Sanatorio de Agua de Dios
Empresa Social del Estado

RESOLUCIÓN No. 10.39.309 DE 2025

(Junio 12)

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información del Sanatorio de Agua de Dios E.S.E."

EL GERENTE DEL SANATORIO DE AGUA DE DIOS

EMPRESA SOCIAL DEL ESTADO

En uso de sus atribuciones legales y estatutarias en especial las conferidas por el articulo 20 en el Decreto 3040 de 1997, y demás normas concordantes.

CONSIDERANDO:

Que la información es uno de los activos más valiosos para la adecuada prestación de servicios de salud, la toma de decisiones y la gestión institucional del Sanatorio de Agua de Dios E.S.E.

Que, en cumplimiento del ordenamiento jurídico colombiano, incluyendo la Ley 1581 de 2012, la Ley 1712 de 2014, la Ley 594 de 2000, y demás normas que regulan la protección de datos personales, la transparencia, la gestión documental y la ciberseguridad, las entidades públicas deben establecer mecanismos para garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información;

Que el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) ha definido lineamientos y guías técnicas que orientan a las entidades públicas en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), con el fin de fortalecer la confianza digital y la protección de los datos;

Que se elaboró el documento titulado *"Política de Seguridad y Privacidad de la Información del Sanatorio de Agua de Dios E.S.E."*, el cual fue revisado y validado por las áreas competentes, y contiene los lineamientos estratégicos, roles, responsabilidades, controles y procedimientos necesarios para gestionar adecuadamente la información institucional;

Que la Alta Dirección ha manifestado su compromiso con la implementación del MSPI y la adopción de esta política como instrumento esencial del sistema de gestión institucional.

Sanatorio de Agua de Dios
Empresa Social del Estado

RESOLUCIÓN No. 10.39.309 DE 2025

(Junio 12)

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información del Sanatorio de Agua de Dios E.S.E."

RESUELVE:

ARTÍCULO 1°. Adoptar la Política de Seguridad y Privacidad de la Información del Sanatorio de Agua de Dios E.S.E., como instrumento institucional que establece los principios, lineamientos, responsabilidades, procedimientos y controles necesarios para garantizar la protección integral de los activos de información, la cual hace parte integral de la presente resolución.

ARTÍCULO 2°. La presente política será de obligatorio cumplimiento para todos los servidores públicos, contratistas, proveedores, usuarios y demás partes interesadas que accedan, gestionen, almacenen, procesen o transmitan información institucional, en cualquiera de sus formatos y en todas las fases de su ciclo de vida.

ARTÍCULO 3°. Desígnese a la **Coordinación GIT Planeación, Gestión Documental y TIC'S** o quien haga sus veces, como la dependencia responsable de coordinar la implementación, seguimiento, evaluación y mejora continua de la **Política de Seguridad y Privacidad de la Información** del Sanatorio de Agua de Dios E.S.E.

La Coordinación GIT Planeación, Gestión Documental y TIC'S deberá designar formalmente a un (1) funcionario como **Responsable de Seguridad y Privacidad de la Información**, quien actuará como enlace técnico con la Alta Dirección, el Comité de Gestión y Desempeño Institucional, y los demás procesos institucionales. Esta persona tendrá, entre otras, las siguientes funciones:

a) Coordinar la ejecución de los lineamientos, controles, estrategias y procedimientos definidos en la política, en articulación con las demás áreas de la entidad.

b) Proponer los ajustes normativos, técnicos o procedimentales necesarios, conforme a los resultados de auditorías, incidentes reportados, evaluación de riesgos o cambios normativos.

c) Hacer seguimiento al cumplimiento de los indicadores del Modelo de Seguridad y Privacidad de la Información – MSPI.

d) Consolidar informes periódicos dirigidos a la Alta Dirección y al Comité de Gestión y Desempeño Institucional sobre el estado de la seguridad y privacidad de la información.

e) Promover campañas de sensibilización, formación y apropiación sobre la protección de datos y el uso seguro de la información institucional.

RESOLUCIÓN No. 10.39.309 DE 2025

(Junio 12)

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información del Sanatorio de Agua de Dios E.S.E."

f) Actuar como punto de contacto frente a requerimientos de entes de control, autoridades competentes y titulares de datos personales, en relación con el tratamiento de la información.

g) Coordinar la autoevaluación del nivel de madurez del MSPI y las acciones derivadas de su resultado.

Parágrafo 1. El **Responsable de Seguridad y Privacidad de la Información** en el Sanatorio de Agua de Dios E.S.E. será el funcionario que ejerza el rol de **Coordinador GIT Planeación, Gestión Documental y TIC'S** o quien haga sus veces.

ARTÍCULO 4°. La Oficina de Control Interno (o quien haga sus veces) realizará auditorías periódicas para verificar el cumplimiento de la presente política, proponiendo las acciones de mejora que correspondan.

