

 Supersolidaria	INFORME DEFINITIVO ACTIVIDAD DE AUDITORÍA	Código: FT-COIN-007 Julio - 2026 Versión: 03
--	--	---

FECHA DE EMISIÓN DEL INFORME	Día:	19	Mes:	8	Año:	2026
-------------------------------------	-------------	----	-------------	---	-------------	------

Nombre de la auditoría	Seguimiento al Plan de Seguridad y Privacidad de la Información
Dependencia, proceso y/o grupo de trabajo, objeto de auditoria	Oficina Asesora de Planeación y Sistemas – OAPS. Gestión de Tecnologías de la Información – GETI.
Funcionarios directivos, coordinadores o líderes del proceso a auditar	
Tipo de Auditoría (Ley o Interna)	De Ley.
Objetivo y alcance	Validar el cumplimiento de los lineamientos y estándares para la estrategia de seguridad digital y del modelo de seguridad y privacidad.
Objetivos específicos	Para los siguientes alcances, se hará sobre lo actuado y gestionado desde el 01-01-2025 hasta 30-06-2026. • Validar la aplicación de la Resolución 500 de 2021 (10-03-2021) "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". • Validar la aplicación de la Resolución 2277 de 2025 (03-06-2025) "Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia". • Conceptuar sobre el cumplimiento de controles del mapa de riesgos del proceso auditado relacionados con los objetivos anteriores y/o proponer nuevos controles y riesgos.
Criterios Normativos y / o Administrativos:	• 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". • Documentos internos de la Entidad en materia de Seguridad y Privacidad de la Información: Políticas, Manuales, procedimientos, Mapa de riesgos, entre otros.

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

 Supersolidaria	INFORME DEFINITIVO ACTIVIDAD DE AUDITORÍA	Código: FT-COIN-007 Julio - 2026 Versión: 03
--	--	---

1. COMPROMISO ÉTICO EN EL EJERCICIO DE LA AUDITORÍA INTERNA

La Oficina de Control Interno, tiene en cuenta para la actividad de auditoría, los siguientes documentos:

- Código de Ética del Auditor Interno que tiene como bases fundamentales, la integridad, objetividad, confidencialidad, conflictos de interés y competencia de este.
- Estatuto de auditoría, en el cual se establecen y comunican las directrices fundamentales que definen el marco dentro del cual se desarrollan las actividades de la Oficina de Control Interno, según los lineamientos de las normas internacionales de auditoría.

2. COMPROMISO DEL AUDITADO

De conformidad con la Ley, para la realización de la presente auditoría, se expidió la Carta de representación el 16-07-2026, suscrita por [REDACTED], como jefe o líder del proceso a unidad auditada, mediante la cual, ha declarado su responsabilidad en la oportuna preparación, presentación integral y consistencia de la información solicitada y entregada en el marco de la auditoría a la oficina de control interno.

3. ACTIVIDADES REALIZADAS

Durante las etapas de planeación, apertura, ejecución y cierre de la actividad de auditoría, se desarrollaron las siguientes actividades:

- Conocimiento del proceso o dependencia. A través de una reunión previa sostenida con el proceso el 06-07-2026 en la cual se indagó sobre los alcances gestionados en el cumplimiento de las resoluciones definidas en los criterios y de acuerdo con el informe de auditoría de vigencias anteriores.
- Diseño del plan de trabajo de la actividad de auditoría: Se definieron el objetivo y los objetivos primarios, soportados en los criterios legales o administrativos a tener en cuenta para su definición y su respectivo cronograma de actividades de trabajo.
- Reunión de apertura: la apertura de la auditoría se realizó en reunión virtual, el 09-07-2026, en donde se expuso el plan de trabajo de la actividad de auditoría ante los responsables de la dependencia y grupo de trabajo sujetos de la auditoría, atendiendo con oportunidad inquietudes al respecto, para lo cual se dejó constancia en acta grabada de la reunión en la IA GEMINI.
- Obtención y análisis de la información: Fue solicitada la información pertinente, relacionada con el objetivo (s) y alcance(s), que fuese relevante, útil, basada en hechos y confiable. Soportada en los respectivos papeles de trabajo. La información fue allegada a la OCI, el 16-07-2026.

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

 Supersolidaria	INFORME DEFINITIVO ACTIVIDAD DE AUDITORÍA	Código: FT-COIN-007 Julio - 2026 Versión: 03
--	--	---

- e) Análisis y evaluación de la información. La revisión se realizó en el plazo estipulado y fue basada en factores críticos de éxito, en estrategias y objetivos del aspecto evaluable, en los riesgos altos y extremos, metas y objetivos del proceso, con enfoque hacia la consecución de los alcances de la auditoría.
- f) Informe preliminar. Se emitió y notificó el informe preliminar, el 06/08/2026, a través de correo electrónico dirigido al Jefe de la Dependencia Auditadas y Jefes de Grupo respectivos, los cuales tuvieron un periodo de revisión para interponer observaciones, aclaraciones, solicitudes de precisión, etc., conforme el debido proceso, ante el contenido del informe y los mismos hallazgos y observaciones.
- g) Presentación de observaciones al informe preliminar. El Jefe de la dependencia, reportó a la OCI, el 11/08/2026, mediante correo electrónico las respectivas observaciones a dicho informe. Copia del referido oficio reposa en la carpeta de la respectiva auditoría DRIVE de la OCI.
- h) Respuesta de la OCI al oficio de observaciones del proceso auditado. Mediante correo electrónico remitido el 19/08/2026, la OCI dio respuesta al oficio interpuesto de observaciones en contra del informe preliminar, ante lo cual, en el desarrollo del informe definitivo quedan reflejados los hallazgos confirmados con su respectiva observación interpuesta y la respuesta de la OCI. Copia del referido oficio reposa en la carpeta de la respectiva auditoría DRIVE de la OCI.
- i) Informe definitivo de Auditoría. Una vez, realizada las anteriores actividades, se procede a presentar el presente informe definitivo.

4. DESARROLLO DE AUDITORÍA

CRITERIO GENERAL DE LOS ASPECTOS AUDITADOS:

De conformidad con el artículo 2 de la Resolución 500 de 2021, sus disposiciones aplican a los sujetos obligados definidos en el artículo 2.2.9.1.1.2 del Decreto 1078 de 2015 (DUR-TIC), el cual establece que la Política de Gobierno Digital es obligatoria para las entidades que conforman la administración pública, y por tanto, la Superintendencia de la Economía Solidaria, en su calidad de entidad pública del orden nacional e integrante de la administración pública, se encuentra dentro de los sujetos obligados de dicha política.

La Supersolidaria debe implementar y mantener los lineamientos relacionados con:

- El Modelo de Seguridad y Privacidad de la Información (MSPI).
- La Estrategia de Seguridad Digital.
- La gestión de riesgos de seguridad de la información.
- La gestión de incidentes de seguridad digital.
- Los controles de privacidad y protección de datos.
- El seguimiento, monitoreo y auditoría de la seguridad de la información.

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

 Supersolidaria	INFORME DEFINITIVO ACTIVIDAD DE AUDITORÍA	Código: FT-COIN-007 Julio - 2026 Versión: 03
--	--	---

Asimismo, debe aplicar las modificaciones introducidas por la Resolución 746 de 2022 y la actualización del Anexo 1 efectuada mediante la Resolución 2277 de 2025.

A nivel jerárquico, se puede ilustrar estos lineamientos de la siguiente manera:

Elemento	Descripción	Jerarquía
Política de Gobierno Digital	Es la directriz oficial establecida por el MinTIC mediante el Decreto 767 de 2022, para promover el uso y aprovechamiento de las TIC y mejorar la gestión pública, la competitividad y la relación del Estado con los ciudadanos. Esta estrategia se integra operativamente con el Modelo Integrado de Planeación y Gestión (MIPG). Sus habilitadores: • Arquitectura: Gestión ordenada de los elementos tecnológicos y de datos en las entidades públicas. • Seguridad y Privacidad de la Información: Protección de los datos y garantía de confianza digital. • Servicios Ciudadanos Digitales: Facilitación de trámites interoperables y eficientes para la población. • Cultura y Apropiación: Fomento de capacidades digitales tanto en servidores públicos como en la ciudadanía.	MIPG. Más alto nivel
Resolución 500 -2021	Su objetivo es fijar los lineamientos de seguridad digital y adoptar el Modelo de Seguridad y Privacidad de la Información (MSPI).	Marco normativo
MSPI	Es el marco de referencia definido por MinTIC para implementar la seguridad y privacidad de la información y responde al " Qué debe hacerse ". La Resolución 500 de 2021 obliga a adoptar el MSPI como habilitador de la Política de Gobierno Digital.	Modelo de gestión
PSPI	El Plan de Seguridad y Privacidad de la Información es el instrumento de planificación mediante el cual la entidad ejecuta el MSPI. Normalmente contiene objetivos anuales, actividades, cronograma, responsables, recursos, indicadores y metas de cumplimiento. El PSPI responde al "Cómo, Cuándo y Quién lo hará".	Plan de implementación del modelo de gestión

El MSPI constituye el modelo o marco de gestión que establece los lineamientos, requisitos y controles para la seguridad y privacidad de la información, mientras que el PSPI corresponde al instrumento de planificación mediante el cual la entidad implementa, ejecuta y realiza seguimiento a las actividades para dar cumplimiento a dicho modelo.

