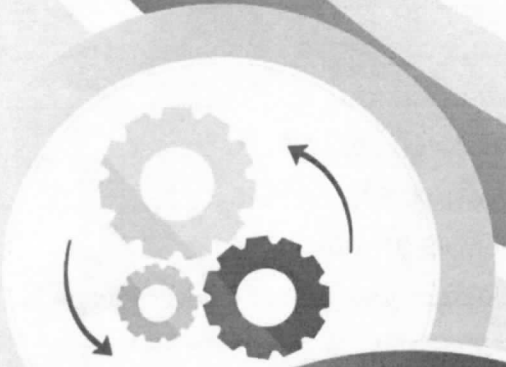
HOSPITAL DEL SARARE
Empresa Social del Estado

INFORME SEGUIMIENTO AL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (SIS-01-R03) Y PLAN DE TRATAMIENTO DE RIESGOS Y PRIVACIDAD DE LA INFORMACIÓN (SIS-01-R04)
II CUATRIMESTRE 2026

SEGUIMIENTO INSTITUCIONAL
CONTROL INTERNO



Sistema Integrado de Gestión







1. Tabla de Contenido

Tabla de contenido

1. Tabla de Contenido 2
2. Introducción 3
3. Objetivo del Informe 3
5. Metodología 4
6. Resultados del seguimiento 5
6.1 Políticas institucionales 5
6.1.1 Política Gobierno Digital 5
6.1.2 Política de Seguridad Digital 6
6.1.3 Política de Protección de Datos Personalesç 8
7. Planes institucionales 8
7.1 Plan estratégico de las tecnologías de la información PETI 2024-2027. 9
7.2 Plan de contingencia gestión de la información PLAN-00-S01 del 2018 9
7.3 Manual de políticas de seguridad de la información SIS-01-M01 del 2018. 10
7.4 Se evidencia SIS-01-R04 Plan de Tratamiento de Riesgos y seguridad y privacidad de la información del 30-11-2021 11
7.5 Plan de mantenimiento de servicios tecnológicos 11
8. Resultados FURAG 2025 12
9. MATRIZ DE RIEGOS 16
10. AUDITORIA INTERNA 17
11. Recomendaciones 18
12. Glosario de Términos 18
13. Control de Elaboración 18

Vigilado Supersalud

2. Introducción

Atendiendo uno de los propósitos del sistema de Control Interno, el cual está orientado a lograr la eficiencia, eficacia y transparencia en el ejercicio de las funciones de la entidad, la Oficina de Control Interno dando cumplimiento a la Ley 87 de 1993, Decreto 1068 de 26 de mayo de 2015, Decreto 371 de 2021 del 08 de abril del 2021 y Decreto 3036 de 2016 Art 16; presenta Informe de seguimiento al Plan de Seguridad y privacidad de la información y al plan de tratamiento de riesgos segundo cuatrimestre de la vigencia 2026 en lo relacionado a la Política de Seguridad Digital del MIPG.

3. Objetivo del Informe

Verificar la implementación del Plan de seguridad y privacidad de la información, así como el avance del seguimiento a los tratamientos de riesgos de seguridad de la información para la vigencia en el marco de los lineamientos de la política MIPG Seguridad digital con alcance al segundo cuatrimestre de la vigencia 2026

4. Línea estratégica y normativa

- Estrategia nacional de Seguridad digital de Colombia 2025-2027
- Resolución No 02277 del 03/06/2025 de Mintic por el cual se Actualiza el anexo 1 de la Resolución 500 del 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de las políticas de Gobierno digital.
- Decreto 767 de 2022 Por medio del cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Vigilado Supersalud

- Decreto 338 de 2022 Fortalece la gobernanza de la seguridad digital en Colombia.
- Decreto 620 de 2020 reglamenta parcialmente la Ley 1437 de 2011 y establece lineamientos para el uso y operación de los servicios ciudadanos digitales en Colombia.
- Resolución 500 del 2021 establece lineamientos y estándares para la estrategia de seguridad digital y adopta un modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital en Colombia.
- Documentos CONPES 3701 de 2011, 3854 de 2016 y 3995 de 2020, los cuales han guiado la política de seguridad digital del país en la última década.
- Decreto 1078 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
- Ley Estatutaria 1712 de 2014 por medio del cual se crea la Ley de Transparencia y del derecho de acceso a la información pública Nacional y se dictan otras disposiciones.
- Modelo Integrado de Planeación y Gestión (MIPG) Versión 6.1 del 2026.