ARTÍCULO 5°. La Gerencia del Sanatorio de Agua de Dios E.S.E. deberá garantizar la disponibilidad y asignación efectiva de los recursos humanos, tecnológicos, físicos y financieros necesarios para la adecuada implementación, mantenimiento y mejora continua de la Política de Seguridad y Privacidad de la Información, así como para la operación eficiente del Modelo de Seguridad y Privacidad de la Información (MSPI).
Este compromiso incluye, entre otros:

a) Incluir dentro de la planeación estratégica, presupuestal y operativa institucional las acciones derivadas de la implementación de la política y del MSPI.

b) Asegurar la disponibilidad de personal capacitado y con competencias específicas para ejercer los roles definidos en la política.

c) Destinar los recursos tecnológicos requeridos para la protección de los activos de información (software, hardware, conectividad, respaldo, ciberseguridad).

d) Apoyar la ejecución de planes de formación, sensibilización y gestión del cambio organizacional orientados a fortalecer la cultura de seguridad de la información.

e) Promover la articulación del MSPI con otros sistemas de gestión institucional y planes estratégicos como el Plan Anticorrupción y de Atención al Ciudadano, el Plan Estratégico de Tecnología (PETI) y el Plan de Gobierno Digital.

RESOLUCIÓN No. 10.39.309 DE 2025

(Junio 12)

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información del Sanatorio de Agua de Dios E.S.E."

ARTÍCULO 6°. Comuníquese la presente resolución a todas las áreas de la entidad y publíquese en los medios institucionales correspondientes, con el fin de garantizar su apropiación e implementación efectiva.

ARTÍCULO 7°. La TC-PO-003 **POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN del Sanatorio de Agua de Dios E.S.E.**, hace parte integral de la presente resolución.

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE

Dada en Agua de Dios, a los doce (12) días del mes de junio del año dos mil veinticinco (2025).

ANTONIO RUIZ FLOREZ
Gerente

Proyectó: *Jose Guillermo Trujillo Mayorga – Secretario*
Revisó: *Luis Jerónimo Pérez Pérez– Asesor Jurídico*

POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

ELABORADO POR:

JOSE GUILLERMO TRUJILLO MAYORGA

SANATORIO DE AGUA DE DIOS E.S.E.

MACROPROCESO GESTION DE APOYO

PROCESO GESTION TECNOLOGICA

2025

FECHA DE APROBACIÓN: 12/06/2025

TABLA DE CONTENIDO

1 INTRODUCCIÓN 4

2 TÍTULO DE LA POLÍTICA 5

3 OBJETIVO 5

3.1 Objetivos Específicos 5

4 ALCANCE 5

5 ENFOQUE DIFERENCIAL 7

6 MARCO NORMATIVO 7

7 DEFINICIONES 8

8 DECLARACIÓN DE LA POLÍTICA 10

9 LINEAMIENTOS 11

10 RESPONSABILIDADES 14

10.1 Alta Dirección 15

10.2 Comité de Gestión y Desempeño Institucional 15

10.3 Responsable u oficial de Seguridad y Privacidad de la Información 15

10.4 Oficina de Sistemas de Información 16

10.5 Área de Gestión Documental y Archivo 16

10.6 Área de Talento Humano 16

10.7 Coordinadores y/o Responsables de áreas 17

10.8 Responsable u oficial del tratamiento de datos personales 17

10.9 Todos los funcionarios, contratistas y terceros 17

10.10 Oficina de Control Interno (o quien haga sus veces) 17

11 MONITOREO Y EVALUACIÓN 17

11.1 Plan de seguimiento al MSPI 18

11.2 Indicadores de gestión 18

11.3 Auditorías internas y externas 18

11.4 Evaluación del impacto 19

11.5 Ciclo de mejora continua 19

11.6 Procedimientos mínimos 19

11.7 Consideraciones complementarias para la implementación 21

12 REVISIÓN Y ACTUALIZACIÓN 22

12.1 Frecuencia de revisión 22

12.2 Responsables de la revisión 23

12.3 Mecanismos de actualización 23

12.4 Registro documental 23

13 REFERENCIAS 23

14 APROBACIÓN 25

15 CONTROL DE CAMBIOS 25

1 INTRODUCCIÓN

El Sanatorio de Agua de Dios E.S.E., en cumplimiento de las disposiciones normativas vigentes y alineado con la Estrategia de Gobierno Digital liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), establece la presente Política de Seguridad y Privacidad de la Información, como un instrumento fundamental para la protección, gestión y uso adecuado de los activos de información institucionales.

Esta política tiene como propósito garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información que se gestiona en el marco de las funciones asistenciales, administrativas, científicas y comunitarias del Sanatorio. De esta manera, se asegura el cumplimiento de la legislación colombiana en materia de protección de datos personales, acceso a la información pública, habeas data, ciberseguridad y otros lineamientos aplicables al sector salud.

La información es uno de los activos más valiosos para la toma de decisiones en salud pública y administración sanitaria. Por ello, el Sanatorio de Agua de Dios E.S.E. asume el compromiso institucional de adoptar buenas prácticas internacionales en seguridad de la información, como las definidas en la norma ISO/IEC 27001, integrándolas a su sistema de gestión, cultura organizacional y procesos estratégicos.