Esto se confirma en el PSPI de la Entidad que indica "(...) *el presente Plan de Seguridad y Privacidad de la Información tiene como propósito fortalecer las capacidades organizacionales en gestión de riesgos y protección de la información, así como plantear las actividades que permitan el cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI), en el marco de la normatividad vigente.*"

En consecuencia, dado que el alcance de la auditoría se definió como "Seguimiento al Plan de Seguridad y Privacidad de la Información (PSPI)", resulta necesario validar no solo la

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

 Supersolidaria	INFORME DEFINITIVO ACTIVIDAD DE AUDITORÍA	Código: FT-COIN-007 Julio - 2026 Versión: 03
--	--	---

ejecución de las actividades incluidas en el plan, sino también su alineación y contribución al cumplimiento de los requisitos del Modelo de Seguridad y Privacidad de la Información (MSPI), es decir, **el ejercicio auditor y alcance definido implica verificar el cumplimiento de la Resolución 500 de 2021 y sus modificaciones.**

Por otro lado, es importante precisar que, tener implementada o certificada en la Entidad la ISO/IEC 27001 no constituye por sí sola evidencia suficiente de cumplimiento total de la Resolución 500 de 2021 ni de la Resolución 2277 de 2025, por cuanto, es un soporte muy importante que facilita gran parte del cumplimiento. Existe una alta correspondencia entre ISO 27001 y el MSPI; de hecho, el artículo 4 de la Resolución 500 señala que las entidades deben propender por la incorporación de estándares internacionales y mejores prácticas en seguridad de la información, sin embargo, la ISO 27001 es un medio de cumplimiento, pero no reemplaza el cumplimiento normativo de la Resolución 500 de 2021 ni de la Resolución 2277 de 2025.

Como metodología para el desarrollo de los tres alcances definidos en la auditoría, se realizó una reunión preliminar con el proceso auditado, durante la cual se contextualizó la aplicación de las resoluciones objeto de evaluación y se expuso, de manera general, el estado de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

Adicionalmente, el 06-07-2026 se efectuó un requerimiento de información orientado a obtener los entregables, soportes y evidencias relacionadas con el cumplimiento de la Resolución 500 de 2021 y la Resolución 2277 de 2025. La información solicitada fue suministrada por el proceso el 16-07-2026. Posteriormente, se realizó el análisis y validación de los documentos y evidencias aportadas, con base en lo cual se desarrolló y concluyó el presente ejercicio de auditoría.

A continuación, se describe el ejercicio realizado:

4.1. OBJETIVO ESPECÍFICO UNO. Validar la aplicación de la Resolución 500 de 2021 (10-03-2021) "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".

Posterior a validar los soportes, evidencias y respuestas suministradas por el proceso, se identificó que el proceso ha realizado una gestión positiva y fue suministrada evidencia en los siguientes aspectos:

- Planes de Seguridad y Privacidad de la Información del 2025 y 2026.
- Matrices de riesgo de seguridad de la información.
- Difusión, capacitación y concientización sobre seguridad de la Información.
- Documentación sobre políticas y procedimientos de seguridad de la información.

Por otra parte, se identificaron las siguientes situaciones o debilidades:

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

 Supersolidaria	INFORME DEFINITIVO ACTIVIDAD DE AUDITORÍA	Código: FT-COIN-007 Julio - 2026 Versión: 03
--	--	---

HALLAZGO 1. Inexistencia del Acto administrativo de aprobación de la Estrategia de Seguridad Digital, junto con su publicación o socialización.

Condición

Se solicitó el Acto administrativo de aprobación formal de la Estrategia de Seguridad Digital y las evidencia de publicación o socialización, para lo cual, se aportaron actas de comité que evidencian la presentación y aprobación de los Planes de Seguridad y Privacidad de la Información de las vigencias 2025 y 2026; sin embargo, no se suministró evidencia documental del acto administrativo de carácter general mediante el cual se aprueba formalmente la Estrategia de Seguridad Digital, ni los soportes suficientes de su publicación o divulgación institucional.

Criterio

El artículo 5 de la Resolución 500-2021, establece que la Estrategia de Seguridad Digital debe:

- Los sujetos obligados deben adoptar la estrategia de seguridad digital.
- Integrarse al Plan de Seguridad y Privacidad de la Información.
- Ser aprobada a través de un acto administrativo de carácter general.

Causa

- Debilidad en formalización documental de la estrategia y en la gestión del cumplimiento normativo asociado al MSPI.

Consecuencias

- Riesgo de incumplimiento de la Resolución 500 de 2021 y en la gobernanza de seguridad digital.
- Riesgo de falta de trazabilidad frente a la adopción institucional de la estrategia de seguridad digital.

Recomendaciones

1. Adoptar formalmente la Estrategia de Seguridad Digital por medio de un acto administrativo de carácter general o mediante el procedimiento formal que aplique la entidad.

Al respecto, el proceso respondió al informe preliminar indicando:

*"Frente a esta recomendación, se precisa que la Estrategia de Seguridad Digital se encuentra incorporada en la planeación institucional a través del PETI, aprobado mediante Acta No. 6 de 2025 (se adjunta Acta No. 6 Comité G&D Sesión 29Ago firmado) cuyo proyecto es mencionando en el acta 001 de 2026 del Comité de Gestión y Desempeño Proyecto PY02 "Implementar seguridad digital y el Modelo de Seguridad de la Información", el cual contempla acciones para la implementación del MSPI, incluyendo la selección de controles y la Declaración de Aplicabilidad. La ejecución de esta estrategia se complementa mediante los planes de seguridad de la información, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y demás instrumentos asociados. Asimismo, su direccionamiento y seguimiento se realiza a través de las instancias de gobierno institucional, como se evidencia en el Acta No. 01-2025 del Comité de Seguridad y Privacidad de la Información y el Acta No. 01-2026 del Comité de Gestión y Desempeño.
Por lo anterior, precisa que la recomendación ya fue aplicada, toda vez que la Entidad ya cuenta con instrumentos formales para la planeación, ejecución y seguimiento de la Estrategia de Seguridad*

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

 Supersolidaria	INFORME DEFINITIVO ACTIVIDAD DE AUDITORÍA	Código: FT-COIN-007 Julio - 2026 Versión: 03
--	--	---

Digital, debidamente articulados con el PETI y el MSPI, por lo que no se considera necesario establecer un acto administrativo adicional para su adopción" y,

Respuesta OCI:

La respuesta no desvirtúa la recomendación formulada, dado que se fundamenta en que la Estrategia de Seguridad Digital se encuentra incorporada dentro del PETI, el MSPI y los instrumentos de planeación institucional, sin embargo, el artículo 5 de la Resolución 500 de 2021 establece expresamente que la Estrategia de Seguridad Digital debe **ser aprobada mediante acto administrativo de carácter general**. La evidencia aportada corresponde a instrumentos de planeación y seguimiento, mas no al acto formal requerido por la norma.

En consecuencia, la recomendación se mantiene.

HALLAZGO 2. Falta de evidencia que demuestre que se haya promovido la cultura para la seguridad digital y de la información y la incorporación en el Plan Institucional de Capacitación - PIC.

Condición

En el PSPI 2026 se identifican actividades específicas y objetivos de fortalecimiento de la cultura de seguridad de la información alineadas con el criterio evaluado:

- 30 campañas "Jueves Seguro".
- 3 charlas de seguridad.
- 1 ejercicio de ingeniería social y.
- Seguimiento mediante indicador de sensibilización en seguridad.
- Objetivo: "Consolidar la cultura organizacional de seguridad mediante campañas, charlas y ejercicios de ingeniería social".

Por otra parte, el Plan Estratégico de Talento Humano contempla el PIC como herramienta para fortalecer conocimientos, habilidades y competencias de los servidores públicos, incluyendo temas de tecnología dentro de sus líneas de formación.

No obstante, la evidencia suministrada presenta limitaciones para demostrar plenamente el cumplimiento del criterio auditado, dado que:

- No se aportaron los documentos específicos del PIC del 2025 y del 2026, sino el Plan Estratégico de Talento Humano que únicamente hace referencia a este.
- No se evidenció una programación específica para el 2025 y 2026 asociada a Seguridad de la información, Seguridad digital, MSPI, Gestión de incidentes, Gestión de riesgos de seguridad digital, descritos en el criterio.
- Aunque el Plan de Seguridad 2026 contempla actividades de sensibilización, no se evidenció la articulación formal entre dichas actividades y el PIC, aspecto mencionado por el proceso en su respuesta.
- El plan de seguridad 2025 no contó con actividades de difusión, capacitación y concientización.

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

 Supersolidaria	INFORME DEFINITIVO ACTIVIDAD DE AUDITORÍA	Código: FT-COIN-007 Julio - 2026 Versión: 03
--	--	---

Criterio

El numeral 4 del artículo 5 de la Resolución 500-2021, establece que en la estrategia de seguridad digital debe:

"4. Establecer e implementar los principios, lineamientos y estrategias para promover una cultura para la seguridad digital y de la información que incluya actividades de difusión, capacitación y concientización tanto al interior de la entidad como frente a usuarios y terceros que ésta considere relevantes para mejorar habilidades y promover conciencia en la seguridad de la información. Estas actividades deben realizarse anualmente y pueden incluirse, adicionalmente, en el Plan Institucional de Capacitaciones PIC, o el que haga sus veces".

Causa

- Posible debilidad en la trazabilidad documental entre el Plan de Seguridad y Privacidad de la Información y los instrumentos institucionales de capacitación.
- Desarticulación con el proceso de Talento Humano, en planear un PIC asociando las necesidades de capacitación en el componente de seguridad digital, como medida institucional relevante.

Consecuencias

- Riesgo de incumplimiento de la Resolución 500 de 2021.
- Riesgo de desarticulación entre las estrategias de seguridad digital y los programas institucionales de formación.

Recomendación

- Incorporar expresamente en el PIC las actividades de capacitación y sensibilización derivadas del MSPI y de la Estrategia de Seguridad Digital, estableciendo un programa, unos objetivos, unas metas, unas estrategias y los indicadores respectivos.
- Establecer trazabilidad entre las actividades de capacitación programadas, ejecutadas y evaluadas en materia de seguridad digital y seguridad de la información.

