FECHA DE EMISIÓN DEL INFORME	**Día:**	31	**Mes:**	07	**Año:**	2025

Dependencia y/o /Proceso	OFICINA ASESORA DE PLANEACION Y SISTEMAS / Gestión de Servicios de Tecnologías de la Información.
Nombre(s) y cargo:	ANGELICA MARIA ZAMORA ACOSTA; jefe Oficina Asesora De Planeación y Sistemas. / Ing. Luis Edwin Osorio.
Tipo de Auditoria:	Evaluación, Gestión y prevención de Riesgos. Seguimiento de Ley
Objetivo(s) de la Auditoria:	Evaluar la efectividad en la implementación del modelo de seguridad y privacidad de la información en la SES, regulado principalmente, en el Decreto 1078 de 2015 respecto a la estrategia de Gobierno Digital, derivando la obligación en la implementación del Modelo
Alcance de la Auditoría:	• Verificar la existencia, socialización, implementación y monitoreos de los controles definidos previamente para el cumplimiento de la política de seguridad y privacidad de la información, por cada una de las políticas complementarias que contiene el documento fuente de la SES PO-GETI-003. • Verificar la realización de las actividades programadas durante el primer semestre del año 2025 y su impacto en cada uno de los objetivos propuestos en el plan de actividades en materia de seguridad y privacidad de la información MSPI, aprobado por el respectivo comité el presente año. • Verificar el documento Modelo de Seguridad y Privacidad de la Información de la SES, implementado en la entidad, cuyos objetivos y metas fueron establecidos y son la fuente de definición de los respectivos indicadores de dicho modelo, conforme lo regula la guía del MINTIC. • Determinar cuál es el estado actual de los indicadores de Gestión de Seguridad de la Información o en su defecto, la existencia de evidencias que indican avances en los mismos, específicamente los cuales registraban evidente retraso en el Dx y, por tanto, tienen proyectado aumentar el porcentaje de implementación durante el año, del 10% en promedio. • Evaluar el procedimiento para la recolección de información asociada a los indicadores del PSI (presentados en comité de seguridad y privacidad de la información) y las herramientas empleadas para obtener dicha información.
Criterios de la Auditoría:	• Documentos publicados MINTIC: Documento maestro; Gestión de incidentes, Gestión de inventarios, Indicadores Críticos PSPI, Modelo Nacional de Gestión del Riesgo de la Seguridad de la Información, Roles y Responsabilidades • Ley 1581 de 2012. Por la cual se dictan disposiciones

	generales para la protección de datos personales. • Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012. • Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. • Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones. • Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. • Decreto 1083 de 2015 establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital". • CONPES 3854 de 2016. Política Nacional de Seguridad digital. • Decreto 1008 del 2018. 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. • Decreto 612 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. • Decreto 2106 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones. • Ley 1952 de 2019. Por medio de la cual se expide el código general disciplinario

Reunión de Apertura			Ejecución de la Auditoría								Reunión de Cierre		
Día	**Mes**	**Año**	**Desde**	**Día**	**Mes**	**Año**	**Hasta**	**Día**	**Mes**	**Año**	**Día**	**Mes**	**Año**
07	07	2025		07	07	2025		30	07	2025	30	07	2025

Jefe oficina de Control Interno	Auditor(es)
JORGE HERNANDO PEDRAZA VARGAS	**MARTHA ROCIO YANQUEN PARRA**

1. COMPROMISO ETICO EN EL EJERCICIO DE LA AUDITORIA INTERNA

i. Código de Ética del Auditor Interno que tiene como bases fundamentales, la integridad, objetividad, confidencialidad, conflictos de interés y competencia de esté.

ii. 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

Mediante carta de representación de 07 de julio de 2025, suscrita por Ing. Angelica Zamora como jefe o líder de la Oficina Asesora de Planeación y Sistemas, ha declarado su responsabilidad en la oportuna preparación, presentación integral y consistencia de la información que fue entregada en el marco de la auditoría a la unidad de control interno.

3. METODOLOGÍA

Teniendo en cuenta el objetivo(s) y alcance de la auditoria(s), mencionados anteriormente, se desarrollaron de manera previa o posterior, respectivamente, las siguientes actividades:

a) Conocimiento del proceso o dependencia.

b) Diseño del plan de auditoría: Se estableció la programación del plan de trabajo para el desarrollo de la auditoría, de modo que permitiera lograr el objetivo propuesto.

c) Reunión de apertura: la apertura de la auditoría se realizó el 07 de julio de 2025 donde se describió la metodología a utilizar para esta actividad.

d) 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.

e) Análisis y evaluación de la información. La revisión 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 auditoria.

f) Informe preliminar e informe final: Socialización del informe preliminar, recepción de inquietudes sobre hallazgos y observaciones, mediante correo electrónico el día 31/07/205 y con respuesta de la OCI, por el mismo medio, el 01/08/2025, previo a la emisión del presente informe.

g) Definición y suscripción del plan de mejoramiento. A partir de la notificación del presente informe y con base en los hallazgos de la auditoria, se definirá conjuntamente con la unidad auditada, la definición y suscripción del respectivo plan de mejoramiento.

4. DESARROLLO DE AUDITORIA

RIESGOS Y CONTROLES EVALUADOS:

Este acápite de evaluar riesgos dentro del informe, se presenta por la misma naturaleza del rol de la oficina y aunado a los hechos que la entidad ha sido víctima de dos ataques informáticos, a pesar de que se cuenta con el manual de gestión de riesgos en los procesos de sistemas de información de la SES, obligando a verificar el cumplimiento de los controles, ya que es evidente la materialización de dos riesgos en la entidad: “Inaccesibilidad a los servicios de TI” y “Continuidad del negocio”, respectivamente.

CONDICION: La OCI, procedió a revisar el documento, PO-PLES-002-Política de Administración de Riesgos de la SES, en la cual en el numeral 5.3.2.4 Tercera Línea de Defensa se estableció lo siguiente: *"(…)*Responsabilidades riesgos de seguridad de la información*,* Para el tratamiento de riesgos de seguridad de la información, la entidad debe designar un responsable, perteneciente a la alta Dirección (línea estratégica) que ostente la calidad de oficial de seguridad de la información, quien tendrá a cargo: a) Definir el procedimiento para la identificación y valoración de activos de información. b) Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad de la información (Identificación, Análisis, Evaluación y Tratamiento), con base en la identificación de los activos de información, cuyo nivel de criticidad sea alto… (…)", por consiguiente, se revisó el mapa de riesgos de la entidad, observando que el área de sistemas, tiene identificados los siguientes riesgos:

