BOGOTÁ | SUBRED INTEGRADA DE SERVICIOS DE SALUD SUR OCCIDENTE ESE

NOTA INTERNA
SSO-2026-240-002535-3

Bogotá,28 de mayo de 2026

DE: **GUILLERMO CERON SANDOVAL**
OFICINA DE CONTROL INTERNO
JEFE DE CONTROL INTERNO

PARA **ANDREA ELIZABETH HURTADO NEIRA**
GERENTE
DESPACHO DEL GERENTE

Asunto: Seguimiento a la implementación y cumplimiento del Modelo de Seguridad y Privacidad de la Información - MSPI

Respetada doctora Andrea, cordial saludo.

En cumplimiento del Decreto 1083 de 2015, artículo 2.2.21.4.7, Parágrafo 1° (modificado por el artículo 1 del Decreto 338 de 2019) que establece: "*Los informes de auditoría, seguimientos y evaluaciones* [emitidos por la Oficina de Control Interno] *tendrán como destinatario principal el representante legal de la entidad y el Comité Institucional de Coordinación de Control Interno y/o Comité de Auditoría y/o Junta Directiva, (…)*" (Subrayado fuera de texto), de manera atenta le envío el Informe Final N° OCI-SISSSO-IL-2026-11 de la auditoría interna de cumplimiento: **Seguimiento a la implementación y cumplimiento del Modelo de Seguridad y Privacidad de la Información - MSPI** del período comprendido entre el 1 de enero de 2025 y el 31 de marzo de 2026.

Agradezco su acostumbrado respaldo en nuestra labor de auditoría interna, su atención y gestión pertinente, y manifiesto nuestra disposición para atender cualquier duda o inquietud que surja en el marco de esta auditoría de cumplimiento.

Cordialmente,

GUILLERMO CERON SANDOVAL
JEFE DE CONTROL INTERNO

Anexos: Informe OCI-SISSSO-IL-2026-11 Seguimiento a la implementación y cumplimiento del Modelo de Seguridad y Privacidad de la Información - MSPI

Copia a: Marcia Greicy Guacaneme- jefe Oficina Asesora de Desarrollo Institucional (Miembro CICSCI)
Carmen Esther Acero García- jefe Oficina Asesora de Comunicaciones (Miembro CICSCI)
Julio Alfonso Peñuela Saldaña - jefe Oficina Jurídica (Miembro CICSCI)
Rosa Viviana Cubillos Medrano - jefe Oficina de Participación Comunitaria y Servicio al Ciudadano (Miembro CICSCI)
Hernando Miguel Mojica Mugno - jefe Oficina de Sistemas de Información TICs (Miembro CICSCI)
Mónica Amparo Varón Aguirre - jefe Oficina de Calidad (Miembro CICSCI)
Ana Lucia Quintero Mojica - Subgerente Corporativa (Miembro CICSCI)
Bertha Lucia Mora Quiñones - Subgerente Prestación de Servicios de Salud (Miembro CICSCI)

Declaramos que hemos revisado el presente documento y lo encontramos ajustado a las normas y disposiciones legales, y por lo tanto, lo presentamos para firma.	
Cargo funcionario / Contratista	Nombre/Cargo
Aprobado por:	GUILLERMO CERON SANDOVALOCIOCI
Revisado por:	GUILLERMO CERON SANDOVAL / OCI
Elaborado por:	MARTHA PATRICIA PALOMINO RAMIREZ / OCI

N° INFORME: OCI-SISSSO-IL-2026-11

NOMBRE TRABAJO DE AUDITORÍA: Seguimiento a la implementación y cumplimiento del Modelo de Seguridad y Privacidad de la Información - MSPI

DESTINATARIOS[1]

Integrantes Comité Institucional de Coordinación del Sistema de Control Interno:

- Andrea Elizabeth Hurtado Neira Gerente
- Ana Lucia Quintero Mojica - Subgerente Corporativa
- Bertha Lucia Mora Quiñones - Subgerente Prestación de Servicios de Salud
- Hernando Miguel Mojica Mugno - Jefe Oficina de Sistemas de Información TICs
- María Greicy Guacaneme Valbuena - Jefe Oficina Asesora de Desarrollo Institucional
- Carmen Esther Acero García- Jefe Oficina Asesora de Comunicaciones
- Julio Alfonso Peñuela Saldaña - Jefe Oficina Asesora Jurídica
- Rosa Viviana Cubillos Medrano - Jefe Oficina de Participación Comunitaria y Servicio al Ciudadano
- Mónica Amparo Varón Aguirre - Jefe Oficina de Calidad

EMITIDO POR: Guillermo Cerón Sandoval, Jefe Oficina de Control Interno

EQUIPO AUDITOR: Jorge Orlando Sánchez Alcalá, Profesional Especializado I -OPS

1. OBJETIVO GENERAL

Realizar evaluación y seguimiento a la implementación y cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI), de acuerdo con los lineamientos de la Estrategia de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC y la Norma Técnica Colombiana NTC-ISO-IEC 27001:2013 *"Tecnología de La Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos"*.

2. OBJETIVOS ESPECÍFICOS

Mediante documentación remitida por la Oficina de Gestión Informática (Gestión de TICS), se validarán los componentes del Modelo de Seguridad y Privacidad de la Información (MSPI):

- Roles y Responsabilidades.
- Gestión de Incidentes de seguridad de la información.
- Indicadores de Gestión de Seguridad de la Información.

