BOGOTÁ | SUBRED INTEGRADA DE SERVICIOS DE SALUD SUR OCCIDENTE ESE

NOTA INTERNA
SSO-2025-240-005482-3

Bogotá, 30 de septiembre de 2025

DE: **CLAUDIA PATRICIA QUINTERO COMETA**
JEFE DE CONTROL INTERNO
OFICINA DE CONTROL INTERNO

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

Asunto: Alcance - Informe de Evaluación y Seguimiento a la implementación y cumplimiento del Modelo de Seguridad y Privacidad de la Información -MSPI emitido el 29/06/2025.

Respetada doctora Andrea, cordial saludo.

De conformidad con lo requerido por el Comité Institucional de Coordinación del Sistema de Control Interno en sesión ordinaria 02-2025 llevada a cabo el 05/08/2025 y registrado en el acta correspondiente, la Oficina de Control Interno procedió a realizar de nuevo la validación, análisis y/o ajustes solicitados al contenido del Informe OCI-SISSSO-IL-2025-16 Evaluación y seguimiento a la implementación y cumplimiento del Modelo de Seguridad y Privacidad de la Información - MSPI inicialmente emitido el 29/06/2025, y comunicado al comité mediante oficio con radicado Ágilsalud SSO-2025-240-003910-3 de la misma fecha.

Es importante mencionar que, el Comité Institucional de Coordinación del Sistema de Control Interno "*como órgano asesor e instancia decisoria en los asuntos del control interno*" (Decreto 1083 de 2015, Art. 2.2.21.1.5) en la Subred Sur Occidente, tiene dentro de sus funciones "*servir de instancia para resolver las diferencias que surjan en desarrollo del ejercicio de auditoría interna"*, tal como lo establece el numeral 6 del artículo 6° de la Resolución interna 0391 de 2022 y el literal "e" del artículo 2.2.21.1.6 del Decreto 1083 de 2015

Con los nuevos resultados obtenidos, esta oficina procedió a dar **Alcance** al Informe OCI-SISSSO-IL-2025-16 **Evaluación y Seguimiento a la implementación y cumplimiento del Modelo de Seguridad y Privacidad de la Información - MSPI**, por lo que, adjunto remito de nuevo el **Informe N° OCI-SISSSO-IL-2025-16** dando cumplimiento al 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 Auditoria y/o Junta Directiva, (…)*" (Subrayado fuera de texto).

Es importante precisar que, la Oficina de Control Interno desarrolla las actividades de auditoría interna bajo los principios de independencia, objetividad y enfoque basado en riesgos, en cumplimiento de los roles asignados en el Decreto 648 de 2017 y conforme lo establecido en la Ley 87 de 1993, la Guía de auditoría Interna para entidades públicas y la Guía rol de las Oficinas de Control Interno (Función Pública, 2023). El propósito de esta labor es aportar valor a la gestión institucional mediante la evaluación de controles, riesgos y cumplimiento normativo.

Agradezco su acostumbrado respaldo en nuestra labor de auditoría, 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,

CLAUDIA PATRICIA QUINTERO COMETA
JEFE DE CONTROL INTERNO

Anexos: Informe OCI-SISSSO-IL-2025-16 Alcance - Evaluación y Seguimiento a la implementación y cumplimiento del Modelo de Seguridad y Privacidad de la Información - MSPI

Copia a: Marcia Greicy Gucaneme Valbuena - 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 Asesora 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)
Jeansy Milena Ramírez Martínez - Jefe Oficina de Calidad (Miembro CICSCI)
Ruby Liliana Cabrera Calderón - 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:	CLAUDIA PATRICIA QUINTERO COMETAOCIOCI
Revisado por:	CLAUDIA PATRICIA QUINTERO COMETA / OCI
Elaborado por:	MARTHA PATRICIA PALOMINO RAMIREZ / OCI

N° INFORME: OCI-SISSSO-IL-2025-16

NOMBRE TRABAJO DE AUDITORÍA: **Alcance** - Evaluación y 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
- Bertha Lucía Mora Quiñones, Subgerente Prestación de Servicios de Salud
- Ruby Liliana Cabrera Calderón, Subgerente Corporativa
- Marcia Greicy Guacaneme Valbuena, jefe Oficina Asesora de Desarrollo Institucional
- Jeansy Milena Ramírez Martínez, jefe Oficina de Calidad
- Julio Alfonso Peñuela Saldaña, jefe Oficina Jurídica
- Carmen Esther Acero García, jefe Oficina Asesora de Comunicaciones
- Rosa Viviana Cubillos Medrano, jefe Oficina Participación Comunitaria y Servicio Ciudadano
- Hernando Miguel Mojica Mugno, jefe Oficina de Sistemas de Información - TIC

EMITIDO POR: Claudia Patricia Quintero Cometa, jefe Oficina de Control Interno

EQUIPO AUDITOR: Jorge Orlando Sánchez Alcalá, Profesional Especializado (OPS)

I. OBJETIVO

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*."

[1] Parágrafo 1° del Artículo 2.2.21.4.7 del Decreto 1083 de 2015 (modificado por el Artículo 1 del Decreto 338 de 2019). Parágrafo 1. "*Los informes de auditoría, seguimientos y evaluaciones 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, (…)*".

II. ALCANCE

Esta auditoría interna de cumplimiento comprendió la revisión documental aportada por la Oficina de Sistemas de Información, que soporta el cumplimiento o adaptación de los habilitadores y/o propósitos relacionados con el Modelo de Seguridad y Privacidad de la Información - MSPI.

Período auditado: 1 de enero de 2024 a 31 de marzo de 2025.