La presente política está dirigida a todos los servidores públicos, contratistas, proveedores, usuarios y demás partes interesadas que accedan, manipulen, administren o custodian información en la entidad, y forma parte del ciclo de mejora continúa previsto en el Modelo de Seguridad y Privacidad de la Información (MSPI).

2 TÍTULO DE LA POLÍTICA

POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

3 OBJETIVO

Establecer los lineamientos y directrices que permitan garantizar la seguridad y la privacidad de la información institucional en el Sanatorio de Agua de Dios E.S.E., mediante la implementación de controles, procedimientos y prácticas que aseguren la confidencialidad, integridad y disponibilidad de los activos de información, contribuyendo así al cumplimiento de la misión institucional, la protección de los datos personales y el fortalecimiento de la confianza de los usuarios y partes interesadas.

3.1 Objetivos Específicos

- Implementar un marco de gestión de riesgos que permita identificar, evaluar y mitigar las amenazas que afectan la seguridad y privacidad de la información en los procesos asistenciales, administrativos y de apoyo de la entidad.
- Establecer roles, responsabilidades y procedimientos internos que garanticen el uso adecuado, seguro y responsable de los activos de información, promoviendo la cultura organizacional en torno a la protección de los datos y el cumplimiento normativo.
- Asegurar el cumplimiento de la normativa nacional sobre protección de datos personales, acceso a la información pública, habeas data y ciberseguridad, mediante la adopción de buenas prácticas y la integración del MSPI al sistema de gestión institucional.

4 ALCANCE

La presente Política de Seguridad y Privacidad de la Información aplica a todas las áreas, procesos, dependencias, sistemas de información, servicios digitales, activos de información y personal vinculado al Sanatorio de Agua de Dios E.S.E., incluyendo

servidores públicos, contratistas, proveedores, personal en misión, pasantes y terceros que accedan, gestionen o administren información institucional.

Esta política abarca el tratamiento de la información en todos sus formatos (físico, digital, electrónico, audiovisual, entre otros) y en todas las fases de su ciclo de vida: recolección, registro, almacenamiento, procesamiento, transmisión, uso, intercambio, archivo y disposición final.

Tiene aplicación específica sobre la información relacionada con:

- Los usuarios de los servicios de salud, en especial personas diagnosticadas con enfermedad de Hansen (lepra) u otras patologías crónicas de interés en salud pública.
- Los datos personales, clínicos y administrativos de los pacientes, trabajadores, contratistas y visitantes.
- La documentación técnica y científica generada en los procesos asistenciales, investigativos y comunitarios.
- Los registros derivados de los sistemas de información en salud (RIPS, historia clínica electrónica, SISMUESTRAS, PAIWEB, etc.).
- Los activos de información críticos que soportan los servicios institucionales, incluyendo bases de datos, plataformas, redes y archivos físicos.
- La información compartida con entidades del orden municipal, departamental y nacional, así como con organismos de control y entes cooperantes.

El alcance de esta política se extiende a todos los procesos internos e interinstitucionales en los que se genere, gestione o transmita información en custodia del Sanatorio, con el objetivo de garantizar el cumplimiento de la legislación vigente en materia de **protección de datos personales, derechos de los usuarios, confidencialidad clínica y acceso a la información pública**, preservando la dignidad y los derechos fundamentales de las personas atendidas.

5 ENFOQUE DIFERENCIAL

El Sanatorio de Agua de Dios E.S.E, se acoge a los lineamientos normativos del Plan de Atención Integral en Salud, con el desarrollo de estrategias de enfoque de género y enfoque diferencial a la población que demande los servicios de salud ofertados, para la población que se identifique en situación de vulnerabilidad: víctimas del conflicto armado, grupos étnicos, población en situación de discapacidad; personas de talla baja; habitantes de calle; población dispersa; según el curso de vida (gestantes y adulto mayor) de conformidad con la Política de atención diferencial definida por la entidad. ¨Para esto los colaboradores deberán respetar las diferencias socio culturales; identidades de género y orientación sexual; identificarán las condiciones especiales de la población, darán cumplimiento a las estrategias para atender condiciones especiales aplicables, la Alta Dirección brindará capacitación al talento humano sobre enfoque diferencial y las estrategias adoptadas, contará con los recursos necesarios para implementar las estrategias definidas, realizará seguimiento a la implementación de las mismas, evaluará la efectividad de la implementación y formulará los planes de mejora a que haya lugar, cuando se identifiquen desviaciones en su cumplimiento.

6 MARCO NORMATIVO

- **Ley 1581 de 2012:** Por la cual se dictan disposiciones generales para la protección de datos personales en Colombia.
- **Decreto 1377 de 2013:** Reglamenta parcialmente la Ley 1581 de 2012 en lo relativo a la autorización del tratamiento de datos personales.
- **Ley 1712 de 2014:** Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- **Ley 1266 de 2008:** Por la cual se dictan normas generales del habeas data y se regula el manejo de la información contenida en bases de datos personales.