[1] En virtud de lo establecido en el Decreto 1083 de 2015 **Artículo 2.2.21.4.7**, Parágrafo 1° (modificado por el Artículo 1 del Decreto 338 de 2019) *"Los informes de auditoría, seguimientos y evaluaciones* [emitidos por la Oficina de Control Interno] *tendrán como destinatario principal el representante legal de la entidad y el Comité Institucional de Coordinación de Control Interno y/o Comité de Auditoria y/o Junta Directiva, (…)"*

- Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas.
- Gestión Inventario de Activos e Infraestructura Critica.
- Seguimiento a la implementación Política de Seguridad y Privacidad de la Información.

3. ALCANCE (Periodo Auditado: 01/01/2025 a 31/03/2026)

Este seguimiento se realiza, teniendo en cuenta los siguientes enunciados del Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC realizados en el documento MSPI (pág. 20):

"La seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno en línea, permite alinearse al componente de TIC para la Gestión al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad.

La Seguridad y Privacidad de la Información se alinea al componente de TIC para Servicios apoyando el tratamiento de la información utilizada en los trámites y servicios que ofrece la Entidad, observando en todo momento las normas sobre protección de datos personales, así como otros derechos garantizados por la Ley que exceptúa el acceso público a determinada información.

El componente de TIC para Gobierno Abierto se alinea con el componente de Seguridad y Privacidad de la Información que permite la construcción de un estado más transparente, colaborativo y participativo al garantizar que la información que se provee tenga controles de seguridad y privacidad de tal forma que los ejercicios de interacción de información con el ciudadano, otras entidades y la empresa privada sean confiables."

Nota: El establecimiento de este período no limita la facultad de la Oficina de Control Interno para pronunciarse sobre hechos previos o posteriores que, por su nivel de riesgo o materialidad, deban ser revelados.

4. CRITERIOS

- **Ley 1581 de 2012** (octubre 17) "*Por la cual se dictan disposiciones generales para la protección de datos personales."*
- **Ley 1712 de 2014** (marzo 6) "*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 1078 de 2015** (mayo 26) "*Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"*
- **Norma Técnica Colombiana - NTC ISO/IEC 27001:2013** *Sistemas de Gestión de la Seguridad de la Información (SGSI).*

- **Decreto 1008 de 2018** *(junio 14) " 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 (marzo 10) del MinTIC** *"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"*. Esta resolución se fundamenta en la norma ISO 27001 versión 2013.
- **Decreto 338 de 2022** *(marzo 8) del MinTIC "Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones".*

5. MÉTODOS, PROCEDIMIENTOS Y TÉCNICAS

Para la ejecución de la auditoría se aplicaron principalmente técnicas y/o procedimientos de análisis, comparación e inspección documental, muestreos y pruebas de recorrido; el detalle de cada procedimiento se encuentra en los papeles de trabajo, los cuales se encuentran ubicados en el sistema institucional de gestión, siendo esta la fuente oficial y definitiva de la información del proceso.

En atención a los lineamientos normativos y procedimentales aplicables a las Oficinas de Control Interno, en la ejecución de este trabajo se aplicó un enfoque sistemático y disciplinado que abarcó tres (3) fases: planeación (describiendo las herramientas y las hojas de trabajo que se desarrollarán en la auditoria), ejecución (verificación documental y de procedimientos en cumplimiento a los lineamientos definidos por MinTIC y el Departamento Administrativo de la Función Pública) y comunicación (permitiendo realizar la verificación de los resultados obtenidos y de esta manera desarrollar el plan de acción o de mejora que se considere pertinente por la unidad auditada), desarrolladas de acuerdo con el cronograma de trabajo establecido para la auditoría interna de cumplimiento.

Se realizó verificación documental y de concurrencia, haciendo uso del Documento Maestro del MPSI, el cual presenta las fases y el ciclo del MPSI y en apoyo con la norma NTC: ISO/IEC 27001, que define el Sistema de Gestión de la Seguridad de la Información.

En esta auditoría interna de cumplimiento se realizó la verificación de los ítems que tienen relación directa con el MSPI (en el marco de Gobierno Digital), según el programa de trabajo definido, así:

TEMA(S)	REQUISITOS NORMATIVOS A VERIFICAR	INSUMO(S) PARA VALIDAR EL CUMPLIMIENTO DEL REQUISITO NORMATIVO
Roles y Responsabilidades	Norma ISO/IEC 27001 Anexo A. Ítem A.6.1.1. Roles y responsabilidades para la seguridad de la información. MSPI - Documento Maestro, Controles del Anexo A del estándar ISO/IEC 27001:2013 y dominios a los que pertenece - Num. A.6.1.1 Roles y responsabilidades para la seguridad de información.	* Matriz de roles y perfiles, en los sistemas de información. * Matriz de roles y perfiles, de acceso al dominio en estaciones de trabajo.
Gestión de Incidentes de seguridad de la información.	Norma ISO/IEC 27001 Anexo A. ítem A.16.1. Gestión de incidentes y mejoras en la seguridad de la información MSPI - Documento Maestro, Gestión de incidentes de seguridad de la información Anexo A ítem A.16.1. Gestión de incidentes y mejoras en la seguridad de la información.	* Matriz de reporte y seguimiento de incidentes de seguridad. * Pan de acción para mitigar incidentes de seguridad. * Política de atención o gestión de incidentes de seguridad. * Plan de prevención de incidentes de seguridad.
Indicadores de Gestión de Seguridad de la Información.	MSPI - Guía - Indicadores Gestión de Seguridad de la Información.	* Identificar los Indicadores de Gestión de Seguridad de la Información, propuestos en la entidad.
Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas.	Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas (MNGRSI) - Gobierno digital - MinTIC	* Último documento presentado.
Gestión Inventario de Activos e Infraestructura Critica.	MSPI - inventario y clasificación de activos de información e infraestructura critica cibernética nacional	* Inventario de infraestructura, equipos y sistemas de información.
Seguimiento a la implementación Política de Seguridad y Privacidad de la Información	Política de seguridad y privacidad de la información, Subred Integrada De Servicios de Salud Sur Occidente E.S.E. Plan de acción para el manejo de Seguridad de la información, Subred Integrada De Servicios de Salud Sur Occidente E.S.E.	* Política de seguridad y privacidad de la información (Código 01-01-OD-0029) V4 Almera. * Plan de acción para el manejo de Seguridad de la información (Código EQ ME GER INF 07) Almera.

6. DESCRIPCIÓN DEL TRABAJO REALIZADO,

Mediante la Nota Interna SSO-2026-240-001537-3, se notificó a la Oficina de Gestión Informática (Gestión TIC) el inicio de las actividades de auditoría, en cumplimiento de lo dispuesto en el artículo 12 de la Ley 87 de 1993, el Plan Anual de Auditoría aprobado para la vigencia 2026 y el Decreto 648 de 2017, particularmente en lo relacionado con el rol de evaluación y seguimiento.

La evaluación se realizó mediante la comparación de la información suministrada por el área auditada con los requisitos establecidos en la norma ISO/IEC 27001 y los lineamientos definidos por el MinTIC, en el marco del Modelo de Seguridad y Privacidad de la Información, alineado con el Marco de Referencia de Arquitectura TI;

Se desarrolló esta auditoría, realizando la evaluación de los temas propuestos por El Modelo de Seguridad y Privacidad de la Información – MSPI, donde describe en su documento maestro, unas faces de Planificación, Operación, Evaluación de Desempeño y Mejoramiento continuo, relacionándolos en los resultados de las pruebas de auditoría aplicadas, donde se menciona a continuación lo evidenciado:

En la prueba de Revisión Documental, a través de la prueba se evaluó las temáticas del Modelo de Seguridad y Privacidad de la Información (MSPI) referentes a: Roles y Responsabilidades, Gestión de Incidentes de Seguridad de la Información, Indicadores de Gestión de Seguridad de la Información y Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas (MNGRSI) - Gobierno digital MinTIC; que en la revisión documental aportada por el auditado y recopilada por el auditor de las herramientas e la entidad, como lo son la página web y el aplicativo Almera, donde se cuenta con los soportes de lo aquí mencionado.

En el desarrollo de la revisión documental, con la que daremos el alcance a la evolución de las temáticas: Roles y Responsabilidades, Gestión de Incidentes de seguridad de la información, Indicadores de Gestión de Seguridad de la Información y Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas (MNGRSI), se evaluaron los siguientes ítems:

- En la definición y asignación de todas las responsabilidades de la seguridad de la información en la entidad, se cuenta con el Acuerdo No. 55 de 2019, Octubre 17 de 2019, en las páginas de la 28 a la 31, definiendo que la Oficina de Sistemas de Información - TIC, como el responsable de la seguridad y a su vez al Jefe de Oficina.

- Para la descripción de las políticas, procedimientos, manuales y matrices, definidas para la asignación de los roles y permisos, en los sistemas de información y acceso al dominio, en estaciones de trabajo; se cuenta con el documento: 13-00-OD-0006 Matriz de Roles y Perfiles del Dominio V1, en el aplicativo Almera, así como también se ubican los documentos: 01-01-OD-0029 Política de seguridad y privacidad de la información y 13-00-OD-0004 Plan de Seguridad y Privacidad de la Información, con los que soportan la gestión de seguridad de acceso a la información de la entidad.

- En referencia a la matriz de incidentes y los reportes realizados, identificando lo

seguimientos y acciones ejecutadas, en la herramienta Almera de la entidad, se ubican los documentos: 13-02-FO-0005 Reporte de incidentes de seguridad de la información, formato en Excel y también hallamos el Reporte de Incidentes de Seguridad 2020; La Oficina de Sistemas de Información – TICs, indica que en la vigencia que se desarrollara la auditoria y a la fecha actual, no cuentan con reportes de Incidentes o fallos presentados, que generaran novedades o afectación del servicio.

- Evaluando el plan de acción, para la gestión de los incidentes de seguridad registrados en la entidad, se identifica que se cuenta con el 13-00-PL-0004 Plan de acción de seguridad y privacidad de la información V6, publicado en la herramienta Almera, sumado a que la Oficina de Sistemas de Información - TICs cuenta con el procedimiento gestión de backup bases de datos y sistemas de información 13-00-PR-0002 para salvaguardar los datos en caso de novedades críticas que puedan afectar la integridad de la información en los sistemas de informáticos misionales, con el que dan alcance y gestión al plan de acción.

