Fecha de elaboración: 08/04/2026 **Auditoría Interna No.** 4

LIDER DE PROCESO Y/O SUBPROCESO, PROYECTO
MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y POLÍTICA DE GOBIERNO DIGITAL
1. OBJETIVO
Verificar el grado de implementación del modelo de Seguridad y privacidad de la información y política de gobierno digital.
2. ALCANCE
Verificar y evaluar las actividades ejecutadas del modelo de Seguridad y privacidad de la información y política de gobierno digital en la ESE Hospital del Sarare desde su planeacion, ejecución, verificación
3. CRITERIOS
NTC 5854:2011 Decreto 767 del 2022 Lineamientos Política Gobierno Digital Ley 1437 de 2011 Resolución número 00500 de marzo 10 de 2021 emanada de MinTic, "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital" Resolución N° 001519 de 24 de agosto de 2020, emanada de MinTic, Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos". Decreto 2573 de 2014. " Por el cual se establecen los lineamientos generales del a Estrategia de Gobierno en Línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones". Ley 1712 de 2014. " Por medio de la cual se crea la ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones". El Artículo 2.2.9.1.2.1 del Decreto 1078 de 2015, "Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones" Decreto 1499 de 2017 Decreto 1008 del 14 de junio de 2018. "Por la cual se establecen los lineamientos generales del a política de Gobierno Digital". Decreto 2106 del 22 de noviembre de 2019. Directiva Presencial 002 de 2002. "Derechos de autor con el uso de programas de computador (Sotware)". Resolución 2710 de 2017." Por la cual se establecen los lineamientos para la adopción del protocolo IPv6". Decreto nacional 103 de 2015. "Estándares de MINTIC para la publicación de información pública en concordancia con la estrategia de Gobierno en Línea" el Artículo 2.2.17.1.1. del Decreto 1078 de 2015 reglamenta parcialmente los artículos 53, 54. 60. 61 y 64 de la Ley 1437 de 2011, los literales e, j y el parágrafo 2" del artículo 45 de la Ley 1753 de 2015, el

Numeral 3 del artículo 147 de la Ley 1955 de 2019. y el artículo 9 del Decreto 2106 de 2019. Ley 1266 de 2008. " por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones Ley 1341 de 2009."Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización del as Tecnologías del a información y las comunicaciones". Resolución No 02277 del 03 de junio del 2025 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".

4. EQUIPO AUDITOR	
Yenny Carolina Suárez	Líder de Auditoria / Asesora Control Interno

Reunión de Apertura					**Ejecución de la Auditoría**				**Reunión de Cierre**					
18	**Mes**	03	**Año**	2026	**Desde**	18/03/26 D / M / A	**Hasta**	25/03/26 D / M / A	Día	30	Mes	03	Año	2026

5. INFORME DE VERIFICACION (RESUMEN EJECUTIVO)

Verificar el grado de implementación del modelo de Seguridad y privacidad de la información y política de gobierno digital.

Metodología

1. Entendimiento y recorrido de:
   a) Proceso y flujo de información
   b) Áreas involucradas en el proceso
   c) Actividades de control a nivel entidad

2. Identificación, valoración de riesgos y controles clave del proceso.
3. Planeación y ejecución de pruebas a controles (diseño, efectividad, detalle).
4. Identificación de posibles brechas de control y oportunidades de mejoramiento.
5. Discusión y validación del informe con el del líder del proceso y definición de planes de acción estructurales para su mejoramiento.

Cada etapa de auditoría (entendimiento del proceso, evaluación del riesgo, evaluación y prueba de controles) será desarrollada mediante:

1. Lectura de la documentación vigente del proceso;
2. Entrevistas con el líder del proceso y el personal involucrado en el mismo;
3. Inspección de documentos relacionados con la ejecución del proceso;
4. Solicitud de documentos relacionados con la ejecución del proceso
5. Verificación de:

5.1 Grado de implementación de la política de seguridad y privacidad de la información
5.2 Grado de implementación de la política de Gobierno digital
5.3 Verificación del Plan estratégico de las tecnologías de la información PETI en ciclo PHVA
5.4 Software
5.5 Inventario equipos de computo
5.6 Accesibilidad en la página web bajo la NTC 5854
5.7 Verificación datos abiertos, pagina web (transparencia y acceso a la información).

Para facilitar la comprensión y orden del presente informe se presenta la siguiente tabla de Contenido.

Contenido

METODOLOGIA

El equipo auditor interno realizó visita a la oficina de Sistemas de información de la ESE Hospital del Sarare, la auditoria fue atendida por la Ingeniera de Sistemas líder de la entidad.

Se aplicó una lista de chequeo con los siguientes capítulos:

1.ASPECTOS GENERALES
2. POLICITA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
3.POLITICA GOBIERNO DIGITAL (Decreto 767 de 2022)
4. PLAN ESTRATEGICO DE LAS TECNOLOGIAS DE LA INFORMACION (PETI)
5.SOFTWARE
6.INVENTARIOS EQUIPOS DE COMPUTO
7.ACCESIBILIDAD A LA PAGINA WEB (NTC 5458)
8. DATOS ABIERTOS Y PAGINA WEB (TRANSPARENCIA Y ACCESO A LA INFORMACIÓN
9. MANUAL DE POLITICAS Y PROCEDIMIENTOS – HABEAS DATA

Resultados que se obtuvo de la lista de verificación al modelo de Seguridad y privacidad de la información y política de gobierno digital con un porcentaje del 60%

SISTEMA INTEGRADO DE GESTIÓN

HOSPITAL DEL SARARE
Empresa Social del Estado

CODIGO SEI-01-F05

REVISIÓN No. 1

LISTA DE VERIFICACION - AUDITORIA INTERNA

Evolucionamos pensando en usted

FECHA DE AUDITORIA:		19 DE MARZO DE 2026
PROCESO AUDITADO:		GESTIÓN INTEGRAL DE LA INFORMACIÓN
SUBPROCESO AUDITADO:		GESTIÓN DE LAS TECNOLOGÍAS Y SISTEMA DE INFORMACIÓN
LIDER DEL PROCESO AUDITADO:		JUAN ALEXIS ARCHILA MANRIQUE
LIDER DEL SUB PROCESO AUDITADO:		YANET MORENO VELASCO
OBJETIVO DE LA AUDITORIA:		Verificar el grado de implementacion del modelo de Seguridad y privacidad de la información y politica de gobierno digital
ALCANCE DE LA AUDITORIA:		Verificar y evaluar las actividades ejecutadas del modelo de Seguridad y privacidad de la información y politica de gobierno digital en la ESE Hospital del Sarare desde su planeacion, ejecucion, verificacion
AUDITOR:		YENNY CAROLINA SUAREZ / Asesor Control Interno GERALDINE REAL LOZANO / Profesional Universitario Apoyo Control Interno

Marco Normativo.

NTC 5854:2011
Decreto 767 del 2022 Lineamientos Política Gobierno Digital
Ley 1437 de 2011
Resolución número 00500 de marzo 10 de 2021 emanada de MinTic, "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital"
Resolución N° 001519 de 24 de agosto de 2020, emanada de MinTic, Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos".
Decreto 2573 de 2014. " Por el cual se establecen los lineamientos generales del e Estrategia de Gobierno en Línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones".
Ley 1712 de 2014. " Por medio de la cual se crea la ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".
El Artículo 2.2.9.1.2.1 del Decreto 1078 de 2015, "Por medio del cual se expide el Decreto Única Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"
Decreto 1499 de 2017
Decreto 1008 del 14 de junio de 2018. "Por la cual se establecen los lineamientos generales del e política de Gobierno Digital".
Decreto 2106 del 22 de noviembre de 2019.
Directiva Presencial 002 de 2002. "Derechos de autor con el uso de programas de computador (Software)".
Resolución 2710 de 2017. " Por la cual se establecen los lineamientos para la adopción del protocolo IPv6".
Decreto nacional 103 de 2015. "Estándares de MINTIC para la publicación de información pública en concordancia con la estrategia de Gobierno en Línea"
el Artículo 2.2.17.1.1. del Decreto 1078 de 2015 reglamento parcialmente los artículos 53, 54, 60, 61 y 64 de la Ley 1437 de 2011, los literales a, j y el parágrafo 2° del artículo 45 de la Ley 1753 de 2015, el Numeral 3 del artículo 147 de la Ley 1955 de 2019, y el artículo 9 del Decreto 2106 de 2019.
Ley 1266 de 2008. " por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones
Ley 1341 de 2009. "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización del os Tecnologías de la información y las comunicaciones".
Este derecho constitucional se recoge en los artículos 15 y 20 de la Constitución Política; en la Ley
Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la ley de Protección de Datos

Decreto 886 del 2014 por medio del cual reglamento el articulo 25 de la ley 1581 del 2012 relativo al Registro Nacional de bases de datos.
Decreto 1074 de 2015 por medio del cual se expide el decreto unico reglamentario del sector comercio, industrial y turismo.

