Sanatorio de Agua de Dios
Empresa Social del Estado

RESOLUCIÓN No. 10.39.310 DE 2025

(Junio 12)

Por la cual se adopta la Política de Gobierno Digital y de Seguridad Digital 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 el Gobierno Digital constituye una estrategia del Estado colombiano orientada a mejorar la gestión pública, garantizar la transparencia, la participación ciudadana, la eficiencia administrativa y la prestación de servicios digitales de calidad, accesibles y centrados en el ciudadano;

Que la Seguridad Digital es un componente esencial para proteger la información institucional, prevenir incidentes cibernéticos y garantizar la continuidad operativa de los procesos misionales y de apoyo;

Que en cumplimiento de los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, y de acuerdo con las normas vigentes en materia de seguridad de la información, protección de datos personales, interoperabilidad y gestión digital, es deber de las entidades públicas implementar políticas que garanticen el uso estratégico, seguro y responsable de las tecnologías de la información y las comunicaciones (TIC);

Que la Coordinación GIT Planeación, Gestión Documental y TIC'S ha elaborado el documento "Política de Gobierno Digital y de Seguridad Digital", el cual ha sido revisado y validado por las instancias competentes;

RESUELVE:

ARTÍCULO 1°. Adoptar la Política de Gobierno Digital y de Seguridad Digital del Sanatorio de Agua de Dios E.S.E., como instrumento de gestión institucional orientado a fortalecer la transformación digital, la eficiencia administrativa, la transparencia, la protección de la información y la prestación de servicios digitales centrados en el ciudadano, la cual hace parte integral de la presente resolución.

ARTÍCULO 2°. La presente política será de obligatorio cumplimiento para todos los servidores públicos, contratistas, pasantes, estudiantes, proveedores y demás terceros que hagan uso, desarrollo, administración o gestión de tecnologías de la información y comunicaciones, sistemas de información, activos digitales o datos institucionales.

ARTÍCULO 3°. Desígnese a la Coordinación GIT Planeación, Gestión Documental y TIC'S o quien haga sus veces, como encargada de coordinar, liderar y supervisar la implementación de la Política de Gobierno Digital y de Seguridad Digital. Esta dependencia será responsable de articular los planes de acción, ejecutar el seguimiento técnico, presentar informes de avance y garantizar el cumplimiento de los lineamientos establecidos.

RESOLUCIÓN No. 10.39.310 DE 2025

(Junio 12)

Por la cual se adopta la Política de Gobierno Digital y de Seguridad Digital del Sanatorio de Agua de Dios E.S.E.

Parágrafo 1. El responsable de Gobierno Digital en el Sanatorio de Agua de Dios E.S.E. será el funcionario que ejerza como Coordinador GIT Planeación, Gestión Documental y TIC'S o quien haga sus veces. Este funcionario tendrá bajo su cargo la coordinación del Plan Estratégico de Tecnologías de la Información (PETI), la supervisión de la ciberseguridad institucional, la adopción de estándares de interoperabilidad, y el cumplimiento de la normativa vigente en materia digital. En caso de ausencia, la Alta Dirección deberá designar formalmente un encargado con las competencias necesarias.

ARTÍCULO 4°. La Gerencia del Sanatorio de Agua de Dios E.S.E. garantizará la disponibilidad de los recursos humanos, tecnológicos, financieros y físicos necesarios para la implementación, mantenimiento y mejora continua de la presente política. Este compromiso institucional incluye:

a. La integración de esta política al direccionamiento estratégico y los sistemas de gestión.
b. La asignación presupuestal para el fortalecimiento de la infraestructura tecnológica.
c. La promoción de una cultura organizacional basada en la transformación digital.
d. La supervisión del cumplimiento mediante el Comité de Gestión y Desempeño.

ARTÍCULO 5°. El Comité de Gestión y Desempeño Institucional será el órgano encargado de realizar el seguimiento, evaluación y mejora continua de la política adoptada, incluyendo la revisión de indicadores de cumplimiento, auditorías internas y propuestas de actualización.

ARTÍCULO 6°. Comuníquese la presente resolución a todas las áreas de la entidad, publíquese en la página web institucional y en medios internos, y archívese para los fines pertinentes.