- Para evaluar el plan de prevención de incidentes de seguridad, la entidad con el 13-00-OD-0005 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el 02-01-FO-0013 Plan de TRABAJO tratamiento de riesgos I trimestre 2026, publicados en la herramienta Almera, soportando su ejecución con las herramientas mencionadas por la Oficina de Sistemas de Información – TICs, evidencias aportadas en los documentos y soportes solicitados.

- En cuanto a la revisión de la ejecución y cumplimiento de los indicadores propuestos por la entidad y la Oficina Sistemas de Información TIC (Gestión Informática), se realiza una revisión del estado actual de los indicadores del año 2025 y para el 2026 a corte 31 de marzo, en la herramienta Almera, los cuales presentan un porcentaje de desarrollo o avance acorde a los tiempos establecidos, en la periodicidad definida. Para el año 2025, los indicadores ya se encuentran desarrollados en su totalidad y cuentan con los soportes de las actividades realizadas; para el año 2026, los indicadores han sido desarrollados, según la periodicidad definida y cuentan con los soportes de las actividades realizadas.

- Para la revisión del documento presentado y validar cumplimiento, con relación al MNGRSI - Gobierno digital – MinTIC; la Oficina Sistemas de Información TIC (Gestión Informática), aportó el documento: “AUTODIAGNÓSTICO SE SEGURIDAD DE LA INFORMACIÓN MINTIC 2025”, con el que soportan la presentación del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas (MNGRSI) - Gobierno digital, ante el MinTIC.

En la prueba de recorrido visitando algunas unidades, a través de la prueba se verifica que los usuarios a los cuales se les aplicó la prueba y se tomó evidencia, cuentan con usuario de dominio unipersonal, con el que realizan el ingreso a sus equipos de cómputo, a los sistemas de información de la entidad y la información pertinente alojada en sus equipos y repositorios local y web.

Mediante recorrido en las Unidades: ASDINGO, Sede Administrativa Cundinamarca, Sede Administrativa Puente Aranda, CDS Carvajal, Carvajal Archivo; se verifica con muestra aleatoria, el cumplimiento de la matriz de Roles y Perfiles de la entidad, aplicado a los usuarios de Dominio; así como también, se cuenta con el documento

Código 13-00-OD-0006 Matriz de Roles y Perfiles del Dominio V1, ubicado en el aplicativo Almera.

En la prueba Gestión Inventario de Activos e Infraestructura Critica: a través de la prueba se obtuvo el estado actual de los inventarios de equipos de la entidad, contenidos en los Activos e Infraestructura Critica, Activos de Información de la entidad y Equipos de Cómputo; obteniendo la información requerida, mediante los soportes aportados por la Oficina de Gestión Informática (Gestión de TICS), y de lo hallado en la página web de la Subred Integrada de Servicios de Salud Sur Occidente E.S.E., ruta referente (https://subredsuroccidente.gov.co/transparencia-y-acceso-a-la-informacion/datos-abiertos-2/7. Datos Abiertos/7.1 Instrumentos de gestión de la información/7.1.1 Registros de activos de información/Inventario de activos de información – 2025/Documento: Inventario de activos de información de la Subred Sur Occidente 2025; documentos que permiten dar cumplimiento a lo establecido por el Modelo de Seguridad y Privacidad de la información (MSPI).

En la prueba de Seguimiento a la implementación Política de Seguridad y Privacidad de la Información: a través de la prueba se identifica como se estableció y se está aplicando la política; la revisión de soportes y documentación aportada por la Oficina de Gestión Informática (Gestión de TICS), junto con la información publicada en Almera, se identifica que la gestión realizada a la Política de Gobierno Digital, esa llevada a cabo mediante los Indicadores PAA-13-05 Implementación de Gobierno Digital y Transformación Digital Subred Sur Occidente ESE é Indicador EQ ME GER INF 07 Porcentaje de cumplimiento del plan de acción para el manejo de Seguridad de la información Sub Red Sur Occidente ESE, se observa que la Política de Gobierno Digital, ha sido gestionada acorde a la planeación realizada, dando gestión a los indicadores mencionados y asociados en ella.

7. CONFORMIDADES

Evaluando el desarrollo y cumplimiento de las Fases del Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI, se observa lo siguiente:

Fase 1: Planificación

"Para el desarrollo de esta fase se deben utilizar los resultados de la fase anterior y proceder a elaborar el Plan de Seguridad y Privacidad de la Información, con el objetivo de que la entidad realice la planeación del tiempo, recursos y presupuesto de las actividades que va a desarrollar relacionadas con el MSPI."

7.1. Contexto
7.1.1. Comprensión de la organización y de su contexto
7.1.2. Necesidades y expectativas de los interesados
7.1.3. Definición del alcance del MSPI

La descripción e información pertinente a este numeral, se encuentra en el documentado Código 01-01-OD-0029 Política de seguridad y privacidad de la información V4.; documento que describe y caracteriza la política, con sus componentes y actividades a realizar, para el seguimiento y cumplimiento de esta,

7.2. Liderazgo

7.2.1. Liderazgo y Compromiso: Mediante la ejecución de la prueba documental de auditoría, se verificó que el Acuerdo No. 55 del 17 de octubre de 2019, en las páginas 28 a 31, establece de manera explícita que la Oficina de Sistemas de Información – TIC es la dependencia responsable de la seguridad de la información en la entidad, asignando dicha responsabilidad directamente al Jefe de la Oficina.

