

	INFORME FINAL DE AUDITORIA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE CONTROL	GCO-IPA	220

DATOS GENERALES DE LA AUDITORIA			
LUGAR DE REALIZACION DE LA AUDITORIA:		Sede Administrativa	
AUDITORIA No.	04 de 2026	FECHA DEL INFORME	4 de marzo de 2026
PROCESO/DEPENDENCIA AUDITADO		GESTION DE SISTEMAS DE INFORMACION	
LIDER DEL PROCESO/ RESPONSABLE		JEFE OFICINA ASESORA DE COMUNICACIONES Y SISTEMAS	
PERIODO DE REALIZACION DE LA AUDITORIA		VIGENCIA 2025	
OBJETIVO			
Verificar el nivel de cumplimiento de: • Plan de Comunicaciones • Plan de Seguridad Informática • Políticas de transparencia, acceso a la información pública y lucha contra la corrupción • Política de gestión documental. • Política de Gobierno Digital. • Estado de las Tablas de Retención Documental, Tablas de Valoración Documental, y demás documentos requeridos por la Ley General de Archivos. • Estado de licenciamiento del Software SIOS • Actualización Módulos SIOS • Matriz de riesgos del proceso			
JUSTIFICACION			
La oficina de Control Interno, en cumplimiento de sus funciones de seguimiento, control y de acuerdo a las Auditorias programadas para la vigencia 2026, requiere efectuar una auditoría al proceso Gestión de Sistemas de Información, durante la vigencia 2025, bajo los principios de eficacia, eficiencia, atención optima y mejoramiento continuo con el objeto de verificar su correcto acatamiento al ordenamiento jurídico.			
PRODUCTO			
• Plan de Comunicaciones • Plan de Seguridad Informática • Políticas de transparencia, acceso a la información pública y lucha contra la corrupción • Política de gestión documental. • Política de Gobierno Digital. • Estado de las Tablas de Retención Documental, Tablas de Valoración Documental, y demás documentos requeridos por la Ley General de Archivos. • Estado de licenciamiento del Software SIOS • Actualización Módulos SIOS • Matriz de riesgos del proceso.			
ALCANCE			
La presente auditoria se llevó a cabo en las instalaciones de la Oficina Asesora de Comunicaciones y Sistemas y en la Oficina de Control Interno en la Sede Administrativa, revisando la información relacionada con los productos a auditar y que son correspondientes a la vigencia 2025.			

	INFORME FINAL DE AUDITORIA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE CONTROL	GCO-IPA	220

HECHOS

Mediante comunicación Oficial 202605200002531 del 4 de febrero de 2026 la Oficina de Control Interno informo a la Oficina Asesora de Comunicaciones y Sistemas sobre la apertura de la Auditoria de Gestión No. 04 de 2026, la cual se llevó a cabo en la Oficina de Comunicaciones y Sistemas el día 6 de febrero de 2026.

Se procedió a analizar, revisar y evaluar los documentos producto de esta auditoría, dentro de los cuales se encontró lo siguiente:

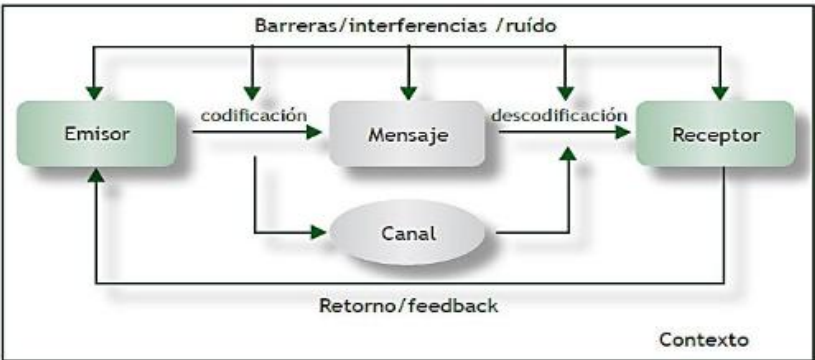
PLAN DE COMUNICACIONES

La Empresa Social del Estado Pasto Salud E.S.E., aborda el componente comunicacional y educativo desde una perspectiva transversal, implementando estrategias internas y externas que respondan a las necesidades de los grupos de interés, a través de la formulación del Plan de Comunicación que incorpora metodologías basadas en conceptos organizacionales y comunitarios que benefician a los actores del sistema de salud, enmarcadas en la participación, el diálogo y la calidad humana de sus colaboradores y la comunidad.

Se evidencia que el 20 de febrero de 2024 se dio tramite de actualización al “Plan de Comunicaciones” de PASTO SALUD ESE, versión 11.0 para la vigencia 2023, el cual determina su objetivo general, objetivos específicos y alcance. Este plan esta diseñado para ejecutarse para las vigencias 2021 a 2024, es decir podemos deducir que se encuentra desactualizado y no se encuentra ajustado al plan estratégico 2025-2028

El Objetivo es, Responder a las necesidades de comunicación e información que se presentan en la organización, para garantizar procesos comunicativos asertivos, claros y eficaces que aporten en los procesos de transformación cultural.

Dentro del documento encontramos el establecimiento del Modelo de Comunicación para la empresa, basado en la participación de 3 elementos claves (emisor, mensaje, receptor y canales), como se observa en la siguiente imagen.



Fuente: Documento “Como elaborar el plan de comunicación”

	INFORME FINAL DE AUDITORIA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE CONTROL	GCO-IPA	220

En el numeral 4.4 denominado Modelo De Las Seis Dimensiones De La Comunicación Institucional M6D

El M6D que se presenta a continuación, no es un modelo único o inflexible, y de igual manera que cada empresa tiene su propio organigrama según sus necesidades; en la comunicación, las áreas o dimensiones de comunicación pueden organizarse de tantas maneras como sea necesario, agrupando o desagrupando áreas o sub-áreas, según las necesidades.

“4.4. MODELO DE LAS SEIS DIMENSIONES DE LA COMUNICACIÓN INSTITUCIONAL M6D



Fuente: Documento “Como elaborar el plan de comunicación”

En el numeral 7 denominado ESTRATEGIAS DE COMUNICACIÓN se definen las estrategias y productos para:

- COMUNICACIÓN EXTERNA
- COMUNICACIÓN CORPORATIVA
- COMUNICACIÓN INTERNA
- RELACIONES PÚBLICAS
- PARTICIPACION CIUDADANA
- COMUNICACIÓN DIGITAL
- COMUNICACIÓN DE CRISIS

Boletines de prensa

- Boletines informativo
- Capsulas radiales

	INFORME FINAL DE AUDITORIA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE CONTROL	GCO-IPA	220

- Post
- Cuñas radiales
- Podcast
- Programas de radio
- Programas de tv
- Notas página web
- Videos
- Registros fotográficos

Para las cuales se establecieron un total de 177 actividades, las cuales según el informe semestral relaciona un nivel de cumplimiento del 100%

El Plan de Comunicaciones en el numeral 8 establece cuales son los indicadores para hacer la medición a este plan, los cuales una vez revisado el informe de Ejecución del Plan de Comunicaciones se puede determinar que el mismo tuvo un 100% de ejecución.

Los indicadores plasmados en el Plan de Comunicaciones tienen la siguiente tendencia en la vigencia 2025:

INDICADOR	META	RESULTADO I SEM	RESULTADO II SEM
Nivel de satisfacción con las comunicaciones internas	90%	100%	100%
Nivel de satisfacción con las comunicaciones externas	70%	99,80	98,11
Nivel de apropiación de la información desplegada para cada estrategia (corporativa, externa y ciudadana)	80%	100%	100%
Porcentaje de cumplimiento del Plan de Acción de comunicaciones	100%	100%	100%

Participación de los funcionarios por redes y sede administrativa en número: ____	Medición de Canales de Comunicación: Red Institucional YouTube Número de Suscriptores: 991 Numero de Publicaciones: 415 videos Red Institucional Facebook Número de Suscriptores: 15.080 Red Institucional Instagram Número de Suscriptores: 1.604 Numero de Publicaciones: 448
---	--

	INFORME FINAL DE AUDITORIA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE CONTROL	GCO-IPA	220

PARTICIPACION DE FUNCIONARIOS EN PASTO SALUD	
PRIMER SEMESTRE-2025	176
SEGUNDO SEMESTRE-2025	237

El informe también contiene resultados de diferentes encuestas realizadas midiendo aparte de la satisfacción, la oportunidad y la comprensión.

La oficina de Comunicaciones y Sistemas realiza la medición de los canales de comunicación, la satisfacción de la información recibida y el impacto o apropiación de los temas desplegados de manera semestral, en esta ocasión realiza el despliegue del instrumento de medición (Encuesta) a través de la circular 202405500091863 del 04 de diciembre de 2024, a todo el personal de Pasto Salud ESE y a los integrantes de la Junta Directiva.