ARTÍCULO 7°. La TC-PO-002 **POLÍTICA DE GOBIERNO DIGITAL Y DE SEGURIDAD DIGITAL 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: *José Guillermo Trujillo Mayorga – Secretario*
Revisó: *Luis Jerónimo Pérez Pérez– Asesor Jurídico*

POLÍTICA DE GOBIERNO DIGITAL Y DE SEGURIDAD DIGITAL

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

En el marco de la transformación digital del Estado colombiano y en cumplimiento de los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), el Sanatorio de Agua de Dios E.S.E. adopta la presente Política de Gobierno Digital y de Seguridad Digital con el propósito de fortalecer la gestión institucional, mejorar la calidad de los servicios ofrecidos a la ciudadanía y garantizar la protección de la información.

El Gobierno Digital constituye una estrategia clave para promover el uso efectivo y seguro de las tecnologías de la información y las comunicaciones (TIC) en los procesos administrativos, asistenciales y misionales de la Entidad, asegurando la eficiencia, la transparencia y la participación ciudadana. En este contexto, la Seguridad Digital se convierte en un pilar fundamental para proteger la integridad, disponibilidad y confidencialidad de los activos de información, así como para prevenir, detectar y responder de manera oportuna a los riesgos cibernéticos.

Esta política se formula teniendo en cuenta las particularidades del Sanatorio de Agua de Dios E.S.E., su rol como institución especializada en la atención de patologías crónicas y transmisibles como la enfermedad de Hansen, y su compromiso con la prestación de servicios de salud humanizados, seguros y centrados en el paciente. Así mismo, responde a la necesidad de alinear los procesos institucionales con las buenas prácticas en gestión digital y seguridad de la información, promoviendo una cultura organizacional orientada a la innovación y al uso ético de la tecnología.

2 TÍTULO DE LA POLÍTICA

POLÍTICA DE GOBIERNO DIGITAL Y DE SEGURIDAD DIGITAL

3 OBJETIVO

Implementar y fortalecer el modelo de Gobierno Digital y la gestión de la Seguridad Digital en el Sanatorio de Agua de Dios E.S.E., con el fin de optimizar la prestación de servicios de salud, garantizar la protección de la información institucional y fomentar la transparencia, la participación ciudadana y la eficiencia administrativa mediante el uso estratégico de las tecnologías de la información y las comunicaciones (TIC).

3.1 Objetivos Específicos

- Adoptar el Modelo Integrado de Gobierno Digital en los procesos misionales y de apoyo de la Entidad, promoviendo la transformación digital institucional y el acceso efectivo a los servicios a través de medios digitales.
- Establecer y aplicar lineamientos de Seguridad Digital que permitan prevenir, detectar, gestionar y mitigar los riesgos asociados al uso de las TIC, protegiendo la confidencialidad, integridad y disponibilidad de la información.
- Fomentar una cultura organizacional digital mediante procesos de capacitación, sensibilización y apropiación de herramientas tecnológicas, fortaleciendo las competencias digitales del talento humano y la confianza en el uso de los servicios digitales por parte de los ciudadanos.

4 ALCANCE

La presente política aplica a todos los procesos, dependencias, funcionarios, contratistas, docentes, estudiantes que realicen prácticas, pasantías o trabajos de grado, bajo el marco de un contrato y/o convenio académico y demás terceros que intervienen en el uso, desarrollo, implementación, administración y gestión de tecnologías de la información y las comunicaciones (TIC) dentro del Sanatorio de Agua de Dios E.S.E. Asimismo, abarca los sistemas de información, infraestructuras

tecnológicas, servicios digitales, activos de información y canales electrónicos dispuestos para la gestión institucional y la prestación de servicios de salud.

Esta política incluye los lineamientos para la adopción del Modelo de Gobierno Digital definido por el Ministerio TIC, en sus componentes de TIC para la gestión, servicios digitales, seguridad digital, ciudadanos digitales y confianza digital. También contempla la implementación de medidas técnicas, organizacionales y normativas para la protección de la información y la gestión de riesgos asociados al entorno digital.

