad digital" que indica en el numeral 5:

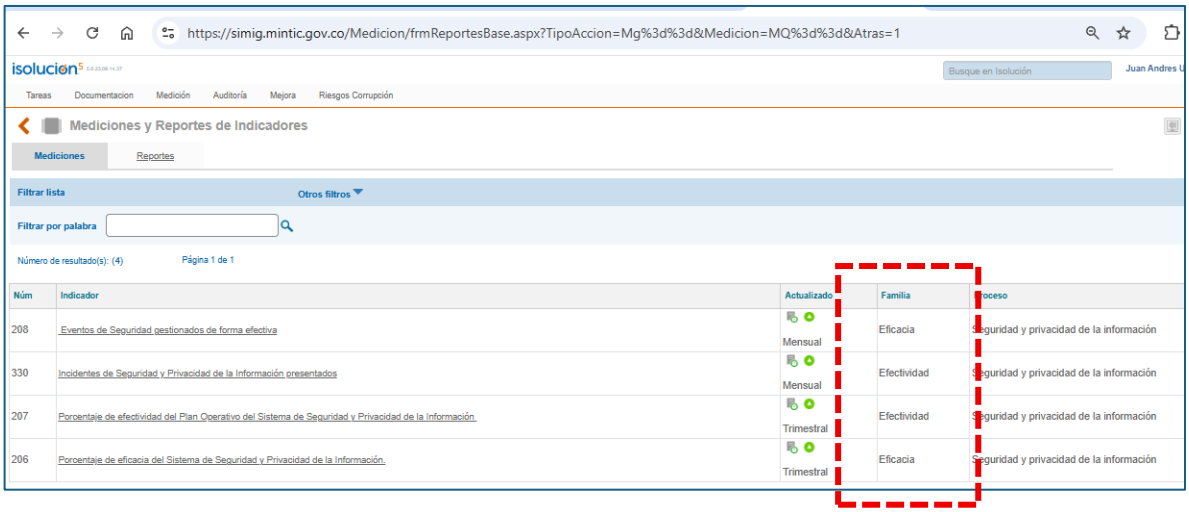
> “*5. Los sujetos obligados, según el análisis e investigación de los incidentes y teniendo en cuenta la causa raíz, deben realizar los respectivos planes de mejoramiento, para lo cual el responsable de seguridad digital de la entidad supervisará y hará seguimiento a su cumplimiento*”.

Hallazgo 1.3. No se identifican indicadores para medir la eficiencia de la gestión de la seguridad de la información y la seguridad digital.

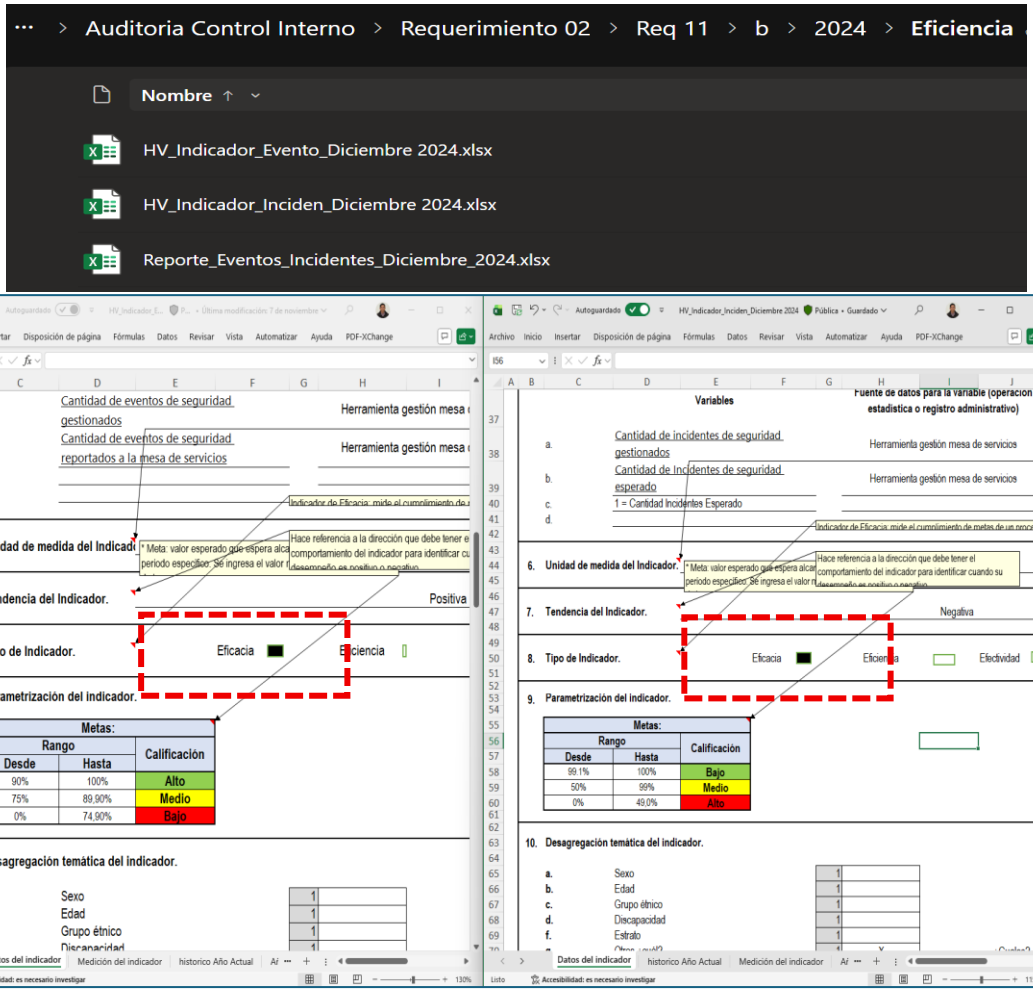
Con el requerimiento 2.11.b se solicitaron los indicadores definidos para medir la eficacia, efectividad y eficiencia de la gestión de la seguridad de la información y la seguridad digital, para lo cual el proceso suministró varios soportes y hojas de vida de los indicadores:



y entre otros, adjuntó la siguiente imagen:



Pese a que, en el soporte anterior, se identifica que no existen indicadores de Eficiencia, se validaron los soportes de los indicadores de “Eficiencia” remitidos para el 2024 y 2025, sin embargo, se evidenció que los mismos corresponden a indicadores para medir la “Eficacia” (“Monitoreo de los incidentes de Seguridad y Privacidad de la Información” y “Monitoreo de los eventos de Seguridad y Privacidad de la Información”) como se observa a continuación:



Por lo anterior, no existen indicadores para medir la Eficiencia de la gestión de la seguridad de la información y la seguridad digital, situación que está en contravía con lo establecido en el artículo 15 de la Resolución 500 de 2021 que indica:

> "*15. Control de las actividades incluidas en la estrategia de seguridad digital y gestión de riesgos. (…)* ***Así mismo, deberán contar con indicadores para medir la eficacia, efectividad y eficiencia de la gestión de la seguridad de la información y la seguridad digital***". (Énfasis fuera de texto).

Hallazgo 1.4. Ausencia de análisis formal, estructurado y verificable de las partes interesadas en seguridad de la información.

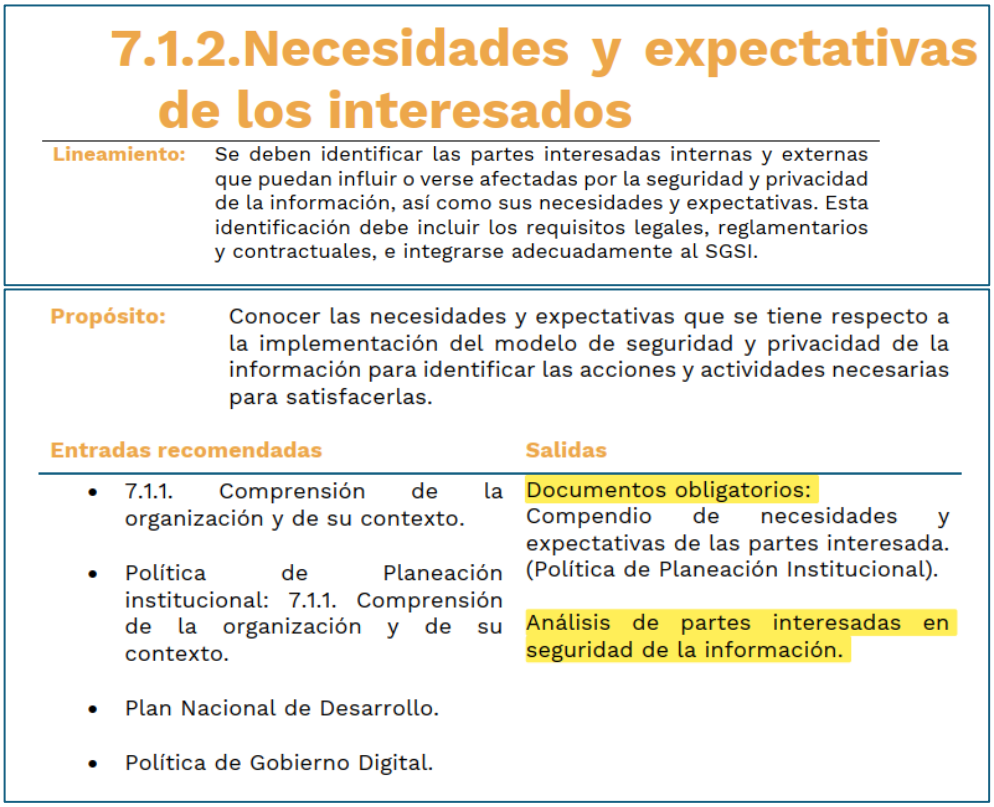
Con los requerimientos 4.3 y 4.4 se solicitó al proceso el "Compendio de necesidades y expectativas de las partes interesadas (Política de Planeación Institucional)" y el "Análisis de partes interesadas en seguridad de la información". En respuesta, el proceso adjuntó el Manual MIG para el punto 3 y no remitió documento formal para el punto 4.

No obstante, el proceso para el punto 4 indicó que se realizaron ajustes en la matriz de requisitos legales, la incorporación de nuevas normativas relacionadas con

inteligencia artificial (Circular Externa 002 de 2024 – SIC y CONPES 4144 de 2025) y definió un plan de acción para abordar aspectos de privacidad, seguridad y gobernanza de IA. Adicionalmente, indicó que envió un correo electrónico a las partes interesadas externas consultando posibles cambios asociados al Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI).

Con la remisión del Manual MIG, la respuesta informada al punto 4 y la consulta por correo realizada frente a las partes interesadas externas, no se cuenta con evidencia suficiente que permita demostrar, entre otros aspectos, la metodología aplicada para identificar y analizar las partes interesadas, los criterios de priorización, las fechas de actualización, la validación formal con las partes interesadas y el control de cambios.

Por lo tanto, no se evidencia un análisis formal, estructurado y verificable de las partes interesadas internas y externas en materia de seguridad y privacidad de la información, situación que conlleva al incumplimiento de la salida documental obligatoria establecida en el lineamiento 7.1.2 “Necesidades y expectativas de los interesados” del Documento Maestro de Lineamientos del MSPI:



7.1.2. Necesidades y expectativas de los interesados

Lineamiento: Se deben identificar las partes interesadas internas y externas que puedan influir o verse afectadas por la seguridad y privacidad de la información, así como sus necesidades y expectativas. Esta identificación debe incluir los requisitos legales, reglamentarios y contractuales, e integrarse adecuadamente al SGSI.

Propósito: Conocer las necesidades y expectativas que se tiene respecto a la implementación del modelo de seguridad y privacidad de la información para identificar las acciones y actividades necesarias para satisfacerlas.

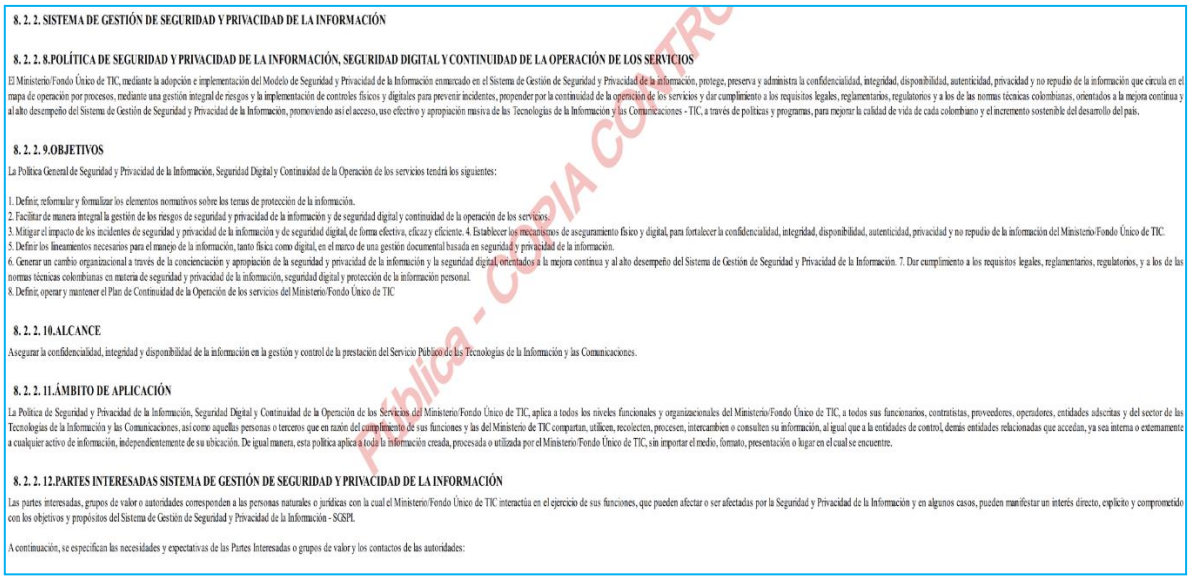
Entradas recomendadas	Salidas
• 7.1.1. Comprensión de la organización y de su contexto. • Política de Planeación institucional: 7.1.1. Comprensión de la organización y de su contexto. • Plan Nacional de Desarrollo. • Política de Gobierno Digital.	Documentos obligatorios: Compendio de necesidades y expectativas de las partes interesada. (Política de Planeación Institucional). Análisis de partes interesadas en seguridad de la información.

Hallazgo 1.5. Falta de delimitación clara del alcance del Modelo de Seguridad y Privacidad de la Información.

Con el requerimiento 4.5 se solicitó indicar el “Alcance del MSPI”, para lo cual el proceso adjuntó como evidencia el documento Manual del MIG (MIG-TIC-MC-001) e indicó que:

> "*El Ministerio/Fondo Único de TIC a través de su Sistema de Gestión de Seguridad y Privacidad de la Información da cumplimiento al Modelo de Seguridad y Privacidad de la Información, es por esto, al igual de que el sistema de gestión, MSPI establece su alcance por medio del documento MIG-TIC-MC-001 – Manual del MIG en su artículo. 2.2.10. Alcance".*

Al validar el documento suministrado y la respuesta, se identificó que, este presenta un apartado denominado "Alcance" (asociado a la política de SPI) y un "Ámbito de Aplicación" (describiendo a quiénes aplica la política), sin embargo, estos no definen el alcance formal del MSPI.



8. 2. 2. SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

8. 2. 2. 8.POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, SEGURIDAD DIGITAL Y CONTINUIDAD DE LA OPERACIÓN DE LOS SERVICIOS

El Ministerio/Fondo Único de TIC, mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información enmarcado en el Sistema de Gestión de Seguridad y Privacidad de la información, protege, preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información que circula en el mapa de operación por procesos, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales para prevenir incidentes, propender por la continuidad de la operación de los servicios y dar cumplimiento a los requisitos legales, reglamentarios, regulatorios y a los de las normas técnicas colombianas, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad y Privacidad de la Información, promoviendo así el acceso, uso efectivo y apropiación masiva de las Tecnologías de la Información y las Comunicaciones - TIC, a través de políticas y programas, para mejorar la calidad de vida de cada colombiano y el incremento sostenible del desarrollo del país.

8. 2. 2. 9.OBJETIVOS

La Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios tendrá los siguientes:

1. Definir, reformular y formalizar los elementos normativos sobre los temas de protección de la información.
2. Facilitar de manera integral la gestión de los riesgos de seguridad y privacidad de la información y de seguridad digital y continuidad de la operación de los servicios.
3. Mitigar el impacto de los incidentes de seguridad y privacidad de la información y de seguridad digital, de forma efectiva, eficaz y eficiente. 4. Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información del Ministerio/Fondo Único de TIC.
5. Definir los lineamientos necesarios para el manejo de la información, tanto física como digital, en el marco de una gestión documental basada en seguridad y privacidad de la información.
6. Generar un cambio organizacional a través de la concienciación y apropiación de la seguridad y privacidad de la información y la seguridad digital, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad y Privacidad de la Información. 7. Dar cumplimiento a los requisitos legales, reglamentarios, regulatorios, y a los de las normas técnicas colombianas en materia de seguridad y privacidad de la información, seguridad digital y protección de la información personal.
8. Definir, operar y mantener el Plan de Continuidad de la Operación de los servicios del Ministerio/Fondo Único de TIC

8. 2. 2. 10.ALCANCE

Asegurar la confidencialidad, integridad y disponibilidad de la información en la gestión y control de la prestación del Servicio Público de las Tecnologías de la Información y las Comunicaciones.

8. 2. 2. 11.ÁMBITO DE APLICACIÓN

La Política de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios del Ministerio/Fondo Único de TIC, aplica a todos los niveles funcionales y organizacionales del Ministerio/Fondo Único de TIC, a todos sus funcionarios, contratistas, proveedores, operadores, entidades adscritas y del sector de las Tecnologías de la Información y las Comunicaciones, así como aquellas personas o terceros que en razón del cumplimiento de sus funciones y las del Ministerio de TIC compartan, utilicen, recolecten, procesen, intercambien o consulten su información, al igual que a la entidades de control, demás entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información, independientemente de su ubicación. De igual manera, esta política aplica a toda la información creada, procesada o utilizada por el Ministerio/Fondo Único de TIC, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

8. 2. 2. 12.PARTES INTERESADAS SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Las partes interesadas, grupos de valor o autoridades corresponden a las personas naturales o jurídicas con la cual el Ministerio/Fondo Único de TIC interactúa en el ejercicio de sus funciones, que pueden afectar o ser afectadas por la Seguridad y Privacidad de la Información y en algunos casos, pueden manifestar un interés directo, explícito y comprometido con los objetivos y propósitos del Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI.

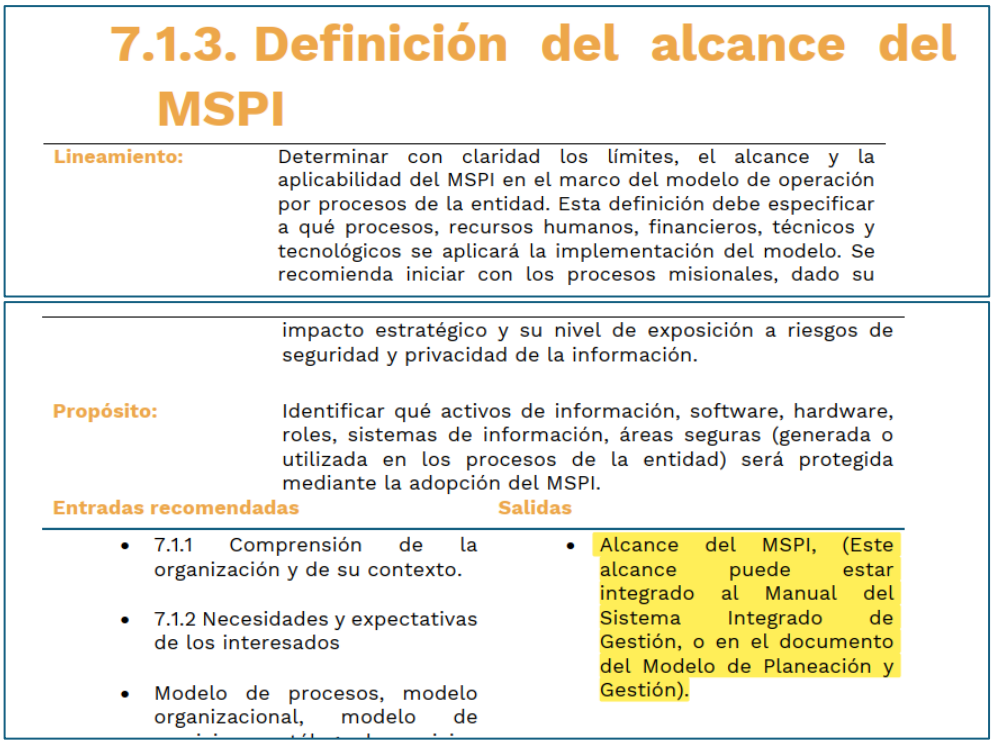
A continuación, se especifican las necesidades y expectativas de las Partes Interesadas o grupos de valor y los contactos de las autoridades:

Es importante mencionar que, de acuerdo con el Documento Maestro de Lineamientos del MSPI, la Política de seguridad y privacidad de la información es un producto del resultado de la implementación del modelo, por lo cual, no debe considerarse que el alcance de la política sea el alcance del MSPI.

El lineamiento 7.1.3 exige que la Entidad defina con claridad los límites, el alcance y la aplicabilidad del MSPI, especificando:

- Procesos (Misionales, estratégicos y de apoyo a los cuales aplica el modelo).
- Recursos humanos, financieros, técnicos y tecnológicos incluidos en la implementación.
- Activos de información, software, hardware, roles, sistemas de información y áreas seguras que serán protegidos mediante el MSPI.
- La existencia del "Alcance del MSPI" como salida obligatoria del lineamiento.

Por lo anterior, no se evidencia el cumplimiento del lineamiento 7.1.3, dado que el documento remitido no cuenta con un alcance formal del MSPI, debidamente estructurado y documentado conforme a lo establecido en el Documento Maestro de Lineamientos:



7.1.3. Definición del alcance del MSPI

Lineamiento:	Determinar con claridad los límites, el alcance y la aplicabilidad del MSPI en el marco del modelo de operación por procesos de la entidad. Esta definición debe especificar a qué procesos, recursos humanos, financieros, técnicos y tecnológicos se aplicará la implementación del modelo. Se recomienda iniciar con los procesos misionales, dado su impacto estratégico y su nivel de exposición a riesgos de seguridad y privacidad de la información.
Propósito:	Identificar qué activos de información, software, hardware, roles, sistemas de información, áreas seguras (generada o utilizada en los procesos de la entidad) será protegida mediante la adopción del MSPI.

Entradas recomendadas	**Salidas**
• 7.1.1 Comprensión de la organización y de su contexto. • 7.1.2 Necesidades y expectativas de los interesados • Modelo de procesos, modelo organizacional, modelo de	• Alcance del MSPI, (Este alcance puede estar integrado al Manual del Sistema Integrado de Gestión, o en el documento del Modelo de Planeación y Gestión).

Hallazgo 1.6. Incumplimiento de la periodicidad en la revisión del MSPI y ausencia de su formalización en la normativa interna y matriz de roles.

Con el requerimiento 4.21 se solicitó al proceso el soporte de todas las revisiones periódicas realizadas en la adopción del MSPI, para lo cual, el proceso remitió como evidencias las actas del Comité MIG No. 80 y No. 92.

Al validar las actas suministradas, se evidenció que:

No se cuenta con evidencia de que la revisión del MSPI se realice con la periodicidad establecida por el Documento Maestro de Lineamientos del MSPI, el cual indica que la revisión de la adopción del MSPI debe realizarse dos veces al año. Las actas aportadas corresponden a reuniones del 06-06-2024 y 21-08-2025.

TIC	ACTA DE REUNIÓN	

CODIGO TRD: 1100.				
ACTA No. 80	**LUGAR:** MinTIC – Virtual	**FECHA:** 06 de junio 2024	**HORA DE INICIO:** 09:00 a.m.	**HORA FINAL:** 11:00 a.m

OBJETO DE LA REUNION
Sesión ordinaria Comité MIG No. 80

ORDEN DEL DÍA

Temas de Aprobación.