Al respecto, el proceso respondió al informe preliminar indicando:

"Frente a las recomendaciones formuladas, la OAPS En articulación con el grupo de Talento Humano ha incluido capacitaciones del MSPI en el PIC, ya que estás se encuentran en el eje temático: Transformación Digital y Cibercultura. Estas capacitaciones se dan de acuerdo con los lineamientos que establezca la Oficina de Talento Humano, teniendo en cuenta que esta dependencia es la responsable de la estructuración, programación y seguimiento del Plan Institucional de Capacitación (PIC). Por parte de la OAPS, las actividades de capacitación y sensibilización en seguridad digital y seguridad de la información se encuentran contempladas en el MSPI y en el Plan de Seguridad y Privacidad de la Información (PSPI). Para su articulación con el PIC, Talento Humano solicita a la OAPS las actividades de capacitación correspondientes; como evidencia, se adjunta el correo (EVIDENCIA_PIC) de solicitud realizado para la vigencia 2026. Adicionalmente, la OAPS desarrolla actividades permanentes de sensibilización, entre ellas la campaña "Jueves Seguro", y gestiona otras capacitaciones de acuerdo con las necesidades identificadas, articulando con Talento Humano la convocatoria cuando corresponda. Las evidencias de las capacitaciones, campañas y actividades de sensibilización realizadas se consolidan y conservan en el repositorio oficial de la OAPS, permitiendo mantener los soportes y la trazabilidad de las acciones ejecutadas. En consecuencia, la OAPS continuará suministrando la información, actividades y

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

 Supersolidaria	INFORME DEFINITIVO ACTIVIDAD DE AUDITORÍA	Código: FT-COIN-007 Julio - 2026 Versión: 03
--	--	---

evidencias que sean requeridas para su articulación con el PIC, atendiendo los lineamientos, mecanismos e instrumentos que defina Talento Humano como responsable de dicho Plan”.

Respuesta OCI.

El soporte suministrado corresponde a un requerimiento de Secretaría general a la OAPS solicitando apoyo para programar una reunión en el mes de julio de 2026 en temas de MSPI (Seguridad de la Información, PETI y Riesgos tecnológicos), citando a los profesionales de planta y como tema principal, el Plan Institucional de Capacitación PIC. Adicionalmente, esta actividad soporta gestión en el último mes del alcance de la auditoría, no evidenciando acciones desde enero del 2025.

La respuesta suministra elementos adicionales que evidencian avances en la articulación entre la OAPS y Talento Humano. No obstante, continúa siendo importante fortalecer la inclusión explícita y verificable de las actividades del MSPI dentro de los instrumentos de capacitación institucional. Por tal motivo, la recomendación No. 1 se mantiene con enfoque de fortalecimiento documental.

Con relación a la recomendación No. 2, la OCI considera atendida parcialmente la misma, en virtud de que se aportan evidencias de coordinación interinstitucional. No obstante, se sugiere fortalecer la conservación sistemática de los soportes asociados de manera permanente y consecutiva. Por lo anterior, esta recomendación se excluye del informe final de auditoría.

Finalmente, la recomendación No. 3 permanece vigente, toda vez que la evidencia aportada permite acreditar conservación documental pero no demuestra plenamente la trazabilidad integral de las actividades de capacitación en materia de seguridad de la información.

HALLAZGO 3. No se ha informado o reportado al Comité Institucional de Gestión y Desempeño sobre los resultados del análisis de riesgos y de incidentes.

Condición

Se solicitó evidencias de reportes presentados al “Comité institucional de gestión y desempeño” sobre los resultados del análisis de riesgos y gestión de incidentes”, y para lo cual el proceso aportó:

- El acta No. 1 de 2025 del Comité SPI trató los temas de su Conformación e instalación, sobre los avances del MSPI 2024, y sobre el Plan 2025.
- El Acta No. 3 de 2025 del Comité SPI contiene la presentación del incidente de ciberseguridad, la propuesta de actualización del mapa de riesgos de seguridad de la información y el seguimiento al Plan de Seguridad y Privacidad de la Información.
- Dos (2) resoluciones de modificación del Comité Institucional de Gestión y Desempeño y supresión del Comité de Seguridad y Privacidad de la Información.
- Se excluyen los siguientes soportes:

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

 Supersolidaria	INFORME DEFINITIVO ACTIVIDAD DE AUDITORÍA	Código: FT-COIN-007 Julio - 2026 Versión: 03
--	--	---

- Acta del 2024: Por fuera del alcance de vigencia de la auditoría.
- Acta Reunión Ordinaria 1 del 2026: Corresponde al Comité CICCI.

Pese a lo anterior, no se suministró evidencia de la presentación de los análisis o seguimientos realizados a los resultados de riesgos de seguridad de la información o de la gestión de incidentes, como lo indica el criterio.

Criterio

El numeral 3 del artículo 6 de la Resolución 500 de 2021, indica:

“Art 6. La gestión de la seguridad de la información, seguridad digital y la gestión de riesgos de la entidad. Los sujetos obligados deben determinar e implementar controles para mitigar los riesgos que pudieran afectar la seguridad digital y física de acuerdo con el resultado del análisis y evaluación de riesgos y cumplir con las siguientes características y responsabilidades:

3. Reportar los resultados del análisis de riesgos y gestión de incidentes al comité institucional de gestión y desempeño o quien haga sus veces”.

Causa

- Falta de trazabilidad documental de los reportes a la alta dirección.
- Desconocimiento de los miembros del comité, sobre sus funciones y responsabilidades en materia de seguridad digital.

Consecuencias:

- Riesgo de incumplimiento de la Resolución 500 de 2021 por debilidades en la gobernanza de seguridad digital.
- Riesgo de materialización de vulnerabilidades por falta de información y direccionamiento estratégico para la toma de decisiones.

Recomendación

- Realizar una reinducción a los integrantes del comité de gestión y desempeño, con el fin tengan claridad de todos los informes periódicos que se deben llevar al comité en la entidad, en este caso debe incluir, el informe periódico de seguridad digital.

Al respecto, el proceso respondió al informe preliminar indicando:

"No se acepta la recomendación, teniendo en cuenta que las funciones relacionadas con seguridad y privacidad de la información fueron asumidas por el Comité Institucional de Gestión y Desempeño, instancia que absorbió las funciones del anterior Comité de Seguridad y Privacidad de la Información.

En consecuencia, los asuntos relacionados con la gestión de riesgos e incidentes de seguridad digital son tratados en el marco de esta instancia institucional. Frente a los incidentes de seguridad digital, se cuenta con evidencia de su presentación y análisis ante el Comité. Particularmente, en la Sesión Extraordinaria No. 2 se incluyó expresamente dentro de la agenda la "Presentación Análisis Incidente de Seguridad, ruta de trabajo y pasos a seguir", bajo responsabilidad de la Oficina Asesora de Planeación. Si bien, la información de los incidentes de seguridad digital se encuentra en el sistema de gestión de incidentes, se debe fortalecer la comunicación y el seguimiento de los incidentes de seguridad digital, para garantizar la transparencia y la rendición de cuentas en los procesos de fortalecimiento.

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

 Supersolidaria	INFORME DEFINITIVO ACTIVIDAD DE AUDITORÍA	Código: FT-COIN-007 Julio - 2026 Versión: 03
--	--	---

Asimismo, dentro de las acciones definidas como resultado del análisis se contempló expresamente la actualización del mapa de riesgos, junto con el fortalecimiento de controles de navegación, VPN y acceso remoto, accesos privilegiados, campañas de sensibilización, continuidad del negocio e infraestructura tecnológica. Adicionalmente, respecto de la gestión de riesgos, en revisión por la Dirección realizada el 23 de junio de 2026 fueron presentados los riesgos de la Entidad, lo cual evidencia que esta temática también ha sido puesta en conocimiento y sometida a consideración de dicha instancia”.

Respuesta OCI.

El criterio auditado no exige únicamente que se presenten incidentes o riesgos ante una instancia directiva; el enfoque del criterio exige expresamente "**Reportar los resultados del análisis** de riesgos y gestión de incidentes al Comité Institucional de Gestión y Desempeño o quien haga sus veces". Esta expresión resaltada implica presentar al Comité las conclusiones de un ejercicio ejecutado, como, por ejemplo:

- Acciones de tratamiento implementadas.
- Conclusiones y decisiones requeridas por la alta dirección.
- Resultados de la valoración de riesgos.
- Riesgos residuales y materializados.
- Comportamientos y evolución de los riesgos.
- Efectividad de los controles.

En la respuesta del proceso, se observa que se presenta ante el comité el incidente de seguridad y las acciones adoptadas frente a este y la actualización del mapa de riesgos presentados en una revisión por la dirección.

Sin embargo, no se aporta evidencia de que se hayan reportado al Comité Institucional de Gestión y Desempeño los resultados del análisis de riesgos de seguridad de la información, entendidos como el seguimiento al comportamiento de los riesgos, la evaluación de controles, la efectividad de los tratamientos y las conclusiones derivadas de dicho análisis. Tampoco se evidencia la presentación formal y periódica de los resultados de la gestión de incidentes en los términos exigidos por la Resolución 500 de 2021.

En consecuencia, la respuesta demuestra que se trataron algunos temas relacionados con seguridad digital, pero no demuestra el cumplimiento específico del criterio evaluado.

Por lo anterior, la recomendación se mantiene con el objetivo de que todos los miembros del comité conozcan qué información, temas e informes deben recibir, y así, poder hacer gestión y seguimiento a los mismos.

HALLAZGO 4. Ausencia de análisis de riesgo específico para determinar la pertinencia de contratar servicios especializados de atención de incidentes de seguridad digital.