ID Riesgo	Descripción del Riesgo	Tipo de Riesgo	Causa Principal	Descripción del Control
GSTI-2	Inaccesibilidad a los servicios de TI.	Riesgo Tecnológico	Inadecuada gestión de la infraestructura Tecnológica.	El técnico administrativo o contratista designado por la Oficina Asesora de Planeación y Sistemas mensualmente genera reporte de los incidentes presentados en la mesa de servicios relacionados con la infraestructura tecnológica y de información. Como evidencia quedará el reporte de incidentes.
				El profesional y/o contratista encargado mensualmente realiza la verificación del estado de los servidores y servicios TI, como evidencia quedará Informe de Disponibilidad Servicios Tecnológicos.
GSTI-3	Pérdida de información digital de la Entidad.	Riesgo de Seguridad Digital	Incumplimiento de la política de backup del Modelo de Seguridad y Privacidad de la Información	El Profesional o contratista designado por la Oficina Asesora de Planeación y Sistemas reporta los backups realizados mensualmente para los diferentes aplicativos y servicios en funcionamiento. Como evidencia quedará el reporte de backup de los servidores de datos.
				El líder de seguridad digital designado por la OAPS realiza trimestralmente validación aleatoriamente de copias y restauración de un sistema de información. Como evidencia quedarán acta de las pruebas realizadas.
GETI-1	Ineficiente planeación estratégica en TIC.	Riesgo Estratégico	Falta de articulación de los planes de TI con la estrategia.	El Jefe(a) de la Oficina Asesora de Planeación y Sistemas periódicamente valida necesidades y requerimientos en materia tecnológica con las diferentes áreas a fin de determinar la articulación con la planeación estratégica de la entidad a través de mesa de trabajo y/o solicitudes formales. Como evidencia quedará las actas de reunión, el formato FT-GETI-002 de requerimientos, control de asistencia y/o memorandos o correos de solicitud.
				El Jefe(a) de la Oficina Asesora de Planeación y Sistemas junto con el equipo de trabajo realiza el análisis de actualizaciones requeridas del Plan Estratégico de Tecnología de la Información - PETI de acuerdo al nuevo marco estratégico institucional, normatividad vigente y demás planes institucionales de TI. Como evidencia PETI actualizado y aprobado.

ID Riesgo	Descripción del Riesgo	Tipo de Riesgo	Causa Principal	Descripción del Control
				El Jefe(a) de la Oficina Asesora de Planeación y Sistemas trimestralmente realiza seguimiento al avance de implementación de los proyectos definidos en el Plan Estratégico de Tecnología de la Información - PETI. Como evidencia quedará el indicador de Avance PETI.
GETI-2	Posible ausencia de la medición en la implementación de las Políticas o Lineamientos en el proceso.	Riesgo Estratégico	Falta de mecanismo de medición	El Jefe(a) de la Oficina Asesora de Planeación y Sistemas en el primer semestre aprobará el mecanismo de medición de la implementación de los lineamientos y políticas establecidas. Como evidencia quedará el mecanismo aprobado.
				El Jefe(a) de la Oficina Asesora de Planeación y Sistemas en el segundo semestre iniciará la medición de la implementación de los lineamientos y políticas establecidas a través del mecanismo de medición. Como evidencia quedará el mecanismo diligenciado de manera trimestral.

De acuerdo con el seguimiento realizado, se evidenció la existencia de los respectivos soportes de controles realizados; sin embargo, teniendo en cuenta la materialización del riesgo GSTI-002-Inaccesibilidad a los servicios de TI, en el primer semestre de la actual vigencia, la OCI, recomienda evaluar e incluir algunos ejemplos, que la guía del MINTIC proporciona un marco más amplio para la identificación y gestión de riesgos en el contexto de seguridad y privacidad de la información.

- **Ataques cibernéticos:**
  Incluyen el robo de información, el acceso no autorizado a sistemas, el ransomware (secuestro de datos) y el phishing (fraude electrónico).
- **Error humano:**
  Fallas en la configuración de sistemas, errores en el manejo de información sensible, o la falta de capacitación en seguridad pueden llevar a la exposición de datos.
- **Fallas técnicas:**
  Fallas en la infraestructura tecnológica, como servidores o redes, pueden causar interrupciones en el servicio y pérdida de información.
- **Fuga de información:**
  La divulgación no autorizada de información confidencial, ya sea por errores o intenciones maliciosas.
- **Incumplimiento normativo:**
  No seguir las leyes y regulaciones relacionadas con la protección de datos puede generar sanciones y multas.
- **Suplantación de identidad:**
  Personas malintencionadas pueden hacerse pasar por usuarios legítimos para acceder a sistemas o datos sensibles.
- **Denegación de servicio:**
  Ataques que buscan impedir el acceso a sistemas o servicios, afectando la disponibilidad de la información.

Por otra parte, es importante señalar, que el documento de LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS, en el numeral 4.1.2 Alcance para aplicar la gestión de riesgos de seguridad digital, indica:

El alcance de la administración del riesgo de seguridad digital debe ser ***extensible y aplicable a los procesos de la entidad pública*** que indiquen los criterios diferenciales del Modelo de Seguridad y Privacidad de la Información, habilitador de la Estrategia de Gobierno Digital expedida por el MINTIC.

Por lo tanto, se hace un llamado para que se establezcan controles de seguridad de la información en todos los procesos, a fin de evitar, que la operación de los mismos se vea afecta cuando se presentan estos eventos catastróficos, específicamente en los procesos misionales y nómina.

RECOMENDACIÓN: Actualizar el procedimiento PLAN DE RECUPERACION ANTE DESASTRES, incluyendo los riesgos identificados en la guía: LINEAMIENTOS PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL EN ENTIDADES PÚBLICAS, en el numeral 4.1.2.

DESARROLLO DE LA AUDITORIA SEGÚN ALCANCES PROPUESTOS:

ALCANCE 1. VERIFICAR LA EXISTENCIA, SOCIALIZACIÓN, IMPLEMENTACIÓN Y MONITOREOS DE LOS CONTROLES DEFINIDOS PREVIAMENTE PARA EL CUMPLIMIENTO DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, POR CADA UNA DE LAS POLÍTICAS COMPLEMENTARIAS QUE CONTIENE EL DOCUMENTO FUENTE DE LA SES PO-GETI-003.

CONDICION: Se recibió un documento de la oficina de TI de 76 páginas, contentivo de las acciones de control definidas e implementadas en lo corrido de la vigencia, por cada una de las políticas del documento PO-GETI-003, lo cual indica el cumplimiento del alcance evaluado; sin embargo, la política de relación con proveedores, no se ha definido concretamente los requerimientos y características que contempla el artículo 6.1. de la Resolución 0500 de 2021 del MINTIC. Igualmente, debido al tamaño del documento de gestión de estrategias de control de las políticas, no se presenta en el contenido del presente informe, quedando anexo en la carpeta de papeles de trabajo de esta auditoría.

Vale señalar que el cronograma de actividades presentado y evaluado, fue definido en la entidad a partir del PETI Plan Estratégico de Tecnologías de la Información; sin embargo, todo plan de seguridad de la información debe hacer parte del Modelo de Seguridad y Privacidad de la Información, el cual contempla una metodología que permite caracterizar nuestro propio modelo, siguiendo las pautas de la Resolución 500 de 2021 y de la Resolución 2277 de 2025, respectivamente. Si bien es cierto el MSPI es uno de los proyectos del PETI, en últimas todos los proyectos del PETI están dirigidos a la seguridad de la información, por tanto, estamos hablando, en otros términos, ya que en realidad en la entidad debe denominarse e imperar el MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION y los temas de proyectos de TI, son los que deben ir separados como PETI.