1. "Política De Seguridad Y Privacidad de la Información (GIT de Seguridad y Privacidad de la Información)
2. "Política De Tratamiento De Datos Personales" (GIT de Seguridad y Privacidad de la Información)
3. "Solicitud de cambio iniciativa "Fortalecimiento del sector TIC y Postal" Proyecto "Fortalecimiento de la Industria de Telecomunicaciones (CONPES 3983-4109)" (Dirección de Industria de Comunicaciones)
4. Disminución de la meta DATIC y DED en el PES de Formaciones Finalizadas en Habilidades Digitales, a razón de redistribución de la meta a nivel VTD (Dirección de Apropiación TIC-Dirección de Economía Digital)
5. Solicitud de actualización del presupuesto de las iniciativas E1-L2-3000/Capacidades para la resiliencia en Seguridad Digital y E1-L2-4000 Cultura de seguridad digital para prevención y preparación del estado colombiano (Grupo Interno de Trabajo COLCERT)

Temas de Conocimiento.

1. Seguimiento a Indicadores de Fortalecimiento Organizacional (GIT de Transformación Organizacional)
2. Seguimiento a Acciones de Mejora (Oficina Tecnologías de Información)
3. Seguimiento a la Gestión De Riesgos de Gestión, Corrupción y Fiscales (GIT de Transformación Organizacional)
4. Arquitectura de Procesos (GIT de Transformación Organizacional)
5. Evaluación del Desempeño Laboral (Subdirección para la Gestión de Talento Humano)
6. Acuerdos de Gestión (Subdirección para la Gestión de Talento Humano)
7. Estrategia de Divulgación 2024 (Oficina Asesora de Prensa)
8. Balance Estrategia de Comunicaciones (Oficina Asesora de Prensa)
9. Encuesta de Medición (Oficina Asesora de Prensa)
10. Avance Indicadores Código de Buen Gobierno (Oficina Asesora de Planeación y Estudios Sectoriales)
11. Avance Metas Plan Nacional de Desarrollo (Oficina Asesora de Planeación y Estudios Sectoriales)
12. Avance Metas Planes Estratégicos (Oficina Asesora de Planeación y Estudios Sectoriales)
13. Avance Plan de Acción (Oficina Asesora de Planeación y Estudios Sectoriales)
14. Gestión de Riesgos Iniciativas y Proyectos del Plan de Acción (Oficina Asesora de Planeación y Estudios Sectoriales)

TIC	ACTA DE REUNIÓN	

CODIGO TRD: 1100				
ACTA No. 92	**LUGAR:** MinTIC – Virtual	**FECHA:** 21 de agosto 2025	**HORA DE INICIO:** 10:00 a.m.	**HORA FINAL:** 12:00 p.m.

OBJETO DE LA REUNION
Sesión MIG No. 92

ORDEN DEL DÍA

Temas de Aprobación.

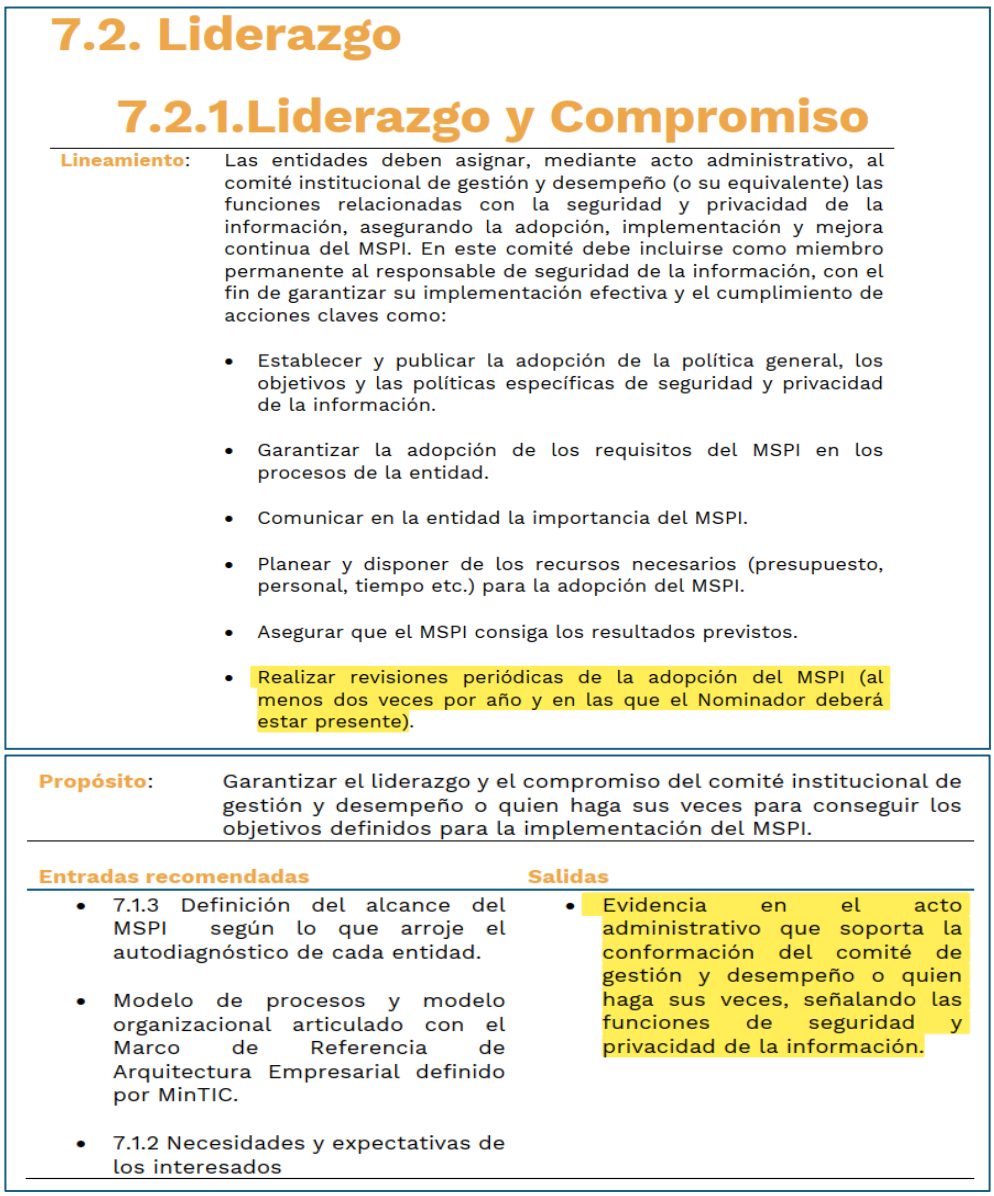
1. Modificación Cronograma de actividades Plan de Bienestar e Incentivos 2025
2. Plan de trabajo cultura, clima e integridad organizacional Ministerio TIC
3. Modificación del Plan de Seguridad y Privacidad de la Información
4. Declaración de Aplicabilidad - SOA
5. Plan para el Fortalecimiento y la Gestión Institucional –FOGEDI 2025
6. Solicitud modificación iniciativa 2025_E1_L1_7000 Fortalecimiento del Sector TIC y Postal

Temas de Conocimiento.

1. Informe consolidado PQRSD
2. Seguimiento a la gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la operación de los servicios – Riesgos de Interrupción
3. Seguimiento Gestión de Eventos e Incidentes de Seguridad y Privacidad de la Información
4. Revisión/Actualización de las Políticas del Sistema de Gestión de Seguridad y Privacidad de la Información
5. Actualización del autodiagnóstico MSPI
6. Seguimiento a la gestión de riesgos
7. Actualización en la iniciativa E2-D2-1000 Estrategia y operación de tecnología para lograr una transformación digital con enfoque social y democrático en la entidad.
8. Actualización en las iniciativas E1-L3-3000 Apropiación TIC para el Cambio y E1-L3-4000/Internet Seguro y Responsable.
9. Indicadores código de Buen Gobierno
10. Avance Metas PND 2022-2026 corte 31 de julio de 2025
11. CIFRAS PES PEI 2T
12. Avances Plan de Acción 2 Trimestre
13. Avance ejecución presupuestal Corte 8 de agosto de 2025
14. Seguimiento Vigencias Futuras Inversión Corte: Cierre julio 2025

Asimismo, al validar la Resolución 860 de 2025 y la Matriz de roles y responsabilidades MIG-TIC-DI-029, no se identificó documentada la acción de realizar revisiones periódicas al menos dos veces por año para la adopción, implementación

y mejora continua del MSPI, incumpliendo con lo establecido en el Documento Maestro del MSPI en el numeral 7.2.1.Liderazgo y compromiso:



7.2. Liderazgo

7.2.1.Liderazgo y Compromiso

Lineamiento: Las entidades deben asignar, mediante acto administrativo, al comité institucional de gestión y desempeño (o su equivalente) las funciones relacionadas con la seguridad y privacidad de la información, asegurando la adopción, implementación y mejora continua del MSPI. En este comité debe incluirse como miembro permanente al responsable de seguridad de la información, con el fin de garantizar su implementación efectiva y el cumplimiento de acciones claves como:

- Establecer y publicar la adopción de la política general, los objetivos y las políticas específicas de seguridad y privacidad de la información.
- Garantizar la adopción de los requisitos del MSPI en los procesos de la entidad.
- Comunicar en la entidad la importancia del MSPI.
- Planear y disponer de los recursos necesarios (presupuesto, personal, tiempo etc.) para la adopción del MSPI.
- Asegurar que el MSPI consiga los resultados previstos.
- Realizar revisiones periódicas de la adopción del MSPI (al menos dos veces por año y en las que el Nominador deberá estar presente).

Propósito: Garantizar el liderazgo y el compromiso del comité institucional de gestión y desempeño o quien haga sus veces para conseguir los objetivos definidos para la implementación del MSPI.

Entradas recomendadas	Salidas
• 7.1.3 Definición del alcance del MSPI según lo que arroje el autodiagnóstico de cada entidad. • Modelo de procesos y modelo organizacional articulado con el Marco de Referencia de Arquitectura Empresarial definido por MinTIC. • 7.1.2 Necesidades y expectativas de los interesados	• Evidencia en el acto administrativo que soporta la conformación del comité de gestión y desempeño o quien haga sus veces, señalando las funciones de seguridad y privacidad de la información.

Hallazgo 1.7. El Manual de Seguridad y Privacidad no fue revisado y aprobado por el Comité de Gestión y Desempeño (Comité MIG).

Respecto de la revisión por parte de la Dirección a la Política y al Manual de Seguridad y Privacidad, con el requerimiento 4.30 se solicitaron los soportes de:

a. Revisiones realizadas.
b. Acta y documento de revisión por la Dirección.
c. Compromisos de la revisión por la Dirección.

Como respuesta, el proceso adjuntó las actas de Comité MIG No. 80 y No. 92, e indicó frente al ítem (c) que "*No se establecen compromisos por la Dirección en los comités #80 y #92*".

El lineamiento 9.3 Revisión por la dirección, establece que:

> "La Política y el **Manual de Seguridad y Privacidad** deben ser **revisados y aprobados por el Comité de Gestión y Desempeño** o por decisión del nominador, considerando los cambios en las necesidades de las partes interesadas. (Énfasis fuera de texto)

Al validar las actas suministradas se identificó que:

- Las actas del Comité MIG No. 80 y No. 92 evidencian que se realizó la revisión y aprobación de la Política de Seguridad y Privacidad de la Información, sin embargo, no se encontró evidencia de revisión, análisis o aprobación del Manual de Seguridad y Privacidad, documento que también debe ser revisado y aprobado conforme al lineamiento.

- La falta de aprobación del Manual de Seguridad y Privacidad y la ausencia de reconocimiento de esta actividad por parte del comité, evidencian debilidades en los compromisos derivados de la revisión efectuada por la Dirección. El documento Maestro del MSPI establece como salida obligatoria los "Compromisos de la Revisión por la Dirección" y, adicionalmente, define como lineamiento que el Manual de Seguridad y Privacidad debe ser revisado y aprobado por el Comité de Gestión y Desempeño, o por decisión del nominador, considerando los cambios en las necesidades de las partes interesadas. En este sentido, se recomienda que en cada revisión periódica de la adopción del modelo se registren de manera clara y formal los compromisos asumidos por el comité, con el fin de asegurar la adecuada evaluación de la conveniencia, adecuación y eficacia del MSPI.

TIC	**ACTA DE REUNIÓN**	MIG

CODIGO TRD: 1100				
ACTA No.	**LUGAR:**	**FECHA:**	**HORA DE INICIO:**	**HORA FINAL:**
92	MinTIC – Virtual	21 de agosto 2025	10:00 a.m.	12:00 p.m.

OBJETO DE LA REUNION
Sesión MIG No. 92

ORDEN DEL DÍA

Temas de Aprobación.

1. Modificación Cronograma de actividades Plan de Bienestar e Incentivos 2025
2. Plan de trabajo cultura, clima e integridad organizacional Ministerio TIC
3. Modificación del Plan de Seguridad y Privacidad de la Información
4. Declaración de Aplicabilidad - SOA
5. Plan para el Fortalecimiento y la Gestión Institucional –FOGEDI 2025
6. Solicitud modificación iniciativa 2025_E1_L1_7000 Fortalecimiento del Sector TIC y Postal

Temas de Conocimiento.

1. Informe consolidado PQRSD
2. Seguimiento a la gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la operación de los servicios – Riesgos de Interrupción
3. Seguimiento Gestión de Eventos e Incidentes de Seguridad y Privacidad de la Información
4. Revisión/Actualización de las Políticas del Sistema de Gestión de Seguridad y Privacidad de la Información
5. Actualización del autodiagnóstico MSPI
6. Seguimiento a la gestión de riesgos
7. Actualización en la iniciativa E2-D2-1000 Estrategia y operación de tecnología para lograr una transformación digital con enfoque social y democrático en la entidad.
8. Actualización en las iniciativas E1-L3-3000 Apropiación TIC para el Cambio y E1-L3-4000/Internet Seguro y Responsable.
9. Indicadores código de Buen Gobierno
10. Avance Metas PND 2022-2026 corte 31 de julio de 2025
11. CIFRAS PES PEI 2T
12. Avances Plan de Acción 2 Trimestre
13. Avance ejecución presupuestal Corte 8 de agosto de 2025
14. Seguimiento Vigencias Futuras Inversión Corte: Cierre julio 2025

TIC	**ACTA DE REUNIÓN**	MIG

CODIGO TRD: 1100.				
ACTA No.	**LUGAR:**	**FECHA:**	**HORA DE INICIO:**	**HORA FINAL:**
80	MinTIC – Virtual	06 de junio 2024	09:00 a.m.	11:00 a.m

OBJETO DE LA REUNION
Sesión ordinaria Comité MIG No. 80

ORDEN DEL DÍA

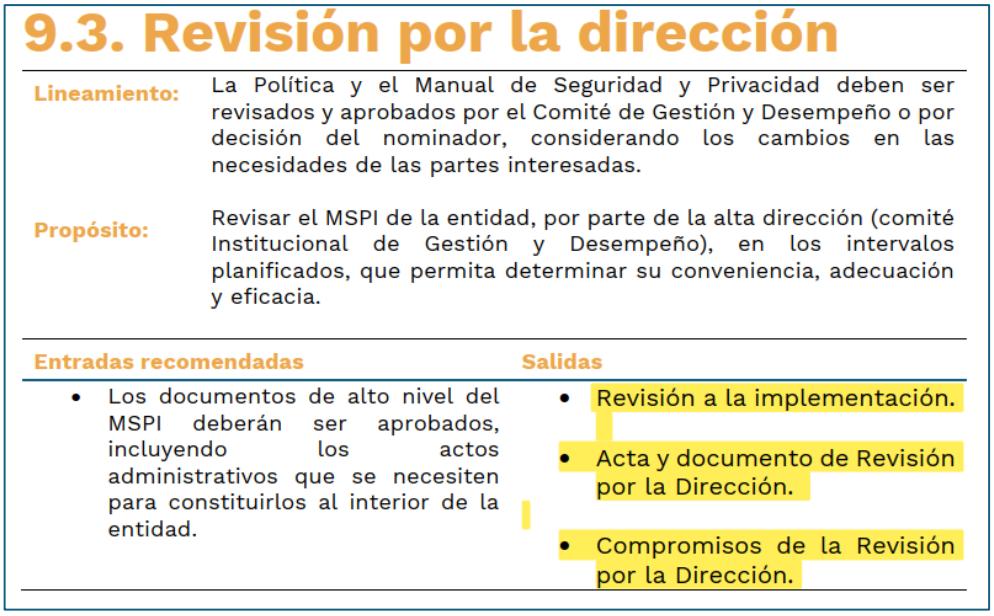
Temas de Aprobación.

1. "Política De Seguridad Y Privacidad de la Información (GIT de Seguridad y Privacidad de la Información)
2. "Política De Tratamiento De Datos Personales" (GIT de Seguridad y Privacidad de la Información)
3. "Solicitud de cambio iniciativa "Fortalecimiento del sector TIC y Postal" Proyecto "Fortalecimiento de la Industria de Telecomunicaciones (CONPES 3983-4109)" (Dirección de Industria de Comunicaciones)
4. Disminución de la meta DATIC y DED en el PES de Formaciones Finalizadas en Habilidades Digitales, a razón de redistribución de la meta a nivel VTD (Dirección de Apropiación TIC-Dirección de Economía Digital)
5. Solicitud de actualización del presupuesto de las iniciativas E1-L2-3000/Capacidades para la resiliencia en Seguridad Digital y E1-L2-4000 Cultura de seguridad digital para prevención y preparación del estado colombiano (Grupo Interno de Trabajo COLCERT)

Temas de Conocimiento.

1. Seguimiento a Indicadores de Fortalecimiento Organizacional (GIT de Transformación Organizacional)
2. Seguimiento a Acciones de Mejora (Oficina Tecnologías de Información)
3. Seguimiento a la Gestión De Riesgos de Gestión, Corrupción y Fiscales (GIT de Transformación Organizacional)
4. Arquitectura de Procesos (GIT de Transformación Organizacional)
5. Evaluación del Desempeño Laboral (Subdirección para la Gestión de Talento Humano)
6. Acuerdos de Gestión (Subdirección para la Gestión de Talento Humano)
7. Estrategia de Divulgación 2024 (Oficina Asesora de Prensa)
8. Balance Estrategia de Comunicaciones (Oficina Asesora de Prensa)
9. Encuesta de Medición (Oficina Asesora de Prensa)
10. Avance Indicadores Código de Buen Gobierno (Oficina Asesora de Planeación y Estudios Sectoriales)
11. Avance Metas Plan Nacional de Desarrollo (Oficina Asesora de Planeación y Estudios Sectoriales)
12. Avance Metas Planes Estratégicos (Oficina Asesora de Planeación y Estudios Sectoriales)
13. Avance Plan de Acción (Oficina Asesora de Planeación y Estudios Sectoriales)
14. Gestión de Riesgos Iniciativas y Proyectos del Plan de Acción (Oficina Asesora de Planeación y Estudios Sectoriales)

Por lo anterior, la situación mencionada se encuentra en contravía del lineamiento 9.3 Revisión por la dirección, el cual establece que el Manual de Seguridad y Privacidad debe ser revisado y aprobado por el Comité de Gestión y Desempeño, incluyendo los compromisos de la revisión por la dirección.



9.3. Revisión por la dirección

Lineamiento:	La Política y el Manual de Seguridad y Privacidad deben ser revisados y aprobados por el Comité de Gestión y Desempeño o por decisión del nominador, considerando los cambios en las necesidades de las partes interesadas.
Propósito:	Revisar el MSPI de la entidad, por parte de la alta dirección (comité Institucional de Gestión y Desempeño), en los intervalos planificados, que permita determinar su conveniencia, adecuación y eficacia.

Entradas recomendadas	Salidas
• Los documentos de alto nivel del MSPI deberán ser aprobados, incluyendo los actos administrativos que se necesiten para constituirlos al interior de la entidad.	• Revisión a la implementación. • Acta y documento de Revisión por la Dirección. • Compromisos de la Revisión por la Dirección.

Hallazgo 1.8. Ausencia del Plan Anual de Mejora del MSPI.

Con el requerimiento 4.31 se solicitó al proceso el "Plan Anual de Mejora del MSPI" y como respuesta, se remitieron: El Instrumento de Autodiagnóstico MSPI, el documento denominado "Plan de Implementación Seguimiento_2025" y el "Plan de SPI – Vigencia 2025", y se explicó que:

> *"Teniendo en cuenta que el MSPI está soportado en la implementación del SGSPI, el seguimiento a este plan está inmerso en el seguimiento a las actividades definidas en el Plan de Seguridad y Privacidad de la información donde a través de diferentes actividades y tareas de varias gestiones se soporta la implementación y el mantenimiento del sistema de gestión. Su evaluación a nivel de resultados se ve reflejado en el avance del autodiagnóstico del MSPI y en el nivel de madurez que se identifica en este instrumento, al igual que el resultado de las diferentes auditorias de certificación."*

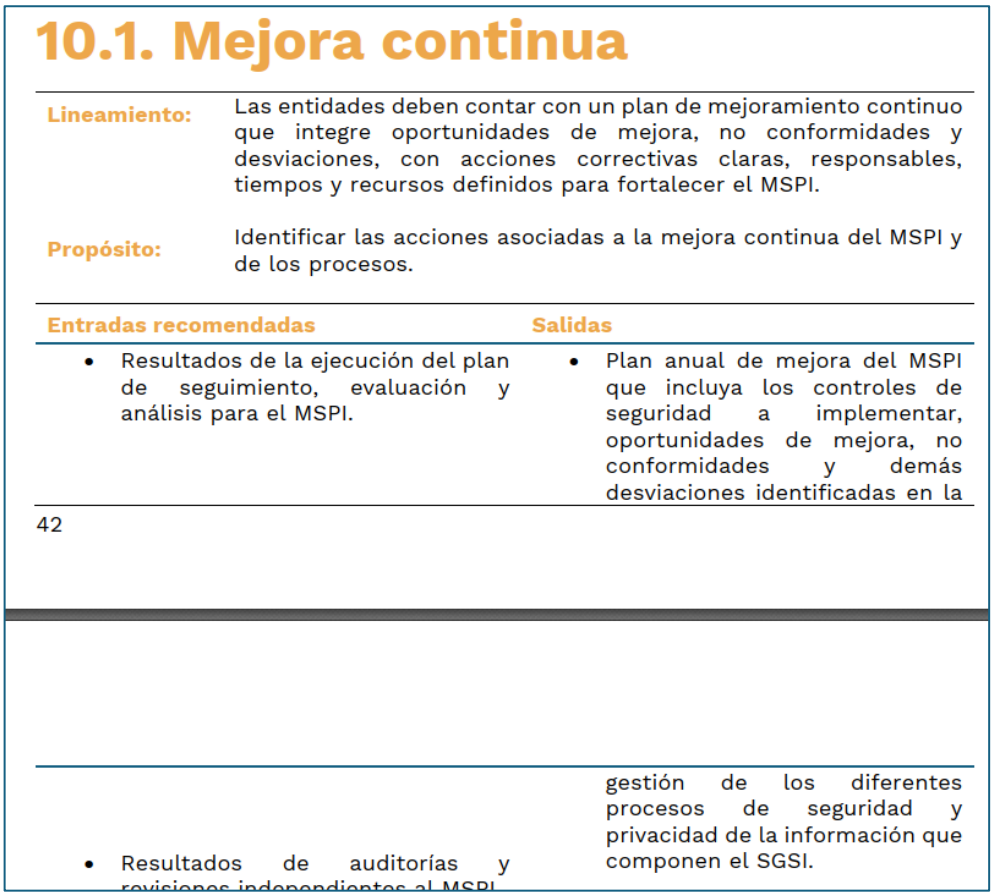
El capítulo 10.1 Mejora continua establece que:

> *"Las entidades deben contar con un plan de mejoramiento continuo que integre oportunidades de mejora, no conformidades y desviaciones, con acciones correctivas claras, responsables, tiempos y recursos definidos para fortalecer el MSPI.*
> *Salida: Plan anual de mejora del MSPI que incluya los controles de seguridad a implementar, oportunidades de mejora, no conformidades y demás*

desviaciones identificadas en la gestión de los diferentes procesos de seguridad y privacidad de la información que componen el SGSI."

Al validar los documentos suministrados se identificó que no existe un Plan Anual de Mejora del MSPI. Adicionalmente, las evidencias entregadas corresponden a documentos que contienen actividades operativas del SGSI, pero no cumplen con los elementos exigidos para el Plan de Mejora del MSPI, dado que no consolidan oportunidades de mejora identificadas, no incluyen no conformidades, desviaciones o brechas específicas, no contienen acciones correctivas formales, ni su trazabilidad, no especifican responsables, tiempos, recursos, ni articulan la mejora continua como un plan anual integral, y en general, no contienen los mecanismos de seguimiento, tal como lo exige el modelo.