Personales (LEPD); en el decreto 1074 de 2015, y capítulo 25 sección 3 Articulo 2.2.2.25.3.2. del decreto
1074 de 2015, por el cual se reglamenta parcialmente la 1581 de 2012.
Ley 1273 del 2009 Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"
Decreto 1377 del 2013 Por medio del cual se reglamenta parcialmente la ley 1581 de 2012

LISTA DE VERIFCACION

1. ASPECTOS GENERALES

ASPECTO A EVALUAR	%	CUMPLE	EVIDENCIA	OBSERVACION	ITEM
1 ASPECTO GENERALES					
EVALUACIÓN TOTAL	33%				61%

Ilustración 1 Lista de verificación Auditoria

1. ASPECTOS GENERALES

1.1 Información documentada

Se realiza verificación en la carpeta IP4 dispuesta para la información documental de cada proceso, no Se evidenció documentos ni formatos.
Informan que los documentos se encuentran publicados en la página1.3 web y en dinámica Gerencial

Ilustración 2 https://hospitaldelsarare.gov.co/publicaciones/proteccion-de-datos.html

Tales documentos como:

1_ Plan de Privacidad y Seguridad de la Información
2_ Plan de Tratamiento de Riesgo y Privacidad de la Información
3_ Plan Estratégico de las Tecnologías de la Información -PETI
4_ Plan de Mantenimiento de Servicios Tecnológicos
5_ Plan de Contingencia Gestión de la Información y la Comunicación
6_Instructivos de manejo de módulos de dinámica gerencial

Para algunos de estos documentos se necesitan actualización.

1.2 Plan de acción

La ESE cuenta con Resolución No 016 del 28 de enero del 2026 por el cual se aprueban los planes de acción para la vigencia 2026, allí se incluye el plan de acción del Proceso Gestión integral de la información donde está incluido actividades del subproceso Gestión de tecnologías y sistemas de información.

Se evidencia plan de acción publicado en la https://hospitaldelsarare.gov.co/images/TRANSPARENCIAYACCESOALAINFORMACION/PLANES-DE-ACCION-DE-LOS-PROCESOS-2026.pdf

Última actualización: 30 Enero 2026

PLAN DE ACCIÓN

VIGENCIA 2026

- PLAN DE ACCIÓN VIGENCIA 2026
- RESOLUCIÓN N° 026 APROBACIÓN PLANES DE ACCIÓN 2026

Ilustración 3 Plan de Acción Publicado página web

1.3 Riesgos

Se cuenta documentado Plan de tratamiento de Riesgos de Seguridad y Privacidad de la información la cual se encuentra publicada en la intranet \\192.168.1.4\comites institucionales\24_COMITE DE ADMINISTRACIÓN RIESGO\1_MATRIZ DE RIESGOS\2025

HOSPITAL DEL SARARE

DIR-01-F07

REVISIÓN No. 2

Evolucionamos pensando en usted

Proceso:	SISTEMA DE RIESGOS Y PROGRAMA DE TRANSPARENCIA Y ETICA EMPRESARIAL
Objetivo:	
Alcance:	

	IDENTIFICACIÓN DEL RIESGO								ANÁLISIS DEL RIESGO INHERENTE								EVALUACIÓN DEL RIESGO - VALORACIÓN DE CTES									
																		ATRIBUTOS						
	TIPO DE RIESGO	ACTIVOS DE LA INFORMACIÓN	DESCRIPCIÓN Y VIGENCIA EVIDENCIA	CAUSA INMEDIATA	CAUSA RAIZ	RIESGO DE CORRUPCIÓN	CLASIFICACIÓN RIESGO	ANÁLISIS DE LA CONTEXTUALIZACIÓN	PROBABILIDAD INHERENTE	%	CLASIFICACIÓN	CRITERIOS DE IMPACTO	Observación de criterio	IMPACTO INHERENTE	%	ZONA DE RIESGO INHERENTE	NO. CONTROL	DESCRIPCIÓN DEL CONTROL	Tipo	Probabilidad	Afectación	Documentación	Frecuencia	Evidencia
1	Seguridad_de_la_Información	SEGURIDAD DIGITAL	1.Fallas tecnicas en medios físicos y virtuales de los servicios tecnológicos	Obsolescencia y brechas de seguridad por uso de sesionamiento	Falta de Mantenimientos	Perdida de Cofidencilidad, integridad y/o disponibilidad de la	Fallas Tecnologicas	La entidad que conlleva el riesgo se ejecuta de 3 a 24 veces	Baja	40%	Afectación_Económica_o_presupuestal	Entre 10 y 50 SMLMV	Entre 10 y 50 SMLMV	Menor	40%	Moderado	1	Control de acceso	Preventivo	Probabilidad	Manual	40%	Documentado	Aleatoria	Con Registro
3	Seguridad_de_la_Información	SEGURIDAD DIGITAL	Arquitectura de Red Insegura	Perdida de conectividad	Falta de reingeniera de la Red de Datos y migracion a IPV6	La infraestura de la red de datos no cumple con los protocolos de la norma	Fallas Tecnologicas	La entidad que conlleva el riesgo se ejecuta mínimo 500	Alta	80%	Pérdida_Reputacional	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	Moderado	60%	Alto	1	Seguridad de redes	Preventivo	Probabilidad	Manual	40 %	Documentado	Continua	Con Registro
2	Seguridad_de_la_Información	SEGURIDAD DE LA INFORMACION	1.Ausencia o insuficiencia de pruebas de software 2.Despegue y uso	Insuficiente oferta de capacitaciones y formación continua	Falta de aplicación de pruebas de escritorio al sofware	Perdida de Cofidencilidad, integridad y/o disponibilidad de la	Fallas Tecnologicas	La entidad que conlleva el riesgo se ejecuta de 2 a 24 veces	Baja	40%	Pérdida_Reputacional	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	Moderado	60%	Moderado	1	Control de acceso	Preventivo	Probabilidad	Automático	60%	Documentado	Continua	Con Registro
4	Seguridad_de_la_Información	SEGURIDAD DE LA INFORMACION	Ataque externo a los sistemas de información y/o falta de mantenimiento a	Perdida de Cofidencilidad, integridad y/o disponibilidad de la información	La ingeniería social.	Perdida de Cofidencilidad, integridad y/o disponibilidad de la	Usuarios, productos y practicas , organizacionales	La entidad que conlleva el riesgo se ejecuta como	Muy Baja	20%	Afectación_Económica_o_presupuestal	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	Moderado	60%	Moderado	1	Restriccion de acceso a la informacion.	Preventivo	Probabilidad	Manual	40 %	Documentado	Continua	Con Registro
5	Seguridad_de_la_Información	SEGURIDAD DE LA INFORMACION	1.Ausencia de Personal 2.Formacion Insuficiente sobre seguridad	Falta de recursos o ausencia de implementación adecuada de los	Falta de personal	Perdida de Cofidencilidad, integridad y/o disponibilidad de la	Usuarios, productos y practicas , organizacionales	La entidad que conlleva el riesgo se ejecuta como	Muy Baja	20%	Afectación_Económica_o_presupuestal	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos	Moderado	60%	Moderado	1	concienca de seguridad de la informacion, educación y formación	Preventivo	Probabilidad	Manual	40 %	Documentado	Continua	Con Registro

Ilustración 4 Matriz de riesgos institucional

Se evidencia información documentada publicada en la página web institucional. https://hospitaldelsarare.gov.co/images/publicaciones/Planeacion/PLANEACION/SIS-01-R04-Plan-de-Tratamiento-de-Riesgos-de-Seguridad-y-Privacidad-de-la-Informacin-.pdf documento formulado en la vigencia 2021, requiere revisión para su respectiva actualización.

No se evidencia seguimiento a las actividades planeadas para la prevención de riesgos.

Ilustración 5 https://hospitaldelsarare.gov.co/13-planeacion/520-planeacion-20.html

1.4 Indicadores

En la matriz de riesgos definió indicadores, a los cuales amerita realizar su registro, seguimiento y verificación.

1.5 Sistemas de información

Se realiza un software llamado Service Manager HS donde se evidencia el historial de mantenimiento de los equipos de computas, las hojas de vida y demás información necesaria de los equipos, así mismo se tiene Dinámica Gerencial.

