

	INFORME DE AUDITORIA	Auditoría no.	35 -25	
		Fecha del informe		
		Día	Mes	Año
		20	10	2025

Informe	<input type="checkbox"/>	Preliminar	<input checked="" type="checkbox"/>	Final
----------------	--------------------------	-------------------	-------------------------------------	--------------

1. INFORMACIÓN GENERAL

Tipo de Informe	<input checked="" type="checkbox"/>	Auditoría	<input type="checkbox"/>	Seguimiento
Procesos auditados /Evaluado	Seguridad y Privacidad de la Información			
Auditor líder	Alberto Castiblanco Bedoya	Equipo Auditor	Raúl Alberto Ruiz García	
Responsable del proceso, dependencia, área o actividad auditada /evaluada	Rubén Darío Ochoa Arbeláez Johana Cañón Londoño			

2. OBJETIVO

Evaluar la gestión del Proceso de Seguridad y Privacidad de la Información, conforme a los requisitos legales e institucionales tales como procedimientos, políticas, planes y demás lineamientos aplicables, así como la eficacia de las acciones de los planes de mejora y la de los controles frente a los riesgos.

3. ALCANCE

Verificar el nivel de cumplimiento de las actividades del Proceso de Seguridad y Privacidad de la información, en el marco de los procedimientos, instructivos, políticas, riesgos y planes estratégicos definidos, correspondiente al periodo comprendido entre Junio de 2024 a julio de 2025 e implica realizar una revisión de los sistemas, aplicaciones, gestiones, operaciones, el uso de datos y otros procesos relacionados con las tecnologías de la información en COPNIA, con el fin de verificar el acatamiento normativo, la efectividad de los controles definidos, identificar nuevos riesgos y formular recomendaciones para que el sistema logre las características de concordancia, integralidad e integridad y efectividad que promueven tanto las normas de calidad como las que regulan los sistema de información y tecnología del Estado Colombiano y el cumplimiento de las políticas definidas por el Copnia en su Plan Estratégico de Tecnologías de la Información y las Comunicaciones - PETIC.

4. ACTIVIDADES DESARROLLADAS

Dentro de la auditoría realizada al proceso se evaluaron los criterios generales relacionados con:

	INFORME DE AUDITORIA	Auditoría no.	35 -25	
		Fecha del informe		
		Día	Mes	Año
		20	10	2025


Criterios generales	Descripción
Decreto 767 de 2022	"Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"
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."
Modelo de Seguridad y Privacidad de la Información de 2021 versión 4	Incluye como referentes principales: Documento Maestro del Modelo de Seguridad de y Privacidad de la Información de MINTIC Norma ISO 27001:2013 "Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos"
Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6 Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas - Guía riesgos 2018	Comprende los lineamientos internacionales para la gestión de datos, que abarcan gobierno, calidad, arquitectura, seguridad, metadatos, interoperabilidad y análisis de información.
Norma ISO 9001: 2105	Norma de gestión de calidad que establece requisitos para asegurar la mejora continua de procesos. En el caso del proceso TIC, incluye los documentos de caracterización, políticas, planes, indicadores y procedimientos asociados. Documentación del proceso: <ul style="list-style-type: none"> • Caracterización • Políticas • Planes • Indicadores

	INFORME DE AUDITORIA	Auditoría no.		35 -25
		Fecha del informe		
		Día	Mes	Año
		20	10	2025


	<ul style="list-style-type: none"> • Procedimientos
Decreto 620 de 2018	“Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado”

Las actividades efectuadas en el desarrollo de la auditoría y sus resultados correspondientes se presentan a continuación, divididas en la estructura de controles y lineamientos establecidos en las normas y buenas prácticas :

Documento	Validación	Enlace
Caracterización del proceso	<p>Se validó la caracterización del proceso SPI-cp-01, con fecha de octubre de 2023 versión 1.</p> <p>Dentro de esta validación se identifica los ítems de la caracterización así: objetivo, alcance, objetivos estratégicos, actividades, responsables y los productos asociados.</p> <p>Los productos de la caracterización serán evaluados desde el punto de vista de las buenas prácticas de la Política de Gobierno Digital en sección posterior.</p>	Caracterización SPI
Política	<p>El proceso de Seguridad y Privacidad de la Información cuenta con dos documentos de Política:</p> <ul style="list-style-type: none"> • Resolución Nacional R2025030612 del 14 julio de 2025 Por medio de la cual se actualiza la Política de Gestión y Desempeño de Seguridad Digital para el Consejo Profesional Nacional de Ingeniería – COPNIA • Resolución Nacional R2025031943 22 julio de 2025 Por medio de la cual se actualiza y modifica la Política de 	Política de Seguridad y Privacidad de la Información Política de Seguridad Digital

	INFORME DE AUDITORIA	Auditoría no.		35 -25
		Fecha del informe		
		Día	Mes	Año
		20	10	2025

	<p>Seguridad y privacidad de la información para el Consejo Profesional Nacional de Ingeniería – COPNIA</p> <p>La Política será evaluada desde el punto de vista de las buenas prácticas de la Política de Gobierno Digital en sección posterior.</p>	
Planes	<p>El proceso cuenta con los siguientes planes:</p> <ul style="list-style-type: none"> • Plan de Seguridad y Privacidad de la Información de enero de 2024 versión 1. • Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de Marzo de 2025 versión 2. 	<p>Plan de Seguridad y Privacidad de la Información</p> <p>Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información</p>
Procedimientos	<p>El proceso cuenta con los siguientes procedimientos:</p> <ul style="list-style-type: none"> • SPI-pr-01 PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN de julio de 2025 versión 1 	<p>SPI-pr-01</p>
Normograma	<p>Se valida que el proceso cuenta con el normograma con fecha septiembre de 2024 Versión 2</p>	<p>Normograma</p>
Listado maestro de documentos externos	<p>Se valida que se cuenta con el documento con fecha abril de 2024 Versión 1 del proceso</p>	<p>Listado maestro de documentos externos</p>