Condición

La evidencia suministrada corresponde a una matriz de riesgos de seguridad de la

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

 Supersolidaria	INFORME DEFINITIVO ACTIVIDAD DE AUDITORÍA	Código: FT-COIN-007 Julio - 2026 Versión: 03
--	--	---

información, en la cual se identifican activos, amenazas, vulnerabilidades, riesgos, controles implementados, responsables y niveles de riesgo, identificando en esta matriz, riesgos asociados a ciberataques y a deficiencias en las capacidades de monitoreo, alerta y respuesta ante incidentes de ciberseguridad.

No obstante, el criterio evaluado no exige únicamente la existencia de una matriz de riesgos de seguridad de la información, sino el análisis de riesgo específico orientado a determinar la pertinencia de contratar o implementar un servicio especializado para la atención de incidentes de seguridad digital, contemplando aspectos como: Características del proveedor, Herramientas requeridas, Servicios especializados, Privacidad de la información y la justificación de la decisión de contratar o no contratar.

Durante la revisión de la matriz aportada no se evidenció el análisis específico sobre la necesidad de contar con equipo especializado o servicio externo de respuesta a incidentes, o la evaluación comparativa de las alternativas internas o externas, entre otros, incluyendo la conclusión documentada respecto a la pertinencia o no de contratar dichos servicios.

Si bien la matriz constituye un insumo relevante y requerido para la gestión del riesgo, por sí sola no demuestra el cumplimiento del criterio.

Criterio

El numeral 8 del artículo 6 de la Resolución 500 de 2021, indica:

“Art 6. La gestión de la seguridad de la información, seguridad digital y la gestión de riesgos de la entidad. Los sujetos obligados deben determinar e implementar controles para mitigar los riesgos que pudieran afectar la seguridad digital y física de acuerdo con el resultado del análisis y evaluación de riesgos y cumplir con las siguientes características y responsabilidades:

8. Realizar un análisis de riesgo para determinar la pertinencia de contratar o implementar el servicio de un equipo especializado para atender incidentes de seguridad digital. El análisis debe identificar las características del proveedor, herramientas, servicios y privacidad de la información, entre otros”.

Causas

- Falta de desarrollo de un análisis específico derivado de los resultados de la gestión de riesgos de seguridad digital.
- Debilidad en la documentación de decisiones relacionadas con la gestión y respuesta especializada ante incidentes de seguridad.

Consecuencias

- Incumplimiento de los requisitos establecidos en la Resolución 500 de 2021.
- Limitaciones para sustentar técnica y formalmente la capacidad institucional de respuesta ante incidentes de seguridad digital.

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

Recomendaciones

- Elaborar y documentar un análisis de riesgo específico que evalúe la pertinencia de implementar o contratar servicios especializados para la atención de incidentes de seguridad digital.
- Incorporar en dicho análisis la evaluación de proveedores, herramientas, alcance de servicios, costos, capacidades institucionales y aspectos de privacidad y protección de la información.

Al respecto, el proceso respondió al informe preliminar indicando:

"Frente a esta recomendación, no se acoge la elaboración de un análisis de riesgo adicional y específico, teniendo en cuenta que la Entidad ya realizó el análisis de los riesgos asociados a la seguridad digital y seguridad de la información, cuyos resultados se encuentran incorporados en el mapa de riesgos, en el cual se identificaron y valoraron los riesgos y se definieron los controles necesarios para su tratamiento. La definición de estos controles se realizó considerando las capacidades institucionales, técnicas y presupuestales de la Entidad, determinando los mecanismos requeridos para prevenir, detectar y atender la materialización de los riesgos identificados. Como parte de estas capacidades, actualmente se cuenta con monitoreo SOC y acompañamiento técnico especializado, así como con soporte de fabricantes y especialistas de las soluciones de seguridad implementadas, entre ellas SIEM, Firewall, NAC y EDR, entre otras.

Como resultado del análisis efectuado, no se identificó la necesidad de contratar servicios especializados para la atención de incidentes de seguridad digital y seguridad de la información, ya que la Entidad cuenta con capacidades institucionales, técnicas y presupuestales para prevenir, detectar y atender la materialización de los riesgos identificados. Como parte de estas capacidades, actualmente se cuenta con monitoreo SOC y acompañamiento técnico especializado, así como con soporte de fabricantes y especialistas de las soluciones de seguridad implementadas, entre ellas SIEM, Firewall, NAC y EDR, entre otras. Independiente orientado exclusivamente a determinar la contratación de servicios especializados.

Respuesta OCI.

El proceso justifica ante el equipo auditor por qué se consideran suficientes las capacidades actuales, pero no aporta la evidencia del análisis específico ejecutado y exigido por la norma de sustentar formalmente dicha decisión.

La respuesta suministrada no desvirtúa el hallazgo, debido a que la existencia de una matriz de riesgos institucional no sustituye el análisis específico requerido por la Resolución 500 de 2021 para determinar la pertinencia de contratar o implementar o no, servicios especializados para la atención de incidentes. Las justificaciones expuestas en la respuesta son las que se deberían incluir como conclusiones del ejercicio del análisis de riesgo realizado.

En consecuencia, el hallazgo y las recomendaciones se mantienen.

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

 Supersolidaria	INFORME DEFINITIVO ACTIVIDAD DE AUDITORÍA	Código: FT-COIN-007 Julio - 2026 Versión: 03
--	--	---

HALLAZGO 5. Ausencia de evidencia de auditorías de seguridad de la información con componentes técnicos de evaluación de vulnerabilidades sobre sistemas críticos.

Condición

El artículo 15 de la Resolución 500 de 2021 establece que los sujetos obligados deben implementar mecanismos de control que permitan verificar el cumplimiento de la política de seguridad de la información, "realizando auditorías de seguridad de la información al menos una vez al año", condicionado a un requisito específico señalando "que contemplen aspectos técnicos de la seguridad digital como análisis de vulnerabilidades a sistemas de información críticos, entre otros".

Se solicitó al proceso el soporte de las auditorías de seguridad de la información llevadas a cabo, incluyendo los planes de mejoramiento implementados. El proceso respondió que:

"Respecto a este requerimiento, se aclara que la ejecución de las auditorías internas es responsabilidad de la Oficina de Control Interno, de conformidad con sus funciones. En consecuencia, las evidencias relacionadas con la planeación, ejecución, informes de auditoría, resultados y hallazgos reposan en dicha dependencia. Por lo anterior, respetuosamente se solicita que esta información sea verificada directamente desde su dependencia".

La Oficina de Control Interno manifiesta respetuosamente que no la considera suficiente frente a la observación planteada, toda vez que evidencia una limitada consideración sobre la importancia del tema objeto de análisis. Adicionalmente, es pertinente señalar que durante la vigencia 2025 la Oficina de Control Interno realizó una auditoría al Modelo de Seguridad de la Información, de la cual se derivó el correspondiente plan de mejoramiento. En este sentido, se considera que la respuesta debió hacer referencia a dicho ejercicio, así como entregar los respectivos informes, reporte, avances e información al cumplimiento de las acciones definidas de acuerdo con la solicitud del equipo auditor.

La respuesta se limitó a señalar una responsabilidad organizacional, pero no demuestra el cumplimiento del requisito normativo y no se suministró información que permita evidenciar y verificar, entre otros:

- La ejecución de auditorías de seguridad de la información.
- La inclusión de pruebas técnicas de seguridad digital.
- La realización de análisis de vulnerabilidades sobre sistemas críticos.
- La ejecución de evaluaciones técnicas de ciberseguridad.
- Los informes y hallazgos identificados y sus planes de tratamiento.

Por otra parte, con relación a la responsabilidad de la Oficina de Control Interno mencionada en la respuesta del proceso, la Ley 87 de 1993 asigna a las Oficinas de Control Interno la función de **evaluación independiente** del Sistema de Control Interno y el seguimiento a la gestión institucional, sin embargo, la misma ley establece que el control interno (como sistema) es responsabilidad de toda la Entidad y no exclusivamente de la OCI. A este respecto, dentro del Plan Anual de Auditoría Interna se pueden incluir

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

 Supersolidaria	INFORME DEFINITIVO ACTIVIDAD DE AUDITORÍA	Código: FT-COIN-007 Julio - 2026 Versión: 03
--	--	---

actividades de la OCI como:

- Auditoría al MSPI o a la seguridad de la información.
- Evaluación de la eficacia de los controles de seguridad.
- Verificación al cumplimiento de la Resolución 500 de 2021.

Si bien es cierto, la Oficina de Control Interno puede realizar evaluaciones y auditorías internas de gestión del MSPI en el marco de sus funciones de evaluación independiente, no puede ser la responsable de ejecutar los componentes técnicos obligatorios que exige el artículo 15 de la Resolución 500 de 2021 de MinTIC.

La OCI realiza auditorías tradicionales generalmente orientadas a evaluar procesos, controles, cumplimiento normativo y gestión de riesgos; el criterio evaluado exige expresamente actividades con naturaleza técnica, como un análisis de vulnerabilidades, pruebas de penetración, revisión de configuraciones de seguridad, entre otros, que no son aplicables a las actividades de la OCI.

Todo lo anterior conlleva a:

- Riesgo de **confusión de roles en las líneas de defensa**, dado que la ejecución de los análisis técnicos de vulnerabilidades, escaneos y monitoreos preventivos corresponde a la Segunda Línea de Defensa (Ejemplo: Oficina de TI, Responsable de Seguridad de la Información); el rol de la OCI (Tercera Línea) es auditar que se hayan realizado efectivamente dichos análisis una vez al año y haya mitigado los hallazgos.
- **Contradicción al Principio de independencia y objetividad** de las Oficinas de Control Interno. Para el caso evaluado, un análisis de vulnerabilidades (o pruebas de penetración / hacking ético) es una actividad de control netamente operativa e informática. Si la OCI operara el software para buscar vulnerabilidades en los servidores de la entidad, estaría coadministrando, lo cual le prohíbe la Ley 87 de 1993 y la Guía de Auditoría del DAFP.
- Se presenta una **falta de idoneidad técnica**. Las OCI por lo general no cuentan con la infraestructura, herramientas de software especializadas (Ejemplo: Nessus), ni los perfiles técnicos de ciberseguridad requeridos para ejecutar de forma directa un análisis de vulnerabilidades profundo a la infraestructura crítica de la entidad.