1.6 Recurso humano

Se cuenta con Ingeniera de Sistemas de la institución, programador de apoyo, y el equipo operativo de plan de mantenimiento de equipos informáticos. Consideran fundamental contar de manera permanente con un perfil de Ingeniería de redes.

2. POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2.1 Información documentada

La entidad cuenta con información documentada del Plan de seguridad y privacidad de la información, documento publicado:

https://hospitaldelsarare.gov.co/images/publicaciones/Planeacion/PLANEACION/SIS-01-R03-Plan-de-privacidad-y-seguridad-de-la-informacin.pdf

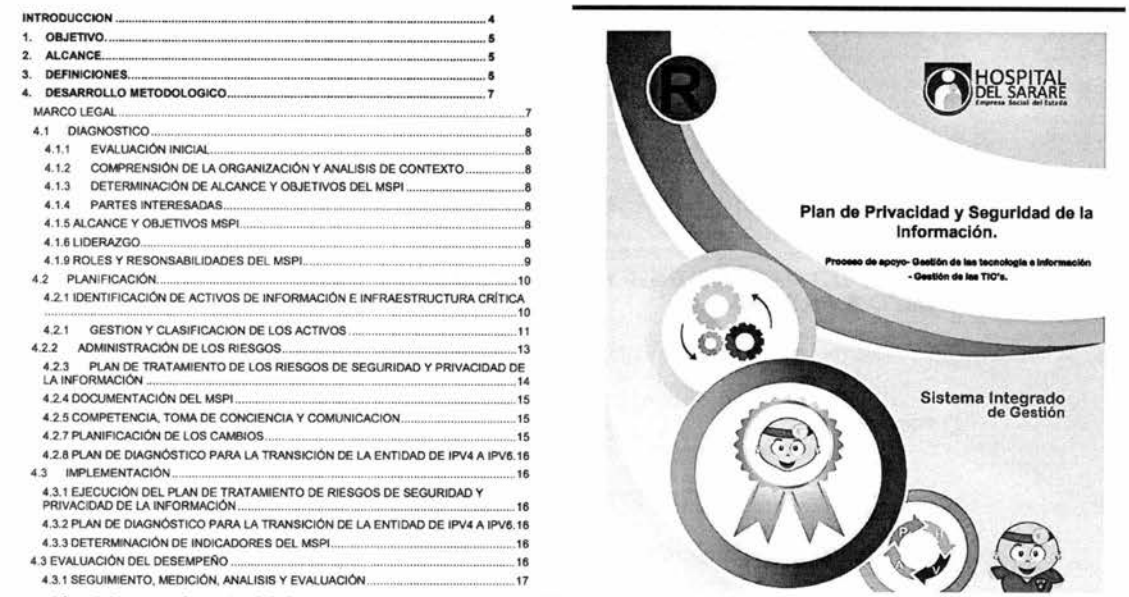


Ilustración 6 https://hospitaldelsarare.gov.co/images/publicaciones/Planeacion/PLANEACION/SIS-01-R03-Plan-de-privacidad-y-seguridad-de-la-informacin.pdf

Documento creado en el 2021, el cual amerita revisión para determinar el estado de actualización.

2.2 Diagnóstico

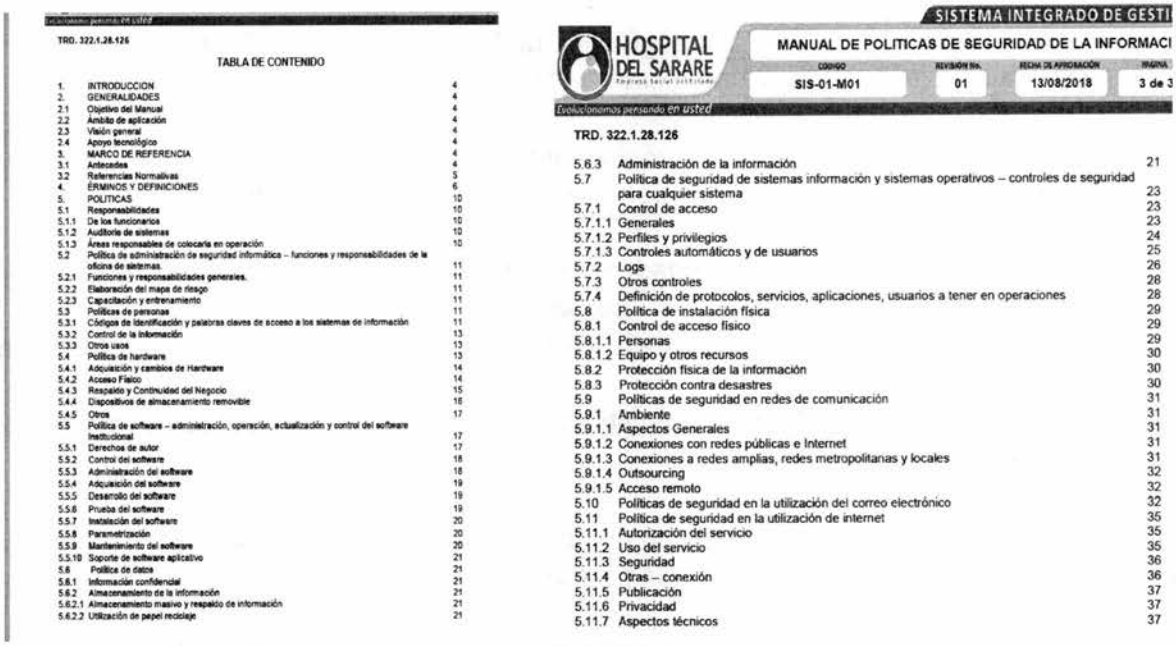
Para la vigencia 2025 en el contrato de prestación de servicios para la administración de red de datos de la ESE el ingeniero entrega los planos y el diagnóstico de la ipV6, lo cual se realizo avances en la Sede UNAP, la nueva urgencia, consulta externa y cirugía, así mismo hace falta terminar los demás servicios de la Sede principal, Sede C y sede Incora.

2.3 Política

La ESE cuenta con Resolución No 065 del 15 de marzo del 2021 por la cual se adopta la política de seguridad digital, dicho acto administrativo se encuentra publicado https://hospitaldelsarare.gov.co/images/publicaciones/politicas/RESOLUCION-N-065-POLITICA-SEGURIDAD-DIGITAL.pdf

En el acto administrativo en su artículo 6. Implementación menciona que todas las acciones definidas en la presente política se implementarán a través del Manual de políticas de seguridad de la información.

La ESE cuenta con información documentada SIS-014-M01 MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN el cual está publicado https://hospitaldelsarare.gov.co/publicaciones/proteccion-de-datos/politicas-de-seguridad-de-la-informacion.html



TRD. 322.1.28.126

TABLA DE CONTENIDO

SISTEMA INTEGRADO DE GESTI
HOSPITAL DEL SARARE
MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACI
CODIGO SIS-01-M01 | REVISIÓN No. 01 | FECHA DE APROBACIÓN 13/08/2018 | PAGINA 3 de 3
Evolucionamos pensando en usted

TRD. 322.1.28.126

Ilustración 7 https://hospitaldelsarare.gov.co/images/publicaciones/Planeacion/PLANEACION/SIS-01-R03-Plan-de-privacidad-y-seguridad-de-la-informacin.pdf

Documento creado en el 2021, el cual amerita revisión para determinar el estado de actualización.

2.3.1 Seguimiento a la Política Furag

La entidad cuenta con actas de comité de gestión y desempeño, se verificaron las correspondientes a la vigencia 2025 en la cual se realizó asignación de referentes para cada política MIPG, revisión de resultados FURAG. Pero no se evidenció tema específico a la política de seguridad y privacidad de la información.

2.4 Roles y responsabilidades

En el Manual de Políticas de seguridad y privacidad de la información en numeral 5.2. Política de administración de seguridad informática – funciones y responsabilidades de la oficina de sistemas 5.2.1. Funciones y responsabilidades presenta las siguientes funciones:

La oficina de sistemas es la responsable de:

1. Definir, implementar, controlar y mantener las políticas, normas, estándares, procedimiento, funciones y responsabilidades necesarias para preservar y proteger la confidencialidad, disponibilidad e integridad de la información del hospital, en donde esta resida (aplicaciones, bases de datos, sistemas operativos, redes, backup y otros medios).

2. Propender por alinear las estrategias de seguridad informática con planes estratégicos y de operación del hospital

3. Autorizar las excepciones a las políticas de seguridad, de las cuales se debe dejar constancia de los riesgos que en forma consciente se están asumiendo y el periodo de vigencia de la excepción.