CRITERIO:

A continuación, se relacionan las políticas definidas en la Supersolidaria, en documento PO-GETI-003 V2.

a) **Política de Backup y Restauración:** Con evidencias de copias de seguridad (Veeam Backup & Replication, HPE StoreOnce) y pruebas de restauración, incluyendo respaldo en cintas.

b) **Política de Control de Acceso:** Mediante perfiles de usuario, autenticación robusta y la gestión a través de Directorio Activo (LDAP).
c) **Política de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información:** Integrando la seguridad desde las fases iniciales del ciclo de vida del desarrollo de software.
d) **Política de Llaves Criptográficas:** Asegurando la protección de datos con cifrado (ej., correo electrónico con TLS, certificados web HTTPS).
e) **Política de Gestión de Activos de Información:** Con inventario, clasificación y manejo seguro de activos documentados.
f) **Política de Relación con Proveedores:** Incorporando cláusulas de seguridad en contratos.
g) **Política de Seguridad de las Comunicaciones:** Usando protocolos seguros, cifrado y herramientas como FortiGate, FortiNAC, VLANs, portal cautivo y VPN.
h) **Política de Seguridad de las Operaciones:** Con gestión de vulnerabilidades (Gamma Ingenieros, FortiWeb, PCSecure) y monitoreo de logs (FortiAnalyzer).
i) **Política de Seguridad de los Recursos Humanos:** A través de inducción, sensibilización y control de accesos al desvincular personal.
j) **Política de Seguridad Física y del Entorno:** Con sistemas de vigilancia, control de acceso físico (recepciones, tarjetas, biometría en el Centro de Datos).

Así mismo, La Resolución MINTIC 500 de 2021, contempla:

"*ARTÍCULO 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. (*subrayado fuera de texto).

Así mismo, deberán contar con indicadores para medir la eficacia, efectividad y eficiencia de la gestión de la seguridad de la información y la seguridad digital……...

.. ARTÍCULO 6.1 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA LAS RELACIONES CON LOS PROVEEDORES. <Artículo adicionado por el artículo 3 de la Resolución 746 de 2022. El nuevo texto es el siguiente:> Los sujetos obligados deben determinar e implementar los controles para mitigar los riesgos asociados a la adquisición de productos y servicios de seguridad digital señalados en el Anexo número 2 de la presente resolución, así como cumplir con los siguientes requerimientos y características.

1.Definir claramente los roles y responsabilidades de seguridad de la información con respecto a la relación con el proveedor.

2.Propender por mantener una arquitectura de seguridad al adquirir productos o servicios de Seguridad Digital

3.Analizar los riesgos de Seguridad Digital propios de la integración de soluciones e implementar controles para su mitigación.

4.Implementar controles que permitan minimizar los riesgos asociados a la transferencia de datos generada por cambios de fabricante o proveedor.

5.Identificar la vida útil de los productos y servicios adquiridos con el fin de planificar cualquier migración o transferencia y respaldar los datos para garantizar la continuidad de la operación.

6. Optimizar la gestión de los riesgos de Seguridad Digital estableciendo estrategias soportadas en servicios de nube.

PARÁGRAFO. Los controles para mitigar los riesgos asociados a la adquisición de productos y servicios de seguridad digital señalados en el Anexo número 2, hacen parte integral de la presente resolución y serán actualizados por el MinTIC a través de las sucesivas versiones de cada uno de los documentos que lo componen y previo informe del equipo técnico. La actualización se publicará en la sede electrónica del MinTIC." (subrayado fuera de texto).

CAUSA: Desatención de los lineamientos normativos.

CONSECUENCIAS: Posibles sanciones a la entidad; vulnerabilidad ante ataques informáticos y afectación de la imagen institucional.

RECOMENDACIONES:

1. Identificar y valorar los riesgos contemplados en el anexo número 2 de la Resolución 500 de 2021 MINTIC, así como cumplir con los requerimientos y características contemplados en el artículo 6.1. de la misma resolución.

2. Separar del PETI todos los proyectos y lo concerniente con el MSPI, ya que son dos cosas diferentes; el PETI se debe enfocar a mejorar y afianzar los software y hardware de la entidad en un horizonte de tiempo y el MSPI es un programa normado por el Gobierno Nacional, con sus propias guías, documentos y propósitos y herramientas de gestión.

ALCANCE 2. VERIFICAR LA REALIZACIÓN DE LAS ACTIVIDADES PROGRAMADAS DURANTE EL PRIMER SEMESTRE DEL AÑO 2025 Y SU IMPACTO EN CADA UNO DE LOS OBJETIVOS PROPUESTOS EN EL PLAN DE ACTIVIDADES EN MATERIA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN MSPI, APROBADO POR EL RESPECTIVO COMITÉ EL PRESENTE AÑO.

CONDICION:

La OAPS, allega Excel denominado: "Plan_de_seguridad_de_la_informacion_2025_alineado_PETI", el cual, revisando el avance con corte a 30 de junio, se observa un promedio general del 70% de cumplimiento, evidenciando que se presenta incumplimiento en algunas actividades, lo cual obedece a que, en los meses de abril, mayo y junio, se presentaron los incidentes informáticos, retrasando el cronograma de actividades del plan de trabajo. Se aclara que el documento recibido es más amplio a la información solicitada, ya que puntualmente se pretendía verificar el cumplimiento del plan de trabajo presentado al comité de seguridad y privacidad de la información en el mes de febrero de 2025; por tanto, se evidencia un gran paso al unificar el plan de actividades, totalmente alienado con el PETI, tal como se aprecia en la siguiente tabla:

PETI	NÚMERO	TÍTULO DE LA TAREA	ENTREGABLES / HITOS	FECHA DE ENTREGA	% CUMPLIDO DE LA TAREA
FASE 4	1.1	**Implementación de procedimiento de amenazas, riesgos, vulnerabilidades**	Informe de implementación	30/05/25	70%
	1.2	**Actualización de riesgos identificados por activos de información**	Mapa de riesgos actualizado con planes de mitigación.	30/05/25	70%
	1.3	Aseguramiento Contratación y vinculación (seguridad de recursos)	Clausulado de contratos	30/05/25	100%
	1.4	**Identificar activos de información y actualizar su inventario**	**Inventarios actualizados y aprobados.**	30/06/25	30%
	1.5	**Evaluar y aprobar los riesgos asociados a los activos**	Mapa de riesgos actualizado con planes de mitigación.	30/05/25	70%
	1.6	**Establecer métricas y tableros de control**	Tableros de control implementados	30/06/25	70%
	1.8	**Actualización procedimiento de incidentes de seguridad**	Procedimiento actualizado	30/05/25	70%
FASE 5	2.1	Controles propuestos ISO 27001:2013 - ISO 27001:2022	Matriz de validación con controles	31/03/25	100%
	2.2	Homologar controles del nuevo modelo de seguridad y privacidad de información	Controles actualizados y alineados con la versión 2022 de la norma.	31/03/25	100%
	2.6	Lineamientos software seguro	Matriz lineamientos software seguro	31/03/25	100%
FASE6	3.1	Revisión autodiagnóstico de implementación vigencia 2024	Informe implementación MSPI (Actual)	30/03/25	100%
	3.2	Documento con declaración de aplicabilidad	Documento actualizado con controles implementados.	30/03/25	100%
	3.3	**Revisar la normativa nacional aplicable (Ley 1581, Decreto 1078, Circular 003)**	Informe de brechas y plan de acción para cumplimiento normativo.	31/03/25	70%
	3.4	**Actualizar políticas de seguridad alineadas al MSPI**	Políticas revisadas y aprobadas por el Comité de Seguridad.	30/06/25	70%
FASE 2	4.1	**Construcción de estrategias de recuperación por dominio (comunicaciones, servidores, seguridad)**	**Estrategias de Recuperación**	01/06/25	0%
	4.2	**Construir plan de pruebas de recuperación**	**Plan de pruebas de recuperación**	01/06/25	0%
	4.3	**Aprobación de DRP (OAPS)**	**Acta o documento de aprobación DRP**	01/06/25	0%
	4.4	Pruebas de DRP	Plan de pruebas de DRP y resultados	01/06/25	100%
FASE UNICA	5.1	**Diseño e Implementación de la Infraestructura Tecnológica**		01/06/25	0%
	5.2	**Definición de Procesos y Procedimientos Operativos**		01/06/25	0%
	5.3	**Conformación del Blue Team y Red Team**		01/06/25	0%
PLAN DE SEGURIDAD	6.1	**Análisis de Impacto al Negocio (BIA)**	**Documento BIA**	30/06/25	20%
	6.2	**Gestión de Riesgos de Continuidad**	**Identificación y control de Riesgos de (PCN)**	30/06/25	0%
	6.3	**Diseño del Plan de Continuidad del Negocio**	**Plan de continuidad**	30/06/25	0%

- Las filas resaltadas en color rojo, reflejan cuales actividades registran retraso significativo, frente a la programación prevista a realizarse dentro del primer semestre del año 2025, cuya situación se origina por qué el equipo de trabajo se vio obligados a atender los dos ataques informáticos a la entidad, registrados entre los meses de abril, mayo y junio.

- Las filas resaltadas en amarillo, son tareas que registran avance importante sobre el 70%; mientras que las filas resaltadas en color verde, evidencias total cumplimiento.

CRITERIO: Teniendo en cuenta que el PETI (plan estratégico de tecnologías de la información), es el documento que contiene el plan de actividades de seguridad de la información, se presenta en la siguiente tabla el plan de trabajo completo previsto para el año 2025, sobre el cual se evaluó cumplimiento de enero a junio 2025.

	PETI	NÚMERO	TÍTULO DE LA TAREA	ENTREGABLES / HITOS	FECHA DE INICIO	FECHA DE ENTREGA
PY2	FASE 4	**1**	**Implementar seguridad digital y el modelo de seguridad y privacidad de la información**			
		1.1	Implementación de procedimiento de amenazas, riesgos, vulnerabilidades	Informe de implementación	01/01/25	30/05/25
		1.2	Actualización de riesgos identificados por activos de información	Mapa de riesgos actualizado con planes de mitigación.	01/01/25	30/05/25
		1.3	Aseguramiento Contratación y vinculación (seguridad de recursos)	Clausulado de contratos	01/01/25	30/05/25
		1.4	Identificar activos de información y actualizar su inventario	Inventarios actualizados y aprobados.	01/04/25	30/06/25
		1.5	Evaluar y aprobar los riesgos asociados a los activos	Mapa de riesgos actualizado con planes de mitigación.	01/04/25	30/05/25
		1.6	Establecer métricas y tableros de control	Tableros de control implementados	01/04/25	30/06/25
		1.7	Incrementar la concienciación y capacitación de los colaboradores	Plan de sensibilización - Material de apoyo	15/01/25	31/12/25
		1.8	Actualización procedimiento de incidentes de seguridad	Procedimiento actualizado	01/04/25	30/05/25
		1.9	Realizar simulacros del plan de respuesta a incidentes	Informe de simulacros realizados	01/10/25	28/11/25
	FASE 5	**2**	**Selección de controles a implementar**			
		2.1	Controles propuestos ISO 27001:2013 - ISO 27001:2022	Matriz de validación con controles	01/03/25	31/03/25
		2.2	Homologar controles del nuevo modelo de seguridad y privacidad de información	Controles actualizados y alineados con la versión 2022 de la norma.	15/01/25	31/03/25
		2.3	Generación de autodiagnóstico de implementación.	Autodiagnóstico MINTIC	01/07/25	31/12/25
		2.4	Implementar controles prioritarios según análisis de riesgos	Evidencias de controles aplicados.	01/03/25	31/10/25
		2.5	Realizar pruebas de vulnerabilidad y penetración (ethical hacking)	Informes con hallazgos y recomendaciones.	01/06/25	31/07/25
		2.6	Lineamientos software seguro	Matriz lineamientos software seguro	01/03/25	31/03/25
		2.7	Implementación SOC	Informe de implementación	01/07/25	31/12/25
	FASE	**3**	**Declaración de Aplicabilidad**			

	PETI	NÚMERO	TÍTULO DE LA TAREA	ENTREGABLES / HITOS	FECHA DE INICIO	FECHA DE ENTREGA
		3.1	Revisión autodiagnóstico de implementación vigencia 2024	Informe implementación MSPI (Actual)	01/03/25	30/03/25
		3.1	Análisis del nivel de madurez y alcance del nuevo modelo de seguridad y privacidad de información	Autodiagnóstico MINTIC	01/07/25	31/12/25
		3.2	Documento con declaración de aplicabilidad	Documento actualizado con controles implementados.	01/03/25	30/03/25
		3.3	Revisar la normativa nacional aplicable (Ley 1581, Decreto 1078, Circular 003)	Informe de brechas y plan de acción para cumplimiento normativo.	01/02/25	31/03/25
		3.4	Actualizar políticas de seguridad alineadas al MSPI	Políticas revisadas y aprobadas por el Comité de Seguridad.	01/04/25	30/06/25
PY03	FASE 2	**4**	**Implementación Plan de Recuperación de Desastres TI**			
		4.1	Construcción de estrategias de recuperación por dominio (comunicaciones, servidores, seguridad)	Estrategias de Recuperación	01/01/25	01/06/25
		4.2	Construir plan de pruebas de recuperación	Plan de pruebas de recuperación	01/01/25	01/06/25
		4.3	Aprobación de DRP (OAPS)	Acta o documento de aprobación DRP	01/01/25	01/06/25
		4.4	Pruebas de DRP	Plan de pruebas de DRP y resultados	01/01/25	01/06/25
PY06	FASE UNICA	**5**	**Centro de Monitoreo para redes e infraestructura y Seguridad (NOC/SOC)**			
		5.1	Diseño e Implementación de la Infraestructura Tecnológica		01/01/25	01/06/25
		5.2	Definición de Procesos y Procedimientos Operativos		01/01/25	01/06/25
		5.3	Conformación del Blue Team y Red Team		01/01/25	01/06/25
PLAN DE SEGURIDAD		**6**	**Fortalecimiento del Plan de Continuidad del Negocio (PCN)**			
		6.1	Análisis de Impacto al Negocio (BIA)	Documento BIA	01/04/25	30/06/25
		6.2	Gestión de Riesgos de Continuidad	Identificación y control de Riesgos de (PCN)	01/04/25	30/06/25
		6.3	Diseño del Plan de Continuidad del Negocio	Plan de continuidad	01/04/25	30/06/25