- **Ley 527 de 1999:** Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, comercio electrónico y firmas digitales.
- **Ley 594 de 2000:** Ley General de Archivos, que establece las normas para la gestión de documentos y archivos públicos.
- **Ley 1438 de 2011 y Ley 1751 de 2015:** Reformas al Sistema General de Seguridad Social en Salud, con implicaciones sobre el manejo de información clínica.
- **Decreto 1078 de 2015:** Decreto Único Reglamentario del Sector TIC, que incorpora el componente de seguridad y privacidad de la información en la Estrategia de Gobierno Digital.
- **Decreto 886 de 2014:** Sobre el Registro Nacional de Bases de Datos y las obligaciones de los responsables del tratamiento de datos.
- **ISO/IEC 27001:** Sistema de Gestión de Seguridad de la Información.
- **ISO/IEC 27002:** Código de buenas prácticas para controles de seguridad de la información.
- **ISO/IEC 27005:** Gestión de riesgos en seguridad de la información.
- **ISO 31000:** Principios y directrices para la gestión del riesgo.
- **Guías del Modelo de Seguridad y Privacidad de la Información – MSPI**, emitidas por el Ministerio TIC.

7 DEFINICIONES

- **Seguridad de la información:** Proceso mediante el cual se garantiza la **confidencialidad, integridad y disponibilidad** de la información institucional, mediante la implementación de controles administrativos, técnicos y físicos.

- **Privacidad de la información:** Derecho que tienen todas las personas a que sus **datos personales y sensibles** sean protegidos durante su tratamiento, conforme a la Ley 1581 de 2012, garantizando el respeto por la **intimidad, el buen nombre** y el ejercicio del **habeas data**.
- **Datos personales:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ej. nombre, número de documento, historia clínica, datos de contacto).
- **Datos sensibles:** Aquellos datos que afectan la intimidad del titular o cuyo uso indebido puede generar discriminación, tales como los relativos a la salud, origen étnico, orientación sexual, convicciones religiosas, políticas o filosóficas.
- **Tratamiento de datos personales:** Cualquier operación realizada sobre datos personales: recolección, almacenamiento, uso, circulación o supresión.
- **Activos de información:** Cualquier recurso que contenga o permita el procesamiento de información y que tenga valor para la organización. Incluye bases de datos, documentos físicos, sistemas informáticos, redes, personal y procesos.
- **Incidente de seguridad de la información:** Evento que ha comprometido o podría comprometer la seguridad de la información, afectando su confidencialidad, integridad o disponibilidad.
- **Riesgo de seguridad de la información:** Probabilidad de que una amenaza explote una vulnerabilidad causando un impacto negativo sobre los activos de información.
- **Responsable del tratamiento:** Persona natural o jurídica, pública o privada, que decide sobre la base de datos y/o el tratamiento de los datos personales.
- **Encargado del tratamiento:** Persona natural o jurídica, pública o privada, que realiza el tratamiento de datos personales por cuenta del responsable.
- **Sistema de Gestión de Seguridad de la Información (SGSI):** Conjunto de políticas, procesos, recursos, responsabilidades y actividades que permiten

implementar, operar, monitorear, revisar y mejorar la seguridad de la información dentro de la entidad.

- **Confidencialidad:** Propiedad de la información que garantiza que solo sea accesible a las personas autorizadas.
- **Integridad:** Propiedad que asegura que la información no ha sido alterada de manera no autorizada.
- **Disponibilidad:** Garantía de que la información esté accesible y utilizable cuando sea requerida por personas autorizadas.
- **Información clasificada o reservada:** Información pública cuyo acceso se restringe de manera legítima por razones de interés público, legalidad o privacidad, conforme a lo dispuesto en la Ley 1712 de 2014.

8 DECLARACIÓN DE LA POLÍTICA

La Alta dirección del **Sanatorio de Agua de Dios E.S.E.**, consciente del valor estratégico de la información en la prestación de servicios de salud, la gestión institucional y la garantía de los derechos fundamentales de los ciudadanos, expresa mediante la presente política su **compromiso institucional con la seguridad y privacidad de la información** como uno de los pilares de la buena administración pública y la confianza de la comunidad.

Esta declaración tiene como propósito establecer los lineamientos que aseguren la **confidencialidad, integridad, disponibilidad y privacidad de la información**, en cumplimiento de las normas legales vigentes, las buenas prácticas internacionales (como la norma ISO/IEC 27001) y los principios de la Estrategia de Gobierno Digital.

En este sentido, la Alta Dirección se compromete a:

- **Apoyar y liderar la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI)** en todos los niveles de la entidad.