4. Igualmente, es la encargada de definir la "Arquitectura de seguridad" para el hospital y facilitar la incorporación de prácticas de seguridad de la información en todas las dependencias.

5. Establecer e implementar un plan de seguridad informática que permita controlar el entorno lógico y físico de la "Información estratégica del hospital", teniendo en cuenta los criterios de confidencialidad, integridad, auditabilidad, disponibilidad, autenticidad y no repudio de la información.

6. Participar activamente en los proyectos informativos del hospital para proveerlos de la seguridad informática adecuadas.

7. Contar con mecanismo de monitoreo con el fin de detectar oportunamente procedimiento inseguro para los sistemas operacionales, aplicativos, datos y redes.

8. Implementar procedimientos que permitan verificar que la información enviada esté libre de software malicioso.

9. Monitorear los sistemas de seguridad de la información y reportar periódicamente su efectividad.

10. Promulgar la cultura de "seguridad informática" a todos los usuarios a través de informativos, videos, cartillas, entre otros.

11. Proponer por que el hospital cuente con ambientes indispensables de desarrollo, prueba y producción en sus ambientes de misión crítica y prioritaria.

12. Velar porque los mantenimientos a los sistemas informáticos sean autorizados, probados e implementados de acuerdo con los requerimientos de los usuarios y que no comprometan la seguridad informática del hospital. Además, que los sistemas de información queden correctamente documentados y se dé la capacitación necesaria a los usuarios finales.

13. Custodiar las llaves informáticas del hospital y velar porque las generaciones de las mismas sean realizadas de acuerdo con el procedimiento establecido (mínimo en dos (2) partes independientes cada una de no menos de ocho (8) caracteres). Los custodios del hospital son en su orden, oficina de sistemas y auditoria de sistemas.

14. Efectuar pruebas periódicas de penetración a los sistemas de redes y computación del hospital.

En el documento SIS-01-R03-Plan-de-privacidad-y-seguridad-de-la-información numeral 4.1.9 ROLES Y RESPONSABILIDADES DEL MSPI.

4.1.9 ROLES Y RESONSABILIDADES DEL MSPI

Definir los roles y responsabilidades necesarios para la implementación, administración, operación, mantenimiento y mejora del Modelo de gestión seguridad y privacidad de la información MSPI los cuales se articularán de acuerdo a la estructura organizacional del Hospital el Sarare E.S.E y el modelo de operación por procesos, áreas o dependencias y comité institucional de gestión y desempeño. Estos roles y responsabilidades deberán ser integrados en la **Matriz de responsabilidad y autoridad del Sistemas Integrados de Gestión SGI - SGI-00-F09** los cuales deben ser adoptados, monitoreado su desempeño, reporte y seguimiento mediante el comité institucional de gestión y desempeño de la institución. Garantizar su socialización a todos los colaboradores de la institución.

Establecer el **rol del Oficial de seguridad y privacidad de la información** y definir el equipo humano necesario para coordinar la implementación del MSPI mediante acto administrativo; el responsable designado deberá ser incluido como miembro del comité de gestión institucional de gestión de desempeño con voz y voto y en el comité de control interno tendrá voz.

Ilustración 8 Plan de privacidad y seguridad de la información

En dicho documento menciona la matriz de Responsabilidad y autoridad del Sistemas Integrados de Gestión SGI-00-F09. Se requiere verificar dicha matriz.

2.5 Socialización y capacitación de roles y responsabilidades

Se realiza capacitación al personal nuevo que ingresa a la institución sobre el funcionamiento de Dinámica Gerencial y temas de seguridad y privacidad de la información, así mismo se tienen las listas de asistencia de estas capacitaciones.

2.6 Identificación, valoración y clasificación de activos de información

Se elabora anualmente para informe de Contraloría General, (los computadores, impresoras, servidores Software, servidores), se realiza manera de inventario en la institución. Se requiere actualizar el publicado en la página web.

https://hospitaldelsarare.gov.co/publicaciones/proteccion-de-datos/inventario-de-activos-de-informacion.html

2.7 Controles acceso y seguridad de la información

La ESE cuenta con información documentada SIS-014-M01 MANUAL DE POLITICAS DE SEGURIDAD DE LA INFORMACIÓN el cual está publicado https://hospitaldelsarare.gov.co/publicaciones/proteccion-de-datos/politicas-de-seguridad-de-la-informacion.html

Se cuenta con monitoreo a través del antivirus y fortines, si se detecta el equipo técnico de sistemas ubica el equipo, se realiza revisión del estado de actualización de antivirus, si se encuentra identificado en el inventario de activos. Si tiene virus se debe formatear, restaurar, para incluirlo de nuevo a la red. Esto queda registrado en la hoja de vida de los equipos.

Se cuenta con mecanismos de seguridad para ingreso acorde a roles y perfiles de seguridad.

2.8 Minutas Contractuales o funciones

Se cuenta en las minutas contractuales las cláusulas en los contratos de termino fijo en la ***Clausura Tercera - ítem 26*** " Facilitar el acceso a la información del paciente sobre su proceso de atención, respetando la confidencialidad y los derechos de habeas data." y ***Vigésima Tercera - item 9*** "Violar el acuerdo de confidencialidad determinado por el Hospital del Sarare E.S.E. 10. No cumplir con sus obligaciones estipuladas en la cláusula séptima"

Para la Licencia del IQ, se dejará el mismo proveedor y se ampliará el contrato por dos (2) meses.

3. POLITICA DE GOBIERNO DIGITAL (Decreto 767 del 2022)

3.1 Autodiagnóstico

Se evidencia realización del autodiagnóstico de MIPG de la Política de Gobierno Digital

Calificación Total:

Ilustración 9 Calificación Total MIPG Política Gobierno digital

Calificacion de los Habilitadores de la Politica de Gobierno Digital

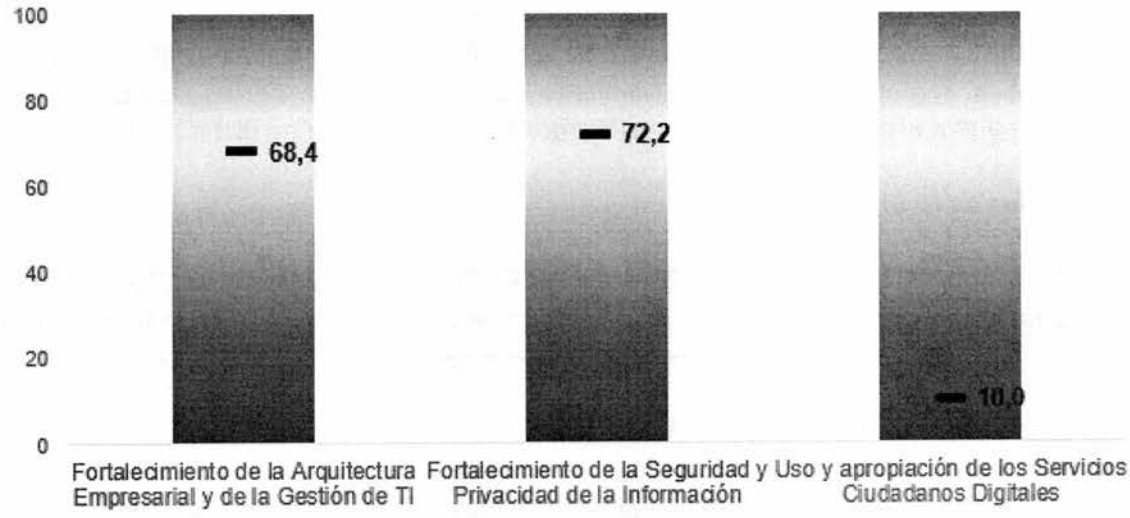


Ilustración 10 Calificación Habilitadores MIPG

Calificación de los Propositos de la Politica de Gobierno Digital

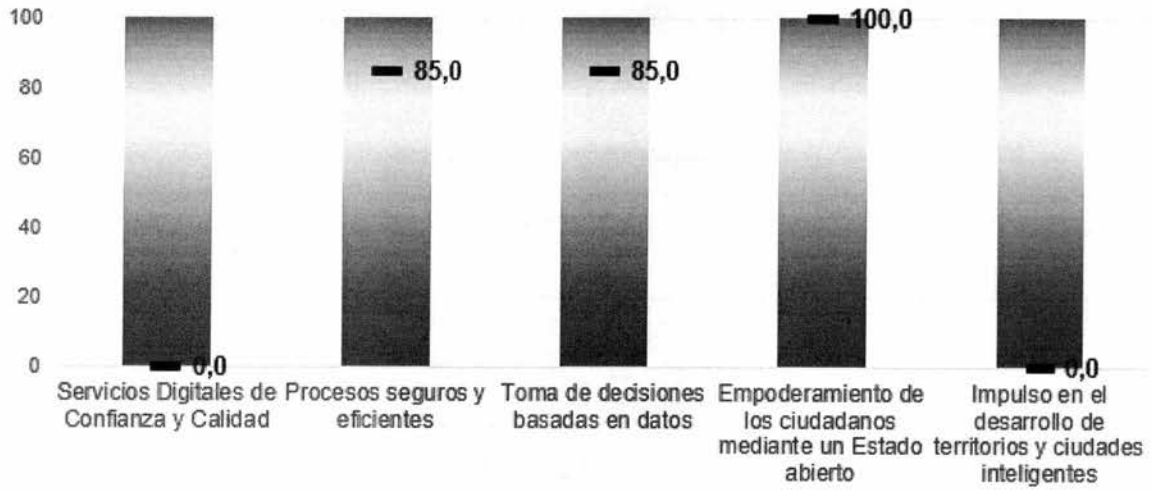


Ilustración 11 Calificación de los Propósitos MIPG

Por lo cual es necesario, realizar seguimiento al uso y apropiación de los servicios ciudadanos digitales, a los servicios digitales de confianza y calidad e impulso en el desarrollo de territorios y ciudades inteligentes.