Criterio

El artículo 15 de la Resolución 500 de 2021 indica:

"15. Control de las actividades incluidas en la estrategia de seguridad digital y gestión de riesgos. Los sujetos obligados deben establecer los mecanismos de control al interior de la entidad que permitan verificar el cumplimiento de las disposiciones establecidas en la política de seguridad de la información que hayan aprobado internamente, realizando auditorías de seguridad de la información al menos una vez al año, que contemplen aspectos técnicos de la seguridad digital como análisis de vulnerabilidades a sistemas de información críticos, entre otros". (Énfasis fuera de texto).

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

 Supersolidaria	INFORME DEFINITIVO ACTIVIDAD DE AUDITORÍA	Código: FT-COIN-007 Julio - 2026 Versión: 03
--	--	---

Causas

- Ausencia de incorporación de evaluaciones técnicas de seguridad digital dentro de los mecanismos de control implementados por la entidad.
- Interpretación del requisito centrada exclusivamente en auditorías de control interno sin considerar los componentes técnicos exigidos por la norma.

Consecuencias

- Posible desconocimiento de vulnerabilidades técnicas presentes en sistemas de información críticos.
- Debilidad en la evaluación de la efectividad de los controles de seguridad digital implementados por la entidad.

Recomendaciones

- Implementar auditorías o evaluaciones de seguridad de la información que incluyan actividades técnicas como análisis de vulnerabilidades, revisión de configuraciones seguras, pruebas técnicas de seguridad y evaluación de sistemas críticos.

Al respecto, el proceso respondió al informe preliminar indicando:

"Frente a esta recomendación, no se acoge, teniendo en cuenta que la Entidad sí realiza evaluaciones técnicas de seguridad, análisis de vulnerabilidades y pruebas de seguridad sobre sus activos y sistemas. Como evidencia de estas actividades, se cuenta con el "Informe Final Ethical Supersolidaria" correspondiente a la vigencia 2025, resultado de la evaluación técnica 1 [REDACTED]". Se aclara que, al momento de atender la solicitud de información, el término "auditorías de seguridad de la información" fue interpretado por el equipo de Seguridad de la Información como auditorías formales de cumplimiento, tales como evaluaciones frente al MSPI, ISO/IEC 27001 u otros marcos de referencia, similares a los ejercicios realizados por la Oficina de Control Interno. Por esta razón, inicialmente no se asociaron al requerimiento las actividades de análisis de vulnerabilidades, revisión de configuraciones y demás pruebas técnicas de seguridad que realiza la Entidad.

Una vez precisado el alcance de la recomendación, se aclara que dichas actividades se encuentran implementadas y se realizan como parte de la gestión de seguridad de la información y de vulnerabilidades. No obstante, los documentos que contienen vulnerabilidades, resultados y hallazgos técnicos no serán entregados como evidencia documental, debido a la naturaleza sensible de la información que contienen, relacionada con activos, vulnerabilidades, configuraciones y demás aspectos técnicos de seguridad de la Entidad. Para efectos de su verificación, los informes y evidencias técnicas podrán ser exhibidos directamente al auditor, en el momento que este determine y bajo condiciones controladas de consulta, sin que ello implique la entrega, reproducción o incorporación de dichos documentos al paquete de evidencias. En consecuencia, no se acoge la recomendación, toda vez que las evaluaciones y actividades técnicas recomendadas ya se encuentran implementadas. La situación presentada obedeció a la interpretación inicial del alcance del término "auditoría" durante la solicitud de evidencias, y no a la ausencia de evaluaciones técnicas de seguridad.

Respuesta OCI.

Es importante señalar que la solicitud de información remitida al proceso incluyó expresamente los criterios de evaluación aplicables, con el propósito de delimitar claramente el alcance de los requerimientos y facilitar la identificación de las evidencias y soportes necesarios para atenderlos. En este sentido, se recomienda que, para futuras solicitudes, la información requerida sea analizada de manera integral, de modo que las respuestas y los soportes aportados correspondan de forma suficiente, pertinente y

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

 Supersolidaria	INFORME DEFINITIVO ACTIVIDAD DE AUDITORÍA	Código: FT-COIN-007 Julio - 2026 Versión: 03
--	--	---

completa a los aspectos objeto de evaluación.

El proceso manifiesta que sí se realizaron evaluaciones técnicas de seguridad, análisis de vulnerabilidades y pruebas de seguridad, e incluso menciona la existencia del “Informe Final de Ethical”, sin embargo, simultáneamente indica que los informes y soportes no serán entregados debido a la sensibilidad de la información contenida en ellos y que únicamente podrían ser consultados posteriormente bajo condiciones controladas.

En consecuencia, la respuesta permite inferir que posiblemente las actividades existen, pero no demuestra documentalmente su ejecución ante el equipo auditor. La sola manifestación del proceso respecto a la existencia de los informes no constituye evidencia de auditoría suficiente para desvirtuar un hallazgo. La sensibilidad de la información no elimina la obligación de acreditar su existencia y ejecución mediante mecanismos de consulta controlada, actas de validación, certificaciones, informes ejecutivos, evidencias restringidas o cualquier otro mecanismo institucional que permita la verificación correspondiente.

Respecto a la posibilidad de realizar la revisión de las evidencias únicamente mediante mesas de trabajo o consultas controladas, la OCI considera que este mecanismo no es viable para la totalidad de la información requerida. Lo anterior, en razón a los tiempos y actividades definidos en el Plan Anual de Auditoría, los cuales no permiten destinar jornadas adicionales para efectuar revisiones presenciales. En consecuencia, las evidencias deben aportarse de manera oportuna y completa, para su análisis, validación y conservación dentro de los papeles de trabajo que soportan las conclusiones de la auditoría. Por todo lo anteriormente presentado, se mantiene la recomendación.

Por otra parte, se reitera la posición de la Oficina de Control Interno frente a la atención de los requerimientos de información, situación que ya había sido advertida con ocasión de la Auditoría al Software ADA realizada durante la presente vigencia:

De conformidad con lo establecido en la Ley 87 de 1993, la Oficina de Control Interno ejerce funciones de evaluación independiente del Sistema de Control Interno, asesoría, seguimiento y evaluación de la gestión institucional, para lo cual se encuentra plenamente facultada para solicitar y acceder a la información, documentación, registros, bases de datos, sistemas de información, soportes y demás evidencias que resulten necesarias para el cumplimiento de sus funciones constitucionales y legales. En consecuencia, dicho acceso no puede ser restringido, condicionado o diferido de manera discrecional por parte de las dependencias o servidores responsables de la información requerida.

En este mismo sentido, la Ley 1712 de 2014, por la cual se regula el derecho de acceso a la información pública, establece que toda información que repose en poder de las entidades públicas se presume pública, salvo las excepciones expresamente previstas en la Constitución o la ley. Por lo tanto, cualquier limitación al acceso debe encontrarse debidamente sustentada en una causal legal de reserva o clasificación, identificando expresamente la norma que la soporta y la motivación correspondiente. En consecuencia, argumentos asociados a una supuesta “reserva para socialización”, “información en

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

 Supersolidaria	INFORME DEFINITIVO ACTIVIDAD DE AUDITORÍA	Código: FT-COIN-007 Julio - 2026 Versión: 03
--	--	---

construcción”, “pendiente de aprobación” u otras consideraciones similares no constituyen, por sí solos, fundamento legal válido para negar, restringir o aplazar la entrega de información a la Oficina de Control Interno en ejercicio de sus funciones.

Adicionalmente, debe precisarse que la información requerida por la Oficina de Control Interno no se solicita para fines de divulgación o publicación, sino para el desarrollo de actividades de aseguramiento, evaluación y seguimiento, dentro del marco de las competencias legalmente asignadas y bajo los deberes de reserva, confidencialidad y manejo adecuado de la información que resulten aplicables.

Por lo anterior, se recuerda que la entrega oportuna, integral y completa de la información requerida durante los ejercicios de auditoría constituye un deber de los responsables de los procesos y una condición necesaria para el adecuado desarrollo de las actividades de evaluación independiente. La entrega parcial, tardía o injustificadamente restringida de la información puede generar limitaciones al alcance de la auditoría, afectar la obtención de evidencia suficiente y competente, e impactar las conclusiones del ejercicio auditor.

Finalmente, la negativa injustificada, la obstrucción, la dilación o cualquier actuación que limite el acceso a la información requerida por la Oficina de Control Interno pueden constituir una restricción al ejercicio de las funciones de control interno y dar lugar a las actuaciones que correspondan por parte de las instancias competentes, de conformidad con el marco normativo aplicable, incluido el régimen disciplinario previsto en la Ley 1952 de 2019 y demás disposiciones que regulan los deberes de los servidores públicos en materia de colaboración con los organismos de control y evaluación institucional.

HALLAZGO 6. Falta de entrega de evidencias para evaluar las Etapas generales de la gestión de incidentes de seguridad digital.