	INFORME DE AUDITORIA	Auditoría no.		35 -25
		Fecha del informe		
		Día	Mes	Año
		20	10	2025


Validación técnica

Posterior a esta actividad se realiza la validación de la documentación base del proceso, se realizó el análisis desde el punto de vistas técnico de la siguiente manera:

- **Diagnóstico de seguridad y privacidad de la información**

Se validó con el Profesional de Gestión del Proceso el instrumentos de Diagnóstico del Modelo de Seguridad y Privacidad de la Información para la Entidad, encontrando que:

Criterio	Pregunta Orientadora	Verificación	Observaciones
Decreto 767 de 2022 Modelo de Seguridad y Privacidad de la Información	Se cuenta con un diagnóstico del Modelo de Seguridad y Privacidad de la Información	SI	Para el diagnóstico, el Profesional de Gestión del proceso aplicó el diagnóstico que para tal fin propone el Ministerio TIC, con fecha de elaboración 01/06/2025
	El diagnóstico cumple con los parámetros definidos	Parcialmente	<p>Se evidenció en el instrumento aplicado que no todos los campos correspondientes a las columnas de brechas, recomendación y evidencias fueron debidamente diligenciados.</p> <p>Esta situación constituye una debilidad, ya que limita la trazabilidad y dificulta la validación de los controles, requiriendo la intervención directa de personal con conocimiento detallado del estado de implementación de cada control.</p> <p>El Profesional de Gestión informó durante la prueba de recorrido que para el próximo diagnóstico se están teniendo en cuenta los ajustes necesarios con el fin de subsanar esta situación y</p>

	INFORME DE AUDITORIA	Auditoría no.		35 -25
		Fecha del informe		
		Día	Mes	Año
		20	10	2025

		<p>asegurar un registro más completo y confiable.</p> <p>Se identifican debilidades en el diagnóstico de seguridad teniendo en cuenta que:</p> <p>Durante la prueba de recorrido de los lineamientos, realizada con el fin de validar la correcta aplicación del instrumento, se identificó una inconsistencia en la calificación del control A.14.2.1 (Política de desarrollo seguro) y del control A.17.1.2 (Continuidad de negocio). La puntuación registrada en el instrumento de diagnóstico no coincide con la información suministrada por el Oficial de Seguridad de la Información, ni con el nivel de madurez (80) determinado por el auditor a partir de la validación cruzada entre el cuestionario aplicado y las evidencias presentadas.</p>
--	--	--

- **Gestión de incidentes de seguridad y privacidad de la información**

Se validó con el Profesional de Gestión del Proceso el procedimiento de Gestión de incidentes de seguridad y privacidad de la información encontrando que:

Criterio	Pregunta Orientadora	Verificación	Observaciones
resolución 500 de 2021	Se cuenta con un procedimiento de gestión de incidentes	SI	Se cuenta con el SPI-pr-01 procedimiento para la gestión de incidentes de seguridad y privacidad de la información que cumple con los lineamientos de la Resolución 500 de 2021

	INFORME DE AUDITORIA	Auditoría no.	35 -25	
		Fecha del informe		
		Día	Mes	Año
		20	10	2025

	El procedimiento cuenta con los requisitos mínimos de las buenas prácticas	SI	Se valida que el procedimiento cuenta con Objetivo y alcance, lineamientos mínimos de respuesta, roles y responsabilidades, etapas del incidente, tipificación, priorización, contactos y formatos consistentes con las necesidades de la entidad y las buenas prácticas.
	Se tienen evidencias de la aplicación del procedimiento	NO	Al solicitar una prueba de recorrido, se informa que el procedimiento tiene fecha de Julio de 2025 por lo cual aún no se ha utilizado para la gestión de incidentes de seguridad

- **Gestión de riesgos de seguridad digital**

Se valida si la entidad cuenta con lineamientos asociados a la gestión de riesgos de seguridad digital así:

Criterio	Pregunta Orientadora	Verificación	Observaciones
Guía para la Administración del Riesgo de la Función Pública anexo 4 de la Guía para la Administración del Riesgo de la	Se cumple con la implementación del Modelo de Gestión de Riesgos de Seguridad Digital definidos en el anexo 4 de la Guía para la Administración del Riesgo de la	SI	Se presenta dentro de la prueba de recorrido el Documento de Contexto interno y externo – Análisis del entorno institucional y digital que impacta la seguridad.

<p>Función Pública denominada Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas</p> <p>Resolución 500 de 2021</p>	<p>Función Pública denominada Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas</p>	SI	Se presenta dentro de la prueba de recorrido definición del alcance de la GRSD – Procesos y áreas donde se aplicará la gestión de riesgos.
		SI	Se cuenta con una Política Institucional de administración del riesgo
		SI	Se valida dentro del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, la política de gestión de riesgos de seguridad digital.
		Parcialmente	<p>Asignación de roles y responsabilidades – Designación del Responsable de Seguridad Digital y definición de las líneas de defensa. (parcialmente), no se identifican las responsabilidades del líder de seguridad, dentro de la prueba de recorrido se presenta n los roles del subcomité, Oficina TIC, Oficina de seguridad) en Resolución R202531943 de julio de 2025</p> <p>Se recomienda que se realiza alineación con la Política de Administración de Riesgo Resolución Nacional 1252 de 2028 y el Procedimiento de administración del riesgo DE-pr-02 de Diciembre 2022 versión 8 en cuanto a las responsabilidades de segunda línea de defensa y la actualización de la gestión del riego ante la Guía para la Gestión Integral de Riesgos en Entidades Públicas - Versión 7 de la Función Pública.</p>

INFORME DE AUDITORIA

Auditoría no.

