INFORME DE AUDITORÍA AL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN No. 27 – 2026

Fecha del informe: 08/07/2026 **Período auditado: 01-2026 – 04-2026**

Responsable: Víctor Julio Gómez Carvajal - Jefe Oficina de Sistemas de Información TIC's

1 OBJETIVO

Evaluar el estado de la implementación y cumplimiento de los requisitos del Modelo de Seguridad y Privacidad de la Información (MSPI) y las políticas internas, con el fin de determinar su capacidad para proteger la confidencialidad, integridad y disponibilidad de la información, identificando oportunidades de mejora.

2 ALCANCE

Evaluar la gestión realizada por la oficina de Sistemas de información TIC durante la vigencia 2025 para el cumplimiento de los requerimientos y anexos del modelo de Seguridad y Privacidad de la Información (MSPI) en la Subred Norte.

3 CRITERIOS

- Resolución 2277 de 2025. "*Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia."*
- Resolución 746 de 2022. "*Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución número 500 de 2021*."
- 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."*
- Ley 1581 de 2012. "*Por la cual se dictan disposiciones generales para la protección de datos personales."*
- Ley 1712 de 2014. "*Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones*."
- Ley 1273 de 2009. "*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."*
- NTC-ISO/IEC 27001:2022. "*Requisitos. Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información."*
- AP-GI-M-02 *Manual de políticas de seguridad y privacidad de la Información Versión 4.*

- AP-GI-I-45 *Instructivo de Separación de ambientes. Versión 1.*
- AP-GI-I-16 *Instructivo Gestión de incidentes de seguridad de la información. Versión 2.*
- AP-GI-PL-02 *Plan de seguridad y privacidad de la información. Versión 7.*

4 DESARROLLO DE LA EVALUACIÓN

4.1 Cumplimiento del Modelo de Seguridad y Privacidad de la Información - MSPI.

Teniendo en cuenta la revisión efectuada a la información del subproceso cargada en Almera, en página Web (inventario de activos de información) y la suministrada por la Oficina de Sistemas de Información TIC's, a través de oficio No. 2026-001800-3 de junio 5 de 2026, junto con las evidencias recolectadas en la visita del día 4 de junio de 2026, esta auditoría observó:

4.1.1 Revisión de documentación

Como parte del trabajo de auditoría de escritorio, se realizó revisión de los principales documentos frente a los lineamientos del Modelo se Seguridad y Privacidad de Información. A continuación, se muestran los resultados:

Documento Manual de Políticas de Seguridad y Privacidad Código AP-GI-M-02 Versión 4 Fecha: 21/03/2025
Contenido El manual define 13 políticas sobre: dispositivos móviles, recurso humano, teletrabajo, gestión de activos, control de acceso, copias de respaldo, seguridad física, operaciones, comunicaciones, relaciones con proveedores, gestión de incidentes y buenas prácticas del colaborador. Cada política define objetivos, responsables de ejecución y cumplimiento, directrices y referencias a los controles del Anexo A de ISO 27001:2013
Observaciones • El manual referencia a la norma técnica ISO/IEC 27001:2013, no obstante, la versión vigente es ISO/IEC 27001:2022, introduce cambios en el Anexo A (de 114 a 93 controles, reorganizados en 4 temáticas). • Ausencia de un lineamiento a política de criptografía: el autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (Instrumento Evaluación MSPI - noviembre 2024.xlsx), reportó el A.10 (ISO 27001:2013) en nivel inexistente (0/100), de igual forma el Manual no contempla directrices sobre cifrado, gestión de claves ni uso de certificados digitales. • La política de gestión de activos de información establece responsabilidades de etiquetado de información para el Grupo de Gestión Documental. No obstante, durante la visita se evidenció que no existe un esquema de etiquetado implementado (control A.5.13 de ISO/IEC 27001:2022) • La política de gestión de activos de información, delega la clasificación de los activos a los líderes de proceso, sin establecer periodicidad de actualización del inventario ni mecanismo de verificación del cumplimiento.
Documento Plan de Seguridad y Privacidad de la Información 2026 (PESI) Código AP-GI-PL-02 Versión 7 Fecha: 31/01/2026

Contenido

El Plan 2026 establece el marco estratégico del SGSI-MSPI para la vigencia, articulado con el ciclo PHVA, el MIPG y la Política de Gobierno Digital. Incorpora resultados del autodiagnóstico MSPI 2025, define 5 estrategias específicas (gobernanza, gestión de riesgos, controles, gestión de incidentes, cultura y cumplimiento), un portafolio de 6 proyectos y un cronograma trimestral. Define roles y responsabilidades para 10 actores institucionales.

Observaciones

- Dentro del Numeral 9.2. “El portafolio de proyectos / actividades 2026” de este documento no se observa lo respectivo a criptografía, pese a que el autodiagnóstico identifica como la brecha más crítica (0/100). La Estrategia 3 define a la criptografía como prioridad; sin embargo, no hay proyecto ni cronograma asignado a la implementación de este control.
- El Plan referencia como marco normativo la ISO/IEC 27001:2022, no obstante, conserva la tabla de autodiagnóstico con la estructura de dominios de ISO/IEC 27001:2013 (A.5–A.18).
- El cronograma no asigna mes de ejecución a la Meta 1 (Autodiagnóstico MSPI), lo cual indica que no se tiene priorizado para la actual vigencia. la vigencia.
- Se cuenta con un indicador definido para el seguimiento del plan: “Porcentaje de cumplimiento del Plan de Seguridad y Privacidad de la Información”. Se recomienda implementar indicadores de impacto como se sugiere en la guía de “*Lineamientos de Indicadores de Gestión de Seguridad de la Información*” del MINTIC. (por ejemplo, porcentaje de cumplimiento del portafolio, nivel MSPI alcanzado).

Documento

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2026
Código AP-GI-PL-03 Versión 6
Fecha: 31/01/2026

Contenido

El Plan desarrolla la metodología de gestión de riesgos articulada con la Guía DAFP V6 y los Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información MinTIC V5.0 (abril 2025). Establece el ciclo PHVA para la gestión de riesgos, define escalas de probabilidad e impacto, formato de mapa de riesgos, evaluación de riesgo residual y el modelo de tres líneas de defensa.

Observaciones

- La metodología de gestión de riesgos no se articula con Guía DAFP V7.
- Según el Plan: “para cada riesgo se deben asociar los activos (o grupos de activos) del proceso y analizar las amenazas y vulnerabilidades que podrían causar su materialización…”, la matriz de riesgos no cumple con dicha característica.
- El cronograma 2026 tiene 4 actividades programadas, con baja granularidad y sin asignación presupuestal. La Meta 1 (fortalecer gestión) no tiene periodo asignado.
- No se define el apetito de riesgo institucional ni los criterios de aceptación del riesgo residual como documento independiente aprobado por el Comité.

Documento

Instructivo de Análisis de Vulnerabilidades
Código AP-GI-I-23 Versión 1
Fecha: 11/07/2023

Contenido

El instructivo define metodología para el análisis de vulnerabilidades sobre la infraestructura tecnológica de la Subred, incluyendo: procedimiento de escaneo-priorización-remediación-re-test, y roles del Oficial de Seguridad e Ingeniero de Infraestructura.

Observaciones

- El instructivo se encuentra desactualizado y no incorpora lineamientos MinTIC 2025 ni la normatividad vigente (Resolución 746/2022, Resolución 02277/2025)
- Las referencias bibliográficas del instructivo apuntan a guías MinTIC de 2016, que han sido actualizadas por versiones más recientes.
- El instructivo no incluye análisis de vulnerabilidades en ambientes de nube ni en servicios expuestos a Internet. Sin embargo, el proyecto 4 del Plan Estratégico de Seguridad de la información 2026 sí lo contempla como: "On-premise, Cloud y/o servicios expuestos a internet", generando incoherencia con el instructivo.
- El procedimiento definido en el instructivo no establece tiempos para la remediación por nivel de criticidad. La norma técnica ISO 27001:2022, exige tratar vulnerabilidades y riesgos en forma oportuna, tomando como base buenas prácticas
- No contempla la gestión de vulnerabilidades de día cero (0-day) ni la articulación con fuentes de inteligencia de amenazas (COLCERT, CERT nacionales).
- El procedimiento no incluye el reporte al Comité de Gestión y Desempeño, que es exigido en la matriz de roles del Plan de Seguridad y Privacidad de la Información 2026.
- Las referencias bibliográficas del instructivo apuntan a guías MinTIC de 2016, que han sido actualizadas por versiones más recientes.

Documento

Instructivos operativos (backups, vulnerabilidades, ingreso/desvinculación de personal, proveedores, transferencias, mantenimiento, recuperación de desastres, separación de ambientes, protección de activos, protección contra código malicioso, ingreso seguro a sistemas, Instructivo de aseguramiento de servicios)

Contenido

Complementan la implementación de las políticas del manual AP-GI-M- 02 y del Plan Estratégico de Seguridad de la Información, en procedimientos de operación. Estos instructivos responden directamente a dominios MSPI.

Los instructivos de backups, recuperación de desastres y continuidad están alineados conceptualmente con ISO 22301 [1]y con la definición de BCP/DRP.

No es coherente el título del “Instructivo para el tratamiento de seguridad en los acuerdos con los proveedores” ya que este corresponde al “Instructivo Retiro de Activos”

Observaciones

- Actualizar los instructivos conforme a la normatividad vigente, incorporando de manera explícita la referencia al Modelo de Seguridad y Privacidad de la Información actualizado y a la norma ISO/IEC 27001:2022.

[1] (https://www.iso.org/standard/75106.html) La norma ISO 22301 es el estándar internacional para los Sistemas de Gestión de la Continuidad del Negocio (SGCN). Proporciona un marco para que las organizaciones planifiquen, establezcan, implementen, operen, supervisen, revisen, mantengan y mejoren continuamente un sistema de gestión documentado para protegerse contra incidentes disruptivos, reducir su probabilidad y garantizar la recuperación ante ellos.

- Incluir en los instructivos de proveedores y nube cláusulas mínimas de seguridad alineadas a lineamientos cloud (ANS, ubicación de datos, cifrado, gestión de incidentes, responsabilidad compartida, terminación del servicio y portabilidad).
- Vincular cada instructivo con la política correspondiente (referencia cruzada al número de política y dominio MSPI),
- Incorporar métricas de ejecución (ej. % backups probados, tiempos de recuperación reales, % proveedores evaluados, etc.)

La documentación del Sistema de Seguridad de la Información presenta fortalezas en materia de gobernanza, actualización y cobertura temática. Sin embargo, se identifican oportunidades de mejora en la incorporación de controles de criptografía y en el fortalecimiento de la gestión de activos de información y de riesgos. Asimismo, se evidencia desactualización en el referente ISO/IEC 27001:2022.