Fuente: OAPS

CAUSA: La ocurrencia de los dos ataques informáticos presentados en la entidad, incidieron en el retraso en el cumplimiento de las tareas del plan de trabajo, previstas para el año 2025.

COSECUENCIAS: Posibles presencia de nuevos riesgos informáticos, mientras se implementan y consolidan los procedimientos de control de ciberseguridad en la SES.

RECOMENDACIÓN: Duplicar esfuerzos para poner al día las tareas atrasadas del primer semestre del año 2025, para ser reprogramadas y realizadas en el tercer trimestre del año 2025.

ALCANCE 3. VERIFICAR EL DOCUMENTO MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA SES, IMPLEMENTADO EN LA ENTIDAD, CUYOS OBJETIVOS Y METAS FUERON ESTABLECIDOS Y SON LA FUENTE DE DEFINICIÓN DE LOS RESPECTIVOS INDICADORES DE DICHO MODELO, CONFORME LO REGULA LA GUÍA DEL MINTIC.

CONDICION: Se recibió el documento Plan de Seguridad de la Información; manifestando en reunión del 23 de julio, que no era obligatorio elaborar y documentar el Manual de Seguridad y Protección de la Información; sin embargo, a este respecto se precisa que según la Resolución 500 del 2021, emitida por el MINTIC, establece que cada entidad debe elaborar el MSPI, según Artículo 5, parágrafo 1 y 2, respectivamente.; de hecho, la guía que profirió al respecto en el año 2021 (última versión) fue derogada por el MINTIC, mediante Resolución 2277 de1 05/07/2025, definiendo un único anexo, todas las guías que había publicado el MINTIC en página web, debidamente actualizadas y son el referente para tener en cuenta desde esa fecha, incidiendo en la revisión y actualización de todos los documentos originados en la SES sobre el MPSI; además el articulado de la Resolución 500 de 2021, no fue modificada ni derogada..

Igualmente, en se revisaron los documentos expedidos en PABLO referidos a la seguridad de la información, encontrando el PR-GETI-005, GESTION DE INCIDENTES, no contiene los pasos y pormenores contemplados en el artículo 9º de la resolución 500 de 2021, especialmente los numerales 3., 4., 5, respectivamente.

CRITERIO: El Ministerio de Tecnologías de la Información, mediante Resolución 500 del 2021, "por *medio de 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*", estableció los siguientes aspectos que fundamentan la obligatoriedad de elaborar en la SES el Modelo de Seguridad y Privacidad de la Información, estableció al respecto del alcance en cuestión:

…" ARTÍCULO 1o. OBJETO. La presente resolución tiene por objeto establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establecer los lineamientos y estándares para la estrategia de seguridad digital.

ARTÍCULO 2o. ÁMBITO DE APLICACIÓN. Serán sujetos obligados de la presente resolución los señalados en el artículo 2.2.9.1.1.2. del Decreto número 1078 de 2015 (DUR- TIC), por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones,
"ARTÍCULO 2.2.9.1.1.2. Ámbito de aplicación. Los sujetos obligados a las disposiciones contenidas en el presente ***capítulo serán las entidades que conforman la administración pública en los términos del Artículo 39 de la Ley 489 de 1998*** *y los particulares que cumplen funciones administrativas…... (Negrilla* fuera de texto).

ARTÍCULO 3o. LINEAMIENTOS GENERALES. Los sujetos obligados deben adoptar……..
Las entidades deben contar con políticas, procesos, procedimientos, guías, manuales y formatos para garantizar el cumplimiento al ciclo PHVA del MSPI. ***En ese sentido, deben adoptar los lineamientos del MSPI****, guía de riesgos y gestión de incidentes de seguridad digital que se relacionan en el Anexo 1 de la presente resolución. …... (Negrilla* fuera de texto).

ARTÍCULO 4o. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL. ***Los sujetos obligados deben aplicar los modelos, guías, y demás documentos técnicos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones a través*** *del habilitador de seguridad y privacidad de la información en el marco de la Política de Gobierno Digital y propenderán por la incorporación de estándares internacionales y sus respectivas actualizaciones o modificaciones, al igual que otros marcos de trabajo que defina mejores prácticas en la materia. (Negrilla* fuera de texto).

ARTÍCULO 5o. LA ESTRATEGIA DE SEGURIDAD DIGITAL. Los sujetos obligados deben adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital. Dicha estrategia se debe incluir en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos artículo 2.2.22.3.14. del Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto número 1083 de 2015, Único Reglamentario del Sector de Función Pública, o la norma que la modifique, adicione, subrogue o derogue.

El Plan de Seguridad y Privacidad de la Información contempla la protección de la información digital, medios impresos y físicos digitales y no digitales*.* Negrilla fuera de texto

La estrategia de seguridad digital debe definirse en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes de seguridad digital, incorporadas en el Anexo 1 de la presente resolución y estar debidamente articulada al habilitador de seguridad y privacidad de la Política de Gobierno Digital. Negrilla fuera de texto

Adicionalmente, la estrategia de seguridad digital debe:

1. *Ser aprobada a través de un acto administrativo de carácter general.*
2. *Contar con un análisis y tratamiento de riesgos de seguridad digital e implementar controles que permitan gestionarlos.*
3. *Establecer los roles y responsabilidades al interior de la entidad asociados a la seguridad digital.*
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.*** Negrilla fuera de texto

PARÁGRAFO 1o. Los sujetos obligados deben adoptar el Modelo de Seguridad y Privacidad de la Información (MSPI) señalado en el Anexo 1 de la presente resolución, como habilitador de la política de Gobierno Digital.
PARÁGRAFO 2o. El Modelo de Seguridad y Privacidad de la Información (MSPI) señalado en el Anexo 1 será actualizado por el MinTIC a través de las sucesivas versiones de cada uno de los documentos que lo componen y previo informe del equipo técnico. La actualización se publicará en la sede electrónica de MinTIC. Negrilla y subrayado fuera de texto.