- **Asignar los recursos necesarios** (humanos, técnicos y financieros) para el funcionamiento efectivo del sistema de gestión de seguridad de la información.
- **Designar formalmente los roles y responsabilidades** requeridos para la implementación, seguimiento y mejora continua del MSPI.
- **Fomentar una cultura organizacional orientada a la protección de los datos personales**, el respeto por los derechos de los usuarios y el cumplimiento normativo.
- **Integrar la seguridad de la información** en los procesos misionales, de apoyo y estratégicos del Sanatorio, incluyendo aquellos relacionados con la atención clínica, la gestión documental, la investigación, la salud pública y la administración institucional.
- **Garantizar el cumplimiento de la legislación vigente** en materia de protección de datos personales (Ley 1581 de 2012), acceso a la información pública (Ley 1712 de 2014), historia clínica (Resolución 1995 de 1999), ciberseguridad y demás normas que rigen el sector salud.

La presente política será revisada periódicamente y actualizada conforme a las necesidades institucionales, los avances tecnológicos, los cambios normativos y las oportunidades de mejora identificadas.

9 LINEAMIENTOS

Para garantizar el cumplimiento de los objetivos institucionales y legales relacionados con la seguridad y privacidad de la información, el Sanatorio de Agua de Dios E.S.E. adopta los siguientes lineamientos:

- **Protección de la información**

Toda la información que repose en el Sanatorio será tratada como un activo institucional valioso. Se implementarán controles adecuados para garantizar su confidencialidad, integridad, disponibilidad y trazabilidad, de acuerdo con su nivel de criticidad y sensibilidad.

- **Cumplimiento normativo**

Se garantizará el estricto cumplimiento de las normas nacionales e internacionales aplicables, tales como la Ley 1581 de 2012, la Ley 1712 de 2014, el Decreto 1078 de 2015 y la norma ISO/IEC 27001. Cualquier tratamiento de datos personales o uso de información pública deberá estar fundamentado en el marco legal vigente.

- **Responsabilidad institucional**

Los servidores públicos, contratistas, terceros y demás usuarios con acceso a los activos de información serán responsables del uso adecuado de los mismos, conforme a los principios de legalidad, ética, reserva, confidencialidad y respeto por los derechos de los titulares de la información.

- **Control de accesos**

Se establecerán mecanismos de control físico y lógico que aseguren el acceso autorizado a la información, minimizando el riesgo de accesos no autorizados, filtraciones, modificaciones no consentidas o pérdida de información.

- **Clasificación de la información**

Toda la información será clasificada según su nivel de sensibilidad (pública, reservada, clasificada, confidencial, sensible, etc.) y tratada conforme a su naturaleza, en especial aquella relacionada con datos personales y clínicos.

- **Continuidad del servicio**

Se desarrollarán e implementarán planes de contingencia y continuidad del negocio, para asegurar que la operación institucional no se vea interrumpida por eventos que afecten la disponibilidad de los activos de información.

- **Capacitación y sensibilización**

Se ejecutarán planes periódicos de formación, sensibilización y capacitación dirigidos a todo el personal sobre la importancia de la seguridad y privacidad de la información y sobre sus responsabilidades al respecto.

- **Auditoría y mejora continua**

La política y el sistema de gestión de seguridad de la información serán sometidos a auditorías internas y externas, con el fin de verificar su cumplimiento, detectar no conformidades y generar acciones de mejora continua.

- **Protección de datos personales**

Todo tratamiento de datos personales se realizará bajo los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad, tal como lo establece la Ley 1581 de 2012. Se garantizarán los derechos de los titulares mediante procedimientos claros y accesibles.

- **Historia clínica y sistemas de información en salud**

El Sanatorio garantizará la confidencialidad, integridad y acceso controlado a la historia clínica de los usuarios, conforme a la Resolución 1995 de 1999 y demás normativas vigentes. Los sistemas de información como RIPS, HIS, PAIWEB y SISMUESTRAS deberán contar con controles de acceso y respaldo, minimizando el riesgo de exposición indebida o pérdida de datos clínicos.

- **Información de población con enfermedad de Hansen**

La información clínica, social o administrativa relacionada con personas diagnosticadas con enfermedad de Hansen será tratada con especial reserva y sensibilidad, dada su condición como dato sensible y las posibles implicaciones de discriminación o estigmatización. Se aplicarán controles adicionales conforme al enfoque de derechos humanos, salud pública y no discriminación.

- **Video vigilancia y datos biométricos**

El uso de sistemas de video vigilancia, control de ingreso por huella o reconocimiento facial deberá ser debidamente informado a los titulares de la información, indicando el fin, responsable del tratamiento y mecanismos de consulta. Estos datos serán tratados bajo los principios de proporcionalidad, legalidad y minimización.

- **Transferencia de información a terceros**

Toda transferencia de información a entidades externas, nacionales o internacionales, deberá estar respaldada por **acuerdos de confidencialidad**, convenios interinstitucionales o bases legales explícitas. En ningún caso se permitirá la entrega de información personal sin autorización del titular o sin una causa legal justificada.

- **Recolección de datos en procesos comunitarios**

En los procesos de atención extramural, brigadas, actividades de promoción y prevención o atención en zonas rurales, se garantizará que la recolección de datos personales cumpla con los principios de consentimiento informado, finalidad específica y seguridad en el almacenamiento y transporte de la información.