4.1.2 Gestión de Riesgos de Seguridad y Privacidad de la Información

La evaluación de los riesgos de seguridad de la información se fundamentó en la coherencia metodológica entre el Plan de Tratamiento de Riesgos y la Guía para la Gestión Integral del Riesgo en Entidades Públicas del DAFP (Versión 7). Asimismo, se analizó el grado de cumplimiento del Inventario de Activos de Información y la Matriz de Riesgos y Controles del proceso, evaluando su alineación con los estándares e instrumentos del Modelo de Seguridad y Privacidad de la Información (MSPI).

Tras comparar y analizar los instrumentos aportados, la Oficina de Control Interno identificó las siguientes novedades estructurales y metodológicas:

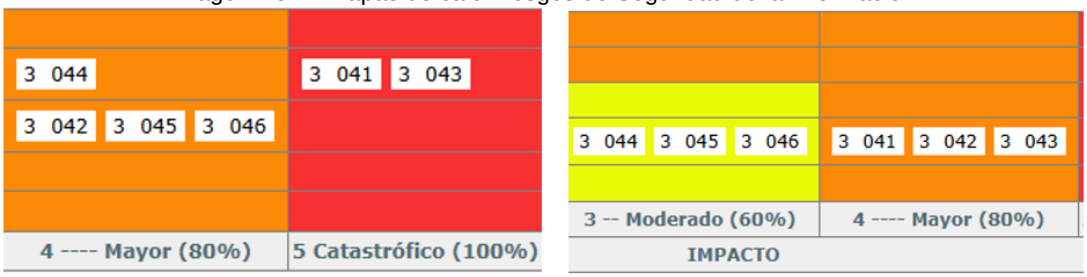
a) Se evidenció desactualización del Plan de Tratamiento de Riesgos frente a los lineamientos del Departamento Administrativo de la Función Pública (DAFP) y el Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC.

b) El Inventario de Activos de Información (archivo en formato Excel) no se encuentra plenamente articulado con las directrices del modelo, presentando las siguientes novedades:

   - El documento publicado en el portal institucional como correspondiente a la vigencia 2025, contiene en realidad la información y estructura de la vigencia 2024.
   - El universo evaluado comprende 1.057 registros, clasificados con nivel de criticidad (Muy alto: 71, Alto: 232, Medio: 275, Bajo: 465 y N/A: 14)
   - Utiliza una escala de valoración diferente a la propuesta por el MSPI; mientras el MinTIC define una escala de tres niveles (Alta, Media, Baja), con valores cualitativos (A/M/B) o numéricos (1/2/3), el inventario actual emplea una escala de cuatro niveles (muy alto, alto, medio, bajo), con valores numéricos 3, 2, 1 y 0, y calcula un promedio aritmético de los tres campos para determinar la criticidad, generando también cuatro categorías en lugar de tres.
   - No se incluye análisis de infraestructura critica cibernética (ICCN).

c) La Matriz de Riesgos presenta Seis (6) riesgos de seguridad digital relacionados en su totalidad con el proceso de Gestión de Tics, con el siguiente comportamiento en sus mapas de calor:

Imagen No. 1: Mapas de calor riesgos de Seguridad de la Información



Mapa de riesgo inherente Mapa de riesgo residual

Fuente: Sistema Almera

- El perfil de riesgo inherente ubica los riesgos en cuadrantes de alta exposición: dos (2) en zona Catastrófica y cuatro (4) en zona Mayor.
- Los doce (12) controles formulados genera un desplazamiento positivo en el mapa de calor, pasando dos (2) riesgos catastróficos a zona "Mayor" y tres (3) de los riesgos mayores a la zona "Moderado". No obstante, el riesgo con código "042" no presenta variación en impacto y mantiene su calificación en zona "Mayor".
  Respecto a la valoración de estos controles, esta auditoría no pudo validar los cálculos realizados. Al respecto, se advierte que los únicos riesgos con controles correctivos que pueden disminuir el nivel de impacto son 44 y 45; los demás riesgos cuentan únicamente con controles preventivos, los cuales están diseñados para mitigar la frecuencia, pero no el impacto del riesgo.
- Los riesgos descritos en la matriz se estructuraron de manera genérica, puesto que no hacen referencia explícita a los activos de información o grupos de activos comunes previamente tipificados en el inventario.

4.1.3 Evaluación de controles

La verificación se realizó sobre los 93 controles incluidos en el Anexo A del lineamiento del Modelo de Seguridad y Privacidad de la Información, con base en el análisis documental disponible en Almera y en las evidencias aportadas por el proceso auditado al momento de la visita. Adicionalmente se realizó comparación con los resultados del autodiagnóstico realizado por el proceso para la vigencia 2025.

Tabla No. 1: Contexto MSPI – Niveles de madurez (autodiagnóstico noviembre 2025)

Dominio MSPI	Puntaje / 100	Nivel
Control de acceso	81	Optimizado
Continuidad del negocio	77	Gestionado
Seguridad física	74	Gestionado
Seguridad de operaciones	79	Gestionado
Gestión de incidentes	70	Gestionado
Seguridad de recursos humanos	67	Gestionado
Gestión de riesgos / general	66	Gestionado
Cumplimiento normativo	68.5	Gestionado
Gestión de activos	57	Efectivo
Criptografía	0	Inexistente

Fuente: Plan de Seguridad y Privacidad de la Información

Por otra parte, no se realizaron pruebas de penetración ni análisis forense de sistemas y los controles declarados como No Aplica (3) corresponden a desarrollo de software (A.8.25, A.8.26, A.8.28). En las siguientes tablas se presentan los resultados obtenidos:

Tabla No. 2: Criterios de valoración de cumplimiento de controles

Cumplimiento	Criterio
Cumple	Existe evidencia documental de que el control está diseñado, aprobado e implementado conforme al criterio.
Cumple parcial	Existe evidencia documental limitada o implementación parcial del control.
No Cumple	No existe evidencia de documentación ni implementación del control.
No Aplica	El control fue excluido en la declaración de aplicabilidad.

Fuente: Oficina de Control Interno - Basada en Instrumento de Evaluación del MSPI

Tabla No. 3: Dominio A.5 – Controles Organizacionales (37 controles)

Código	Control	Cumplimiento	Observación
A.5.1	Políticas para la seguridad de la información	Cumple	Existe el Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04), que contiene 11 políticas específicas y cubre a funcionarios, contratistas y terceros. En la visita en sitio se verifica que el Manual hace parte del contenido del curso de inducción y reinducción institucional.
A.5.2	Roles y responsabilidades en seguridad de la información	Cumple parcial	El Plan de Seguridad y Privacidad de la Información (AP-GI-PL-02-07, Estrategia 1) define la formalización del esquema de gobernanza y roles, incluido el rol del Oficial de Seguridad de la Información. En la visita se evidencia la necesidad de integrar el rol de la mesa técnica con el comité de seguridad, a fin de completar la estructura de gobernanza conforme a los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).
A.5.3	Segregación de funciones	Cumple parcial	El Instructivo de Ingreso Seguro a los Sistemas de Información (AP-GI-I-48-01) y la Política de Control de Acceso del Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) establecen el principio de mínimo privilegio y la segregación de funciones. En la visita se verifica que, en el servicio de Directorio Activo, el área de Control Interno opera con un usuario de red asignado por equipo de cómputo y no por persona. En aplicativos misionales los usuarios están establecidos de forma individual.
A.5.4	Responsabilidades de la dirección	Cumple	El Plan de Seguridad y Privacidad de la Información (AP-GI-PL-02-07, Estrategia 1) identifica el fortalecimiento del liderazgo y compromiso de la alta dirección en el Sistema de Gestión de Seguridad de la Información (SGSI). En la visita se verifica la existencia de una directiva del Comité de Gestión y Desempeño institucional que respalda la exigencia de cumplimiento de las políticas de seguridad.
A.5.5	Contacto con autoridades	Cumple parcial	El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (AP-GI-PL-03-06) referencia al Grupo de Respuesta a Emergencias Cibernéticas de Colombia (ColCERT) como actor relevante en infraestructura crítica cibernética. En la visita se identifica que la entidad cuenta con el Instructivo de Gestión de Incidentes de Seguridad de la Información (AP-GI-I-16); sin embargo, el documento no incluye un procedimiento de contacto y notificación a autoridades competentes. Se recomienda actualizar el instructivo para incorporar este procedimiento.

Código	Control	Cumplimiento	Observación
A.5.6	Contacto con grupos de interés especial	Cumple parcial	El Plan de Seguridad y Privacidad de la Información (AP-GI-PL-02-07) no contempla la participación en grupos de seguridad especializados. En la visita se verifica que el Oficial de Seguridad de la Información (CISO) participa en un grupo de mensajería instantánea (WhatsApp) del Equipo Distrital de Seguridad Digital. Verificar la gestión de inteligencia de amenazas y la documentación del control establecido.
A.5.7	Inteligencia de amenazas	Cumple parcial	El Instructivo de Análisis de Vulnerabilidades (AP-GI-I-23-01) establece la identificación de vulnerabilidades técnicas. En la visita se constata que los incidentes de seguridad se recopilan de manera aleatoria, sin evidencia de recolección ni seguimiento. Existe una matriz de registro y gestión de incidentes; no obstante, se recomienda revisar integralmente el proceso de inteligencia de amenazas planificado conforme a los lineamientos del Plan de Seguridad y Privacidad de la Información (AP-GI-PL-02-07).
A.5.8	Seguridad de la información en la gestión de proyectos	Cumple	Se observa que el Instructivo de Gestión de Cambios (AP-GI-I-36) incluye el análisis de impacto en seguridad por parte del Oficial de Seguridad de la Información (CISO). En la visita se verifica la inclusión de requisitos de seguridad en el proyecto Meliportal y la supervisión del Oficial de Seguridad en su aplicación.
A.5.9	Inventario de información y otros activos asociados	Cumple parcial	La Matriz de Inventario de Activos de Información se encuentra publicada en el portal de transparencia de la entidad de acuerdo con los criterios de Confidencialidad, Integridad y Disponibilidad (CID) del Sistema de Gestión de Seguridad de la Información (SGSI). En la visita se constata que el inventario corresponde a la vigencia 2024 y no registra actualización para la vigencia 2025. La actualización de la vigencia 2026 está planeada para el último cuatrimestre del año. Se recomienda establecer la periodicidad de actualización.
A.5.10	Uso aceptable de información y activos asociados	Cumple	La Política de Buenas Prácticas de Seguridad para el Colaborador y la Política de Control de Acceso contenidas en el Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) regulan el uso aceptable de activos de información y aplican a funcionarios, contratistas y terceros. En la visita se informa que la socialización está programada para la vigencia 2026 conforme al plan de uso y apropiación institucional.
A.5.11	Devolución de activos	Cumple parcial	Se observa que en el Instructivo de Retiro de Activos (AP-GI-I-41-01) y el Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) se establecen los procedimientos de devolución de activos y revocación de accesos al momento de la desvinculación o cambio de rol. En la visita se observa que el instructivo contempla únicamente activos de hardware. Se recomienda ampliar su alcance para incluir otros tipos de activos de información, como credenciales de acceso lógico, información digital y documentos físicos clasificados.
A.5.12	Clasificación de la información	Cumple parcial	La Matriz de Inventario de Activos incluye la clasificación de activos conforme a la metodología de valoración de Confidencialidad, Integridad y Disponibilidad (CID) definida en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (AP-GI-PL-03-06), con niveles ALTA=5, MEDIA=3 y BAJA=1. En la visita se confirma que el inventario está clasificado con otra escala y presenta atraso en su actualización, tal como se evidencia en el control A.5.9. El autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) ubica la gestión de activos en nivel Efectivo con una puntuación de 57 sobre 100, lo que refleja la aplicación incompleta del control.
A.5.13	Etiquetado de la información	No Cumple	El Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) establece niveles de clasificación de la información;