5. Metodología

El seguimiento se realiza a través de las siguientes actividades:

- Verificación de la información documentada.
- Solicitud de información al subproceso de Gestión de las tecnologías y sistemas de información
- Revisión de los resultados de la ESE Hospital del Sarare en el FURAG vigencia anterior.
- Registros de información al subproceso de Gestión de las tecnologías y sistemas de información.
- Información publicada en la página web institucional
- Verificación de la metodología gestión por procesos

Vigilado Supersalud

6. Resultados del seguimiento

6.1 Políticas institucionales

6.1.1 Política Gobierno Digital

Revisión marco normativo según Decreto 0767 del 2022:

Artículo 2.2.9.1.1.2. Ámbito de aplicación. Los sujetos obligados a las disposiciones contenidas en el presente Capítulo serán las entidades que conforman la administración pública en los términos del artículo 39 de la Ley 489 de 1998 y los particulares que cumplen funciones administrativas.

PARÁGRAFO. La implementación de la Política de Gobierno Digital en las ramas legislativa y judicial, en los órganos de control, en los autónomos e independientes y demás organismos del Estado, se realizará bajo un esquema de coordinación y colaboración armónica en aplicación de los principios señalados en los artículos 113 y 209 de la Constitución Política.

Artículo 2.2.9.1.3.2. Responsable Institucional de la Política de Gobierno Digital. El representante legal de cada sujeto obligado, o quien haga sus veces, será el responsable de coordinar, adoptar, implementar y hacer seguimiento y verificación de la implementación de la Política de Gobierno Digital en su respectiva entidad.

Artículo 2.2.9.1.3.3. Responsable de orientar la implementación de la Política de Gobierno Digital. Los Comités Institucionales de Gestión y Desempeño de que trata el artículo 2.2.22.3.8 del Decreto 1083 de 2015, serán los responsables de orientar la implementación de la Política de Gobierno Digital, conforme a lo establecido en el Modelo Integrado de Planeación y Gestión.

Artículo 2.2.9.1.3.4. Responsable de liderar la implementación de la Política de Gobierno Digital. El Director, Jefe de Oficina o Coordinador de Tecnologías y Sistemas de la Información y las Comunicaciones, o quien haga sus veces, del respectivo sujeto obligado, tendrá la responsabilidad de liderar la implementación y la mejora continua de la Política de Gobierno Digital. Las demás áreas de la entidad serán corresponsables de la implementación de la Política de Gobierno Digital en los temas de su competencia.

De acuerdo a lo anterior se verificó y la ESE cuenta con: Adopción de la política Gobierno Digital a través de la Resolución No 073 del 2026.

https://hospitaldelsarare.gov.co/images/publicaciones/politicas/2026/Adopcion-Politica-de-Gobierno-Digital.pdf

Vigilado Supersalud

HOSPITAL DEL SARARE
Empresa Social del Estado
NIT. 800231215-1
Evolucionamos pensando en Usted

T.R.D 300.29 Resolución No. 073 Página 1 de 3

RESOLUCIÓN No. _073_ DEL _2026_
(27 marzo de 2026)

"Por medio de la cual se adopta e Implementa la Política de Gobierno Digital en el Hospital del Sarare ESE"

LA GERENTE DEL HOSPITAL DEL SARARE E.S.E

En ejercicio de las facultades legales otorgadas por el artículo 11, numeral 4, de la Ordenanza 03E de 1997, y especialmente las conferidas por el Decreto N° 505 del 22 de marzo de 2024 y el Acta de Posesión No. 051 del 1 de abril de 2024, emitidos por el Despacho del Señor Gobernador del Departamento de Arauca y,

CONSIDERANDO

CONCLUSIÓN:

Se evidencia correcto estado de actualización marco normativo Decreto 255 del 2022.

Se realizó verificación en la página web institucional y se evidencia la Adopción de la política de gobierno digital en el Hospital del Sarare E.S.E con fecha del 27/03/2026, para la implementación serán definidas a través del Plan Estratégico de Tecnologías de la Información (PETI), el Plan de Seguridad y Privacidad de la Información y el Plan de Acción de la Vigencia.

6.1.2 Política de Seguridad Digital

De acuerdo a lo anterior se verificó y la ESE cuenta con: Adopción de la política de seguridad digital a través de la Resolución No 065 del 2021.

https://hospitaldelsarare.gov.co/images/publicaciones/politicas/RESOLUCION-N-065-POLITICA-SEGURIDAD-DIGITAL.pdf

Vigilado Supersalud



HOSPITAL DEL SARARE
Empresa Social del Estado
NIT. 800231215-1
Evolucionamos pensando en usted

Vigilado Supersalud

Ministerio de la Protección Social
Departamento de Arauca

Resolución No 065 de 15 de Marzo de 2021.