***Nota**: El establecimiento de este período no limitaba 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.*

Justificación de alcance a Informe OCI-SISSSO-IL-2025-16 emitido inicialmente el 29/06/2025 y comunicado a la Representante Legal de la Subred Sur Occidente mediante oficio con radicado Ágilsalud SSO-2025-240-003910-3 de la misma fecha y a los demás integrantes del Comité Institucional de Coordinación del Sistema de Control Interno.

En sesión ordinaria del Comité Institucional de Coordinación del Sistema de Control Interno llevada a cabo el 05/08/2025, se presentaron las siguientes situaciones, las cuales se encuentran debidamente registradas en el Acta 02-2025 de dicho comité, así:

Punto 5 del orden del día: "*Presentación de resultados de las auditorías internas*".

- *"**De cumplimiento**. Seguimiento al cumplimiento del Modelo de Seguridad y Privacidad de la Información.*

(…).

En este punto le fue concedida la palabra a la doctora Claudia Quintero, en calidad de jefe de la Oficina de Control Interno, quien inició su exposición manifestando que este tema se incluyó en el orden del día por las diferencias que surgieron entre el auditado (líder de la actividad o proceso auditado) y el equipo auditor, en el desarrollo de los trabajos de auditoría antes mencionados, teniendo en cuenta que, es función del Comité Institucional de Coordinación del Sistema de Control Interno "servir de instancia para resolver las diferencias que surjan en desarrollo del ejercicio de auditoría interna", tal como lo establece el numeral 6 del artículo 6° de la Resolución 0391 de 2022 y el literal e del artículo 2.2.21.1.6 del Decreto 1083 de 2015.

(…).

(…), la doctora Claudia Quintero manifestó a los miembros del comité que, más allá de evaluar la gestión operativa de la Subred, su gestión financiera o los resultados obtenidos en un período, es labor de la Oficina de Control Interno evaluar el desempeño y/o funcionamiento del Sistema de Control Interno, es decir, que esté presente y funcionando. Presente se refiere a que todos los controles estén documentados en sus procedimientos, instructivos, políticas, etc., al igual que éstos se revisen y

actualicen de conformidad con las normas internas y externas; y funcionando se refiere a que los controles se ejecuten tal como están diseñados o documentados.

Seguidamente, la jefe de la Oficina de Control Interno informó a los miembros del comité que, aunque se llevaron a cabo mesas de trabajo con los auditados para aclarar dudas e inquietudes sobre el contenido del informe preliminar de las auditorías mencionadas, antes de emitir el informe final, una vez recibidas las respuestas del auditado junto con las evidencias (en los casos aplicables), y analizadas por el equipo auditor, los resultados y/o conclusiones registrados por la Oficina de Control Interno en el informe final de cada auditoría continúan presentando diferencias con el criterio del auditado o con los resultados que éste considera deben registrarse en tales informes, situaciones que generaron los siguientes eventos:

(…).

Terminada la exposición, la doctora Andrea Hurtado (presidente del comité) manifestó que esta es una alternativa viable para lograr resolver las diferencias que aún persisten en las auditorías internas objeto de discusión, por lo que, manifiesta solicitar a la jefe de la Oficina de Control Interno la revisión del contenido del informe final (…) del seguimiento al cumplimiento del Modelo de Seguridad y Privacidad de la Información (…), precisando que, no existe el interés de ejercer presión sobre las decisiones y/o resultados obtenidos en las auditorías, el ejercicio de auditoría es totalmente independiente, pero en aras del debido proceso y hacer uso de los canales de comunicación abiertos en los que se ha escuchado a las partes y puesto sobre la mesa estas situaciones, es importante aprovechar estas alternativas de solución.

(…), el comité aprobó requerir a la Oficina de Control Interno realizar las gestiones necesarias para efectuar los ajustes y/o modificaciones a los tres (3) informes de auditoría mencionados en el párrafo anterior, dando alcance mediante un nuevo informe, de acuerdo con los resultados que se obtengan de la revisión y análisis de la información y soportes, igualmente indicados en el párrafo anterior."

Por lo antes descrito, y en atención al requerimiento del Comité Institucional de Coordinación del Sistema de Control Interno "*como órgano asesor e instancia decisoria en los asuntos del control interno*" (Decreto 1083 de 2015, Art. 2.2.21.1.5), la Oficina de Control Interno procedió a realizar de nuevo la validación, análisis y/o ajustes solicitados al contenido del informe inicialmente emitido el 29/06/2025, con cuyos resultados generó este nuevo informe de alcance.

III. MARCO NORMATIVO

- **Ley 1273 de 2009** (enero 5) "*Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones*".

- **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*"

- **Ley 1952 de 2019** (enero 28) "*Por medio de la cual se expide el código general disciplinario se derogan la ley 734 de 2002 y algunas disposiciones de la ley 1474 de 2011, relacionadas con el derecho disciplinario*". **Artículo 38**. "*Son deberes de todo servidor público: (…). 5. Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función en forma exclusiva para los fines a que están afectos. 6. Custodiar y cuidar la documentación que, por razón de su empleo, cargo o función, conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos."* **Artículo 62.** *"Faltas relacionadas con la moralidad pública. (…). 4. Atentar con cualquier propósito, contra la inviolabilidad de la correspondencia y demás formas de comunicación, u obtener información o recaudar prueba con desconocimiento de los derechos y garantías constitucionales y legales. 5. Causar daño a los equipos estatales de informática, alterar, falsificar, introducir, borrar, ocultar o desaparecer información en cualquiera de los sistemas de información oficial contenida en ellos y en los que se almacene o guarde la misma, o permita el acceso a ella a personas no autorizadas."*

- **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*".