Con respecto a la gestión de incidentes de seguridad digital, la Resolución 2277 de 2021, contempla:

"*ARTÍCULO 9o. GESTIÓN DE INCIDENTES DE SEGURIDAD DIGITAL. Los sujetos (PR-GETI-005,*

GESTION DE INCIDENTES)
obligados deben establecer un procedimiento de gestión de incidentes de seguridad digital, para realizar el tratamiento, investigación y gestión de los incidentes de seguridad digital que se presente en relación con los activos de información de cada proceso, para lo cual deben:
1. Gestionar los incidentes de seguridad digital, según el procedimiento establecido por MinTIC, para lo cual deben crear una bitácora que contenga la descripción de cada una de las actividades desarrolladas en la gestión de estos.
2. Designar dentro de la entidad los responsables de gestionar y dar respuesta a los incidentes de seguridad digital, liderado por el responsable de seguridad digital.
3. Una vez identificado el incidente de seguridad digital se deberá reportar ante el CSIRT (Equipo de Respuesta a Incidentes de Seguridad Digital) de Gobierno, los incidentes catalogados como Muy Grave y Grave por la entidad, para el respectivo apoyo y coordinación en la gestión de estos a través del formato de reporte establecido por el CSIRT Gobierno, el cual estará disponible por los canales de comunicación del CSIRT Gobierno.
4. Los incidentes catalogados por el responsable de seguridad digital de la entidad, como Menos Grave y Menor, deben ser comunicados al CSIRT Gobierno en el formulario establecido una vez sea gestionado, con el fin de poder llevar una estadística de los incidentes y conocer las tipologías de estos.
5. Los sujetos obligados, según el análisis e investigación de los incidentes y teniendo en cuenta la causa raíz, deben realizar los respectivos planes de mejoramiento, para lo cual el responsable de seguridad digital de la entidad supervisará y hará seguimiento a su cumplimiento.) …….

…….ARTÍCULO 17. ETAPAS GENERALES DE LA GESTIÓN DE INCIDENTES DE SEGURIDAD DIGITAL. Los sujetos obligados deben incluir en su estrategia de seguridad digital las actividades a realizar en las etapas de prevención; protección y detección; respuesta y comunicación; recuperación y aprendizaje, como mínimo deberán incorporar:
1. Prevención
La función de prevención admite la capacidad de limitar o contener el impacto de un posible incidente de seguridad digital. En esta etapa, los sujetos obligados deben cuando menos:
1.1. Establecer, mantener y documentar los controles de acceso (lógicos, físicos y procedimentales), protección de infraestructura y gestión de identidades, privacidad y protección de la información.
1.2. Adoptar políticas, procedimientos y mecanismos para evitar la fuga de datos e información.
1.3. Gestionar y documentar la seguridad de la plataforma tecnológica.
1.4. Contar con los recursos tecnológicos necesarios para realizar una adecuada gestión de seguridad de la información y la ciberseguridad.
1.5. Identificar, y gestionar los riesgos de seguridad de la información que puedan llegar a afectar a la entidad y establecer controles para su mitigación.
1.6. Considerar dentro del plan de continuidad del negocio la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques de seguridad de la información.
1.7. Realizar pruebas del plan de continuidad del negocio que simulen la materialización de ataques de seguridad de la información.
1.8. Determinar la necesidad de contar con herramientas o servicios que permitan hacer correlación de eventos que puedan alertar sobre incidentes de seguridad, entre otros, SIEM (Gestión de eventos de información de seguridad) o SOC (Centro de operaciones de seguridad).
1.9. De acuerdo con la estructura, infraestructura, canales de atención, volumen transaccional y número de clientes, monitorear diferentes fuentes de información institucionales oficiales tales como sistemas de información, infraestructuras críticas, correos electrónicos, sitios web, blogs, dispositivos y perfiles oficiales de redes sociales con el propósito de identificar posibles ataques cibernéticos contra la

entidad.
1.10. Colaborar y articular con las autoridades que hacen parte del modelo nacional de gestión de ciberseguridad en los proyectos que se adelanten con el propósito de fortalecer la gestión de la ciberseguridad a nivel nacional.
2. Protección y detección
La función de protección y detección permite el descubrimiento oportuno de eventos e incidentes de ciberseguridad y cómo protegerse ante los mismos. Los sujetos obligados deben:
1.1. Adoptar procedimientos y mecanismos para identificar y analizar los incidentes de seguridad que se presenten.

1.2. Gestionar las vulnerabilidades de aquellas infraestructuras críticas o plataformas que soporten activos de información críticos y que estén expuestos en el ciberespacio.
1.3. Realizar un monitoreo continuo a su plataforma tecnológica e infraestructura crítica con el propósito de identificar y predecir comportamientos inusuales que puedan evidenciar ataques contra la entidad.
1.4. Implementar tecnologías que permitan a la Entidad identificar el origen de los ataques, tipos de ataques, comportamientos y la detección predictiva de amenazas.
1.5. Realizar periódicamente auditorías de seguridad de la información tanto para los aspectos de gestión como para los aspectos técnicos, como podrían ser: auditorías internas y externas al modelo de Seguridad y Privacidad de la Información, análisis de vulnerabilidades, Hacking ético, pruebas de penetración a sistemas informático y pruebas de ingeniería social entre otras.
3. Respuesta y comunicación
Aún con las medidas de seguridad adoptadas, los sujetos obligados deben desarrollar e implementar planes de respuesta a incidentes de seguridad digital. Para hacerle frente a esta situación los sujetos obligados deben:
1.1. Establecer planes y procedimientos de respuesta a incidentes digitales y de seguridad de la información.
1.2. Establecer los procedimientos para reportar, cuando se considere pertinente, al Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT) o quien haga sus veces, a través del CSIRT sectorial, los incidentes de seguridad Digital que requieran de su gestión.
1.3. Comunicar a las autoridades competentes después de una fuga o afectación a la privacidad de la información de la Entidad o ciudadanos.
1.4. Dar un tratamiento adecuado a las evidencias forenses para que las áreas de seguridad digital y las autoridades puedan realizar su identificación, recolección, embalaje y disposición en las investigaciones correspondientes.
4. Recuperación y aprendizaje
Desarrollar e implementar actividades apropiadas para definir y mantener los planes de recuperación, resiliencia y restauración de las infraestructuras críticas, servicios, sistemas de información, procesos o en general de un activo de información que se haya deteriorado debido a un incidente de seguridad digital. Los sujetos obligados deben:
1.1. Adoptar los mecanismos necesarios para recuperar los sistemas de información e infraestructuras al estado en que se encontraban antes del ataque de seguridad.
1.2. Ajustar sus sistemas de gestión de riesgo y de seguridad de la información como consecuencia de los incidentes presentados, adoptando los controles que resulten pertinentes.
1.3. Socializar, cuando la entidad lo considere pertinente, las lecciones aprendidas al interior de la organización y con las entidades de su sector. “

CAUSA: Desatención de las normas y guías que regulan la seguridad y privacidad de la información

CONSECUENCIAS: Incumplimiento a lineamientos normativos

RECOMENDACIONES:

1. Realizar el proceso de elaboración, socialización e implementación del Manual de Privacidad y Seguridad en la Información, propio de la SES, con base en el anexo único de la Resolución 2277 del 05/07/2025, del MINTIC y lo regulado en el articulado de la Resolución 500 de 2021.