3.2 Seguimiento a la política

Se evidenciaron actas de comité de gestión y desempeño donde se realizó asignación de referentes por cada política, seguimiento al diligenciamiento FURAG y revisión de los resultados, pero no se evidenció de manera específica la revisión del avance planes de acción de dicha política.

3.3 Tecnologías de la información

Contrato CD 456 de 2025 para la administración de Red de datos de la entidad, lo cual solo cuentas con los planos y el diagnóstico de la ipV6, esto se refleja en velocidad de la red, y conectividad, se realizaron avances en la Sede UNAP, Urgencia Nueva, Cirugía y Consulta Externa.

La ESE cuenta con nube para Dropbox.

Se cuenta con tablero de producción, indicadores hospitalarios, contratación venta de servicios, análisis de datos de caracterización. Para mantener acceso a este se requiere licencias.

3.4 Satisfacción del usuario

En la pagina web no se evidencio link o mecanismo para medición de la satisfacción en relación al acceso a medios digitales e información mediante la página web institucional.

3.5 Datos abiertos

El ESE cargo reporte en la página de DATOS ABIERTOS, se realiza opción publica de una matriz, pero se genera error y no se ha podido publicar ni aprobar.

3.6 Interacción con Grupos de Valor

La entidad cuenta con pagina web, la cual requiere actualización, página de Instagram, TikTok y YouTube.
https://www.facebook.com/share/1BLtqr1zKE/?mibextid=wwXIfr
https://www.instagram.com/hospitaldelsarare?igsh=MWNkd25sdjQ3YjN5Mg==
https://www.tiktok.com/@hospitaldelsarare? r=1& t=ZS-94lerWL2Qg1
https://www.youtube.com/@hospitaldelsararee.s.e.2910

4. PLAN ESTRATEGICO DE LAS TECNOLOGIAS DE LA INFORMACION (PETI)

Se evidencia Plan estratégico de tecnologías de la información (PETI) aprobado e inmerso en el plan de acción anual aprobado mediante Resolución No 030 del 30 de enero del 2024 la cual esta publicada en la pagina web institucional, en el articulo 4 aprueba los planes institucionales con vigencia del cuatrenio, periodo 2024-2027.

hospitaldelsarare.gov.co/images/publicaciones/Planeacion/2024/RESOLUCION-N-030---PLANES-2024.pdf

Se evidencia Plan estratégico de tecnologías de la información (PETI) aprobado e inmerso en el plan de acción anual aprobado mediante Resolución No 030 del 30 de enero del 2024 la cual esta publicada en la página web institucional, en el artículo 4 aprueba los planes institucionales con vigencia del cuatrenio, periodo 2024-2027.

Ilustración 12 PETI-ESE-HOSPITAL-DEL-SARARE-2024.pdf

Se realizo verificación del contenido y se identifico que falta incluir la información relacionada con el presupuesto o recursos para la ejecución del PETI.

Se evidencia la necesidad de estructurar soporte técnico, a través de un mecanismo de registro de ordenes de servicio, soporte técnico articulado con proveedor de dinámica gerencial, y ampliación de capacidad para dar cobertura a la necesidad de los usuarios de sistemas de información.

No se evidencio catálogo de los Sistemas de Tecnología de Información actualizado y se requiere realizar caracterización del sistema de información.

Actualmente no se encuentra ejecutando la capacidad de la infraestructura tecnológica.

4.1 Plan de mantenimiento preventivo y evolutivo

Se evidencia documentado un plan de mantenimiento preventivo y evolutivo (mejoramiento) sobre la infraestructura de tecnología de la información, este a través del documento Plan de contingencia el cual se encuentra publicado en la pagina web institucional PLAN DE CONTINGENCIA DE TIC'S

4.2 Disposición final de los residuos tecnológicos

Se evidencia documentado plan de gestión ambiental para cada vigencia, https://hospitaldelsarare.gov.co/images/publicaciones/Planeacion/PLAN_GESTION_AMBIENTAL/2_6_PLAN-GESTION-AMBIENTAL-PGIRASA.pdf , en el ítem 5.1.1.5 Identificación de condiciones para la segregación en la fuente de residuos menciona el Anexo -02 SIG-01-M01 Manual de Gestión de Residuos Sólidos Especiales y Convencionales, el cual establece la manera de entrega para la disposición final de los residuos tecnológicos.

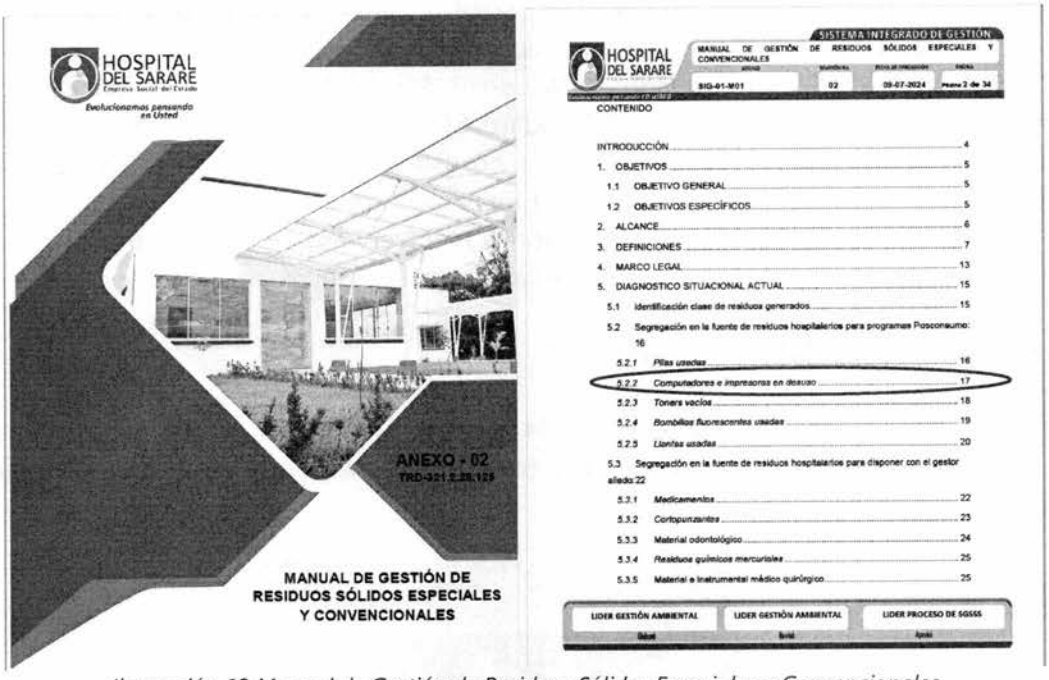


Ilustración 13 Manual de Gestión de Residuos Sólidos Especiales y Convencionales

Para entregar computadores e impresoras usados se debe tener en cuenta:

1. Deben clasificarse de acuerdo al tipo de máquina, de acuerdo a los siguientes tipos:
- Computadores de escritorio (incluyendo los periféricos)
- Computadores portátiles
- Impresoras

2.Empaca los aparatos electrónicos en desuso en cajas

3. Rotúlalos como "Residuos de Computadores y Periféricos" y el tipo de máquina.

4. Registra la cantidad y peso de los residuos

5. Acopiarlas en un lugar acorde en el cual se encuentren protegidas

6. Revise el listado de sistemas presentados y los datos de contacto para encontrar el sistema que corresponda al tipo y marca del computador o periférico.