"Por la cual se adopta la Política de Seguridad Digital"

EL GERENTE DE LA E.S.E HOSPITAL DEL SARARE en uso de sus facultades y

CONSIDERANDO:

Que el Hospital del Sarare Empresa Social del Estado, es una entidad púbica descentralizada del Orden Departamental, de conformidad con lo propuesto en el artículo 194 de la Ley 100 de 1993 y de la ordenanza Nro. 07E de 2008, que modifica los artículos 3 y 4 y el parágrafo 7 de la ordenanza 03E/97.

Que el artículo 2 de la constitución política de Colombia establece "que son fines esenciales del

Conclusión:

Una vez revisada la Resolución No. 065 del 15 de marzo de 2021, mediante la cual se adopta la Política de Seguridad Digital del Hospital del Sarare E.S.E., se evidencia que la entidad cuenta con una política formalmente adoptada que establece lineamientos generales orientados a minimizar los riesgos de seguridad de la información, proteger los activos tecnológicos y fortalecer la cultura de seguridad institucional. No obstante, por su fecha de expedición y frente a la evolución normativa y técnica presentada posteriormente, el documento requiere actualización integral. En particular, no evidencia la incorporación del marco vigente derivado de:

- CONPES 3995 de 2020: Política Nacional de Confianza y Seguridad Digital, actualiza el enfoque de seguridad digital en Colombia
- Resoluciones MinTIC 500 de 2021, 746 de 2022 y 2277 de 2025
- Decreto 338 de 2022, ni los desarrollos recientes relacionados con el Modelo de Seguridad y Privacidad de la Información —MSPI— y la interoperabilidad de la Historia Clínica Electrónica.

Además, se identifica la necesidad de fortalecer aspectos asociados con gobernanza, gestión de riesgos, protección de datos personales y datos sensibles de salud, gestión de incidentes, continuidad de la operación, seguridad de proveedores, controles tecnológicos, responsabilidades, indicadores y seguimiento.

En conclusión, se recomienda adelantar la revisión y actualización de la política y de los documentos que la desarrollan, asegurando su articulación con el MSPI vigente, la gestión integral de riesgos institucional y las disposiciones específicas aplicables al sector salud.

Vigilado Supersalud

6.1.3 Política de Protección de Datos Personalesç

Se realizó verificación en la página web institucional y se identifica acto administrativo No 148 del 2025.

HOSPITAL DEL SARARE
Empresa Social del Estado
NIT. 800231215-1
Evolucionamos pensando en Usted

Página 1 de 5

T.R.D 300.29 Resolución Nro. 148

RESOLUCIÓN No. 148 DE 2025
(22 de agosto de 2025)

"Por la cual se actualiza la Política de Tratamiento de Datos Personales del Hospital del Sarare ESE y se deroga la resolución No 03 A del 2019"

LA GERENTE DEL HOSPITAL DEL SARARE E.S.E

En ejercicio de las facultades legales otorgadas por el artículo 11, numeral 4, de la Ordenanza 03E de 1997, y especialmente las conferidas por el Decreto N° 505 del 22 de marzo de 2024 y el Acta de Posesión N° 051

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

CONCLUSIÓN:

Se evidencia correcto estado de actualización marco normativo Decreto 255 del 2022.

La ESE documentó en la vigencia 2025 el Manual de políticas y procedimientos Habeas data SIS-01-M02 el cual fue aprobado mediante el comité de Gestión y desempeño el 28 de mayo del 2025.

Se evidencia plan de mejoramiento en el marco de Auditoría interna de Riesgos.

7. Planes institucionales

- PGIRASA 2026

GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

- PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN
- PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
- PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES PETI
- PLAN DE MANTENIMIENTO DE SERVICIOS TECNOLÓGICOS
- PLAN DE CONTINGENCIA DE LA INFORMACIÓN

Vigilado Supersalud

7.1 Plan estratégico de las tecnologías de la información PETI 2024-2027.

Se realizó verificación en la página web institucional y se identificó documento Plan Estratégico de las tecnologías de la información PETI el cual en el alcance incluye... *aplica para todos los procesos que contribuyen al desarrollo de los recursos de tecnologías de información y dando cumplimiento con los lineamientos que establece la política de Gobierno Digital, siendo susceptible de ajustes a corto y mediano plazo para implementar en la Entidad.*

https://hospitaldelsarare.gov.co/images/publicaciones/Planeacion/TICS/PETI/PETI-ESE-HOSPITAL-DEL-SARARE-2024.pdf
Dicho documentó requiere actualización ya que está basado en el Decreto Nacional 2573 de 2014 el cual fue derogado por el Decreto 0767 del 2022 el cual Establece los lineamientos generales de la Política de Gobierno Digital y define la Seguridad y Privacidad de la Información como uno de sus habilitadores, exigiendo la implementación de lineamientos de seguridad y privacidad en los procesos, trámites, servicios, sistemas de información, infraestructura y activos de información, con el propósito de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

CONCLUSIÓN:
Se evidencia necesidad de realizar revisión del Plan Estratégico de Tecnologías de la Información - PETI del Hospital del Sarare E.S.E, alineándolo con la Política de Gobierno Digital establecida en el Decreto 767 de 2022 y con el Marco de Referencia de Arquitectura Empresarial y el Modelo de Gestión y Gobierno de TI - MGGTI vigentes.