Lo anterior incumple lo establecido en el lineamiento 10.1 Mejora Continua, el cual define que las entidades deben contar con un Plan de mejoramiento continuo que integre de manera formal las oportunidades de mejora, las No conformidades y las desviaciones identificadas en la gestión de los diferentes procesos de seguridad y privacidad de la información que componen el SGSI.



10.1. Mejora continua

Lineamiento:	Las entidades deben contar con un plan de mejoramiento continuo que integre oportunidades de mejora, no conformidades y desviaciones, con acciones correctivas claras, responsables, tiempos y recursos definidos para fortalecer el MSPI.
Propósito:	Identificar las acciones asociadas a la mejora continua del MSPI y de los procesos.

Entradas recomendadas	Salidas
• Resultados de la ejecución del plan de seguimiento, evaluación y análisis para el MSPI.	• Plan anual de mejora del MSPI que incluya los controles de seguridad a implementar, oportunidades de mejora, no conformidades y demás desviaciones identificadas en la gestión de los diferentes procesos de seguridad y privacidad de la información que componen el SGSI.
• Resultados de auditorías y revisiones independientes al MSPI	

42

Alertas tempranas

Adicional a los hallazgos anteriormente indicados, se identificaron situaciones que no tienen un incumplimiento total del criterio evaluado, pero que sin las adecuadas acciones preventivas a futuro podrían convertirse en hallazgos potenciales. A continuación, se describen y detallan cada una:

Alerta temprana 1: El análisis del contexto publicado tiene fechas posteriores previo a los mapas de riesgos.

Con el requerimiento 2.1.e se solicitaron los documentos del Establecimiento del Contexto del Proceso de Seguridad y Privacidad de la Información, especificando las versiones y las fechas de publicación. Se realiza la validación a todos los procesos de la entidad, para verificar que se haya realizado el proceso de Gestión de riesgos de SPI de acuerdo con los "Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas".

Inicialmente, se solicitó a la OAPES el cronograma de actualización de riesgos 2025 en la Entidad, para lo cual, se entregó el memorando radicado 252028070 del 19-02-2025 en el que se notificó a todos los procesos sobre la actualización de los riesgos, incluidos los de SPI, y en el Anexo 2 se adjuntaba el cronograma de actividades lideradas por el GIT de SPI para la actualización de riesgo de SPI:

Anexo 2. Cronograma de actividades y proyección de cronograma de Mesas de Trabajo para la actualización Perfil de Riesgo de Riesgo de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios (riesgos de interrupción) 2025.

Gestión	Actividades	Tareas	Responsable de la Tarea	Fechas Programación Tareas	
				Fecha Inicio	Fecha Final
	Sensibilización	Socialización de lineamientos y herramienta para la Gestión de Riesgos de Seguridad y privacidad de la Información y Seguridad Digital	Equipo de Gestión de Riesgos SPI	17-mar-25	31-may-25
	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	Contexto, Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información y Seguridad Digital	Equipo de Gestión de Riesgos SPI Líderes, Gestores y equipo de trabajo del Proceso	17-mar-25	18-jul-25
		Realimentación, revisión y verificación de los riesgos identificados (Ajustes)	Equipo de Gestión de Riesgos SPI Líderes, Gestores y equipo de trabajo del Proceso	28-abr-25	18-jul-25
Gestión de Riesgos	Aceptación de Riesgos Identificados	Aceptación, aprobación riesgos identificados y planes de tratamiento	Equipo de Gestión de Riesgos SPI Líderes, Gestores y equipo de trabajo del Proceso	5-may-25	26-jul-25
	Publicación	Publicación mapas de riesgos de los procesos en SIMIG	Gestor del Proceso	9-jun-25	31-jul-25
	Seguimiento Fase de Tratamiento	Seguimiento implementación de controles y planes de tratamiento de riesgos los identificados (verificación de evidencias)	Equipo de Gestión de Riesgos SPI	20-ene-25	26-dic-25
	Monitoreo y Revisión	Medición, presentación y reporte de indicadores	Equipo de Gestión de Riesgos SPI	20-ene-25	26-dic-25

Este cronograma está alineado al Plan de SPI vigencia 2025. Al validar los documentos como resultado del ejercicio ("Establecimiento del contexto" y "Mapa de Riesgos SPI") para cada proceso, se identificó que, en algunos de ellos la fecha de

aprobación en SIMIG, del establecimiento del contexto, es superior a la fecha de aprobación en SIMIG del mapa de riesgos de SPI:

Establecimiento del contexto			Mapa de Riesgos SPI		
Proceso	Fecha creación	L M D_ Revisa	Version	Fecha Creación	Fecha Aprobacion
Arquitectura Empresarial	25/sept./2025	02/oct./2025	5	11/abr./2025	14/abr./2025
Gestión de Compras y Contratación	30/sept./2025	16/oct./2025	8	19/may./2025	27/may./2025
Gestión Financiera	25/sept./2025	14/oct./2025	8	28/abr./2025	19/may./2025
Planeación y Formulación de Políticas TIC	25/sept./2025	01/oct./2025	9	30/abr./2025	16/may./2025
Uso y Apropiación de las TIC	23/sept./2025	01/oct./2025	8	30/jul./2025	20/ago./2025

Arquitectura Empresarial

Proceso	Codigo	Titulo Documento	Plantilla	Version	Fecha Creación	L M D_ Revisa	L M D_ Aprueba	Fecha Aprobacion	Elaboro
Arquitectura Empresarial	AEM-TIC-DI-004	Establecimiento del contexto del Proceso Arquitectura Empresarial	Documento Interno	3	25/sept./2025	Javier Linares Palomino,Guillermo Adolfo Bernal Pedraza,Susen Dayana Mateus Vargas	Andres Diaz Molina,Juddy Alexandra Amado Sierra	02/oct./2025	Diego Alejandro Duque Duque
Arquitectura Empresarial	AEM-TIC-DI-001	Mapa de Riesgos Arquitectura Empresarial	Documento Interno	4	26/nov./2024	Claudia Yanet Dantonio Adame,Joseth Steven Tibaduiza Celeita,Sandra Del Pilar Arteaga Vela,Carolina Castañeda de Avila	Andres Diaz Molina,Juddy Alexandra Amado Sierra	02/dic./2024	Diego Alejandro Duque Duque
Arquitectura Empresarial	AEM-TIC-DI-002	Mapa de Riesgos SPI - Arquitectura Empresarial	Documento Interno	5	11/abr./2025	Javier Linares Palomino,Giovanni Andres Espitia Roa,Susen Dayana Mateus Vargas	Andres Diaz Molina,Juddy Alexandra Amado Sierra	14/abr./2025	Diego Alejandro Duque Duque

Compras y contratación

Número de resultado(s): (4) Página 1 de 1

Proceso	Codigo	Titulo Documento	Plantilla	Version	Fecha Creación	L M D_ Revisa	L M D_ Aprueba	Fecha Aprobacion	Elaboro
Gestión de Compras y Contratación	GCC-TIC-DI-007	ESTABLECIMIENTO DEL CONTEXTO DEL PROCCESO DE GESTIÓN DE COMPRAS Y CONTRATACIÓN	Documento Interno	3	30/sept./2025	Yomaira Esperanza Rodriguez Pinzon,Arlex Jonathan Rios,Loreine Angelica Viana Rua,Susen Dayana Mateus Vargas	Gina del Rosario Nuñez Polo,Juliana Fernanda Ramirez Zambrano,Juddy Alexandra Amado Sierra	16/oct./2025	Nubia del Carmen Camacho
Gestión de Compras y Contratación	GCC-TIC-DI-004	Mapa de Riesgos Gestión de Compras y Contratación	Documento Interno	6	01/abr./2025	Esmeralda Carolina Orduz Olaya,Arlex Jonathan Rios,Loreine Angelica Viana Rua,Yomaira Esperanza Rodriguez Pinzon,Carolina Castañeda de Avila	Gina del Rosario Nuñez Polo,Juliana Fernanda Ramirez Zambrano,Juddy Alexandra Amado Sierra	25/abr./2025	Nubia del Carmen Camacho
Gestión de Compras y Contratación	GCC-TIC-DI-006	Mapa de Riesgos SPI - Gestión de Compras y Contratación	Documento Interno	8	19/may./2025	Yomaira Esperanza Rodriguez Pinzon,Arlex Jonathan Rios,Giovanni Andres Espitia Roa,Carolina Castañeda de Avila	Gina del Rosario Nuñez Polo,Juliana Fernanda Ramirez Zambrano,Juddy Alexandra Amado Sierra	27/may./2025	Nubia del Carmen Camacho

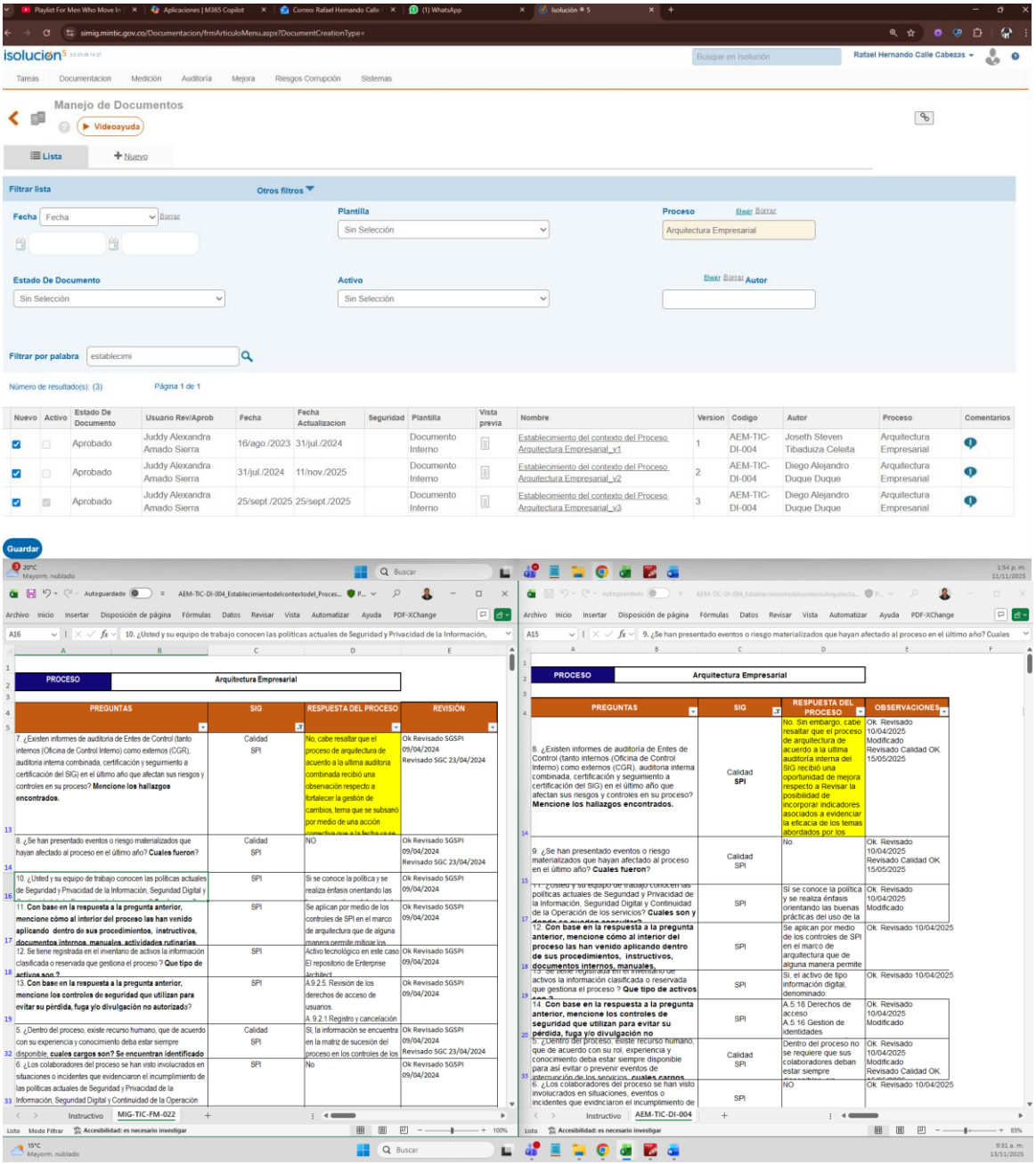
Esta misma situación identificada para los procesos de “Gestión Financiera”, “Planeación y Formulación de políticas” y “Uso y apropiación de las TIC.

Lo anterior en contravía de lo definido en el documento “Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas” y “Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6”, los cuales definen que el análisis del contexto se realiza previo a la definición de riesgos.

Al consultar con los gestores de riesgos de la Entidad, manifiestan que el documento del contexto se realiza previo a la definición de riesgos y que los soportes se encuentran en correos electrónicos y que este documento de contexto no tiene obligatoriedad de publicación en SIMIG, por lo cual se recomienda, que este documento se publique en SIMIG cada vez que sea modificado.

De la misma manera, se realiza la validación de las versiones preliminares y vigentes del documento de contexto (tomando como ejemplo el proceso de Arquitectura Empresarial), y estos documentos no presentan claramente los cambios de cada ítem (SPI, calidad, SST, Ambiental, ERSI, etc.) de una versión a otra, por lo tanto, la

validación es dispendiosa y no tan clara. Se recomienda buscar estrategias para que el documento sea amigable y permita identificar fácilmente cuales fueron los cambios de una versión a otra y si el cambio de una versión fue producto del SPI, o de calidad, o SST, o Ambiental o ERSI.



Alerta temprana 2: No se identificó un análisis y valoración para determinar la conveniencia de contar con garantías que cubran los costos asociados a ataques cibernéticos.

El artículo 16 "Seguridad digital y responsabilidad" indica que:

> *"Los sujetos obligados <u>podrán incluir</u> en su estrategia de seguridad digital los elementos de valoración que se requerirán para determinar la conveniencia de contar con garantías que cubran los costos asociados a ataques cibernéticos" y para lo cual se solicitó "Indicar si el MinTIC ha contado con garantías que cubran los costos asociados a ataques cibernéticos.".*

El proceso respondió que "*A través de correo electrónico, se solicitó a la Subdirección Administrativa informar si el Ministerio cuenta con garantías que cubran costos asociados a ataques cibernéticos. En respuesta la subdirección confirma actualmente el Ministerio no cuenta con una garantía específica para atender ataques cibernéticos*", sin embargo, existe la posibilidad de que se materialice un riesgo de ataques cibernéticos en la Entidad.

Se recomienda realizar el análisis y valoración para determinar la conveniencia de contar con garantías que cubran los costos asociados a ataques cibernéticos. Es importante que el proceso de SPI conozca y mantenga en apropiación, la información de si se tienen o no garantías vigentes.

Alerta temprana 3: No se identifica socialización de las lecciones aprendidas de la etapa de Recuperación y aprendizaje.

Con el requerimiento 2.16.f y g se solicitaron los soportes y evidencias donde se hayan compartido las lecciones aprendidas relacionadas con la etapa de recuperación y aprendizaje de la gestión de incidentes de seguridad digital y los informes de cierre del incidente con apartado de lecciones aprendidas.
El proceso indicó que "*Se anexa el documento compartido dentro de las actividades de documentación de las lecciones aprendidas: Sugerencias Estrategias de Contingencia IntegraTIC*" y suministró un documento que contiene las recomendaciones del proveedor para "*establecer lineamiento para la construcción de un plan de contingencia sobre los componentes que soportan la operación de IntegraTIC (…) para contar con consideraciones claves para la construcción y definición de un DRP "Plan de Recuperación Ante Desastres*" y remitió un Informe de cierre de un incidente.

El artículo 17 "Etapas generales de la gestión de incidentes de seguridad digital" de la Resolución 500 de 2021 establece que:

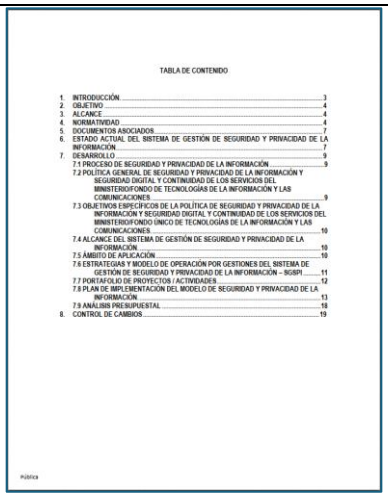
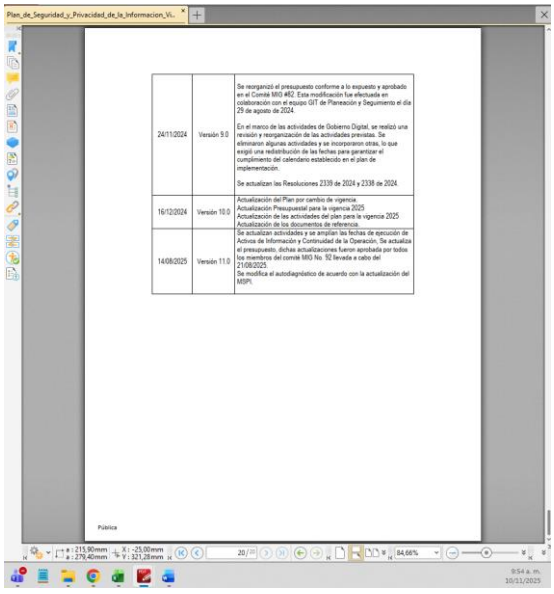
> "*4. Recuperación y aprendizaje. Desarrollar e implementar actividades apropiadas para definir y mantener los planes de recuperación, resiliencia y restauración de las infraestructuras críticas, servicios, sistemas de información, procesos o en general de un activo de información que se haya deteriorado debido a un incidente de seguridad digital. Los sujetos obligados deben:*
> *1.3. Socializar, <u>cuando la entidad lo considere pertinente,</u> las lecciones aprendidas al interior de la organización y con las entidades de su sector*",

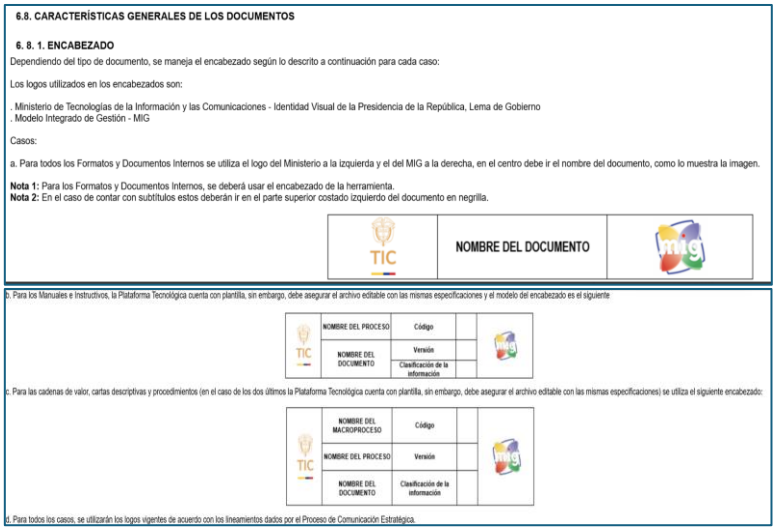
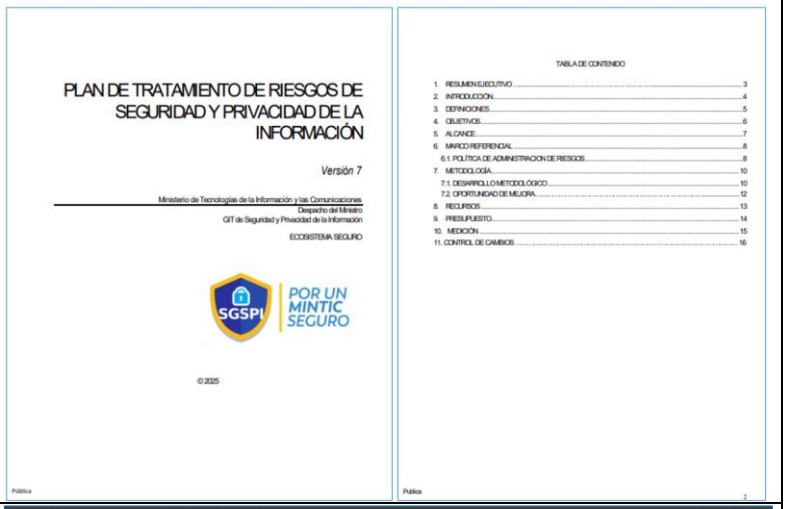
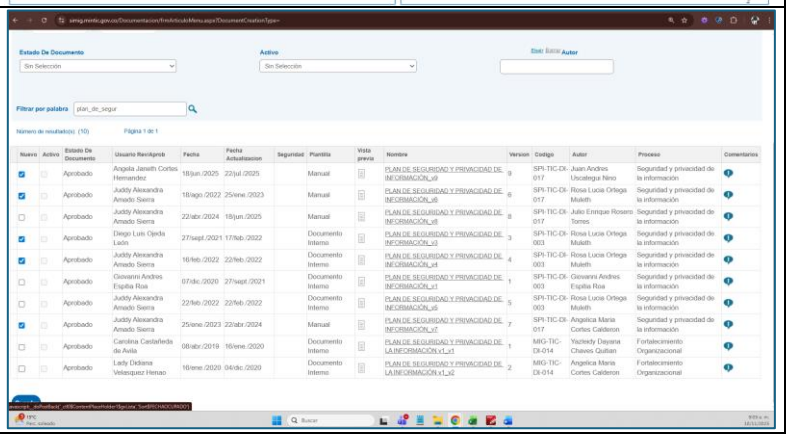
sin embargo, con el soporte suministrado, no se identificó evidencia de la socialización de las lecciones aprendidas al interior de la Entidad, ni que todos los informes de los incidentes contengan esta información.

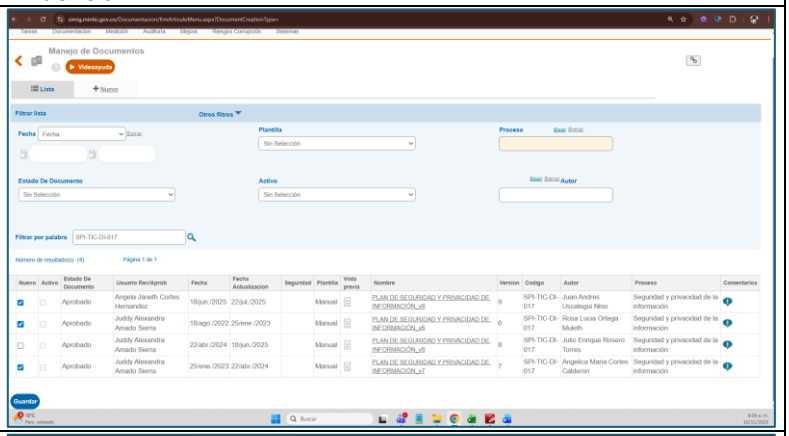
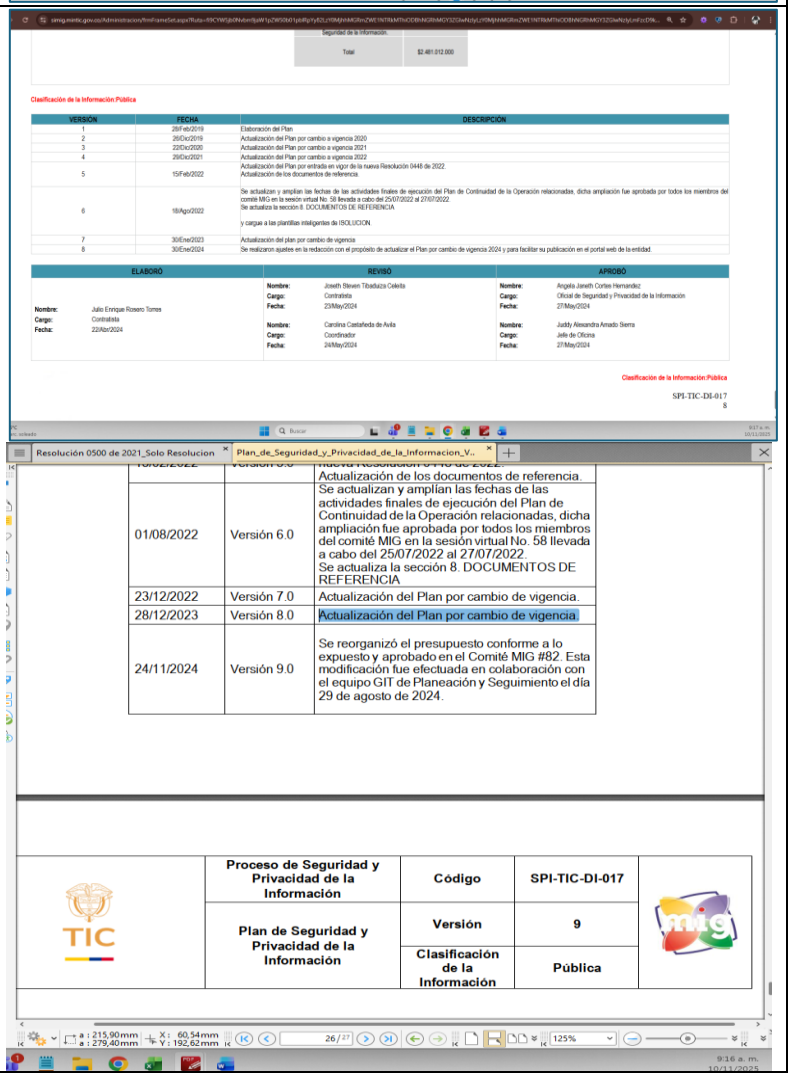
Aunque se precise en el artículo que es a consideración de la Entidad, se recomienda realizar estas socializaciones con regularidad, y tener referencia de aplicación el capítulo 10.1. Lecciones aprendidas “Lineamientos De Gestión de incidentes de seguridad de la información y seguridad digital MSPI”.

