RED DE SALUD DEL CENTRO E.S.E

INFORME DE AUDITORIA AL PROCESO GESTION DE LAS TECNOLOGIAS Y LA INFORMACION 101.7.1.4.19

Dra. NATALI MOSQUER NARVAEZ
Gerente

SANDRA LILIANA ESCOBAR SOLANO
Asesora de Control Interno

Santiago de Cali, 18 de junio de 2026

1. INTRODUCCIÓN:

La Oficina de Control Interno en ejercicio de su rol de evaluación y seguimiento establecido en el Plan Anual de Auditorías 2026, llevó a cabo la Auditoría Interna enfocada en el proceso de Gestión de Tecnología y la Información con énfasis el subproceso de Gestión de Seguridad Informática y la evaluación del Plan Estratégico de Tecnologías de la Información (PETI).

2. METODOLOGÍA:

La auditoría se realizó bajo un enfoque práctico y de verificación directa, desarrollado en tres etapas:

- **Planeación**: Definición de los criterios de evaluación con base en las políticas de seguridad de la información, la normativa vigente y las metas del PETI.

- **Trabajo de campo y validación técnica**: Se realizó visita presencial para entrevistar a la líder del proceso y observar la operación en tiempo real. Asimismo, se efectuó la validación técnica de la información, verificando los respaldos y soportes de avance del PETI.

- **Informe**: Consolidación de observaciones, socialización previa y redacción del informe final con las recomendaciones.

3. CRITERIOS DE LA AUDITORÍA:

- GTI-PL-001 Plan Estratégico de Tecnología de Información y Comunicaciones - PETI
- GTI-PO-005 Política de Seguridad y Privacidad de la Información
- GTI-PO-006 Política Tratamiento de Riesgos de Seguridad y Privacidad de la Información
- GTI-M-002 Manual de Políticas y Estándares de Seguridad Informática

4. OBJETIVO:

Evaluar la ejecución y seguimiento de los controles del subproceso de Gestión de Seguridad Informática y el estado de cumplimiento del Plan Estratégico de Tecnologías de la Información (PETI)

5. ALCANCE:

El alcance de la auditoría corresponde a los resultados obtenidos en la vigencia 2025 y avances en el primer cuatrimestre de la vigencia actual.

6. RESULTADOS DEL SEGUIMIENTO REALIZADO

6.1. Cronograma del Modelo de Seguridad y Privacidad de la Información (MPSI)

El cronograma del Modelo de Seguridad y Privacidad de la Información (MPSI) de la Entidad está proyectado para ejecutarse entre las vigencias 2025 y 2027. Consta de tres componentes: Seguridad, Privacidad y Adopción del protocolo (previsto para iniciar en el segundo semestre de 2026).

El esquema de seguridad y privacidad se componen de cinco (5) fases ordenadas de la siguiente manera:

6.1.1. Diagnóstico:

Fase orientada a determinar el estado actual de la gestión de seguridad y privacidad de la información, evaluar el nivel de madurez de los controles e identificar el avance en la operación. De igual forma, contempla la verificación del cumplimiento legal en protección de datos, la adopción de buenas prácticas en ciberseguridad y el diagnóstico del estado de los activos de información de la Entidad. Esta fase se ejecutó satisfactoriamente durante la vigencia 2025.

El proceso utilizó la [1]herramienta de autodiagnóstico de Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.

6.1.2. Planificación:

Esta fase comprende dos componentes: seguridad y privacidad, las cuales están programadas para desarrollarse durante el primer trimestre de 2026. Durante la visita de verificación del cronograma, se evidenció que las actividades se encuentran dentro del tiempo establecido. El cumplimiento total de esta fase será evaluado en el próximo seguimiento.

Actividades del componente de seguridad: comprende el desarrollo y la formalización de la Política y los Procedimientos de Seguridad y Privacidad de la Información, así como la definición clara de los roles y responsabilidades en la materia. Asimismo, abarca la consolidación del inventario de activos de información y la integración del Modelo de Seguridad y Privacidad de la Información (MSPI) con el Sistema de Gestión Documental. Finalmente, incluye la identificación, valoración y tratamiento de riesgos, articulados con un plan de comunicaciones estratégico y el plan de diagnóstico para la transición de IPv4 a IPv6.

Actividades del componente de privacidad: Este componente contempla la elaboración, aprobación por parte de la alta dirección y socialización interna de la Política de Privacidad, el Manual de Políticas de Seguridad y Privacidad de la Información, y el Plan de Gestión de la Privacidad sobre la Información.

[1] ***Herramienta de autodiagnóstico del Ministerio TIC***: *Instrumento en formato Excel diseñado para que las entidades públicas evalúen su nivel de madurez, cumplimiento y gestión en políticas de Tecnologías de la Información (TI), tales como el Modelo de Seguridad y Privacidad de la Información (MSPI) y Gobierno Digital.*

Adicionalmente, incluye la definición formal de roles en relación con la información, el establecimiento de los procedimientos de privacidad correspondientes y la ejecución de un plan de capacitación dirigido a todo el personal de la entidad.