IV. METODOLOGÍA

De conformidad con el Plan Anual de Auditoría de la vigencia 2025 aprobado por el Comité Institucional de Coordinación del Sistema de Control Interno de la Subred Integrada de Servicios de Salud Sur Occidente E.S.E. (en adelante, Subred Sur Occidente), la Oficina de Control Interno mediante oficio con radicado Ágilsalud SSO-2025-240-001793-3 de fecha 26/03/2025 informó a la Oficina de Sistemas de Información TICs el inicio del Seguimiento a la implementación y cumplimiento del Modelo de Seguridad y Privacidad de la Información - MSPI en la Subred Sur Occidente comparado con los lineamientos de la norma NTC: ISO/IEC 27001; modelo propuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, alineado con el Marco de Referencia de Arquitectura TI (Tecnología de Información), el cual soporta transversalmente los componentes de la Política de Gobierno Digital.

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 PARA 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.

TEMA(S)	REQUISITOS NORMATIVOS PARA VERIFICAR	INSUMO(S) PARA VALIDAR EL CUMPLIMIENTO DEL REQUISITO NORMATIVO
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.

V. DESCRIPCIÓN DEL TRABAJO REALIZADO, OBSERVACIONES Y RECOMENDACIONES

Se revisa la documentación remitida por la Oficina Sistemas de Información TIC y requerida por la Oficina de Control Interno para evaluar los siguientes parámetros o temas:

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

En la revisión de la documentación, se identificó y evaluó las dimensiones del MSPI, como también se analizó la gestión de la entidad. En la evaluación y seguimiento se obtuvieron los resultados detallados a continuación por cada parámetro o tema:

a. Roles y Responsabilidades

Dentro de lo evaluado en este ítem, tenemos: Norma ISO/IEC 27001 Anexo A. Ítem A.6.1.1. Roles y responsabilidades para la seguridad de la información; y 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.

Sobre el particular, la Oficina de Control Interno solicitó documentación y soportes relacionados con: i) Matriz de roles y perfiles en los sistemas de información y, ii) Matriz de roles y perfiles de acceso al dominio en estaciones de trabajo.

- Al verificar la definición y asignación de todas las responsabilidades de la seguridad de la información, según la información aportada, se observó que se cuenta con un documento de Roles sistema de información Dinámica Gerencial, Almera y Ágilsalud (Código 13-04-OD-0002) versión 3 de fecha 07/04/2025. Al respecto, en el Plan Estratégico de Tecnología de la Información y las Comunicaciones - PETIC, en el ítem 9.2.3 "*Estructura organizacional de TI*" se observó la descripción de las funciones generales de la Oficina de Sistemas de Información estableciendo su operación por equipos de trabajo mediante coordinaciones, entre ellas, la coordinación de Infraestructura TI que tiene la función de seguridad de la información, la Coordinación HIS que tiene por función brindar adecuada articulación con las políticas de seguridad de la información, en cuanto a la accesibilidad al HIS y confidencialidad de la historia clínica; aunque el responsable directo de la seguridad es el jefe de la Oficina de Sistemas de Información, quien según el Manual de Funciones y Competencias Laborales establecido en el Acuerdo 055 de 2019 (página 29) tiene la siguiente: "*3. Dirigir, administrar e implementar las políticas, programas y proyectos en materia de desarrollo, modernización y tecnología informática que garanticen la seguridad de los sistemas de información de la Subred, de conformidad con los procesos y procedimientos establecidos".*

  Se verifica la documentación aportada por la Oficina de Sistemas y también la que ha sido cargada en el aplicativo Almera, identificando el Catálogo de sistemas de información (Código 13-02-FO-0008) versión 2 de fecha 14/04/2025, en el que relacionan un listado de software y aplicaciones empleadas por la institución, de los cuales no se identificó una Matriz de Roles y Perfiles para los usuarios interventores en cada una de las aplicaciones o software.

  Análisis de observaciones y/o respuesta del auditado. Mediante correo electrónico del 20/06/2025, la Oficina de Sistemas informó:

"El 7 de abril quedo normalizado el documento de roles y perfiles de Dinámica, Ágilsalud y Almera. En el mes de enero había quedado solo el de Dinámica.

Las matrices de roles y perfiles se hacen para los sistemas críticos o regulados trazadores para la entidad, los sistemas de información de menor importancia o uso no requieren la especificación de roles y perfiles, esto se define en el modelo RBAC (Control de acceso basado en roles). Por favor indicar la norma distrital o nacional que contraviene esta metodología definida y utilizada internacionalmente."

Pronunciamiento de la OCI: Estos aspectos se encuentran relacionados en la Norma ISO/IEC 27001 Anexo A. Ítem A.6.1.1. Roles y responsabilidades para la seguridad de la información; y 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.

Continua el informe de auditoría:

Se identifican las siguientes aplicaciones o software: 1) Hosvital; 2) Seven; 3) Kactus; 4) SIIES; 5) HIMS; 6) INNOVADOC; 7) SICHOK; 8) Vacunación - PAIWEB; 9) Reuso Odontología; 10) Reuso Terapia Respiratoria; 11) Censo de Camas APP; 12) Censo de Camas Aplicación Web; 13) Epidemiologia - BAI (Búsqueda Activa Institucional); 14) TSH; 15) Dashboard CDA's; 16) Dashboard TSH; 17) Dashboard HelpDesk; 18) HIPÓCRATES, entre otros derivados de estos mismos. Esta situación evidencia que la Matriz de Roles y Perfiles está incompleta y requiere ser actualizada.

Análisis de observaciones y/o respuesta del auditado. Mediante correo electrónico del 20/06/2025, la Oficina de Sistemas informó:

"La mayoría de estas aplicaciones son históricas y por ende solo se tiene usuarios de consulta.

Efectivamente los sistemas de los Hospitales anteriores son herramientas de solo consulta que hoy día no son objeto ni de parametrización ni de registro dado que no son las herramientas actuales de operación, esto se explicó al auditor pero la observación realizada indica que no fue entendida la explicación."