Revisar el documento en lo relacionado a los sistemas relacionados como Windows Server 2003, Windows Server 2008, Windows 7, Windows 8, SQL Server 2008 R2 y Office 2010. Esto debe verificarse físicamente y contra inventario. Si dichos sistemas siguen actualmente en producción, no sería únicamente un problema de actualización documental del PETI, sino un riesgo tecnológico y de seguridad que requeriría tratamiento específico.

MinTIC actualmente dispone de la Guía de construcción PETI v. 3.0, dentro del MGGTI, que sería una referencia apropiada para realizar la actualización.

7.2 Plan de contingencia gestión de la información PLAN-00-S01 del 2018

Se evidencia PLAN-00-S01 Plan de contingencia gestión de la información el cual se encuentra publicado en la pagina web institucional.

https://www.hospitaldelsarare.gov.co/images/publicaciones/Planeacion/TICS/PLANDECONTINGENCIA/formato_202312_f22_cda_PlandeContingenciadelaInformacion.pdf

Vigilado Supersalud

CONCLUSIÓN:

Requiere actualización prioritaria. El documento conserva una estructura útil de contingencia y recuperación, pero corresponde a una versión de 2018 y presenta información tecnológica, riesgos, procedimientos y mecanismos de respaldo que deben ser ajustados a la infraestructura actual y al marco vigente de seguridad y privacidad de la información.

- PGINASA 2026

GESTIÓN DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

- PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACIÓN
- PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
- PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES PETI
- PLAN DE MANTENIMIENTO DE SERVICIOS TECNOLÓGICOS
- PLAN DE CONTINGENCIA DE LA INFORMACIÓN

7.3 Manual de políticas de seguridad de la información SIS-01-M01 del 2018.

Se evidencia Manual de políticas de seguridad de la información SIS-01-M01 el cual se encuentra publicado en la página web institucional

MANUALDEPOLITICASDESEGURIDADDELAINFORMACION.pdf

CONCLUSIÓN:

Es necesario revisar el estado de publicación en la pagina web, se encuentra en micrositio Planeación, pero en el menú de transparencia y acceso a la información no se visualiza, al parecer es información publicada desactualizada que falta por depurar en las publicaciones.

El Manual de Políticas de Seguridad de la Información del Hospital del Sarare E.S.E., aprobado en agosto de 2018, mantiene lineamientos básicos aplicables para la protección de la información; sin embargo, su marco normativo, técnico y metodológico no se encuentra plenamente armonizado con las disposiciones actualmente vigentes en materia de seguridad digital, Gobierno Digital y seguridad y privacidad de la información. Se recomienda realizar una actualización integral que contemple, entre otros referentes, el Decreto 767 de 2022, el Modelo de Seguridad y Privacidad de la Información – MSPI actualizado mediante la Resolución 2277 de 2025, y los lineamientos actuales para gestión de riesgos, incidentes, activos de información, proveedores, continuidad, servicios en la nube y nuevas tecnologías. La actualización deberá igualmente articularse con el PETI, la Política de Seguridad Digital, el Plan de Seguridad y Privacidad de la Información y el Plan de Tratamiento de Riesgos institucionales.

Vigilado Supersalud

7.4 Se evidencia SIS-01-R04 Plan de Tratamiento de Riesgos y seguridad y privacidad de la información del 30-**11-202**1

Se evidencia SIS-01-R04 Plan de Tratamiento de Riesgos y seguridad y privacidad de la información el cual se encuentra publicado en la página web institucional.

SIS-01-R04-Plan-de-Tratamiento-de-Riesgos-de-Seguridad-y-Privacidad-de-la-Informacin-.pdf

CONCLUSIÓN:

Es necesario revisar el estado de publicación en la página web, se encuentra en micrositio Planeación, pero en el menú de transparencia y acceso a la información no se visualiza, al parecer es información publicada desactualizada que falta por depurar en las publicaciones.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información presenta una estructura metodológica básica para la identificación, tratamiento, seguimiento y evaluación de riesgos; sin embargo, fue formulado para la vigencia 2022 y conserva referencias normativas, metodológicas y técnicas anteriores. Se recomienda actualizar el documento para la vigencia actual, armonizándolo con el MSPI vigente, la metodología actual de administración del riesgo, la política institucional de gestión integral del riesgo, el PETI, el Plan de Seguridad y Privacidad de la Información y demás instrumentos institucionales relacionados. Asimismo, se deberán actualizar los riesgos, activos de información, controles, responsables, cronogramas, indicadores, metas, tratamiento del riesgo residual, y mecanismos de seguimiento.