6.1.3. Implementación:
Prevista para iniciar durante el segundo semestre de la vigencia 2026.

6.1.4. Evaluación y Desempeño:
Programada para ejecutarse en el transcurso de la vigencia 2027.

6.1.5. Mejora Continua:
Fase final de la vigencia 2027.

6.2. Con base en la evidencia aportada y la verificación en sitio, se constató:

6.2.1. El cumplimiento del PETI vigencia 2025.
Durante la vigencia 2025, se ejecutó y actualizó el Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI) en un 55%, logrando así el cumplimiento de la meta establecida; asimismo, se evidenció que este plan se encuentra alineado con el Plan de Desarrollo 2024-2027.

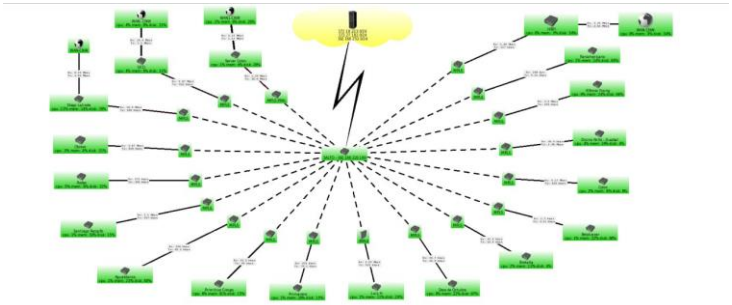
6.2.2. El seguimiento diario del rendimiento de la base de datos.
Diariamente se genera el informe de monitoreo de la base de datos para evaluar el rendimiento y la seguridad del sistema, permitiendo identificar puntos de congestión, prevenir caídas y asegurar su disponibilidad.

6.2.3. El respaldo de información mediante backups.
Se realizan copias de seguridad (backups) completas con periodicidad semanal y de forma extraordinaria cuando se requiere.

6.2.4. La suscripción de acuerdos de confidencialidad.
Los funcionarios suscriben un acuerdo de confidencialidad y protección de datos debido a su acceso a información reservada y sensible de usuarios, colaboradores, contratistas y demás actores relacionados con la operatividad. Asimismo, se cuenta con la certificación expedida por la Asociación Gremial Especializada en Salud del Occidente (AGESOC), la cual ampara a los afiliados partícipes en misión.

6.2.5. El funcionamiento del centro de datos y el control de conectividad en las IPS.
En el centro de datos se almacena, procesa y distribuye, de forma segura, un alto volumen de información. Asimismo, se monitorea la conectividad de todas las sedes que conforman la Red de Salud del Centro.

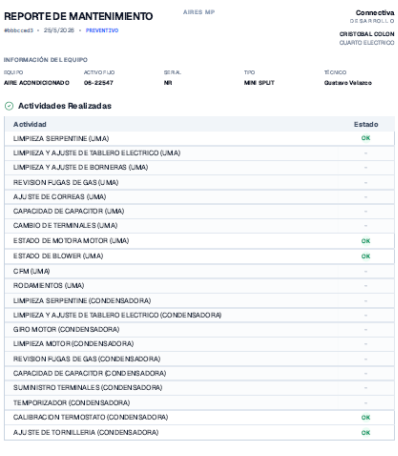
Conectividad Red de Salud del Centro E.S.E.



El color verde de cada nodo significa que la conectividad en todas las sedes está funcionando correctamente.

El área dispone de condiciones de refrigeración y seguridad verificables mediante la lectura del aire acondicionado y el diligenciamiento de los formatos GTI-F-020 Control de temperatura y humedad ambiental para cuarto de servidores y GTI-F-030 Control de ingreso de personal al Datacenter. Sin embargo, se evidencia la ausencia de un termohigrómetro que facilite el monitoreo simultáneo de la temperatura y la humedad relativa del entorno.

Por otra parte, con base en el reporte de mantenimiento del contratista y el registro de la planilla de ingreso, se constató la ejecución del mantenimiento preventivo del aire acondicionado el pasado 25 de mayo. No obstante, se identificó que el equipo carece del adhesivo de control correspondiente a dicha intervención, conservando únicamente etiquetas de fechas anteriores asociadas a proveedores previos.

Reporte de mantenimiento	Aire acondicionado
	

REPORTE DE MANTENIMIENTO

AIRES MP

Connectiva
DESARROLLO

CRISTOBAL COLON
CUARTO ELECTRICO

INFORMACIÓN DEL EQUIPO

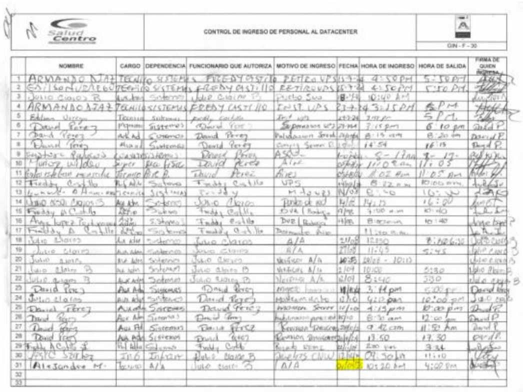
EQUIPO	ACTIVO FIJO	SERIAL	TIPO	TÉCNICO
AIRE ACONDICIONADO	06-22547	NR	MINI SPLIT	Gustavo Velasco