Pronunciamiento de la OCI: La actividad por realizar es la depuración del listado identificado como Catálogo de sistemas de información (Código 13-02-FO-0008) versión 2 de fecha 14/04/2025 y del cual, una vez realizada la depuración de los software o aplicaciones que no se estén utilizando, deben incluir los que si están siendo utilizados, así sea de consulta, en la matriz de roles y permisos.

Continua el informe de auditoría:

Sumado a lo anterior, no se observó una matriz o política de asignación de usuarios y

contraseñas de dominio, como tampoco la disposición de una cuenta de correo institucional para algunos colaboradores, lo que hace que utilicen cuentas de correo personal, toda vez que, se identificó en los hospitales visitados que algunos usuarios ingresaban a los equipos de cómputo con usuario y contraseña de **dominio genérico**. Esta situación genera una brecha de seguridad en el tráfico y trato de la información que facilita su manipulación en los procesos, causando una posible vulnerabilidad en la seguridad informática y de la información de la institución, que puede generar materialización de riesgos económicos y/o reputacionales, causando pérdidas a la entidad.

Respuesta, justificación y/o comentarios del auditado. Mediante correo electrónico del 20/06/2025, la Oficina de Sistemas informó:

"Se cuenta con el 13-00-PR-0003 Procedimiento gestión de usuarios y contraseñas.

La entidad no cuenta con el recurso económico para que cada colaborador tenga una cuenta de correo.

No es viable y no corresponde a cada colaborador de planta, menos aun de OPS la asignación de una cuenta de correo corporativa, en primer lugar, debido a que la inversión para lograr esto superaría la capacidad de recursos de la entidad, y principalmente por que la totalidad de colaboradores no tiene funciones que hagan obligatoria la asignación de cuentas de correo, por favor, indicar la norma distrital o nacional que define la obligatoriedad de dar a cada colaborador una cuenta de correo.

Solo utilizan usuarios de dominio genéricos quienes cambian de turnos frecuentemente y no guarda información importante en el equipo ya que solo trabaja en Dinámica o páginas de consultas. Adicional, por tantos cambios frecuentes de personal debido a variables como el tipo de contrato OPS, el cual no hay una estabilidad laboral. Sin embargo, los usuarios al sistema de información Dinámica cada uno tiene su usuario personalizado."

Pronunciamiento de la OCI: Mediante la Resolución 500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) se adoptó el Modelo de Seguridad y Privacidad de la Información (MSPI) en Colombia, con el objeto de establecer los lineamientos generales para la implementación de dicho modelo, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, entre otros aspectos. En referencia, se puede observar el contenido de la Resolución 2239 de 2024 "*Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación del Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, (…)*", que indica en el Capítulo VII. *"Responsabilidades de los colaboradores frente al uso de los servicios tecnológicos"*, Artículo 22. *"Política de Seguridad Digital*", lo siguiente: "*Todos los empleados públicos o contratistas que hagan uso de los recursos tecnológicos del Ministerio de Tecnologías de la Información y las Comunicaciones tienen la responsabilidad de cumplir*

cabalmente las políticas establecidas para su uso aceptable; entendiendo que el uso no adecuado de los recursos pone en riesgo la continuidad de la operación de los servicios y por ende, el cumplimento de la misión institucional. Para ello, deben acatar las siguientes disposiciones: a. Del uso del ***correo*** *electrónico. El* ***correo*** *electrónico institucional es una herramienta de apoyo a la ejecución de funciones y obligaciones de los empleados públicos y contratistas del Ministerio/Fondo Único de TIC, cuyo uso se facilitará en los siguientes términos: (…)",* por ejemplo, aborda temas de seguridad y confidencialidad en el manejo de información, donde el correo electrónico institucional podría ser un componente relevante.

En cuanto al uso de usuarios de dominio genéricos, en áreas administrativas o de apoyo, que no son asistenciales de cara al paciente o usuario, se recomienda validar el estado actual y proceder con la pertinente creación de usuarios para los colaboradores que actualmente están ingresando a los equipos con usuarios genéricos, caso particular, colaboradores de la Oficina de Control Interno.

Continua el informe de auditoría:

La situación antes descrita evidencia inobservancia de la Resolución 500 de 2021 *"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital",* siendo este el marco normativo principal para definir los roles y responsabilidades dentro del MSPI en Colombia.

- Al analizar las políticas, procedimientos, manuales y matrices que la Entidad tenga definidas para la asignación de los roles y perfiles en los sistemas de información y acceso al dominio en estaciones de trabajo para el acceso a la información, no se evidenció Políticas de dominio y en consola de administración del antivirus y Políticas de Seguridad Firewall establecidas y normalizadas, toda vez que, los documentos aportados no corresponden a una política, lo suministrado correspondió a imágenes de reportes obtenidos de algún tipo de software o herramienta de gestión o monitoreo; de igual manera, se realizó búsqueda en la herramienta Almera de la entidad sin lograrse identificar una Política de seguridad de dominio o de Seguridad de Firewall definida y normalizada.

  Análisis de observaciones y/o respuesta del auditado. Mediante correo electrónico del 20/06/2025, la Oficina de Sistemas informó:

  "En el 13-00-MA-0001 Manual de Seguridad de la Información se expone la política de firewall y la política de contraseñas en él se incluye acceso a nivel operativo de Windows (dominio) página 45.

No se tiene establecida la obligatoriedad de tener documentos separados para especificar estas políticas, se tienen incluidas en el documento expuesto, cabe añadir que en ningún documento se puede especificar la particularidad de la parametrización de elementos como el firewall pues dicho documento podría convertirse en la guía de uso de cualquier atacante de la seguridad informática de la empresa."