Para la disposición final se realizaron actividades de Pos consumo para los días de 23 al 24 de septiembre de la vigencia 2025 en compañía de la Alcaldía Municipal del Municipio de Saravena y Empresa de Acueducto ECAAAS-EP

4.3 Transferencias derechas de autor

No se cuenta con clausuras en lo contratos sobre los derechos de autor para la vigencia 2025.

5. SOFTWARE

- Se tienen controladas las licencias del software:
- Sitemas operativos: Windows 11 y windows 10 -licencia perpetua.
- Ofimatica: Microsoft office 2016 licencia perpetua
- Antivirus/Seguridad: Endpoint Security - vigencia hasta agosto del 2026
- Sistema operativos para servidores: Windows Server 2022 Standard, Windows Server 2019 Standard, Windows Server 2008 R2 Standard, SQL 2014, SQIL 2022. - Licencia perpetua y OEM
- Algunos equipos tienen office 2022 que no esté licenciado por el office 2016 ya se quedó obsoleto y no responde ante archivos de Excel robustos.

Se realizan capacitaciones para las actualizaciones a través de divulgación, pero se requieren sean previas al desarrollo de la actualización y así evitar efectos negativos en los procesos.

6. INVENTARIO DE EQUIPOS DE COMPUTO

Se diseño una herramienta tecnológica llamada Service Manager HS donde encuentran las hojas de vida del equipo de cómputo, los mantenimientos correctivos, la vida útil del equipo, placa y demás información relevante para general un informe.

Ilustración 14 Software Service Manager HS

Se requiere mejorar dotación y orden del banco de trabajos para realizar las actividades de mantenimiento y reparación de equipos. No se evidencia stock de repuestos, partes, accesorios.

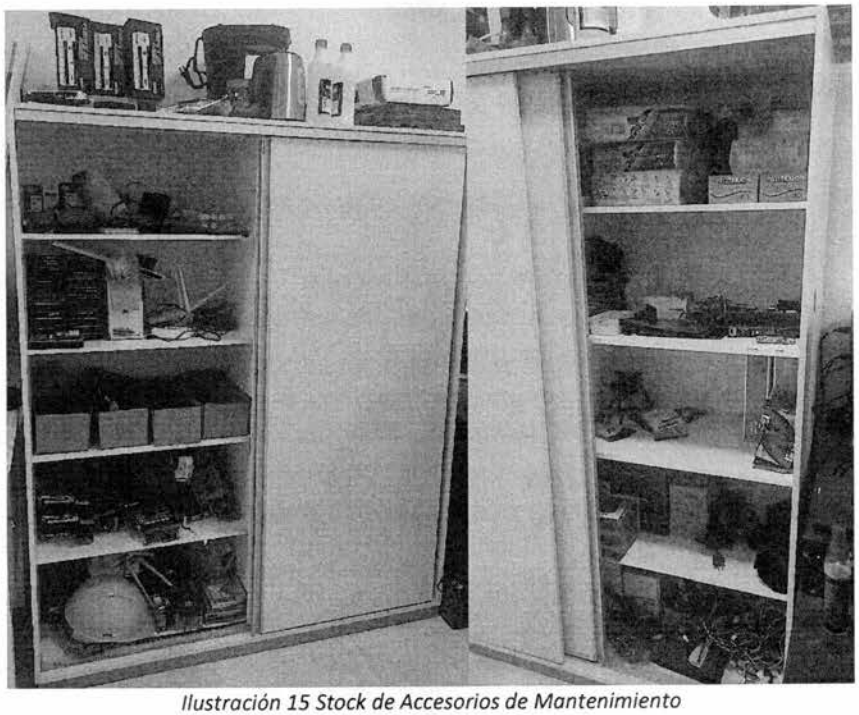


Ilustración 15 Stock de Accesorios de Mantenimiento

Se evidencia bodega de almacenamiento

Ilustración 16 Bodega de sistemas

Durante la vigencia 2025 la entidad dio de baja equipos de computo a través de su respectivo comité.

- Resoluciones No 051 del 25 de marzo de 2025
- Resolución No 106 del 26 de junio de 2025
- Resolución No 169 del 29 de septiembre de 2025
- Resolución No 272 del 23 de diciembre de 2025.

7. ACCESIBILIDAD A LA PAGINA WEB NTC 5854

7.1 Principios

PRINCIPIO	
Perceptible	En algunos videos se evidencian subtítulos, pero no evidencia audio descripción.
Operable	No se evidencian ayudas técnicas para usuarios con dificultades cognitivas, se evidencia la necesidad de estructurar que permita diferenciar y acceder fácilmente a los contenidos.
Comprensible	Se evidencian encabezados para cada sección, y chat de consultas, se considera el lenguaje claro para el lector. Se requiere reordenar para facilitar las rutas de ubicación en la web.
Robusto	La información publicada en la web corresponde a los mínimos normativos, se evidencia fiabilidad en la información, pero en unos apartados aun requiere actualización.

8. DATOS ABIERTOS Y PAGINA WEB (TRANSPARENCIA Y ACCESO A LA INFORMACION)

8.1 Principios

Aun no se cuenta con la aprobación y publicación de estos, informan problemas técnicos aún pendiente por resolver.

En la página web se encuentra publicado en la sección Transparencia y acceso a la información pública, Esquema de publicación de información.

9. MANUAL DE POLITICAS Y PROCEDIMIENTOS –HABEAS DATA

RESPECTO DEL CUMPLIMIENTO DE LOS PRINCIPIOS PREVISTOS EN LA LEY 1581 DE 2012	**VALORACION**
1. ¿Se está solicitando autorización al titular de la información? Lo anterior, de acuerdo con lo establecido en los artículos 9, 12 y 19 de la ley 1581 de 2012 y en los 2.2.2.25.2.2, 2.2.2.25.2.3 y 2.2.2.25.2.4 del decreto 1074 de 2015; que indica que el	NC

Tratamiento sólo puede ejercerse con el consentimiento previo, expreso e informado del titular; los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.	
2. ¿Se está informando la finalidad para la cual se recolectan los datos personales? Lo anterior, de acuerdo con lo establecido en el literal **B** del artículo 4, y los artículos 12 y 17 de la ley 1581 de 2012, y a los artículos 2.2.2.25.2.1, 2.2.2.25.3.1 y 2.2.2.25.3.2 del decreto 1074 de 2015; dónde indica que el Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al titular.	NC
3. ¿Se están conservando las copias de las autorizaciones obtenidas de los titulares? Lo anterior, en atención a los artículos 8 literal b y 9 de la ley 1581/2012, que expresan que se debe conservar copia de la autorización obtenida del titular para su posterior consulta en caso de que el titular lo requiera.	C
4. ¿Desde qué fuente se están obteniendo los datos (directamente del titular, fuentes de acceso público, contratos de recepción de bases de datos)? Lo anterior, de conformidad con lo establecido en los artículos 17 y 18 de la ley 1581 de 2012 y los artículos 2.2.2.25.2.5 y 2.2.2.25.3.7 del decreto 1074 de 2015; dónde se manifiesta la necesidad de tener conocimiento de la fuente de la cual se están recopilando y obteniendo los datos personales y la forma del tratamiento de estos.	C
5. ¿Usted firmó acuerdo de confidencialidad cuando se vinculó a laborar o posterior a la vinculación? Lo anterior, de acuerdo con lo establecido en el literal h del artículo 4, los artículos 17 y 18 de la ley 1581 de 2012 y de los artículos 2.2.2.25.5.2 y 2.2.2.25.6.1 del decreto 1074 de 2015; que refiere sobre la confidencialidad de la información de los datos personales que manejan los colaboradores.	NC
6. ¿Dónde se están guardando los documentos que tienen en físico? De acuerdo con lo establecido en el literal g del artículo 4, artículos 17 y 18 de la ley 1581 de 2012 y en los artículos 2.2.2.25.3.6, 2.2.2.25.5.2 y 2.2.2.25.6.1 del decreto 1074 de 2015; cuando refiere respecto de las medidas de seguridad de la información sujeta a tratamiento de datos por parte del responsable establecidas en la normatividad.	C
7. ¿Cómo se solicita la autorización cuando se recolectan datos de menores de edad? Lo anterior, de conformidad con los artículos 7 y 12 literal b de la Ley 1581/2012; los cuales, respecto de los datos de los menores de edad, indican que debe solicitarse autorización al representante legal del menor para el tratamiento de los datos.	NC
8. ¿Qué medidas de seguridad o qué procedimiento especial se aplica respecto de los datos de los menores de edad? Lo anterior, de acuerdo con lo establecido en los artículos 5, 6, 7 y 12 de la ley 1581 de 2012 y de los artículos 2.2.2.25.2.3, 2.2.2.25.2.9 y 2.2.2.25.3.4 del decreto 1074 de 2015; que indican respecto del procedimiento específico para el manejo de los datos personales de menores de edad.	NC
9. ¿Actualmente se informa que no es obligatorio autorizar el tratamiento de datos de los menores? Lo anterior, en atención a lo establecido por la Ley 1581 de 2012 en sus artículos 5, 6 y 12 literal b. Y lo preceptuado en el decreto reglamentario 1074 de 2015 en su Artículo 2.2.2.25.2.3. dónde se indica que se debe informar la "no-obligatoriedad" de autorizar el tratamiento de datos de los menores por tratarse de datos sensibles.	NC