Código	Control	Cumplimiento	Observación
			sin embargo, en la visita se constata que no existe un esquema de etiquetado físico ni digital que identifique de forma sistemática el nivel de clasificación de los documentos institucionales. No se evidencia la aplicación práctica del control ni mecanismos automáticos de etiquetado en los sistemas de información.
A.5.14	Transferencia de información	Cumple parcial	El Instructivo de Transferencia de Información (AP-GI-I-44-01) establece los procedimientos de identificación de necesidad, clasificación del activo, selección del canal seguro, registro y trazabilidad de las transferencias. La Política de Seguridad en las Comunicaciones del Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) complementa este control. En la visita se identifica que el instructivo presenta debilidades en la cobertura del proceso de transferencia de información, por lo que se recomienda su revisión y actualización.
A.5.15	Control de acceso	Cumple parcial	El Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) contiene la Política de Control de Acceso. En la visita se identifica que el documento de referencia en sitio corresponde al Instructivo de Control de Acceso Físico (AP-GI-I-35-01), el cual regula el acceso físico a instalaciones y no el acceso lógico a sistemas de información. Se recomienda verificar que los controles de acceso lógico estén documentados en el instructivo correspondiente y que los parámetros de autenticación multifactor (MFA), mínimo privilegio y segregación estén configurados y operativos en los sistemas críticos.
A.5.16	Gestión de identidades	Cumple	El Instructivo de Ingreso y Desvinculación del Personal cubre el ciclo de vida completo de identidades, incluyendo altas, modificaciones, traslados, suspensiones y bajas de accesos lógicos en Directorio Activo, inicio de sesión único, correo electrónico, red privada virtual (VPN) y aplicativos, así como accesos físicos. Se requiere autorización de jefatura y la suscripción de acuerdos de confidencialidad previos al otorgamiento de accesos.
A.5.17	Información de autenticación	Cumple parcial	Se observa que el Instructivo de Administración de Cuentas de Usuario (AP-GI-I-02-03) y la Política de Control de Acceso del Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04, sección 6.6) establecen los criterios de gestión de contraseñas y autenticación. En la visita se verifica que el doble factor de autenticación está implementado en el servicio de correo electrónico institucional y que la periodicidad de cambio de contraseña se cumple en el ERP. Sin embargo, los parámetros de longitud mínima de contraseña no se cumplen en todos los sistemas. Se recomienda unificar la política de contraseñas para la totalidad de los sistemas de información.
A.5.18	Derechos de acceso	Cumple	El Formato de Creación, Modificación e Inactivación de Usuarios en Sistemas de Información (AP-GI-F-40-04) y las solicitudes gestionadas a través de la mesa de servicios soportan el proceso de asignación, modificación y revocación de accesos. En la visita se constata que los privilegios de red están asignados por equipo de cómputo, mientras que en el ERP y en los aplicativos de apoyo se gestionan por usuario. Se recomienda extender la gestión de accesos individualizada a todos los servicios.
A.5.19	Seguridad en relaciones con proveedores	Cumple	El Instructivo para el Tratamiento de la Seguridad en los Acuerdos con los Proveedores establece cláusulas de confidencialidad, controles de Confidencialidad, Integridad y Disponibilidad (CID) y mecanismos de seguimiento. El autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) ubica el dominio de proveedores en nivel Efectivo con 60 sobre 100. En la visita se verifica el cumplimiento de requisitos de seguridad en el contrato con el proveedor de servicios en la nube (TIGO Cloud).

Código	Control	Cumplimiento	Observación
A.5.20	Abordaje de la seguridad en acuerdos con proveedores	Cumple	El Instructivo para el Tratamiento de la Seguridad en los Acuerdos con los Proveedores establece cláusulas de confidencialidad y controles de Confidencialidad, Integridad y Disponibilidad (CID). En la visita se constata que los contratos incluyen cláusulas de obligatorio cumplimiento de confidencialidad por parte del proveedor, como se evidencia en el contrato de adquisición de licencia de software de respaldo Veeam Backup para máquinas virtuales.
A.5.21	Gestión de seguridad en cadena de suministro TIC	Cumple parcial	El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (AP-GI-PL-03-06) identifica los activos de hardware y software como sujetos de valoración de riesgos. El Plan de Seguridad y Privacidad de la Información (AP-GI-PL-02-07) contempla servicios en la nube, incluyendo la plataforma Azure referenciada en el Instructivo de Generación de Copias de Seguridad – Backups (AP-GI-I-03). En la visita no se evidencia un proceso de evaluación de riesgos en la cadena de suministro de Tecnologías de la Información y las Comunicaciones (TIC), incluyendo la verificación de condiciones de seguridad de fabricantes, integradores y proveedores de servicios en la nube.
A.5.22	Seguimiento y revisión de servicios de proveedores	Cumple	El Instructivo de Gestión de Cambios (AP-GI-I-36) y el Instructivo para el Tratamiento de la Seguridad en los Acuerdos con los Proveedores establecen mecanismos de supervisión y seguimiento de proveedores. El autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) ubica el dominio de proveedores en nivel Efectivo con 60 sobre 100. En la visita se verifica la realización de seguimiento durante la vigencia 2025 a proveedores como NECTSOFT (contratos BYS-042-2025 y CONT-200), Iron Mountain, proveedores de repuestos y Solution Copy, con cronograma ejecutado en los meses de abril y agosto de 2025.
A.5.23	Seguridad de la información en servicios en la nube	Cumple parcial	El Instructivo de Generación de Copias de Seguridad – Backups (AP-GI-I-03) referencia el almacenamiento en la nube de Microsoft Azure. El Plan de Seguridad y Privacidad de la Información (AP-GI-PL-02-07) contempla el fortalecimiento de controles en servicios en la nube. En la visita se verifica la existencia de un contrato de Cloud Server con cláusulas de seguridad. Sin embargo, no se evidencia una política específica de seguridad en la nube que defina controles de acceso, cifrado, residencia de datos y auditoría para los servicios contratados.
A.5.24	Planificación y preparación de gestión de incidentes	Cumple parcial	El Plan de Seguridad y Privacidad de la Información (AP-GI-PL-02-07, Estrategia 4) establece como entregable la adopción y operación de un procedimiento de gestión de incidentes. El autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) ubica la gestión de incidentes en nivel Gestionado con 70 sobre 100. En la visita se verifica que el Instructivo de Gestión de Incidentes de Seguridad de la Información (AP-GI-I-16) está documentado; no obstante, no abarca la totalidad del ciclo de vida de gestión de incidentes, incluyendo las fases de contención, erradicación, recuperación y lecciones aprendidas, con tiempos de respuesta definidos.
A.5.25	Evaluación y decisión sobre eventos de seguridad	Cumple parcial	El Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) contiene la Política de Gestión de Incidentes. El Instructivo de Gestión de Incidentes de Seguridad de la Información (AP-GI-I-16) contiene el flujo de evaluación y clasificación de eventos de seguridad. El Plan de Seguridad y Privacidad de la Información (AP-GI-PL-02-07) reconoce la necesidad de fortalecer este proceso. Sin embargo, como se señala en el control A.5.24, "no cubre la totalidad del ciclo de vida del incidente".

Código	Control	Cumplimiento	Observación
A.5.26	Respuesta a incidentes de seguridad	Cumple parcial	Se observa que la estrategia 4 de Plan de Seguridad y Privacidad de la Información (AP-GI-PL-02-07), define como entregable la implementación de un procedimiento de gestión de incidentes con registro y métricas. El autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) ubica el dominio en nivel Gestionado con 70 sobre 100. El Instructivo de Gestión de Incidentes de Seguridad de la Información (AP-GI-I-16) está documentado, sin embargo, como se señala en el control A.5.24, "no cubre la totalidad del ciclo de vida del incidente".
A.5.27	Aprendizaje de incidentes de seguridad	No Cumple	El Plan de Seguridad y Privacidad de la Información (AP-GI-PL-02-07, Estrategia 4) menciona las lecciones aprendidas como entregable esperado. No se evidencia en la documentación del proceso un registro de lecciones aprendidas de incidentes previos. En la visita se constata que se han presentado incidentes de seguridad ocasionados por la misma vulnerabilidad (ej. KLA73122) en períodos sucesivos. El Instructivo de Gestión de Incidentes de Seguridad de la Información (AP-GI-I-16) no incluye un mecanismo de registro y seguimiento de lecciones aprendidas.
A.5.28	Recolección de evidencia	Cumple parcial	El Instructivo de Análisis de Vulnerabilidades (AP-GI-I-23-01) establece procedimientos de identificación de vulnerabilidades, y el Instructivo de Retiro de Activos (AP-GI-I-41-01) menciona la cadena de custodia de activos. No se evidencia un procedimiento específico de recolección, preservación y cadena de custodia de evidencia digital para procesos de investigación de incidentes de seguridad.
A.5.29	Seguridad de la información durante una interrupción	Cumple parcial	Se observa que el Instructivo de Recuperación de Desastres contempla la disponibilidad de sistemas durante interrupciones. El autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) ubica la continuidad del negocio en nivel Gestionado con 77 sobre 100. El Plan de Seguridad y Privacidad de la Información (AP-GI-PL-02-07) contempla la integración de la gestión de incidentes con los planes de continuidad. No se evidencia la inclusión explícita de controles de Confidencialidad, Integridad y Disponibilidad (CID) dentro del plan de recuperación ante desastres (DRP) para su aplicación durante contingencias.
A.5.30	Preparación de TIC para continuidad del negocio	Cumple	El Instructivo de Recuperación de Desastres y el Plan de Continuidad del Negocio (ES-GE-PL-03) están documentados. El autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) ubica el dominio en nivel Gestionado con 77 sobre 100. El Plan de Seguridad y Privacidad de la Información (AP-GI-.PL-02-07) contempla la realización de ejercicios y simulacros como entregable pendiente vigencia 2026.
A.5.31	Requisitos legales, estatutarios, reglamentarios y contractuales	Cumple Parcial	El Plan de Seguridad y Privacidad de la Información (AP-GI-PL-02-07) y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (AP-GI-PL-03-06) incluyen una matriz de requisitos normativos que abarca la Ley 1581 de 2012, la Ley 1712 de 2014, el Decreto 1078 de 2015, la Resolución 500 de 2021 y el Modelo de Seguridad y Privacidad de la Información (MSPI). El autodiagnóstico ubica el cumplimiento normativo en 68,5 sobre 100. En la visita se confirma desactualización normativa en la documentación, Ej. (Resolución 2277 de 2025, norma ISO/IEC 27001:2013).