Pronunciamiento de la OCI: Se realizó revisión del documento mencionado, Manual de Seguridad de la Información (Código 13-00-MA-0001) versión 6 con fecha 28/06/2024. En el numeral "*6.15 POLÍTICA DE FIREWALL"* (página 44) se observan tres párrafos que incluyen una definición de lo que es un "Firewall" y la mención de quién debe diseñar las políticas de acceso; sin embargo, ésta no contiene un enunciado que permita identificar a qué se compromete la Subred con esta política, como tampoco un objetivo al cual se asocian unas metas e indicadores para medir el cumplimiento de dicha política, entre otros aspectos que ésta debería contener. Además, cabe mencionar que en consulta en la web, se encontró que "*Una política de firewall se compone de reglas que especifican cómo el firewall debe manejar el tráfico de red. Estas reglas definen el comportamiento del firewall en función de criterios como la dirección de origen y destino, el protocolo, el puerto y la acción a realizar (permitir, denegar, etc.) (…)".*

Continua el informe de auditoría:

La situación antes descrita evidencia inobservancia de la Resolución 500 de 2021 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",* que se fundamenta en la norma ISO 27001 versión 2013.

b. Gestión de Incidentes de Seguridad de la Información.

En la evaluación de este ítem, se tuvo en cuenta: Norma ISO/IEC 27001 Anexo A. ítem A.16.1. Gestión de incidentes y mejoras en la seguridad de la información; y 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.

Sobre el particular, la Oficina de Control Interno solicitó documentación y soportes, relacionados con: i) Matriz de reporte de incidentes de seguridad y seguimientos, ii) Plan de acción para mitigar incidentes de seguridad reportados, iii) Política de atención o gestión de incidentes de seguridad y, iv) Plan de prevención de incidentes de seguridad.

En la verificación, se observó:

i) Matriz de reporte de incidentes de seguridad y seguimientos. En la documentación aportada no se observó esta matriz y los seguimientos que debió realizarse a los reportes de incidentes de seguridad presentados en el período de evaluación y seguimiento.

Análisis de observaciones y/o respuesta del auditado. Mediante correo electrónico del 20/06/2025, la Oficina de Sistemas informó:

"No se recibieron ni por mesa de ayuda ni de ninguna otra forma un reporte de incidente de seguridad, por ende se envió las capturas de todas las políticas que se tienen configuradas y que resultado de la gestión realizada no tenemos incidentes de seguridad materializados.

Sin embargo, si se tiene registro de incidentes de seguridad de la información en los casos donde se han presentado eventos que acorde a nuestro procedimiento han sido reportados al CSIRT, dispongo de la evidencia la cual no me fue solicitada."

Pronunciamiento de la OCI: En reunión realizada el 24/06/2025 el auditado manifestó que, en el año 2024 no recibieron ningún tipo de incidente de seguridad, pero que en el año 2023 si tuvieron 2, los cuales fueron atendidos y mitigados, mostrando la gestión realizada con ellos. Sin embargo, no se generó una Matriz de Reporte de Incidentes de Seguridad y Seguimientos para hacer trazabilidad cuando éstos se han presentado, así como lo indica la Guía para la Gestión y Clasificación de Incidentes de Seguridad del MPSI.

Continua el informe de auditoría:

Sobre este asunto es importante precisar que, si bien en el aplicativo Almera se observó que se cuenta con un "Instructivo incidentes de seguridad" (Código 13-02-IN-0001) versión 2 de fecha 27/12/2024 y un formato denominado "Reporte de incidentes de seguridad de la información" (Código 13-02-FO-0005) versión 2 de fecha 03/01/2025, estos documentos no correspondían a lo solicitado.

La situación antes descrita evidencia inobservancia de la Resolución 500 de 2021 *"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".*

ii) Plan de acción para mitigar (o gestionar) incidentes de seguridad reportados. La documentación solicitada no se recibió, por lo que se concluye que la Entidad no cuenta con un plan de acción para mitigar (o gestionar) incidentes de seguridad reportados que esté en ejecución.

iii) Política de atención o gestión de incidentes de seguridad. No se obtuvo soporte o documentación, que evidencie que la entidad cuenta con esta política.

Análisis de observaciones y/o respuesta del auditado. Mediante correo electrónico del 20/06/2025, para los ítems ii) y iii) la Oficina de Sistemas informó:

"En el 13-00-MA-0001 Manual de seguridad de la información V6 se encuentra la política de incidentes de seguridad, en él está el proceso que se debe realizar en caso de que surja un incidente. Adicional, está el 13-02-IN-0001 Instructivo incidentes de seguridad. (…)."

Pronunciamiento de la OCI: Revisados los documentos mencionados por el auditado en la reunión del 24/06/2025 y en la respuesta del informe preliminar, se observó que cuentan con un Instructivo Incidentes de Seguridad (Código 13-02-IN-0001) versión 2 de fecha 27/12/2024, y un Manual de Seguridad de la Información (Código 13-00-MA-0001) versión 6 de fecha 28/06/2024. En el numeral 6.14 del manual que refiere la "*Política de incidentes de seguridad"* de la entidad, se observa que su contenido corresponde a la indicación de una serie de pasos a seguir, en caso de presentarse incidentes de seguridad en la Subred, para que éstos sean registrados y atendidos oportunamente; sin embargo, ésta no contiene un enunciado que permita identificar a qué se compromete la Subred con esta política, como tampoco un objetivo al cual se asocian unas metas e indicadores para medir el cumplimiento de dicha política, entre otros aspectos que ésta debería contener. Además, cabe mencionar que en consulta en la web, se encontró que "*Una política de gestión de incidentes de seguridad típicamente incluye la definición de qué constituye un incidente, la clasificación de los incidentes, los roles y responsabilidades, los procedimientos de reporte y escalamiento, las medidas de contención y recuperación, la comunicación, y la revisión y mejora continua. (…)."*

Continua el informe de auditoría:

iv) Plan de prevención de incidentes de seguridad. No se obtuvo soporte o documentación, que evidencie que la entidad cuenta con este plan.