7.5 Plan de mantenimiento de servicios tecnológicos

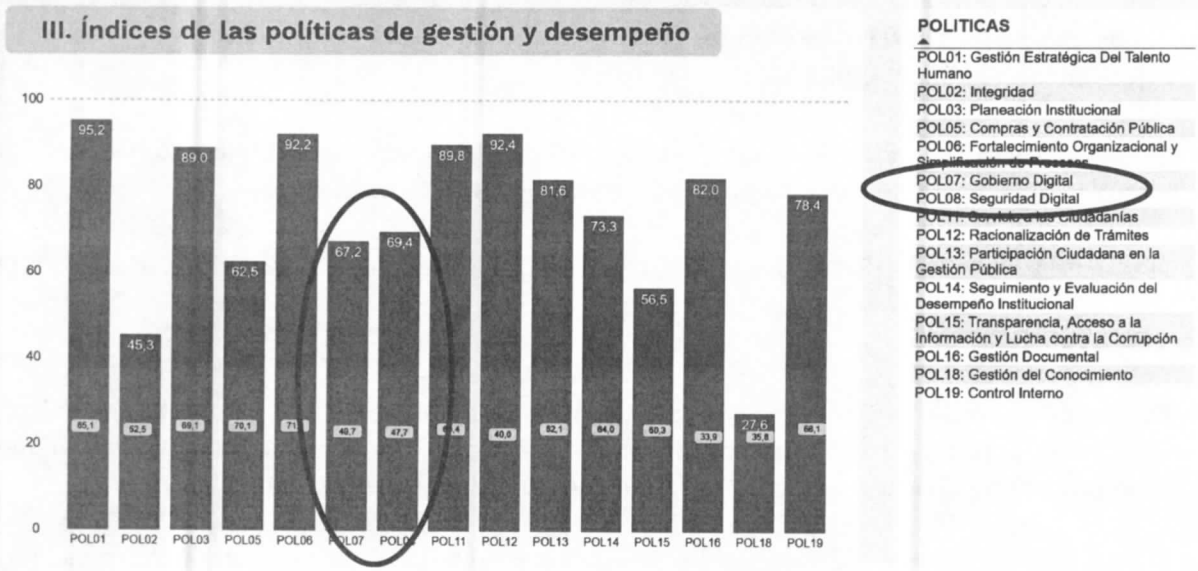
Se evidencia SIS-01-R05 Plan de Mantenimiento de servicios tecnológicos de la información el cual se encuentra publicado en la página web institucional.

https://hospitaldelsarare.gov.co/images/publicaciones/Planeacion/PLANEACION/SIS-01-R05-Plan-de-Mantenimiento-de-Servicios-Tecnologicos.pdf

Se recomienda actualizar el documento conforme a la infraestructura tecnológica actualmente disponible en la institución, articulando con el plan Institucional de mantenimiento hospitalario.

Vigilado Supersalud

8. Resultados FURAG 2025



RECOMENDACIONES:

Gobierno Digital

Recomendación
Incluir en el Plan de Acción Anual de la entidad proyectos con enfoque experimental para generar soluciones novedosas y creativas que hagan uso de TIC, con la participación de actores de la ciudadanía, sector privado, academia y sector público.
Elaborar un tablero de control con indicadores para hacer seguimiento a la implementación del Plan Estratégico de Tecnologías de la Información (PETI).
Implementar la hoja de ruta definida en el Plan Estratégico de Tecnologías de la Información (PETI).
Integrar el proceso de Arquitectura Empresarial al Sistema de Gestión de Calidad de la entidad.
Establecer indicadores de seguimiento a la ejecución de los ejercicios de Arquitectura Empresarial en la entidad.
Definir los roles necesarios para la implementación del proceso de Arquitectura Empresarial en la entidad.
Definir un repositorio para almacenar los ejercicios de Arquitectura Empresarial que realice la entidad.