Código	Control	Cumplimiento	Observación
A.5.32	Derechos de propiedad intelectual	Cumple	Se observa que el Instructivo de Adquisición y Mantenimiento de Software regula la gestión, el licenciamiento y el control del software institucional. La Política de Seguridad de las Operaciones del Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) complementa este control. En la visita se verifica el cumplimiento del control a través del informe de derechos de autor y las políticas de gestión configuradas en los dispositivos institucionales.
A.5.33	Protección de registros	Cumple parcial	El Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) establece controles de acceso y protección de la información, y el Instructivo de Generación de Copias de Seguridad – Backups (AP-GI-I-03) define el respaldo de información crítica. No se evidencia un mecanismo de retención y protección de registros y documentos individuales. En la visita se verifica la existencia de registros de auditoría (logs) en el (ERP). Se recomienda definir una política de retención, protección y custodia de registros y documentos.
A.5.34	Privacidad y protección de datos personales	Cumple parcial	El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (AP-GI-PL-03-06) y el Plan de Seguridad y Privacidad de la Información (AP-GI-PL-02-07) incorporan explícitamente la Ley 1581 de 2012 y el Decreto 1377 de 2013. El Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) incluye política de privacidad. La entidad cuenta con la Política de Tratamiento de Datos Personales publicada y con el Manual de Historias Clínicas que regula la reserva legal del historial clínico. En la visita se constata que no existe un procedimiento documentado para la gestión integral de solicitudes de derechos de datos personales, como acceso, rectificación, cancelación y oposición.
A.5.35	Revisión independiente de la seguridad de la información	Cumple	El Plan de Seguridad y Privacidad de la Información (AP-GI-PL-02-07) contempla la verificación como parte del ciclo (PHVA) del Sistema de Gestión de Seguridad de la Información (SGSI). El autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) 2025 constituye una revisión de madurez. Para la actual vigencia se observa una evaluación al Sistema de Gestión de Seguridad de la Información (SGSI).
A.5.36	Cumplimiento de políticas, normas y estándares	Cumple parcial	El Plan de Seguridad y Privacidad de la Información (AP-GI-PL-02-07, Estrategia 1) contempla indicadores y reportes periódicos de cumplimiento. El autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) con corte de noviembre de 2025 registra un promedio de 66 sobre 100. No se evidencia un mecanismo para la verificación periódica del cumplimiento de políticas de seguridad por parte de los líderes de proceso.
A.5.37	Procedimientos de operación documentados	Cumple	Se evidencia en Almera la existencia de instructivos documentados para las actividades operativas de seguridad de la Información: copias de seguridad, análisis de vulnerabilidades, gestión de cambios, acceso a sistemas, protección contra códigos maliciosos, separación de ambientes, acuerdos con proveedores y transferencia de información, entre otros. En la visita se verifica que documentos como el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, Manual de Políticas de Seguridad y Privacidad de la Información, hacen referencia a la norma ISO/IEC 27001:2013, conforme a lo evidenciado en el numeral A.5.31. Se recomienda actualizar los documentos para alinearlos con los requisitos de la norma ISO/IEC 27001:2022 vigente.

Fuente: Elaboración Oficina de Control Interno – Basada en Anexo A del lineamiento del MSPI

Tabla No. 4: Dominio A.6 – Controles de Personas (8 controles)

Código	Control	Cumplimiento	Observación
A.6.1	Verificación de antecedentes	Cumple	El Instructivo de Ingreso y Desvinculación del Personal establece controles al momento de la vinculación del personal. En la visita se verifica que, durante el proceso de selección y contratación, se realizan validaciones de antecedentes a través de la Dirección de Contratación y la Dirección de Talento Humano. Adicionalmente, cada proveedor de servicios debe diligenciar el formato (SARLAFT) de conocimiento del cliente, con las validaciones reglamentarias correspondientes.
A.6.2	Términos y condiciones de empleo	Cumple parcial	Se observa que el Instructivo de Ingreso y Desvinculación del Personal exige la suscripción de acuerdos de confidencialidad previo al otorgamiento de accesos, y el Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) establece la obligatoriedad de cumplimiento de las políticas para el personal. En la visita se verifica que la minuta de los contratos de prestación de servicios incluye cláusula de confidencialidad y referencia al cumplimiento de las políticas de seguridad y privacidad de la información.
A.6.3	Concienciación, educación y formación en seguridad	Cumple parcial	El Plan de Seguridad y Privacidad de la Información (AP-GI-PL-02-07, Estrategia 3 – Concientización) establece como entregable un plan anual de capacitación y sensibilización. El autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) ubica la seguridad de los recursos humanos en nivel Gestionado con 67 sobre 100. En la visita se verifica la existencia de un cronograma de capacitación que incluye dos temas relacionados con seguridad y privacidad de la información. Se recomienda ampliar la cobertura temática, garantizar la ejecución y registrar evidencias de participación del personal.
A.6.4	Proceso disciplinario	Cumple parcial	El Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) establece la obligatoriedad del cumplimiento de las políticas de seguridad. No se evidencia el tratamiento de incumplimientos de seguridad de la información, integrado con los procesos de Talento Humano.
A.6.5	Responsabilidades tras finalización o cambio de empleo	Cumple parcial	El Instructivo de Ingreso y Desvinculación del Personal establece la revocación de accesos sobre el (ERP), el Directorio Activo (Active Directory), el correo electrónico, la red privada virtual (VPN) y las aplicaciones al momento de la desvinculación y el Formato de Creación, Modificación e Inactivación de Usuarios en Sistemas de Información (AP-GI-F-40) soporta el proceso. En la visita se verifica el cumplimiento de la revocación de accesos en el sistema Dinámica Gerencial y el correo electrónico; no obstante, no se evidencia la revocación en otros servicios como el dominio de red.
A.6.6	Acuerdos de confidencialidad o no divulgación	Cumple parcial	El Instructivo de Ingreso y Desvinculación del Personal exige acuerdos de confidencialidad previo al otorgamiento de accesos. El Instructivo para el Tratamiento de la Seguridad en los Acuerdos con los Proveedores establece requisitos de confidencialidad para terceros. En la visita se verifica que los acuerdos de confidencialidad en el tratamiento de historias clínicas se encuentran formalizados a través del Manual de Historias Clínicas.
A.6.7	Trabajo remoto	Cumple	Se observa que en el Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04), se incluye la Política de Teletrabajo en modalidad suplementaria, que establece el uso de red privada virtual (VPN) como Client-to-Site, antivirus actualizado en los dispositivos y controles específicos para el trabajo remoto. Los formularios AP-TH-F-122-01 y AP-TH-F-123-01, el Procedimiento de Teletrabajo AP-TH-P-06 y el Manual de Políticas de Teletrabajo soportan este control. En la visita se verifica la existencia de

Código	Control	Cumplimiento	Observación
			solicitudes autorizadas de conexión a la red privada virtual para teletrabajadores.
A.6.8	Reporte de eventos de seguridad de la información	Cumple	El Plan de Seguridad y Privacidad de la Información (AP-GI-PL-02-07, Estrategia 4) contempla el canal de reporte de incidentes. El Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) incluye la Política de Gestión de Incidentes. En la visita se verifica que el reporte de eventos de seguridad se realiza a través de la mesa de servicios y que el Instructivo de Reporte de Incidentes (AP-GI-I-30) establece la forma en que debe realizarse el reporte.

Fuente: Elaboración Oficina de Control Interno – Basada en Anexo A del lineamiento del MSPI

Tabla No. 5 Dominio A.7 – Controles Físicos (14 controles)

Código	Control	Cumplimiento	Observación
A.7.1	Perímetros de seguridad física	Cumple	El Instructivo de Control de Acceso Físico define las áreas críticas de la entidad, incluyendo centros de datos, salas de servidores, cuartos de comunicaciones. El Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) establece la Política de Seguridad Física y del Entorno. El autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) ubica la seguridad física en nivel Gestionado con 74 sobre 100.
A.7.2	Entrada física	Cumple	El Instructivo de Control de Acceso Físico y el Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) establecen los mecanismos de autenticación física. En la visita se verifica que el centro de datos de la sede Chapinero cuenta con control biométrico de acceso y planilla de control de ingreso mediante el Formato de Control de Ingreso al Centro de Datos (AP-GI-F-55-01). Se identifica que la versión actual del formato es la versión 2, por lo que se recomienda verificar y actualizar a la versión del documento en el sistema de gestión.
A.7.3	Seguridad de oficinas, despachos e instalaciones	Cumple	El Instructivo de Protección de Activos y la Política de Seguridad Física y del Entorno del Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) establecen los controles de seguridad en oficinas e instalaciones, incluyendo la política de escritorio limpio. En la visita se verifica que el personal de seguridad física realiza control de ingreso a las oficinas. No obstante, se observa que los usuarios no bloquean la sesión de sus equipos de cómputo al ausentarse del puesto de trabajo. Se recomienda reforzar la política de pantalla limpia y configurar el bloqueo automático de sesión.
A.7.4	Monitorización de la seguridad física	Cumple	Se observa que el Instructivo de Control de Acceso Físico establece el monitoreo y la trazabilidad de ingresos y salidas mediante bitácoras, sistemas electrónicos y circuito cerrado de televisión (CCTV). En la visita se verifica que el centro de datos de la sede Chapinero no cuenta con cámaras de seguridad según el numeral 4.7.3 del instructivo. El control compensatorio vigente en dicha sede es la bitácora de acceso física y el control biométrico de ingreso.
A.7.5	Protección contra amenazas físicas y ambientales	Cumple	Se evidencia que el Instructivo de Recuperación de Desastres contempla las amenazas físicas y ambientales como parte de la planificación de continuidad. El autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) ubica el dominio de continuidad en nivel Gestionado con 77 sobre 100. En la visita se verifica que las condiciones están articuladas con el plan hospitalario de gestión del riesgo institucional, y que las instalaciones cuentan con sistema de aire acondicionado, alarma contra incendios, sistema de alimentación ininterrumpida (UPS) y planta eléctrica de respaldo. Las sedes de menor tamaño cuentan con sistemas de alimentación ininterrumpida (UPS).