35 -25

Fecha del informe

Día

Mes

Año


20

10

2025

		SI	Plan de recursos – Identificación y asignación de personal Dentro de la prueba de recorrido se valida Los planes del proceso y asignación de personal
		SI	Dentro de la prueba de recorrido se presenta el Inventario de activos de seguridad Digital – Listado y valoración de aplicaciones, bases de datos, redes, servicios y otros activos críticos.
		SI	Dentro de la prueba de recorrido no se aporta documento de identificación de infraestructuras críticas de la Entidad
		SI	Matriz de riesgos inherentes – Identificación de amenazas, vulnerabilidades y riesgos sobre los activos. Se aporta dentro de la prueba de recorrido y está relacionada con la matriz de riesgos de seguridad digital
		SI	Plan de tratamiento de riesgos – Estrategias para evitar, mitigar, aceptar o transferir riesgos. Dentro de la prueba de recorrido se valida que el Plan de tratamiento de riesgos de Seguridad y Privacidad de la Información contenga la estrategia
		SI	Definición de indicadores de gestión – Métricas para evaluar la eficacia de los planes y controles
		SI	Dentro de la documentación publicada del sistema de gestión de calidad se identifica un Procedimiento formal asociado a la gestión de riesgos de seguridad de
	Se cuenta con Procedimiento de gestión de riesgos de seguridad de la información		

			la información que hace parte del proceso de Direccionamiento Estratégico, DEpr-02 Administración del riesgo.
		SI	Se presenta dentro de las evidencias y se realiza prueba de recorrido
		SI	1. Ser aprobada a través de un acto administrativo de carácter general. Se aprueba por el Director de la Entidad
		SI	2. Contar con un análisis y tratamiento de riesgos de seguridad digital e implementar controles que permitan gestionarlos. Se identifica dentro de la validación que cuenta con análisis y tratamiento de riesgos
	Se cuenta con una matriz de gestión de riesgos de seguridad	SI	3. Establecer los roles y responsabilidades al interior de la entidad asociados a la seguridad digital. Dentro de la prueba de recorrido esto se valida en: <ul style="list-style-type: none"> Resolución Nacional No. 1252 Política de Administración de Riesgo: Líneas de Defensa Resolución Nacional No. R2025030612 Política de Gestión y Desempeño de Seguridad Digital: Subcomité de Seguridad de la Información Resolución Nacional No. R2025031943 Política de Gestión y Desempeño de Seguridad y Privacidad de la Información: niveles de responsabilidad

	INFORME DE AUDITORIA	Auditoría no.	35 -25	
		Fecha del informe		
		Día	Mes	Año
		20	10	2025

		SI	<p>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.</p>
--	--	----	--

- **Inventario de activos de información**

Se valida el alineamiento de contar con un inventario de clasificación de activos e infraestructura crítica de acuerdo con el MSP en la sección 11.3 Guía - Gestión inventario clasificación de activos e infraestructura crítica así:

Criterio	Pregunta Orientadora	Verificación	Observaciones
Decreto 767 de 2022 Modelo de Seguridad y Privacidad de la Información	Se cuenta con un inventario de activos de información relacionado con seguridad de la información e infraestructuras críticas	SI	<p>En la prueba de recorrido, la Profesional de Gestión Oficina de Seguridad y Privacidad de la Información informa que la entidad cuenta con activos clasificados en: bienes físicos, documentales y tecnológicos.</p> <p>Adicionalmente explica el proceso de identificación, plaquetización y actualización de activos y destaca la importancia de integrar todos los activos en una sola matriz consolidada, tal como se presenta.</p>

Las recomendaciones para este lineamiento son:

- Incluir explícitamente referencias normativas en la matriz del inventario de activos (ejemplo Ley 1712 de 2042, Ley 1581 de 2012, etc.)
- Evaluar, de acuerdo con la realidad de la Entidad, la existencia un campo en la matriz que caracterice si el activo contiene datos de niños, niñas y adolescentes.

	INFORME DE AUDITORIA	Auditoría no.	35 -25	
		Fecha del informe		
		Día	Mes	Año
		20	10	2025


- Integrar en la matriz los activos de información de acuerdo con el lineamiento, la tipificación: Información; Software; Hardware; servicios; personas.
- Actualizar los lineamientos de acuerdo con la última versión del Modelo de Seguridad y Privacidad de la Información para la Vigencia 2025.

- **Matriz de riesgos**

Para la validación se revisa el cumplimiento del Modelo de Seguridad y Privacidad de la Información lineamiento 7.3.2 Valoración de los riesgos de seguridad de la información

Criterio	Pregunta Orientadora	Verificación	Observaciones
Decreto 767 de 2022 Modelo de Seguridad y Privacidad de la Información	Se cuenta con una matriz de riesgos de seguridad de la información	SI	<p>En la prueba de recorrido se identificó que, actualmente, la matriz incluye diferentes tipos de activos (activos digitales, recursos humanos, bases de datos, etc.)</p> <p>Por otro lado se identifica que la criticidad de activos se valora según confidencialidad, integridad y disponibilidad y se incorporan los activos de criticidad alta.</p> <p>También se identifica que:</p> <p>Se sugiere considerar activos con valoración media y alta en la matriz de riesgos, conforme lo definido por el Modelo Nacional de Gestión de Riesgos.</p> <p>Se identifica la necesidad de generar actas o registros de socialización y acompañamiento a los líderes de proceso para fortalecer la apropiación, así como la identificación y ejecución de controles.</p>

	Identificar los riesgos que causen la pérdida de confidencialidad, integridad, disponibilidad, privacidad de la información, así como la continuidad de la operación de la Entidad dentro del alcance del MSPI.	SI	Dentro de la prueba de recorrido se identifica que la matriz de riesgos considera la confidencialidad, integridad, disponibilidad, privacidad de la información.
	Identificar los dueños de los riesgos.	SI	Dentro de la prueba de recorrido se identifica que la matriz de riesgos tiene un alcance relacionado con los activos de seguridad digitales y no de los riesgos de seguridad de la información
	Definir criterios para valorar las consecuencias de la materialización de los riesgos, y la probabilidad de su ocurrencia.	SI	Dentro de la prueba de recorrido se identifica que la matriz de riesgos tiene un alcance relacionado con los activos de seguridad digitales y no de los riesgos de seguridad de la información
	Determinar el apetito de riesgos definido por la Entidad	SI	Dentro de la prueba de recorrido se identifica que la matriz de riesgos contiene columnas relacionadas con el ítem.