Actividades Realizadas

Actividad	Estado
LIMPIEZA SERPENTINE (UMA)	OK
LIMPIEZA Y AJUSTE DE TABLERO ELECTRICO (UMA)	-
LIMPIEZA Y AJUSTE DE BORNERAS (UMA)	-
REVISION FUGAS DE GAS (UMA)	-
AJUSTE DE CORREAS (UMA)	-
CAPACIDAD DE CAPACITOR (UMA)	-
CAMBIO DE TERMINALES (UMA)	-
ESTADO DE MOTORA MOTOR (UMA)	OK
ESTADO DE BLOWER (UMA)	OK
CFM (UMA)	-
RODAMIENTOS (UMA)	-
LIMPIEZA SERPENTINE (CONDENSADORA)	-
LIMPIEZA Y AJUSTE DE TABLERO ELECTRICO (CONDENSADORA)	-
GIRO MOTOR (CONDENSADORA)	-
LIMPIEZA MOTOR (CONDENSADORA)	-
REVISION FUGAS DE GAS (CONDENSADORA)	-
CAPACIDAD DE CAPACITOR (CONDENSADORA)	-
SUMINISTRO TERMINALES (CONDENSADORA)	-
TEMPORIZADOR (CONDENSADORA)	-
CALIBRACION TERMOSTATO (CONDENSADORA)	OK
AJUSTE DE TORNILLERIA (CONDENSADORA)	OK

Al indagar sobre el formato de registro de temperatura y humedad, el encargado manifestó que no conserva dichos soportes.

Por otra parte, tras la revisión detallada del formato GTI-F-030 “Control de ingreso de personal al Datacenter”, se evidenció la existencia de dos registros sin firma y con la fecha incompleta. Asimismo, se constató que el último registro en la planilla anterior data de marzo de 2025, evidenciando además el uso de un formato con codificación obsoleta.



6.2.6. El procedimiento para la creación de usuarios y capacitación en los sistemas.
Se verificó que el control de acceso a los sistemas SERVINTE y RING se encuentra regulado y respaldado; ante el ingreso de un nuevo colaborador, Gestión del Talento Humano tramita la solicitud de usuario y se convoca a la capacitación correspondiente. Este proceso cuenta con los listados de asistencia firmados, los cuales actúan como evidencia previa a la activación de las cuentas.

6.2.7. La realización de la capacitación sobre el MPESI en la vigencia 2025.
La capacitación y evaluación de conocimientos sobre el Manual de Políticas y Estándares de Seguridad Informática (MPESI) se llevó a cabo en noviembre de 2025 a través de la plataforma Moodle. Posteriormente, el 20 de diciembre, se programó una formación presencial para quienes no participaron o reprobaron el examen, la cual contó con la asistencia de 36 personas. Con esto, la participación total alcanzó el 73%. El detalle se puede observar en la siguiente imagen:

Consolidado Evaluacion 2025 [solo lectura] - Excel

	Virtual			Presencial			
PROCESO	Habilitados	Presentados	Participación	Participantes	Nuevo presentados	Nueva Participación	Reprobados
DIRECCIONAMIENTO ESTRATEGICO Y PLANEACION	26	10	38%		10	38%	1
ATENCION AMBULATORIA	73	29	40%	10	39	53%	4
REHABILITACION INTEGRAL	28	12	43%	5	17	61%	
ATENCION INTRAHOSPITALARIA	79	40	51%	8	48	61%	5
REFERENCIA Y TRASLADO DE PACIENTES - POOL	110	62	56%	1	63	57%	1
GESTION HUMANA	6	4	67%		4	67%	1
RECEPCION Y ATENCION AL USUARIO	60	44	73%	3	47	78%	4
ATENCION AMBULATORIA - ODONTOLOGIA	37	29	78%		29	78%	
PROMOCION Y MANTENIMIENTO DE LA SALUD	44	36	82%	2	38	86%	6
REFERENCIA Y TRASLADO DE PACIENTES - SICO	48	39	81%	4	43	90%	4
GESTION FINANCIERA	12	10	83%	1	11	92%	
GESTION DE LA CALIDAD Y LA EXCELENCIA	13	11	85%		11	85%	
APOYO DIAGNOSTICO - LABORATORIO	28	25	89%	1	26	93%	6
RELACION CON EL CIUDADANO	18	17	94%		17	94%	
ATENCION INTEGRAL AL CANCER	20	20	100%		20	100%	
CONTROL DE GESTION	2	2	100%		2	100%	
GESTION DE LA TECNOLOGIA Y LA INFORMACION	23	23	100%		23	100%	
GESTION DE MERCADEO Y COMUNICACIONES	2	2	100%		2	100%	
GESTION DEL AMBIENTE FISICO	6	6	100%		6	100%	1
GESTION LOGISTICA	7	7	100%		7	100%	
RECEPCION Y ATENCION AL USUARIO - FACTURACION	16	16	100%	1	17	106%	1
TOTALES	**658**	**444**	**67%**	**36**	**480**	**73%**	**34**

6.3 Evaluación de los controles asociados a los riesgos de Seguridad de la Información

Como resultado de la auditoría realizada al proceso de Gestión de Tecnologías y la Información y a los riesgos de seguridad de la información identificados por la entidad, se verificó la gestión y seguimiento de cinco (5) riesgos asociados a la confidencialidad, integridad y disponibilidad de la información institucional, distribuidos en tres procesos.