La situación antes descrita evidencia inobservancia del Decreto 338 de 2022 "*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*", marco normativo impulsado por el MinTIC, exigiendo a las entidades públicas que desarrollen un Plan de Seguridad y Privacidad de la Información. Este plan debe incluir medidas para prevenir incidentes de seguridad y proteger la información.

Análisis de observaciones y/o respuesta del auditado. Mediante correo electrónico del 20/06/2025, la Oficina de Sistemas informó:

"Se realiza la evaluación de riesgos para evitar los incidentes. Se presentó la metodología aplicada de tratamiento de riesgos la cual es institucional."

Pronunciamiento de la OCI: Se revisó la información reportada por el auditado, quien al conocer los resultados preliminares de la auditoría, informó que en la página web de la entidad (https://subredsuroccidente.gov.co) se ubica el documento: "*Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información"* (Código 13-00-PL-0003); el cual muestra el trato que se da a los riesgos de seguridad y a los eventos que se puedan presentar. Esta información no fue allegada con antelación al auditor, por ello, no se tuvo en cuenta para la evaluación de este ítem en la auditoría.

Por lo anterior, se da por subsanada la observación emitida.

Continua el informe de auditoría:

c. Indicadores de Gestión de Seguridad de la Información.

Para la evaluación de este ítem, se consideró la siguiente normativa:

Resolución 500 de 2021 *"Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".*

Guía Indicadores Gestión de Seguridad de la Información, que indica: *"La creación de indicadores de gestión está orientada principalmente en la medición de efectividad, eficiencia y eficacia de los componentes de implementación y gestión definidos en el modelo de operación del marco de seguridad y privacidad de la información, indicadores que servirán como insumo para el componente de mejora continua, permitiendo adoptar decisiones de mejora". Los objetivos de estos procesos de medición en seguridad de la información son:*

- *Evaluar la efectividad de la implementación de los controles de seguridad*
- *Evaluar la eficiencia del Modelo de Seguridad y Privacidad de la Información al interior de la entidad.*
- *Proveer estados de seguridad que sirvan de guía en las revisiones del Modelo de Seguridad y Privacidad de la Información, facilitando mejoras en seguridad de la información y nuevas entradas a auditar.*
- *Comunicar valores de seguridad al interior de la entidad.*
- *Servir como insumos al plan de análisis y tratamiento de riesgos."*

Al respecto, en la documentación relacionada en el aplicativo Almera no se identificó algún tipo de Indicador especifico a lo asociado en la Resolución o evaluado dentro del MPSI

que diera cuenta del cumplimiento a lo establecido en la Resolución 500 de 2021 y en el Modelo de Seguridad y Privacidad de la Información - MPSI.

Análisis de observaciones y/o respuesta del auditado. Mediante correo electrónico del 20/06/2025, la Oficina de Sistemas informó:

"Se tienen 11 controles para los riesgos operativos y de corrupción asignados a sistemas, los cuales, hacen referencia a la seguridad de la información.

Se tiene indicador "cumplimiento del plan de acción para el manejo de Seguridad de la información" para la política de seguridad y privacidad de la información."

Pronunciamiento de la OCI: Como se indicó en la reunión del día 24/06/2025, el control de un riesgo no es un indicador.

Tal como se define en la Guía para la construcción y análisis de indicadores de gestión (versión 4) emitida por la Función Pública en mayo de 2018, un indicador "*Es una representación (cuantitativa preferiblemente) establecida mediante la relación entre dos o más variables, a partir de la cual se registra, procesa y presenta información relevante con el fin de medir el avance o retroceso en el logro de un determinado objetivo en un periodo de tiempo determinado, ésta debe ser verificable objetivamente, la cual al ser comparada con algún nivel de referencia (denominada línea base) puede estar señalando una desviación sobre la cual se pueden implementar acciones correctivas o preventivas según el caso."* (página 18)

De otra parte, al revisar el Plan Estratégico de Tecnología de la Información y las Comunicaciones PETIC (Código 13-00-PL-0001) versión 8 de fecha 30/01/2025 cargado en el aplicativo Almera, se observó que en el numeral 9.2.2 referente a "*Indicadores y Factores Críticos de Éxito*" se menciona "*En el **Anexo 1** se puede observar el Plan Operativo actual con sus respectivos indicadores*"; este anexo no se evidenció ni tampoco fue suministrado por el auditado en la reunión del 24/06/2025.

Continua el informe de auditoría:

d. Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas.

El Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas, Anexo 4 de los documentos asociados al MPSI, indica: *"Conforme lo indica el ámbito de aplicación del Decreto 1078 de 2015 respecto a la estrategia de Gobierno Digital, las entidades públicas deben realizar la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) con el objetivo de implementar un Sistema de Gestión de Seguridad de la Información al interior de la Entidad. El MSPI integra en cada una de sus fases tareas asociadas a la gestión de riesgos de seguridad de la información,*

ya que esta práctica constituye su base fundamental. La guía para la gestión del riesgo de función pública, junto con el presente Anexo, llevarán a cumplir dichas tareas de gestión de riesgo de seguridad de la información requeridas en el MSPI".

Teniendo en cuenta los lineamientos anteriores, en la evaluación de la documentación aportada o consultada, se observó lo siguiente:

- En el aplicativo Almera no se identificó documentación e/o información que diera cuenta de la gestión de riesgos de seguridad de la información en la entidad, conforme los lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información, por lo que se requiere implementar las acciones pertinentes para aplicarlo en la entidad.

  Análisis de observaciones y/o respuesta del auditado. Mediante correo electrónico del 20/06/2025, la Oficina de Sistemas informó:

  "Se tienen 11 controles para los riesgos operativos y de corrupción asignados a sistemas, los cuales, hacen referencia a la seguridad de la información.