Esta disposición evidencia que la entidad ha definido formalmente la autoridad, liderazgo y compromiso institucional para la gestión de la seguridad de la información, en concordancia con los lineamientos del MSPI y los requisitos del numeral 7.2.1.

7.2.2. Política de seguridad y privacidad de la información: En la verificación realizada, se constató que la entidad cuenta con la Política de Seguridad y Privacidad de la Información, identificada con el Código 01-01-OD-0029, versión V4, la cual se encuentra publicada y disponible en la herramienta Almera.

La existencia y divulgación de este documento evidencian que la entidad ha formalizado su directriz institucional en materia de seguridad y privacidad de la información, cumpliendo con los requisitos establecidos en el numeral 7.2.2 del MSPI.

7.2.3. Roles y responsabilidades: En la verificación realizada, se evidenció que la entidad cuenta con documentación formal que define los roles y responsabilidades asociados a los sistemas de información y al acceso al dominio. Específicamente, se identificaron los documentos Código 13-04-OD-0002 “Roles sistema de información Dinámica Gerencial Agilsalud Almera V3” y Código 13-00-OD-0006 “Matriz de Roles y Perfiles del Dominio V1”, los cuales se encuentran publicados y disponibles en la herramienta Almera.

La existencia y disponibilidad de estos documentos permiten confirmar que la entidad ha establecido y documentado la asignación de roles, perfiles y permisos, cumpliendo con los requisitos del MSPI en materia de control de acceso y responsabilidades asociadas a la seguridad de la información.

7.3. Planeación

7.3.1. Identificación de activos de información e infraestructura critica cibernética: En la verificación realizada, se evidenció que la entidad cuenta con inventarios actualizados de los activos de información y de la infraestructura crítica cibernética. Para ello, se revisó el documento “inventario_activos_de_informacion_todos_los_procesos_2025”, publicado en la página web institucional, el cual consolida los activos de información de todos los procesos.

Adicionalmente, se constató la existencia del Inventario de Equipos – marzo 2026 y del Inventario de Servidores 2026, documentos que complementan la identificación y clasificación de los activos tecnológicos de la entidad.

La disponibilidad y actualización de estos inventarios permiten concluir que la entidad mantiene un registro formal y vigente de sus activos de información y de

infraestructura, cumpliendo con los requisitos establecidos por el MSPI para este componente.

7.3.2. Valoración de los riesgos de seguridad de la información: En la verificación realizada, se evidenció que la entidad cuenta con la valoración formal del riesgo asociado a la seguridad de la información, identificado como Riesgo Código 13013, el cual describe la *posibilidad de afectación económica y reputacional (incluida la vulneración de derechos humanos) por alteración de la seguridad, integridad, confidencialidad y disponibilidad de la información*, derivada de un ataque de ciberseguridad externo, un ataque de ingeniería social o la divulgación de información confidencial de los pacientes.

Asimismo, se constató que dicho riesgo posee cuatro controles implementados, los cuales se encuentran documentados y vigentes:

1. Plan de acción anual de seguridad y privacidad de la información, definido por la Oficina de Sistemas de Información – TICs y ejecutado conforme a la periodicidad establecida.
2. Consola de antivirus corporativa, utilizada para el seguimiento y monitoreo de amenazas que puedan comprometer la seguridad de la red institucional.
3. Acuerdos de niveles de servicio (SLA) incluidos en los contratos de red, que establecen tiempos y mecanismos de atención frente a fallas reportadas, con seguimiento permanente por parte de la entidad.
4. Procedimiento de gestión de copias de seguridad de bases de datos y sistemas de información (Código 13-00-PR-0002), orientado a salvaguardar la integridad de la información ante incidentes críticos que puedan afectar los sistemas misionales.

La existencia de este riesgo, junto con sus controles asociados, evidencia que la entidad realiza la identificación, análisis y tratamiento de riesgos de seguridad de la información, en cumplimiento de los lineamientos del MSPI y de la norma ISO/IEC 27001.

7.3.3. Plan de tratamiento de los riesgos de seguridad de la información: En la verificación realizada, se evidenció que la entidad cuenta con un plan formalmente establecido para el tratamiento de los riesgos de seguridad y privacidad de la información. Este se encuentra documentado en el Código 13-00-PL-0003 “Plan de tratamiento de riesgos de seguridad y privacidad de la información”, versión V5, el cual está publicado y disponible en la herramienta Almera.

La existencia y accesibilidad de este documento permiten concluir que la entidad ha definido las acciones, responsables y controles necesarios para gestionar los riesgos identificados, cumpliendo con los requisitos establecidos por el MSPI y la norma ISO/IEC 27001 en materia de tratamiento de riesgos.

7.4. Soporte

Durante la verificación realizada, se evidenció que la entidad cuenta con los documentos de soporte necesarios para la gestión de la seguridad y privacidad de la información, los cuales se encuentran formalmente publicados y disponibles para consulta. Entre estos soportes se identificaron:

- Código 02-01-FO-0013 – Plan de Trabajo de Seguridad y Privacidad de la Información, I Trimestre 2026, que evidencia la programación y seguimiento de actividades operativas.
- Código 13-00-OD-0005 – Plan de Acción para el Tratamiento de Riesgos de Seguridad y Privacidad de la Información, que soporta la ejecución de acciones orientadas a mitigar los riesgos identificados.
- Código 13-00-PL-0003 – Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, versión V5, que establece las medidas y controles definidos para la gestión de riesgos.