Vigilado Supersalud

Desarrollar una hoja de ruta de Arquitectura Empresarial y hacer seguimiento a su implementación en la entidad.
Ejecutar el proceso de Arquitectura Empresarial en la entidad.
Integrar el proceso de gestión de proyectos con componentes de Tecnologías de la Información con el Sistema de Gestión de Calidad de la entidad.
Establecer los planes de comunicaciones para la gestión de cada proyecto con componentes de Tecnologías de la Información en la entidad.
Determinar el alcance de los proyectos con componentes de Tecnologías de la Información en la entidad, así como la priorización de actividades asociadas a cada uno.
Realizar seguimiento a través de indicadores de eficiencia y eficacia a la ejecución de proyectos con componentes de Tecnologías de la Información en la entidad.
Realizar análisis y tratamiento de riesgos de los proyectos con componentes de Tecnologías de la Información en la entidad.
Establecer una metodología para la gestión de proyectos con componentes de Tecnologías de la Información.
Documentar las lecciones aprendidas de los proyectos con componentes de Tecnologías de la Información implementados.
Definir un proceso de gestión y gobierno de Tecnologías de la Información, formalizado a través del Sistema Integrado de Gestión de Calidad de la entidad.
Hacer seguimiento a través de indicadores de eficiencia y eficacia a los procesos asociados a la gestión y gobierno de Tecnologías de la Información.
Desarrollar e implementar una estrategia de uso y apropiación de tecnologías actuales y emergentes (blockchain, inteligencia artificial, internet de las cosas, automatización robótica de procesos).
Establecer estrategias para consolidar el conocimiento y las lecciones aprendidas del área de Tecnologías de la Información.
Implementar en la entidad las 3 fases del modelo de adopción de IPv6: planeación, implementación y pruebas de funcionalidad.
Realizar el plan de diagnóstico, como parte de las actividades de la fase 1 del modelo de adopción de IPv6 en la entidad.
Realizar el plan de direccionamiento IPv6, como parte de las actividades de la fase 1 del modelo de adopción de IPv6 en la entidad.
Realizar el diseño detallado de red, como parte de las actividades de la fase 1 del modelo de adopción de IPv6 en la entidad.
Realizar el plan de contingencias de IPv6, como parte de las actividades de la fase 1 del modelo de adopción de IPv6 en la entidad.
Realizar el documento de activación de políticas de seguridad para IPv6 como parte de las actividades de la fase 2 y 3 del modelo de adopción de IPv6 en la entidad.

Vigilado Supersalud

Realizar el informe de pruebas piloto y de implementación de IPv6, como parte de las actividades de la fase 2 y 3 del modelo de adopción de IPv6 en la entidad.
Realizar el acta de cumplimiento a satisfacción sobre el funcionamiento e implementación de los elementos que fueron intervenidos con IPv6, como parte de las actividades de la fase 2 y 3 del modelo de adopción de IPv6 en la entidad.
Registrar a la entidad en la Tienda Virtual del Estado Colombiano (TVEC).
Capacitar a los servidores públicos de la entidad en temáticas de la Política de Gobierno Digital.
Capacitar a los contratistas de la entidad en temáticas de la Política de Gobierno Digital.
Capacitar a los grupos de valor e interés (ciudadanía, sector privado, sociedad civil, academia, otras entidades públicas) en temáticas de la Política de Gobierno Digital.
Formular, aprobar, implementar y actualizar la política de seguridad y privacidad de la información de la entidad, mediante un proceso de mejora continua.
Definir, aprobar, implementar y actualizar los procedimientos de seguridad y privacidad de la información, mediante un proceso de mejora continua.
Aprobar, clasificar y actualizar el inventario de activos de seguridad y privacidad de la información de la entidad, mediante un proceso de mejora continua.
Identificar, aprobar, implementar un proceso de valoración y actualizar los riesgos de seguridad y privacidad de la información de la entidad, mediante un proceso de mejora continua.
Definir indicadores para medir la eficiencia y eficacia del sistema de gestión de seguridad y privacidad de la información (MSPI) de la entidad, aprobarlos mediante el comité de gestión y desempeño institucional, implementarlos y actualizarlos mediante un proceso de mejora continua.
Utilizar datos externos a la entidad para apoyar la toma de decisiones relacionadas con su misionalidad.
Implementar la fase de 'intercambio' del ciclo de vida del dato en la entidad.
Implementar la técnica de 'análisis descriptivo' para el análisis de datos en la entidad. El uso de esta técnica permite describir una situación pasada o actual en la entidad.
Implementar la técnica de 'análisis de causalidad' para el análisis de datos de la entidad. El uso de esta técnica permite analizar como un conjunto de variables puede afectar el comportamiento de otra variable.
Implementar la técnica de 'análisis predictivo' para el análisis de datos de la entidad. El uso de esta técnica permite predecir las tendencias o posibles comportamientos futuros de una variable.
Implementar la técnica de 'análisis prescriptivo' para el análisis de datos de la entidad. El uso de esta técnica permite establecer cuál es la mejor acción para tomar bajo un contexto específico.
Elaborar un catálogo interno de datos maestros de la entidad.
Identificar cuáles de los datos maestros de la entidad son datos de referencia.
Generar y actualizar los conjuntos de datos abiertos propios de la entidad.