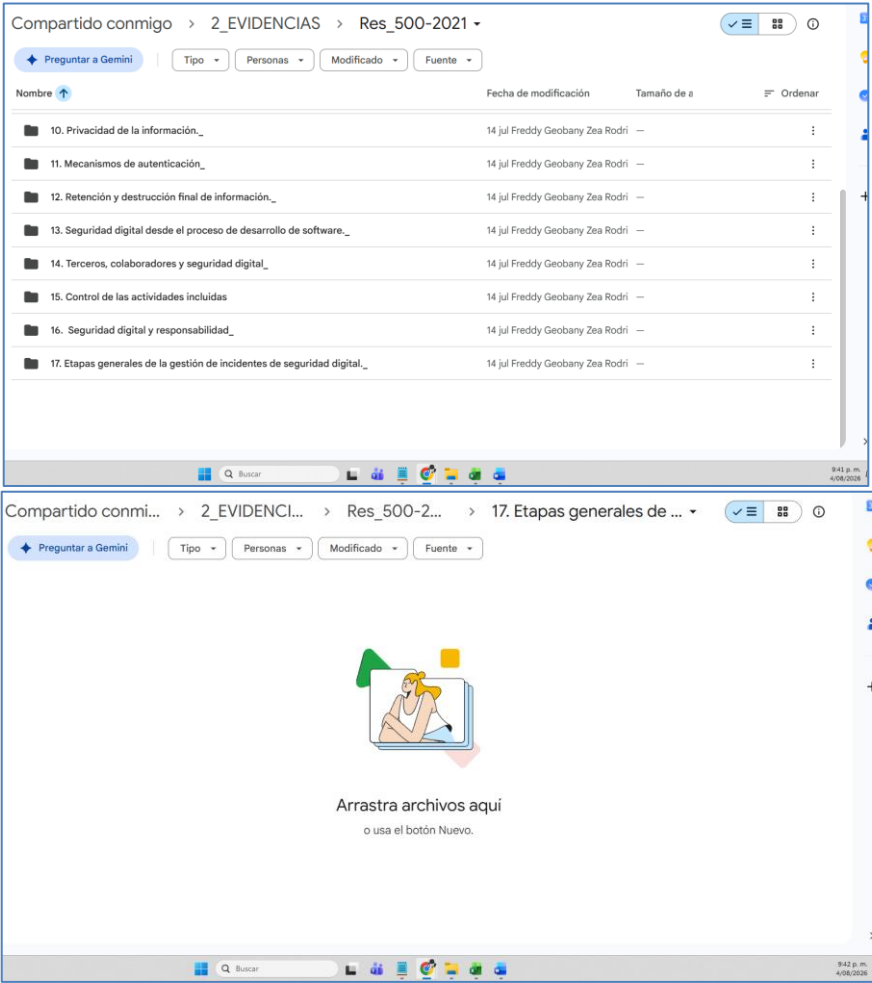
Condición

Durante la ejecución de la Auditoría se solicitó información y evidencia para verificar la implementación y cumplimiento de las etapas generales de la gestión de incidentes de seguridad digital establecidas en el artículo 17 de la Resolución 500 de 2021.

No obstante, el proceso no suministró la documentación, registros, reportes, evidencias o soportes requeridos para validar la ejecución de dichas etapas, impidiendo verificar el cumplimiento normativo asociado a la identificación, reporte, contención, análisis, tratamiento, recuperación, cierre y demás actividades relacionadas con la gestión de incidentes de seguridad digital.

Asimismo, durante el desarrollo de la auditoría se presentaron limitaciones para el acceso y verificación de algunas evidencias requeridas, lo que impidió evaluar integralmente los aspectos de la gestión de incidentes de seguridad digital. Esta situación pone de manifiesto la necesidad de fortalecer los mecanismos de disponibilidad, custodia y acceso oportuno a la información requerida en ejercicios de seguimiento, auditoría y control; lo anterior, no implica una valoración de la disposición de colaboración por parte del proceso.

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno



Criterio

- **Resolución 500 de 2021 del Ministerio TIC:** Artículo 17. *Etapas generales de la gestión de incidentes de seguridad digital*, mediante el cual se establece que las entidades obligadas deben implementar y gestionar las etapas definidas para la atención de incidentes de seguridad digital y disponer de los mecanismos, procedimientos y evidencias que soporten su ejecución.
- **Ley 87 de 1993:** El Sistema de Control Interno debe garantizar la existencia de mecanismos de verificación, evaluación, control y generación de información necesaria para demostrar el cumplimiento de los objetivos institucionales y de las disposiciones legales aplicables.
- **Carta de Compromiso:** La dependencia auditada se comprometió a:
 - Entregar oportunamente la información requerida y suministrar toda la información relacionada con la gestión del proceso evaluado.
 - Garantizar que la información proporcionada fuera válida, integral y completa para los propósitos del proceso auditor.

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

 Supersolidaria	INFORME DEFINITIVO ACTIVIDAD DE AUDITORÍA	Código: FT-COIN-007 Julio - 2026 Versión: 03
--	--	---

Causas

- Debilidades en la gestión, conservación y disponibilidad de los registros y evidencias asociadas a la gestión de incidentes de seguridad digital.
- Falta de seguimiento y control por parte de los responsables del proceso para garantizar la disponibilidad de la información requerida.

Riesgos

- Incumplimiento de los lineamientos de la Resolución 500 de 2021.
- Imposibilidad de demostrar la adecuada gestión de incidentes de seguridad digital, afectando la capacidad institucional para proteger la confidencialidad, integridad y disponibilidad de la información.

Recomendaciones

- Fortalecer los mecanismos de almacenamiento, custodia, disponibilidad y verificación de las evidencias, con el fin de garantizar su acceso oportuno y trazabilidad durante los ejercicios de seguimiento, auditoría y control (no sujeta de plan de mejoramiento).

Al respecto, el proceso respondió al informe preliminar indicando:

"Frente a esta observación, se precisa que la información relacionada con las etapas generales de la gestión de incidentes de seguridad digital sí se había preparado para su entrega en el marco de la auditoría. Se aclara que, durante el proceso de auditoría no se informó a la OAPS sobre la imposibilidad de acceder o consultar dichas evidencias, ni se efectuó una nueva solicitud para su entrega, circunstancia que habría permitido verificar y subsanar oportunamente el inconveniente técnico. Una vez conocida la situación, se procedió a disponer nuevamente la información para su correspondiente verificación en la misma ruta.

De igual manera, se solicita respetuosamente retirar la afirmación relacionada con "incumplimiento de los compromisos adquiridos por la dependencia auditada mediante la Carta de Compromiso", dado que dicha situación no obedeció a algo deliberado por parte del equipo responsable. La novedad presentada correspondió exclusivamente a una situación técnica asociada al cargue de archivos por su tamaño, la cual se está subsanando. En este sentido, la situación presentada no debería interpretarse como una falta de colaboración, disposición o incumplimiento en la entrega de información".

Respuesta OCI.

La justificación remitida por el proceso no desvirtúa el hallazgo, pero sí permite confirmar o aclarar la causa de la situación, indicando que se presentó un tema técnico asociado al cargue de archivos; por lo anterior, se considera razonable y se procede a ajustar la redacción del informe eliminando referencias relacionadas con una presunta falta de colaboración o incumplimiento de la Carta de Compromiso.

De la misma manera, se modifican las recomendaciones orientadas a la causa asociada.

No obstante, esta circunstancia no modifica el resultado de auditoría, dado que el hallazgo se fundamentó en la imposibilidad de verificar las evidencias requeridas durante el ejercicio auditor.

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

 Supersolidaria	INFORME DEFINITIVO ACTIVIDAD DE AUDITORÍA	Código: FT-COIN-007 Julio - 2026 Versión: 03
--	--	---

4.2. OBJETIVO ESPECÍFICO DOS. Validar la aplicación de la Resolución 2277 de 2025 (03-06-2025) "Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia".

Se identificaron las siguientes situaciones o debilidades:

HALLAZGO 7. Debilidades en la formalización y completitud de las salidas requeridas para la fase de contexto y alcance del MSPI definido en el Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información.

Condición

La entidad aportó un Manual de Seguridad y Privacidad de la Información no oficial (en construcción), el cual contiene apartados relacionados con el contexto organizacional, las partes interesadas y el alcance del MSPI, sin embargo, no se evidenciaron de manera independiente o formalizada algunas de las salidas obligatorias exigidas por el modelo, particularmente el compendio de necesidades y expectativas de las partes interesadas y el análisis de partes interesadas en seguridad de la información.

Realizando un análisis puntual a cada numeral, se identifica que:

- **Para “7.1.1 Comprensión de la organización y su contexto”:** Se evidenció que el documento aportado incluye un capítulo denominado “Comprensión de la organización y de su contexto”, que contienen factores internos y externos que pueden impactar la seguridad y privacidad de la información, tales como aspectos regulatorios, tecnológicos, operativos, presupuestales y de talento humano.

No obstante, el criterio establece como salida el documento “Contexto de la entidad (Política de Planeación Institucional)”. La evidencia suministrada corresponde a un manual del MSPI en proceso de elaboración, por lo que no permite verificar su articulación con el documento institucional exigido ni confirmar el cumplimiento de la salida requerida.

- **Para “7.1.2 Necesidades y expectativas de las partes interesadas”:** El manual contiene una sección orientada a la identificación de las necesidades y expectativas de las partes interesadas en materia de seguridad de la información, sin embargo, el documento remite a la “Matriz de partes interesadas del MSPI”, la cual no fue aportada como evidencia.
- **Para “7.1.3 Definición del alcance del MSPI”:** Se identificó un apartado relacionado con la determinación del alcance del MSPI, donde se establece de manera general que el modelo cubre procesos, activos de información, sistemas de información, infraestructura tecnológica y recurso humano que soportan la misión institucional, sin embargo, el alcance presentado no define de forma específica los límites, procesos, recursos y sistemas cubiertos por el modelo, conforme a lo

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

 Supersolidaria	INFORME DEFINITIVO ACTIVIDAD DE AUDITORÍA	Código: FT-COIN-007 Julio - 2026 Versión: 03
--	--	---

requerido por el criterio. Adicionalmente, la información se encuentra en un documento que aún no ha sido revisado, aprobado ni formalizado.

La evidencia aportada muestra avances significativos e importantes en la implementación del MSPI versión 2025, sin embargo:

- El documento presentado se encuentra en proceso de construcción y aprobación.
- No corresponde a una versión formalizada por la Entidad.
- No permite validar la totalidad de las salidas exigidas en el criterio analizado.
- Hace referencia a documentos complementarios no suministrados.