Con corte a diciembre de 2025 se logra la participación de 237 personas de todas las redes operativas Norte, Sur, Oriente, Occidente y sede administrativa.

CANALES DE COMUNICACIÓN INTERNA

¿Qué medio de comunicación utiliza con mayor frecuencia para revisar información de la Entidad?

El canal principal utilizado para revisar información es el correo electrónico, con un 83,9% de preferencia, lo que lo posiciona como el medio más eficaz y accesible para los colaboradores. Otros medios importantes incluyen reuniones (36,4%) y la página institucional (30,1%), que complementan la comunicación formal, aunque con un alcance significativamente menor. Los boletines informativos (24,5%) y aplicaciones de mensajería, como Spark (10,5%) y Google Chat (4,9%), tienen un uso limitado, indicando áreas de oportunidad para diversificar y mejorar la comunicación multicanal.

Se recomienda fortalecer el uso del correo electrónico, manteniéndolo como el medio prioritario, pero optimizando su uso con mensajes claros, organizados y periódicos, potenciar la página institucional y reuniones como medios complementarios, asegurando que la información relevante esté siempre actualizada y accesible, promover el uso de boletines informativos con diseño atractivo y contenido condensado para captar mayor interés entre los colaboradores, revisar el bajo uso de aplicaciones de mensajería (Spark y Google Chat), considerando capacitación o campañas de sensibilización para fomentar su adopción como herramientas rápidas y accesibles e integrar estrategias de comunicación multicanal, combinando medios tradicionales con digitales para alcanzar a todos los empleados según sus preferencias y necesidades.

Se muestra también la medición de los canales de comunicación, como YouTube, Facebook e Instagram.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Oficina Asesora de Comunicaciones y Sistemas, siguiendo las directrices en materia de seguridad digital y de la información de acuerdo al Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.1.3. Principios. Define la seguridad de la información como principio de la Política de Gobierno

	INFORME FINAL DE AUDITORIA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE CONTROL	GCO-IPA	220

Digital, de igual manera en el artículo 2.2.9.1.2.1 define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales.

Teniendo en cuenta lo anterior, mediante Resolución 090 del 27 de enero de 2025, se adopta el Plan de Seguridad y Privacidad de la Información de Pasto Salud ESE para la vigencia 2025. Cuyo objetivo principal es: Proteger los activos de información, así como el uso adecuado de los recursos y gestión del riesgo, con el fin de preservar la disponibilidad, integridad y confidencialidad de la información.

Y un alcance que aplica a todas las sedes de Pasto Salud E.S.E, a todos sus grupos de interés y aquellas personas o terceros que en razón del cumplimiento de sus funciones y las de Pasto Salud E.S.E generen, compartan, utilicen, recolecten, procesen, intercambien o consulten su información, sin importar el medio, formato o presentación o lugar en el cual se encuentre.

Cuenta con una Política De Seguridad De La Información, En Pasto Salud E.S.E. nos comprometemos a mantener la confidencialidad, integridad y disponibilidad de la información mediante la implementación de un Modelo de Seguridad y Privacidad, gestionando integralmente los riesgos y cumpliendo los requisitos legales que aseguran la privacidad de la información de nuestros grupos de interés, con un enfoque en la mejora continua.

Se evidencia la definición de un MODELO Y OPERACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACION – SGCI como se puede observar en la siguiente imagen.



Adopta el Modelo de Seguridad y Privacidad de la Información enmarcado en el Sistema de Gestión de Seguridad de la información, el cual protege, preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información que circula en el mapa de operación por procesos, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales para prevenir incidentes, propender por la continuidad de la operación de los servicios y dar cumplimiento a

	INFORME FINAL DE AUDITORIA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE CONTROL	GCO-IPA	220

los requisitos legales, reglamentarios y regulatorios, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información.

Dentro del mismo documento se formuló un Plan de Implementación del Modelo de Seguridad y privacidad de la Información, para su adecuada implementación en la empresa, el cual consta con los siguientes objetivos específicos:

1. Identificar, clasificar, y gestionar los activos de la información de la empresa
2. Sensibilizar al talento humano en las mejores prácticas de la seguridad y privacidad de la información.
3. Fortalecer los mecanismos de respaldo de la información física como digital para su preservación y conservación.
4. Gestionar los incidentes de seguridad y privacidad de la información

Plan de Seguridad, realizo una auditoría interna en la misma dependencia, con el fin de determinar unos hallazgos y controles de la Información 2025, llevada a cabo el pasado 18 de julio de 2025.

Esta sesión, dirigida a los técnicos de las redes de atención de Pasto Salud ESE, constituyó la segunda instancia de verificación de las actividades ejecutadas entre abril y junio de 2025 en las diferentes sedes de Pasto Salud de la entidad.

El objetivo principal fue revisar el avance de las acciones implementadas, entre las que se destacan el control y seguimiento del plan, la ejecución de simulacros del plan de contingencia y las capacitaciones en seguridad de la información.

En el proceso auditor se realizó una reunión, desarrollada a través del canal virtual oficial de la empresa (<https://meet.google.com/ufo-xtas-adn>), contó con la participación activa del personal técnico.

Para la auditoría del año 2025, se definió las siguientes actividades críticas de control y seguimiento para la seguridad de la información:

- Gestión de Activos: Validar la existencia y exactitud de un inventario de equipos de cómputo, alineado con los hallazgos de la revisión inicial.
- Protección de Endpoints: Garantizar la actualización del parque informático al 100% con la solución antivirus Sophos, junto con la evaluación programada para la renovación de hardware obsoleto.
- Gestión de la Conectividad: Realizar el monitoreo y seguimiento al estado de la conectividad de red en el centro de salud auditado.
- Concientización y Preparación: Evaluar el nivel de conocimiento del personal en políticas de seguridad de la información y en la ejecución de los planes de contingencia de los sistemas.

Alcance y Metodología de la Auditoría, con base en las recomendaciones previas, la estrategia de auditoría para el control y seguimiento del Plan de Seguridad de la Información y el Plan de Contingencia contempló una cobertura de muestreo del 70% de los equipos desplegados en la red de atención de Pasto Salud ESE. Este alcance implicó la ampliación de las visitas in situ a las sedes de la empresa para una verificación física directa.

	INFORME FINAL DE AUDITORIA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE CONTROL	GCO-IPA	220

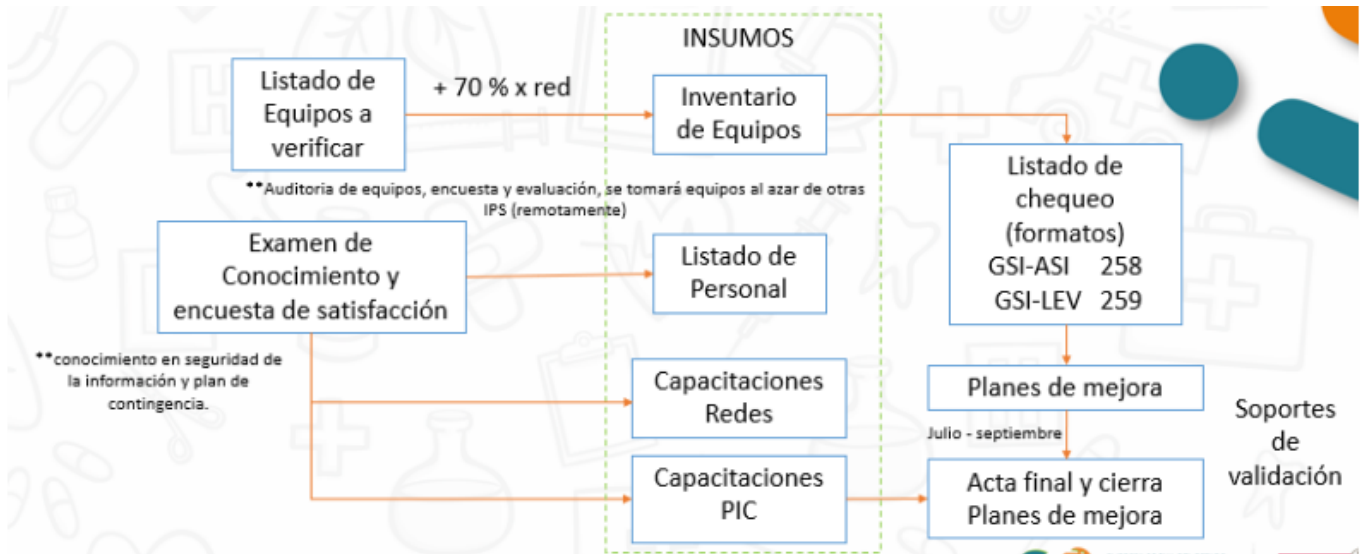


Imagen 4. Desarrollo de control y seguimiento seguridad de la información 2025. Fuente: Comunicaciones y Sistemas

Durante la Auditoría se tuvo en cuenta los siguientes criterios:

- Inventario actualizado de equipos computo conforme a la revisión realizada durante la auditoria en el inventario único de equipos de cómputo.
- Verificar copias de seguridad y capacitación al personal en la realización de las mismas.
- Actualizar de totalidad de equipo con antivirus Sophos y revisar actividades concertadas de actualización física de equipos (hardware).
- Capacitaciones y despliegue de socialización en temáticas de seguridad de la información, delitos informáticos y plan de contingencia
- Seguimiento a conectividad de centro de salud auditado.