	INFORME DE AUDITORIA	Auditoría no.	35 -25	
		Fecha del informe		
		Día	Mes	Año
		20	10	2025

	Aplicar el proceso de valoración del riesgo que permita determinar los riesgos asociados a la pérdida de confidencialidad, integridad y disponibilidad de la información que se encuentre dentro del alcance.	SI	Dentro de la prueba de recorrido se identifica que la matriz de riesgos contiene columnas relacionadas con el ítem.
	Determinar los niveles de riesgo.	SI	Dentro de la prueba de recorrido se identifica que la matriz de riesgos contiene columnas relacionadas con el ítem.
	Realizar la comparación entre los resultados del análisis y los criterios de los riesgos establecidos en este mismo numeral.	SI	Dentro de la prueba de recorrido se identifica que la matriz de riesgos contiene columnas relacionadas con el ítem.
	Priorización de los riesgos analizados para su tratamiento.	SI	Dentro de la prueba de recorrido se identifica que la matriz de riesgos contiene columnas relacionadas con el ítem.

Se identifica que:

- Se debe considerar activos con valoración media y alta en la matriz de riesgos, conforme al Modelo Nacional de Gestión de Riesgos.
- Se identificó la necesidad de generar actas o registros de socialización y acompañamiento a los líderes de proceso para fortalecer la apropiación, así como la identificación y ejecución de controles.
- **Actualización documental del proceso**

Se valida que la información asociada al proceso de Seguridad y Privacidad de la Información sea actualizada periódicamente, así:

Criterio	Pregunta Orientadora	Verificación	Observaciones
----------	----------------------	--------------	---------------

<p>ISO 217001:2015 7.5.3 Control de la información documentada</p>	<p>Se valida la actualización de los documentos asociados al proceso</p>	<p>Parcialmente</p>	<p>Dentro de la validación de los documentos se encuentra que : En el documento Normograma del proceso con fecha septiembre de 2024 versión 2 no se identifican las normas:</p> <p>Resolución 2277 de 2025, actualización del a Resolución 500 de 2021</p> <p>Decreto 767 de 2022 Actualización de la Política de Gobierno Digital, en lo correspondiente a seguridad de la Información</p> <p>Se informa de parte del profesional de Gestión del proceso que este documento está en proceso de aprobación</p>
--	--	---------------------	--

INFORME DE AUDITORIA

Auditoría no.

35 -25

Fecha del informe

Día

Mes

Año

20

10

2025

		<p>Parcialmente</p>	<p>En el documento Listado maestro de documentos externos con fecha abril de 2024 no se identifica la actualización de los siguientes documentos:</p> <p>No se encuentra dentro del listado de Documentos externos:</p> <p>Modelo de seguridad y Privacidad de la Información versión 5</p> <p>Guía para la Gestión Integral de Riesgos en Entidades Públicas - versión 7</p> <p>Documento Maestro del Marco de Referencia de Arquitectura Empresarial - versión 1</p> <p>Autodiagnóstico MSPI 2025</p>
		<p>SI</p>	<p>Se informa en las sesiones de auditoría que la actualización del inventario de activos debe realizarse al menos una vez al año o cuando existan cambios normativos, tecnológicos u organizacionales.</p>
		<p>Parcialmente</p>	<p>Se valida actualización de la Política de Seguridad y privacidad de la información con Resolución Nacional R2025031943 del 22 julio de 2025.</p> <p>En esta no se hace referencia en el considerando a:</p> <p>Conpes 3995 Política Nacional De Confianza y Seguridad Digital</p>

INFORME DE AUDITORIA

Auditoría no.

35 -25

Fecha del informe

Día

Mes

Año

20

10

2025

		Resolución 500 del 10/03/2021 y su actualización: Resolución 2277 de 2025
	Parcialmente	Se valida actualización de la Política de Seguridad Digital con Resolución Nacional R2025030612 del 14 julio de 2025 En esta no se hace referencia en el considerando a: Conpes 3995 Política Nacional de Confianza y Seguridad Digital Resolución 500 del 10/03/2021 y su actualización: Resolución 2277 de 2025
	SI	Se valida formalización del procedimiento SPI-pr-01 Procedimiento para la gestión de incidentes de seguridad y privacidad de la información
	NO	Se valida la actualización del documento Plan de Seguridad y Privacidad de la Información publicado en la página web de la Entidad, con fecha de enero de 2024 versión 1, de acuerdo con el Decreto 612 de 2018, se identifica que este documento no fue actualizado para la vigencia 2025
	SI	Se valida la actualización del documento Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información publicado en la página web de la Entidad, con fecha de Marzo de 2025 versión 2, de acuerdo con el Decreto 612 de 2018, se identifica que este documento si fue actualizado para la vigencia 2025

	INFORME DE AUDITORIA	Auditoría no.		35 -25
		Fecha del informe		
		Día	Mes	Año
		20	10	2025

		NO	Se valida si el documento Plan de Seguridad y Privacidad de la Información publicado en la página web de la Entidad, con fecha de enero de 2024 versión 1, cuenta con indicadores, no se evidencia que esta situación
		SI	Se valida si el documento Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información publicado en la página web de la Entidad, con fecha de Marzo de 2025 versión 2, cuenta con indicadores, no se evidencia que esta situación

De esta manera, Se identifican debilidades en la actualización de documentos del proceso de Seguridad y Privacidad de la información en los documentos:

- Política de Seguridad Digital
- Política de Seguridad y Privacidad de la Información
- Plan de Seguridad y Privacidad de la Información
- Normograma
- Listado de Documentos externos

Se recomienda realizar la actualización del proceso SDI a la última versión del MSPI teniendo presente que el MinTIC ha alineado el documento con la versión 2022 de la ISO 27001 en junio de 2025 de acuerdo con la 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" en la cual se actualiza el MSPI a su versión 5 y así como sus guías relacionadas.