2. Revisar y determinar si la SES tiene ajustada la gestión de seguridad de la información, conforme a la Resolución 500 de 2021, procediendo a tomar las medidas pertinentes en la documentación referente en la SES, presentando informe sobre sus resultados al comité de seguridad y privacidad de la información de la SES.

3. Definir el Plan de Seguridad de la información, partiendo del MSPI de la SES, dicho documento debe ser actualizado anualmente, de acuerdo con los resultados de dicho plan y la aplicación de los indicadores definidos en el mismo modelo, según lo contemplado en el numeral 10 artículo 6º Resolución 500 de 2021.

4. Actualizar el procedimiento de gestión de incidentes de seguridad de la SES, respecto a las consideraciones que establece los artículos 9º y 17º, respectivamente, de la Resolución 500 de 2021.

ALCANCE 4. DETERMINAR CUÁL ES EL ESTADO ACTUAL DE LOS INDICADORES DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN O EN SU DEFECTO, LA EXISTENCIA DE EVIDENCIAS QUE INDICAN AVANCES EN LOS MISMOS, ESPECÍFICAMENTE LOS CUALES REGISTRABAN EVIDENTE RETRASO EN EL DX Y, POR TANTO, TIENEN PROYECTADO AUMENTAR EL PORCENTAJE DE IMPLEMENTACIÓN DURANTE EL AÑO, DEL 10% EN PROMEDIO.

CONDICION:

El proceso allegó el archivo “instrumento autoevaluación MPSI julio_2024.xls” indicando que este correspondía a los indicadores, lo cual, de acuerdo a la evaluación realizada por la OCI, no cumple con los criterios de un indicador, sino como su nombre lo dice, es la AUTOEVALUACIÓN del MPSI. Por lo tanto, se concluye que no existen indicadores que permitan realizar un seguimiento al proceso de implementación del modelo.

De igual manera, la OCI, procedió a revisar en el aplicativo PABLO – SIG, si existen indicadores, evidenciando que existe un indicador como se muestra en la siguiente imagen:

Indicador	Tendencia	Meta	Última Medición	Frecuencia	Actualizado	Descripción	Formula	Formula Descripción	Tipo de Indicador	Proceso	Fuer
						PLANEADAS EN EL PETI. ANUAL (JUNIO DE CADA VIGENCIA)				INFORMACIÓN	
IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)	Positiva	70	Rojo	TRIMESTRAL	Sin Medicion	ESTE INDICADOR MIDE EL PORCENTAJE DE AVANCE EN LA IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD DE LA INFORMACIÓN (MSPI), DE ACUERDO CON LOS OBJETIVOS ESTABLECIDOS EN EL PLAN DE SEGURIDAD DE LA INFORMACIÓN. SU PROPÓSITO ES ASEGURAR QUE SE CUMPLAN LOS ESTÁNDARES DE SEGURIDAD Y QUE SE GESTIONEN ADECUADAMENTE LOS RIESGOS ASOCIADOS A LA PROTECCIÓN DE LOS DATOS DE LA ENTIDAD.	(A/ B)*100	= (NUMERO DE ACTIVIDADES COMPLETADAS)/ (TOTAL DE ACTIVIDADES PLANIFICADAS)*100 A= NUMERO DE ACTIVIDADES COMPLETADAS B= TOTAL DE ACTIVIDADES PLANIFICADAS	EFICACIA	GETI - GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN	SEGUIMIE DEL PLAN SEGURIDA PRIVACID LA INFOR

Sin embargo, se observó que el mismo no presenta medición en la actual vigencia, por lo que definitivamente se concluye que no se ejecuta una medición del modelo.

Por consiguiente, esta oficina a continuación, señala algunos ejemplos de indicadores que se pueden utilizar para evaluar la seguridad y privacidad de la información:

- ✓ **ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN.**
  El indicador permite determinar y hacer seguimiento, al compromiso de la dirección, en cuanto a seguridad de la información, en lo relacionado con la asignación de personas y responsabilidades relacionadas a la seguridad de la información al interior de la entidad.

- ✓ **CUBRIMIENTO DEL SGSI EN ACTIVOS DE INFORMACIÓN.**
  El indicador permite determinar y hacer seguimiento al cubrimiento que se realiza a nivel de activos críticos de información de una entidad y los controles aplicados.

- ✓ **TRATAMIENTOS DE EVENTOS RELACIONADOS EN MARCO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN**
  El indicador permite determinar la eficiencia en el tratamiento de eventos relacionados la seguridad de la información. Los eventos serán reportados por los usuarios o determinadas en las auditorías planeadas para el sistema.

- ✓ **PLAN DE SENSIBILIZACIÓN**
  El indicador permite medir la aplicación de los temas sensibilizados en seguridad de la información por parte de los usuarios finales. Estas mediciones se podrán realizar por medio de auditorías especializadas en el tema o de forma aislada por parte de los responsables de la capacitación y sensibilización.

- ✓ **CUMPLIMIENTO DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LA ENTIDAD**
  Cumplimiento de políticas de seguridad de la información en la entidad.

- ✓ **IDENTIFICACIÓN DE LINEAMIENTOS DE SEGURIDAD DE LA ENTIDAD**

Grado de la seguridad de la información y los equipos de cómputo.

- ✓ **VERIFICACIÓN DEL CONTROL DE ACCESO**
  Grado control de acceso en la entidad.

- ✓ **PORCENTAJE DE IMPLEMENTACIÓN DE CONTROLES**
  Grado de avance en la implementación de controles de seguridad.

CRITERIOS: Incumplimiento de la dimensión 4 "Evaluación de resultados" del MIPG en dos momentos, el primero, el seguimiento a la gestión institucional y segundo, la evaluación propiamente de los resultados obtenidos. Tanto el seguimiento como la evaluación exigen contar con indicadores para monitorear y medir el desempeño de las entidades.

Igualmente, la Resolución 2277 de 2021, regula al respecto:

*"**ARTÍCULO** 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.*
Así mismo, deberán contar con indicadores para medir la eficacia, efectividad y eficiencia de la gestión de la seguridad de la información y la seguridad digital". Subrayado y negrilla fuera de texto.

A su vez, la guía – Indicadores de gestión de seguridad de la información, que estaba vigente antes del 05 de julio de 2025, proferida por el MINTIC, contiene la necesidad de definir los indicadores dentro de una ficha técnica, conforme los estándares de MIPG, en el siguiente sentido (además que el nuevo anexo no modifica este aspecto):

"…*2. Construcción de indicadores*

Acorde con la Guía para Diseño, Construcción e Interpretación de Indicadores del DANE, para la construcción de indicadores se debe tener en cuenta un tratamiento adecuado de la información que será la base del proceso de revisión control y mejora, de esta forma, dentro de la elaboración de indicadores se tienen definidos cuatro etapas específicas, como se menciona a continuación: ……

3. Indicadores propuestos

A continuación, se definen una serie de indicadores para medir la gestión y el cumplimiento en el avance de implementación del Nuevo Modelo de Seguridad y Privacidad de la Información, esperando que sirva de base para que los encargados de la seguridad de la información en las entidades y sea un ejemplo para apoyarlos en esta labor.