Código	Control	Cumplimiento	Observación
A.7.6	Trabajo en áreas seguras	Cumple parcial	El Instructivo de Protección de Activos y el Instructivo de Control de Acceso Físico establecen restricciones de acceso a áreas críticas, respaldadas por la sección 6.8 del Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04). En la visita se confirma que no existen lineamientos específicos para el trabajo en áreas seguras que regulen aspectos para la prohibición del uso de dispositivos de almacenamiento externo, cámaras o equipos no autorizados en cuartos de servidores.
A.7.7	Escritorio limpio y pantalla limpia	Cumple parcial	La Política de Buenas Prácticas del Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) establece los controles de escritorio y pantalla limpia. En la visita se confirma que no existe verificación periódica de esta política ni registros de su cumplimiento, ni se evidencian controles de bloqueo automático de sesión configurados en los equipos de los usuarios. Situación que es consistente con lo observado en el control A.7.3.
A.7.8	Ubicación y protección de los equipos	Cumple	El Instructivo de Mantenimiento de Equipos establece la planificación, el registro, el inventario de equipos y la verificación de la seguridad de la información durante las actividades de mantenimiento. El Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) complementa este control en la sección 6.8. En la visita se verifica que los cuartos principales de cableado y el centro de datos cuentan con dispositivos de protección eléctrica de equipos.
A.7.9	Seguridad de activos fuera de las instalaciones	Cumple parcial	El Instructivo de Retiro de Activos establece los controles para el retiro, la devolución y la baja de activos, incluyendo el borrado seguro y la cadena de custodia. La Política de Teletrabajo del Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) establece controles para el uso de equipos (hardware) fuera de las instalaciones, no incluye otros activos. El soporte documental del proceso se registra en el Formato AP-GI-F-40. En la visita se verifica el uso de red privada virtual (VPN) por parte de los teletrabajadores como control de acceso remoto.
A.7.10	Medios de almacenamiento	Cumple parcial	El Instructivo de Transferencia de Información (AP-GI-I-44-01) y el Instructivo de Generación de Copias de Seguridad – Backups (AP-GI-I-03) establecen controles sobre los medios de almacenamiento. El Plan de Disposición Final de Residuos Tecnológicos de Tecnologías de la Información – Residuos de Aparatos Eléctricos y Electrónicos (AP-GI-PL-05) regula la disposición final. En la visita se constata que los documentos de gestión documental en el sistema Almera no pueden descargarse directamente: requieren autorización del área de calidad y se generan con marca de agua como control de trazabilidad. No se evidencia un procedimiento integral del ciclo de vida de los medios de almacenamiento removibles.
A.7.11	Servicios de suministro	Cumple	El Instructivo de Recuperación de Desastres contempla los requerimientos de disponibilidad de infraestructura. El Instructivo de Aseguramiento de Servicios en la Red (AP-GI-I-48-01) aplica a este control. En la visita se verifica a través de formatos de mantenimiento, que las sedes principales (Fray, Simón Bolívar, Suba, Engativá y Chapinero) cuentan con sistema de alimentación ininterrumpida (UPS) y planta eléctrica de respaldo, como mecanismos de redundancia del suministro eléctrico.
A.7.12	Seguridad del cableado	Cumple parcial	El Instructivo de Aseguramiento de Servicios en la Red (AP-GI-I-48-01) establece los parámetros de configuración de la infraestructura de red. En la visita se verifica la existencia de cableado estructurado instalado mediante tuberías, canaletas y escalerillas en los niveles 6 (con 2.968 puntos) y 6A (con 1.879 puntos). Sin embargo, no se evidencia la certificación vigente de dicho cableado estructurado. y formalizarla en el expediente de infraestructura. Se recomienda

Código	Control	Cumplimiento	Observación
			realizar lo correspondiente para mantener la certificación y la documentación en completitud en el expediente de infraestructura.
A.7.13	Mantenimiento de equipos	Cumple	El Instructivo de Mantenimiento de Equipos establece la planificación, el registro, el inventario y el mantenimiento preventivo y correctivo de equipos, con verificación de la seguridad de la información y cierre documentado. El Plan de Mantenimiento de la Infraestructura y Dotación (AP-AT-PL-05-02) y el plan de mantenimiento de equipos de cómputo complementan este control. En la visita se verifica la existencia de un plan de mantenimiento con seguimiento documentado (hoja de vida) de las actividades de mantenimiento preventivo y correctivo realizadas a los equipos de cómputo (hardware y software).
A.7.14	Eliminación o reutilización segura de equipos	Cumple parcial	El Instructivo de Retiro de Activos (AP-GI-I-41-01) establece el borrado seguro de la información antes del retiro o reutilización de equipos, con cadena de custodia documentada. El Plan de Disposición Final de Residuos Tecnológicos de Tecnologías de la Información – Residuos de Aparatos Eléctricos y Electrónicos (AP-GI-PL-05) formaliza la gestión de residuos tecnológicos. En la visita realizada no se evidencian registros de ejecución del proceso de disposición final de residuos tecnológicos para la vigencia 2025. Se recomienda ejecutar y documentar conforme al plan establecido.

Fuente: Elaboración Oficina de Control Interno – Basada en Anexo A del lineamiento del MSPI

Tabla No. 6: Dominio A.8 – Controles Tecnológicos (34 controles)

Código	Control	Cumplimiento	Observación
A.8.1	Dispositivos de punto final del usuario	Cumple	El Instructivo de Protección contra Códigos Maliciosos establece las directrices para el uso de herramientas de antivirus y antimalware, la detección de amenazas, la respuesta ante infecciones y la recuperación de los sistemas. El Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) incluye la Política de Dispositivos Móviles. En la visita se verifica la implementación de controles de antivirus, certificado de capa de puertos seguros (SSL) y gestión de dominio en los equipos institucionales.
A.8.2	Derechos de acceso privilegiado	Cumple parcial	En el Instructivo de Ingreso Seguro a los Sistemas de Información (AP-GI-I-48-01) hace referencia a la revisión trimestral de privilegios de usuarios, la autenticación multifactor (MFA) para accesos críticos y el monitoreo de accesos privilegiados. El autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) ubica el control de acceso en nivel Optimizado con 81 sobre 100. En la visita se verifica la ejecución de actividades de ajuste fino (tuning) en la base de datos como parte de la gestión de accesos privilegiados. Se recomienda documentar registros de las revisiones periódicas de cuentas con privilegios elevados, como se determina en el instructivo.
A.8.3	Restricción de acceso a la información	Cumple	El Instructivo de Ingreso Seguro a los Sistemas de Información establece el principio de mínimo privilegio y la segregación de funciones. La Política de Control de Acceso del Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) lo complementa. En la visita se verifica el cumplimiento de este control a través de la Política de Gestión de Accesos.
A.8.4	Acceso al código fuente	Cumple parcial	El Instructivo de Adquisición y Mantenimiento de Software regula el control del software institucional. En la visita se declara que este control no aplica, sin que se aporte la justificación correspondiente. Se recomienda documentar la declaración de no aplicabilidad, indicando si la entidad no desarrolla software propio o si el desarrollo es completamente externalizado, conforme a los requisitos de la norma ISO/IEC 27001:2022 para controles excluidos.

Código	Control	Cumplimiento	Observación
A.8.5	Autenticación segura	Cumple parcial	El Instructivo de Ingreso Seguro a los Sistemas de Información establece la autenticación multifactor (MFA), contraseñas de acceso con parámetros de bloqueo por intentos fallidos y supervisión de alertas de acceso no autorizado. El autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) ubica el control de acceso en nivel Optimizado con 81 sobre 100. En la visita se verifica la implementación de autenticación en el (ERP) Dinámica Gerencial. Se recomienda extender la verificación de la configuración al Directorio Activo (Active Directory) y a los demás sistemas críticos.
A.8.6	Gestión de la capacidad	Cumple parcial	El Plan de Seguridad y Privacidad de la Información (AP-GI-PL-02-07) contempla la revisión en tiempo real del estado y las vulnerabilidades de los equipos. El Instructivo de Aseguramiento de Servicios en la Red (AP-GI-I-48-01) establece la supervisión continua. Se cuenta con el Instructivo de Gestión de Capacidad (AP-GI-I-47) del proceso de gestión de capacidad. Sin embargo, en la visita realizada no se evidenció registro de aplicación de las actividades de gestión de capacidad definidas.
A.8.7	Protección contra malware	Cumple	El Instructivo de Protección contra Códigos Maliciosos establece la identificación de sistemas que requieren protección antimalware, la detección de amenazas, la respuesta ante infecciones (contención y erradicación) y la recuperación de los sistemas. Se recomienda verificar la fecha de la última actualización de firmas de la solución antimalware y los registros de eventos recientes.
A.8.8	Gestión de vulnerabilidades técnicas	Cumple parcial	El Instructivo de Análisis de Vulnerabilidades (AP-GI-I-23-01) establece los procedimientos de identificación de vulnerabilidades técnicas. El Plan de Seguridad y Privacidad de la Información (AP-GI-PL-02-07) contempla el fortalecimiento del endurecimiento de plataformas y las operaciones seguras. No se evidencia una periodicidad definida para la ejecución de escaneos de vulnerabilidades ni registro de planes de remediación y seguimiento.
A.8.9	Gestión de la configuración	Cumple parcial	El Instructivo de Aseguramiento de Servicios en la Red (AP-GI-I-48-01) establece la configuración de firewalls, redes de área local virtuales (VLAN) y segmentación lógica. El Instructivo de Gestión de Cambios (AP-GI-I-36) controla las modificaciones a la infraestructura. No se evidencia la existencia de líneas base de configuración segura documentadas por servicio y/o tipo de dispositivo.
A.8.10	Eliminación de información	Cumple parcial	En el Instructivo de Retiro de Activos (AP-GI-I-41-01) se establece el borrado seguro de la información previo al retiro o reutilización de equipos. En la visita no se presentan registros de borrado seguro.
A.8.11	Enmascaramiento de datos	Cumple parcial	El Instructivo de Separación de Ambientes establece el uso de datos de prueba ficticios o enmascarados en los ambientes de desarrollo y pruebas, con el fin de no comprometer datos reales de usuarios o pacientes. En la visita se verifica que el entorno de pruebas del ERP, contempla información relevante de pacientes y/o usuarios sin anonimización o enmascaramiento. Se recomienda verificar que el enmascaramiento se aplique efectivamente en las pruebas de sistemas que operan con datos de pacientes y controlar su cumplimiento.
A.8.12	Prevención de fuga de datos	Cumple parcial	En el Instructivo de Transferencia de Información (AP-GI-I-44-01) establece controles de clasificación y uso de canales seguros para las transferencias de información. El Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) incluye controles antispam y de filtrado de contenido. No se evidencia la implementación de una solución de prevención de pérdida de datos (DLP) a nivel de endpoint o de red. Se recomienda documentar los controles compensatorios vigentes.