- Procedimientos relacionados con Seguridad y Privacidad de la Información

Se valida dentro de la página web, sección mapa de procesos, los procedimientos asociados y se validan con el Modelo de Seguridad y Privacidad de la Información, así:

Criterio	Pregunta Orientadora	Verificación	Observaciones
----------	----------------------	--------------	---------------

<p>ISO 217001:2015 7.5.3 Control de la información documentada</p> <p>Decreto 767 Modelo de Seguridad y Privacidad de la Información</p>	<p>Se cuenta con los siguientes procedimientos relacionados con la seguridad y privacidad de la información</p>	NO	<p>A.8.2.2 Etiquetado de la información</p> <p>Control: Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización</p>
		SI	<p>A.14.2.2 Procedimientos de control de cambios en sistemas</p> <p>Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambio</p>
		SI	<p>A.16.1.1 Responsabilidad y procedimientos</p> <p>Control: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información</p>
		SI	<p>Procedimiento de inventario y Clasificación de la Información e infraestructura críticas</p>
		SI	<p>Procedimiento de gestión de riesgos de seguridad de la información</p>


5. HALLAZGOS

Para el desarrollo de la auditoria se aplicó un total 53 criterios, de los cuales, 0 son no conformidad y 5 son conformidad con observación; dando como resultado del ejercicio auditor un cumplimiento del 100% frente a los criterios de auditoría evaluados.

	INFORME DE AUDITORIA	Auditoría no.	35 -25	
		Fecha del informe		
		Día	Mes	Año
		20	10	2025

5.1. REQUISITOS CON CUMPLIMIENTO – CONFORMIDADES CON OBSERVACION


Criterio	Evidencia
<p>Decreto 767 de 2022 Modelo de Seguridad y Privacidad de la Información 06. Diagnóstico Lineamiento: Identificar a través de la herramienta de autodiagnóstico (Análisis GAP) el estado actual de la Entidad respecto a la Seguridad y privacidad de la Información.</p>	<p>Se evidencian debilidades en la aplicación del instrumento de autoevaluación del MSPI en cuanto a que:</p> <p>En el diligenciamiento no todos los campos correspondientes a las columnas de brechas, recomendación y evidencias fueron debidamente diligenciados.</p> <p>Esta situación constituye una debilidad, ya que limita la trazabilidad y dificulta la validación de los controles, requiriendo la intervención directa de personal con conocimiento detallado del estado de implementación de cada control.</p> <p>Adicionalmente, se identificó una inconsistencia en la calificación del control A.14.2.1 (Política de desarrollo seguro) y del control A.17.1.2 (Continuidad de negocio). La puntuación registrada en el instrumento de diagnóstico no coincide con la información suministrada por el Oficial de Seguridad de la Información, ni con el nivel de madurez (80) determinado por el auditor a partir de la validación cruzada entre el cuestionario aplicado y las evidencias presentadas.</p>
<p>Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6 de la Guía para la Administración del Riesgo de la Función Pública denominada Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas</p> <p>Resolución 500 de 2021 Asignación de roles y responsabilidades – Designación del Responsable de Seguridad Digital y</p>	<p>Se presentan debilidades en la alineación de las funciones de la seguridad y privacidad de la información debido a contar con varias fuentes de información que incluyen:</p> <ul style="list-style-type: none"> • Resolución Nacional 1252 de 2028 - Política de Administración de Riesgo • DE-pr-02 Procedimiento de administración del riesgo de Diciembre 2022 versión 8 • RESOLUCIÓN NACIONAL R2025031943 del 22 julio de 2025. Política de Seguridad y privacidad de la información • RESOLUCIÓN NACIONAL R2025030612 del 14 julio de 2025 Política de Seguridad Digital <p>En cuanto a las responsabilidades de segunda línea de defensa en lo concerniente a la labor del profesional de Gestión de Seguridad y Privacidad de la Información de</p>

	INFORME DE AUDITORIA	Auditoría no.	35 -25	
		Fecha del informe		
		Día	Mes	Año
		20	10	2025

definición de las líneas de defensa	acuerdo con lo contemplado en la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas Versión 6 de la Función Pública.
ISO 27001:2013 Control 5.1.2 Revisión de las políticas para seguridad de la información. 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.	<p>Se evidencia que en la Resolución Nacional R2025030612 del 14 julio de 2025 "Por medio de la cual se actualiza la Política de Gestión y Desempeño de Seguridad Digital para el Consejo Profesional Nacional de Ingeniería – COPNIA" y la RESOLUCIÓN NACIONAL R2025031943 del 22 julio de 2025 "Por medio de la cual se actualiza y modifica la Política de Seguridad y privacidad de la información para el Consejo Profesional Nacional de Ingeniería – COPNIA" no se hace referencia en el considerando a:</p> <p>Conpes 3995 POLÍTICA NACIONAL DE CONFIANZA Y SEGURIDAD DIGITAL</p> <p>Resolución 500 del 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 su actualización: Resolución 2277 de 2025 "Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia"</p>
ISO 9001:2015 7.5.3 Control de la información documentada Decreto 612 de 2018	<p>Se identifican debilidades en la actualización de documentos del proceso de Seguridad y Privacidad de la información en los documentos:</p> <ul style="list-style-type: none"> • Plan de Seguridad y Privacidad de la Información • Normograma • Listado de Documentos externos
Decreto 767 de 2022 Modelo de Seguridad y Privacidad de la Información ISO 9001:2015 9.1 Seguimiento, medición, análisis y evaluación	Debilidades en el Plan de Seguridad y Privacidad de la Información publicado en la página web de la Entidad, con fecha de enero de 2024 versión 1, debido a que no cuenta con indicadores definidos para su seguimiento y control

5.2. REQUISITO DE NO CUMPLIMIENTO – NO CONFORMIDADES

No se presentan requisitos de no cumplimiento para el presente informe de auditoría.