- **Sistemas de información internos y externos**

Cualquier desarrollo, adquisición o uso de software y plataformas tecnológicas por parte del Sanatorio deberá contemplar criterios de **seguridad por diseño**, privacidad por defecto y cumplimiento de las normas nacionales sobre protección de datos.

10 RESPONSABILIDADES

Para garantizar la aplicación efectiva de la presente política, el Sanatorio de Agua de Dios E.S.E. establece los siguientes roles y funciones institucionales:

10.1 Alta Dirección

- Aprobar oficialmente la Política de Seguridad y Privacidad de la Información.
- Liderar y respaldar la implementación del MSPI dentro de la entidad.
- Asignar los recursos humanos, tecnológicos y financieros necesarios para la gestión de la seguridad de la información.
- Designar al responsable institucional de seguridad y privacidad de la información.
- Velar por la integración del MSPI con los demás sistemas de gestión institucional.

10.2 Comité de Gestión y Desempeño Institucional

- Asesorar a la Alta Dirección en la toma de decisiones relacionadas con seguridad y privacidad de la información.
- Aprobar los planes de tratamiento de riesgos, políticas internas, procedimientos y controles relacionados.
- Realizar seguimiento periódico al cumplimiento del MSPI y proponer acciones de mejora.

10.3 Responsable u oficial de Seguridad y Privacidad de la Información

- Coordinar la implementación del MSPI en toda la entidad.
- Liderar la elaboración de los procedimientos de seguridad, controles y matrices de riesgo.
- Velar por la correcta clasificación y protección de los activos de información.
- Coordinar con las áreas de tecnología, gestión documental, atención al usuario y talento humano para el cumplimiento de la política.

- Reportar a la Alta Dirección los incidentes, avances y necesidades en materia de seguridad de la información.

10.4 Oficina de Sistemas de Información

- Garantizar la seguridad lógica de la infraestructura tecnológica (servidores, redes, estaciones de trabajo, sistemas de información).
- Aplicar controles de acceso, respaldo, monitoreo, actualización y recuperación ante desastres.
- Implementar buenas prácticas en ciberseguridad y gestión de vulnerabilidades.
- Apoyar técnicamente la implementación del protocolo IPv6 y la seguridad en plataformas tecnológicas.

10.5 Área de Gestión Documental y Archivo

- Garantizar el cumplimiento de las normas archivísticas vigentes (Ley 594 de 2000, TRD).
- Clasificar adecuadamente la información según su sensibilidad y definir controles de acceso físico.
- Asegurar el almacenamiento, conservación y disposición final adecuada de los documentos con datos personales.

10.6 Área de Talento Humano

- Incluir en los procesos de inducción, reinducción y capacitación, temas de seguridad y privacidad de la información.
- Establecer cláusulas de confidencialidad en los contratos laborales y de prestación de servicios.
- Velar por la asignación y retiro oportuno de permisos y accesos a los sistemas de información.

10.7 Coordinadores y/o Responsables de áreas

- Implementar y aplicar los controles de seguridad definidos en sus procesos.
- Informar oportunamente incidentes, riesgos o vulnerabilidades detectadas.
- Asegurar el cumplimiento de la política en sus áreas de responsabilidad.

10.8 Responsable u oficial del tratamiento de datos personales

- Ejecutar los procesos de tratamiento de datos conforme a las instrucciones del responsable.
- Asegurar la confidencialidad y custodia adecuada de la información tratada.

10.9 Todos los funcionarios, contratistas y terceros

- Cumplir con las disposiciones establecidas en esta política.
- Usar de forma responsable la información y los recursos tecnológicos asignados.
- Reportar de forma inmediata cualquier incidente, pérdida, acceso indebido o riesgo que afecte la seguridad de la información.

10.10 Oficina de Control Interno (o quien haga sus veces)

- Realizar auditorías periódicas al cumplimiento del MSPI.
- Emitir recomendaciones para la mejora continua del sistema de seguridad de la información.
- Verificar el cumplimiento normativo en materia de protección de datos y transparencia.

11 MONITOREO Y EVALUACIÓN

Con el fin de asegurar el cumplimiento, efectividad e impacto institucional de la Política de Seguridad y Privacidad de la Información, el Sanatorio de Agua de Dios

E.S.E. implementará un sistema de **seguimiento, medición y evaluación periódica**, bajo los siguientes lineamientos:

11.1 Plan de seguimiento al MSPI

Se elaborará y actualizará anualmente un plan de seguimiento y evaluación del Modelo de Seguridad y Privacidad de la Información, que incluirá:

- Revisión de la implementación de los controles establecidos.
- Evaluación del nivel de cumplimiento de la política.
- Medición del nivel de madurez del MSPI según los criterios definidos en el modelo.
- Análisis de riesgos residuales y nuevos riesgos identificados.