El alcance de esta política se extiende a los procesos misionales, estratégicos y de apoyo de la Entidad, tanto en la sede principal como en sus unidades operativas y áreas asistenciales, con el fin de garantizar la transformación digital institucional, la seguridad de la información y el cumplimiento de las normas vigentes en materia de protección de datos personales, seguridad digital y transparencia.

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

- **Decreto 620 de 2020** – Regula el Modelo Integrado de Gobierno Digital y los Servicios Ciudadanos Digitales para todas las entidades públicas.
- **Documento CONPES 3975 de 2019** – Línea base de la política de transformación digital e inteligencia artificial en el sector público.
- **Decreto 1499 de 2017 (MIPG)** – Integra planeación y gestión institucional (MIPG), al que debe alinearse toda estrategia digital.
- **Ley 1978 de 2019** – Moderniza el sector TIC y crea un regulador único, facilitando la infraestructura que soporta los servicios digitales del Estado.
- **Política Nacional de Seguridad Digital – CONPES 3995 de 2020** – Marco de gestión de riesgos, gobernanza y capacidades en seguridad digital.
- **CONPES 4045 de 2021** – Profundiza en ciberseguridad e inteligencia estratégica para la resiliencia nacional.
- **ISO/IEC 27001:2022** – Requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI).
- **NIST Cybersecurity Framework 2.0 (2024)** – Buenas prácticas internacionales de gestión de riesgos cibernéticos, adoptables en el sector salud colombiano.
- **Ley 1581 de 2012** – Régimen general de protección de datos personales.
- **Decreto 1377 de 2013** – Reglamenta parcialmente la Ley 1581 (consentimiento y registro de bases de datos).

7 DEFINICIONES

- **Gobierno Digital:** Estrategia del Estado colombiano que promueve el uso e implementación efectiva de tecnologías de la información y las comunicaciones

(TIC) para mejorar la gestión pública, fortalecer la transparencia, aumentar la participación ciudadana y ofrecer servicios digitales de calidad, accesibles y centrados en el ciudadano.

- **Seguridad Digital:** Conjunto de políticas, procedimientos, herramientas y controles que buscan garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información digital, así como proteger los sistemas informáticos de la organización frente a amenazas internas y externas.
- **Sistema de Gestión de Seguridad de la Información (SGSI):** Modelo estructurado de gestión basado en la norma ISO/IEC 27001, que permite identificar, evaluar y controlar los riesgos asociados a la seguridad de la información en una organización.
- **Datos Personales:** Cualquier información vinculada o que pueda asociarse a una persona natural identificada o identificable, incluyendo datos sensibles relacionados con la salud, orientación sexual, religión, entre otros.
- **Protección de Datos Personales:** Conjunto de principios, derechos y procedimientos establecidos por la Ley 1581 de 2012 y sus reglamentaciones, que buscan garantizar el adecuado tratamiento de los datos personales, especialmente en entornos digitales.
- **Servicios Digitales:** Servicios prestados por la entidad mediante el uso de plataformas tecnológicas y canales digitales (como páginas web, aplicaciones móviles o portales institucionales), permitiendo la interacción eficiente y segura con los usuarios.
- **Transformación Digital:** Proceso de cambio organizacional que implica la adopción de tecnologías digitales para rediseñar modelos operativos, procesos y servicios, buscando mayor eficiencia, impacto y valor público.
- **Ciberseguridad:** Capacidad para proteger los sistemas de información frente a incidentes cibernéticos que puedan comprometer sus funciones, datos o

continuidad, mediante la implementación de medidas preventivas, de detección, respuesta y recuperación.

- **Ciudadano Digital:** Persona que utiliza las tecnologías de la información y las comunicaciones para ejercer sus derechos, participar en la vida pública, acceder a servicios del Estado y realizar trámites en línea de manera segura y eficiente.

8 DECLARACIÓN DE LA POLÍTICA

El Sanatorio de Agua de Dios E.S.E., en cumplimiento de la normatividad nacional y comprometido con la mejora continua de su gestión institucional, adopta esta Política de Gobierno Digital y Seguridad Digital como marco orientador para fortalecer la transparencia, la eficiencia administrativa, la protección de la información y la prestación de servicios de salud con enfoque digital, accesibles y centrados en el ciudadano.