Código	Control	Cumplimiento	Observación
A.8.13	Respaldo de la información	Cumple parcial	El Instructivo de Generación de Copias de Seguridad – Backups (AP-GI-I-03) establece esquemas de frecuencia diaria, semanal y mensual, almacenamiento en nube externa (plataforma Azure de Microsoft), y pruebas de restauración con periodicidad semanal y mensual. La Política de Copias de Respaldo del Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) complementa este control. En la visita se evidencia que la información contenida en equipos de cómputo no se respalda. Se recomienda registrar las últimas pruebas de restauración exitosa, las evidencias de almacenamiento externo y la extensión del respaldo para la información crítica alojada en equipos de escritorio.
A.8.14	Redundancia de instalaciones de procesamiento	Cumple	Se observa que Instructivo de Recuperación de Desastres contempla la disponibilidad de los sistemas. El autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) ubica la continuidad en nivel Gestionado con 77 sobre 100. Se evidencia documentación de arquitectura con componentes redundantes para los sistemas críticos.
A.8.15	Registro de actividades (logging)	Cumple parcial	El Instructivo de Aseguramiento de Servicios en la Red (AP-GI-I-48-01) establece el registro de alertas en switches, firewalls, routers y servidores. El Instructivo de Ingreso Seguro a los Sistemas de Información establece la auditoría de accesos. No se evidencia un mecanismo documentado para la retención de registros de auditoría (logs) ni controles de protección contra alteración.
A.8.16	Actividades de monitoreo	Cumple parcial	El Instructivo de Aseguramiento de Servicios en la Red (AP-GI-I-48-01) establece la supervisión mediante herramientas de monitoreo y el registro de alertas. El autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) ubica la seguridad de operaciones en nivel Gestionado con 79 sobre 100. En la visita se observa que el Log de transacciones del ERP, se conserva integro desde su primera transacción. Se recomienda verificar la herramienta de monitoreo con cobertura sobre sistemas críticos.
A.8.17	Sincronización de relojes	Cumple	El Instructivo de Aseguramiento de Servicios en la Red (AP-GI-I-48-01) abarca la configuración de la infraestructura de red. En la visita se verifica la existencia de un servidor de protocolo de tiempo de red (NTP), sincronizado contra la Hora Legal de Colombia, certificada por la Superintendencia de Industria y Comercio.
A.8.18	Uso de programas de utilidades privilegiadas	Cumple parcial	El Instructivo de Adquisición y Mantenimiento de Software y el Instructivo de Ingreso Seguro a los Sistemas de Información regulan los accesos y el uso del software. En la visita se informa la existencia de 20 usuarios con perfil de administrador. No se evidencia un control específico sobre herramientas de utilidades privilegiadas, como consolas de administración y herramientas de diagnóstico de red. Se recomienda documentar el inventario de herramientas privilegiadas autorizadas y los controles de uso.
A.8.19	Instalación de software en sistemas operativos	Cumple	Se evidencia la existencia del Instructivo de Adquisición y Mantenimiento de Software, que regula la instalación y el control del software institucional. La Política de Seguridad de las Operaciones del Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) lo complementa. Se recomienda verificar la lista de software autorizado, el mecanismo de restricción de instalación usuarios y los registros de control.

Código	Control	Cumplimiento	Observación
A.8.20	Seguridad en redes	Cumple	Se observa que los Instructivos de: Aseguramiento de Servicios en la Red (AP-GI-I-48-01), de Servicio de Gestión de la Infraestructura, Redes y Comunicaciones (AP-GI-I-07) establecen la configuración de firewalls, redes de área local virtuales (VLAN), segmentación lógica y supervisión continua. La Política de Seguridad en las Comunicaciones del Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) lo complementa. En la visita se verifica el diagrama de red actualizado, la documentación de segmentación por redes de área local virtuales (VLAN) y la configuración de firewall.
A.8.21	Seguridad de los servicios de red	Cumple parcial	El Instructivo para el Tratamiento de la Seguridad en los Acuerdos con los Proveedores establece cláusulas de seguridad y mecanismos de seguimiento con proveedores de servicios de red. No se evidencia un mecanismo específico de verificación de acuerdos de nivel de servicio de seguridad con operadores de telecomunicaciones.
A.8.22	Segregación de redes	Cumple	El Instructivo de Separación de Ambientes establece la separación entre los ambientes de desarrollo, pruebas y producción. El Instructivo de Aseguramiento de Servicios en la Red (AP-GI-I-48-01) establece las redes de área local virtuales (VLAN) y la segmentación lógica. En la visita se verifica el diagrama de red actualizado con la segmentación implementada.
A.8.23	Filtrado web	Cumple	El Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) establece el uso de antivirus, antispam y filtros de contenido. El Instructivo de Protección contra Códigos Maliciosos contempla controles preventivos de navegación. En la visita se verifica la existencia de una solución de filtrado web activa, con listas de categorías bloqueadas y cobertura de red.
A.8.24	Uso de criptografía	No cumple	El autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) 2025 ubica la criptografía en nivel INEXISTENTE con 0 sobre 100, identificándola como brecha crítica. El Plan de Seguridad y Privacidad de la Información (AP-GI-PL-02-07, Estrategia 3) prioriza el fortalecimiento de los controles de criptografía. El Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) menciona el cifrado de correos con información confidencial y el uso de firmas digitales; sin embargo, no existe una política de criptografía que defina algoritmos aprobados, longitudes de clave, gestión del ciclo de vida de certificados y casos de uso obligatorio. En la visita no se registran observaciones adicionales que modifiquen la calificación.
A.8.25	Ciclo de vida del desarrollo seguro	No Aplica	El Instructivo de Separación de Ambientes y el Instructivo de Gestión de Cambios (AP-GI-I-36) incluyen controles en el proceso de desarrollo de software. El Plan de Seguridad y Privacidad de la Información (AP-GI-PL-02-07) contempla la implementación del ciclo de vida de desarrollo seguro (SDL) como meta. En la visita se declara que este control no aplica, sin que se aporte la justificación correspondiente. Se recomienda documentar la declaración de no aplicabilidad conforme a los requisitos de la norma ISO/IEC 27001:2022.
A.8.26	Requisitos de seguridad de las aplicaciones	No Aplica	El Instructivo de Gestión de Cambios (AP-GI-I-36) incluye el análisis de impacto en seguridad y la verificación por parte del Oficial de Seguridad de la Información (CISO). En la visita se declara que este control no aplica, sin que se aporte la justificación correspondiente. Se recomienda documentar la declaración de no aplicabilidad o, si aplica, del proceso de levantamiento de información de requisitos de seguridad desde el inicio del ciclo de vida de las aplicaciones, conforme al requisito 6.1.3 de la norma ISO/IEC 27001:2022.

Código	Control	Cumplimiento	Observación
A.8.27	Arquitectura de sistemas seguros	Cumple parcial	El Plan de Seguridad y Privacidad de la Información (AP-GI-PL-02-07) contempla el endurecimiento de plataformas como meta de la Estrategia 3. No se evidencia documentación de arquitectura de referencia segura que incorpore principios de defensa en profundidad, mínimo privilegio y diseño orientado a fallar de forma segura.
A.8.28	Codificación segura	No Aplica	El Instructivo de Adquisición y Mantenimiento de Software regula el proceso de desarrollo. Se evidencia la adopción de estándares de codificación segura (Proyecto Abierto de Seguridad en Aplicaciones Web – OWASP, o equivalentes) proporcionadas a título personal por el desarrollador. En la visita se declara que este control no aplica, sin que se aporte justificación correspondiente. Se recomienda documentar la declaración de no aplicabilidad conforme a la norma ISO/IEC 27001:2022.
A.8.29	Pruebas de seguridad en desarrollo y aceptación	Cumple	El Instructivo de Gestión de Cambios (AP-GI-I-36) establece pruebas técnicas y funcionales antes del paso a producción, con validación del Oficial de Seguridad de la Información (CISO). En la visita se verifica la realización de pruebas de seguridad en el proyecto Meliportal, incluyendo actividades de análisis de vulnerabilidades en el proceso de aceptación.
A.8.30	Desarrollo externalizado	Cumple parcial	El Instructivo para el Tratamiento de la Seguridad en los Acuerdos con los Proveedores establece cláusulas de seguridad aplicables al desarrollo externalizado. No se evidencia un proceso de revisión del código de terceros, pruebas de aceptación de seguridad ni auditoría de proveedores de desarrollo de software.
A.8.31	Separación de ambientes de desarrollo, pruebas y producción	Cumple parcial	El Instructivo de Separación de Ambientes establece la separación entre los ambientes de desarrollo, pruebas y producción, así como el uso de datos ficticios o enmascarados en ambientes no productivos. En la visita se verifica que el sistema de planificación de recursos empresariales (ERP) cuenta con ambiente de pruebas. No obstante, se evidencia que en las réplicas de bases de datos para pruebas no se anonimiza la información de pacientes u otros datos sensibles.
A.8.32	Gestión de cambios	Cumple	El Instructivo de Gestión de Cambios (AP-GI-I-36) establece el proceso de gestión de cambios con clasificación por impacto, análisis de riesgo con el Oficial de Seguridad de la Información (CISO), aprobación del Jefe de Sistemas, pruebas y validación, documentación de la implementación y plan de retorno (rollback). El autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI) ubica el dominio de adquisición y desarrollo en nivel Gestionado con 61 sobre 100.
A.8.33	Información de pruebas	No Cumple	El Instructivo de Separación de Ambientes establece el uso de datos ficticios o enmascarados en los ambientes de pruebas. No obstante, el equipo auditor constató que en las réplicas de bases de datos utilizadas en los procesos de prueba no se aplica la anonimización de la información sensible, incluyendo datos de pacientes, contrario a lo establecido en el instructivo, constituyendo un incumplimiento del control.
A.8.34	Protección de sistemas durante pruebas de auditoría	Cumple parcial	El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (AP-GI-PL-03-06) contempla la gestión de riesgos sobre los sistemas de información. No se evidencia un procedimiento específico de coordinación de pruebas de auditoría sobre sistemas en producción. En la visita se verifica que el sistema (ERP) Dinámica Gerencial, mantiene registros de auditoría (logs) desde enero de 2023, con trazabilidad de la primera transacción registrada.

Fuente: Elaboración Oficina de Control Interno – Basada en Anexo A del lineamiento del MSPI

La verificación de 93 controles del Anexo A de los lineamientos del MSPI, evidencia avances en controles físicos, copias de seguridad y gestión de accesos, al tiempo que evidencia oportunidades de mejora en criptografía, etiquetado de la información, aprendizaje de incidentes y protección de datos en ambientes de prueba.