El proceso de Gestión de Mercadeo y Comunicaciones tiene identificado un riesgo relacionado con la posible afectación de la disponibilidad, integridad y confidencialidad de los formatos de autorización de uso de imagen de mayores y menores de edad, derivada de deficiencias en la infraestructura física y tecnológica y de la exposición a amenazas del entorno.

Por su parte, el proceso de Gestión de Tecnologías y la Información tiene identificados tres riesgos asociados a: i) la afectación de la confidencialidad, integridad y disponibilidad de la infraestructura tecnológica debido a variaciones eléctricas que puedan alterar las condiciones térmicas del centro de datos; ii) la posible afectación de la confidencialidad de la información institucional por debilidades en el control de permisos y perfiles de acceso, especialmente ante el retiro de funcionarios o colaboradores; y iii) la afectación de la disponibilidad, confidencialidad e integridad de la información como consecuencia de vulnerabilidades explotadas por ciberdelincuentes, asociadas a debilidades en las políticas de seguridad, insuficiencia de monitoreo continuo y necesidades de fortalecimiento en las prácticas de ciberseguridad.

Adicionalmente, el proceso de Gestión Jurídica y Contractual tiene identificado un riesgo relacionado con el potencial compromiso de la integridad, confidencialidad y disponibilidad de los expedientes contractuales y judiciales, debido a deficiencias en la implementación de medidas y protocolos para su adecuada protección.

Durante la auditoría se evidenció que los controles asociados a los riesgos evaluados cuentan, en términos generales, con seguimiento documentado a través de la herramienta Almera y presentan un nivel de implementación. Asimismo, se verificó la ejecución de actividades relacionadas con la gestión de respaldos de información, monitoreo de infraestructura tecnológica, mantenimiento de las condiciones ambientales del centro de datos, control de accesos a los sistemas de información, suscripción de acuerdos de confidencialidad y ejecución de copias de seguridad, evidenciándose cumplimiento de los controles establecidos y contribución a la mitigación de los riesgos identificados.

Se evidenció una oportunidad de mejora en el proceso de Gestión de Mercadeo y Comunicaciones, debido a inconsistencias en el diligenciamiento de los formatos de Autorización de Uso de Derechos de Imagen sobre Fotografías, Producciones Audiovisuales y Propiedad Intelectual (Código: GMC-F-002). En la revisión realizada se encontraron 21 formatos archivados (11 de la vigencia 2025 y 10 de la vigencia 2026), algunos de los cuales carecen de información esencial, como huella dactilar, fecha de suscripción y número de documento de identidad, aspectos necesarios para fortalecer la integridad y validez de los soportes documentales.

Recomendaciones para el proceso Gestión de Tecnologías y la Información

- Priorizar la implementación de una UPS exclusiva para el centro de datos y complementar el monitoreo ambiental mediante herramientas que permitan el seguimiento permanente de la temperatura y demás condiciones operativas de la infraestructura tecnológica.
- Continuar avanzando en la implementación de la Política de Seguridad y Privacidad de la Información, especialmente en lo relacionado con la identificación, clasificación y asignación de responsables de los activos de información institucionales.
- Culminar la implementación de la plataforma unificada de gestión de identidades y control de accesos, con el fin de fortalecer los mecanismos de autenticación, trazabilidad, monitoreo y auditoría de los accesos a los sistemas de información.

Recomendaciones para el proceso Gestión Jurídica y contractual

- Se recomienda continuar con el fortalecimiento de las actividades relacionadas con la digitalización, control de accesos, clasificación de la información y aplicación de los lineamientos de gestión documental, con el fin de consolidar la implementación integral del control y asegurar su sostenibilidad en el tiempo.
- Complementar las actividades de gestión documental realizadas con jornadas de socialización en seguridad de la información, conforme a lo establecido en el control definido.

En conclusión, la auditoría permitió evidenciar el cumplimiento de los controles asociados a los riesgos de seguridad de la información evaluados, así como avances importantes en la gestión de dichos riesgos. No obstante, la implementación de las oportunidades de mejora identificadas y recomendaciones, contribuirá al fortalecimiento de la madurez institucional en materia de seguridad de la información, optimizando la protección de los activos de información y reduciendo la probabilidad de ocurrencia de eventos que puedan afectar su confidencialidad, integridad y disponibilidad.

7. RESUMEN DE HALLAZGOS

Hallazgo 1: Deficiencia en los controles de acceso al Data Center y en el monitoreo diario de control de temperatura y humedad del lugar.

Hallazgo 2: Debilidad en el diligenciamiento del formato GMC-F-002 Autorización de Uso de Derechos de Imagen sobre Fotografías y Producciones Audiovisuales y de Propiedad Intelectual.

CRITERIO	RESULTADO
7.1 Deficiencia en el control de ingreso al Data Center y en el monitoreo diario de temperatura y humedad de la infraestructura.	Parcialmente cumplido
7.2 Debilidad en el diligenciamiento del formato GMC-F-002 Autorización de Uso de Derechos de Imagen sobre Fotografías y Producciones Audiovisuales y de Propiedad Intelectual.	Parcialmente cumplido

8. RECOMENDACIONES

8.1. Restablecer el registro y monitoreo de la temperatura y humedad en el Data Center, con el propósito de mitigar riesgos asociados a la condensación, prevenir sobrecalentamientos en los equipos y optimizar el consumo energético.