11.2 Indicadores de gestión

Se establecerán **indicadores de desempeño** para evaluar la eficacia y eficiencia del sistema, entre los cuales se pueden incluir:

- Número de incidentes de seguridad reportados y atendidos.
- Porcentaje de personal capacitado en seguridad y privacidad de la información.
- Nivel de cumplimiento en la clasificación de activos de información.
- Avance en el tratamiento de riesgos priorizados.
- Índice de cumplimiento normativo en protección de datos personales.

Los resultados de estos indicadores se presentarán semestralmente ante la Alta Dirección y el Comité de Gestión y Desempeño Institucional.

11.3 Auditorías internas y externas

Se programarán **auditorías periódicas**, realizadas por la Oficina de Control Interno o por auditores externos, para:

- Verificar el cumplimiento de la política, los procedimientos y controles implementados.
- Validar el nivel de protección de la información en los sistemas y procesos críticos.
- Detectar no conformidades, oportunidades de mejora y cumplimiento legal.

11.4 Evaluación del impacto

Se medirá el **impacto institucional** de la política en términos de:

- Reducción de incidentes y pérdidas de información.
- Fortalecimiento de la cultura de seguridad en la entidad.
- Mejora en la calidad de la atención y la confianza de los usuarios.
- Cumplimiento de requerimientos de entes de control y de auditoría.

11.5 Ciclo de mejora continua

Los hallazgos de auditoría, los resultados de indicadores y los cambios normativos o tecnológicos darán lugar a la formulación de planes de mejora continua, que serán aprobados por la Alta Dirección y gestionados por el responsable de Seguridad de la Información.

11.6 Procedimientos mínimos

Para dar cumplimiento a la presente política, el Sanatorio de Agua de Dios E.S.E. adoptará y documentará como mínimo los siguientes **procedimientos institucionales**, los cuales deben ser aprobados por la Alta Dirección y socializados a toda la entidad:

- **Procedimiento para la gestión de incidentes de seguridad de la información**

Define las etapas para identificar, registrar, analizar, contener, solucionar y documentar incidentes que afecten la confidencialidad, integridad o disponibilidad de la información (ej. fugas de datos, accesos no autorizados, malware).

- **Procedimiento para la clasificación y manejo de la información**

Establece las categorías de clasificación (pública, reservada, confidencial, sensible) y las reglas de acceso, almacenamiento, circulación, conservación y eliminación de la información de acuerdo con su nivel de criticidad.

- **Procedimiento para el control de accesos**

Establece cómo se asignan, modifican y revocan los accesos a sistemas de información, carpetas compartidas, correo electrónico y bases de datos, incluyendo criterios de autenticación, perfiles y segregación de funciones.

- **Procedimiento para el tratamiento de datos personales**

Regula la recolección, uso, almacenamiento y eliminación de datos personales de pacientes, funcionarios, proveedores y demás titulares, incluyendo el cumplimiento del consentimiento informado y el ejercicio de los derechos de los titulares (consultas, reclamos, supresión).

- **Procedimiento de respaldo y recuperación de información**

Define las rutinas, herramientas y responsabilidades para el **respaldo periódico** de los activos de información digitales, así como los pasos para su restauración ante fallas o pérdida de datos.

- **Procedimiento para la gestión de riesgos**

Incluye la metodología para identificar, valorar, tratar y monitorear los riesgos de seguridad de la información, con base en estándares como ISO 27005 o la Guía No. 7 del MinTIC.

- **Procedimiento para la gestión documental**

Asegura que los documentos físicos y electrónicos, especialmente los que contienen datos sensibles o personales, se gestionen conforme a las Tablas de Retención Documental y demás normas archivísticas.

- **Procedimiento para la destrucción segura de información**

Define las técnicas y procesos autorizados para la destrucción física o lógica de documentos y archivos que han cumplido su ciclo de vida, garantizando la **no recuperación** de la información.

- **Procedimiento para la administración de proveedores y terceros**

Incluye los controles y cláusulas que deben exigirse a los proveedores o terceros que accedan o gestionen información institucional, incluyendo acuerdos de confidencialidad, revisiones técnicas y requisitos de seguridad contractual.

- **Procedimiento de capacitación y sensibilización**

Establece la programación, contenidos y estrategias para capacitar al personal sobre buenas prácticas de seguridad, cultura de privacidad y cumplimiento normativo.