	INFORME DE AUDITORIA	Auditoría no.	35 -25	
		Fecha del informe		
		Día	Mes	Año
		20	10	2025

6. EVALUACIÓN DEL RIESGO DEL PROCESO

De acuerdo con el Mapa de riesgos de seguridad digital versión 2 de febrero de 2024 del proceso, se establecen 7 riesgos:

Una vez validada la matriz de riesgo se encuentra lo siguiente:

1. Controles poco diversificados

- La mayoría de los controles se repiten en torno a backup, roll back, logs de auditoría, y asignación de roles/perfiles.
- No se observan controles más avanzados como:
 - Segmentación de red.
 - Doble factor de autenticación (MFA).
 - Monitoreo en tiempo real (SIEM).
 - Pruebas de penetración o auditorías técnicas.

Esto genera una dependencia excesiva en copias de seguridad y en medidas reactivas.

2. Enfoque reactivo más que preventivo

- Varias medidas son “restaurar backup” o “realizar roll back”, que actúan después de que ocurre el incidente, no antes.
- Controles preventivos como endurecimiento de configuraciones, control de parches, o gestión de accesos privilegiados son tratados de manera superficial.


3. Falta de controles sobre terceros

- En riesgos donde participan contratistas o agentes externos, el control se limita a cláusulas de confidencialidad.
- No se evidencian:
 - Auditorías a proveedores.
 - Aseguramiento de SLA en ciberseguridad.
 - Validación de cumplimiento de normativa por terceros.

3. Ausencia de indicadores de eficacia

- Se mencionan capacitaciones, logs o planes de backup, pero no hay métricas que permitan medir si los controles son eficaces (ej. porcentaje de pruebas de restauración exitosas, número de accesos fallidos detectados).

5. Riesgo residual poco detallado

	INFORME DE AUDITORIA	Auditoría no.		35 -25
		Fecha del informe		
		Día	Mes	Año
		20	10	2025

- Aunque aparece la columna de riesgo residual, la mayoría queda en niveles similares al inicial, lo que evidencia que se deben fortalecer los controles definidos.

6. Cobertura limitada de amenazas modernas

- Se cubren riesgos tradicionales (errores de configuración, pérdida de equipos, fallas de software), pero faltan amenazas actuales:
 - Ransomware y malware avanzado.
 - Phishing y ataques de ingeniería social.
 - Fugas de información en la nube.
 - Riesgos por inteligencia artificial o deepfakes.

7. Responsabilidades genéricas

- El propietario del riesgo casi siempre es “Profesional de gestión del Área TIC” junto con Seguridad y Privacidad.
- Aunque se evidencia el responsable general como líder del proceso, debe haber internamente una asignación clara a responsables específicos (ej. administrador de red, DBA, responsable de continuidad), así como un seguimiento a su implementación.

Recomendaciones de mejora


- Incluir controles proactivos: MFA, DLP, SIEM, segmentación de red, pruebas de seguridad periódicas.
- Detallar controles de terceros: auditorías a proveedores, cláusulas específicas de ciberseguridad.
- Incorporar indicadores de eficacia de controles (KRI/KPI).
- Reforzar la gestión del riesgo residual con fortalecimiento de ellos riesgos definidos
- Ampliar el espectro de amenazas: ransomware, phishing, riesgos en la nube.
- Ajustar la asignación de responsabilidades a roles más específicos.

Se adjunta el detalle del análisis de la Matriz de Riesgos del proceso en el Anexo 1. Análisis matriz de Riesgo SDI.

7. CONCLUSIONES Y RECOMENDACIONES

Se evidencia que el proceso, a poco tiempo de crearse, logra un cumplimiento importante de los criterios de evaluación de esta auditoría, cifra significativa para el poco tiempo de creado y con una sola persona trabajando en el proceso.

La implementación de un Sistema de Gestión de Seguridad de la Información debe lograr comprometer a toda la Entidad en el cumplimiento de las Políticas de seguridad de la Entidad y permitir alinear los diversos procesos y normatividad aplicable al Copnia.

	INFORME DE AUDITORIA	Auditoría no.		35 -25
		Fecha del informe		
		Día	Mes	Año
		20	10	2025

Luego de la realización del proceso auditor es importante tener presente las siguientes recomendaciones:

- Realizar seguimiento a la implementación del SPI-M-01 Manual de seguridad de la información de parte de los responsables.
- Se sugiere planear e implementar un calendario de revisiones semestrales de la normatividad y buenas prácticas para garantizar el cumplimiento continuo.
- Se recomienda diligenciar adecuadamente el documento de Diagnóstico del MSPI para evitar confusión y garantizar que se cumplan adecuadamente los requisitos de seguridad.
- Continuar con la adopción de la norma ISO 27001:2022 para alinearse con la actualización de buenas prácticas.
- Realizar la actualización periódica de las bases de datos inscripción de la base de datos en el Registro Nacional de Bases de Datos RNBD.

8. SEGUIMIENTO A PLANES DE MEJORAMIENTO

Durante la auditoría al proceso de Seguridad y Privacidad de la Información SDI, se evaluó el Plan de Mejoramiento de acuerdo con el aporte de evidencias así:

Código NC	Descripción	Evaluación de eficacia	Eficaz/No eficaz
1-3524-1	1. Elaborar un procedimiento de clasificación y gestión unificada de activos, donde se integre el inventario de activos de información. Plazo de cumplimiento: 1/12/2025	Se presenta como evidencia los documentos: Resolución Nacional RN2025NALA004772 del 8 de octubre de 2025 "Por medio de la cual se adopta el documento SPI-pr-02 Procedimiento para la Gestión de Activos de Información"	Eficaz
2-3524-1	Incorporar en el procedimiento para la gestión de activos de información los lineamientos para el esquema formal del etiquetado	Se presenta como evidencia los documentos: Resolución Nacional RN2025NALA004772 del 8 de octubre de 2025 "Por medio de la cual se adopta el documento SPI-pr-02 Procedimiento para la Gestión de Activos de Información"	Eficaz