Vigilado Supersalud

Llevar a cabo actividades de innovación basadas en el enfoque experimental y en el uso de las TIC tales como el desarrollo de soluciones novedosas y creativas, y la identificación de los beneficiarios; la formulación y prueba de hipótesis; el desarrollo, validación y ensayo de prototipos y productos mínimos viables; o la participación en actividades externas a la entidad con enfoque experimental.
Llevar a cabo actividades de innovación pública digital a través de alianzas con otros actores, o de laboratorios propios de innovación, tales como la identificación de problemáticas y retos públicos; la generación de proyectos, iniciativas o metas compartidas de fortalecimiento institucional; la producción y generación de datos e información; investigaciones o desarrollos tecnológicos o de innovación; la gestión de recursos o sponsor; la obtención de apoyo técnico; la participación en redes de conocimiento o en comunidades de práctica; o la participación en conferencias o eventos de innovación.
Forjar alianzas con otros actores o laboratorios de innovación para experimentar en el desarrollo de soluciones a retos públicos a través del uso de las TIC, que le permitan a la entidad financiar los proyectos o iniciativas; aprovechar espacios que incentiven la innovación pública digital sin comprometer los recursos propios; fortalecer las capacidades de los servidores públicos; acceder a apoyo técnico para abordar los proyectos o iniciativas de la entidad; o identificar actores relevantes en el ecosistema de la innovación pública digital.
Utilizar tecnologías emergentes de la cuarta revolución industrial para desarrollar procesos de innovación pública digital en la entidad, tales como tecnologías de desintermediación, DLT (Distributed Ledger Technology) como cadena de bloques (Blockchain) o contratos inteligentes; análisis masivo de datos (Big data); Inteligencia Artificial (AI); Internet de las Cosas (IoT); robótica y similares; realidad aumentada o realidad virtual; automatización robótica de procesos; entre otras.
Implementar el servicio de interoperabilidad en la entidad a través de la plataforma X-ROAD para reducir los tiempos de respuesta de los trámites, reducir los costos de operación, entre otros.
Cumplir con los lineamientos establecidos en el Decreto 1263 de 2022 para ejecutar los proyectos de transformación digital (uso de infraestructura de datos; interoperabilidad entre los sistemas de información públicos; uso de mecanismos de digitalización y automatización de trámites, servicios y procesos y su vinculación al Portal Único del Estado Colombiano; uso de mecanismos de agregación de demanda; implementación, migración y uso de servicios de nube; uso de mecanismos exploratorios de regulación como Sandbox; uso de tecnologías emergentes tales como inteligencia artificial, internet de las cosas, big data o blockchain).
Disponer en línea los trámites de la entidad inscritos en el Sistema Único de Información de Trámites (SUIT).
Digitalizar los trámites inscritos por la entidad en el Sistema Único de Información de Trámites (SUIT).
Automatizar los trámites inscritos por la entidad en el Sistema Único de Información de Trámites (SUIT).
Vincular a X-ROAD todos los servicios de intercambio de información requeridos para la realización de trámites de la entidad.

Vigilado Supersalud

Seguridad Digital

Recomendación
Separar los equipos que realizan las copias de respaldo de la información, del software e imágenes de los sistemas de la red de servidores y computadores.
Almacenar las copias de respaldo en un lugar aislado, en un segmento diferente de red a la de servidores y equipos.
Realizar pruebas de respaldo a las copias de seguridad de la información de los aplicativos misionales, estratégicos, soporte y de mejora, de manera programada para asegurar la disponibilidad de los datos en caso de Ransomware, de manera coordinada con los responsables del proceso.
Contar con un Plan de Continuidad del Negocio -BCP-, que esté definido, documentado e implementado para los procesos críticos y misionales de la entidad.
Identificar y gestionar los posibles riesgos de seguridad digital (Ciberseguridad) de sus infraestructuras on premise.
Identificar y gestionar los posibles riesgos de seguridad digital (Ciberseguridad) en los servicios de Nube Pública/Privada que utiliza.
Verificar y asegurar que los proveedores y contratistas de la entidad cumplan con las políticas de ciberseguridad internas.
Establecer, documentar e implementar un procedimiento para la gestión de incidentes de seguridad digital (Ciberseguridad) que incluya la notificación a las autoridades pertinentes (CSIRT Gobierno / COLCERT).