La existencia y disponibilidad de estos documentos permiten concluir que la entidad cuenta con los elementos de soporte requeridos para la implementación y seguimiento del MSPI, en cumplimiento de los lineamientos establecidos para este componente.

7.4.1. Recursos: En la verificación realizada, se evidenció que la entidad cuenta con los recursos documentales necesarios para soportar la implementación y seguimiento del Modelo de Seguridad y Privacidad de la Información (MSPI), los cuales se encuentran formalmente definidos y disponibles en los repositorios institucionales. Entre los recursos identificados se encuentran:

- Para los numerales 7.1.3 Definición del alcance del MSPI y 7.2.2 Política de seguridad y privacidad de la información, se constató la existencia del documento Código 01-01-OD-0029 – Política de Seguridad y Privacidad de la Información V4, publicado en Almera.
- Para el numeral 7.2.3 Roles y responsabilidades, se verificó la disponibilidad de los documentos Código 13-04-OD-0002 – Roles del sistema de información Dinámica Gerencial Agilsalud Almera V3 y Código 13-00-OD-0006 – Matriz de Roles y Perfiles del Dominio V1, ambos publicados en Almera.
- Para el numeral 7.3.3 Plan de tratamiento de los riesgos de seguridad de la información, se evidenció el documento Código 13-00-PL-0004 – Plan de Acción de Seguridad y Privacidad de la Información V6, que soporta la gestión de los controles y actividades definidas.
- En relación con la matriz de riesgos de seguridad y privacidad de la información, se verificó la existencia del Riesgo Código 13013, que describe la posibilidad de afectación económica y reputacional por incidentes de ciberseguridad, y que cuenta con cuatro controles implementados para su mitigación.
- Para los inventarios de activos de información, sistemas de información e infraestructura tecnológica, se constató la disponibilidad del documento inventario_activos_de_informacion_todos_los_procesos_2025, publicado en la página web institucional, así como del Inventario de Equipos – marzo 2026 y el Inventario de Servidores 2026, los cuales complementan la identificación y administración de los activos tecnológicos.

La existencia y accesibilidad de estos recursos permiten concluir que la entidad cuenta con los insumos documentales necesarios para soportar la gestión del MSPI, en cumplimiento de los lineamientos establecidos por MinTIC y la norma ISO/IEC 27001.

7.4.2. Competencia, toma de conciencia y comunicación: En la verificación realizada, se evidenció que las actividades relacionadas con la competencia, toma de conciencia y comunicación en materia de seguridad y privacidad de la información se

desarrollan en el marco de los Comités Institucionales de Gestión y Desempeño Institucional.

Se constató que el comité más reciente tuvo lugar en marzo de 2026, y como soporte de esta actividad se revisó la presentación elaborada por la Oficina de Sistemas de Información TIC (Gestión Informática), en la cual se socializan los avances, responsabilidades y lineamientos asociados al MSPI.

Lo anterior permite concluir que la entidad realiza acciones formales de comunicación y sensibilización, cumpliendo con los requisitos establecidos para este componente del MSPI.

7.4.3. Información documentada: En la verificación realizada, se evidenció que la entidad dispone de la información documentada requerida para la gestión del Modelo de Seguridad y Privacidad de la Información (MSPI). La documentación pertinente se encuentra alojada en la página web institucional y en el aplicativo Almera, lo que garantiza su disponibilidad y acceso para los actores responsables.

Adicionalmente, se revisaron los soportes suministrados por la Oficina de Sistemas de Información TIC (Gestión Informática), los cuales complementan y respaldan la información publicada en los repositorios oficiales.

Con lo anterior, se concluye que la entidad mantiene organizada, accesible y actualizada la información documentada necesaria, cumpliendo con los requisitos establecidos para este componente del MSPI.

Fase 2: Operación

"Tras finalizar la fase 7 de planeación del MSPI, se iniciará la implementación de los procesos de seguridad de la información: gestión de activos, riesgos, incidentes, vulnerabilidades, tratamiento y evaluación de controles. Se fomentará la cultura de seguridad y se definirán criterios de cumplimiento y mecanismos de control para procesos y servicios externos relevantes, asegurando su alineación con el SGSI."

8.1. Control y planeación operacional: En la verificación realizada, se evidenció que la entidad cuenta con la documentación necesaria para soportar las actividades de control y planeación operacional del Modelo de Seguridad y Privacidad de la Información (MSPI), conforme a los lineamientos establecidos por MinTIC y la norma ISO/IEC 27001.
Se identificó lo siguiente:

- Respecto al numeral 7.3.2 Valoración de los riesgos de seguridad de la información, se constató la existencia del Riesgo Código 13013, que describe la posibilidad de afectación económica y reputacional por incidentes de ciberseguridad, el cual se encuentra publicado en Almera y cuenta con controles definidos para su mitigación.
- Para el numeral 7.3.3 Plan de tratamiento de los riesgos de seguridad de la información, se verificó el documento Código 13-00-PL-0003 – Plan de tratamiento de riesgos de seguridad y privacidad de la información V5, que establece las acciones y controles orientados a gestionar los riesgos identificados.
- En relación con el Plan de Seguridad y Privacidad de la Información, se evidenció el documento Código PRIV_INF_2026, publicado en Almera, el cual define la

implementación de controles de seguridad e incluye actividades, fechas, responsables y presupuesto, cumpliendo con los requisitos mínimos establecidos para este componente.