RESULTADOS DE SEGUIMIENTO Y CONTROL TOTAL REDES DE ATENCIÓN FORMATO GSI-ASI 259

RED DE ATENCIÓN	No TOTAL DE EQUIPOS VERIFICADOS	CUMPLIMIENTO %	INCUMPLIMIENTO %
Red Norte	60	94.7	5.18
Red Sur	74	98.8	1.202
Red Oriente	52	94.69	5.277
Red Occidente	61	97.04	2.94
Total	247	95.97	3.957

RESULTADOS FORMATO GSI-ASI 258 LISTA DE CHEQUEO AUDITORIA DE SEGURIDAD DE LA INFORMACION – GESTIÓN SISTEMAS DE INFORMACIÓN

RED DE ATENCIÓN	CUMPLIMIENTO %	INCUMPLIMIENTO %
Red Norte	23 (92%)	2 (8%)

	INFORME FINAL DE AUDITORIA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE CONTROL	GCO-IPA	220

Red Sur	25 (100%)	0 (0%)
Red Oriente	22 (88%)	3 (12%)
Red Occidente	24 (96%)	1 (4%)
Total	94 (94%)	6 (6%)

Como resultado de la auditoria se presentaron las siguientes observaciones:

Se cuenta con un inventario actualizado de todos los equipos de su red por IPS?, Durante el I semestre 2025, solo el (6.493%) 15 de los 231 equipos de cómputo verificados durante la actividad de seguimiento y control, no contaban con un registro totalmente actualizado en el sistema de hojas de vida de Equipos de cómputo, teniendo como comparativa la configuración de hardware, actualización de dispositivos, ubicación de área de trabajo y placa asignada por almacén, sin embargo, esta última actividad, depende del área de almacén, ya que algunos traslados no se han realizado por parte de esta área, se toma como realiza las respectivas recomendaciones a todos los Técnicos para la oportuna actualización, ya que el registro y actualización de la información debe ser permanentemente desde comienzo hasta el final del año revisado.

Como se mencionó anteriormente, se evidencia inconsistencias en el manejo de placas asignadas para equipos de cómputo, como es el caso de equipos que no se encuentran debidamente señalados, o números de placa ilegibles, además casos particulares en donde se encontraron placas duplicadas errores que crearon confusión durante el seguimiento y control de los equipos, por ello, se dejará constancia sobre esta acta, la notificación a la oficina de almacén de realizar las respectivas actualizaciones en conjunto con los técnicos de cada red de atención y poder resolver esta necesidad. Es importante contar con inventario de equipos actualizado, por ello, los técnicos en las redes durante la visita de verificación y control reciben las indicaciones necesarias para registrar la información de los equipos revisados.

Se ha socializado las políticas de seguridad informática y de la información al personal de la IPS en la Red de Atención asignada?, se evidencia que han sido socializadas varias capacitaciones en seguridad de la información por parte de los técnicos en los centros de salud, sin embargo, la cobertura de participación del personal asistencial y administrativo no puede ser comparado con la meta establecida por medio del plan institucional de capacitaciones el cual debe ser superior al 80% en cobertura y en la evaluación de conocimiento debe estar sobre el 90%, teniendo en cuenta antiguos seguimientos realizados en años anteriores.

Actividad: Teniendo reforzar el conocimiento del personal asistencial y administrativo en política de seguridad de la información y plan de contingencia en sistemas de información que permita la apropiación de las temáticas en el personal asistencial y administrativo de los centros de salud de Pasto Salud ESE. una vez terminado este tiempo se procederá a evaluar el conocimiento de los centros de salud visitados y los restantes.

El Office instalado en los equipos cuenta con licenciamiento?, se evidencia en todos los centros de salud una gran ausencia en el uso y licenciamiento autorizado de paquete básico de office, recurriendo a utilizar software que no cuenta con las condiciones mínimas para su funcionamiento.

	INFORME FINAL DE AUDITORIA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE CONTROL	GCO-IPA	220

De acuerdo a las observaciones encontradas en la auditoria, se establece un cronograma plan de contingencia en sistemas de información.

En desarrollo de las actividades contempladas para la vigencia 2025, se entrega un resumen de las actividades que fueron planteadas durante 2025, para el semestre II -2025, se tendrá en cuenta las calificaciones obtenidas en la evaluación del plan institucional de capacitaciones y el cronograma de simulacros para el presente año.

- Evaluación de contingencia – PIC / conocimiento de personal
- Contingencia programada – septiembre / octubre 2025

Propósito de simulacros de plan de contingencia para el año 2025, tiene como propósito ampliar la cobertura de simulacros de plan de contingencia en sistemas de información a varias sedes de la empresa, adicionalmente fortalecer el conocimiento y apropiación de conocimiento del personal en temáticas referentes a plan de contingencia y seguridad de la información

- Centro de Salud Catambuco
- Centro de Salud San Vicente
- Hospital Santa Mónica
- Hospital Local Civil

Al igual que las auditorias en seguridad de la información, al finalizar la auditoria los simulacros en planes de contingencia en sistemas de información por cada Red de atención de Pasto Salud ESE deberá obtener un resultado superior o igual al 90% lo cual otorgará como resultado de CUMPLIMIENTO, en caso contrario NO CUMPLIMIENTO se procederá a realizar plan de mejora de la red de atención afectada.

Cada uno de los objetivos cuenta con actividades en el ciclo de Planear, Hacer, Verificar y Actuar para su ejecución, determinando la meta, evidencias, plazo de ejecución, responsable y presupuesto.

Una vez revisados las actividades dispuestas para cada uno de los objetivos, encontramos lo siguiente:

- En lo relacionado a la apropiación del talento humano de la política de seguridad y privacidad de la información, se evidencia que se realizaron las siguientes capacitaciones en la vigencia 2025:
Se evidencia una cobertura del 83.85% en seguridad de la información y 74% en planes de contingencia, con calificaciones promedio superiores al 95%. Sin embargo, se identifican oportunidades de mejora para fortalecer las competencias TIC del personal.
- En lo relacionado con la realización de auditorías de seguridad de la información en las sedes priorizadas, se evidencia que se priorizaron el 90% del total de las sedes de Pasto Salud ESE, el porcentaje de cumplimiento 94% (22 sedes totales), se realizaron en la red norte 60 equipos, en la red sur 74 equipos, en la red oriente 52 equipos y en la red occidente 61 equipos, se observan los resultados en cuanto al cumplimiento de requisitos según la lista de chequeo por sede.
- Ejecución de las actividades de respaldo de la información (Backups). Se cuenta con el procedimiento Copias de Copias de Seguridad GSI-PD 119, el cual tiene como objetivo respaldar la información de

	INFORME FINAL DE AUDITORIA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE CONTROL	GCO-IPA	220

los procesos de la organización mediante la utilización de herramientas tecnológicas asegurando la confidencialidad, integridad, disponibilidad de la información. El seguimiento y control se realiza con el indicador "Copias de seguridad" y el formato "Realización de backups de bases de datos del servidor GSI-BDS 255" en el cual se registran la cantidad de backups de base de datos realizados sobre programados. Para la vigencia 2025 el cumplimiento fue del 100% el cual se observó en la matriz.

También se puede observar que, desde el administrador de base de datos para SQL Server, se programan las tareas para la ejecución automática de los backups en los horarios establecidos, al cual se debe ingresar con usuario y contraseña.

- Se evidencia cumplimiento de la identificación, clasificación y gestión de los activos de información, actualizado en el mes de julio de 2025, por cuanto en la página web institucional están relacionados la vigencia 2021 al 2025, tal como se puede corroborar en el link <https://www.pastosaludese.gov.co/site/nuestra-entidad/estructura-administrativa/comunicaciones-y-sistemas/135-activos-de-la-informacion-y-clasificacion/1760-activos-de-la-informacion-y-clasificacion-de-documentos-2025>

Análisis De Indicadores De Seguridad De La Información (Vigencia 2025)

En 2025 se evaluaron 5 indicadores. En la consolidación anual: 3 cumplieron meta, 2 no cumplieron con la meta.