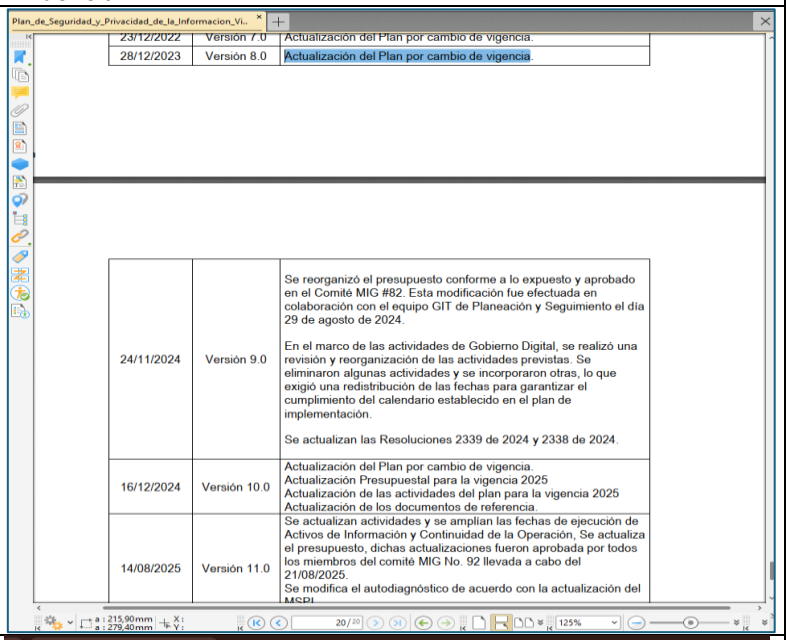
Alerta temprana 4. Debilidades en la definición y publicación de los Planes de SPI.

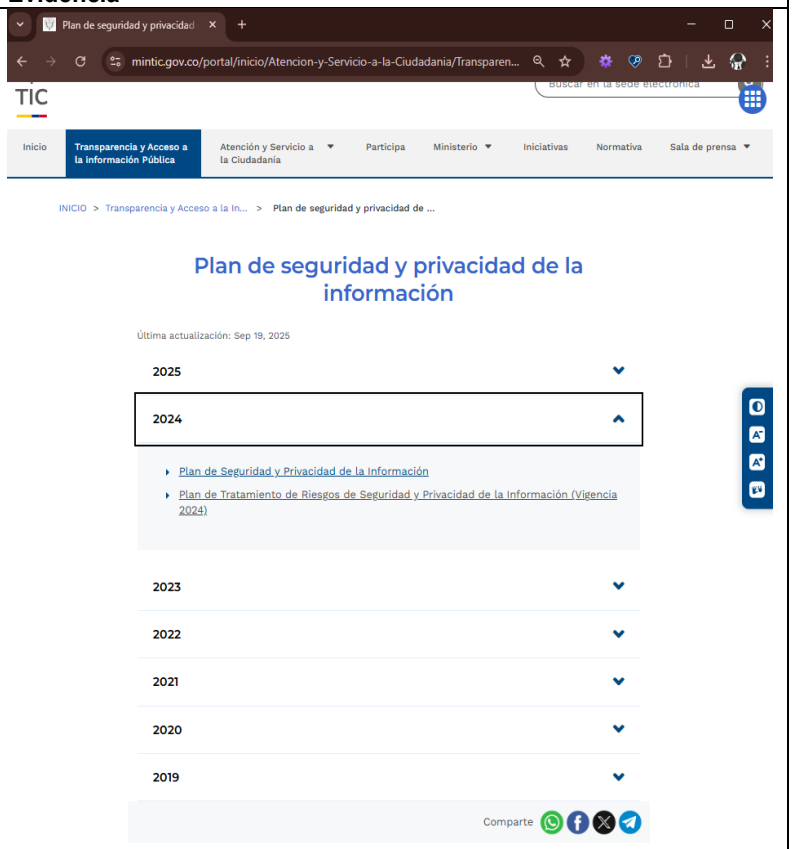
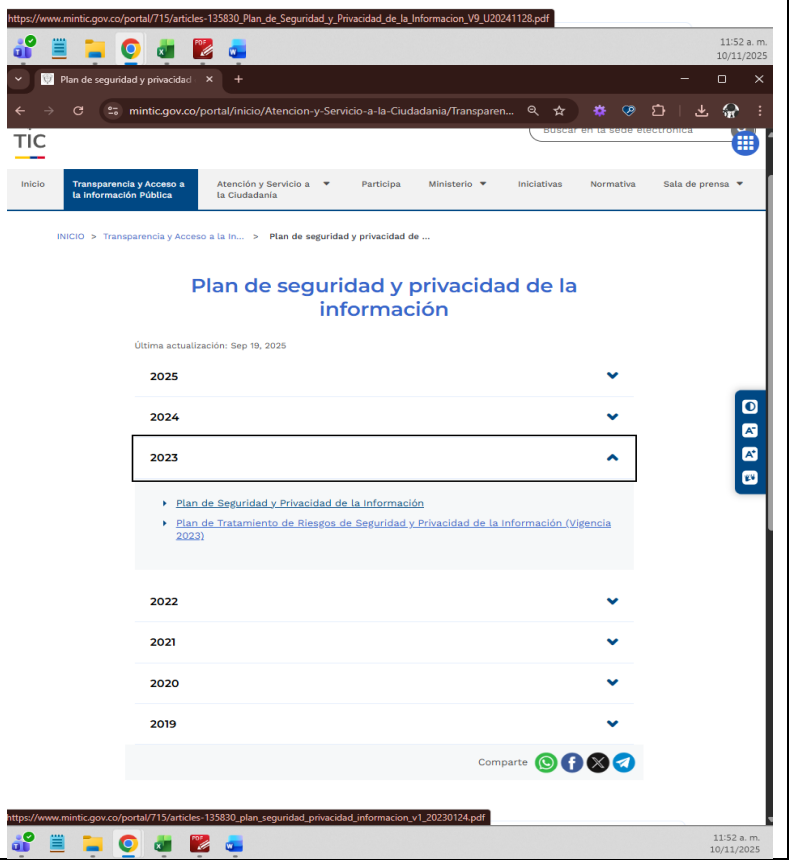
Con el requerimiento 2.1.c se solicitaron los Planes de SPI y al validar la información entregada se evidenció que:

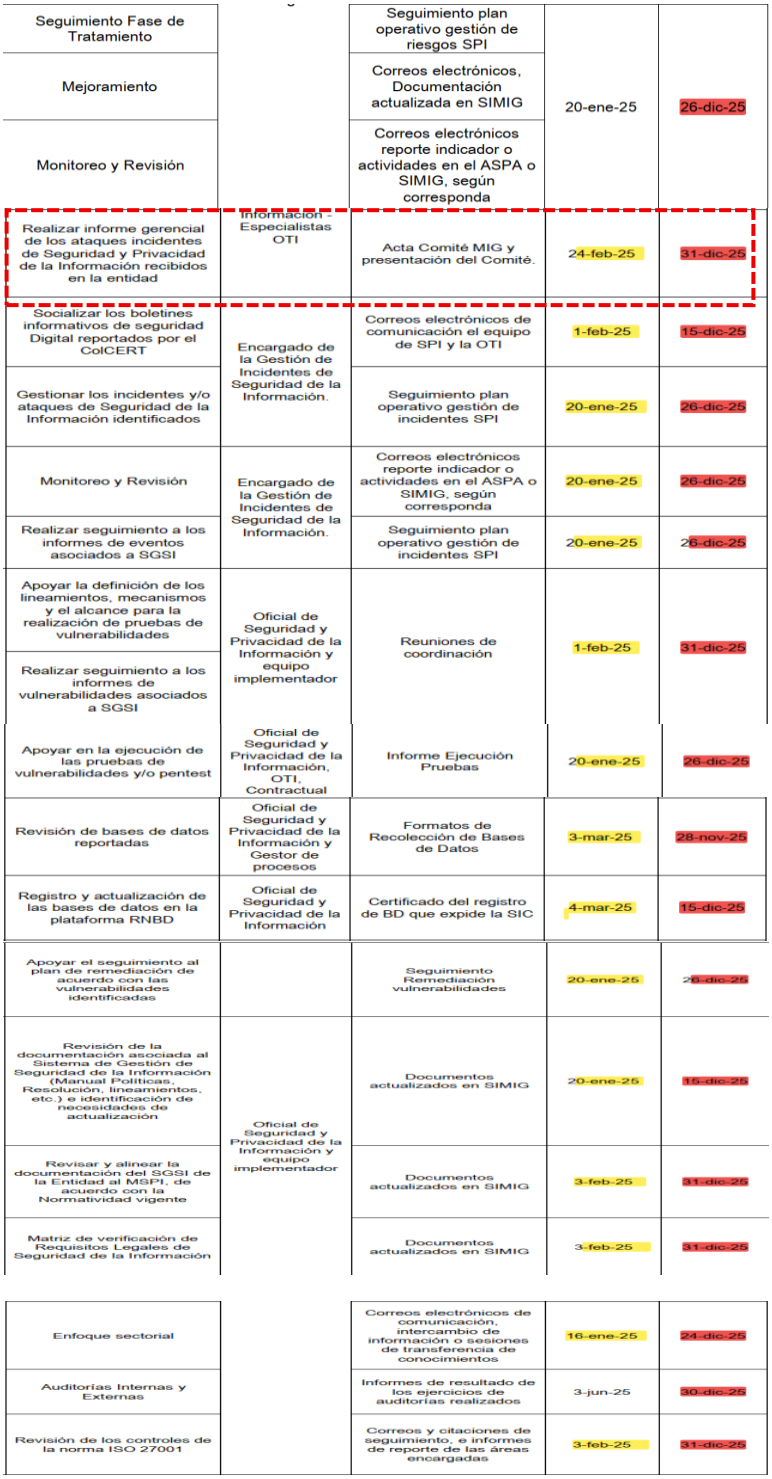
Id	Observación	Evidencia
a	La versión 11 suministrada no contiene la estructura de documento oficial de la entidad, en lo correspondiente a la codificación de documentos en SIMIG, incumpliendo el documento de norma fundamental de la Entidad que define la estructura de todos los documentos oficiales e institucionales. Asimismo, en el control de cambios no se tiene identificada la fecha de aprobación del documento. Se consultó al proceso e indicó que, a partir del 2025, esos planes no se publican en SIMIG sino directamente en la página de transparencia, para lo cual se solicita aclarar en qué directriz oficial de la Entidad se definió, la no publicación del documento en SIMIG. Se debe tener en cuenta que el Manual Norma Fundamental indica en el capítulo: **6.5. VERSIONAMIENTO** *Para el control de versiones se utiliza los siguientes criterios:* *La Versión representa los cambios sustanciales (estructura, contenido, objetivo, alcance, descripción de actividades, etc.) que ha tenido el documento a través del tiempo. Por ejemplo: 1, 2, 3, (.), dicho cambio genera automáticamente una versión mayor en la Plataforma Tecnológica. Para los casos de la documentación que requiere ser adjuntada en la Plataforma Tecnológica, tales como cadena de valor, formatos y* ***documentos internos*** *la versión deberá identificarse de la siguiente manera: V1, V2, V3, (.).* ***Definiciones:***	  

Id	Observación	Evidencia
	3.7. Documento Interno: Información documentada que evidencia el cumplimento normativo de los requisitos del Sistema Integrado de Gestión o resultados de aplicación de las actividades del proceso, los cuales pueden ser auditables. Ejemplo: Mapa de riesgos, planes, cronogramas. Nota: Esta misma situación se identificó para el documento del Plan de tratamiento de Riesgos de Seguridad y Privacidad de la Información versión 7.	Documento: Manual norma fundamental.  6.8. CARACTERÍSTICAS GENERALES DE LOS DOCUMENTOS 6. 8. 1. ENCABEZADO Dependiendo del tipo de documento, se maneja el encabezado según lo descrito a continuación para cada caso: Los logos utilizados en los encabezados son: . Ministerio de Tecnologías de la Información y las Comunicaciones - Identidad Visual de la Presidencia de la República, Lema de Gobierno . Modelo Integrado de Gestión - MIG Casos: a. Para todos los Formatos y Documentos Internos se utiliza el logo del Ministerio a la izquierda y el del MIG a la derecha, en el centro debe ir el nombre del documento, como lo muestra la imagen. **Nota 1:** Para los Formatos y Documentos Internos, se deberá usar el encabezado de la herramienta. **Nota 2:** En el caso de contar con subtítulos estos deberán ir en el parte superior costado izquierdo del documento en negrilla. TIC NOMBRE DEL DOCUMENTO b. Para los Manuales e Instructivos, la Plataforma Tecnológica cuenta con plantilla, sin embargo, debe asegurar el archivo editable con las mismas especificaciones y el modelo del encabezado es el siguiente TIC NOMBRE DEL PROCESO Código Versión Clasificación de la información NOMBRE DEL DOCUMENTO c. Para las cadenas de valor, cartas descriptivas y procedimientos (en el caso de los dos últimos la Plataforma Tecnológica cuenta con plantilla, sin embargo, debe asegurar el archivo editable con las mismas especificaciones) se utiliza el siguiente encabezado: TIC NOMBRE DEL MACROPROCESO Código NOMBRE DEL PROCESO Versión NOMBRE DEL DOCUMENTO Clasificación de la información d. Para todos los casos, se utilizarán los logos vigentes de acuerdo con los lineamientos dados por el Proceso de Comunicación Estratégica. **Plan de tratamiento de Riesgos de Seguridad y Privacidad de la Información versión 7:**  PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN *Versión 7* Ministerio de Tecnologías de la Información y las Comunicaciones Despacho del Ministro GIT de Seguridad y Privacidad de la Información ECOSISTEMA SEGURO SGSPI POR UN MINTIC SEGURO ©2025 Pública TABLA DE CONTENIDO 1. RESUMEN EJECUTIVO ... 3 2. INTRODUCCIÓN ... 4 3. DEFINICIONES ... 5 4. OBJETIVOS ... 6 5. ALCANCE ... 7 6. MARCO REFERENCIAL ... 8 6.1. POLÍTICA DE ADMINISTRACIÓN DE RIESGOS ... 8 7. METODOLOGÍA ... 10 7.1. DESARROLLO METODOLÓGICO ... 10 7.2. OPORTUNIDAD DE MEJORA ... 12 8. RECURSOS ... 13 9. PRESUPUESTO ... 14 10. MEDICIÓN ... 15 11. CONTROL DE CAMBIOS ... 16 Pública 2
b	Se consulta en SIMIG en la opción "Manejo de documentos" las versiones 10 y 11 y estas no se visualizan; tampoco permite la opción de consultarlo con la restricción de permisos de accesos que si aparecen para otros documentos (Únicamente los usuarios que cumplan con la configuración de seguridad de este documento son los que pueden consultarlo). Lo anterior incumpliendo el documento de norma fundamental de la entidad que define la estructura de todos los documentos oficiales e institucionales.	 Estado De Documento Activo Autor Filtrar por palabra Nuevo Activo Estado De Documento Usuario Recibprob Fecha Fecha Actualizacion Seguridad Plantilla Vista previa Nombre Version Codigo Autor Proceso Comentarios Aprobado Angela Janeth Cortes Hernandez 18/jun./2025 22/jul./2025 Manual PLAN DE SEGURIDAD Y PRIVACIDAD DE INFORMACIÓN_v9 9 SPI-TIC-DI-017 Juan Andres Uscategui Niño Seguridad y privacidad de la información Aprobado Juddy Alexandra Amado Sierra 18/ago./2022 25/ene./2023 Manual PLAN DE SEGURIDAD Y PRIVACIDAD DE INFORMACIÓN_v8 8 SPI-TIC-DI-017 Rosa Lucia Ortega Muleth Seguridad y privacidad de la información Aprobado Juddy Alexandra Amado Sierra 22/abr./2024 18/jun./2025 Manual PLAN DE SEGURIDAD Y PRIVACIDAD DE INFORMACIÓN_v8 8 SPI-TIC-DI-017 Julio Enrique Rosero Torres Seguridad y privacidad de la información Aprobado Diego Luis Ojeda León 27/sept./2021 17/feb./2022 Documento Interno PLAN DE SEGURIDAD Y PRIVACIDAD DE INFORMACIÓN_v3 3 SPI-TIC-DI-003 Rosa Lucia Ortega Muleth Seguridad y privacidad de la información Aprobado Juddy Alexandra Amado Sierra 16/feb./2022 22/feb./2022 Documento Interno PLAN DE SEGURIDAD Y PRIVACIDAD DE INFORMACIÓN_v4 4 SPI-TIC-DI-003 Rosa Lucia Ortega Muleth Seguridad y privacidad de la información Aprobado Giovanni Andres Espitia Roa 07/dic./2020 27/sept./2021 Documento Interno PLAN DE SEGURIDAD Y PRIVACIDAD DE INFORMACIÓN_v1 1 SPI-TIC-DI-003 Giovanni Andres Espitia Roa Seguridad y privacidad de la información Aprobado Juddy Alexandra Amado Sierra 22/feb./2022 22/feb./2022 Documento Interno PLAN DE SEGURIDAD Y PRIVACIDAD DE INFORMACIÓN_v5 5 SPI-TIC-DI-003 Rosa Lucia Ortega Muleth Seguridad y privacidad de la información Aprobado Juddy Alexandra Amado Sierra 25/ene./2023 22/abr./2024 Manual PLAN DE SEGURIDAD Y PRIVACIDAD DE INFORMACIÓN_v7 7 SPI-TIC-DI-017 Angelica Maria Cortes Calderon Seguridad y privacidad de la información Aprobado Carolina Castañeda de Avila 08/abr./2019 16/ene./2020 Documento Interno PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN v1_v1 1 MIG-TIC-DI-014 Yackeidy Dayana Chaves Quiñan Fortalecimiento Organizacional Aprobado Lady Diliana Velasquez Henao 16/ene./2020 04/dic./2020 Documento Interno PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN v1_v2 2 MIG-TIC-DI-014 Angelica Maria Cortes Calderon Fortalecimiento Organizacional

Id	Observación	Evidencia
		
c	Se validan las fechas y descripciones de los cambios de las versiones 8, 9 y 11, y se identificó que la versión 8 presenta fecha y descripción del documento "*30/Ene/2024.Se realizaron ajustes en la redacción con el propósito de actualizar el Plan por cambio de vigencia 2024 y para facilitar su publicación en el portal web de la entidad*", sin embargo, la información se encuentra diferente en las versiones 9 y 11 que contienen otras fechas y descripciones: "*28/12/2023. Actualización del Plan por cambio de vigencia*", lo cual implica una incoherencia documental que no permite conocer la información de fecha y descripción reales de los documentos y las justificaciones de los cambios. Lo anterior incumpliendo el documento de norma fundamental de la entidad que define la estructura de todos los documentos oficiales e institucionales. Nota: Las fechas de estas versiones tienen una diferencia de más de 1 mes.	

Id	Observación	Evidencia
		
d	Se validó la publicación en la página de la Entidad de todas las versiones del plan de SPI, sin embargo, se identificaron estas situaciones: **i.** El plan de SPI versión 10 no se encuentran publicado. **ii.** Las fechas de publicación de los documentos no se identifican, incumpliendo la Resolución 1519 de 2020, específicamente en el Anexo 2. Estándares de publicación y divulgación información, en el criterio "2.4.1 Criterios generales de publicación de información pública" ítem e. Todo documento o información debe indicar la fecha de su publicación en página web. **iii.** No se identificó la ruta de cómo llegar a los Planes de SPI; dado que no aparece ni en el mapa del sitio ni por búsqueda en la sede electrónica, incumpliendo el Criterio de la precitada Resolución: "*CC23. Utilice textos adecuados en títulos, páginas y secciones. Los títulos de las páginas deben ser claros e indicar la ubicación dentro del sitio web*". Se buscó por internet y se encontró la siguiente url: https://www.mintic.gov.co/portal/inicio/Atencion-y-Servicio-a-la-Ciudadania/Transparencia/135830:Plan-de-seguridad-y-privacidad-de-la-informacion Haciendo el ejercicio de buscar la ruta, se identificó que la posible ruta es:	

Id	Observación	Evidencia
	Inicio / Ministerio / Planes / Plan de Seguridad y Privacidad de la información. Nota: Esta misma situación se identificó para el documento “Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información | Vigencia 2025 (PDF descargable)”	 

Id	Observación	Evidencia
e	Al validar el cronograma del Plan de SPI del 2025 (versión 11) se identificó que: **i.** 22 de 42 de actividades que tiene el cronograma del Plan del SPI se definieron con fecha inicial al primer o primeros meses del año y finalizan en diciembre de 2025, sin embargo, un cronograma con estas características de actividades traslapadas no permite claramente poder realizar un seguimiento de cumplimiento a este, por ejemplo, la actividad "Realizar informe gerencial de los ataques incidentes de SPI recibidos en la entidad" con fecha inicial de febrero y final de diciembre, no se confirma cuándo se va a presentar al Comité. **Se recomienda** detallar las actividades y los cronogramas del Plan de SPI con el objetivo que la Entidad, cualquier proceso, entes de control (internos o externos) y cualquier persona o grupos de interés, puedan ejercer su rol de seguimiento y control. **ii.** Algunas actividades definidas en el plan son muy generales y no permiten conocer el detalle de lo que se va a realizar en dicha actividad. Por ejemplo: <u>Línea Estratégica "Planeación y seguimiento":</u> - "Enfoque sectorial" fechas programadas del 16/01/2025 al 24/12/2025 - "Auditorías Internas y Externas" fechas programadas del 3/06/2025 al 30/12/25. <u>Línea Estratégica "Fortalecimiento del Modelo de gestión de seguridad y privacidad de la información", Gestión "Riesgos de Seguridad de la Información"</u> de acuerdo con el cronograma se tiene definido:	**Ítem i:** 