Tabla No. 7: Resultados por Dominio

Dominio	Controles	Cumple	Cumple Parcial	No Cumple	No Aplica	% C
A.5 – Controles Organizacionales	37	13	21	2	0	35.1%
A.6 – Controles de Personas	8	3	5	0	0	37.5%
A.7 – Controles Físicos	14	8	6	0	0	57.1%
A.8 – Controles Tecnológicos	34	12	1	2	3	38.7%
TOTAL	93	36	50	4	3	40%

Fuente: Elaboración Oficina de Control Interno – Basada en Anexo A del lineamiento del MSPI

El dominio A.6 Controles de Personas registra el nivel de cumplimiento más bajo (37.5%), con 5 de los 8 controles en estado Cumple Parcial. El dominio A.7 Controles Físicos es el de mayor madurez, con un 57.1% de controles en estado Cumple.

Los 50 controles en estado Cumple Parcial presentan implementación incompleta, evidencia limitada o ejecución inconsistente.

Se identificaron 4 controles en estado No Cumple, que constituyen hallazgos. Adicionalmente, 3 controles declarados “No Aplica” (A.8.25, A.8.26, A.8.28) carecen de justificación documentada, lo que representa una oportunidad de mejora.

4.1.4 Revisión de los resultados de desempeño institucional - vigencia 2023 - 2024.

Con el propósito de contrastar la efectividad de los controles frente a los resultados de la Medición del Desempeño Institucional (MDI), reportados en el Formulario Único de Reporte y Avance de Gestión (FURAG), se presenta el siguiente balance sobre el comportamiento de la política de "Seguridad Digital" y el índice de "Seguridad y Privacidad de la Información" para las vigencias 2023 y 2024:

Tabla No. 8: Resultados de evaluación Índice de Desempeño Institucional

Indicador	2023	2024	Observación
Política Seguridad Digital	89,2	96,5	La variación +7,3 puntos muestran fortalecimiento de la Estrategia de Seguridad Digital y del SGSI/MSPI.
Implementación Lineamientos de la Política	86,7	96,7	la variación de +10 puntos, muestra un avance en la adopción de los lineamientos del MSPI y de la política de seguridad digital del MinTIC.
Índice Seguridad y Privacidad de la información	91,7	88,7	La variación de −3 puntos, muestra que, aunque el valor sigue siendo alto, la tendencia es descendente, lo que sugiere oportunidades de mejora en la operación del MSPI (gestión de riesgos, controles, incidentes, vulnerabilidades, madurez de dominios tipo criptografía, activos, proveedores).

Fuente: Elaboración Oficina de Control Interno – Basada en resultados FURAG

Los indicadores muestran un desempeño global positivo en la Política de Seguridad Digital, con una mejora en la implementación de lineamientos y un retroceso de 3 puntos en el índice de seguridad y privacidad de la información para la vigencia 2024.

Esta contracción en el Índice Seguridad y Privacidad de la información es consistente con las observaciones y los hallazgos identificadas previamente por esta auditoría (desactualización de guías, escala en medición de activos y gestión de riesgos de seguridad de la información estancados). En particular:

- El puntaje MSPI de 0/100 en Criptografía (Hallazgo H-4), que es el dominio con mayor brecha absoluta y mayor potencial de impacto en el índice
- El puntaje de 57/100 en Gestión de Activos, consistente con las deficiencias estructurales y de actualización del Inventario de Activos
- El puntaje de 66/100 en Gestión de Riesgos, coherente con la ausencia de Indicadores de Riesgos KRI y la problemática identificada en el numeral 4.1.2 del presente informe.

Teniendo en cuenta el comportamiento del resultado de los indicadores, la Oficina de Control Interno recomienda:

- Establecer un esquema de seguimiento a incidentes, vulnerabilidades y brechas detectadas en los autodiagnósticos anuales del MSPI.
- Priorizar la implementación de los proyectos definidos (análisis de vulnerabilidades, controles perimetrales, inventario de activos, cultura de seguridad), priorizando dominios críticos (criptografía, activos y riesgos).
- Asegurar que todos los riesgos priorizados cuenten con controles debidamente implementados, con monitoreo continuo.
- Revisar y ajustar los indicadores de seguridad y privacidad que permitan medir la efectividad del control (tiempos de respuesta, cumplimiento de planes de tratamiento, madurez de dominios).

4.1.5 Indicadores de Gestión

Dentro de la verificación realizada a los indicadores que tiene el subproceso, se identificó que se tienen reportados en el sistema de información Almera, los siguientes indicadores relacionados con seguridad y privacidad de la información:

Imagen No. 2 Indicadores registrados en Aplicativo Almera

Código	Nombre
GI01	Porcentaje de implementación del Plan de Acción de transformación digital definido para la Subred Norte
GI02	Porcentaje de Cumplimiento del Plan de Adquisiciones de Sistemas
GI03	Porcentaje de cumplimiento del plan de trabajo del Plan Estratégico de Tecnologías de la Información PETI.
GI04	Porcentaje de Cumplimiento del Plan de Trabajo de Estabilización DGH.
GI05	Índice de Incidentes de Seguridad de la Información (IISI)
GI06	Porcentaje de Tramites y Servicios Transformados Digitalmente
GI07	Porcentaje de implementación de lineamientos del Marco de Referencia de Arquitectura Empresarial.
GI08	Porcentaje de Implementación de Herramientas Tecnológicas a Nivel Institucional
GI09	Nivel de cumplimiento en el tratamiento de datos personales (TCTDP)
GI10	Adherencia al Manual de Políticas de Seguridad y Privacidad de la Información
GI11	Porcentaje de Trámites y Servicios Digitalizados
GI12	Incidentes de Seguridad y privacidad de la Información
GI13	Incidentes de Seguridad Digital

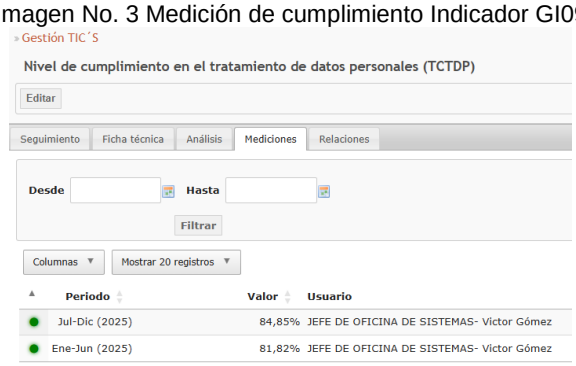
Fuente: Sistema Almera

Al verificar el seguimiento y evaluación de los indicadores, se identificó que *GI05 "Índice de incidentes de seguridad de la información (IISI)" (mensual), GI12 "Incidentes de Seguridad y Privacidad de la información" (trimestral) y GI13 "Incidentes de Seguridad digital" (trimestral)* miden la misma variable, variando únicamente en su periodicidad.

Ante esta situación, se recomienda evaluar la viabilidad de depurar estos indicadores con el fin de unificar el seguimiento y control en una sola métrica.

El indicador GI09 "*Nivel de cumplimiento en el tratamiento de datos personales (TCTDP)*". presenta una meta del 80% con una medición semestral. Durante la vigencia 2025 presentó el siguiente cumplimiento:

Imagen No. 3 Medición de cumplimiento Indicador GI09



Fuente: Sistema Almera

El propósito del indicador es medir el porcentaje de controles de protección de datos personales implementados por la Subred Norte, contrastándolos con los definidos en el Análisis de Brechas (GAP). De acuerdo con los reportes del proceso, los resultados obtenidos demuestran el cumplimiento de la meta establecida.

Frente a la evaluación del indicador GI10 *"Adherencia al manual de políticas de Seguridad y Privacidad de la información"* (medición trimestral, meta del 80%), se identificó un incumplimiento reiterado. Durante la vigencia 2025, la meta solo se superó en el cuarto trimestre con un 88%, mostrando resultados inferiores al 80% en los periodos restantes. Esta situación de rezago persiste en el primer trimestre de 2026.

Imagen No. 4 Medición de cumplimiento Indicador GI10

Fuente: Sistema Almera

Al consultar sobre el incumplimiento de esta meta, la oficina de Sistemas de Información comunica que realizó un análisis en temas de seguridad de la información identificando las principales amenazas identificadas, entre las que se encuentran el phishing, ingeniería social, gestión deficiente de contraseñas y pérdida de datos, y con base en ese análisis planea realizar una capacitación en modalidad virtual dirigido a funcionarios y contratistas mediante la presentación de 6 módulos temáticos que involucran fundamentos cibernéticos, autenticación, privacidad, dispositivos y respuesta a incidentes.

Por otro lado, en atención al documento "*Lineamientos de Indicadores de Gestión de Seguridad de la Información del MSPI" del MINTIC en su capítulo 4,* en el que menciona la implementación de un total de 20 indicadores, se pudo identificar que la entidad solo tiene 2 indicadores implementados y cargados en el sistema de información de Almera.

5 PLANES DE MEJORAMIENTO

En el aplicativo Almera se observaron las siguientes acciones relacionadas con el tema de seguridad y privacidad de la información:

Tabla No. 9: Resumen de Planes de Mejoramiento Relacionados con Seguridad de la Información

Emisor	Año del informe				Acciones identificadas
	2023	2024	2025	2026	
Autoevaluación acreditación (3 informes / planes)	5	4	3		12
Autoevaluación de MIPG (2 informes / Planes)	10	2			12
Control Interno (3 informes / Planes)		3		4	7
Icontec (1 informe/plan)			4		4
Revisoría Fiscal (9 informes /Planes)	9	5	12	5	31
Total general	**24**	**14**	**19**	**9**	**66**

Fuente: Elaboración Oficina de Control Interno

1. Se requiere fortalecer la concientización del personal para reducir errores humanos y mejorar la aplicación de buenas prácticas.
2. Se observan necesidades de actualización, revisión y mejora de los controles para mitigar riesgos materializados en el proceso TIC.
3. Brechas en seguridad perimetral e infraestructura tecnológica, módulos pendientes de implementación y un nivel de madurez de seguridad aún básico, lo que limita la protección efectiva.
4. Acceso físico insuficientemente controlado a áreas críticas, cuartos y racks de comunicaciones con puertas abiertas, cerraduras inoperativas o ausencia de mecanismos adecuados de custodia.
5. Las copias se ejecutan de manera irregular, incluso con medios personales o carpetas compartidas, elevando el riesgo de pérdida de información.
6. El plan de contingencia y los mecanismos de respuesta ante incidentes requieren actualización y ejercicios de validación.
7. Reforzar indicadores, seguimiento y revisión periódica para soportar decisiones y evidenciar el desempeño del sistema.