10. ¿Qué medidas de seguridad se aplican a los datos sensibles? ¿Se les otorga un tratamiento especial? Lo anterior, de conformidad con lo establecido en los artículos 5 y 6 de la ley 1581 de 2012 y el artículo 2.2.2.25.2.3 del decreto 1074 de 2015; respecto del tratamiento de datos sensibles (aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, los datos relativos a la salud, a la vida sexual y los datos biométricos)	NC
11. ¿De qué manera se reciben y que tratamiento se les da a las PQRS de los titulares de la información? De conformidad con lo establecido en el literal e del artículo 4 y los artículos 8, 14 y 15 de la ley 1581 de 2012 y los artículos 2.2.2.25.2.6, 2.2.2.25.3.6, 2.2.2.25.4.2, 2.2.2.25.4.3 y 2.2.2.25.4.4 del decreto 1074 de 2015; dónde indica respecto al procedimiento adoptado para el manejo de las consultas, peticiones y en general el ejercicio de los derechos por parte de los titulares de la información respecto de sus datos.	NC
12. ¿En qué término (tiempo) se está dando respuesta a las peticiones hechas por los titulares en materia de datos personales? Lo anterior, de conformidad con los derechos que tienen los titulares, consagrados en el artículo 12 de la ley 1581 de 2012, además, la SIC indica el término de atención de las consultas (máximo de 10 días hábiles contados a partir de la fecha de recibo; con prórroga por máximo 5 días hábiles más, previa justificación al interesado y señalando la fecha en que se atenderá la petición.	NC
13. ¿Se están informando los derechos que tienen los titulares? Lo anterior de conformidad a lo establecido en el artículo 12 de la ley 1581 de 2012 y 2.2.2.25.2.3 del decreto 1074 de 2015, en lo referente a la obligatoriedad de informar a los titulares los derechos que tienen frente a su información personal.	NC
14. ¿Existe una Política de tratamiento de datos personales al interior de la entidad? Lo anterior, de conformidad con lo establecido en los artículos 2 y 4 de la ley 1581 de 2012 y en los artículos 2.2.2.25.3.1 y 2.2.2.25.3.2 del decreto 1074 de 2015, respecto de la existencia de una política para el tratamiento de datos personales que garantice la integridad de la información personal en las diferentes etapas del ciclo de vida del dato (recolección, circulación y disposición final).	C
15. ¿Conoce la existencia de un documento de seguridad dónde reposen las medidas para el tratamiento de la información? Lo anterior de conformidad con lo establecido en el artículo 4, literal (g) de la ley 1581 de 2012 y los artículos 2.2.2.25.6.1 del decreto 1074 de 2015; con relación al documento de seguridad de la información personal sé que debe tener al interior de la institución.	NC
16. ¿Conoce quién es el encargado de la seguridad de las claves, creación y eliminación de perfiles de acceso? Lo anterior de conformidad con lo establecido en el literal g del artículo 4 de la ley 1581 de 2012 y el artículo 2.2.2.25.3.7 del decreto 1074 de 2015; respecto del control de acceso, la seguridad de la información personal y otros.	C
17. ¿Manejan un registro de incidencias? Lo anterior, en atención a lo establecido en los artículos 4, 13, 17, 18 y 26 de la ley 1581 de 2012 y de los artículos 2.2.2.25.3.6, 2.2.2.25.5.1 y 2.2.2.25.5.2 del decreto 1074 de 2015; que indica respecto de las incidencias que ocurren con cada una de las bases de datos propiedad de la institución.	NC
18. ¿Se registra el ingreso y/o salida de los equipos que contienen información de carácter personal? De conformidad con lo establecido en los artículos 4 y 17 de la ley	NC

1581 de 2012 y los artículos 2.2.2.25.6.1 y 2.2.2.25.6.2 del decreto 1074 de 2015; respecto a los procedimientos relativos a la validación de datos de entrada y/o salida.	
19. ¿Se tiene una matriz de riesgos en materia de datos personales? Lo anterior de conformidad con lo establecido en la ley 1581/2012 en su artículo 4 literal (g) referente a la seguridad; en lo concerniente a la matriz de riesgo que se debe adoptar para identificar el ciclo de vida del dato y en cada una de las etapas los riesgos asociados a la misma.	NC
20. ¿Se comparten datos con terceras empresas o entidades? De acuerdo con lo establecido en el artículo 26 de la ley 1581 de 2012, en los artículos 2.2.2.25.2.1, 2.2.2.25.5.1 y 2.2.2.25.5.2 del decreto 1074 de 2015 y la circular 005 de 2017; respecto de la cesión de datos a terceras empresas y/o entidades.	NC
21. ¿Están manejando acuerdos de confidencialidad con clientes y proveedores? Lo anterior, de acuerdo con lo establecido en el literal h del artículo 4, los artículos 17 y 18 de la ley 1581 de 2012, dónde indica de la necesidad de la suscripción de contratos con acuerdos de confidencialidad para clientes y proveedores.	C
22. ¿Tienen un acta en la que se haya nombrado a un oficial de protección de datos? ¿Conoce quién es el oficial de protección de datos? De conformidad con lo establecido en la ley 1581 de 2012 en su artículo 3 literal (e) y el decreto 1074 de 2015 en su artículo 2.2.2.25.3.1; en lo que atañe a la tenencia de un Oficial de Protección de Datos y a la tenencia de la documentación referente al responsable del tratamiento de datos personales.	NC
23. ¿Se están realizando consultas remotas? ¿Varias áreas/departamentos tienen acceso a la misma información? Lo anterior, de acuerdo con lo previsto en el literal f del artículo 4 y el artículo 11 y 13 de la ley 1581 de 2012, y en el artículo 2.2.2.25.4.2 del decreto 1074 de 2015; respecto del acceso y circulación restringida, anotando que el tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones legales y aquellas establecidas en la Constitución.	C
24. ¿Los computadores y demás dispositivos con acceso a información de carácter personal tienen contraseña? Lo anterior, de conformidad con lo establecido en el literal g del artículo 4, artículos 17 y 18 de la ley 1581 de 2012 y en los artículos 2.2.2.25.3.6, 2.2.2.25.5.2 y 2.2.2.25.6.1 del decreto 1074 de 2015; cuando refiere respecto de las medidas de seguridad de la información sujeta a tratamiento de datos por parte del responsable establecidas en la normatividad.	NC
25. ¿Se están realizando auditorías en materia de seguridad de la información? Lo anterior para dar cumplimiento a lo establecido en el artículo 2.2.2.25.7.5 dónde se establecen los requisitos generales de las normas corporativas vinculantes, en su numeral octavo, sobre las auditorías de protección de datos y métodos para garantizar acciones correctivas para proteger los derechos del titular del dato.	NC
26. ¿Qué protocolo tienen establecido para la disposición final de la información (archivo, supresión, destrucción...)? ¿Se deja acta en estos procedimientos? Lo anterior, para cumplimiento de lo establecido en los artículos 2.2.2.25.2.8, 2.2.2.25.3.6	NC

y 2.2.2.25.4.3 del decreto 1074 de 2015; respecto de la disposición final de la información y el protocolo que se tiene para esta.	

Lo cual arroja el siguiente resultado:

CUMPLE	NO CUMPLE	CANTIDAD EVALUADA	Porcentaje cumplimiento.	Porcentaje Incumplimiento.
7	18	25	28%	72%

Porcentaje cumplimiento.	Porcentaje Incumplimiento.
28%	72%

9.1 Base de datos identificadas

En el Manual de Políticas y Procedimientos de Habeas Data en el ítem 12. base de datos y sistemas de información se encuentran los siguientes:

1_Base de datos de Pacientes - nivel alto de seguridad
2_Base de datos de empleados y contratistas- nivel alto de seguridad
3_Base de datos de proveedores - nivel básico de seguridad
4_Base de datos de donantes de sangre- nivel alto de seguridad

9.2 Documentadas medidas de seguridad para datos privados según el tipo de bases de datos

Se evidencia en el Manual de Políticas y Procedimientos de Habeas Data en la tabla Impedidas de seguridad para datos privados según el tipo de base de datos.