Dichos indicadores son:

INDICADOR 01- ORGANIZACIÓN DE SEGURIDAD DE LA INFORMACIÓN.					
IDENTIFICADOR	*SGIN01*				
DEFINICIÓN					
El indicador permite determinar y hacer seguimiento, al compromiso de la dirección, en cuanto a seguridad de la información, en lo relacionado con la asignación de personas y responsabilidades relacionadas a la seguridad de la información al interior de la entidad					
OBJETIVO					
Hacer un seguimiento a la asignación de recursos y responsabilidades en gestión de seguridad de la información, por parte de la alta dirección.					
TIPO DE INDICADOR					
Indicador de Gestión					
DESCRIPCIÓN DE VARIABLES		***FORMULA***		***FUENTE DE INFORMACIÓN***	
VSI01: Número de personas con su respectivo rol definió según el modelo de operación capítulo 2.		*(VSI01/VSI02) *100*		*Capítulo 2 de la guía del modelo de operación del marco de seguridad y privacidad de la información.*	
VSI02: Número de personas con su respectivo rol definió después de un año.				*Actas de asignación de personal.*	
METAS					
MÍNIMA	***75-80%***	***SATISFACTORIA***	*80-90%*	***SOBRESALIENTE***	*100%*
OBSERVACIONES					
De acuerdo a lo establecido en el capítulo 2 de la guía del modelo de operación del marco de seguridad y privacidad de la información, es necesario crear nuevos cargos y asignar responsabilidades en los actuales, por lo tanto, el indicador está enfocado, no solo a la contratación de nuevas personas, sí no a la asignación de responsabilidades.					

- **CAUSA**: Ausencia de mecanismos de medición y/o debilidades en la aplicación de las guías e instrumentos generados por el MINTIC.

- **CONSECUENCIAS O EFECTOS**: Incumplimiento a lineamientos normativos

- **RECOMENDACIÓN:** Definir e implementar los indicadores de gestión de seguridad de la información prioritarios en la SES, acordes con las políticas, MSPI y plan de seguridad de la vigencia; siguiendo los lineamientos del anexo único de la Resolución 2277 de 2025 del MINTIC y lo regulado en la Resolución 500 de 2021.

a) RECOMENDACIONES Y SUSCRIPCION DE PLAN DE MEJORAMIENTO

No	Descripción Del Hallazgo	Repetitivo (si/no)	Acciones de mejoramiento recomendadas por la Oficina de Control Interno
1	Se recibió un documento de la oficina de TI de 76 páginas, contentivo de las acciones de control definidas e implementadas en lo corrido de la vigencia, por cada una de las políticas del documento PO-GETI-003, lo cual indica el cumplimiento del alcance evaluado; sin embargo, la política de relación con proveedores, no se ha definido concretamente los requerimientos y características que contempla el artículo 6.1. de la Resolución 0500 de 2021 del MINTIC.	NO	Identificar y valorar los riesgos contemplados en el anexo número 2 de la Resolución 500 de 2021 MINTIC, así como cumplir con los requerimientos y características contemplados en el artículo 6.1. de la misma resolución.
2	La OAPS, allega Excel denominado: “Plan_de_seguridad_de_la_informacion _2025_alineado_PETI”, el cual, revisando el avance con corte a 30 de junio, se observa un promedio general del 70% de cumplimiento, evidenciando que se presenta incumplimiento en algunas actividades, lo cual obedece a que, en los meses de abril, mayo y junio, se presentaron los incidentes informáticos, retrasando el cronograma de actividades del plan de trabajo.	NO	Con el fin de dar cumplimento oportuno a las actividades, dentro del seguimiento que ejecuta la OAPS, evaluar todas las circunstancias que no permitan dar cumplimiento oportuno e identificar cuales requieren ser reprogramadas y realizadas en el siguiente trimestre del año 2025.
3	Se recibió el documento Plan de Seguridad de la Información; manifestando en reunión del 23 de julio, que no era obligatorio elaborar y documentar el Manual de Seguridad y Protección de la Información; sin embargo, a este respecto se precisa que según la Resolución 500 del 2021, emitida por el MINTIC, establece que cada entidad debe elaborar el MSPI, según Artículo 5, parágrafo 1 y 2, respectivamente.; de hecho, la guía que profirió al respecto en el año 2021 (última versión) fue derogada por el MINTIC, mediante Resolución 2277 de1 05/07/2025,	NO	Adoptar las directrices, lineamientos, guías, protocolos, modelos, procedimiento y procedimientos que indique el anexo único de la Resolución 2277 de 2025. Por tanto, el tema que esta resolución está por fuera del alcance la auditoría, no tiene fundamento, ya que precisamente es una auditoria de seguimiento de Ley, la cual justamente, fue modificada en el transcurso de la auditoría, debiendo ser tenida en cuenta por la OCI y la SES, lo cual le da legalidad y oportunidad a la SES acogiéndola. Actualizar el procedimiento de gestión de incidentes de seguridad de la SES, respecto a las consideraciones que establece los artículos 9º y 17º, respectivamente, de la Resolución 500 de 2021.

No	Descripción Del Hallazgo	Repetitivo (si/no)	Acciones de mejoramiento recomendadas por la Oficina de Control Interno
4	Incumplimiento de la dimensión 4 “Evaluación de resultados” del MIPG en dos momentos, el primero, el seguimiento a la gestión institucional y segundo, la evaluación propiamente de los resultados obtenidos. Tanto el seguimiento como la evaluación exigen contar con indicadores para monitorear y medir el desempeño de las entidades.	NO	Definir e implementar los indicadores de gestión de seguridad de la información prioritarios en la SES, acordes con las políticas, MSPI y plan de seguridad de la vigencia; siguiendo los lineamientos del anexo único de la Resolución 2277 de 2025 del MINTIC y lo regulado en la Resolución 500 de 2021.

Se requiere que la Oficina Asesora De Planeación Y Sistemas / Gestión de Servicios de Tecnologías de la Información., la definición y suscripción del respectivo plan de mejoramiento. La etapa inicial de FORMULACION, ha sido diligencia por la oficina de control interno, quien, como valor agregado, ha incluido recomendaciones para cada hallazgo; sin embargo, las propias que proponga el auditado junto con las acá recomendadas, deben ser consensuadas, durante la etapa siguiente de DEFINICION Y SUSCRIPCION de dicha actividad.

Por lo anterior, se enviará 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.

Atentamente,

(ORIGINAL FIRMADO)
Jorge Hernando Pedraza Vargas
Jefe Oficina de Control Interno

Elaboró: Martha Rocio Yanquen Parra – Profesional Especializada