ID	Indicador	Meta	Resultado anual	Cumple	Meses sin cumplir	Meses con dato
1	Oportunidad en la Atención de Asistencias Técnicas.	≤ 48 horas	66.19 h	No cumple	Enero, febrero, marzo, abril, mayo, junio, Diciembre	12
2	Gestión de Usuarios y Contraseñas	≤48 Hora	9.19	Cumple	Febrero	12
3	Solicitud e Gestión de Incidentes de Seguridad de la Información	≥ 0.999 (99.9%)	100%	Cumple	Sin Datos No hubo reportes	5
4	Efectividad para mitigar el riesgo de pérdida de información por ataques de software malicioso y virus informático	≥ 0.950 (95.0%)	97.02%	Cumple	Julio, agosto, Noviembre	12

	INFORME FINAL DE AUDITORIA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE CONTROL	GCO-IPA	220

5	Copias de Respaldo de base de datos	≥ 0.999 (99.9%)	98.91%	No cumple	Agosto Incidente ataque cibernético Ransomware	12
---	-------------------------------------	-----------------	--------	-----------	--	----

Indicador 1. Oportunidad en la Atención de Asistencias Técnicas

Meta 2025: ≤ 48 horas.

Resultado anual (promedio 2025): 66.19 h | Rango mensual: 24.63 h – 224.03 h | Meses con dato: 12/12.

Cumplimiento anual: No cumple.

Meses con desviación frente a la meta: Enero, febrero, marzo, abril, mayo, junio, diciembre.

Análisis: Los tiempos de atención presentaron sobrepaso de la meta, con picos relevantes (enero). Esto sugiere acumulación de solicitudes, limitación de capacidad de respuesta, o ausencia de priorización/escala en ciertos periodos.

Indicador 5. Copias de Respaldo de base de datos

Meta 2025: ≥ 0.999 (99.9%).

Resultado anual (promedio 2025): 98.91% | Rango mensual: 86.89% – 100.00% | Meses con dato: 12/12. Cumplimiento anual: No cumple.

Meses con desviación frente a la meta: Agosto.

Análisis: El desempeño anual (98,91%) no alcanzó la meta (99,9%) debido a una caída significativa en agosto (86,89%). Esto incrementa el riesgo de pérdida de información y afecta la continuidad de los servicios. El evento ocurrido obedeció al ataque cibernético Ransomware en el mes de agosto 2025.

Principales hallazgos:

- Oportunidad en asistencias técnicas: promedio anual 66,19 horas (meta ≤48h); desviaciones concentradas en el primer semestre y diciembre.
- Copias de respaldo de base de datos: promedio anual 98,91% (meta ≥99,9%); desviación principal en agosto (86,89%).

	INFORME FINAL DE AUDITORIA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE CONTROL	GCO-IPA	220

El porcentaje % de Disponibilidad del Servicio de Conectividad: La meta establecida para el porcentaje de disponibilidad del servicio de conectividad es del 99%. Los resultados muestran niveles superiores al 99%, indicando un desempeño consistente y cumplimiento de la meta.

La oficina de Comunicaciones y Sistemas, en su compromiso con la evaluación permanente de la conectividad, realiza un seguimiento mensual a los servicios prestados en los 22 centros de salud y la sede administrativa de Pasto Salud ESE. Este informe tiene como objetivo identificar y solucionar cualquier inconveniente, minimizando riesgos de pérdida de información y caídas en el sistema, lo que garantiza el adecuado registro de datos en la historia clínica y el acceso al sistema de información SIOS. Pasto Salud ESE cuenta con conectividad en todas sus sedes, integradas mediante fibra óptica y radioenlaces, permitiendo la transmisión segura de datos y la consulta de información en cualquier punto de atención.

RESUMEN NO DISPONIBILIDAD DE SERVICIO El indicador refleja la suma total de minutos en los que cada red experimentó interrupciones en el servicio de conectividad a lo largo del mes. Dichos tiempos de no disponibilidad se acumulan considerando únicamente los horarios de atención establecidos en los centros de salud.

RESUMEN SERVICIO DE CONECTIVIDAD ENERO 2025

	ENERO
SUBTOTAL NORTE	76,168 (99.8%)
SUBTOTAL SUR	91,580 (99.89%)
SUBTOTAL OCCIDENTE	86,691 (99.78%)
SUBTOTAL ORIENTE	68,186 (99.68%)
TOTAL	322,625 (99.8%)

Tabla 1. Porcentaje de cumplimiento de conectividad Redes de Atención Pasto Salud ESE ENERO, 2025, fuente: comunicaciones y sistemas herramienta PRTG.

RESUMEN NO DISPONIBILIDAD DE SERVICIO

El indicador refleja la suma total de minutos en los que cada red experimentó interrupciones en el servicio de conectividad a lo largo del mes. Dichos tiempos de no disponibilidad se acumulan considerando únicamente los horarios de atención establecidos en los centros de salud.

	ENERO
SUBTOTAL NORTE	152
SUBTOTAL SUR	100

	INFORME FINAL DE AUDITORIA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE CONTROL	GCO-IPA	220

SUBTOTAL OCCIDENTE	189
SUBTOTAL ORIENTE	214
TOTAL	655 (10.917 horas)

Tabla 2. Número de minutos de no disponibilidad del servicio conectividad en las Redes de Atención Pasto Salud Enero, 2025, fuente: comunicaciones y sistemas herramienta PRTG.

Conclusiones generales

Tras el seguimiento y monitoreo de los canales de conectividad, internet y servicio de seguridad perimetral, se verificó que, durante el período del 1 al 31 de enero de 2025, el proveedor alcanzó un cumplimiento del 99.8% (99.90%). Las incidencias reportadas a través de la plataforma Osticket estuvieron relacionadas principalmente con el uso del sistema de información y la conectividad en algunos puntos. Además, se identificaron días específicos con afectaciones en el servicio, como se detalla en las gráficas.

Para garantizar la estabilidad del servicio y minimizar futuras incidencias, se ha mantenido una comunicación constante con el proveedor, realizando reuniones periódicas para la verificación de cumplimiento y el análisis de reportes de seguimiento. Asimismo, es fundamental continuar con la ejecución del cronograma de conexión, la afinación de puntos, la estabilización de la red e internet, la actualización de políticas de seguridad y la coordinación de la apertura de nuevos centros de salud.

Para la verificación de conectividad, se verifico el informe mensual de sistemas palacios, en la cual se reportan los datos críticos en diferentes sedes, también se verifico la meta mensual, en la cual alcanza el cumplimiento.

Informe Técnico Del Incidente De Ciberseguridad Ataque De Virus Ransomware

Fecha del Incidente: 19 de agosto de 2025

Periodo de Afectación: 19 al 24 de agosto de 2025

El día 19 de agosto de 2025, a las 10:38 p.m., los sistemas de información de Pasto Salud E.S.E. fueron impactados por un ataque externo de tipo ransomware, un tipo de código malicioso diseñado para encriptar la información sensible y bloquear el acceso a los sistemas institucionales, con el propósito de extorsionar a la organización a cambio de un rescate económico.

El ataque afectó la disponibilidad y el acceso a diversos servicios tecnológicos, incluyendo servidores críticos del sistema de información institucional, carpetas compartidas y algunos equipos de trabajo conectados a la red corporativa. Al detectarse la situación, se activaron de manera inmediata los protocolos de respuesta y el Plan de Contingencia Institucional, con el fin de garantizar la continuidad mínima de la operación asistencial y administrativa.

	INFORME FINAL DE AUDITORIA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE CONTROL	GCO-IPA	220

El proceso se documentó de manera integral la trazabilidad del incidente, las acciones ejecutadas desde su detección hasta la recuperación total de los servicios, así como los impactos, lecciones aprendidas y medidas de fortalecimiento implementadas.

Activación del Plan de Contingencia

El día 19 de agosto de 2025, a las 10:50 p.m., se procedió a la activación del Plan de Contingencia Institucional de Sistemas de Información, conforme a los lineamientos establecidos por la Oficina Asesora de Comunicaciones y Sistemas.

La decisión se tomó tras confirmarse la indisponibilidad general del sistema de información SIOS en todas las sedes y unidades de atención.

El plan establece un protocolo detallado para la atención de eventos que comprometan la disponibilidad de los sistemas institucionales.

En este caso, el diagnóstico inicial determinó que la contingencia se activaba bajo el escenario de “Daño en los servidores principales y/o servidores virtuales del clúster del Data Center” y “Daño en las bases de datos institucionales”, cuya causa raíz fue posteriormente al día siguiente identificada como un ataque cibernético tipo ransomware.