11.7 Consideraciones complementarias para la implementación

Con el fin de garantizar la sostenibilidad, pertinencia y mejora continua de la presente política, el Sanatorio de Agua de Dios E.S.E. adoptará progresivamente los siguientes elementos estratégicos, recomendados por el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio TIC:

Aspecto	Implementación
Matriz de activos y clasificación	Elaborar y mantener actualizada una matriz institucional de activos de información, identificando su clasificación (pública, reservada, confidencial, sensible) y nivel de criticidad. Esta matriz podrá adjuntarse como anexo técnico o integrarse a los procedimientos.
Enlace con planes institucionales	Garantizar la integración de esta política con el PEI, el Plan Anticorrupción y de Atención al Ciudadano (PAAC), el Plan

	Estratégico de Tecnología de la información y el Plan de Gobierno Digital, como ya se ha descrito en esta política.
Gestión del cambio organizacional	Diseñar e implementar estrategias de sensibilización, formación, liderazgo y apropiación institucional que permitan incorporar la seguridad de la información como parte de la cultura organizacional.
Derechos del titular	Incluir un procedimiento accesible y claro para garantizar el ejercicio de los derechos de los titulares de los datos personales: consulta, corrección, supresión y revocatoria, conforme a la Ley 1581 de 2012.
Evaluación de madurez del MSPI	Realizar anualmente la autoevaluación del nivel de madurez del modelo, en los términos definidos por el MinTIC, e incorporar los resultados en los planes de mejora.
Relación con entes de control	Establecer mecanismos y responsabilidades claras para atender los requerimientos de la Superintendencia Nacional de Salud, la Procuraduría, la Contraloría y demás órganos de control, garantizando la protección legal y segura de la información entregada.

12 REVISIÓN Y ACTUALIZACIÓN

La presente **Política de Seguridad y Privacidad de la Información** será objeto de revisión y actualización periódica con el fin de garantizar su **vigencia, pertinencia y alineación** con los cambios normativos, tecnológicos, organizacionales y del entorno.

12.1 Frecuencia de revisión

La política será revisada como mínimo **una vez al año** o de forma extraordinaria cuando se presenten:

- Cambios significativos en la normatividad nacional o internacional relacionada con protección de datos, ciberseguridad o gestión de información.
- Incidentes de seguridad de alto impacto que exijan ajustes a los controles o lineamientos existentes.

- Cambios organizacionales relevantes, como reestructuración de procesos, incorporación de nuevas tecnologías o nuevas funciones en la entidad.
- Recomendaciones derivadas de auditorías internas o externas, evaluaciones de desempeño o planes de mejora.

12.2 Responsables de la revisión

La **responsabilidad de coordinar la revisión** y actualización de esta política recae sobre el **Responsable de Seguridad y Privacidad de la Información**, en articulación con el **Comité de Gestión y Desempeño Institucional**, y deberá ser validada y aprobada por la **Alta Dirección**.

12.3 Mecanismos de actualización

- Toda versión modificada de la política deberá registrarse mediante **control de cambios** (historial de versiones).
- La nueva versión será **divulgada institucionalmente** a todos los funcionarios, contratistas y terceros a través de medios físicos o electrónicos.
- Se actualizarán también los **procedimientos, manuales y controles** que dependan de los lineamientos de esta política.

12.4 Registro documental

Las versiones anteriores y vigentes de la política deberán conservarse conforme a las disposiciones del Sistema de Gestión Documental de la entidad y a la Ley General de Archivos (Ley 594 de 2000).

13 REFERENCIAS

- Congreso de Colombia. (2000). Ley 594 de 2000. Por medio de la cual se dicta la Ley General de Archivos. Diario Oficial No. 44.083.

- Congreso de Colombia. (2008). Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del habeas data. Diario Oficial No. 47.219.
- Congreso de Colombia. (2012). Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial No. 48.587.
- Congreso de Colombia. (2014). 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. Diario Oficial No. 49.084.
- Congreso de Colombia. (2015). Ley 1751 de 2015. Por medio de la cual se regula el derecho fundamental a la salud. Diario Oficial No. 49.427.
- Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC]. (2022). Guía Modelo de Seguridad y Privacidad de la Información - MSPI. Recuperado de https://www.mintic.gov.co/
- Ministerio de Salud y Protección Social. (1999). Resolución 1995 de 1999. Por la cual se establecen normas para el manejo de la historia clínica. Diario Oficial No. 43.679.
- Organización Internacional de Normalización (ISO). (2013). ISO/IEC 27001:2013 - Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requisitos. Ginebra: ISO.
- Organización Internacional de Normalización (ISO). (2014). ISO/IEC 27002:2014 - Tecnología de la información – Técnicas de seguridad – Código de buenas prácticas para controles de seguridad de la información. Ginebra: ISO.

14 APROBACIÓN

ELABORÓ	REVISÓ	APROBÓ	GESTIÓN DOCUMENTAL
JOSE GUILLERMO TRUJILLO MAYORGA Secretario	EDGAR ANGELICO GAMBOA MUR Responsable Tics	ANTONIO RUIZ FLOREZ Gerente	CESAR MAURICIO UBAQUE TELLEZ Coordinador GIT Planeación, Gestión Documental y TIC'S
FECHA	FECHA	FECHA	FECHA
12/06/2025	12/06/2025	12/06/2025	12/06/2025

15 CONTROL DE CAMBIOS

TIPO DE MODIFICACIÓN	DESCRIPCIÓN DEL CAMBIO	RESPONSABLE	FECHA DEL CAMBIO	VERSIÓN
CREACIÓN	Creación del documento	JOSE GUILLERMO TRUJILLO MAYORGA	12/06/2025	01

FECHA DE APROBACIÓN: 12/06/2025