- La implementación de los controles de seguridad y privacidad se encuentra soportada mediante el Indicador Código EQ ME GER INF 07 – Porcentaje de cumplimiento del plan de acción para el manejo de Seguridad de la Información, disponible en Almera, donde se evidencian las actividades ejecutadas y sus respectivos soportes.

Con lo anterior, se concluye que la entidad cuenta con los elementos documentales y operativos necesarios para la gestión, implementación y seguimiento de los controles del MSPI, cumpliendo con los requisitos establecidos para la fase de operación.

8.2. Plan de tratamiento de riesgos: En la verificación realizada, se evidenció que la entidad gestiona el plan de tratamiento de riesgos de seguridad de la información mediante el Riesgo Código 13013, el cual describe la *posibilidad de afectación económica y reputacional (incluida la vulneración de derechos humanos) por alteración de la seguridad, integridad, confidencialidad y disponibilidad de la información*, derivada de un ataque de ciberseguridad externo, un ataque de ingeniería social o la divulgación de información confidencial de los pacientes.

Este riesgo se encuentra publicado en la herramienta Almera y cuenta con controles definidos para su mitigación, lo que permite concluir que la entidad realiza la gestión del tratamiento de riesgos conforme a los lineamientos del MSPI y la norma ISO/IEC 27001.

8.3. Definición de indicadores de gestión: En la verificación realizada, se evidenció que la entidad ha definido indicadores de gestión para el seguimiento y evaluación de las actividades relacionadas con la seguridad de la información, conforme a los lineamientos del MSPI.

Específicamente, se constató la existencia del Indicador Código EQ ME GER INF 07 – Porcentaje de cumplimiento del plan de acción para el manejo de Seguridad de la Información Subred Sur Occidente ESE, el cual se encuentra publicado en la herramienta Almera.

Dentro del indicador se revisaron las actividades programadas y ejecutadas, así como los soportes asociados, evidenciándose que la entidad realiza seguimiento sistemático al avance del plan de acción y a la implementación de los controles definidos.

Con lo anterior, se concluye que la entidad cuenta con indicadores formales y mecanismos de seguimiento que permiten evaluar el desempeño de la gestión de seguridad de la información, en cumplimiento de los requisitos establecidos para este componente del MSPI.

Fase 3: Evaluación de desempeño

"Una vez culminada las actividades de la fase de operación del MSPI, se evalúa la efectividad de las acciones tomadas a través de los indicadores definidos en la fase de implementación que debe incluir la correcta interacción entre el MSPI, MIPG y los requerimientos de la Ley 1581 de 2012 "Protección de datos personales", Ley 1712 de

2014 "Ley de Transparencia y Acceso a la Información Pública", Decreto 2106 de 2019 o cualquier norma que las reglamente, adicione, modifique o derogue."

9.1. Seguimiento, medición, análisis y evaluación: En la verificación realizada, se evidenció que la entidad realiza actividades de seguimiento, medición, análisis y evaluación de la gestión de seguridad de la información, soportadas principalmente en dos elementos documentales publicados en la herramienta Almera:

- El Riesgo Código 13013, que describe la posibilidad de afectación económica y reputacional —incluida la vulneración de derechos humanos— por alteraciones a la seguridad, integridad, confidencialidad y disponibilidad de la información, derivadas de ataques de ciberseguridad externos, ingeniería social o divulgación de información confidencial de los pacientes. Dentro de este riesgo se revisaron las actividades ejecutadas y los controles implementados, junto con sus respectivos soportes.
- El Indicador Código EQ ME GER INF 07 – Porcentaje de cumplimiento del plan de acción para el manejo de Seguridad de la Información, en el cual se evidencian las actividades programadas, su nivel de avance y los soportes que demuestran su ejecución.

La revisión de estos elementos permitió concluir que la entidad cuenta con mecanismos formales para evaluar el desempeño de la gestión de seguridad de la información, asegurando el seguimiento sistemático de los riesgos y del cumplimiento del plan de acción, en concordancia con los lineamientos del MSPI y la norma ISO/IEC 27001.

9.2. Auditoría Interna: En la verificación realizada, se evidenció que la entidad cuenta con antecedentes de evaluación interna del Modelo de Seguridad y Privacidad de la Información (MSPI). Este componente se encuentra soportado en el Informe de Auditoría OCI-SISSSO-IL-2025-16, correspondiente a la *Evaluación y seguimiento a la implementación y cumplimiento del MSPI*, realizado en junio de 2025.

La existencia de este informe demuestra que la entidad ha ejecutado procesos previos de auditoría interna, lo cual contribuye al seguimiento continuo, la mejora del sistema y el cumplimiento de los lineamientos establecidos por MinTIC y la norma ISO/IEC 27001.

9.3. Revisión por la dirección: En la verificación realizada, se evidenció que la entidad cuenta con la Política y el Manual de Seguridad y Privacidad de la Información debidamente actualizados, documentos que deben ser revisados y aprobados por el Comité de Gestión y Desempeño Institucional o, en su defecto, por decisión del nominador, conforme a los lineamientos del MSPI y a las necesidades de las partes interesadas.