Seguimiento Fase de Tratamiento		Seguimiento plan operativo gestión de riesgos SPI		
Mejoramiento		Correos electrónicos, Documentación actualizada en SIMIG	20-ene-25	26-dic-25
Monitoreo y Revisión		Correos electrónicos reporte indicador o actividades en el ASPA o SIMIG, según corresponda		
Realizar informe gerencial de los ataques incidentes de Seguridad y Privacidad de la Información recibidos en la entidad	Especialistas OTI	Acta Comité MIG y presentación del Comité.	24-feb-25	31-dic-25
Socializar los boletines informativos de seguridad Digital reportados por el ColCERT	Encargado de la Gestión de Incidentes de Seguridad de la Información.	Correos electrónicos de comunicación el equipo de SPI y la OTI	1-feb-25	15-dic-25
Gestionar los incidentes y/o ataques de Seguridad de la Información identificados		Seguimiento plan operativo gestión de incidentes SPI	20-ene-25	26-dic-25
Monitoreo y Revisión	Encargado de la Gestión de Incidentes de Seguridad de la Información.	Correos electrónicos reporte indicador o actividades en el ASPA o SIMIG, según corresponda	20-ene-25	26-dic-25
Realizar seguimiento a los informes de eventos asociados a SGSI		Seguimiento plan operativo gestión de incidentes SPI	20-ene-25	26-dic-25
Apoyar la definición de los lineamientos, mecanismos y el alcance para la realización de pruebas de vulnerabilidades	Oficial de Seguridad y Privacidad de la Información y equipo implementador	Reuniones de coordinación	1-feb-25	31-dic-25
Realizar seguimiento a los informes de vulnerabilidades asociados a SGSI				
Apoyar en la ejecución de las pruebas de vulnerabilidades y/o pentest	Oficial de Seguridad y Privacidad de la Información, OTI, Contractual	Informe Ejecución Pruebas	20-ene-25	26-dic-25
Revisión de bases de datos reportadas	Oficial de Seguridad y Privacidad de la Información y Gestor de procesos	Formatos de Recolección de Bases de Datos	3-mar-25	28-nov-25
Registro y actualización de las bases de datos en la plataforma RNBD	Oficial de Seguridad y Privacidad de la Información	Certificado del registro de BD que expide la SIC	4-mar-25	15-dic-25
Apoyar el seguimiento al plan de remediación de acuerdo con las vulnerabilidades identificadas		Seguimiento Remediación vulnerabilidades	20-ene-25	26-dic-25
Revisión de la documentación asociada al Sistema de Gestión de Seguridad de la Información (Manual Políticas, Resolución, lineamientos, etc.) e identificación de necesidades de actualización	Oficial de Seguridad y Privacidad de la Información y equipo implementador	Documentos actualizados en SIMIG	20-ene-25	15-dic-25
Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente		Documentos actualizados en SIMIG	3-feb-25	31-dic-25
Matriz de verificación de Requisitos Legales de Seguridad de la Información		Documentos actualizados en SIMIG	3-feb-25	31-dic-25
Enfoque sectorial		Correos electrónicos de comunicación, intercambio de información o sesiones de transferencia de conocimientos	16-ene-25	24-dic-25
Auditorías Internas y Externas		Informes de resultado de los ejercicios de auditorías realizados	3-jun-25	30-dic-25
Revisión de los controles de la norma ISO 27001		Correos y citaciones de seguimiento, e informes de reporte de las áreas encargadas	3-feb-25	31-dic-25

Id	Observación	Evidencia
	- "Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación" desde el 17/03/2025 al 18/07/2025 - "Aceptación de Riesgos Identificados" desde el 05/05/2025 al 26/07/2025 - "Publicación" desde el 05/05/2025 al 26/07/2025. - "Seguimiento Fase de Tratamiento", "Mejoramiento" y "Monitoreo y Revisión" y desde el 20/01/2025. (Las 3 actividades tienen las mismas fechas de ejecución). **iii.** Se define "Responsable de la tarea" en las que se especifican "Equipo Activos", "Equipo de Gestión de Riesgos", "equipo implementador" y "Equipo de Gestión de Cultura", sin embargo, en el documento no es claro quienes lo componen o en donde se puede consultar esta información, y si estos responsables fueron notificados de que tenían estas actividades a cargo. **Se recomienda** aclarar en el documento los responsables en la Entidad. **iv.** No se identifican en el Plan de SPI cuáles son los "controles" definidos, incumpliendo con lo establecido en el documento "Documento Maestro de Los Lineamientos del MSPI" el cual indica que: "*Plan de seguridad y privacidad de la información que defina la implementación de controles de seguridad y privacidad de la información y contenga como mínimo:* ***controles****, actividades, fechas, responsable de implementación y presupuesto*". Es necesario indicar cuales son los controles incluidos dentro del Plan de SPI.	**Ítem ii.** Seguimiento Fase de Tratamiento — Seguimiento plan operativo gestión de riesgos SPI Mejoramiento — Correos electrónicos, Documentación actualizada en SIMIG — 20-ene-25 — 26-dic-25 Monitoreo y Revisión — Correos electrónicos reporte indicador o actividades en el ASPA o SIMIG, según corresponda Monitoreo y Revisión — Encargado de la Gestión de Incidentes de — Correos electrónicos reporte indicador o actividades en el ASPA o SIMIG, según corresponda — 20-ene-25 — 26-dic-25 Enfoque sectorial — Correos electrónicos de comunicación, intercambio de información o sesiones de transferencia de conocimientos — 16-ene-25 — 24-dic-25 **Ítem iii.**

Líneas Estratégicas	Gestión	Actividades	Responsable de la Tarea	Evidencia	Fechas Programación Tareas	
					Fecha Inicio	Fecha Final
Fortalecimiento del Modelo de gestión de seguridad y privacidad de la información	Activos de Información	Apoyar en la identificación, clasificación, valoración y rotulado de activos de los activos de información, de acuerdo con lo establecido en la Resolución 2239 de 2024 Art. 5 literal a	Equipo Activos	Matriz de inventario activos de información actualizada y enviada para validación a las áreas correspondientes	1-feb-25	30-jul-25
		Realizar e, seguimiento a la Publicación de la Matriz de inventario de Activos de Información actualizada		Correos electrónicos frente al seguimiento de la publicación en la plataforma SIMIG, sitio Web de Entidad y portal de datos abiertos	30-jul-25	30-ago-25
		Asesorar frente a las necesidades identificación, clasificación, valoración y rotulado de Activos de Información		Solicitudes de identificación, clasificación, valoración y rotulado de Activos de Información	30-ago-25	10-dic-25
	Riesgos de Seguridad de la Información	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	Equipo de Gestión de Riesgos	Correos electrónicos Mapas de riesgos	17-mar-25	18-jul-25
		Aceptación de Riesgos Identificados		Correo electrónico, trazabilidad de aprobación en SIMIG	5-may-25	26-jul-25
		Publicación		Mapas de riesgos publicados en SIMIG		
		Seguimiento Fase de Tratamiento		Seguimiento plan operativo gestión de riesgos SPI	20-ene-25	26-dic-25
		Mejoramiento		Correos electrónicos, Documentación actualizada en SIMIG		
		Monitoreo y Revisión		Correos electrónicos reporte indicador o actividades en el ASPA o SIMIG, según corresponda		

OBJETIVO ESPECÍFICO 2. Verificar el cumplimiento de las obligaciones de los contratos pertenecientes al proceso, incluyendo la adecuada supervisión de estos, se identificaron las siguientes observaciones preliminares.

Para el desarrollo de este objetivo, se solicitó al proceso auditado informar los contratos directamente relacionados con el objetivo específico de la auditoría, con el propósito de determinar una muestra y validar el cumplimiento de las obligaciones contractuales y la gestión de supervisión adelantada.

La muestra de los contratos que fueron objeto de revisión por parte del equipo auditor se relaciona en la siguiente tabla:

Año	Nombre	Número del contrato	Área	Objeto
2023	Consultoría Continuidad de la Operación de los Servicios	1134-2023	GIT de Seguridad y Privacidad de la Información	Prestar servicios de consultoría para la actualización del Plan de Continuidad del Negocio (BCP) del MINTIC basado en la norma ISO/IEC 22301:2019 que garantice el adecuado funcionamiento del modelo de operación por procesos de la entidad.
2023	Consultoría en Protección de Datos Personales	1191-2023	GIT de Seguridad y Privacidad de la Información	Prestar servicios de consultoría para realizar la evaluación, diagnóstico y actualización del Programa Integral de Protección de Datos Personales del Ministerio de Tecnologías de la Información y las Comunicaciones según la normatividad vigente.
2023	Segundo seguimiento a la certificación en ISO/IEC 27001:2013	1222-2023	GIT de Seguridad y Privacidad de la Información	Prestar servicios para realizar auditoria de seguimiento a la certificación otorgada al Sistema de Gestión de Seguridad y Privacidad de la Información (ISO/IEC 27001:2013).
2024	Plan de cambio y cultura	2047-2024	GIT de Seguridad y Privacidad de la Información	Prestar servicios para realizar la medición, diagnóstico y fortalecimiento de la cultura y apropiación en seguridad y privacidad de la información del MinTIC/Fondo Único de TIC, por medio de pruebas de ingeniería social y el licenciamiento de una plataforma en la modalidad Software como Servicio (SaaS) de formación para los colaboradores de la entidad y monitoreo de resultados.

Tabla 3. Tabla de Contratos

De la muestra tomada, se verificó la etapa contractual, teniendo en cuenta, el cumplimiento de obligaciones y requisitos técnicos, y el ejercicio de supervisión realizado, así como las evidencias y documentos que los soportan.

Para cada uno de los contratos seleccionados en la muestra se realizaron las solicitudes de la información relevante para determinar el cumplimiento de los criterios de auditoría, posteriormente se verificaron los soportes que reposan en la carpeta compartida para la consulta de la información de cada contrato.

Se solicitaron soportes y evidencias mediante los siguientes requerimientos:

Requerimiento 3: Realizado el 29/10/2025, en el cual se remite solicitud de información del Contrato 1134 de 2023, relacionado con "Prestar servicios de consultoría para la actualización del Plan de Continuidad del Negocio (BCP) del MINTIC basado en la norma ISO/IEC 22301:2019 que garantice el adecuado funcionamiento del modelo de operación por procesos de la entidad".

Requerimiento 5: Realizado el 10/11/2025, en el cual se remite solicitud de información del Contrato 1191 de 2023, relacionado con "Prestar servicios de consultoría para realizar la evaluación, diagnóstico y actualización del Programa Integral de Protección de Datos Personales del Ministerio de Tecnologías de la Información y las Comunicaciones según la normatividad vigente".

Requerimiento 6: Realizado el 12/11/2025**,** en el cual se remite solicitud de información del Contrato 1222 – 2023, relacionado con: ″Prestar servicios para realizar auditoría de seguimiento a la certificación otorgada al Sistema de Gestión de Seguridad y Privacidad de la Información (ISO/IEC 27001:2013)″ y el Contrato 20247-2024, relacionado con: " Prestar servicios para realizar la medición, diagnóstico y fortalecimiento de la cultura y apropiación en seguridad y privacidad de la información del MinTIC/Fondo Único de TIC, por medio de pruebas de ingeniería social y el licenciamiento de una plataforma en la modalidad Software como Servicio (SaaS) de formación para los colaboradores de la entidad y monitoreo de resultados".

Una vez realizadas las verificaciones del cumplimiento de la ejecución contractual, se generan los siguientes hallazgos:

Hallazgo 2.1 En el contrato 1134 de 2023 y en el contrato 1191 de 2023 no se cumplió con la entrega de las hojas de vida de los profesionales propuestos dentro de los términos establecidos en dichos contratos.

Caso 1. Contrato 1134 de 2023

Con el requerimiento No. 3 se solicitó soporte de entrega de las hojas de vida de los profesionales propuestos que den cumplimiento a los requisitos habilitantes establecidos en el Estudio Previo y en el Pliego de Condiciones. Sin embargo, el proceso remitió respecto al soporte de entrega de las hojas de vida, la siguiente información:

- El consolidado del informe de evaluación final del concurso de méritos abierto No. FTIC-CM-004-2023.
- Evaluación técnica del concurso de méritos abierto No. FTIC-CM-004-2023.

Lo anterior conlleva al incumplimiento de la Obligación específica No. 4 del contrato 1134 de 2023 que señala:

> "*Allegar dentro de los tres (3) días hábiles siguientes a la suscripción del Contrato, las hojas de vida y los soportes de los profesionales propuestos que den cumplimiento a los requisitos habilitantes establecidos en el Estudio Previo*

y en el Pliego de Condiciones y sus Anexos, como requisito previo a la suscripción del acta de inicio".

Caso 2. contrato 1191 de 2023

Con el requerimiento No. 5 se solicitó soporte de entrega de las hojas de vida de los profesionales propuestos que den cumplimiento a los requisitos habilitantes establecidos en el Estudio Previo y en el Pliego de Condiciones. Sin embargo, el proceso remitió respecto al soporte de entrega de las hojas de vida, la siguiente información:

- Memorando remisorio de evaluación técnica al concurso abierto de méritos No. FTIC-CM-005-2023.
- Evaluación Técnica de las ofertas concurso de méritos No. FTIC-CM-005-2023.
- Formato de acreditación de revisión de las hojas de vida con constancia de cargue en el repositorio del GIT de Seguridad y Privacidad de la Información.

Lo anterior conlleva al incumplimiento de la Obligación específica No. 4 del contrato 1191 de 2023 que señala:

"*Dentro de los tres (3) días hábiles siguientes a la suscripción del contrato, el contratista deberá allegar las hojas de vida de los profesionales propuestos que den cumplimiento a los requisitos habilitantes y ponderables establecidos en el estudio previo y en el pliego de condiciones y sus anexos, condición que se considerará requisito previo para la suscripción del acta de inicio*".

Hallazgo 2.2 En el contrato 1134 de 2023 y en el contrato 1191 de 2023 no se cumplió con la entrega del cronograma de reuniones y mesas de trabajo dentro de los términos establecidos ni con la aprobación del supervisor de este cronograma.

Caso 1. Contrato 1134 de 2023

Con el requerimiento No. 3 se solicitó soporte de entrega del cronograma de reuniones y mesas de trabajo con las dependencias para levantamiento de información e insumos para la actualización de toda la documentación que compone el BCP y soporte de aprobación por el supervisor del contrato.

No obstante, el proceso remitió respecto al soporte de entrega del cronograma de reuniones y mesas de trabajo y soporte de aprobación por el supervisor del contrato, la siguiente información:

- Cronograma de trabajo consolidado.
- Acta No. 2 de seguimiento.

Lo anterior conlleva al incumplimiento de la Obligación específica No. 7 del contrato 1134 de 2023 que señala:

"*Realizar y entregar dentro de los cinco (5) días hábiles siguientes al inicio de la ejecución del contrato, un cronograma de reuniones y mesas de trabajo con las dependencias para levantamiento de información e insumos para la actualización de toda la documentación que compone el BCP, el cual deberá ser aprobado por el supervisor del contrato"*.

Caso 2. Contrato 1191 de 2023

Con el requerimiento No. 5 se solicitó soporte de entrega del cronograma de reuniones y mesas de trabajo de acuerdo con las actividades a desarrollar, productos a entregar y los plazos descritos para cada una de las fases señaladas en el anexo técnico y soporte de aprobación por el supervisor del contrato.

No obstante, el proceso remitió respecto al soporte de entrega del cronograma de reuniones y mesas de trabajo y soporte de aprobación por el supervisor del contrato, la siguiente información:

- Acta de reunión inicial No. 1 del 23 de octubre de 2023.
- Grabación de la reunión del 23 de octubre de 2023.

Lo anterior conlleva al incumplimiento de la Obligación específica No. 5 del contrato 1191 de 2023 que señala:

"*Realizar y entregar en un término de tres (3) días hábiles posteriores a la suscripción del contrato un cronograma de reuniones y mesas de trabajo, de acuerdo con las actividades a desarrollar, productos a entregar y los plazos descritos para cada una de las fases señaladas en el anexo técnico, el cual debe ser aprobado por la supervisión del contrato"*.

Hallazgo 2.3 Falta de entrega en el contrato 1134 de 2023 y en el contrato 1191 de 2023 de las Normas Técnicas al Ministerio/FUTIC en versión digital.

Caso 1. Contrato 1134 de 2023

Con el requerimiento No. 3 se solicitó soporte de entrega de las Normas Técnicas ISO/IEC 22301:2019, ISO 27001:2022 en sus últimas versiones físicas y **digitales.** Sin embargo, el proceso remitió respecto al soporte de entrega de las normas técnicas, la siguiente información:

- Las normas técnicas reposan en físico en la oficina de la Coordinadora de Seguridad y Privacidad de la información.

Lo anterior conlleva al incumplimiento de la Obligación específica No. 10 del contrato 1134 de 2023 que señala:

"*Entregar al Ministerio/FUTIC las Normas Técnicas ISO/IEC 22301:2019, ISO 27001:2022 en sus últimas versiones físicas y* ***digitales***".

Caso 2. contrato 1191 de 2023

Con el requerimiento No. 5 se solicitó soporte de entrega de las Normas Técnicas ISO/IEC 22301:2019, ISO 27001:2022 en sus últimas versiones físicas y digitales.

En respuesta, el proceso aclaró que los estudios previos de la consultoría, en el numeral 2.2.2 sobre obligaciones específicas, exigían en el numeral 6, *"Entregar el compendio de Normas Técnicas referente a la serie ISO 27001 y 27701 al MINTIC/FUTIC"*, de manera que la entrega correspondió a la ISO 27001 y 27701, y no a la ISO/IEC 22301:2019, ISO 27001:2022. Aclarado lo anterior, indicó que ambas normas fueron entregadas en formato digital al usuario SPI@MINTIC.GOV.CO en formato digital.

Sin embargo, el proceso remitió respecto al soporte de entrega de las normas técnicas ISO 27001 y 27701 al MINTIC/FUTIC, la siguiente información:

- Documento de pedido del ICONTEC No. # 000026859, evidencia que no demuestra la entrega de las normas técnicas, como se muestra a continuación:

icontec

Copiar

Pedido # 000026859

Completo

Fecha de Orden: 26 de diciembre de 2023

Reordenar Imprimir pedido

Elementos Facturas

Items

Título	SKU	Precio	Cantidad	Subtotal
Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos.	NTC-ISO-IEC27001:2022-E	COP$233.280	Ordenado: 1	COP$233.280
Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información.	GTC-ISO-IEC27002:2022-E	COP$386.400	Ordenado: 1	COP$386.400
Técnicas de seguridad. Ampliación de las NTC-ISO/IEC 27001 y GTC-ISO-IEC 27002 para la gestión de la privacidad de la información. Requisitos y directrices.	NTC-ISO-IEC27701:2020-E	COP$135.000	Ordenado: 1	COP$135.000

Lo anterior conlleva al incumplimiento de la Obligación específica No. 7 del contrato 1191 de 2023 que señala:

"*Entregar el compendio de Normas Técnicas referente a la serie ISO 27001 y 27701 al MINTIC/FUTIC*".

Hallazgo 2.4 En el contrato 1134 de 2023 no se cedieron los derechos patrimoniales de autor de los productos que se generaron de la ejecución del contrato a favor del Fondo Único de TIC.

Con el requerimiento No. 3 se solicitó soporte de la cesión de los derechos patrimoniales de autor de los productos que se generaron en la ejecución del contrato a favor del Fondo Único de TIC. Sin embargo, el proceso respondió respecto al soporte de la cesión de los derechos patrimoniales de autor, lo siguiente:

> "*De acuerdo con la legislación colombiana en materia de propiedad intelectual, no se requiere cesión de derechos de autor respecto de los productos derivados del contrato, por cuanto se trata de documentos técnicos e institucionales elaborados en modalidad de consultoría y por encargo del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) los cuales han sido aprobados previamente*".

Lo anterior conlleva al incumplimiento de la Obligación específica No. 11 del contrato 1134 de 2023 que señala:

> **"***Ceder los derechos patrimoniales de autor de los productos que se generen de la ejecución del contrato a favor del Fondo Único de TIC, una vez se haga entrega y aprobación de la totalidad de los productos previstos en el mismo*".

E incumplimiento del principio de planeación de la contratación estatal, el cual va encaminado a que, lo que se determine en los documentos contractuales se cumpla por el contratista, no obstante, se incluyeron obligaciones que no eran requeridas ejecutar por este.

Hallazgo 2.5 En el contrato 1134 de 2023 no se evidenció soporte de remisión de las actas de reunión de seguimiento a la ejecución del contrato y de las demás mesas de trabajo o reuniones, dentro de los cinco (5) días hábiles siguientes.

Con el requerimiento No. 3 se solicitó soporte de remisión a la Entidad de las actas de reunión de seguimiento a la ejecución del contrato y de las demás mesas de trabajo o reuniones. Sin embargo, el proceso remitió respecto del soporte de entrega a la Entidad de las actas, la siguiente información:

- Las actas de seguimiento firmadas, correspondientes a las reuniones de avance y ejecución del contrato. No evidenciándose el soporte de remisión de estas actas.

Lo anterior conlleva al incumplimiento de la Obligación específica No. 13 del contrato 1134 de 2023 que señala:

> *"Elaborar las actas de reunión de seguimiento a la ejecución del contrato y de las demás mesas de trabajo o reuniones, y remitirlas a la entidad dentro de los cinco (5) días hábiles siguientes para su revisión, ajuste y firma. Lo anterior, de acuerdo con el formato que el Ministerio TIC tiene para tal fin*".

Hallazgo 2.6 En el contrato 1134 de 2023 no se evidenció en la Fase 2 "Gestión del Riesgo", el Plan de acción con las actividades determinadas y Matriz de resultados.

Con el requerimiento No. 3 se solicitó el Plan de acción con las actividades determinadas y Matriz de resultados. Sin embargo, el proceso remitió respecto al Plan de Acción con las actividades determinadas y Matriz de resultados, la siguiente información:

- Tabla 1 del plan de acción extraída del documento "INFORME GESTIÓN DE RIESGOS DE INTERRUPCIÓN- RIA, no evidenciándose el plan de acción, como se muestra a continuación:

ITEM	PROCESO	CÓDIGO RIESGO	DESCRIPCIÓN DEL RIESGO	ZONA DE RIESGO FINAL	TRATAMIENTO	PLAN DE ACCIÓN				
						Actividades Plan de Acción	Responsable	Fecha de implementación	Fecha Seguimiento	Estado
1	ACCESO A LAS TIC	RIACTO4	Posibilidad de retrasos en el proceso de Acceso a las TIC por la no continuidad de los proyectos por fuerza mayor o caso fortuito	Moderado	Reducir	Realizar el seguimiento técnico, jurídico, financiero y administrativo de los terceros a través del formato GCC-TIC-FM-051 informe mensual de ejecución y de las actas que evidencien los comités operativos o reuniones de seguimiento.	Supervisor del contrato	Desde el inicio del contrato	Mensual	En proceso
2	USO Y APROPIACIÓN DE LAS TICS	RIUATO4	Posibilidad de retrasos en el proceso de Uso y Apropiación de las TIC por la no continuidad de los proyectos	Moderado	Reducir	Realizar el seguimiento técnico, operativo y financiero de los terceros a través de los formatos GCC-TIC-FM-051 o GCC-TIC-FM-055	Supervisor del contrato	Desde el inicio del contrato	Mensual	En proceso
3	USO Y APROPIACIÓN DE LAS TICS	RIUATO5	Posibilidad de retrasos en el proceso de Uso y Apropiación de las TIC por demoras en la contratación de proyectos	Moderado	Reducir	Realizar análisis de estudios previos de tal manera que se ajuste a las especificaciones y requerimientos de la entidad. De igual forma realizar revisión y ajustes a la documentación de acuerdo con las actividades definidas en el cronograma de contratación.	Director de Apropiación de las TIC, Director de Economía Digital, Director de Gobierno Digital, Jefe de Oficina de Fomento Regional o quien ellos designen	Desde el inicio del proceso de contratación	Hasta la firma del contrato	En proceso

Tabla 1. Plan de acción riesgos no aceptables.

Lo anterior conlleva al incumplimiento del anexo técnico del contrato 1134 de 2023 que señala:

5.1.2 Gestión de Riesgos

Dentro de la **Actualización, identificación, análisis y valoración de riesgos de Interrupción de la Operación** se realizará la validación y actualización de los posibles riesgos (amenazas, vulnerabilidades, controles e impactos) que podrían ocasionar interrupciones o retrasos e impactar la operación normal de la Entidad (25 procesos).

Entregables: Se generarán los siguientes productos:

- ✓ Actualización de los mapas de riesgos de interrupción de todos los procesos de la Entidad con BCP, de acuerdo con la metodología adoptada por la entidad.
- ✓ Entrevistas con los equipos designados por los procesos con sus respectivos listados de asistencia.
- ✓ Mapas de riesgos de los procesos (mapa de calor y calificación de controles).
- ✓ Plan de acción con las actividades determinadas y Matriz de resultados.

Hallazgo 2.7 En el contrato 1191 de 2023 no se evidenció en la Fase 2 "Actualización Del Sistema De Gestión De Datos Personales Y Construcción del Marco De Gobernanza", el Documento Creación del marco de cumplimiento en Protección de Datos Personales y Responsabilidad Demostrada.

Con el requerimiento 5 se solicitó el documento Creación del marco de cumplimiento en Protección de Datos Personales y Responsabilidad Demostrada.

Sin embargo, el proceso remitió respecto al documento Creación del marco de cumplimiento en Protección de Datos Personales y Responsabilidad Demostrada, la siguiente información:

- Informe de resultados de evaluación y diagnóstico de cumplimento del programa de protección de datos personales.