	Plazo de cumplimiento: 1/12/2025		
3- 3524-1	<p>Documentar e implementar los procedimientos necesarios para dar cumplimiento al Modelo de Seguridad y Privacidad de la Información</p> <p>Plazo de cumplimiento: 1/12/2025</p>	<p>1.Procedimiento de gestión de activos de información</p> <p>Evidencia: Resolución Nacional RN2025NALA004772 del 8 de octubre de 2025 "Por medio de la cual se adopta el documento SPI-pr-02 Procedimiento para la Gestión de Activos de Información" versión 1.</p> <p>2.Procedimiento de Gestión de incidentes de seguridad de la información</p> <p>Evidencia: SPI-pr-01 Procedimiento para la gestión de incidentes de seguridad y privacidad de la información Vigente a partir de julio de 2025 versión 1.</p>	Eficaz
4- 3524-1	<p>1. Actualizar el registro nacional de base de datos en el Registro Nacional de Bases de Datos, según las nuevas implementaciones tecnológicas.</p> <p>Plazo de cumplimiento: 1/12/2025</p>	<p>Evidencia: RN2025NALA004772.pdf, COPNIA registro BD copnia.pdf, GESTOR DOCUMENTAL.pdf, KACTUS.pdf, KACTUS.pdf que soportan el registro de las bases de datos:</p> <ul style="list-style-type: none"> • Gestor documental • Kactus • Seven 	Eficaz

	INFORME DE AUDITORIA	Auditoría no.		35 -25
		Fecha del informe		
		Día	Mes	Año
		20	10	2025

10. ANEXOS

Anexo 1. Análisis matriz de Riesgo SDI.

Activo	Riesgo identificado	Amenaza X vulnerabilidad	Control asociado	Debilidad	Recomendación
BPM; MICROSITIO; GESTOR DOCUMENTAL; PQRS; OFFICE 365; PAGINA WEB; CATEDRA DE ETICA; SEVEN; KACTUS; PLATAFORMA DE PAGOS; INVESDOC	Perdida de confidencialidad	Incorrecta parametrización de permisos sobre la información X Incorrecta administración de la plataforma	Logs de auditoría, asignación de roles y perfiles	No hay segregación de funciones ni MFA en accesos privilegiados	Implementar MFA, segregación de funciones, monitoreo de accesos privilegiados
		Mal funcionamiento del software por ejecución incorrecta de cambios	Realización de etapa de pruebas.	Control reactivo, no hay gestión preventiva de parches	Implementar gestión de parches automatizada, ambientes de pruebas segregados
		Incorrecta utilización de la plataforma X desconocimiento del funcionario	Capacitación a funcionarios	Capacitación puntual, no continua ni medible	Programar capacitaciones periódicas, simulacros de incidentes, campañas de simulacros de phishing

		Acceso, manipulación o divulgación de información X funcionario/tercero por Intereses particulares o presión por parte de un tercero.	Cláusula de confidencialidad de la información, funciones del personal, restricción de acceso a terceros según manual de seguridad	Controles contractuales débiles, sin auditorías a terceros	Implementar SIEM, monitoreo de accesos, auditorías a proveedores Matriz de aplicabilidad
Componentes de red	Perdida de confidencialidad	Manipulación de configuraciones por administrador de red, funcionario o contratista X Incorrecto o mal intencionado manejo de las configuraciones de red	Logs de auditoría de las consolas de administración Asignación de roles y perfiles.	No se contemplan cambios maliciosos ni validación independiente	Implementar control dual, gestión de cambios con revisión independiente
		Mal funcionamiento parche de actualización por Error de despliegue de actualización en control de cambios.	Se genera cronograma de la ventana con backup y roll back	Control reactivo, falta de pruebas de parches antes del despliegue	Pruebas de regresión, sandbox para validación, gestión de parches automatizada
		Agente externo o tercero que manipule la información X Intereses particulares o presión por parte de un tercero.	Se genera línea base sobre los equipos de red y seguridad.	No hay monitoreo activo ni IDS/IPS	Implementar IDS/IPS, firewall de nueva generación, SIEM

INFORME DE AUDITORIA

Auditoría no.

35 -25

Fecha del informe

Día

Mes

Año

20

10

2025

Equipos de cómputo	Perdida de confidencialidad	<p>Acceso no autorizado al equipo de cómputo X Contraseña visible, predecible o realizar la Conexión a redes, paginas o programas no seguros</p>	<p>Asignación de usuario por directorio activo y controles de complejidad y caducidad de contraseñas Línea base de antivirus</p>	<p>No se incluyen MFA, MDM ni cifrado</p>	<p>Cifrado de disco, MFA, soluciones MDM</p>
		<p>Pérdida o robo del equipo de cómputo X Acceso a la información por parte de un tercero</p>	<p>Manual de seguridad de la información donde se implementa usuarios estándar y no administradores, activación e inactivación de usuarios por directorio activo</p>	<p>Sin controles de cifrado ni borrado remoto</p>	<p>Cifrado completo de disco, borrado remoto, MDM</p>
	<p>BPM; MICROSITIO; GESTOR DOCUMENTAL; PQRS; OFFICE 365; PAGINA WEB; CATEDRA DE ETICA; SEVEN; KACTUS; PLATAFORMA DE PAGOS; INVESDOC</p>	<p>Pérdida de Integridad</p>	<p>Incorrecta administración sobre la información X Ejecutar de forma incorrecta un query o alguna acción que modifique o elimine la información</p>	<p>Logs de auditoría de las consolas de administración Asignación de roles y perfiles. Planes de backup sobre las bases de datos</p>	<p>Sin pruebas periódicas de recuperación y monitoreo SQL</p>

INFORME DE AUDITORIA

Auditoría no.