  Esta es una metodología institucional a la que le hace seguimiento el área de desarrollo institucional, por favor, consulte a esta área para que pueda evidenciar la respuesta."

  Pronunciamiento de la OCI: Se realizó revisión de los riesgos asociados al proceso de Gestión de TICs, buscando identificar si en alguno de ellos se cuenta con Indicadores de Gestión de Seguridad de la Información, lo cual no se evidenció.

  Continua el informe de auditoría:

- En el aplicativo Almera se observó el indicador: "*Porcentaje de cumplimiento del plan de acción para el manejo de Seguridad de la información Subred Sur Occidente ESE"* (Código EQ ME GER INF 07) cuyo objetivo es: *"Monitorear el plan de acción para controlar los riesgos de afectación a la confidencialidad de la historia Clínica en la cual se asegura su confidencialidad",* y que cuenta con una ficha técnica que define su medición semestral en porcentaje. En la verificación del cumplimiento del indicador en el periodo auditado, se evidenció que el último registro de actividades fue el 20/12/2024 observándose los respectivos soportes y/o evidencias, dando así un cumplimiento en un 100% para el año 2024. Para el periodo auditado, aún falta tiempo de ejecución del indicador, ya que como lo indica su ficha técnica, la periodicidad es semestral.

e. Gestión Inventario de Activos e Infraestructura Critica.

Dentro de lo evaluado en este ítem, se tuvo en cuenta el documento Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional, el cual forma parte del Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC y que contiene un aparte denominado Guía - Gestión inventario clasificación de activos e infraestructura critica, en el cual *"…. presenta los lineamientos básicos que debe tener en cuenta para realizar una adecuada identificación, gestión y clasificación de activos de información e infraestructura critica de cada entidad y así:*

- *Establecer las responsabilidades de los funcionarios y contratistas de la entidad con los Activos de Información.*
- *Garantizar que los activos de información de la entidad reciban un adecuado nivel de protección de acuerdo con su valoración.*
- *Proporcionar una herramienta que visualice de manera fácil los activos de información de la entidad.*
- *Sensibilizar y promover la importancia de los activos de información de la entidad.*
- *Proveer las pautas requeridas y necesarias para la adecuada identificación, clasificación y valoración de los activos de información de la entidad.*
- *Cumplir con la organización y publicación de los activos de información, respetando tanto las normas como los procedimientos que se deben cumplir.*

El inventario y clasificación de activos hace parte de las actividades más relevantes e importantes del Modelo de Seguridad y Privacidad de la Información y está compuesta por las fases:

- *Identificación y Tipificación de los Activos de Información*
- *Clasificación de los activos de Información*
- *Revisión y Aprobación*
- *Publicación de los Activos de Información."*

Al validar en la página web, se observó la existencia del documento con código 13-04-FO-0001 "*Inventario de activos de información – 2024*" versión 4 de fecha 06/05/2024; documento con el que se da completitud a lo solicitado, y da alcance a lo requerido por el MPSI - Gestión Inventario de Activos e Infraestructura Critica, junto con la demás documentación allegada con anterioridad.

f. Seguimiento a la Implementación de la Política de Seguridad y Privacidad de la Información

Dentro de lo evaluado en este ítem, tenemos: Política de seguridad y privacidad de la información y Plan de acción para el manejo de Seguridad de la información.

En consulta de la información registrada y/o cargada en el aplicativo Almera, se observó:

- Indicador "*Porcentaje de cumplimiento del plan de acción para el manejo de Seguridad de la información Subred Sur Occidente ESE*" (Código EQ ME GER INF 07). Este indicador cuenta con una medición porcentual en una frecuencia semestral y se encuentra desarrollado en su totalidad para el periodo 2024, observándose los respectivos soportes de sus actividades.

- Política de Seguridad y Privacidad de la Información (Código 01-01-OD-0029) en versión 4 que data del 09/07/2021, es decir, que en los últimos cuatro (4) años no ha sido actualizada, aspecto que genera incertidumbre si ha sido revisada para validar su alineación y conformidad con la normatividad vigente y generada desde el año 2021, como lo es el Decreto 338 de 2022 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*."

Análisis de observaciones y/o respuesta del auditado. Mediante correo electrónico del 20/06/2025, la Oficina de Sistemas informó:

"Se radicó la solicitud en enero del 2025 pero no ha sido gestionada, según nos informan la actualización está pendiente por trámite interno dado que la entidad avanza con la actualización de la totalidad de las políticas que soporta la plataforma estratégica.

Por razones fuera del alcance de sistemas se tuvo que radicar solicitud Oportunidad de mejora: ID #3793."

Pronunciamiento de la OCI: La respuesta emitida por el auditado no desvirtúa la observación; por lo tanto, se mantiene la observación.

Continua el informe de auditoría:

En cuanto al Plan de acción para el manejo de Seguridad de la información, en el aplicativo Almera se observó el indicador "*Porcentaje de cumplimiento del plan de acción para el manejo de Seguridad de la información Sub Red Sur Occidente ESE*" (Código EQ ME GER INF 07) que cuenta con una periodicidad de seguimiento semestral y una medición porcentual; su objetivo es: *"Monitorear el plan de acciona para controlar los riesgos de*

afectación a la confidencialidad de la historia Clínica en la cual se asegura su confidencialidad". En los registros de seguimiento a este indicador, se observó dos (2) archivos en Excel denominados "*Ejecución Plan de seguridad de la información 2024 avance 2 trimestre*" y avance 4 trimestre, cargados como evidencia de cumplimiento del indicador, el cual se encuentra finalizado y completo para el periodo 2024; para la vigencia 2025 está en proceso de ejecución, ya que según su ficha técnica la medición es semestral y para la vigencia de la auditoria, aun no se cumple el tiempo de registro de avances y actividades.