8.2. Garantizar el diligenciamiento del formato de control de acceso al Data Center, asegurando el registro de la fecha completa y la firma obligatoria de cada visitante. Asimismo, se debe establecer un mecanismo para el archivo físico o digital y la conservación de dichas planillas.

8.3. Implementar estrategias de socialización del Manual de Políticas y Estándares de Seguridad Informática (MPESI) dirigidas al personal que ingresa a la Entidad, con el fin de asegurar la correcta apropiación y cumplimiento de los lineamientos de seguridad desde su incorporación.

8.4. Reforzar los controles para asegurar el correcto diligenciamiento y verificación del formato GMC-F-002, garantizando el registro completo de la información requerida antes de su archivo. Igualmente, revisar los formatos que presenten omisiones, con el fin de fortalecer la integridad, trazabilidad y protección de la información, así como el cumplimiento de los lineamientos de gestión documental y seguridad de la información.

Finalmente, se invita a revisar el informe al interior del equipo y a realizar un análisis de causas para suscribir acciones encaminadas a subsanar la causa raíz de las debilidades descritas en el seguimiento.

El plan de mejoramiento debe ser suscrito en el sistema de gestión Almera siguiendo la metodología dispuesta por la Entidad dentro de los 15 días hábiles a partir de la fecha de suscripción de este informe.

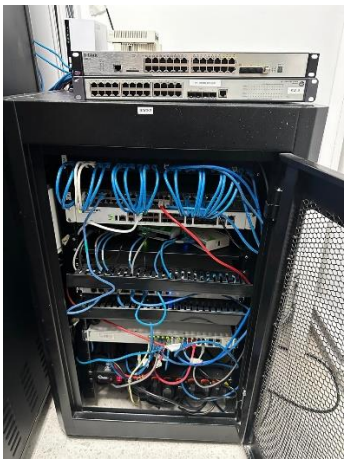
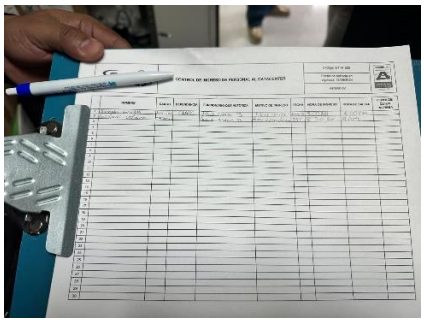
Cordialmente,

Sandra Liliana Escobar Solano
Asesora de Control Interno

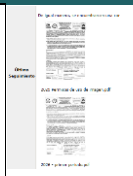
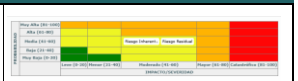
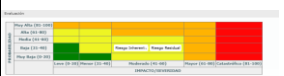
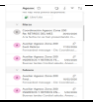
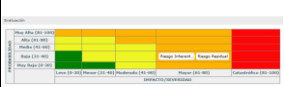
Anexo: Matriz de seguimiento a los controles de los riesgos de seguridad de la información (1) Folio

Elaborado: Gloria Ximena Giraldo R. – Afiliado Partícipe en Apoyo a Control de la Gestión
Revisado: Sandra Liliana Escobar Solano – Asesora Oficina de Control Interno

REGISTRO FOTOGRÁFICO DATA CENTER

<table>
<tr>
<td>  </td>
<td>  </td>
</tr>
<tr>
<td> 
</td>
<td>  </td>
</tr>
</table>