9.3 Acuerdo de Confidencialidad en el Vínculo Laboral

La entidad cuenta con los contratos a término fijo en la clausura Vigésimo Tercera- Terminación Unilateral. - Ítem 9 y clausula Trigésimo Primera- Confidencialidad
Contrato de prestación de Servicio en la cláusula sexta- Obligaciones del contratista - Ítem 1 Eje administrativo y cuidado de recursos (critico).

9.4 Autorización de datos de menores de edad

Se cuenta con formato SIS-01-F10 de Autorización para uso de Imagen de Menores de Edad.

9.5 Política de Tratamiento de Datos Personales

Se cuenta con Política de Tratamiento de Datos Aprobada y publicada en la página web de la entidad

https://hospitaldelsarare.gov.co/images/publicaciones/politicas/2025/politicadettodedatos/Actualizacion-Politica-Tratamiento-de-Datos.PDF

9.6 Oficial de Protección de Datos

Para la protección de datos se deja nombrado oficial a la ingeniera Yanet Moreno líder del sistema de información encargada de desarrollar, coordinador, controlar y verificar el cumplimiento de seguridad recogidas en el Manual de Habeas Data SIS-01-M02, Capitulo I, Políticas y Seguridad de Procedimientos.

10. RECOMENDACIONES

ASPECTOS GENERALES

Información documentada

La información documentada es la evidenciada en la publicación de la página web institucional, se requiere su debida actualización, así como continuar documentando aspectos del manejo a dinámica gerencial.

Plan de acción

No se evidenció seguimiento a las actividades planeadas, se requiere su adecuado seguimiento tanto por el líder del proceso como del subproceso.

Riesgo

La entidad ha avanzado en documentar los riesgos acordes a la Política institucional aprobada, pero no se evidenció su respetivo seguimiento, por lo cual se requiere para un oportuno control realizar el seguimiento periódico a estos, así como al cumplimiento de las actividades propuestas para cada riesgo.

Indicadores

Se evidenciaron unos indicadores documentados en la matriz de riesgos, pero se requiere que se realice su medición y seguimiento.

Sistema de información

Se recomienda para el funcionamiento del subproceso, y las actividades de soporte técnico de la entidad, crear herramientas digitales que permita un registro de las solicitudes de soporte técnico, así como la trazabilidad del servicio prestado, en el que evidencié número de órdenes de trabajo.

POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Se evidenció información documentada, pero se requiere en cumplimiento del MIPG realizar el autodiagnóstico de la Política de seguridad y privacidad de la información.

Se requiere en el marco del comité de gestión y desempeño realizar:
Socializar el resultado del autodiagnóstico MIPG.
Generar un plan de acción de la política con su respectivo seguimiento.
Capacitar en el tema de roles y responsabilidades de seguridad y privacidad de la información.
Identificación, valoración y clasificación de activos de información.
Se requiere actualizar la información publicada en la página web, activos de información.

Controles acceso y seguridad de la información
Se recomienda evaluar las medidas de seguridad y de infraestructura de los espacios donde se almacenan los servidores, evaluar riesgos de humedad, goteras, perdida, daños, robo.

POLTICA DE GOBIERNO DIGITAL
Se requiere generar un plan de acción y su respectivo seguimiento acorde al resultado arrojado del autodiagnóstico de MIPG de la Política de Gobierno Digital.
Socializar el resultado del autodiagnóstico MIPG.
Capacitar en el tema de roles y responsabilidades de seguridad y privacidad de la información.

Tecnologías de la información:
Se espera que sea culminado la red de datos de la entidad y sea entregado los planos de la infraestructura tecnológica.

Satisfacción del usuario:
Se requiere generar una herramienta digital en la página web institucional donde el usuario registre el nivel de satisfacción respecto a la calidad, utilidad, facilidad de acceso a la información publicada.

Datos abiertos
La entidad continua con estado de incumplimiento, por lo cual se requiere acceder a los soportes técnicos brindados por Ministerio de las TICS donde en cumplimiento de la Resolución 1519 de 2020 y del V Plan de Acción de Gobierno Abierto, MinTIC lanza la Hoja de Ruta Nacional de Datos Abiertos Estratégicos, que prioriza datos críticos para su disponibilidad y actualización. También se publican 25 Hojas de Ruta Sectoriales, alineadas con el PNID, para fortalecer la gestión y apertura de datos en sectores clave.

PLAN ESTRATEGICO DE LAS TECNOLOGIAS DE LA INFORMACION (PETI)
Se recomienda estructurar el soporte técnico, a través de un mecanismo de registro de órdenes de servicio, soporte técnico articulado con proveedor de dinámica gerencial, y ampliación de capacidad para dar cobertura a la necesidad de los usuarios de sistemas de información.
Adicionalmente se requiere documentar el catálogo de los Sistemas de Tecnología de Información actualizado y se requiere realizar caracterización del sistema de información.

SOFTWARE

Se requiere de manera prioritaria realizar cotización, asignación presupuestal y compra de licencias de software para dar cobertura al 100% de equipos de cómputo de la entidad.

INVENTARIO DE EQUIPOS DE COMPUTO

Para dar cumplimiento al plan de mantenimiento hospitalario y que este le dé cobertura al 100% de activos de información se requiere de manera prioritaria mantener un stock de elementos y accesorios para los mantenimientos correctivos de los equipos.

ACCESIBILIDAD PAGINA WEB NTC 5854

Se realizó verificación de los principios perceptible, operable, comprensible, robusto para lo cual se identifica la necesidad de documentar los parámetros para los productos audiovisuales generado por la entidad y acorde a ellos los funcionarios o contratistas que genera contenidos los apliquen de manera unificada.

MANUAL DE POLITICAS Y PROCEDIMIENTOS – HABEAS DATA

Se requiere de manera prioritaria el cumplimiento de los tramites aplicables de los datos personales registrados en las bases de datos de la entidad lo que implica garantizar que la información se realice de acuerdo con la ley y los principios de protección de datos, garantizando la veracidad y seguridad de los datos, y permitir el acceso, actualización y rectificación de los mismo.

Así mismo, realizar el respectivo seguimiento de Habeas Data por parte de la oficial de cumplimiento periódicamente.

10. NO CONFORMIDADES Y/O HALLAZGOS/

10.1 No conformidades identificadas en la Auditoria interna

No.	Descripción	Requisito Normativo y/o de proceso
1	No cumplimiento de los principios; perceptible, operable, comprensible, robusto para lo cual requiere ajustes en estructura y algunos contenidos de la página web institucional	NTC 5854:2011

2	No publicación y aprobación de datos abiertos ante MINTIC.	Ley 1712 de 2014 sobre Transparencia y Acceso a la Información Pública Nacional, define los datos abiertos en el numeral sexto como "todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos".
3	No cumplimiento de los principios previstos del Manual de Políticas y Procedimientos – Habeas Data	Ley 1581 de 2012. Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.

11. CONCLUSIÓN GENERAL

La auditoría se ejecutó de acuerdo con lo previsto en el Plan de Auditoría y, a la vez, se cumplió con el objetivo y alcance programado gracias a la disposición de los colaboradores.

Se dejan las recomendaciones y hallazgos detectados en desarrollo del proceso de auditoria conforme los cuales forma parte integral del presente informe.

No habiendo controversias en el presente informe, queda en firme dentro del proceso de auditoría. Se requiere que el subproceso de Planeación efectué el levantamiento del plan de mejora y se suscriba e implementen las acciones que conlleven a contrarrestar los hallazgos y observaciones presentadas, en el formato institucional SGI-01-F01 PLAN MEJORAMIENTO.xlsx, el cual se encuentra en \\192.168.1.4\lideres-sig\3. PLANEACIÓN

Para las evidencias se encuentran en la ruta \\192.168.1.4\lideres-sig\53. CONTROL INTERNO\2026\26_AUDITORIAS INTERNAS\4_SISTEMAS DE INFORMACION.

Para constancia se firma Saravena, a los VEINTIDOS (22) días del mes de Abril del año 2026.

APROBACIÓN DEL INFORME DE AUDITORÍA		
Nombre Completo	**Cargo**	**Firma**
YENNY CAROLINA SUAREZ	Asesora Control Interno	
GERALDINE REAL LOZANO	Profesional Universitario Apoyo control Interno	
YANET MORENO VELASCO	Líder Gestión de las tecnologías y Sistemas de información	