Durante el evento, se puso en marcha la cadena de llamada de contingencia, procedimiento establecido para la atención de incidentes ocurridos fuera del horario laboral. La enfermera jefa del servicio de Urgencias, al detectar la caída del sistema, notifica de inmediato al técnico de sistemas de turno en su sede, quien realiza las pruebas iniciales para determinar si la afectación era temporal o generalizada. Tras aproximadamente 10 minutos de verificación, se confirma la indisponibilidad total del servicio en todas las sedes, motivo por el cual se autoriza formalmente la activación del plan de contingencia a nivel institucional.

Una vez declarado el evento, el personal asistencial y administrativo implementa los procedimientos alternos manuales previamente establecidos, garantizando la continuidad en la atención de los usuarios y el registro básico de la información asistencial. Paralelamente, el equipo de sistemas inicia el proceso de diagnóstico técnico y acciones de contención, priorizando la protección de la infraestructura y la recuperación controlada de los servicios afectados.

Detección del incidente

Se reciben alertas desde las diferentes sedes de Pasto Salud E.S.E. por indisponibilidad del sistema de información SIOS, evidenciándose fallos generalizados en la conexión y en la respuesta del sistema.

La Oficina Asesora de Comunicaciones y Sistemas inicia de inmediato la verificación del evento y confirma que se trata de una afectación generalizada de la infraestructura tecnológica institucional.

Día 19/08/2025 – 10:50 p.m. | Activación del Plan de Contingencia: Responsables: Técnicos de Sistemas de cada sede, Ingeniero Christian de La Rosa Profesional Universitario, William Montenegro Profesional

	INFORME FINAL DE AUDITORIA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE CONTROL	GCO-IPA	220

Universitario Con base en el Plan de Contingencia de Sistemas de Información, se activa la contingencia en todas las sedes de la entidad.

El personal asistencial y administrativo procede a implementar los procedimientos alternos manuales establecidos, con el fin de garantizar la continuidad de la atención a los usuarios mientras se determina la causa del incidente.

Día 20/08/2025 – 07:00 a.m. | Evaluación inicial de afectaciones

Responsables: Ingeniero Iván Ibarra Muñoz, Ingeniero Christian de La Rosa, William Montenegro G., Ingeniero José Fernando Mora M., Ingeniero Diego Sánchez.

El equipo técnico realiza una inspección en el Data Center institucional, identificando archivos encriptados en varias unidades de almacenamiento y servidores. Se determina que el evento corresponde a un ataque tipo ransomware, el cual había comprometido la información y la disponibilidad de los servicios de red.

Día 20/08/2025 – 07:30 a.m. | Aislamiento de infraestructura afectada responsables: Ingeniero Christian de La Rosa, William Montenegro G. Se ejecuta el aislamiento inmediato de los servidores, cabinas de almacenamiento y switches principales, desconectándolos de la red institucional para evitar propagación del código malicioso. Se informa el incidente a los proveedores Infortec y Sistemas Palacios, quienes inician acompañamiento técnico remoto para el diagnóstico y contención del ataque.

Día 20/08/2025 – 08:40 p.m. Recuperación de copias de seguridad (backups)

Día 22/08/2025 – 09:15 a.m. Restauración de bases de datos en SQL Server

Responsables: Ingeniero Christian de La Rosa Finalizada la descarga de los respaldos, se procede a la restauración de las bases de datos en el servidor SQL Server, proceso que culmina el 23 de agosto al mediodía. Cada base requirió aproximadamente 5 horas de restauración y validación de consistencia.

Día 23/08/2025 – 07:00 a.m. Validación de integridad de datos

Día 24/08/2025 – 11:30 p.m. | Actualizaciones de hardware y pruebas finales

Día 25/08/2025 – 06:00 a.m. | Restablecimiento del servicio en producción

Día 26/08/2025 – 07:30 a.m. | Evaluación de resultados de operación

Aplicativos restaurados (14):

Generador de certificados laborales, generador de certificados de retención, desprendible de pago, documento soporte, generador de historia clínica de crónicos consolidado, lavado de manos, nómina novedades, reempaque de medicamentos, integración Bionexo, integración Emssanar, entre otros.

Bases de datos restauradas (22):

SIOS, Génova, Nómina, Contratistas, Kaelum, Lavado Manos, HV equipos, Contratistas Soporte Dian, Reempaque Medicamentos, Bioservice (Bionexo), Integración Client, Bd Calidad, Bodega Indicadores, Bodega RIPS, Facturas PT, FUID, Orfeo, Bd Esterilización, entre otras.

	INFORME FINAL DE AUDITORIA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE CONTROL	GCO-IPA	220

Y así se describe día a día, como se fue restableciendo el sistema, se contrató empresas especializadas con ese fin

Impacto Operacional y Pérdida de Información

Sistemas Afectados

Hardware • Servidores • Unidades Power Vault • Nas Unidades de almacenamiento
Aplicaciones Software • Sistema de Información SIOS • Orfeo (Gestión Documental) • Generador de certificados laborales • Generador de certificados de retención • Desprendible de pago • Documento soporte • Generador de historia clínica de crónicos consolidado • Lavado de manos • Nómina novedades • Reempaque de medicamentos • Integración Bionexo • Integración Emssanar • FUID (Formato único de Inventario Documental) • Hoja de vida de equipos • Esterilización.

Encriptamiento de:

• Sistemas operativos de Servidores y unidades de almacenamiento
Bases de datos • Archivos de usuario final • Aplicaciones de Software • Indisponibilidad de todos los servicios Administrativos y asistenciales • Se pierde información de archivos finales de usuarios, respaldos de bases de datos y archivos en unidades de almacenamiento.

A partir del análisis del incidente de ransomware que afectó la disponibilidad institucional entre el 19 y 24 de agosto de 2025, la ESE orientó inversión y gestión a controles prioritarios de prevención, con tención y fortalecimiento:

1. Planeación y aseguramiento presupuestal (PETIC 2026) • Se proyectó en el PETIC un rubro específico para ciberseguridad, asegurando financiación para la implementación de controles de seguridad multicapa y continuidad operativa, alineado a las recomendaciones del informe (defensa en profundidad y sostenibilidad).
2. Control del soporte remoto y trazabilidad operativa • Se adquirieron 10 licencias de soporte remoto para estandarizar el acceso de soporte, mejorar la trazabilidad y reducir accesos informales/no controlados (en el incidente se aplicó bloqueo temporal de accesos remotos como medida de contención, evidenciando la necesidad de control formal de estos canales).
3. Gestión segura de credenciales • Se adquirió Bitwarden como gestor corporativo de contraseñas
4. Asesoría técnica para inversión en tecnología especializada (capa perimetral, endpoint y servicios gestionados)
5. Medidas técnicas aplicadas y formalización de políticas

La inversión a partir del incidente, es aproximadamente de CUATROCIENTOS VEINTE MILLONES DE PESOS (420.000.000), lo que se requiere para blindar a la ESE, para el proyecto de ciberseguridad, de acuerdo a lo planteado por la Oficina de Sistemas y Comunicaciones, y que es importante que se analice con carácter URGENTE, para su implementación.

Conclusiones y Recomendaciones:

El ataque de tipo ransomware del 19 de agosto de 2025 puso a prueba la capacidad técnica, operativa y de respuesta institucional de Pasto Salud E.S.E.

	INFORME FINAL DE AUDITORIA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE CONTROL	GCO-IPA	220

A pesar del impacto inicial, se logró contener, aislar y recuperar la operación tecnológica mediante la activación oportuna del Plan de Contingencia y el trabajo coordinado entre los equipos internos y los proveedores de soporte.

La respuesta técnica permitió recuperar la mayoría de las bases de datos y aplicativos institucionales en un plazo de cinco días, con pérdidas mínimas de información en las bases de datos críticas.

No obstante, el incidente evidenció la necesidad de fortalecer de manera estructural la infraestructura tecnológica, los mecanismos de seguridad perimetral y las políticas de ciberseguridad de la entidad.

En Conclusión, tenemos:

1. El incidente confirmó la existencia de vulnerabilidades en la red institucional y la necesidad de contar con un esquema de seguridad multicapa (defensa en profundidad).
2. Los respaldos en la nube y la rápida activación del plan de contingencia fueron factores clave para la recuperación.
3. Se requiere formalizar políticas de continuidad del negocio y recuperación ante desastres (BCP/DRP) con actualizaciones periódicas.
4. La experiencia adquirida refuerza la importancia de la capacitación del personal en la detección temprana y manejo de incidentes.