Por lo anterior, no se aportaron las evidencias requeridas para demostrar el cumplimiento de las salidas definidas por el MSPI.

Se incluyen en este mismo hallazgo, las solicitudes de información donde el proceso respondió que la evidencia es “el Manual de Seguridad de la Información, documento que actualmente se encuentra en proceso de construcción, revisión y aprobación”:

- 7.2.3. Roles y responsabilidades. Salidas:
 - Roles y responsabilidades en seguridad de la información de las diferentes áreas o procesos de la entidad.
 - Definición del rol de: responsable de seguridad de la información, indicando sus funciones y responsabilidades.

Criterio

Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información, definido en el anexo 1 de la Resolución 2277 de 2025, que indica:

Fase 1: Planificación.

7.1. Contexto.

7.1.1. Comprensión de la organización y de su contexto

Lineamiento: Determinar los elementos externos e internos que son relevantes con las actividades que realiza la entidad en el desarrollo de su misión y que podrían influir en las capacidades para lograr los objetivos del modelo, alineado con los objetivos estratégicos de la entidad, teniendo en cuenta procesos necesarios y sus interacciones.

Propósito: Conocer en detalle las características de la entidad y su entorno con el fin de implementar el Modelo de Seguridad y Privacidad adaptado a las condiciones específicas de cada entidad.

Salidas: Documentos obligatorios: Contexto de la Entidad (Política de Planeación Institucional).

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.

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

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.

Salidas: Documentos obligatorios: Compendio de necesidades y expectativas de las partes interesada. (Política de Planeación Institucional). Análisis de partes interesadas en seguridad de la información.

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.

Salidas: 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)."

Causas

- El proceso de actualización documental del MSPI se encuentra en etapa de construcción y aprobación.
- No se aportaron todos los documentos soporte asociados a las salidas obligatorias definidas por el modelo.

Consecuencias

- Riesgo de implementación incompleta de la fase de planificación del MSPI.
- Dificultad para demostrar el cumplimiento integral de los requisitos documentales exigidos por el MSPI versión 2025.

Recomendaciones

- Formalizar y aprobar el Manual de Seguridad y Privacidad de la Información y los documentos asociados al contexto, partes interesadas y alcance del MSPI, según lo dispuesto por la Resolución 500 de 2021 y sus modificaciones.
- Modificar la TRD del proceso, con el fin de incluir las evidencias documentales correspondientes a cada salida obligatoria exigida por el modelo.

Al respecto, el proceso respondió al informe preliminar indicando:

*"Frente a esta recomendación, **se acoge**, precisando que la formalización y aprobación del Manual de Seguridad y Privacidad de la Información, así como la actualización de los documentos asociados al contexto, partes interesadas y alcance del MSPI, hacen parte de las actividades previstas para la actualización e implementación del Modelo. Se aclara que los lineamientos e instrumentos del MSPI fueron actualizados recientemente, en alineación con ISO/IEC 27001:2022, lo cual implica la revisión y adecuación de los instrumentos institucionales existentes. En razón de esta actualización, durante la vigencia 2026 la OAPS viene adelantando las actividades necesarias para ajustar, actualizar y formalizar la documentación requerida para dar cumplimiento a la nueva versión del Modelo, incluyendo el Manual de Seguridad y Privacidad de la Información y las demás salidas documentales*

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

 Supersolidaria	INFORME DEFINITIVO ACTIVIDAD DE AUDITORÍA	Código: FT-COIN-007 Julio - 2026 Versión: 03
--	--	---

correspondientes. Por este motivo, estas actividades continúan actualmente en ejecución como parte del proceso de actualización del MSPI.

Respecto de la Tabla de Retención Documental (TRD), se realizará la revisión de las series, subseries y tipologías documentales aplicables, en articulación con el área responsable de la gestión documental, con el fin de determinar los ajustes que resulten necesarios para garantizar la adecuada identificación, conservación y trazabilidad de las evidencias documentales generadas en el marco del MSPI, conforme a los procedimientos institucionales establecidos. En consecuencia, la recomendación se acoge y continuará siendo atendida durante la vigencia 2026, en el marco de las actividades que actualmente desarrolla la OAPS para la actualización e implementación del MSPI y la adecuación de sus instrumentos a los lineamientos vigentes”.

Respuesta OCI.

La respuesta ratifica los hechos identificados en la auditoría y confirma que la documentación requerida se encuentra en proceso de actualización y formalización. El hallazgo se mantiene y las recomendaciones continúan siendo pertinentes.

HALLAZGO 9. Inexistencia del Acto administrativo de aprobación de la Estrategia de Seguridad Digital, junto con su publicación o socialización.

Condición

Se solicitó el Acto administrativo de aprobación formal de la Estrategia de Seguridad Digital y las evidencia de publicación o socialización, para lo cual, se aportaron actas de comité que evidencian la presentación y aprobación de los Planes de Seguridad y Privacidad de la Información de las vigencias 2025 y 2026; sin embargo, no se suministró evidencia documental del acto administrativo de carácter general mediante el cual se aprueba formalmente la Estrategia de Seguridad Digital, ni los soportes suficientes de su publicación o divulgación institucional.

Criterio

El artículo 5 de la Resolución 500-2021, establece que la Estrategia de Seguridad Digital debe:

- Los sujetos obligados deben adoptar la estrategia de seguridad digital.
- Integrarse al Plan de Seguridad y Privacidad de la Información.
- Ser aprobada a través de un acto administrativo de carácter general.

Causa

- Debilidad en formalización documental de la estrategia y en la gestión del cumplimiento normativo asociado al MSPI.

Consecuencias

- Riesgo de incumplimiento de la Resolución 500 de 2021 y en la gobernanza de seguridad digital.
- Riesgo de falta de trazabilidad frente a la adopción institucional de la estrategia de seguridad digital.

Recomendaciones

- Adoptar formalmente la Estrategia de Seguridad Digital por medio de un acto administrativo de carácter general.

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

 Supersolidaria	INFORME DEFINITIVO ACTIVIDAD DE AUDITORÍA	Código: FT-COIN-007 Julio - 2026 Versión: 03
--	--	---

Al respecto, el proceso respondió al informe preliminar indicando:

"Misma respuesta hallazgo No 1".

Respuesta OCI.

Sin embargo, no se desvirtúa el hallazgo, dado que se fundamenta en que la Estrategia de Seguridad Digital se encuentra incorporada dentro del PETI, el MSPI y los instrumentos de planeación institucional; el artículo 5 de la Resolución 500 de 2021 establece expresamente que la Estrategia de Seguridad Digital debe ser aprobada mediante acto administrativo de carácter general. La evidencia aportada corresponde a instrumentos de planeación y seguimiento, mas no al acto formal requerido por la norma. De acuerdo con este análisis, se ajustan las recomendaciones.

Alerta Temprana 10:

Inicialmente, el alcance de la auditoría contemplaba la validación integral de los lineamientos y salidas definidas en la Resolución 500 de 2021 y en el Anexo 1 de la Resolución 2277 de 2025. No obstante, durante el desarrollo del ejercicio se evidenció un alto volumen de documentos, metodologías, procedimientos y registros que aún se encuentran en proceso de construcción, actualización, revisión o aprobación, según lo informado por el proceso auditado.

En tal sentido, y atendiendo los principios de objetividad, razonabilidad y valoración integral de la evidencia, el equipo auditor considera pertinente dar por finalizada la evaluación en esta etapa y permitir que el proceso concluya la implementación de los requisitos y salidas obligatorias del modelo.

Una vez finalizada dicha implementación, se propondrá la realización de una nueva verificación en el marco del Programa Anual de Auditorías Internas, con el fin de evaluar de manera integral el cumplimiento de los lineamientos y verificar la formalización, implementación y efectividad de los entregables exigidos por la normatividad aplicable.

4.3. OBJETIVO ESPECÍFICO TRES. Conceptuar sobre el cumplimiento de controles del mapa de riesgos del proceso auditado relacionados con los objetivos anteriores y/o proponer nuevos controles y riesgos.

Precisión sobre el alcance de este objetivo

Este objetivo específico tuvo un enfoque principalmente consultivo y de asesoramiento, en concordancia con el rol de evaluación y rol de prevención de riesgos que ejerce la Oficina de Control Interno.

En este sentido, los aspectos identificados bajo este objetivo, así como los riesgos y controles sugeridos para evaluación, no constituyen hallazgos de auditoría, incumplimientos normativos ni observaciones con carácter obligatorio, sino

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

 Supersolidaria	INFORME DEFINITIVO ACTIVIDAD DE AUDITORÍA	Código: FT-COIN-007 Julio - 2026 Versión: 03
--	--	---

recomendaciones técnicas y oportunidades de fortalecimiento orientadas a contribuir al mejoramiento continuo de la gestión de riesgos de seguridad y privacidad de la información.

Las recomendaciones formuladas buscan complementar la cobertura actual del mapa de riesgos y aportar elementos de análisis para que el proceso auditado evalúe, de acuerdo con su metodología de administración de riesgos, la pertinencia de incorporar nuevos riesgos, controles o mecanismos de seguimiento relacionados con el MSPI, la seguridad de la información, la privacidad de la información y el cumplimiento normativo.

Por lo anterior, las observaciones presentadas en este apartado deben entenderse como sugerencias técnicas de mejora y asesoramiento, emitidas en ejercicio del rol preventivo y de generación de valor de la Oficina de Control Interno, sin que su ausencia constituya por sí misma un incumplimiento o una desviación frente a los criterios evaluados.

Producto de este análisis, se modificó en este apartado, los conceptos presentados.

El mapa de riesgos presenta un alto grado de madurez, ya que:

- Identifica activos de información.
- Define amenazas y vulnerabilidades.
- Relaciona riesgos con controles específicos de ISO 27001.
- Establece responsables.
- Define periodicidades.
- Mantiene seguimiento de evidencias.
- Incluye evaluación de eficacia de controles.