Seguimiento a los controles de los riesgos de Seguridad de la Información

Proceso	Causa	Codigo del Riesgo	Riesgo	Codigo de Control	Controles	Tipo de Control	Periodicidad del Control	Riesgo Inherente	Riesgo Residual	Tiene seguimiento en Almera?	Evidencia	Observaciones al seguimiento	Controles Efectivos	Recomendaciones	Mapa de Calor
Gestión de Mercadeo y Comunicaciones	Deficiencias en la infraestructura física o de medidas de seguridad tecnológica que pueden provocar pérdida o daño en los formatos de autorización o que exponen los documentos a accesos no autorizados o modificaciones indebidas. Amenazas externas del entorno, como robo, ataques cibernéticos o condiciones ambientales adversas que comprometan la integridad de la información.	E-GMC.R.003	Posibilidad de afectar la disponibilidad, integridad y confidencialidad del formato de autorización de uso de imagen de mayores y menores de edad debido a deficiencias en la infraestructura física y tecnológica, exponiéndolo a posibles amenazas del entorno.	Control-2025.026	Control de Respaldo y Protección de Formatos de Derechos de Imagen: El líder del proceso de gestión de mercadeo y comunicaciones debe asegurar que los formatos de derechos de imagen realizando un backup de los formatos digitalizados trimestralmente en un disco duro externo o en el computador asignado para asegurar la disponibilidad y protección de la información y evitar acciones legales contra la institución. Como evidencia se mantendrá la carpeta física de los formatos de autorización de uso de imagen diligenciados y Backup de la información digitalizada.	Preventivo	Trimestral	Moderado	Moderado	Si		Se evidencia seguimiento en Almera, donde la líder de Comunicaciones cargó los formatos escaneados correspondientes a los permisos de uso de imagen. Se realizó el escaneo de los documentos correspondientes al año 2025 y a los primeros cinco meses del año 2026. Estos documentos se encuentran almacenados en la carpeta de documentación del equipo de Gestión de Mercadeo y Comunicaciones. Se evidencia que los formatos no estan debidamente diligenciados en todos los campos	Parcial	Se evidenció que algunos formatos no se encuentran diligenciados en la totalidad de sus campos, por lo que se recomienda fortalecer los controles de revisión y validación documental antes de su digitalización y archivo, con el fin de asegurar la integridad, completitud y validez de la información registrada.	
Gestión de Tecnologías y la Información	Variaciones eléctricas externas Altas temperaturas que alteren las condiciones térmicas del centro de datos.	E-GTI.R.005	Posibilidad de afectación en la confidencialidad, integridad y disponibilidad de la infraestructura local causado por altas temperaturas que alteren las condiciones térmicas del centro de datos debido a variaciones eléctricas externas.	14 15	Revisión mensual del centro de datos local y chequeo eléctrico con mantenimiento preventivo: El Líder de Gestión de Tecnologías y la Información en articulación con el Líder de Gestión de Ambiente Físico serán responsables de revisar mensualmente el centro de datos local, aplicando lista de chequeo del fluido eléctrico y asegurarán el mantenimiento preventivo. En caso de incumplimiento, se implementarán revisiones semanales y en evento de identificar desviaciones realizará reporte a través del aplicativo RING para su intervención inmediata. Evidencias: Informes mensuales de mantenimiento de la planta eléctrica, reportes trimestrales de mantenimiento de la UPS, reporte de RING´s y documentación de reuniones y auditorías. Revisiones del fluido eléctrico y aire acondicionado: El profesional de infraestructura realizará revisiones del fluido eléctrico y aire acondicionado, informando novedades mediante RING para intervención rápida u optar por una alternativa que permita estabilizar la temperatura del centro de datos. Ante posibles incumplimientos en el mantenimiento correctivo, se implementarán revisiones diarias por el personal de mantenimiento. Las evidencias incluirán informes mensuales de mantenimiento de la planta eléctrica, reportes trimestrales de la UPS y aire acondicionado, y documentación de reuniones y auditorías.	Preventivo Preventivo	Mensual Diario	Moderado Moderado	Moderado Moderado	Si Si	 	En el almera la líder manifestó que se revisan los centros de Rack de cada sede una vez al mes y se informa mediante RING las solicitudes de adecuaciones, asi mismo se revisa el fluido electrico el cual se tiene pendiente de cotizar en la sede de Diego Lalinde el alcance de la planta electrica a la UPS del cuarto de Rack principal. Los ingenieros encargados revisan todos los dias laborales el centor de datos, verificando la temperatura, que el aire acondicionado este en otimas condiciones y se monitoreo el fluido de energia, en le primer trimestre se presentaon varios bajores lo cual se tiene cotizacion pendiente de autorizacion de Gerencia para cotocar una UPS exclusiva al centro de datos, esto queda detenido por la instruccion de traslado hacia belalcazar, se anexa cotizacion gestionada con el proveador HTS.	Si Si	Si bien se evidencia la realización de seguimientos periódicos al centro de datos y a las condiciones ambientales del cuarto de rack, se recomienda priorizar la gestión e implementación de la UPS exclusiva para el centro de datos, considerando los eventos de variaciones en el fluido eléctrico reportados y el riesgo que estos representan para la continuidad y disponibilidad de los servicios tecnológicos. Asimismo, aunque se evidenció la ejecución del mantenimiento del aire acondicionado durante el mes de mayo, se recomienda complementar el control mediante la instalación de un medidor de temperatura con registro permanente, que permita un monitoreo más efectivo de las condiciones ambientales y la adopción oportuna de acciones preventivas.	