Recomendaciones Estratégicas

1. Implementar de forma prioritaria el Plan de Fortalecimiento y Blindaje Tecnológico, contemplado en el numeral 12.6, que incluye renovación de firewall, licencias EDR, y servicios gestionados de ciberseguridad.
2. Asegurar la reubicación del Data Center principal en la sede Santa Mónica y la creación del clúster de contingencia en la sede administrativa.
3. Consolidar un programa permanente de monitoreo y auditoría de seguridad, con retroalimentación.
4. Establecer campañas institucionales de concientización y buenas prácticas de seguridad para todos los funcionarios.
5. Mantener el respaldo financiero y presupuestal por parte de la Gerencia General, garantizando la sostenibilidad de los proyectos tecnológicos y la ejecución del plan de seguridad.
6. Incorporación de un Profesional en Ciberseguridad El incidente del 19 de agosto de 2025 evidenció la necesidad de contar con recurso humano especializado en ciberseguridad, que permita anticipar, prevenir y responder de manera oportuna ante amenazas informáticas.

Por tanto, se recomienda a la Gerencia General de Pasto Salud E.S.E. evaluar la creación o contratación permanente de un Ingeniero en Ciberseguridad, encargado de las siguientes funciones:

- Monitorear y gestionar la infraestructura de seguridad de la entidad (firewall, antivirus, EDR, backups, red y nube).
- Liderar el diseño e implementación de políticas, procedimientos y controles de ciberseguridad bajo estándares internacionales (ISO 27001, NIST, OWASP).
- Coordinar con los proveedores externos de soporte, asegurando el cumplimiento de niveles de servicio y protocolos de seguridad.
- Administrar alertas, vulnerabilidades y reportes generados por las plataformas de seguridad y los sistemas de información.

	INFORME FINAL DE AUDITORIA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE CONTROL	GCO-IPA	220

- Elaborar reportes técnicos y de riesgo ante la Gerencia, y coordinar la respuesta ante incidentes (CSIRT interno).

MIPG – POLITICA DE TRANSPARENCIA, ACCESO A LA INFORMACION PÚBLICA Y LUCHA CONTRA LA CORRUPCION

Se evidencia que en el mes de marzo de 2025 se diligencio por parte del Jefe de la Oficina Asesora de Comunicaciones y Sistemas el Autodiagnóstico del Modelo Integrado de Planeación y Gestión correspondiente a la Política de Transparencia y Acceso a la Información, dando como resultado del ejercicio una calificación total de 95 sobre 100.

Esa política se divide en 8 componentes, los cuales tuvieron los siguientes resultados así:

De las 97 actividades de gestión que se relacionan y evalúan en esta política, se observa que se plantearon 2 acciones de mejora para ejecutarse en la vigencia 2025. Las cuales fueron ejecutadas en su totalidad según informe de seguimiento efectuado por la Oficina de Control Interno y cuya evaluación es de 99 sobre 100.

Se resalta que la realización del autodiagnóstico y formulación de Plan de Mejora es sistemática y deberá volverse a evaluar en la presente vigencia.

MIPG – POLITICA DE GOBIERNO DIGITAL

Se evidencia que en el mes de abril de 2025 se diligencio por parte del Jefe de la Oficina Asesora de Comunicaciones y Sistemas el Autodiagnóstico del Modelo Integrado de Planeación y Gestión correspondiente a la Política de Gobierno Digital, dando como resultado del ejercicio una calificación total de 90 sobre 100, y el seguimiento para febrero de 2026. La evaluación es de 99 sobre 100

Esa política se divide en 3 habilitadores de la Política de Gobierno Digital, los cuales tuvieron los siguientes resultados así:

REQUISITO INCUMPLIDO / ASPECTO A MEJORAR	Puntaje
Criterios de Accesibilidad nivel AA, AAA de acuerdo a la NT5854	90
Criterios de usabilidad en formularios electrónicos página web	100
Realizó la documentación y transferencia de conocimiento a proveedores, contratistas y/o responsables de TI, sobre entregables o resultados de proyectos de tecnología	100
Realizar campañas de difusión y estrategias que busquen la apropiación de las mejoras de los tramites en los servidores públicos de la entidad responsables de su implementación	100

De los 16 ítems que se relacionan y evalúan en esta política, se observa que se plantearon 16 acciones de mejora para ejecutarse en la vigencia 2025. De las cuales se ejecutaron 16 parcialmente, según informe de seguimiento efectuado por la Oficina de Control Interno y recomendaciones de la evaluación del FURAG.

	INFORME FINAL DE AUDITORIA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE CONTROL	GCO-IPA	220

Se resalta que la realización del autodiagnóstico y formulación de Plan de Mejora es sistemática y deberá volverse a evaluar en la presente vigencia.

MIPG – POLITICA DE SEGURIDAD DIGITAL

Es una política que busca que las entidades públicas:

- Protejan la información institucional.
- Gestionen los riesgos de seguridad digital.
- Garanticen la confidencialidad, integridad y disponibilidad de la información.
- Prevengan incidentes de ciberseguridad.
- Fortalezcan la confianza en los servicios digitales del Estado.

Dentro del MIPG, la política implica que las entidades deben:

- Implementar un Sistema de Gestión de Seguridad de la Información (SGSI).
- Identificar y gestionar riesgos digitales.
- Establecer controles de acceso a la información.
- Contar con planes de tratamiento de riesgos.
- Tener protocolos de respuesta ante incidentes.
- Capacitar a los servidores públicos en seguridad digital.
- Realizar monitoreo y mejora continua.

La Política de Seguridad Digital del MIPG consiste en que cada entidad pública debe gestionar de manera estructurada la seguridad de su información y sus sistemas tecnológicos, como parte integral de su gestión institucional y del control interno, de acuerdo al seguimiento realizado a esta política, de acuerdo al plan de mejora, la evaluación es del 100%, dando cumplimiento a todas sus actividades y con soportes, de acuerdo a recomendaciones de la evaluación FURAG.

MIPG POLITICA TRAMITES

La Política de Trámites del MIPG busca que las entidades públicas no le compliquen la vida al ciudadano, sino que hagan sus procedimientos más simples, eficientes y digitales, garantizando el principio de buena administración.

Consiste en que las entidades públicas deben simplificar, estandarizar, optimizar y digitalizar los trámites que ofrecen a ciudadanos y empresas, con el fin de:

- Reducir tiempos y costos.
- Eliminar requisitos innecesarios.
- Evitar duplicidad de documentos.
- Mejorar la experiencia del ciudadano.
- Aumentar la transparencia.

	INFORME FINAL DE AUDITORIA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE CONTROL	GCO-IPA	220

Identificar todos sus trámites y registrarlos en el SUIT.

- Analizar cargas y requisitos.
- Eliminar requisitos sin sustento legal.
- Automatizar o virtualizar cuando sea posible.
- Actualizar permanentemente la información.
- Medir tiempos de respuesta y satisfacción.

La evaluación para el primer seguimiento de 2025, fue de 93.3%, realizado por la Oficina de Control Interno y de acuerdo a la evaluación del FURAG, se estableció un plan de mejora en julio de 2025, a la fecha se encuentra cumplido en el 100%.

MIPG – POLITICA DE GESTION DOCUMENTAL

Se evidencia que en el mes de marzo de 2025 se diligenció por parte de la dependencia de Archivo y Correspondencia el Autodiagnóstico del Modelo Integrado de Planeación y Gestión correspondiente a la Política de Gestión Documental, el formato establecido por el Departamento Administrativo de la Gestión Pública, el cual se implementó un plan de mejora con un 81% de cumplimiento, con los siguientes avances:

Acciones plan de mejora 40

Acciones programadas y evaluadas 40

Acciones evaluadas cumplidas 32

Acciones evaluadas parcialmente cumplidas 1

Acciones evaluadas incumplidas 7

Porcentaje de cumplimiento del plan 81%

El nivel de avance de esta política fue del 81%, que corresponde a la ejecución de 40 actividades, de las cuales 8 actividades no se ejecutaron y que se plantearon para esa vigencia.

Se resalta que la realización del autodiagnóstico y formulación de Plan de Mejora es sistemática.

ESTADO DE LAS TABLAS DE RETENCION DOCUMENTAL Y TABLAS DE VALORACION DOCUMENTAL

Se evidencia que las tablas de retención documental fueron aprobadas en primera instancia por el Comité Institucional de Gestión y Desempeño, del cual se emite posteriormente la Resolución No. 420 del 1 de junio de 2022, por medio de la cual se aprueban las Tablas de Retención Documental de Pasto Salud ESE.