Se constató la existencia de los siguientes documentos:

- Política de Seguridad y Privacidad de la Información V4, Código 01-01-OD-0029, con fecha 2021-07-09.
- Manual de Seguridad de la Información V7, Código 13-00-MA-0001, con fecha 2026-02-13.

Durante la revisión se identificó que, para completar la trazabilidad del proceso de aprobación, se requiere solicitar a Desarrollo Institucional las actas de los Comités de Gestión y Desempeño Institucional en las cuales dichos documentos fueron aprobados formalmente.

Con lo anterior, se concluye que la entidad cuenta con la documentación actualizada, pero se requiere complementar la evidencia de aprobación por parte de la alta dirección, conforme a los requisitos del MSPI.

Fase 4: Mejoramiento continuo

"Una vez culminadas las actividades del MSPI de la fase evaluación y desempeño, se deben consolidar los resultados obtenidos de la fase de evaluación de desempeño y diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas."

10.1. Mejora continua
10.2. Acciones Correctivas y no conformidades

En la verificación realizada, se evidenció que la entidad mantiene acciones orientadas al mejoramiento continuo del Modelo de Seguridad y Privacidad de la Información (MSPI).

El auditado informó que la Política de Seguridad y Privacidad de la Información se encuentra actualmente en proceso de aprobación, sustentada en el acta del comité desarrollado en mayo de 2026, lo cual demuestra la actualización y revisión periódica de los lineamientos institucionales en materia de seguridad de la información.

Con lo anterior, se concluye que la entidad adelanta actividades de revisión y actualización de sus documentos estratégicos, en concordancia con los requisitos del MSPI y los principios de mejora continua.

8. OTRAS SITUACIONES U OBSERVACIONES

Durante el desarrollo de la auditoría, aun cuando se verificó el cumplimiento general de los requisitos establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI) en sus diferentes temáticas y fases, se identificaron las siguientes observaciones que deben ser consideradas para fortalecer la trazabilidad y formalización del modelo:

1. Fase 3: Evaluación de desempeño – Numeral 9.3 Revisión por la dirección
Se constató que la entidad cuenta con la Política de Seguridad y Privacidad de la Información V4, Código 01-01-OD-0029 (fecha 2021-07-09), y con el Manual de Seguridad de la Información V7, Código 13-00-MA-0001 (fecha 2026-02-13).

Sin embargo, no se dispone actualmente de las actas de los Comités de Desarrollo Institucional en las cuales dichos documentos fueron revisados y aprobados, lo cual limita la evidencia formal del proceso de validación por parte de la alta dirección.

2. Fase 4: Mejoramiento continuo

El auditado informó que la Política de Seguridad y Privacidad de la Información se encuentra en proceso de aprobación y normalización, sustentada en el comité de desarrollo institucional realizado en mayo de 2026.

No obstante, no se cuenta aún con las actas correspondientes que respalden formalmente la aprobación de este documento, lo cual constituye una situación a subsanar para garantizar la trazabilidad del proceso de mejora continua.

9. CONCLUSIÓN GENERAL

Con base en la revisión documental y en las pruebas de auditoría realizadas, se concluye que la Subred Integrada de Servicios de Salud Sur Occidente E.S.E. cumple con los lineamientos definidos en el Modelo de Seguridad y Privacidad de la Información (MSPI), particularmente en los componentes evaluados: roles y responsabilidades, gestión de incidentes, indicadores de gestión, gestión del riesgo de seguridad de la información e inventario de activos.

Durante la verificación se evidenció que la entidad cuenta con mecanismos adecuados para la administración de accesos, la gestión de activos de información y el seguimiento a la implementación de la Política de Seguridad y Privacidad de la Información. Asimismo, se destaca la gestión apropiada de los indicadores asociados a la seguridad de la información, los cuales presentan un avance acorde con la planeación institucional establecida.

En consecuencia, se considera que la entidad mantiene un nivel adecuado de cumplimiento frente a los requisitos del MSPI, demostrando una gestión organizada, documentada y alineada con los lineamientos normativos aplicables.

Recomendaciones:

- Mantener la actualización periódica de la documentación del MSPI conforme a cambios normativos, tecnológicos o institucionales.
- Fortalecer el monitoreo preventivo de incidentes de seguridad, aun en ausencia de eventos reportados, para anticipar riesgos emergentes.
- Continuar con las actividades de sensibilización institucional en temas de seguridad y privacidad de la información, promoviendo la cultura organizacional en esta materia.
- Asegurar la trazabilidad y actualización continua del inventario de activos de información, garantizando su correspondencia con los sistemas, procesos y responsables actuales.

Durante la revisión y evaluación realizada, no se identificaron hallazgos. Con base en la documentación aportada, así como en las evidencias y soportes obtenidos durante el desarrollo de la auditoría y la aplicación de las respectivas pruebas, se observó que la entidad cumple con los ítems establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI).

La información revisada demuestra que los requisitos evaluados se encuentran implementados y soportados adecuadamente, sin que se presenten novedades, desviaciones o incumplimientos frente a los criterios definidos.

Bogotá D.C., 28 de mayo de 2026

Guillermo Cerón Sandoval
Jefe Oficina de Control Interno

Elaboró: *Jorge Orlando Sánchez Alcalá, Profesional Especializado I*

Revisó: *Guillermo Cerón Sandoval, Jefe Oficina de Control Interno*