Es de precisar, que este informe de resultados de evaluación y diagnóstico fue un entregable de la Fase 1 "Diagnóstico y Análisis de Impacto de Privacidad" con plazo para su entrega hasta el 31 de octubre de 2025, como se muestra a continuación:

FASE 1. DIAGNÓSTICO Y ANALISIS DE IMPACTO DE PRIVACIDAD	1	Informe ejecutivo con la identificación del nivel de madurez, principales hallazgos y recomendaciones, y resultado del Análisis de Brechas (GAP)[1].	Hasta el 31 de octubre de 2023
	2	Informe de resultados de evaluación y diagnóstico, en donde se indique el estado de cumplimiento por cada proceso frente a la vigencia del Programa de Protección de Datos Personales ya implementado, sus oportunidades de mejora y nuevas estrategias a implementar para atender al principio de responsabilidad demostrada.	Hasta el 31 de octubre de 2023

Y que el documento creación del marco de cumplimiento en Protección de Datos Personales y Responsabilidad Demostrada, fue un entregable de la Fase 2 "Actualización Del Sistema De Gestión De Datos Personales Y Construcción del Marco De Gobernanza" con plazo para su entrega hasta el 31 de noviembre de 2025, como se muestra a continuación:

DE DATOS PERSONALES Y CONSTRUCCIÓN DEL MARCO DE GOBERNANZA		creados o ajustados que reflejen las necesidades de la Protección de Datos Personales para el Ministerio/Fondo Único de TIC.	
	5	Documento Creación del marco de cumplimiento en Protección de Datos Personales y Responsabilidad Demostrada.	Hasta el 31 de noviembre de 2023

Lo anterior, conlleva al incumplimiento del anexo técnico del contrato 1191 de 2023 que señala:

"*5.3. Fases, entregables y resultados esperados*

Fase 2 "Actualización del Sistema de Gestión de Datos Personales y Construcción del Marco De Gobernanza". Entregable: documento *Creación del marco de cumplimiento en Protección de Datos Personales y Responsabilidad Demostrada"*.

Hallazgo 2.8 En el contrato 1134 de 2023 y en el contrato 1191 de 2023 no se evidenció seguimiento a la Matriz de Riesgos establecida en dichos contratos.

Caso 1. Contrato 1134 de 2023

Con el requerimiento No. 3 se solicitó soporte de seguimiento a la Matriz de Riesgos establecida en el contrato.

Sin embargo, el proceso remitió respecto al soporte de seguimiento a la Matriz de Riesgos establecida en el contrato, la siguiente información:

- Respuesta en la que comunicó, que no se materializó ningún riesgo durante la ejecución del Contrato No. 1134-2023.
- Las cuentas de cobro correspondientes al primer y segundo pago.

Caso 2. contrato 1191 de 2023

Con el requerimiento No. 5 se solicitó soporte de seguimiento a la Matriz de Riesgos establecida en el contrato.

Sin embargo, el proceso remitió respecto al soporte de seguimiento a la Matriz de Riesgos establecida en el contrato, la siguiente información:

- Respuesta en la que comunicó, que no se materializó ningún riesgo durante la ejecución del Contrato.
- Actas de seguimiento a la ejecución del contrato.

Lo anterior, conlleva al incumplimiento del Manual de Supervisión e Interventoría GCC-TIC-MA-005 V.2, que señala:

"OBLIGACIONES DE LOS SUPERVISORES E INTERVENTORES

Obligaciones Generales

9. *Realizar seguimiento a la Matriz de Riesgos establecida en el contrato y en general a aquellos riesgos que puedan comprometer los intereses de la Entidad y, ante la ocurrencia de los mismos, iniciar las acciones que correspondan para conjurar la situación".*

Hallazgo 2.9 En el contrato 1134 de 2023 y en el contrato 1191 de 2023 no se ha realizado la liquidación de los contratos.

Caso 1. Contrato 1134 de 2023

Con el requerimiento No. 3 se solicitó Acta de liquidación del contrato, cuyo plazo de ejecución terminó el 30 de diciembre de 2023. Sin embargo, el proceso respecto a la liquidación del contrato informó:

> **"***Actualmente, nos encontramos en el proceso de diligenciamiento de los formatos de lista de chequeo, informe final de ejecución y acta de liquidación. Una vez se complete la documentación en su totalidad, será radicada ante la Subdirección Contractual para su revisión, aprobación y posterior publicación en la plataforma SECOP, conforme a los procedimientos establecidos*"**.**

Lo anterior, conlleva al incumplimiento de la cláusula décima novena del contrato 1134 de 2023, que señala:

> **"***DÉCIMA NOVENA - LIQUIDACIÓN. - Terminada la ejecución del contrato, se procederá a su liquidación bilateral durante los seis (6) meses siguientes a la finalización del plazo de ejecución del presente contrato"*.

Incumplimiento de la cláusula octava, numeral 11 del contrato 1134 de 2023, que señala:

> ***"**11. Solicitar la liquidación del contrato una vez este se termine, adjuntando los soportes correspondientes".*

Incumplimiento del Manual de Supervisión e Interventoría GCC-TIC-MA-005 V.2, que señala:

> *"Responsabilidad de los Supervisores o Interventores*
>
> 4. *Adelantar e impulsar y hacer seguimiento al trámite para la liquidación de los contratos, atendiendo lo previsto en la Ley, el presente Manual y el Procedimiento de la Entidad".*

Caso 2. contrato 1191 de 2023

Con el requerimiento No. 5 se solicitó Acta de liquidación del contrato, cuyo plazo de ejecución terminó el 15 de diciembre de 2023. Sin embargo, el proceso respecto a la liquidación del contrato informó:

> **"***Actualmente, nos encontramos en el proceso de diligenciamiento de los formatos de lista de chequeo, informe final de ejecución y acta de liquidación. Una vez se complete la documentación en su totalidad, será radicada ante la*

*Subdirección Contractual para su revisión, aprobación y posterior publicación en la plataforma SECOP, conforme a los procedimientos establecidos”***.**

Lo anterior, conlleva al incumplimiento de la cláusula décima séptima del contrato 1191 de 2023, que señala:

“*DÉCIMA SÉPTIMA - LIQUIDACIÓN. - Terminada la ejecución del contrato, se procederá a su liquidación bilateral durante los seis (6) meses siguientes a la finalización del plazo de ejecución del presente contrato”*.

Incumplimiento de la cláusula octava, numeral 11 del contrato 1191 de 2023, que señala:

“*11. Remitir a la Subdirección de Gestión Contractual para revisión y ajustes el proyecto de acta de liquidación del contrato una vez este se termine, adjuntando el balance económico y los soportes correspondientes, de ser necesario”.*

Incumplimiento del Manual de Supervisión e Interventoría GCC-TIC-MA-005 V.2, que señala:

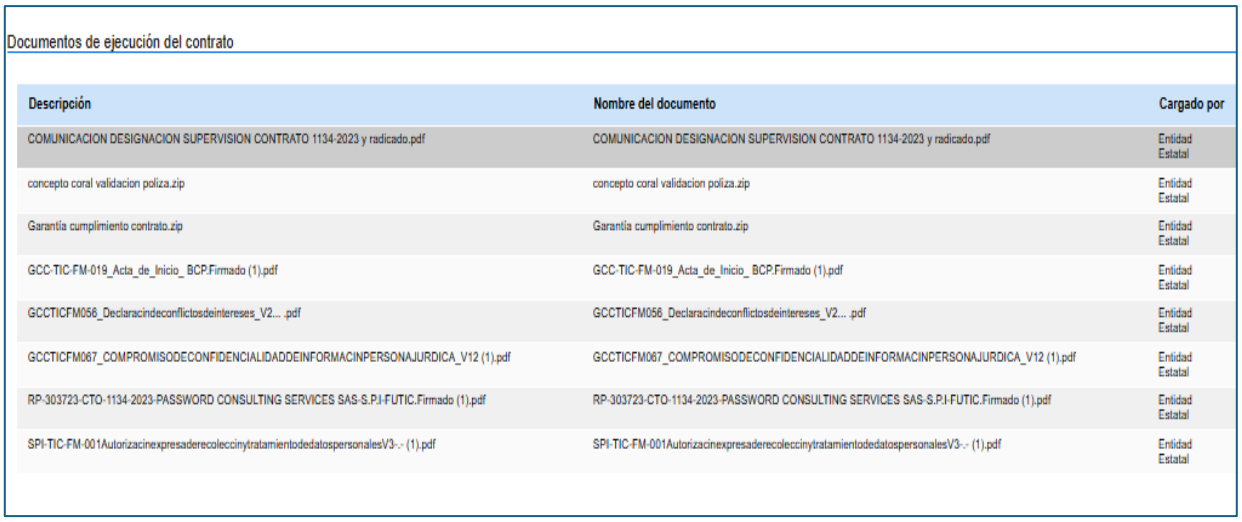
“Responsabilidad de los Supervisores o Interventores

4. *Adelantar e impulsar y hacer seguimiento al trámite para la liquidación de los contratos, atendiendo lo previsto en la Ley, el presente Manual y el Procedimiento de la Entidad”.*

Hallazgo 2.10 En el contrato 1134 de 2023, contrato 1191 de 2023 y contrato 1222 de 2023 no se publicaron en el SECOP II los informes de supervisión GCC-TIC-FM-051y GCC-TIC-FM-055.

Caso 1. Contrato 1134 de 2023

Verificado el SECOP II se evidenció que no se publicaron los informes de supervisión GCC-TIC-FM-051, en el sistema, como se muestra a continuación:

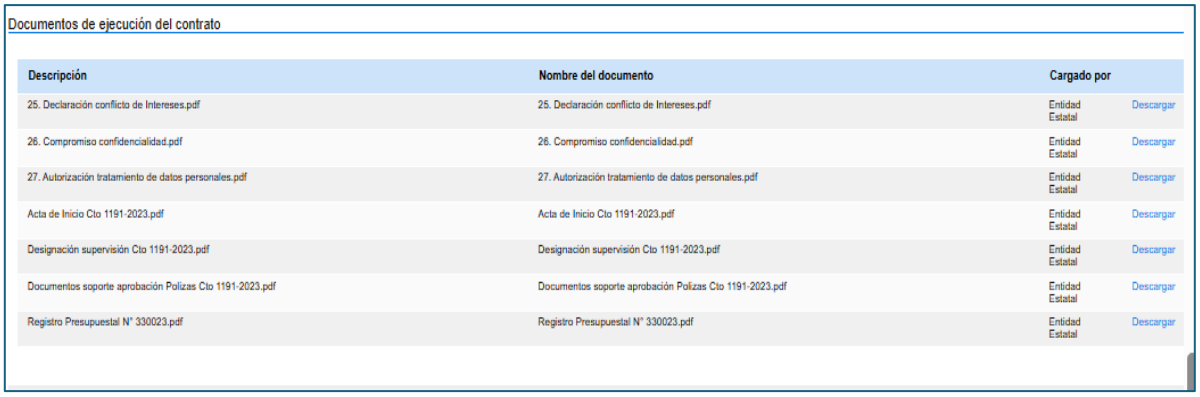


Documentos de ejecución del contrato

Descripción	Nombre del documento	Cargado por
COMUNICACION DESIGNACION SUPERVISION CONTRATO 1134-2023 y radicado.pdf	COMUNICACION DESIGNACION SUPERVISION CONTRATO 1134-2023 y radicado.pdf	Entidad Estatal
concepto coral validacion poliza.zip	concepto coral validacion poliza.zip	Entidad Estatal
Garantía cumplimiento contrato.zip	Garantía cumplimiento contrato.zip	Entidad Estatal
GCC-TIC-FM-019_Acta_de_Inicio_ BCP.Firmado (1).pdf	GCC-TIC-FM-019_Acta_de_Inicio_ BCP.Firmado (1).pdf	Entidad Estatal
GCCTICFM056_Declaracindeconflictosdeintereses_V2... .pdf	GCCTICFM056_Declaracindeconflictosdeintereses_V2... .pdf	Entidad Estatal
GCCTICFM067_COMPROMISODECONFIDENCIALIDADDEINFORMACINPERSONAJURDICA_V12 (1).pdf	GCCTICFM067_COMPROMISODECONFIDENCIALIDADDEINFORMACINPERSONAJURDICA_V12 (1).pdf	Entidad Estatal
RP-303723-CTO-1134-2023-PASSWORD CONSULTING SERVICES SAS-S.P.I-FUTIC.Firmado (1).pdf	RP-303723-CTO-1134-2023-PASSWORD CONSULTING SERVICES SAS-S.P.I-FUTIC.Firmado (1).pdf	Entidad Estatal
SPI-TIC-FM-001Autorizacinexpresaderecoleccinytratamientodedatospersonalesv3-.- (1).pdf	SPI-TIC-FM-001Autorizacinexpresaderecoleccinytratamientodedatospersonalesv3-.- (1).pdf	Entidad Estatal

Caso 2. contrato 1191 de 2023

Verificado el SECOP II se evidenció que no se publicaron los informes de supervisión GCC-TIC-FM-051, en el sistema, como se muestra a continuación:



Documentos de ejecución del contrato

Descripción	Nombre del documento	Cargado por	
25. Declaración conflicto de Intereses.pdf	25. Declaración conflicto de Intereses.pdf	Entidad Estatal	Descargar
26. Compromiso confidencialidad.pdf	26. Compromiso confidencialidad.pdf	Entidad Estatal	Descargar
27. Autorización tratamiento de datos personales.pdf	27. Autorización tratamiento de datos personales.pdf	Entidad Estatal	Descargar
Acta de Inicio Cto 1191-2023.pdf	Acta de Inicio Cto 1191-2023.pdf	Entidad Estatal	Descargar
Designación supervisión Cto 1191-2023.pdf	Designación supervisión Cto 1191-2023.pdf	Entidad Estatal	Descargar
Documentos soporte aprobación Polizas Cto 1191-2023.pdf	Documentos soporte aprobación Polizas Cto 1191-2023.pdf	Entidad Estatal	Descargar
Registro Presupuestal N° 330023.pdf	Registro Presupuestal N° 330023.pdf	Entidad Estatal	Descargar

Caso 3. Contrato 1222 de 2023

Verificado el SECOP II se evidenció que no se publicaron los informes de supervisión GCC-TIC-FM-055, en el sistema, como se muestra a continuación:

Documentos de ejecución del contrato

Descripción	Nombre del documento	Cargado por
19. Declaración conflicto de intereses.pdf	19. Declaración conflicto de intereses.pdf	Entidad Estatal
20. Compromiso de confidencialidad.pdf	20. Compromiso de confidencialidad.pdf	Entidad Estatal
21. Autorización tratamiento de datos personales.pdf	21. Autorización tratamiento de datos personales.pdf	Entidad Estatal
Designación de supervisión Cto 1222-2023.pdf	Designación de supervisión Cto 1222-2023.pdf	Entidad Estatal
Documentos Soporte Aprobación Polizas Cto 1222-2023.pdf	Documentos Soporte Aprobación Polizas Cto 1222-2023.pdf	Entidad Estatal
Registro Presupuestal N° 341223.pdf	Registro Presupuestal N° 341223.pdf	Entidad Estatal

Lo anterior conlleva al incumplimiento del Decreto 1081 de 2015, artículo 2.1.1.2.1.8., que señala:

> **"***Publicación de la ejecución de contratos. Para efectos del cumplimiento de la obligación contenida en el literal g) del artículo 11 de la Ley 1712 de 2014, relativa a la información sobre la ejecución de contratos, el sujeto obligado debe publicar las aprobaciones, autorizaciones, requerimientos o* ***informes del supervisor*** *o del interventor, que prueben la ejecución del contrato***".**

Hallazgo 2.11 En el contrato 2047 de 2024 no se cumplió con los términos establecidos para la entrega de los documentos requeridos en las obligaciones contractuales y no se evidenció la aprobación del supervisor de ciertos documentos.

Caso 1.

Con el requerimiento No. 6 se solicitó soporte de entrega al supervisor del contrato de los informes de las actividades realizadas durante el mes o periodo de ejecución del contrato. Sin embargo, el proceso remitió respecto al soporte de entrega al supervisor del contrato de los informes de las actividades, la siguiente información:

- Los informes de ejecución del contrato 2047-2024 en formato PDF.

Lo anterior, conlleva al incumplimiento de la Obligación General No. 7 del contrato 2047 de 2024, que señala:

> **"***Entregar al supervisor del control de ejecución del contrato dentro de los primeros cinco (5) días hábiles del mes, el informe de las actividades realizadas durante el mes o periodo****…".***

Caso 2

Con el requerimiento No. 6 se solicitó soporte de entrega del plan, del proyecto donde se definió la metodología de trabajo, el plan de trabajo y cronograma de actividades y recursos destinados para la ejecución del proyecto. Sin embargo, el proceso remitió respecto al soporte de entrega del plan, del proyecto donde se definió la metodología de trabajo, el plan de trabajo y cronograma de actividades y recursos destinados para la ejecución del proyecto, la siguiente información:

- Repositorio de los soportes con la información relacionada con las metodologías y los cronogramas de las actividades realizadas.

Lo anterior conlleva al incumplimiento de la obligación especifica No. 5 del contrato 2047 de 2024, que señala:

> "*Proporcionar al Ministerio / Fondo Único de TIC dentro de los dos (2) días hábiles siguientes a la suscripción del acta de inicio y de común acuerdo con el*

supervisor del contrato, un plan de proyecto donde se defina la metodología de trabajo, el plan de trabajo y cronograma de actividades y recursos destinados para la ejecución del proyecto".

Caso 3.

Con el requerimiento No. 6 se solicitó soporte de entrega del informe, en donde se detalle la parametrización de la herramienta SaaS.

Sin embargo, el proceso remitió respecto al soporte de entrega del informe, en donde se detalle la parametrización de la herramienta SaaS, la siguiente información:

- Repositorio de los diferentes soportes relacionados con la parametrización de la herramienta SaaS, incluyendo la evidencia del proceso de configuración de estilos alineados con la imagen corporativa, la habilitación de accesos, la creación y ajuste de cursos y las sesiones de formación brindadas al área funcional.

Lo anterior conlleva al incumplimiento de la obligación especifica No. 8 del contrato 2047 de 2024, que señala:

"*Entregar un informe, dentro de los (8) ocho días hábiles siguientes a la suscripción del acta de inicio, en donde se detalle la parametrización de la herramienta SaaS junto con la versión final de los instrumentos mencionados en la obligación 5 y la documentación para la parametrización de la herramienta. Este informe debe incluir configuración, forma de envío de simulaciones de ingeniería social, sincronización de usuarios e integración con servicios de autenticación, creación de cuentas administrativas, asignación de permisos, incorporación de imagen corporativa, carga de los usuarios y configuración de grupos de usuarios entre otros detalles considerados necesarios para la correcta puesta en funcionamiento del sistema"*.

Caso 4.

Con el requerimiento No. 6 se solicitó soporte de entrega del informe técnico de ejecución en donde se evidencie el detalle de cada prueba realizada, metodología utilizada, evidencias encontradas de las fallas identificadas, análisis del resultado de las pruebas realizadas, el análisis de riesgos que incluya la probabilidad y el impacto que generaría la materialización de estos, el estado (diagnóstico) en materia de seguridad y privacidad de la información, seguridad digital y continuidad de las operaciones en relación con el factor humano y soporte de aprobación por el supervisor del contrato.

Sin embargo, el proceso remitió respecto al soporte de entrega del informe técnico y soporte de aprobación por el supervisor del contrato, la siguiente información:

- El informe técnico.

- No se suministró información sobre la fecha de finalización de las pruebas.

Lo anterior conlleva al incumplimiento de la obligación especifica No. 15 del contrato 2047 de 2024, que señala:

> "*Realizar informe técnico de ejecución en donde se evidencie el detalle de cada prueba realizada, metodología utilizada, evidencias encontradas de las fallas identificadas, análisis del resultado de las pruebas realizadas, el análisis de riesgos que incluya la probabilidad y el impacto que generaría la materialización de estos, el estado (diagnóstico) en materia de seguridad y privacidad de la información, seguridad digital y continuidad de las operaciones en relación con el factor humano*, ***dicho informe deberá ser entregado tres (3) días hábiles después de la finalización de las pruebas y deberá ser aprobado por el supervisor del contrato".***

Caso 5.

Con el requerimiento No. 6 se solicitó soporte de entrega del Informe ejecutivo que resuma el informe técnico y presente una idea general del estado de concienciación de los colaboradores de la entidad y soporte de aprobación por el supervisor del contrato. Sin embargo, el proceso remitió respecto al soporte de entrega del informe ejecutivo y soporte de aprobación por el supervisor del contrato, la siguiente información:

- El informe ejecutivo.

Lo anterior conlleva al incumplimiento de la obligación especifica No. 16 del contrato 2047 de 2024, que señala:

> "*Proporcionar informe ejecutivo que resuma el informe técnico y presente una idea general del estado de concienciación de los colaboradores de la entidad,* ***cuyo contenido deberá ser aprobado por el supervisor del contrato y deberá ser entregado al mismo tiempo que el informe técnico****"*.

Caso 6.

Con el requerimiento No. 6 se solicitó soporte de entrega del Plan de remediación de vulnerabilidades para tratar las brechas de seguridad identificadas en la fase de diagnóstico y soporte de aprobación por el supervisor del contrato. Sin embargo, el proceso remitió respecto al soporte de entrega del plan y soporte de aprobación por el supervisor del contrato, la siguiente información:

- Plan de remediación junto con el documento anexo referente al plan de concienciación propuesto por el contratista**.**

Lo anterior conlleva al incumplimiento de la obligación especifica No. 17 del contrato 2047 de 2024, que señala:

> **"***Entregar un plan de remediación de vulnerabilidades para tratar las brechas de seguridad identificadas en la fase de diagnóstico, el cual determine las recomendaciones a nivel gerencial y técnico, buenas prácticas, manejo y concienciación de los colaboradores del Ministerio/Fondo Único de TIC, así como contener específicamente el diseño de un plan de concienciación de un año, en los términos establecidos en el anexo técnico, el cual hace parte integral de esta contratación*. ***Este plan deberá ser entregado cinco (5) días hábiles después de la finalización de las pruebas y deberá ser aprobado por el supervisor del contrato".***

Caso 7.

Con el requerimiento No. 6 se solicitó soporte de entrega de las hojas de vida que den cumplimiento a los requisitos habilitantes establecidos en el Estudio Previo y en el Pliego de Condiciones y sus Anexos. Sin embargo, el proceso remitió respecto al soporte de entrega de las hojas de vida, la siguiente información:

- Correos electrónicos de revisión de las hojas de vida.

Lo anterior conlleva al incumplimiento de la obligación especifica No. 4 del contrato 2047 de 2024, que señala:

> **"***Allegar dentro de los tres (3) días hábiles siguientes a la suscripción del Contrato, las hojas de vida y los soportes de los profesionales propuestos que den cumplimiento a los requisitos habilitantes establecidos en el Estudio Previo y en el Pliego de Condiciones y sus Anexos".*

Caso 8.

Con el requerimiento No. 6 se solicitó soporte de entrega de los manuales detallados tanto para administradores como para usuarios finales del producto o servicio suministrado. Sin embargo, el proceso remitió respecto al soporte de entrega de los manuales, la siguiente información:

- Dentro de la plataforma se cuenta con apartado tipo Toolkit, en donde se detallan las guías para el uso de los usuarios en la plataforma. Se cargan en el repositorio los pantallazos de dichas guías.

Lo anterior conlleva al incumplimiento del numeral 7.4.2 Características técnicas del anexo técnico, numeral 20 del contrato 2047 de 2024, que señala:

> **"***Entregar manuales detallados tanto para administradores como para usuarios finales del producto o servicio suministrado. Estos manuales deberán contener información clara y completa sobre el funcionamiento, la configuración, la administración y el uso del producto o servicio.* ***La entrega de los manuales deberá realizarse en un plazo máximo de treinta (30) días a partir de la firma del contrato****".*

Hallazgo 2.12 En el contrato 2047 de 2024 no se cumplieron obligaciones específicas, obligaciones frente al Sistema Integrado de Gestión y obligaciones del anexo técnico.

Caso 1.