Esta política establece los lineamientos para incorporar las tecnologías de la información y las comunicaciones (TIC) en los procesos misionales, estratégicos y de apoyo, garantizando la transformación digital institucional de manera articulada, segura y sostenible. Asimismo, define las estrategias para prevenir, detectar y gestionar los riesgos asociados a la seguridad de la información, velando por la confidencialidad, integridad, disponibilidad y trazabilidad de los activos digitales.

El Sanatorio se compromete a implementar un Sistema de Gestión de Seguridad de la Información (SGSI), a fortalecer la cultura de seguridad digital entre sus funcionarios y usuarios, a promover el acceso equitativo a los servicios digitales, y a fomentar una relación transparente y participativa con la ciudadanía a través de canales tecnológicos seguros.

Esta política es de obligatorio cumplimiento para todos los servidores públicos, contratistas y terceros que, en el ejercicio de sus funciones, hagan uso de los activos de información o participen en la gestión de procesos tecnológicos de la entidad.

9 LINEAMIENTOS

A. Planeación y Dirección Estratégica TIC

- Toda iniciativa digital debe estar alineada con el Plan Estratégico Institucional (PEI), el Plan Estratégico de Tecnologías de la Información (PETI) y el Modelo Integrado de Planeación y Gestión (MIPG).
- Las decisiones sobre inversión en TIC deben estar sustentadas en análisis de costo-beneficio, riesgos tecnológicos y sostenibilidad operativa.
- El comité de Gestión y Desempeño orientará, evaluará y supervisará la implementación de esta política.

B. Gestión de la Información y Protección de Datos

- La entidad deberá garantizar el cumplimiento de la Ley 1581 de 2012 y sus decretos reglamentarios, promoviendo el tratamiento responsable y seguro de los datos personales.
- Se mantendrán actualizados los registros de bases de datos ante la Superintendencia de Industria y Comercio.
- La información institucional será clasificada, custodiada y compartida conforme a niveles de seguridad y al principio de mínima divulgación.

C. Servicios Digitales e Interacción con Ciudadanos

- Los trámites y servicios ofrecidos por la entidad deberán estar disponibles a través de canales digitales accesibles, seguros y fáciles de usar.
- Se fomentará la participación ciudadana mediante herramientas tecnológicas como encuestas, buzones físicos y/o virtuales y foros digitales.
- La experiencia del usuario digital será evaluada periódicamente para asegurar mejoras continuas.

D. Seguridad Digital y Gestión del Riesgo Tecnológico

- El Sanatorio deberá implementar y mantener un Sistema de Gestión de Seguridad de la Información (SGSI), con base en la norma ISO/IEC 27001 y buenas prácticas nacionales e internacionales.
- Se aplicarán controles de seguridad preventiva, detectiva y correctiva para proteger los activos de información y reducir riesgos de ciberataques.
- Todos los incidentes de seguridad deberán ser reportados, documentados, gestionados y solucionados oportunamente.

E. Formación y Cultura Digital Institucional

- Todos los servidores públicos y contratistas deberán recibir capacitación periódica en Gobierno Digital, ciberseguridad, protección de datos y buenas prácticas TIC.
- Se promoverá una cultura organizacional que valore la transformación digital como eje de transparencia, eficiencia y servicio al usuario.

F. Interoperabilidad e Infraestructura Tecnológica

- Los sistemas de información institucionales deberán ajustarse a los lineamientos del Ministerio TIC sobre interoperabilidad, arquitectura empresarial, accesibilidad y estándares abiertos.
- Toda adquisición o actualización tecnológica deberá incluir criterios de seguridad, escalabilidad, compatibilidad y sostenibilidad.
- Se promoverá el uso de servicios en la nube conforme a la normativa vigente y con los debidos controles de seguridad.

G. Interoperabilidad y Arquitectura Empresarial

Con el fin de garantizar una gestión eficiente, articulada y basada en datos, el Sanatorio de Agua de Dios E.S.E. promoverá el desarrollo de una **arquitectura**

empresarial institucional, alineada con el modelo de referencia del Ministerio TIC y las buenas prácticas internacionales (por ejemplo, TOGAF).