Se evidencia el envío de la documentación necesaria para la convalidación de las Tablas de Retención Documental al Consejo Departamental de Archivo de Nariño mediante oficio 202205610021001 radicado el 24 de junio de 2022, del cual a la fecha de auditoria no se ha recibido contestación. Igualmente se evidencia oficio 202305610021261 radicado el 25 de abril, sin que haya tenido respuesta alguna. Posteriormente se envía por parte de Pasto Salud ESE un derecho de petición al Consejo Departamental de Archivo de Nariño solicitando agilizar el trámite, sin que tenga respuesta alguna.

	INFORME FINAL DE AUDITORIA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE CONTROL	GCO-IPA	220

Una vez revisada la normatividad aplicable, se observa que según el Acuerdo 04 de 2019 del Archivo General de la Nación en el artículo 13 establece que el concepto técnico debió emitirse dentro de los 90 días hábiles siguientes a la presentación a la instancia competente.

Revisado y analizado lo contenido en el Acuerdo 04 de 2019 del Archivo General de la Nación, se podría asumir que las Tablas de Retención Documental no están convalidadas y no se podrían implementar en Pasto Salud ESE, por lo que se requiere gestiones inmediatas por parte de la Secretaria General y del responsable del área de gestión documental de la empresa.

Por otro lado, no se evidencia avance en la preparación, elaboración y formulación de las Tablas de Valoración Documental, sin embargo, se evidencia acta de Reunión del 24 de octubre de 2023 entre Pasto Salud ESE y el Archivo General de la Nación, en la cual se determina que a la empresa no le aplica las Tablas de Valoración Documental por cuanto no se tiene fondos acumulados en la empresa.

La instancia asesora para estos temas es el Comité de Archivos, cuya función es asesorar a la alta dirección de la entidad en materia archivística y de gestión documental, definir las políticas, los programas de trabajo y los planes relativos a la función archivística institucional, de conformidad con la Ley 594 de 2000 y demás normas reglamentarias, teniendo en cuenta que el Comité Institucional de Gestión y Desempeño absorbe las funciones de ese comité, deberá este último determinar las actuaciones de la entidad en esta materia y por lo tanto, se les deberá poner en conocimiento la demora injustificada del ente territorial en la aprobación de las Tablas de Retención Documental.

LICENCIAMIENTO DEL SOFTWARE SIOS – MANTENIMIENTO

Se observa que la Empresa tiene LICENCIA de uso vitalicia del Sistema de Información para Operaciones en Salud SIOS, para una cantidad ilimitada de instalaciones de computadores que se encuentren dentro de la red de la empresa. Contando con módulos asistenciales, financieros y de talento humano.

Se evidencia la suscripción del Contrato de Prestación de Servicios No. 097- 2025, el cual tiene como objeto “Prestación del servicio de soporte técnico, soporte funcional, actualizaciones, mantenimiento y disponibilidad permanente al sistema de información de operaciones en salud SIOS”, el cual dentro de la cláusula segunda establece unas fases y unas actividades.

El contrato se realiza por una suma total de SESENTA MILLONES (\$60.000.000), en el cual se estipula la forma de pago.

Se evidencia la suscripción del Contrato de Prestación de Servicios No. 0508 – 2025, el cual tiene como objeto “Prestación del servicio de mantenimiento preventivo y correctivo, al sistema de información de operaciones en salud SIOS.

El contrato se realiza por una suma total de TREINTA Y SEIS MILLONES QUINIENTOS NOVENTA Y CUATRO MIL PESOS (\$36.594.000), en el cual se estipula la forma de pago.

	INFORME FINAL DE AUDITORIA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE CONTROL	GCO-IPA	220

Se evidencia la suscripción del Contrato de Prestación de Servicios No. 1024 – 2025, el cual tiene como objeto Prestación del servicio de soporte técnico, funcional y de mantenimiento preventivo y correctivo del sistema de información de operaciones en salud SIOS.

El contrato se realiza por una suma total de TREINTA MILLONES DE PESOS (\$30.000.000), en el cual se estipula la forma de pago.

Se establece como plazo para la ejecución del contrato hasta el día 31 de diciembre de 2025.

Una vez revisado el contrato, se observa que existen criterios puntuales para la actualización de los módulos de facturación, de administración y estadísticas, el cual fue recibido a satisfacción por cada líder de servicio, según actas.

MATRIZ DE RIESGOS DEL PROCESO

Se evidencia la definición de una matriz de riesgos – Seguridad de la información (formato GSI-RSI 411), en el cual se identificaron 6 riesgos aplicables a este proceso. De los cuales 1 está catalogado como MODERADO después de controles, y 5 están catalogados como ALTOS después de controles.

De acuerdo a informe de auditoría de riesgos, se materializo un riesgo en el II semestre de la vigencia 2025.

. Pérdida de la confidencialidad y disponibilidad de la información

1. Se evidencia la materialización del riesgo relacionado con “**pérdida de la confidencialidad y disponibilidad de la información**” por falla en el servidor 229 PowerEdge R740XD - Placa 240899 toda vez que en la realización de mantenimiento preventivo el día 26 de diciembre del 2025 el servidor no inicia el sistema operativo y no reconoce los discos duros impidiendo su funcionamiento, generando perdida de bases de datos de información institucional como por ejemplo (ALFRESCO, ORFEO, SIVIGILA entre otros)

Evidencia que soporta la pérdida de información, Software Orfeo desde el 27 de diciembre de 2024 hasta el 10 de enero de 2025, se presenta falla en la consulta de la imagen principal y documento en PDF de los radicados en Orfeo, al consultar información del año 2022, 2023 y parte del año 2024 no se evidencian las imágenes principales, ni el documento en pdf, lo anterior se realiza mediante reporte oficial No. 202505610010743 del día 18 de febrero de 2025 por la técnica administrativa gestión documental

Desviación de controles

Se evidencia falla en la efectividad del control relacionado con “mantenimientos” toda vez que para el segundo semestre de 2025 no se logra la meta programada respecto a la ejecución de mantenimiento preventivo de los equipos informáticos

Evidencias de incumplimiento:

Segundo semestre 2025

Formula: (mantenimientos preventivos realizados/mantenimientos preventivos programados) *100

	INFORME FINAL DE AUDITORIA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE CONTROL	GCO-IPA	220

Meta: 95%

Julio: $135/195=69,23\%$ Centro hospital la Rosa

Agosto: $69/107=64,49\%$: Hospital santa Mónica

Septiembre: $111/140=79,29\%$ CS San Vicente

Octubre: $106/125=84,80\%$ Hospital Local Civil

Diciembre: $4/7=57,14\%$ CS San Vicente

$6/7=85,76\%$ Centro hospital la Rosa

El proceso gestión de Sistemas de información, tiene identificado 7 riesgos para la vigencia 2025



Para el primer semestre de la vigencia 2025, no se materializó ningún riesgo, pero si se evidenció incumplimiento de 3 acciones a los controles establecidos, el cual se estableció el plan de mejora en la auditoría del sistema de administración del riesgo.

Para el segundo semestre se materializó el riesgo con **“pérdida de la confidencialidad y disponibilidad de la información”** por falla en el servidor 229 PowerEdge R740XD - Placa 240899

CONCLUSIONES

En el desarrollo de la presente auditoría se puede concluir que el Proceso GESTION DE SISTEMAS DE INFORMACION, se verifica algunas inconsistencias con los objetivos de la presente auditoría, por cuanto hay un incumplimiento según lo definido en sus Planes de Comunicación y Plan de Seguridad y Privacidad de la Información.

Se observa que el plan de comunicaciones, para la vigencia 2025 no se elaboró ni se actualizó, con el plan estratégico de Pasto Salud ESE 2025 - 2028, se cuenta con un plan de la vigencia 2024.

En el plan de comunicaciones de acuerdo a los indicadores presentados, se recomienda fortalecer el uso del correo electrónico, manteniéndolo como el medio prioritario, pero optimizando su uso con mensajes claros, organizados y periódicos, potenciar la página institucional y reuniones como medios complementarios, asegurando que la información relevante esté siempre actualizada.

	INFORME FINAL DE AUDITORIA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE CONTROL	GCO-IPA	220

En el plan de seguridad, se realizó una auditoría interna en la misma dependencia, con el fin de determinar unos hallazgos y controles de la Información 2025, con el siguiente resultado:

Se cuenta con un inventario actualizado de todos los equipos de su red por IPS?, Durante el I semestre 2025, solo el (6.493%) 15 de los 231 equipos de cómputo verificados durante la actividad de seguimiento y control, no contaban con un registro totalmente actualizado en el sistema de hojas de vida de Equipos de cómputo, teniendo como comparativa la configuración de hardware, actualización de dispositivos, ubicación de área de trabajo y placa asignada por almacén, sin embargo, esta última actividad, depende del área de almacén, ya que algunos traslados no se han realizado por parte de esta área, se toma como realiza las respectivas recomendaciones a todos los Técnicos para la oportuna actualización, ya que el registro y actualización de la información debe ser permanentemente desde comienzo hasta el final del año revisado.