Con el requerimiento No. 6 se solicitó Informe vigente de evaluación de los estándares del Sistema de Gestión de Seguridad y Salud en el Trabajo y soporte de entrega al supervisor del control de ejecución del contrato de este informe. Sin embargo, el proceso respecto al soporte de entrega del informe y soporte de entrega al supervisor del contrato informó:

> "*Para efectos del objeto a contratar, el informe vigente de evaluación de los estándares del Sistema de Gestión de Seguridad y Salud en el Trabajo y Soporte no aplica. En su lugar, se aporta el certificado del revisor fiscal en el que se acredite que el oferente cumple con el pago de salarios, prestaciones sociales y las obligaciones con los sistemas de salud, riesgos laborales ARL, pensiones y aportes a las cajas de compensación familiar, instituto de bienestar familiar ICBF y Servicio Nacional de aprendizaje – SENA"***.**

Lo anterior conlleva al incumplimiento de la obligación frente al Sistema Integrado de Gestión No. 9 del contrato 2047 de 2024, que señala:

> "*Entregar al supervisor del control de ejecución del contrato, el informe vigente de evaluación de los estándares del Sistema de Gestión de Seguridad y Salud en el Trabajo dentro de los tres (3) días hábiles contados a partir de la suscripción del Acta de Inicio, acorde con lo establecido en la normatividad relacionada"***.**

E incumplimiento del principio de planeación de la contratación estatal, el cual va encaminado a que, lo que se determine en los documentos contractuales se cumpla por el contratista, no obstante, se incluyeron obligaciones que no eran requeridas ejecutar por este.

Caso 2

Con el requerimiento No. 6 se solicitó soporte de la capacitación Certified Penetration Testing Engineer – CPTE avalada por el fabricante: MILE2 para quince (15) beneficiarios y Actas de entrega de las certificaciones firmadas por los beneficiarios de la certificación y el supervisor del contrato. Sin embargo, el proceso remitió respecto al aval del fabricante MILE2 para quince (15) beneficiarios y Actas de entrega de las certificaciones firmadas por los beneficiarios de la certificación y el supervisor del contrato, la siguiente información:

- Memorando de invitación a la capacitación para 12 colaboradores del Ministerio/Fondo Único de TIC.
- Correo electrónico donde se informó la entrega de váuchers o cupones.

Lo anterior conlleva al incumplimiento de la obligación especifica No. 19 del contrato 2047 de 2024, que señala:

> "*Realizar capacitación en la Certificación Certified Penetration Testing Engineer – CPTE la cual debe estar avalada por el fabricante: MILE2 para quince (15) beneficiarios y hacer entrega de los certificados con el acta de entrega correspondiente conforme con lo señalado en el anexo técnico"*.

E incumple el anexo técnico numeral 5.2.1.1 Proceso de Formación, que señala:

> "*Entregable: Actas de entrega de certificaciones Certified Penetration Testing Engineer (CPTE) firmadas por los beneficiarios de la certificación y el supervisor del contrato*".

Caso 3.

Con el requerimiento No. 6 se solicitó soporte de la capacitación virtual con al menos tres (3) talleres prácticos de 4 horas sobre la administración y parametrización de la herramienta, administración de los usuarios, módulos y uso de las funcionalidades de los módulos, dirigida a los usuarios con rol administrador del GIT de Seguridad y Privacidad de la Información.

Sin embargo, el proceso remitió respecto al soporte de la capacitación virtual, la siguiente información:

- Correos electrónicos de planeación sobre unas capacitaciones, donde no se determina a cuáles capacitaciones se refiere.
- Citaciones por Teams a unas capacitaciones (28-04-2025, 11-04-2025, 10-04-2025, 09-04-2025) y pantallazo de capacitación del 09-04-2025, no obstante, no se evidencia que se relacionen con la obligación señalada.

Lo anterior conlleva al incumplimiento del numeral 7.4.2 Características técnicas del anexo técnico, numeral 21 del contrato 2047 de 2024, que señala:

> *"El proveedor deberá efectuar capacitación virtual con al menos tres (3) talleres prácticos de 4 horas sobre la administración y parametrización de la herramienta, administración de los usuarios, módulos y uso de las funcionalidades de los módulos, dirigida a los usuarios con rol administrador del GIT de Seguridad y Privacidad de la Información, las cuales serán programadas en común acuerdo con la supervisión del contrato, en el tiempo comprendido entre las 8:00 a.m. a 5:00 p.m. horario hábil de lunes a viernes. Así mismo, cuatro (4) horas de capacitación (masiva) con talleres prácticos dirigida a los usuarios finales de cada proceso de la entidad, en donde explique cada uno de los módulos visibles en este rol".*

Caso 4.

Con el requerimiento No. 6 se solicitó cronograma para la transferencia de conocimientos sobre la instalación, implementación y operación de la herramienta.

Sin embargo, el proceso remitió respecto al soporte del cronograma, la siguiente información:

- Correos electrónicos de planeación sobre unas capacitaciones, donde no se determina a cuáles capacitaciones se refiere.
- Citaciones por Teams a unas capacitaciones (28-04-2025, 11-04-2025, 10-04-2025, 09-04-2025) y pantallazo de capacitación del 09-04-2025, no obstante, no se evidencia que se relacionen con la obligación señalada.

Lo anterior conlleva al incumplimiento del numeral 7.5 transferencia del conocimiento del anexo técnico, numeral 1 del contrato 2047 de 2024, que señala:

> "*Para asegurar el buen funcionamiento y aprovechamiento de las funcionalidades y soluciones del proveedor, es necesario desarrollar un cronograma para la transferencia de conocimientos sobre la instalación, implementación y operación de la herramienta. Se establece un mínimo de diez (10) horas para la capacitación sobre la solución implementada. Es importante señalar que esta transferencia de conocimiento se hará con el personal designado por el supervisor del contrato, sin límite en el número de participantes*".

Hallazgo 2.13 En el contrato 1222 de 2023 no se cumplieron obligaciones específicas y obligaciones del anexo técnico.

Caso 1.

Con el requerimiento No. 6 se solicitó soporte de radicación de las hojas de vida junto con sus soportes al supervisor del contrato y soporte de aprobación del supervisor de las hojas de vida. Sin embargo, el proceso remitió respecto al soporte de soporte de radicación de la hoja de vida y soporte de aprobación del supervisor de la hoja de vida, la siguiente información:

- Formato para evaluar al auditor líder- Edgar Fernando Suárez Mendoza.
- Hoja de vida de la Ing. Adriana Sandoval
- Hoja de vida de del Ing. Edgar Fernando Suárez.

Lo anterior conlleva al incumplimiento de la obligación especifica No. 4 del contrato 1222 de 2023, que señala:

> "*Presentar dentro de los tres (3) días hábiles siguientes a la suscripción del contrato, los soportes de la formación y experiencia del equipo de trabajo*

requerido para la ejecución del contrato y que se encuentran descritos en el anexo técnico".

E incumple el numeral 5 "Equipo de trabajo" del anexo técnico, que señala:

"*El supervisor del contrato contará con un máximo de dos (2) días hábiles contados a partir de la fecha de radicación de la hoja de vida junto con sus soportes para emitir su aprobación o solicitar corrección o ajustes*".

Caso 2.
Con el requerimiento No. 6 se solicitó soporte de presentación en cualquier programa que incluya mínimo los siguientes aspectos: (1) Presentación del equipo auditor; (2) Comunicación del objetivo y criterios de la auditoria definidos entre las partes; (3) Metodología del proceso de auditoria; (4) Plan de auditoria; y (5) Fecha y duración de la auditoria de acuerdo con el modelo de operación por procesos de la Entidad.

Sin embargo, el proceso remitió respecto al soporte de presentación en cualquier programa, la siguiente información:

- La grabación, de la reunión del Plan de Auditoria, realizada el 30 de octubre de 2023, no obstante, en dicha reunión no se evidenció presentación alguna relacionada con los puntos indicados en la obligación.

Lo anterior conlleva al incumplimiento del anexo técnico punto 4.1 "Desagregación del Objeto. Etapa 1. Preparación" literal C, del contrato 1222 de 2023, que señala:

"Elaborar una presentación en cualquier programa (power point, prezi, google slides, canva, visme, apple keynote, swipe, zohoshow, slidedog, sorma, etc.) que incluya mínimo los siguientes aspectos: (1) Presentación del equipo auditor; (2) Comunicación del objetivo y criterios de la auditoria definidos entre las partes; (3) Metodología del proceso de auditoria; (4) Plan de auditoria; y (5) Fecha y duración de la auditoria de acuerdo con el modelo de operación por procesos de la Entidad".

Caso 3.
Con el requerimiento No. 6 se solicitó soporte de entrega del plan de auditoría de seguimiento a la certificación del sistema de gestión de seguridad de la información.
Sin embargo, el proceso remitió respecto al soporte de entrega del plan de auditoría, la siguiente información:

- La grabación, de la reunión del Plan de Auditoria, realizada el 30 de octubre de 2023.

Lo anterior conlleva al incumplimiento del anexo técnico punto 4.1 "Desagregación del Objeto. Etapa 1. Preparación" literal G, del contrato 1222 de 2023, que señala:

> *"G. Entregar en un máximo de tres (3) días calendario, a la suscripción del contrato, el plan de auditoría de seguimiento a la certificación del sistema de gestión de seguridad de la información que incluya como mínimo: (1) Objetivos de la auditoria; (2) Documentos y criterios de referencia; (3) alcance; (4) fecha; (5) hora y duración de actividades; (6) dependencias, responsabilidades y funciones de los miembros del equipo auditor; y (7) recursos que se emplean".*

Caso 4.

Con el requerimiento No. 6 se solicitó Informe preliminar de auditoría que contenga resultados obtenidos durante la ejecución de la auditoria de seguimiento al Sistema de Gestión de Seguridad de la Información NTC-ISO 27001:2013. Sin embargo, el proceso remitió respecto al Informe preliminar de auditoría, la siguiente información:

- Nota de no conformidad.
- Correos electrónicos comunicando la nota de no conformidad.

Lo anterior conlleva al incumplimiento del anexo técnico punto 4.1 "Desagregación del Objeto. Etapa 3. Presentación de Informe y Resultados" literal A, del contrato 1222 de 2023, que señala:

> "*Presentar en la reunión presencial de cierre un informe preliminar de auditoría que contenga resultados obtenidos durante la ejecución de la auditoria de seguimiento al Sistema de Gestión de Seguridad de la Información NTC-ISO 27001:2013, luego de un (1) día calendario de terminada la etapa 2, que incluya aspectos relevantes como: debilidades, fortalezas, oportunidades de mejora, observaciones, recomendaciones, no conformidades y se comunicará la decisión tomada en relación con la revisión al otorgamiento o seguimiento del certificado*".

Caso 5.

Con el requerimiento No. 6 se solicitó soporte de respuesta a las inquietudes u observaciones presentadas por la entidad, frente al informe preliminar de auditoría de seguimiento entregado por el contratista. Sin embargo, el proceso remitió respecto al soporte de respuesta a las inquietudes u observaciones presentadas por la entidad, frente al informe preliminar de auditoría, la siguiente información:

- Nota de no conformidad.
- Correos electrónicos comunicando la nota de no conformidad.

Lo anterior conlleva al incumplimiento del anexo técnico punto 4.1 "Desagregación del Objeto. Etapa 3. Presentación de Informe y Resultados" literal A, del contrato 1222 de 2023, que señala:

"*Dar respuesta y demás ajustes en un máximo de tres (3) días calendario a las inquietudes u observaciones presentadas por la entidad, frente al informe preliminar de auditoría de seguimiento entregado por el contratista"***.**

Caso 6.

Con el requerimiento No. 6 se solicitó soporte de entrega al supervisor del contrato del informe final de la auditoria de seguimiento a la certificación del sistema de gestión de Seguridad de la Información.

Sin embargo, el proceso remitió respecto al soporte de entrega al supervisor del contrato del informe final de la auditoria, la siguiente información:

- Informe de auditoría.

Lo anterior conlleva al incumplimiento del anexo técnico punto 4.1 "Desagregación del Objeto. Etapa 3. Presentación de Informe y Resultados" literal C, del contrato 1222 de 2023, que señala:

> *"Entregar al supervisor del contrato el informe final de la auditoria de seguimiento a la certificación del sistema de gestión de Seguridad de la Información, máximo a los tres (3) días calendario siguientes a la entrega de las observaciones de la entidad, en la cual se detalle los resultados obtenidos, la conclusión"*.

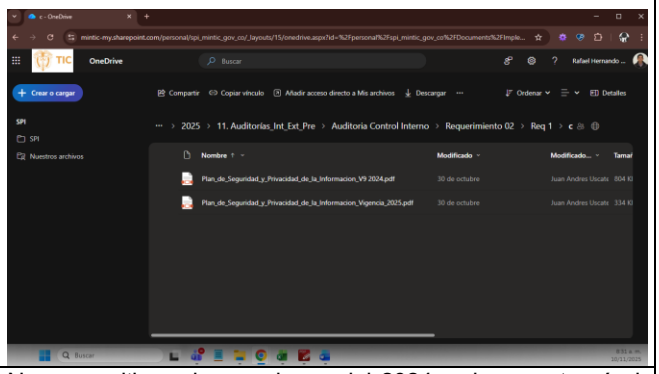
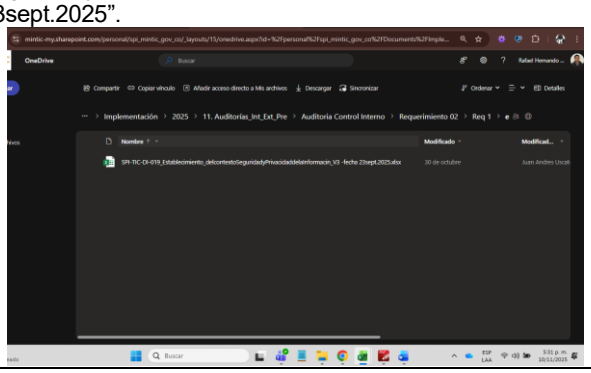
Hallazgo transversal 3.1. Los soportes y evidencias suministrados durante el proceso de auditoría no fueron entregados, se encontraron incompletos, presentan inconsistencias en su contenido, o fueron entregados por fuera de los plazos establecidos.

Al revisar la información y documentos entregados por el proceso en relación con los requerimientos efectuados, se evidenció que algunos de estos no fueron entregados completamente, presentan inconsistencias entre la solicitud realizada y el soporte entregado, o presentan inconsistencias en su contenido, incumpliendo los numerales 1 y 3 definidos en la Carta de representación firmada por el proceso, que indican:

> "*1. Todo el equipo de trabajo que atenderá las solicitudes es responsable de la oportuna preparación, presentación y consistencia de la información que será entregada en el marco de la auditoría interna.*
> *3. La información que suministraremos será válida, integral y completa para los propósitos de la auditoría interna*".

En la siguiente tabla se relacionan el número del requerimiento, el detalle de la solicitud, el documento entregado y la observación en la que se identifica la inconsistencia presentada:

Informe de Auditoría

Id	Req	Descripción de la solicitud	Documentos suministrados o respuesta	Observación
1	2.1.c	c. Planes de Seguridad y Privacidad de la Información, incluyendo todos los anexos y documentos que lo acompañen. Indicar si existieron versiones anteriores, en caso positivo, remitir los documentos.	Versiones 9 y 11.	Se solicitaron todas las versiones del 2024 al 2025, sin embargo, solo se entregaron las versiones 9 y 11. Las versiones 8 y 10 que se encontraban dentro del alcance de la auditoría no fueron suministradas. 
2	2.1.e	e. Documentos de Establecimiento del Contexto del Proceso de Seguridad y Privacidad de la Información, especificando las versiones y las fechas de publicación.	Se incluye el documento de Establecimiento de Contexto vigente. Para el caso de la vigencia 2024, se cargan en el repositorio los documentos aprobados en su momento en SIMIG ya que no tenemos acceso desde esta herramienta para descargar versiones anteriores a la actual.	No se remitieron las versiones del 2024, solo se entregó el documento “SPI-TIC-DI-019_Establecimiento_delcontexto SeguridadyPrivacidaddelaInformacin_V3 -fecha 23sept.2025”. 
3	2.5.e	e. Planes de mejoramiento derivados de incidentes y evidencia de seguimiento.	En el repositorio se cargan carpeta con la evidencia de seguimiento de los casos reportados.	El proceso suministró varios documentos sin un orden lógico de lectura, con soportes individuales de gestión y respuesta, incluyendo que no se identificaron los planes de mejoramiento a los incidentes solicitados.
4	2.8.a	a. Indicar en donde se encuentran establecidos los procesos y procedimientos para retención, conservación y destrucción de información digital. Adicional, remitir el documento oficial de la entidad indicando específicamente donde se encuentra este lineamiento.	Se cuenta con un procedimiento GTI-TIC-PR-007 BORRADO DE INFORMACIÓN V6, donde	Al validar este documento en SIMIG, el código está incorrecto. El código del documento es GTI-TIC-IN-033.

Id	Req	Descripción de la solicitud	Documentos suministrados o respuesta	Observación
5	2.16.f	f. Presentaciones, boletines o correos internos donde se hayan compartido lecciones aprendidas.	Se anexa el documento compartido dentro de las actividades de documentación de las lecciones aprendidas: Sugerencias Estrategias de Contingencia IntegraTIC. Se entregó un documento "Sugerencias Estrategias de Contingencia IntegraTIC".	Al validar este documento, no es claro cómo evidencia la socialización de las lecciones aprendidas.
6	6	Solicitud soportes obligaciones de los contratos 1222-2023 y 2047 -2024.	No se suministró información.	El día 12-11-2025 se solicitó información de los contratos. Esta solicitud se reiteró el día 18-11-2025.Posteriormente, el día 19-11-2025 la OCI, le comunico al Líder del Proceso que el plazo para presentar la información había expirado, de lo cual se dejaría un hallazgo, sin embargo, el proceso suministró la información de forma extemporánea.

7. TABLA DE HALLAZGOS IDENTIFICADOS

Como resultado del proceso de auditoría, se identificaron 22 hallazgos, que a continuación se detallan:

ítem	N. del Hallazgo	Resumen del Hallazgo	Riesgo identificado
1	**Hallazgo 1.1.** No se encuentran establecidos los roles y responsabilidades asociados a la seguridad digital.	Se identifica que el documento entregado como evidencia no tiene establecidos los roles y responsabilidades asociados a la seguridad digital, conllevando al incumplimiento de lo indicado en el "Documento Maestro Lineamientos MSPI".	"No se encuentra identificado en la matriz de riesgos del proceso".
2	**Hallazgo 1.2.** Incumplimiento del artículo 9 de la Resolución 500 de 2021.	Al validar las evidencias suministradas se identificó: **Caso 1.** No se encuentra documentado cómo están catalogados los incidentes Graves o Muy Graves. **Caso 2:** Los incidentes Menos graves o menores no se están comunicando al CSIRT Gobierno. **Caso 3:** Se identificaron incidentes Graves o Muy graves no reportados de acuerdo con la clasificación. **Caso 4:** No se identifican los planes de mejoramiento a los incidentes ni los seguimientos a estos.	"No se encuentra identificado en la matriz de riesgos del proceso".
3	**Hallazgo 1.3.** No se identifican indicadores para medir la eficiencia de la gestión de la seguridad de la información y la seguridad digital.	No existen indicadores para medir la Eficiencia de la gestión de la seguridad de la información y la seguridad digital, situación que está en contravía con lo establecido en el artículo 15 de la Resolución 500 de 2021 que indica: "15. Control de las actividades incluidas en la estrategia de seguridad digital y gestión de riesgos. (…) Así mismo, deberán contar con indicadores para medir la eficacia, efectividad y eficiencia de la gestión de la seguridad de la información y la seguridad digital".	"No se encuentra identificado en la matriz de riesgos del proceso".

ítem	N. del Hallazgo	Resumen del Hallazgo	Riesgo identificado
4	**Hallazgo 1.4.** Ausencia de análisis formal, estructurado y verificable de las partes interesadas en seguridad de la información.	No se evidencia un análisis formal, estructurado y verificable de las partes interesadas internas y externas en materia de seguridad y privacidad de la información, situación que conlleva al incumplimiento de la salida documental obligatoria establecida en el lineamiento 7.1.2 “Necesidades y expectativas de los interesados” del Documento Maestro de Lineamientos del MSPI.	“No se encuentra identificado en la matriz de riesgos del proceso”.
5	**Hallazgo 1.5.** Falta de delimitación clara del alcance del Modelo de Seguridad y Privacidad de la Información.	De acuerdo con el Documento Maestro de Lineamientos del MSPI, la Política de seguridad y privacidad de la información es un producto del resultado de la implementación del modelo, por lo cual, no debe considerarse que el alcance de la política sea el alcance del MSPI. El lineamiento 7.1.3 exige que la Entidad defina con claridad los límites, el alcance y la aplicabilidad del MSPI, especificando Procesos, Recursos, Activos de información y la existencia del “Alcance del MSPI” como salida obligatoria del lineamiento. Por lo anterior, no se evidencia el cumplimiento del lineamiento 7.1.3, dado que el documento remitido no cuenta con un alcance formal del MSPI, debidamente estructurado y documentado conforme a lo establecido en el Documento Maestro de Lineamientos.	“No se encuentra identificado en la matriz de riesgos del proceso”.
6	**Hallazgo 1.6.** Incumplimiento de la periodicidad en la revisión del MSPI y ausencia de su formalización en la normativa interna y matriz de roles.	No se cuenta con evidencia de que la revisión del MSPI se realice con la periodicidad establecida por el Documento Maestro de Lineamientos del MSPI, el cual indica que la revisión de la adopción del MSPI debe realizarse dos veces al año. Las actas aportadas corresponden a reuniones del 06-06-2024 y 21-08-2025. Al validar la Resolución 860 de 2025 y la Matriz de roles y responsabilidades MIG-TIC-DI-029, no se identificó documentada la acción de realizar revisiones periódicas al menos dos veces por año para la adopción, implementación y mejora continua del MSPI, incumpliendo con lo establecido en el Documento Maestro del MSPI en el numeral 7.2.1.Liderazgo y compromiso	“No se encuentra identificado en la matriz de riesgos del proceso”.
7	**Hallazgo 1.7.** El Manual de Seguridad y Privacidad no fue revisado y aprobado por el Comité de Gestión y Desempeño (Comité MIG).	En las actas suministradas como evidencia, se identificó que: • Las actas del Comité MIG No. 80 y No. 92 no evidencia la revisión, análisis o aprobación del Manual de Seguridad y Privacidad, documento que también debe ser revisado y aprobado conforme al lineamiento. • La falta de aprobación del Manual de SPI y la ausencia de reconocimiento de esta actividad por parte del comité, evidencian debilidades en los compromisos derivados de la revisión efectuada por la Dirección, dado que se define como lineamiento que el Manual de Seguridad y Privacidad debe ser revisado y aprobado por el Comité de Gestión y Desempeño, o por decisión del nominador, considerando los cambios en las necesidades de las partes interesadas.	“No se encuentra identificado en la matriz de riesgos del proceso”.

ítem	N. del Hallazgo	Resumen del Hallazgo	Riesgo identificado
		La situación mencionada se encuentra en contravía del lineamiento 9.3 Revisión por la dirección, el cual establece que el Manual de Seguridad y Privacidad debe ser revisado y aprobado por el Comité de Gestión y Desempeño, incluyendo los compromisos de la revisión por la dirección.	
8	**Hallazgo 1.8**. Ausencia del Plan Anual de Mejora del MSPI.	Se identificó que no existe un Plan Anual de Mejora del MSPI. Las evidencias entregadas corresponden a documentos que contienen actividades operativas del SGSI, pero no cumplen con los elementos exigidos para el Plan de Mejora del MSPI, dado que no consolidan oportunidades de mejora identificadas, no incluyen no conformidades, desviaciones o brechas específicas, no contienen acciones correctivas formales, ni su trazabilidad, no especifican responsables, tiempos, recursos, ni articulan la mejora continua como un plan anual integral, y en general, no contienen los mecanismos de seguimiento, tal como lo exige el modelo. Lo anterior incumple lo establecido en el lineamiento 10.1 Mejora Continua, el cual define que las entidades deben contar con un Plan de mejoramiento continuo que integre de manera formal las oportunidades de mejora, las No conformidades y las desviaciones identificadas en la gestión de los diferentes procesos de seguridad y privacidad de la información que componen el SGSI.	"No se encuentra identificado en la matriz de riesgos del proceso".
9	**Hallazgo 2.1.** En el contrato 1134 de 2023 y en el contrato 1191 de 2023 no se cumplió con la entrega de las hojas de vida de los profesionales propuestos dentro de los términos establecidos en dichos contratos.	Con el requerimiento No. 3 y No. 5 se solicitó soporte de entrega de las hojas de vida de los profesionales propuestos que den cumplimiento a los requisitos habilitantes establecidos en el Estudio Previo y en el Pliego de Condiciones. Sin embargo, el proceso remitió respecto al soporte de entrega de las hojas de vida, un soporte diferente al solicitado.	Posibilidad de afectación económica y reputacional por Incumplimiento u omisión de las normas externas e internas por parte de la supervisión A causa de las deficiencias en el seguimiento por parte del supervisor al objeto y obligaciones del contratista en términos de cantidad, calidad y oportunidad del bien o servicio contratado, así como a la ejecución financiera cuando se entreguen recursos por ejecutar y por legalizar, con el fin de evitar la pérdida de competencia para liquidar.