Asimismo, se observaron otros documentos con actualización reciente, tales como: Plan de tratamiento de riesgos de seguridad y privacidad de la información (Código 13-00-PL-0003) versión 5 de fecha 07/01/2025 y Plan de acción de seguridad y privacidad de la información (Código 13-00-PL-0004) versión 6 de fecha 27/12/2024.

Sin embargo, se observó el Plan de seguridad y confidencialidad de la información (Código 13-04-PL-0003) que data del 30/09/2020 en su versión 1, lo que es indicativo que este plan no ha sido actualizado desde la vigencia 2020, situación que genera incertidumbre respecto de la definición y ejecución de las actividades específicas definidas en este plan en las vigencias 2021 a 2025, en virtud de que, en el numeral "***4. Desarrollo del plan***" contiene un cronograma con corte a 31/12/2020. Estas actividades específicas, son: 1) Actualizar la política de tratamiento de datos personales; 2) Acceso a Windows a través de usuarios y contraseñas; 3) Acceso al sistema Dinámica Gerencial con usuario y contraseña; 4) Asignación de perfiles de acceso a usuarios de Dinámica Gerencial; 5) Validación de cambios de claves por usuarios; 6) Análisis desbloqueo de claves por intentos fallidos y olvido de contraseñas; 7) Actualizar el procedimiento de gestión de usuarios y contraseñas; 8) Bloqueo de usuarios que no accedan al sistema en más de 30 días; 9) Firma acta de confidencialidad de la información por usuarios con acceso VPN, y 10) Actualizar el Manual de seguridad de la información.

Análisis de observaciones y/o respuesta del auditado. Mediante correo electrónico del 20/06/2025, la Oficina de Sistemas informó:

"Los planes de cada año incluyendo los del 2025 están publicados en la página de la subred

https://subredsuroccidente.gov.co/transparencia-y-acceso-a-la-informacion/planeacion-2/

Esto se hace y actualiza todos los años dando cumplimiento normativo en los meses de enero, tema que controla desarrollo institucional, de no haberse actualizado algún año la oficina de control interno habría generado este hallazgo años atrás."

Pronunciamiento de la OCI: En la verificación de la información allegada por el auditado con las observaciones y/o respuestas al informe preliminar, ingresando a la página web

de la entidad y validando lo indicado en la respuesta, se observó publicado el documento: Plan de Seguridad y Privacidad de la Información (Código 13-00-PL-0004) versión 6 de fecha 27/12/2024; sin embargo, al plan que se hace referencia en la observación es al **Plan de seguridad y confidencialidad de la información (Código 13-04-PL-0003) que data del 30/09/2020 en su versión 1**, siendo este el documento relacionado que no ha sido actualizado desde la vigencia 2020, situación que genera incertidumbre respecto de la definición y ejecución de las actividades específicas definidas en este plan en las vigencias 2021 a 2025, en virtud de que, en el numeral "***4. Desarrollo del plan***" contiene un cronograma con corte a 31/12/2020.

Continua el informe de auditoría:

RECOMENDACIÓN(ES)

- Realizar las acciones pertinentes para dar alcance a lo normado en el Modelo de Seguridad y Privacidad de la Información (MSPI), toda vez que, se identificó cumplimiento parcial a lo dispuesto en el MSPI, así como también se evidenciaron formatos y documentos no normalizados en el aplicativo Almera. La Resolución 500 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) establece el Modelo de Seguridad y Privacidad de la Información (MSPI) en Colombia, dentro del cual se indican todos sus componentes de los cuales se hace referencia en esta auditoría interna de cumplimiento.

- Construir e implementar una matriz o política para asignación de usuarios y contraseñas de dominio, así como realizar la gestión pertinente para la adquisición de licencias de correo institucionales para los colaboradores (funcionarios y contratistas) de la entidad; obteniendo así una mejora en la seguridad de la información, evitando o disminuyendo el riesgo de manipulación de información sensible de la entidad.

DECLARACIONES DE LA OFICINA DE CONTROL INTERNO

- *Esta auditoría fue realizada con base en el análisis de una muestra aleatoria seleccionada por el auditor a cargo de la realización del trabajo. Una consecuencia de esto es la presencia del riesgo de muestreo, es decir, el riesgo de que la conclusión basada en la muestra analizada no coincida con la conclusión a que se habría llegado en caso de haber examinado todos los elementos que componen la población.*

- *La evidencia recopilada para propósitos de la evaluación efectuada versa en información suministrada por la Oficina de Sistemas de Información TICs, responsable de la unidad objeto de evaluación y seguimiento. Nuestro alcance no pretende corroborar la precisión de la información y su origen.*

- *La naturaleza de la labor de auditoría interna ejecutada por la Oficina de Control Interno, al estar supeditada al cumplimiento del Plan Anual de Auditoría, se encuentra limitada por restricciones de*

tiempo y alcance, razón por la que procedimientos más detallados podrían develar asuntos no abordados en la ejecución de esta actividad.

- *La respuesta ante las situaciones observadas por la Oficina de Control Interno es discrecional de la administración de la Subred Integrada de Servicios de Salud Sur Occidente E.S.E., más se incentiva la consideración de las "Recomendaciones" en la construcción de los planes de mejora a que haya lugar para el mejoramiento del Sistema de Control Interno y el Modelo Integrado de Planeación y Gestión de la entidad*.

Bogotá D.C., 30 de septiembre de 2025

CLAUDIA PATRICIA QUINTERO COMETA
Jefe Oficina de Control Interno

Elaboró: *Jorge Orlando Sánchez Alcalá, Profesional Especializado - OPS*
Revisó: *Claudia Patricia Quintero Cometa, jefe Oficina de Control Interno*