Se evidencia inconsistencias en el manejo de placas asignadas para equipos de cómputo, como es el caso de equipos que no se encuentran debidamente señalados, o números de placa ilegibles, además casos particulares en donde se encontraron placas duplicadas errores que crearon confusión durante el seguimiento y control de los equipos, de estas inconsistencias, se informó a Almacen para lo de su competencia.

Oportunidad en asistencias técnicas: promedio anual 66,19 horas (meta $\leq 48h$); desviaciones concentradas en el primer semestre y diciembre.

Copias de respaldo de base de datos: promedio anual 98,91% (meta $\geq 99,9\%$); desviación principal en agosto (86,89%).

El porcentaje % de Disponibilidad del Servicio de Conectividad: La meta establecida para el porcentaje de disponibilidad del servicio de conectividad es del 99%. Los resultados muestran niveles superiores al 99%, indicando un desempeño consistente y cumplimiento de la meta.

Tras el seguimiento y monitoreo de los canales de conectividad, internet y servicio de seguridad perimetral, se verificó que, durante el período del 1 al 31 de enero de 2025, el proveedor alcanzó un cumplimiento del 99.8% (99.90%).

El ataque de tipo ransomware del 19 de agosto de 2025 puso a prueba la capacidad técnica, operativa y de respuesta institucional de Pasto Salud E.S.E.

A pesar del impacto inicial, se logró contener, aislar y recuperar la operación tecnológica mediante la activación oportuna del Plan de Contingencia y el trabajo coordinado entre los equipos internos y los proveedores de soporte.

El incidente confirmó la existencia de vulnerabilidades en la red institucional y la necesidad de contar con un esquema de seguridad multicapa (defensa en profundidad).

	INFORME FINAL DE AUDITORIA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE CONTROL	GCO-IPA	220

Los respaldos en la nube y la rápida activación del plan de contingencia fueron factores clave para la recuperación.

Se requiere formalizar políticas de continuidad del negocio y recuperación ante desastres (BCP/DRP) con actualizaciones periódicas.

La experiencia adquirida refuerza la importancia de la capacitación del personal en la detección temprana y manejo de incidentes.

A raíz del ataque de tipo ransomware, se generó la pérdida de bases de datos de información institucional como por ejemplo (ALFRESCO, ORFEO, SIVIGILA entre otros).

De igual manera se evidencian un nivel de cumplimiento satisfactorio de los Planes de Mejora definido para las políticas del MIPG asociadas a transparencia y acceso a la información pública y lucha contra la corrupción (95%), gobierno digital (99%) y gestión documental (81%).

Se hace necesario analizar y abordar el nivel de cumplimiento de la Ley General de Archivos (Ley 594 de 2000 y reglamentarias) desde el Comité Institucional de Gestión y Desempeño.

No se evidencia inconsistencias en la ejecución de los contratos 097, 0508 y 1024 de 2025, respecto al mantenimiento y actualización de algunos módulos en SIOS, la cual cuanta con recibido a satisfacción mediante acta por los líderes o responsables de los diferentes módulos.

La materialización del riesgo de pérdida de confidencialidad y disponibilidad de la información exige la formulación inmediata de un Plan de Mejoramiento con acciones correctivas y preventivas, seguimiento trimestral y reporte al Comité Institucional de Gestión y Desempeño.

En la gestión del riesgo se materializa un riesgo, “Pérdida de la confidencialidad y disponibilidad de la información”, el cual debe realizar el plan de mejora en la auditoria de riesgos

HALLAZGOS
1. Se evidencia incumplimiento en la formulación y actualización del Plan de Comunicaciones 2025, en concordancia con el Plan Estratégico 2025-2028 de Pasto Salud E.S.E., manteniéndose vigente únicamente el documento correspondiente a la vigencia 2024. 2. Se evidencia debilidades en la gestión del inventario y control de equipos de cómputo, durante el I semestre de 2025, el 6,493% (15 de 231 equipos verificados) no contaban con registro totalmente actualizado en el sistema de hojas de vida de equipos de cómputo. Se evidenciaron inconsistencias en placas de inventario (placas ilegibles, equipos sin identificación y duplicidad de numeración), principios de control interno relacionados con salvaguarda de activos. 3. Se evidencia incumplimiento en la meta de oportunidad de asistencia técnica, el promedio anual de atención fue de 66,19 horas, superando la meta establecida de ≤ 48 horas, con mayores desviaciones en el primer semestre y diciembre. Lo cual posiblemente hay afectación en la continuidad operativa de los servicios institucionales.

4. Se evidencia un incumplimiento parcial en copias de respaldo de bases de datos, el promedio anual fue de 98,91% frente a una meta $\geq 99,9\%$, con desviación significativa en agosto (86,89%). Afecta la Política de Seguridad y Privacidad de la Información – lineamientos de respaldo y recuperación de información, lo que puede generar posibles fallas técnicas asociadas al incidente de seguridad presentado en agosto.
5. Se evidencia la materialización del riesgo: Pérdida de confidencialidad y disponibilidad de la información, que surgió el 19 de agosto de 2025, el cual se presentó un ataque tipo ransomware que ocasionó pérdida de bases de datos institucionales (ALFRESCO, ORFEO, SIVIGILA, entre otros), evidenciando vulnerabilidades en la red, con la materialización del Mapa de Riesgos Institucional; Política de Seguridad de la Información; lineamientos de Gobierno Digital, el cual presuntamente existió debilidades en el esquema de seguridad perimetral y ausencia de un esquema formalizado de seguridad multicapa y continuidad del negocio y riesgo en la disponibilidad y recuperación de información crítica.
6. Se evidencia un nivel intermedio de avance en la implementación de la política de Gestión Documental, lo anterior por cuanto el 81% de los ítems evaluados se encuentran entre avanzado, y solo el 19% está Inicial, Bajo o Intermedio. Se observa Debilidades en la implementación integral de lineamientos archivísticos y el riesgo de incumplimiento normativo y pérdida de información institucional.

RECOMENDACIONES

1. Continuar aplicando los controles y ejecución de los procedimientos establecidos en el proceso.
2. Diligenciar los autodiagnósticos vigencia 2026 de las políticas establecidas para esta dependencia y establecer planes para su mejora continua.
3. Continuar con las gestiones necesarias ante el ente territorial para la correcta aprobación de las Tablas de Retención Documental.
4. Coordinar entre secretaria general (líder de la política de Gestión Documental) y Jefe Oficina Asesora de Comunicaciones y Sistemas (líder del proceso Sistemas de Información) la forma de abordar y desarrollar los hallazgos presentados en esta auditoría.
5. Implementar de forma prioritaria el Plan de Fortalecimiento y Blindaje Tecnológico, contemplado en el numeral 12.6, que incluye renovación de firewall, licencias EDR, y servicios gestionados de ciberseguridad.
6. Consolidar un programa permanente de monitoreo y auditoría de seguridad, con retroalimentación.
7. Establecer campañas institucionales de concientización y buenas prácticas de seguridad para todos los funcionarios.
8. Mantener el respaldo financiero y presupuestal por parte de la Gerencia General, garantizando la sostenibilidad de los proyectos tecnológicos y la ejecución del plan de seguridad.
9. Incorporación de un Profesional en Ciberseguridad El incidente del 19 de agosto de 2025 evidenció la necesidad de contar con recurso humano especializado en ciberseguridad, que permita anticipar, prevenir y responder de manera oportuna ante amenazas informáticas.
10. Se recomienda a la Gerencia de Pasto Salud E.S.E. evaluar la creación o contratación permanente de un Ingeniero en Ciberseguridad
11. Implementar esquema de seguridad en profundidad.
12. Fortalecer capacitación en ciberseguridad.
13. Actualizar el mapa de riesgos y formular plan de mejora específico.
14. La compra de licencias antivirus anti-ransomware Sophos XDR
15. La compra de licencias SOPHOS EMAIL ADVANCED
16. La compra de licencias Firewall Perimetral.
17. Compra del servicio de Penetración y ataque para detectar vulnerabilidades

FORTALEZAS

 EMPRESA SOCIAL DEL ESTADO PASTO SALUD E.S.E NIT. 900081143-8	INFORME FINAL DE AUDITORIA			
	VERSIÓN	PROCESO / SERVICIO	CODIGO	NUM
	6.0	GESTION DE CONTROL	GCO-IPA	220

ELABORO:	JAIME ALBERTO SANTACRUZ S	FECHA	3 de marzo de 2026
REVISADO POR:	JAIME ALBERTO SANTACRUZ S.	FECHA	3 de marzo de 2026