6 RIESGOS DETECTADOS

Durante el desarrollo del informe se evidenciaron riesgos operacionales y de Seguridad de la información, que afectan la confidencialidad, integridad y disponibilidad de la información. En particular, se destacan los escenarios de acceso no autorizado, indisponibilidad de servicios, manipulación de datos y fallas en la detección oportuna y tratamiento de incidentes de seguridad.

7 FORTALEZAS

Existen controles implementados que están relacionados con la gestión del ciclo de identidades, controles para teletrabajo (VPN y antivirus) y medidas físicas y ambientales en el centro de datos.

La gestión de proveedores y el canal de reporte de incidentes están establecidos y se realizan seguimientos situando algunos dominios de control del modelo de seguridad y privacidad de la información MSPI de en niveles de “Efectivo/Gestionado” (por ejemplo, proveedores 60/100, gestión de incidentes 70/100).

8 OBSERVACIONES Y HALLAZGOS

8.1 Oportunidad de mejora (observaciones)

No: 1	**Numeral: 4.1.3 Domino A7 Controles Físicos**
Descripción	Se evidenció durante la visita fallas de los controles de seguridad física para la restricción de uso de dispositivos de almacenamiento externo, cámaras, así como la no certificación vigente de cableado estructurado, protección de instalaciones, equipos, medios de almacenamiento, cableado, accesos físicos y entornos de trabajo.
Posibles efectos / Riesgos	La materialización de estos eventos (accesos no autorizados, accidentes o daños ambientales), la pérdida de integridad de la información y la afectación en la continuidad del servicio.

No: 2	**Numeral: 4.1.3 Domino A8 Controles Tecnológicos**
Descripción	Se observó que para los controles de seguridad el nivel de madurez es bajo, particularmente en autenticación, control de accesos, auditoría, respaldo, configuración segura, redes, desarrollo seguro y prevención de fuga de información, incrementando el riesgo sobre la confidencialidad, integridad y disponibilidad de la información.
Posibles efectos / Riesgos	Accesos no autorizados, malware, indisponibilidad de sistemas, pérdida de trazabilidad, afectación de servicios críticos y mayor impacto operativo y reputacional.

No: 3	**Numeral: 4.1.3**
Descripción	No se evidenció la declaración de inaplicabilidad, puntualmente para los controles (A.8.25, A.8.26, A.8.28), relacionados con el ciclo de vida del desarrollo seguro, los requisitos de seguridad de aplicaciones y la

	codificación segura, los cuales fueron declarados como "No Aplica". de acuerdo con la norma ISO/IEC 27001:2022 - numeral 6.1.3.
Posibles efectos / Riesgos	Riesgo Operacional, abocar a la entidad a posibles sanciones.

No: 4	**Numeral: 4.1.5 Indicadores de gestión**
Descripción	Se observó en el indicador GI10 "Adherencia al manual de políticas de Seguridad y Privacidad de la información", que durante la vigencia 2025 en tres trimestres y en el primer trimestre de 2026 no se alcanzó la meta de una adherencia superior al 80% por parte de los colabores de la Subred Norte.
Posibles efectos / Riesgos	Riesgo Operacional

8.2 Hallazgo (Incumplimiento)

No 1	**Numeral 4.1.3 A5 Controles Organizacionales**	**Recurrente** **SI NO X**
Descripción	Se evidenció que el Inventario de Activos de Información con código AP-GI-FR-01 presenta desactualización desde el 15 de abril de 2025 y no se encuentra articulado con la matriz de riesgos y carece de análisis de vulnerabilidades y amenazas.	
Criterios	ISO/IEC 27001:2022, Guía para la Gestión Integral del Riesgo en Entidades Públicas v7, Ley 1712 de 2014 artículo 13, Lineamiento para el Inventario y Clasificación de Activos de Información e Infraestructura Crítica Cibernética Nacional del MinTIC v5. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (AP-GI-PL-03-06),	
Posibles efectos / Riesgos	Riesgo Operacional	

No 2	**Numeral 4.1.3 A5 Controles Organizacionales**	**Recurrente** **SI NO X**
Descripción	No existe esquema de etiquetado físico ni digital que identifique el nivel de clasificación de los documentos institucionales. No se evidencia la aplicación del control ni mecanismos automáticos de etiquetado en los sistemas de información.	
Criterios	Control A.5.13 de la norma ISO/IEC 27001:2022 "*Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación de la información adoptado por la organización*"". Manual de Políticas de Seguridad y Privacidad de la Información (AP-GI-M-02-04) contempla la clasificación, pero no el etiquetado operativo	
Posibles efectos / Riesgos	Riesgo Operativo - Reputacional	

No 3	**Numeral 4.1.3 A5 Controles Organizacionales**	**Recurrente** **SI X NO**
Descripción	No se evidenció el registro, seguimiento o retroalimentación sobre situaciones aprendidas por eventos de seguridad previos, adicionalmente, en visita del 4 de junio de 2026 se confirmaron incidentes de seguridad ocasionados por vulnerabilidades como por ejemplo la "KLA67582 falla de ejecución remota de código (RCE) en LibreOffice", presentados en períodos sucesivos. El documento AP-GI-I-16 no incluye el mecanismo para el registro o seguimiento de lecciones aprendidas por eventos reiterativos o recurrentes.	
Criterios	El control A.5.27 de la norma ISO/IEC 27001:2022 "El conocimiento obtenido de los incidentes de seguridad de la información se utilizará para fortalecer y mejorar los controles de seguridad de la información" El Plan AP-GI-PL-02-07 menciona las lecciones aprendidas como entregable esperado (Estrategia 4).	
Posibles efectos / Riesgos	Riesgo Operacional	

No 4	**Numeral 4.1.3 A8 Controles Tecnológicos**	**Recurrente** **SI NO X**
Descripción	No se evidenciaron las reglas para el uso de criptografía que defina los pasos o instrucciones aprobadas de longitudes mínimas de clave, gestión del ciclo de vida de certificados y casos de uso obligatorio. El Manual AP-GI-M-02-04 menciona el cifrado de correos y el uso de firmas digitales, pero sin la política.	
Criterios	El control A.8.24 de la norma ISO/IEC 27001:2022 "Se deben definir e implementar reglas para el uso efectivo de la criptografía, incluida la gestión de claves criptográficas" El Modelo de Seguridad y Privacidad de la Información emitido por MinTIC, establece requisitos específicos para el cifrado de información sensible en entidades públicas de salud. Incumplimiento de la Ley 1581 de 2012 y el Decreto 1078 de 2015	
Posibles efectos / Riesgos	Exposición de información sensible de pacientes y datos institucionales o modificación no autorizada. y los lineamientos MSPI en materia de protección de datos en salud Riesgo Operacional – Reputacional -- Fiscal	

No 5	**Numeral 4.1.3 A8 Controles Tecnológicos**	**Recurrente** **SI NO X**
Descripción	Se evidenciaron copias o réplicas de bases de datos utilizadas en ambiente de prueba del Sistema Dinámica Gerencial (ERP) en las que no se aplicaron técnicas donde se anonimice o proteja la información sensible, incluyendo datos de pacientes. Esta situación contradice lo establecido en el documento AP-GI-I-45 Instructivo de separación de ambientes.	
Criterios	El control A.8.33 de la norma ISO/IEC 27001:2022 indica que "La información de las pruebas se seleccionará, protegerá y gestionará adecuadamente". El Instructivo de Separación de Ambientes - AP-GI-I-45 establece el uso de datos ficticios o enmascarados.	

	La Ley 1581 de 2012 Titulo 3 Articulo 5 “Datos sensibles” se deben proteger datos personales sensibles (datos de salud).
Posibles efectos / Riesgos	Exposición de la entidad a sanciones, Riesgos operacionales y rreputacionales por acceso no autorizado a datos clínicos

8.3 Formulación Plan de Mejoramiento

- Para cada **hallazgo** reportado, debe formular acciones correctivas en el formato “Plan de Mejoramiento Institucional - código ES-GC-F-10-04”, en un plazo no mayor a **cinco (5) días hábiles** contados a partir de la recepción del informe.

Acción Correctiva: Medida tomada para eliminar la causa de una no conformidad (problema) ya detectada, con el fin de evitar su recurrencia.

- Para las **observaciones** identificadas, el proceso auditado decidirá si identifica acciones para incluir en el plan de mejoramiento y en tal caso debe reportarlo además a la oficina de control interno en el plazo señalado anteriormente.

Acción Preventiva: Conjunto de acciones proactivas tomadas para eliminar la causa de un problema potencial u otra situación indeseable que aún no ha sucedido.

La oficina de control interno verificará la eficiencia y efectividad de estas.

9. RECOMENDACIONES

Actualizar el Manual de Políticas (AP-GI-M-02) y demás documentación relacionada al proceso de acuerdo con la norma ISO/IEC 27001:2022 e instrumentos vigentes, tales como la Resolución 2277 de 2025, la Norma ISO 27001:2022 y la Guía DAFP v7 para la gestión integral del riesgo (probabilidad e impacto), entre otros referentes aplicables.

Reformular los riesgos de seguridad y privacidad de la información, vinculándolos a los activos físicos y de información, tomando en cuenta el inventario institucional existente, definiendo los criterios de impacto, probabilidad, responsables y controles asociados, así como documentar las evidencias de seguimiento, para alinearlos a la metodología propuesta por la Guía del DAFP (v.7) y los lineamientos del MSPI.

Fortalecer la gobernanza en seguridad de la información mediante la actualización de roles, responsabilidades, inventario de activos, la gestión de proveedores y el tratamiento de incidentes, asegurando una articulación clara entre el área de seguridad y la operatividad de los controles para garantizar cumplimiento en la asignación de responsables y seguimiento efectivo, evitando generar respuestas inoportunas ante incidentes, duplicidad de información y/o vacíos de responsabilidad.

Fomentar los controles dentro del talento humano, sobre lo relacionado con la seguridad de la información, incluyéndolos en los procesos de pre y post-vinculación, sensibilización, compromisos de confidencialidad, responsabilidades y funciones contratadas, asegurando que todo el personal

conozca, acepte y aplique los lineamientos de seguridad mediante capacitaciones periódicas, segregación de funciones y supervisión, para mitigar riesgos de pérdida, alteración o divulgación de información no autorizada.

Se recomienda documentar e implementar reglas o lineamientos para el uso de criptografía que regulen los casos de cifrado obligatorio, los pasos o instrucciones para la longitud y el ciclo de vida de las claves criptográficas.

Revisar los indicadores definidos en la entidad versus los propuestos en los lineamientos del Modelo de Seguridad y Privacidad de la Información, para la implementación y publicación en Almera de las fichas técnicas correspondientes.

Firmas,

Equipo auditor	Nombre	Firma
Auditor líder	Luis Antonio Tristancho Robles	**Luis Antonio Tristancho Robles**
Auditor de apoyo	Oscar Iván Vergara Medina	

DENIS PARRA SUÁREZ
Jefe Oficina de Control Interno