35 -25

Fecha del informe

Día

Mes

Año

20

10

2025

	<p>Falla en funcionamiento del software o hardware Error o intermitencia de hardware o software que genere X perdida de datos o daño en los existentes</p>	<p>Generación de plan de backup y contratos de mantenimiento y soporte sobre las plataformas tecnológicas</p>	<p>No se mencionan pruebas periódicas de restauración ni redundancia</p>	<p>Implementar redundancia (clústeres, RAID), pruebas de restauración periódicas</p>
	<p>Incorrecta utilización de la plataforma tecnológica X Acción por parte de un funcionario sobre la plataforma que modifique o elimine datos</p>	<p>Capacitación a funcionarios. Plan de backup sobre las bases de datos</p>	<p>Controles centrados en recuperación, no prevención</p>	<p>Entrenamiento continuo, pruebas de restauración, simulacros de ciberataques</p>

		<p>Eliminación o modificación de la información por parte de un funcionario, contratista o tercero X Agente externo que logre acceder a la información o ejerza presión sobre alguien que pertenezca a la entidad y elimine o modifique la información</p>	<p>Generación de plan de backup y contratos de mantenimiento y soporte sobre las plataformas tecnológicas Cláusula de confidencialidad de la información, funciones del personal, restricción de acceso a terceros según manual de seguridad</p>	<p>Medidas centradas en recuperación; no hay DLP</p>	<p>Implementar DLP, SIEM, monitoreo de accesos</p>
Componentes de red	Pérdida de integridad	<p>Modificación o eliminación de configuraciones por administrador de red, funcionario o contratista X Realizar cambios en las configuraciones de seguridad de la red de la entidad</p>	<p>Logs de auditoría de las consolas de administración Asignación de roles y perfiles. Back up sobre las línea base</p>	<p>No hay controles de validación independiente</p>	<p>Implementar control dual, auditorías técnicas, gestión de cambios formal</p>
		<p>Mal funcionamiento parche de actualización por Generar por medio de actualización la</p>	<p>Backup sobre línea base</p>	<p>Ausencia de pruebas de seguridad previas</p>	<p>Establecer pruebas previas en ambiente controlado, automatizar regresiones</p>

		<p>perdida de configuraciones en la seguridad de la red de la entidad</p>			
		<p>Agente externo o tercero que modifique o elimine la información X Realizar cambios mal intencionados o no autorizados en las configuraciones de seguridad de la red de la entidad</p>	<p>Generación de plan de backup y contratos de mantenimiento y soporte sobre la infraestructura tecnológica Cláusula de confidencialidad de la información, funciones del personal, restricción de acceso a terceros según manual de seguridad</p>	<p>Controles reactivos; falta de IDS/IPS</p>	<p>Implementar SIEM, IDS/IPS, segmentación de red</p>
<p>BPM; MICROSITIO; GESTOR DOCUMENTAL; PQRS; OFFICE 365; PAGINA WEB; CATEDRA DE ETICA; SEVEN; KACTUS; PLATAFORMA DE PAGOS; INVESDOC</p>	<p>Pérdida de disponibilidad</p>	<p>Incorrecta administración sobre la información por un usuario con privilegios en el sistema. X Generar por acciones técnicas incorrectas Indisponibilidad de la plataforma</p>	<p>Contratos con disponibilidad de la plataforma de 99.9% Logs de auditoría de las consolas de administración Asignación de roles y perfiles.</p>	<p>Dependencia en contratos, falta de control técnico</p>	<p>Implementar PAM (Privileged Access Management), auditorías de cuentas privilegiadas</p>

INFORME DE AUDITORIA

Auditoría no.

35 -25

Fecha del informe

Día

Mes

Año

20

10

2025

		Falla en funcionamiento del software o hardware por Falla que genere Indisponibilidad de la plataforma tecnológica de la entidad.	Contratos con disponibilidad de la plataforma de 99.9%	Se limita a SLA contractual, sin pruebas de contingencia	Implementar monitoreo de disponibilidad, redundancia, pruebas de DRP
		Agente externo o tercero que afecte el servicio X Generar por acciones técnicas incorrectas o mal intencionadas Indisponibilidad de la plataforma tecnológica de la entidad	Contratos con disponibilidad de la plataforma de 99.9% Logs de auditoría de las consolas de administración Asignación de roles y perfiles.	No hay controles técnicos específicos	Implementar firewalls de nueva generación, SOC, simulacros de ataque
COMPONENTES DE RED	Pérdida de disponibilidad	Incorrecta administración de red, por funcionario o contratista X Generar por acciones técnicas incorrectas Indisponibilidad de la plataforma tecnológica de la entidad.	Contratos de soporte y mantenimiento, logs de administración	Falta de monitoreo en tiempo real y segregación de cambios	Implementar monitoreo activo, SIEM, controles de cambio dual



INFORME DE AUDITORIA

Auditoría no.

35 -25

Fecha del informe

Día

Mes

Año

20

10

2025

	<p>Falla en funcionamiento del software o hardware X Falla que genere Disponibilidad de la plataforma tecnológica de la entidad.</p>	<p>Contratos de soporte y mantenimiento sobre la infraestructura de red para la ejecución de ventanas de mantenimiento</p>	<p>Faltan validaciones de integridad de datos y controles transaccionales</p>	<p>Implementar validaciones automáticas, blockchain/hash de integridad, monitoreo</p>
	<p>Agente externo o tercero que afecte el servicio X Generar por acciones técnicas incorrectas o mal intencionadas Disponibilidad de la plataforma tecnológica de la entidad.</p>	<p>Contratos de soporte y mantenimiento sobre la infraestructura de red Logs de auditoría de las consolas de administración Asignación de roles y perfiles.</p>	<p>No se mencionan cifrado o DLP</p>	<p>Implementar cifrado, DLP, monitoreo de nube</p>

Elaborado por: Raúl Alberto Ruiz García – Contratista Oficina de Control Interno

Revisado por: Alberto Castiblanco Bedoya – Jefe Oficina de Control Interno