9. MATRIZ DE RIEGOS

N° DE RIESGO	TIPO DE RIESGO	SISTEMA	PROCESO	SUBPROCESO	DESCRIPCIÓN DEL RIESGO	FRECUENCIA CON LA CUAL SE REALIZA LA ACTIVIDAD	PROBABILIDAD INHERENTE
48	Riesgos de Seguridad de la Información	Subsistema de administración del riesgo operativo	gestión_INTEGRAL_DE_LA_información	Gestión de las Tecnologías y Sistemas de Información	Posibilidad de perdida de confidencialidad, integridad y/o disponibilidad de la información por acceso no autorizado a la información de pacientes, empleados contratistas, proveedores, donantes de sangre a causa de Obsolescencia y brechas de seguridad por uso de versionamiento desactualizado del entorno de los diferentes sistemas de información. (gestión tecnologías e información) (Seguridad de la información)	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	Muy Baja
49	Riesgos de Seguridad Digital	Sistemas Integrados de Gestión	gestión_INTEGRAL_DE_LA_información	Gestión de las Tecnologías y Sistemas de Información	Posibilidad de perdida de disponibilidad por fallas en la conectividad a causa de Falta de reingeniera de la Red de Datos y migración a IPV6 (gestión tecnologías e información) (Seguridad de la información)	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	Media
50	Riesgos de Seguridad de la Información	Subsistema de administración del riesgo operativo	GESTION_INTEGRAL_DE_LA_INFORMACION	Gestión de las Tecnologías y Sistemas de Información	Posibilidad de perdida de disponibilidad de información a causa de no contar con servidores espejo o copias de seguridad sin condiciónes adecuadas de preservación (gestión tecnologías e información) (Seguridad de la información)	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	Alta

Ilustración 1 Matriz de Riesgos Institucional 2026

Vigilado Supersalud

Para el Segundo Cuatrimestre del año 2026, se gestionaron los riesgos establecidos en la Matriz de Riesgos de seguridad de la información, la cual hace parte del Mapa de Riesgos Institucional Versión 2, lo cual esta disponible para la consulta en la IP4 \\192.168.1.4\lideres-sig\11. GESTION DE RIESGO\2026\MAPA DE RIESGOS INTEGRAL.

Se relacionan los riesgos y sus controles:

Riesgo 1:
Posibilidad de pérdida de confidencialidad, integridad y/o disponibilidad de la información por acceso no autorizado a la información de pacientes, empleados contratistas, proveedores, donantes de sangre a causa de Obsolescencia y brechas de seguridad por uso de versionamiento desactualizado del entorno de los diferentes sistemas de información. (gestión tecnologías e información) (Seguridad de la información).

Control: Es responsable de que existan copias de seguridad de la intranet y la información cargada del usuario en el software de dinámica

Riego 2:
Posibilidad de pérdida de disponibilidad por fallas en la conectividad a causa de Falta de reingeniería de la Red de Datos y migración a IPV6 (gestión tecnologías e información) (Seguridad de la información)

Control: Realizar trabajo de migración de IPV4 a IPV6

Riesgo 3:
Posibilidad de pérdida de disponibilidad de información a causa de no contar con servidores espejo o copias de seguridad sin condiciones adecuadas de preservación (gestión tecnologías e información) (Seguridad de la información)

Control: Se realizan backup cada 12hrs

Masterización de Riesgos:
Durante el Segundo Cuatrimestre de 2026 la Oficina de Tecnologías de la información y las comunicaciones NO recibió alertas correspondientes a la posible materialización de riesgos de Seguridad de la información.

10. AUDITORIA INTERNA

Para el mes de abril de la vigencia 2026 se realizó Auditoria Interna la cual tiene un porcentaje del 60% de cumplimiento, se efectúa el levantamiento del plan de mejora y se suscriba e implementen

Vigilado Supersalud

las acciones que conllevan a contrarrestar los hallazgos y/o observaciones presentadas mediante la Auditoria.

11. Recomendaciones

✓ Realizar revisión del marco normativo vigente y aplicable a la entidad y basado en este realizar la actualización documental.
✓ La entidad cuenta con políticas institucionales, pero no se evidencia soportes o evidencia para verificar el estado de implementación de estas, por lo cual se recomienda en el plan de acción del subproceso incluir actividades de cada política para la vigencia y allí realizar su respectivo seguimiento.
✓ Revisar el estado de actualización de los planes, determinar su pertinencia ya que al parecer se identifica necesidad de depuración documental.
✓ Realizar depuración actualización de la información publicada en la página web institucional relacionada con la seguridad y privacidad de la información y riesgos en el ciclo PHVA.
✓ En el marco del comité de Gestión y desempeño realizar seguimiento a la política de gobierno digital y seguridad de la información.

12. Glosario de Términos

Se remite a los Términos y definiciones de seguridad de la información y seguridad digital de la Contaduría General de la Nación VS 15/11/2024.
https://www.contaduria.gov.co/documents/d/guest/40-terminos-y-definiciones-de-seguridad-de-la-informacion

13. Control de Elaboración

Revisó	Yenny Carolina Suarez Asesor Control Interno	
Realizó	Geraldine Real Lozano Profesional Univ. Apoyo Control Interno	

Vigilado Supersalud