Gestión de Tecnologías y la Información	Falta de un proceso de control para revocar permisos de acceso al momento de la salida del personal. Actualización tardia o inexistente de los perfiles de usuarios en los sistemas de la institución. Ausencia de auditorías periódicas y seguimiento del acceso a la información por parte de ex-colaboradores	E-GTI.R.006	Posible riesgo de afectación a la confidencialidad de cualquier información accesible para funcionarios o colaboradores durante su trabajo en la institución, debido a debilidades en el control de permisos a los perfiles de usuarios incluso despues de la salida del personal.	16 17	Acuerdos de confidencialidad: El líder de Gestión de Tecnologías y la Información asegurará que los servidores públicos y prestadores de servicios que gestionan bases de datos con información sensible en la Red de Salud del Centro ESE, de manera semestral, al iniciar un contrato o cada vez que sean asignadas las funciones, deben aceptar y firmar el acuerdo de confidencialidad. Lo anterior con el fin de garantizar el manejo adecuado de confidencialidad del activo de información a gestionar. En caso de encontrar que un servidor público o prestador de servicio no haya aceptado y firmado el acuerdo de confidencialidad, no podrá continuar con la gestión del activo de información del programa hasta que no se cumpla con la ejecución de este control. Evidencia: Formatos de acuerdo de confidencialidad firmados por cada uno de los encargados de gestionar el activo de información del programa. En caso de desviación: Comunicación oficial al servidor público o prestador de servicio informando la inhabilidad del manejo del activo de información Copia digital datos, archivos y documentos: El personal, que gestiona bases de datos con información sensible, deberá realizar una copia digital de los datos, archivos y documentos. Lo anterior con el fin de respaldar la información y recuperarla en caso que los equipos o las aplicaciones se deterioren. En caso de desviación, el proceso de Gestión de Tecnologías y la Información realizará un copia de la información almacenada en el equipo de gestión. Evidencia: registro de la copia digital de los datos, archivos y documentos.	Preventivo Preventivo	Según necesidad Semanal	Moderado	Moderado	Si Si	 	En conjunto con los procesos Jurídico y de Talento Humano, se implementó el compromiso de confidencialidad para el manejo de los activos de información; se adjunta la respectiva evidencia. Actualmente, se está adelantando la etapa de planeación de la Política de Seguridad y Privacidad de la Información, mediante la cual se definirán los listados de activos de información junto con sus respectivos responsables. Una vez estos sean establecidos, se dará inicio al proceso de firma de los formatos correspondientes. Se cuenta con backup diario de la base de datos del ERP principal y todos los dias habiles se recibe el informe por parte del proveedor, se adjutna evidencia del informe del 331 de marzo de 2026, a su vez se tiene programado los dias martes y jueves la realizacion del backup con la plataforma cobian, esta se realiza con puntero de equipos y se comunica a los usuarios quienes superan el tamaño maximo de realizacion de backup.	Si Si	Se recomienda continuar con la implementación de la Política de Seguridad y Privacidad de la Información, priorizando la identificación, clasificación y asignación de responsables de los activos de información institucionales. Este ejercicio es fundamental para fortalecer la protección de la confidencialidad, integridad y disponibilidad de la información, permitiendo establecer controles adecuados según la criticidad de cada activo. Asimismo, se recomienda desarrollar este proceso de manera articulada con Gestión Documental, considerando que la identificación y administración de los activos de información contribuye al adecuado manejo, conservación, acceso y protección de la información institucional, fortaleciendo así el Sistema de Gestión de Seguridad de la Información y el cumplimiento de los requisitos normativos aplicables. Este control se cumple satisfactoriamente, es importante continuar implemnetandolo	
Gestión de Tecnologías y la Información	Vulnerabilidad explotada por ciberdelincuentes Debilidades en las políticas de seguridad Falta de monitoreo continuo Capacitaciones insuficientes del personal en prácticas de ciberseguridad	E-GTI.R.002	Afectación de la disponibilidad, confidencialidad e integridad de la información por una vulnerabilidad explotada por ciberdelincuentes causada por debilidades en las políticas de seguridad, falta de monitoreo continuo y capacitaciones insuficientes del personal en prácticas de ciberseguridad.	9	Auditar permisos y monitorear actividades con reconfiguración inmediata: La líder de Gestión de Tecnologías y la Información liderará a través de soporte Infraestructura la implementación de un sistema de Gestión de Identidad y Acceso (IAM) para auditar trimestralmente los permisos de los usuarios y supervisar diariamente actividades sospechosas. Las auditorías trimestrales identificarán accesos innecesarios o riesgosos, mientras que alertas automáticas detectarán actividades sospechosas. Ante fallos en el sistema IAM o desviaciones, se realizará una reconfiguración inmediata y el equipo técnico investigará las causas para evitar recurrencias. Evidencias del control: Los informes trimestrales, registros de alertas y documentación del sistema IAM. Inhabilitación y capacitación personalizada para evitar accesos no autorizados a la Red de Salud del Centro: El Líder de Gestión de las Tecnologías y la Información será responsable de inhabilitar el equipo de la red para evitar accesos no autorizados a la red de salud del centro y capacitar de forma personalizada al usuario en el MPESI. Soporte Infraestructura identificará y bloqueará el equipo tecnológico que está ingresando a la red, mientras capacita al funcionario y le informa las medidas correspondientes. Este control se ejecutará cada vez que ocurra el evento.	Preventivo Correctivo	Trimestral Según necesidad	Alto	Alto	Si No	 	Actualmente, la entidad cuenta con controles establecidos para la gestión de accesos a los sistemas de información. En coordinación con el área de Talento Humano, se gestionan las solicitudes de habilitación, modificación y deshabilitación de usuarios, garantizando que los permisos de acceso se otorguen y retiren de acuerdo con las novedades de personal y las necesidades institucionales.Adicionalmente, como parte del fortalecimiento de los controles de seguridad de la información, se tiene previsto para el mes de julio la implementación de una plataforma unificada de gestión de identidades y control de acceso para la infraestructura de servidores, especificamente para los siete (7) terminales donde se encuentra configurado el aplicativo Seriate (ERP) de la Red de Salud Centro E.S.E. Esta solución, basada en la integración de Apache Guacamole y Keycloak IAM con el controlador de dominio institucional (Windows Server), permitirá robustecer los mecanismos de autenticación, autorización, trazabilidad y auditoría de accesos, mejorando tanto la seguridad como la administración de los sistemas. Para realizar el control a este riesgo se recibe por parte de talento humano los ingresos y retiros del mes, si son ingresos tuvieron capacitacion personalizada por parte de sistemas de information, soporte tecnico e infraestructura para informar los tips a tener en cuenta, si el usuario se retira se pasa a desactivar de las plataformas Servitia, RING, desactivacion de VPN si las tiene, se adjutna evidencia de envio de correos.	Si Si	Se recomienda continuar fortaleciendo los controles de gestión de accesos mediante la articulación permanente con Talento Humano para la habilitación y deshabilitación oportuna de usuarios. Asimismo, se considera importante culminar la implementación de la plataforma unificada de gestión de identidades y control de accesos, dado que permitirá mejorar la trazabilidad, auditoría y monitoreo de los accesos a los servidores institucionales, fortaleciendo la seguridad de la información y la gestión de riesgos tecnológicos.	