ítem	N. del Hallazgo	Resumen del Hallazgo	Riesgo identificado
10	**Hallazgo 2.2.** En el contrato 1134 de 2023 y en el contrato 1191 de 2023 no se cumplió con la entrega del cronograma de reuniones y mesas de trabajo dentro de los términos establecidos ni con la aprobación del supervisor de este cronograma.	Con el requerimiento No. 3 y No.5 se solicitó soporte de entrega del cronograma de reuniones y mesas de trabajo con las dependencias para levantamiento de información e insumos para la actualización de toda la documentación que compone el BCP y soporte de aprobación por el supervisor del contrato. No obstante, el proceso remitió respecto al soporte de entrega del cronograma de reuniones y mesas de trabajo y soporte de aprobación por el supervisor del contrato, evidencia que no demuestra el cumplimiento de las obligaciones contractuales.	Posibilidad de afectación económica y reputacional por Incumplimiento u omisión de las normas externas e internas por parte de la supervisión A causa de las deficiencias en el seguimiento por parte del supervisor al objeto y obligaciones del contratista en términos de cantidad, calidad y oportunidad del bien o servicio contratado, así como a la ejecución financiera cuando se entreguen recursos por ejecutar y por legalizar, con el fin de evitar la pérdida de competencia para liquidar.
11	**Hallazgo 2.3.** Falta de entrega en el contrato 1134 de 2023 y en el contrato 1191 de 2023 de las Normas Técnicas al Ministerio/FUTIC en versión digital.	Con el requerimiento No. 3 y No. 5 se solicitó soporte de entrega de las Normas Técnicas ISO/IEC 22301:2019, ISO 27001:2022 en sus últimas versiones físicas y digitales. Sin embargo, el proceso remitió respecto al soporte de entrega de las normas técnicas, evidencia que no demuestra el cumplimiento de las obligaciones contractuales.	Posibilidad de afectación económica y reputacional por Incumplimiento u omisión de las normas externas e internas por parte de la supervisión A causa de las deficiencias en el seguimiento por parte del supervisor al objeto y obligaciones del contratista en términos de cantidad, calidad y oportunidad del bien o servicio contratado, así como a la ejecución financiera cuando se entreguen recursos por ejecutar y por legalizar, con el fin de evitar la pérdida de competencia para liquidar.
12	**Hallazgo 2.4.** En el contrato 1134 de 2023 no se cedieron los derechos patrimoniales de autor de los productos que se generaron de la ejecución del contrato a favor del Fondo Único de TIC.	Con el requerimiento No. 3 se solicitó soporte de la cesión de los derechos patrimoniales de autor de los productos que se generaron en la ejecución del contrato a favor del Fondo Único de TIC. Sin embargo, el proceso no remitió soporte de la cesión de los derechos patrimoniales de autor.	Posibilidad de afectación económica y reputacional por Incumplimiento u omisión de las normas externas e internas por parte de la supervisión A causa de las deficiencias en el seguimiento por parte del supervisor al objeto y obligaciones del contratista en términos de cantidad, calidad y oportunidad del bien o servicio contratado, así como a la ejecución financiera cuando se entreguen recursos por ejecutar y por legalizar, con el fin de evitar la pérdida de competencia para liquidar.
13	**Hallazgo 2.5.** En el contrato 1134 de 2023 no se evidenció soporte de remisión de las actas de reunión de seguimiento a la ejecución del contrato y de las demás mesas de trabajo o	Con el requerimiento No. 3 se solicitó soporte de remisión a la Entidad de las actas de reunión de seguimiento a la ejecución del contrato y de las demás mesas de trabajo o reuniones. Sin embargo, el proceso remitió respecto del soporte de entrega a la Entidad de las actas evidencia que no demuestra el cumplimiento de la obligación contractual.	Posibilidad de afectación económica y reputacional por Incumplimiento u omisión de las normas externas e internas por parte de la supervisión A causa de las deficiencias en el seguimiento por parte del supervisor al objeto y obligaciones del contratista en términos de cantidad, calidad y

ítem	N. del Hallazgo	Resumen del Hallazgo	Riesgo identificado
	reuniones, dentro de los cinco (5) días hábiles siguientes.		oportunidad del bien o servicio contratado, así como a la ejecución financiera cuando se entreguen recursos por ejecutar y por legalizar, con el fin de evitar la pérdida de competencia para liquidar.
14	**Hallazgo 2.6.** En el contrato 1134 de 2023 no se evidenció en la Fase 2 “Gestión del Riesgo”, el Plan de acción con las actividades determinadas y Matriz de resultados.	Con el requerimiento No. 3 se solicitó el Plan de acción con las actividades determinadas y Matriz de resultados. Sin embargo, el proceso remitió respecto al Plan de Acción con las actividades determinadas y Matriz de resultados, evidencia que no demuestra el cumplimiento de la obligación contractual.	Posibilidad de afectación económica y reputacional por Incumplimiento u omisión de las normas externas e internas por parte de la supervisión A causa de las deficiencias en el seguimiento por parte del supervisor al objeto y obligaciones del contratista en términos de cantidad, calidad y oportunidad del bien o servicio contratado, así como a la ejecución financiera cuando se entreguen recursos por ejecutar y por legalizar, con el fin de evitar la pérdida de competencia para liquidar.
15	**Hallazgo 2.7** En el contrato 1191 de 2023 no se evidenció en la Fase 2 “Actualización Del Sistema De Gestión De Datos Personales Y Construcción del Marco De Gobernanza”, el Documento Creación del marco de cumplimiento en Protección de Datos Personales y Responsabilidad Demostrada.	Con el requerimiento No. 5 se solicitó el documento Creación del marco de cumplimiento en Protección de Datos Personales y Responsabilidad Demostrada. Sin embargo, el proceso remitió respecto al documento Creación del marco de cumplimiento en Protección de Datos Personales y Responsabilidad Demostrada, evidencia que no demuestra el cumplimiento de la obligación contractual.	Posibilidad de afectación económica y reputacional por Incumplimiento u omisión de las normas externas e internas por parte de la supervisión A causa de las deficiencias en el seguimiento por parte del supervisor al objeto y obligaciones del contratista en términos de cantidad, calidad y oportunidad del bien o servicio contratado, así como a la ejecución financiera cuando se entreguen recursos por ejecutar y por legalizar, con el fin de evitar la pérdida de competencia para liquidar.
16	**Hallazgo 2.8**. En el contrato 1134 de 2023 y en el contrato 1191 de 2023 no se evidenció seguimiento a la Matriz de Riesgos establecida en dichos contratos.	Con el requerimiento No. 3 y No. 5 se solicitó soporte de seguimiento a la Matriz de Riesgos establecida en el contrato. Sin embargo, el proceso remitió respecto al soporte de seguimiento a la Matriz de Riesgos establecida en el contrato, evidencia que no demuestra el cumplimiento de las obligaciones contractuales.	Posibilidad de afectación económica y reputacional por Incumplimiento u omisión de las normas externas e internas por parte de la supervisión A causa de las deficiencias en el seguimiento por parte del supervisor al objeto y obligaciones del contratista en términos de cantidad, calidad y oportunidad del bien o servicio contratado, así como a la ejecución financiera cuando se entreguen recursos por ejecutar y por legalizar, con el fin de evitar la pérdida de competencia para liquidar.
17	**Hallazgo 2.9.** En el contrato 1134 de 2023 y en el contrato 1191	Con el requerimiento No. 3 y No. 5 se solicitó acta de liquidación de los contratos, cuyo plazo de ejecución terminó. Sin embargo, el proceso no remitió acta de	Posibilidad de afectación económica y reputacional por Incumplimiento u omisión de

ítem	N. del Hallazgo	Resumen del Hallazgo	Riesgo identificado
	de 2023 no se ha realizado la liquidación de los contratos.	liquidación e indicó que están en trámite, incumpliendo las cláusulas contractuales.	las normas externas e internas por parte de la supervisión A causa de las deficiencias en el seguimiento por parte del supervisor al objeto y obligaciones del contratista en términos de cantidad, calidad y oportunidad del bien o servicio contratado, así como a la ejecución financiera cuando se entreguen recursos por ejecutar y por legalizar, con el fin de evitar la pérdida de competencia para liquidar.
18	**Hallazgo 2.10.** En el contrato 1134 de 2023, contrato 1191 de 2023 y contrato 1222 de 2023 no se publicaron en el SECOP II los informes de supervisión GCC-TIC-FM-051 y GCC-TIC-FM-055.	Verificado el SECOP II se evidenció que no se publicaron los informes de supervisión GCC-TIC-FM-051 y GCC-TIC-FM-055, en el sistema.	Posibilidad de afectación económica y reputacional por Incumplimiento u omisión de las normas externas e internas por parte de la supervisión A causa de las deficiencias en el seguimiento por parte del supervisor al objeto y obligaciones del contratista en términos de cantidad, calidad y oportunidad del bien o servicio contratado, así como a la ejecución financiera cuando se entreguen recursos por ejecutar y por legalizar, con el fin de evitar la pérdida de competencia para liquidar.
19	**Hallazgo 2.11.** En el contrato 2047 de 2024 no se cumplió con los términos establecidos para la entrega de los documentos requeridos en las obligaciones contractuales y no se evidenció la aprobación del supervisor de ciertos documentos.	**Caso 1.** Con el requerimiento No. 6 se solicitó soporte de entrega al supervisor del contrato de los informes de las actividades realizadas durante el mes o periodo de ejecución del contrato. Sin embargo, el proceso remitió respecto al soporte de entrega al supervisor del contrato de los informes de las actividades, evidencia que no demuestra el cumplimiento de la obligación contractual. **Caso 2** Con el requerimiento No. 6 se solicitó soporte de entrega del plan, del proyecto donde se definió la metodología de trabajo, el plan de trabajo y cronograma de actividades y recursos destinados para la ejecución del proyecto. Sin embargo, el proceso remitió respecto al soporte de entrega del plan, del proyecto donde se definió la metodología de trabajo, el plan de trabajo y cronograma de actividades y recursos destinados para la ejecución del proyecto, evidencia que no demuestra el cumplimiento de la obligación contractual. **Caso 3** Con el requerimiento No. 6 se solicitó soporte de entrega del informe, en donde se detalle la parametrización de la herramienta SaaS. Sin embargo, el proceso remitió respecto al soporte de entrega del informe, en donde se detalle la parametrización de la herramienta SaaS, evidencia	Posibilidad de afectación económica y reputacional por Incumplimiento u omisión de las normas externas e internas por parte de la supervisión A causa de las deficiencias en el seguimiento por parte del supervisor al objeto y obligaciones del contratista en términos de cantidad, calidad y oportunidad del bien o servicio contratado, así como a la ejecución financiera cuando se entreguen recursos por ejecutar y por legalizar, con el fin de evitar la pérdida de competencia para liquidar.

ítem	N. del Hallazgo	Resumen del Hallazgo	Riesgo identificado
		que no demuestra el cumplimiento de la obligación contractual. **Caso 4** Con el requerimiento No. 6 se solicitó soporte de entrega del informe técnico de ejecución en donde se evidencie el detalle de cada prueba realizada, metodología utilizada, evidencias encontradas de las fallas identificadas, análisis del resultado de las pruebas realizadas, el análisis de riesgos que incluya la probabilidad y el impacto que generaría la materialización de estos, el estado (diagnóstico) en materia de seguridad y privacidad de la información, seguridad digital y continuidad de las operaciones en relación con el factor humano y soporte de aprobación por el supervisor del contrato. Sin embargo, el proceso remitió respecto al soporte de entrega del informe técnico y soporte de aprobación por el supervisor del contrato, evidencia que no demuestra el cumplimiento de la obligación contractual. **Caso 5** Con el requerimiento No. 6 se solicitó soporte de entrega del Informe ejecutivo que resuma el informe técnico y presente una idea general del estado de concienciación de los colaboradores de la entidad y soporte de aprobación por el supervisor del contrato. Sin embargo, el proceso remitió respecto al soporte de entrega del informe ejecutivo y soporte de aprobación por el supervisor del contrato, evidencia que no demuestra el cumplimiento de la obligación contractual. **Caso 6** Con el requerimiento No. 6 se solicitó soporte de entrega del Plan de remediación de vulnerabilidades para tratar las brechas de seguridad identificadas en la fase de diagnóstico y soporte de aprobación por el supervisor del contrato. Sin embargo, el proceso remitió respecto al soporte de entrega del plan y soporte de aprobación por el supervisor del contrato, evidencia que no demuestra el cumplimiento de la obligación contractual. **Caso 7** Con el requerimiento No. 6 se solicitó soporte de entrega de las hojas de vida que den cumplimiento a los requisitos habilitantes establecidos en el Estudio Previo y en el Pliego de Condiciones y sus Anexos. Sin embargo, el proceso remitió respecto al soporte de entrega de las hojas de vida, evidencia que no demuestra el cumplimiento de la obligación contractual. **Caso 8** Con el requerimiento No. 6 se solicitó soporte de entrega de los manuales detallados tanto para administradores como para usuarios finales del producto o servicio suministrado. Sin embargo, el proceso remitió respecto al soporte de entrega de los	

ítem	N. del Hallazgo	Resumen del Hallazgo	Riesgo identificado
		manuales, evidencia que no demuestra el cumplimiento de la obligación contractual.	
20	**Hallazgo 2.12.** En el contrato 2047 de 2024 no se cumplieron obligaciones específicas, obligaciones frente al Sistema Integrado de Gestión y obligaciones del anexo técnico.	**Caso 1** Con el requerimiento No. 6 se solicitó Informe vigente de evaluación de los estándares del Sistema de Gestión de Seguridad y Salud en el Trabajo y soporte de entrega al supervisor del control de ejecución del contrato de este informe. Sin embargo, el proceso respecto al soporte de entrega del informe y soporte de entrega al supervisor del contrato no remitió evidencia. **Caso 2** Con el requerimiento No. 6 se solicitó soporte de la capacitación Certified Penetration Testing Engineer – CPTE avalada por el fabricante: MILE2 para quince (15) beneficiarios y Actas de entrega de las certificaciones firmadas por los beneficiarios de la certificación y el supervisor del contrato. Sin embargo, el proceso remitió respecto al aval del fabricante MILE2 para quince (15) beneficiarios y Actas de entrega de las certificaciones firmadas por los beneficiarios de la certificación y el supervisor del contrato, evidencia que no demuestra el cumplimiento de la obligación contractual. **Caso 3** Con el requerimiento No. 6 se solicitó soporte de la capacitación virtual con al menos tres (3) talleres prácticos de 4 horas sobre la administración y parametrización de la herramienta, administración de los usuarios, módulos y uso de las funcionalidades de los módulos, dirigida a los usuarios con rol administrador del GIT de Seguridad y Privacidad de la Información. Sin embargo, el proceso remitió respecto al soporte de la capacitación virtual, evidencia que no demuestra el cumplimiento de la obligación contractual. **Caso 4** Con el requerimiento No. 6 se solicitó cronograma para la transferencia de conocimientos sobre la instalación, implementación y operación de la herramienta. Sin embargo, el proceso remitió respecto al soporte del cronograma, evidencia que no demuestra el cumplimiento de la obligación contractual.	Posibilidad de afectación económica y reputacional por Incumplimiento u omisión de las normas externas e internas por parte de la supervisión A causa de las deficiencias en el seguimiento por parte del supervisor al objeto y obligaciones del contratista en términos de cantidad, calidad y oportunidad del bien o servicio contratado, así como a la ejecución financiera cuando se entreguen recursos por ejecutar y por legalizar, con el fin de evitar la pérdida de competencia para liquidar.
21	**Hallazgo 2.13.** En el contrato 1222 de 2023 no se cumplieron obligaciones específicas y obligaciones del anexo técnico.	**Caso 1** Con el requerimiento No. 6 se solicitó soporte de radicación de las hojas de vida junto con sus soportes al supervisor del contrato y soporte de aprobación del supervisor de las hojas de vida. Sin embargo, el proceso remitió respecto al soporte de soporte de radicación de la hoja de vida y soporte de aprobación del supervisor de la hoja de vida, evidencia que no demuestra el cumplimiento de la obligación contractual. **Caso 2**	Posibilidad de afectación económica y reputacional por Incumplimiento u omisión de las normas externas e internas por parte de la supervisión A causa de las deficiencias en el seguimiento por parte del supervisor al objeto y obligaciones del contratista en términos de cantidad, calidad y oportunidad del bien o servicio contratado, así como a la

ítem	N. del Hallazgo	Resumen del Hallazgo	Riesgo identificado
		Con el requerimiento No. 6 se solicitó soporte de presentación en cualquier programa que incluya mínimo los siguientes aspectos: (1) Presentación del equipo auditor; (2) Comunicación del objetivo y criterios de la auditoria definidos entre las partes; (3) Metodología del proceso de auditoria; (4) Plan de auditoria; y (5) Fecha y duración de la auditoria de acuerdo con el modelo de operación por procesos de la Entidad. Sin embargo, el proceso remitió respecto al soporte de presentación en cualquier programa, evidencia que no demuestra el cumplimiento de la obligación contractual. **Caso 3** Con el requerimiento No. 6 se solicitó soporte de entrega del plan de auditoría de seguimiento a la certificación del sistema de gestión de seguridad de la información. Sin embargo, el proceso remitió respecto al soporte de entrega del plan de auditoría, evidencia que no demuestra el cumplimiento de la obligación contractual. **Caso 4** Con el requerimiento No. 6 se solicitó Informe preliminar de auditoría que contenga resultados obtenidos durante la ejecución de la auditoria de seguimiento al Sistema de Gestión de Seguridad de la Información NTC-ISO 27001:2013. Sin embargo, el proceso remitió respecto al Informe preliminar de auditoría, evidencia que no demuestra el cumplimiento de la obligación contractual. **Caso 5** Con el requerimiento No. 6 se solicitó soporte de respuesta a las inquietudes u observaciones presentadas por la entidad, frente al informe preliminar de auditoría de seguimiento entregado por el contratista. Sin embargo, el proceso remitió respecto al soporte de respuesta a las inquietudes u observaciones presentadas por la entidad, frente al informe preliminar de auditoría, evidencia que no demuestra el cumplimiento de la obligación contractual. **Caso 6** Con el requerimiento No. 6 se solicitó soporte de entrega al supervisor del contrato del informe final de la auditoria de seguimiento a la certificación del sistema de gestión de Seguridad de la Información. Sin embargo, el proceso remitió respecto al soporte de entrega al supervisor del contrato del informe final de la auditoria, evidencia que no demuestra el cumplimiento de la obligación contractual.	ejecución financiera cuando se entreguen recursos por ejecutar y por legalizar, con el fin de evitar la pérdida de competencia para liquidar.
22	**Hallazgo transversal 3.1.** Los soportes y evidencias suministrados durante el proceso de auditoría no fueron	Al revisar la información y documentos entregados por el proceso en relación con los requerimientos efectuados, se evidenció que algunos de estos no fueron entregados completamente, presentan inconsistencias entre la solicitud realizada y el soporte entregado, o presentan inconsistencias en	"No se encuentra identificado en la matriz de riesgos del proceso".

ítem	N. del Hallazgo	Resumen del Hallazgo	Riesgo identificado
	entregados, se encontraron incompletos, presentan inconsistencias en su contenido, o fueron entregados por fuera de los plazos establecidos.	su contenido, incumpliendo los numerales 1 y 3 definidos en la Carta de representación firmada por el proceso, que indican: "1. Todo el equipo de trabajo que atenderá las solicitudes es responsable de la oportuna preparación, presentación y consistencia de la información que será entregada en el marco de la auditoría interna. 3. La información que suministraremos será válida, integral y completa para los propósitos de la auditoría interna".	

Tabla 4. Hallazgos Identificados

8. FORTALEZAS

- La Entidad cuenta con un marco sólido en la implementación del MSPI: política actualizada, actos administrativos, matriz de roles, metodología de riesgos, inventario de activos, indicadores y la adopción de metodologías alineadas con la ISO/IEC 27001:2022 que evidencian liderazgo y gestión en temas de seguridad y privacidad de la información.
- El proceso de seguridad y privacidad de la información, respecto a la obligación de la suscripción del compromiso de confidencialidad por parte del contratista, cumplió con el seguimiento y verificación a los términos establecidos en los contratos objeto de muestra para la presentación de este.

9. CONCLUSIONES

- Aunque el MSPI muestra un alto nivel de implementación, persisten debilidades en la planificación y mejora continua dado que no se consolidan brechas del autodiagnóstico, el alcance del MSPI es general, no hay un plan formal de implementación de controles ni un Plan Anual de Mejora estructurado con acciones, responsables y plazos.

- Se identificaron debilidades en el ejercicio de supervisión, respecto a la verificación y seguimiento al cumplimiento de las obligaciones por parte de los contratistas, presentándose deficiencias en la documentación o ausencia de soportes que demuestren el oportuno cumplimiento de algunas de ellas, situaciones que se describen en cada uno de los hallazgos**.**

10. RECOMENDACIONES

- Fortalecer la planificación y mejora continua del MSPI mediante la consolidación de brechas y acciones de mejora derivadas del autodiagnóstico; la definición formal del alcance del MSPI; la elaboración del plan de implementación de controles con actividades, responsables y recursos; y la adopción de un Plan Anual de Mejora que incluya oportunidades de mejora, no

conformidades y acciones correctivas, asegurando su coherencia con la ISO 27001:2022 y su aprobación en el Comité MIG.

- Realizar por parte del supervisor seguimiento periódico a las obligaciones establecidas contractualmente, teniendo en cuenta, además los anexos técnicos, lo cual debe quedar evidenciado mediante los informes de supervisión**.**

- Asegurar que, en la planeación de los contratos a cargo del proceso, se identifiquen obligaciones que conlleven a su cumplimiento, con el fin de que en la composición del proceso de contratación no solamente se vea reflejada la satisfacción de la necesidad sino también una buena estructuración de este.

11. PLAZO MÁXIMO PARA ENVÍO DE PLANES DE MEJORAMIENTO:

El proceso deberá elaborar un Plan de Mejoramiento, que permita subsanar las causas de los hallazgos descritos en este informe.

El Plan de Mejoramiento deberá ser enviado al líder de auditoría por correo electrónico dentro de los diez (10) días hábiles posteriores al recibo del presente informe, teniendo en cuenta las instrucciones definidas en el procedimiento “Formulación, seguimiento y cierre de acciones de mejora MIG-TIC-PR-003” y el formato “MIG-TIC-FM-011 Plan de Mejoramiento” vigentes.

Aprobó:

Juan Diego Toro Bautista.
Jefe Oficina de Control Interno

Elaboró: **Equipo auditor:**

Auditor Líder: Rafael Hernando Calle Cabezas.
Auditores: Sonia Alexandra Lobo Martínez
Crhistian Augusto Amador León

REGISTRO DE FIRMAS ELECTRONICAS

Informe Final de Auditoria OCI - Aud. SPI

Ministerio de Tecnología de la Información y las Comunicaciones
gestionado por: azsign.com.co

Id Acuerdo: 20251211-151938-04a0f4-75116687

Creación: 2025-12-11 15:19:38

Estado: Finalizado

Finalización: 2025-12-11 16:02:04

Escanee el código para verificación

Aprobación: Jefe Oficina de Control Interno

Juan Diego Toro Bautista
79569758
jtorob@mintic.gov.co
Jefe de Oficina de Control Interno
Ministerio de Tecnologías de la Información y las Comunicaciones

REPORTE DE TRAZABILIDAD

Informe Final de Auditoria OCI - Aud. SPI

Ministerio de Tecnología de la Información y las Comunicaciones
gestionado por: azsign.com.co

Id Acuerdo: 20251211-151938-04a0f4-75116687
Creación: 2025-12-11 15:19:38
Estado: Finalizado
Finalización: 2025-12-11 16:02:04

Escanee el código para verificación

TRAMITE	PARTICIPANTE	ESTADO	ENVIO, LECTURA Y RESPUESTA
Aprobación	Juan Diego Toro Bautista jtorob@mintic.gov.co Jefe de Oficina de Control Interno Ministerio de Tecnologías de la Información y las	Aprobado	Env.: 2025-12-11 15:19:42 Lec.: 2025-12-11 16:01:56 Res.: 2025-12-11 16:02:04 IP Res.: 181.53.156.20 Canal: Email