No obstante, podría presentar una cobertura integral en todos los componentes exigidos por la Resolución 500 de 2021 y la Resolución 2277 de 2025, dado que la matriz actual está concentrada principalmente en controles tecnológicos y de ciberseguridad operativa.

El mapa constituye un mecanismo adecuado para la administración de riesgos de seguridad de la información, pero se recomienda la incorporación de riesgos y controles adicionales asociados a gobernanza, cumplimiento normativo, gestión documental del MSPI, continuidad del modelo, privacidad de la información y seguimiento de requisitos introducidos en el MSPI 2025.

Fortalezas identificadas: Se evidencian controles alineados con requisitos de la Resolución 500 de 2021, principalmente con los siguientes aspectos:

Control	Valoración
Gestión de accesos	• Gestión de usuarios. • Revisión de privilegios. • MFA. • Gestión de cuentas privilegiadas.

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

Control	Valoración
Monitoreo y detección	• SIEM. • Monitoreo de eventos. • Monitoreo de nube.
Gestión de vulnerabilidades	• Escaneos. • Aplicación de parches. • Remediación.
Protección perimetral	• Firewall. • IDS/IPS. • Seguridad de red.
Malware	• Herramientas EDR/Antivirus. • Seguimiento de incidentes de malware
Desarrollo seguro	• Desarrollo seguro. • Seguridad en aplicaciones. • Pruebas de seguridad.
Continuidad	• Backups. • DRP. • Recuperación ante desastres.
Cultura de seguridad	• Sensibilización y capacitación.

Analizando de forma general la matriz de riesgos frente al MSPI 2025, no se observan riesgos relacionados con:

Situación	Análisis
Cumplimiento normativo del MSPI	La Resolución 2277 de 2025 fortalece componentes como: contexto, Partes interesadas, Alcance, Liderazgo, Gestión documental, Indicadores, Revisión por la dirección, Mejora continua. No existe un riesgo que controle: Incumplimiento de los requisitos del MSPI por ausencia de documentación, seguimiento o actualización del modelo relacionados a: • Incumplimiento de lineamientos del Mintic. • Gobierno Digital y MSPI. • Protección de datos. • Seguridad digital.
Gestión de activos de información	Aunque existe una guía de activos de información, en el mapa no aparece un riesgo relacionado con: Inventario desactualizado, Clasificación incorrecta, Activos sin propietario, Infraestructura crítica sin identificar.

Nuevos riesgos que se recomiendan evaluar su incorporación.

Id	Riesgo	Descripción	Controles sugeridos
1	Incumplimiento del MSPI	Posible incumplimiento de los requisitos del MSPI por falta de actualización,	• Seguimiento trimestral al plan de implementación del MSPI.

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

 Supersolidaria	INFORME DEFINITIVO ACTIVIDAD DE AUDITORÍA	Código: FT-COIN-007 Julio - 2026 Versión: 03
--	--	---

Id	Riesgo	Descripción	Controles sugeridos
		formalización, seguimiento o implementación de las actividades requeridas por la Resolución 2277 de 2025.	- Revisión semestral por Comité Institucional de Gestión y Desempeño. - Medición periódica del nivel de madurez del MSPI.
2	Gestión inadecuada de activos de información	Posible afectación de la confidencialidad, integridad y disponibilidad por inventarios desactualizados o clasificación incorrecta de activos e infraestructura crítica.	- Revisión semestral del inventario de activos. - Validación de propietarios y custodios. - Clasificación anual de activos críticos.
3	Incumplimiento de protección de datos personales	Posible sanción, pérdida reputacional o afectación legal por tratamiento inadecuado de datos personales.	- Revisión periódica de bases de datos. - Validación de autorizaciones. - Seguimiento a incidentes de datos personales.
4	Gestión inadecuada de incidentes de seguridad digital	Posible incremento del impacto de incidentes por ausencia de gestión, análisis y reporte oportuno.	- Bitácora de incidentes. - Reporte al CSIRT. - Comité de seguimiento mensual.
5	Incumplimiento de auditorías técnicas de seguridad	Posible materialización de vulnerabilidades por ausencia de auditorías técnicas y análisis de vulnerabilidades sobre activos críticos.	- Escaneos semestrales. - Ethical hacking anual. - Seguimiento a planes de mejoramiento.

Concepto Final de Auditoría:

Se destaca el trabajo realizado en la identificación y gestión de riesgos asociados a los componentes tecnológicos y de ciberseguridad operativa, evidenciándose la incorporación de controles relacionados con accesos, monitoreo, vulnerabilidades, respaldo de información, continuidad, seguridad perimetral y desarrollo seguro.

No obstante, como oportunidad de fortalecimiento y alineación con los lineamientos vigentes del Modelo de Seguridad y Privacidad de la Información (MSPI), se recomienda ampliar progresivamente el alcance del mapa de riesgos para incorporar elementos relacionados con la gobernanza, el cumplimiento normativo y la madurez del modelo, en concordancia con los requisitos establecidos en la Resolución 500 de 2021 y su actualización mediante la Resolución 2277 de 2025.

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

 Supersolidaria	INFORME DEFINITIVO ACTIVIDAD DE AUDITORÍA	Código: FT-COIN-007 Julio - 2026 Versión: 03
--	--	---

En este sentido, sería conveniente evaluar la inclusión de riesgos y controles asociados a aspectos como la implementación y sostenibilidad del MSPI, la gestión de activos de información e infraestructura crítica, la protección de datos personales, la gestión de incidentes de seguridad digital, las auditorías técnicas de seguridad y el seguimiento al cumplimiento de los requisitos del modelo.

Esta ampliación permitiría contar con una visión más integral de los riesgos de seguridad y privacidad de la información, fortalecer la capacidad de seguimiento y toma de decisiones, y evidenciar de manera más robusta el cumplimiento de las obligaciones y buenas prácticas promovidas por el MSPI.

Nota. Este objetivo pretende retroalimentar la actualización permanente de los mapas de riesgos de gestión, en este caso el tema de seguridad de la información, cuyo propósito es que los informes de la OCI sean consultados en el proceso de identificación y valoración de riesgos en la Supersolidaria. Igualmente, no conllevan acciones de mejoramiento.

5. PLAN DE MEJORAMIENTO.

Se requiere la definición y suscripción del respectivo plan de mejoramiento. La etapa inicial de FORMULACIÓN, será diligenciada por la oficina de control interno, quien, como valor agregado, hará una propuesta de acciones de mejoramiento con base en las recomendaciones para cada hallazgo, sin embargo, las propias que proponga el auditado junto con las acá recomendadas, deben ser consensuadas, hasta su respectiva definición.

Por lo anterior, se remitirá dentro de los 5 días siguientes, desde la OCI, el formato FT-COIN-008, con la formulación del plan de mejoramiento, para lo pertinente, otorgándose el termino de hasta 5 días hábiles para su trámite.

Tener en cuenta las siguientes Normas y Tips:

Normas:

- El artículo 4 Ley 87 /93, establece que la responsabilidad de sus directivos " g. Aplicación de las recomendaciones resultantes de las evaluaciones del control interno "
- El artículo 12. Establece como función de la OCI, k) Verificar que se implanten las medidas respectivas recomendadas
- Decreto 338 2019 y Guía de Autoría del DAFP, establece que en relación con el plan de mejoramiento el Jefe de Control Interno debe: Acompañar a cada área en la formulación adecuada, rigurosa y con enfoque estratégico de las acciones de mejora (rol de prevención, resultante de trabajos de auditoria).

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno

 Supersolidaria	INFORME DEFINITIVO ACTIVIDAD DE AUDITORÍA	Código: FT-COIN-007 Julio - 2026 Versión: 03
--	--	---

Aspectos para tener en cuenta:

- Lea el INSTRUCTIVO del formato, en la parte FORMULACION Y DEFINICION. Va en una hoja del archivo Excel del formato FT_COIN_008.
- Se debe revisar y definir la parte de DEFINICION, la cual lleva una propuesta de la OCI y tenga en cuenta como referencia la parte de FORMULACION, la cual es de competencia de la OCI, siendo inobservable.
- La acción de mejoramiento debe atacar cada causa posible y por ende evitar el hallazgo se repita. Un hallazgo puede tener más de una acción de mejoramiento.
- Fije acciones de mejoramiento acordes con las recomendaciones del informe de auditoría.
- Las acciones de mejoramiento de tipo CORRECTIVO, propuestas por la OCI, tienen una característica casi total, no son negociables.
- Cuando la acción la puede realizar en forma DIRECTA el proceso auditado, tiene un plazo de 1 a 3 meses; cuando es COMPARTIDA, por qué dependen de otro proceso, se otorga de 1 a máximo 6 meses y cuando la acción es de tipo INSTITUCIONAL, conlleva un plazo de 1 a 12 meses, como máximo.
- Las evidencias deben apuntar en forme definitiva e implicar demostrar su gestión de la acción correctiva, siendo eficaces y eficientes. Son tangibles generalmente y deben ser explicadas en la siguiente columna.

Atentamente,

Firmado en original

JORGE HERNANDO PEDRAZA VARGAS

Jefe Oficina de Control Interno

Elaboró: Rafael Hernando Calle Cabezas - Contratista, Líder de la Auditoría.

HISTORIAL DE CAMBIOS

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
0	Noviembre 2020	Primera versión del documento
1	Octubre 2023	Actualización Logos institucionales
2	Marzo 2025	Actualización del procedimiento de acuerdo a la actualización de la Guía de Auditoría Basada en Riesgos SES.
3	Julio 2026	Actualización tips plan de mejoramiento.

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno	Nombre: Jorge Hernando Pedraza Vargas Cargo: Jefe Oficina de Control Interno