Gestión Jurídica y Contractual	Falta de medidas adecuadas para proteger los expedientes Deficiencias en la implementación de protocolos de protección	A-GJC.R.004	Potencial compromiso de la integridad, confidencialidad y disponibilidad de los expedientes contractuales y judiciales debido a la falta de medidas adecuadas para protegerlos, causado por deficiencias en la implementación de protocolos de protección.	7 8	La Líder del proceso de gestión jurídica y contractual, con el apoyo de los procesos de gestión de tecnologías y la información y gestión documental, debe implementar un control integral y progresivo para la organización, digitalización, clasificación, acceso y conservación de los expedientes contractuales y judiciales, priorizando aquellos asociados a riesgos críticos, mediante la definición y aplicación de una política de clasificación de la información, la asignación de metadatos y el establecimiento de controles de acceso bajo los principios de mínimo privilegio y necesidad de conocer, así como la definición de períodos de conservación y procedimientos de eliminación segura de expedientes físicos y digitales, conforme a la disponibilidad institucional, con el fin de fortalecer la trazabilidad, el acceso oportuno y el control administrativo y jurídico. Evidencia esperada: *Lineamientos frente a la clasificación de la información aprobada y socializada (público, interno, confidencial, reservado). *Inventario actualizado de expedientes contractuales y judiciales, con identificación de aquellos asociados a riesgos críticos. *Registros de digitalización y organización de expedientes (repositorios físicos y electrónicos). *Metadatos y etiquetas de clasificación aplicados a los expedientes físicos y digitales. *Matriz de roles y permisos de acceso configurada en los sistemas de información, con evidencias de control de accesos y segregación de funciones. *Registros de revisiones periódicas de accesos y autorizaciones. *Tablas de retención documental y registros de conservación y/o eliminación segura de expedientes, conforme a los procedimientos definidos. *Informes de avance y seguimiento del control, emitidos por el proceso de gestión jurídica y contractual, con apoyo de tecnologías de la información y gestión documental. El líder del proceso de Gestión Jurídica y Contractual debe asegurar que, de manera anual, se brinde capacitación a los responsables que intervienen en la gestión de expedientes contractuales y judiciales en prácticas de manejo seguro de la información, protocolos de protección de la integridad, confidencialidad y disponibilidad de los expedientes, identificación y prevención de amenazas, y procedimientos para el reporte oportuno de incidentes de seguridad, con el fin de reducir la probabilidad de acceso no autorizados, pérdidas de información o compromisos de seguridad derivados de fallas en la aplicación de los controles.	Preventivo Preventivo	Trimestral Anual	Alto	Alto	Si Si	  **Acta de reunion 203.1.28.067.2026**	La Líder del proceso de gestión jurídica y contractual, en articulación con las áreas de tecnologías de la información y gestión documental, implementó un modelo de control integral y progresivo para la organización, digitalización, clasificación, acceso y conservación de los expedientes contractuales y judiciales, tanto en soporte físico como digital. Esta estrategia se desarrolla a través de tres componentes clave: -Inventarios actualizados: Registro y control en tiempo real de los expedientes. -Digitalización sistemática: Migración técnica de los archivos físicos al entorno virtual. -Almacenamiento seguro: Carga de la información en un repositorio digital centralizado (Drive), con permisos de acceso restringidos exclusivamente al personal de la oficina jurídica. El 11 de junio de 2026 se realizó jornada de retroalimentación en gestión documental dirigida al proceso de Gestión Jurídica y Contractual, orientada por la líder de Gestión Documental. Durante la actividad se reforzaron aspectos relacionados con el adecuado diligenciamiento y manejo de formatos, los tiempos de retención y conservación documental conforme a las TRD, la correcta foliación de documentos y la organización, clasificación y ordenación de expedientes. Asimismo, se resolvieron inquietudes y se formularon recomendaciones para fortalecer el cumplimiento de los procedimientos archivísticos, promoviendo la adecuada conservación, custodia, integridad y disponibilidad de la documentación institucional	Si Si	Se evidencian avances en la organización, clasificación y conservación de los expedientes físicos, así como acciones orientadas al fortalecimiento de la gestión documental del proceso. No obstante, algunos componentes del control requieren continuar su desarrollo y documentación para evidenciar su implementación integral. Se recomienda continuar con el fortalecimiento de las actividades relacionadas con la digitalización, control de accesos, clasificación de la información y aplicación de los lineamientos de gestión documental, con el fin de consolidar la implementación integral del control y asegurar su sostenibilidad en el tiempo. Con base en el control definido y la evidencia aportada, se observa que se realizó una jornada de retroalimentación en gestión documental, esta actividad contribuye al fortalecimiento de la gestión de la información y la protección documental. No obstante, el control establece la necesidad de brindar capacitación anual en temas de manejo seguro de la información, protección de la integridad, confidencialidad y disponibilidad de los expedientes, identificación de amenazas y reporte de incidentes de seguridad. Por lo tanto, se recomienda realizar la socialización sobre seguridad de la información.