Se establecerán las siguientes acciones:

- **Diseño de un modelo de arquitectura empresarial:** que contemple los dominios de negocio, información, aplicaciones y tecnología, integrando los procesos asistenciales, administrativos y de apoyo.
- **Adopción de estándares de interoperabilidad:** técnicos, semánticos y organizacionales, que permitan el intercambio seguro y confiable de información entre sistemas internos y con entidades externas (Ej. historia clínica electrónica, SISPRO, RUAF).
- **Inventario y clasificación de activos de información:** con el fin de identificar los flujos de datos críticos, duplicidades, cuellos de botella y oportunidades de integración tecnológica.
- **Uso de herramientas tecnológicas de modelado y gestión:** como repositorios de arquitectura empresarial, modelos de procesos (BPM), y plataformas de integración (middleware o APIs).
- **Definición de líneas base de interoperabilidad y conectividad:** para priorizar inversiones y establecer hojas de ruta de digitalización institucional.
- **Participación activa en iniciativas sectoriales:** de interoperabilidad en salud (HCE interoperable, PISIS, RIPS electrónicos), conforme a los lineamientos del Ministerio de Salud y el MinTIC.

Esta estrategia permitirá una **visión integral** de los procesos institucionales, facilitará la toma de decisiones basada en datos, y aumentará la eficiencia, seguridad y trazabilidad en la gestión de la información.

H. Plan de Continuidad del Negocio y Recuperación ante Desastres Tecnológicos

El Sanatorio de Agua de Dios E.S.E. diseñará, documentará e implementará un **Plan de Recuperación ante Desastres Tecnológicos (DRP)**, como parte del Sistema de Gestión de Seguridad de la Información (SGSI), con el fin de garantizar la disponibilidad de los servicios críticos y la protección de la información ante eventos que puedan afectar la operación institucional. Con el objetivo de establecer las acciones, recursos y responsables necesarios para restaurar los servicios tecnológicos esenciales y proteger la integridad de la información en caso de incidentes, fallos técnicos, desastres naturales o ciberataques.

9.1 Análisis de la Situación Actual

- **Nivel de madurez digital institucional**

Actualmente, el Sanatorio de Agua de Dios E.S.E. presenta avances iniciales en procesos de transformación digital. Sin embargo, existen limitaciones en cuanto a la **integración de plataformas**, **digitalización de trámites administrativos**, y **automatización de servicios al ciudadano**, lo cual impide una gestión más eficiente y centrada en el usuario.

- **Fragmentación de sistemas de información**

La institución cuenta con sistemas de información dispares y no interoperables, lo que afecta la continuidad del flujo de datos entre procesos asistenciales y administrativos. Esta situación limita la capacidad de tomar decisiones basadas en datos, además de incrementar los riesgos asociados a errores en la información y duplicidad de registros.

- **Brechas en seguridad digital**

Si bien existen algunas medidas básicas de protección de la infraestructura tecnológica (antivirus, control de acceso por usuario y contraseña, copias de respaldo), **no se ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI)** bajo estándares internacionales como ISO/IEC 27001. Esto

deja expuesta a la entidad frente a amenazas como el robo de información sensible, ataques cibernéticos o pérdida de datos.

- **Cultura digital limitada**

Existe una necesidad urgente de fortalecer la **formación y sensibilización del talento humano** en temas clave como seguridad digital, protección de datos personales, uso adecuado de tecnologías y transformación digital. Algunos funcionarios aún presentan resistencia al cambio o falta de habilidades para interactuar eficientemente con herramientas digitales.

- **Cumplimiento normativo**

La entidad ha avanzado parcialmente en la implementación de la **Política de Gobierno Digital** del Ministerio TIC. Sin embargo, aún no se cumple a cabalidad con aspectos clave como:

  - ✓ Registro de bases de datos personales ante la Superintendencia de industria y Comercio SIC.
  - ✓ Publicación de trámites digitalizados en el SUIT.
  - ✓ Aplicación del Modelo de Arquitectura Empresarial.
  - ✓ Planes formales de seguridad digital e interoperabilidad.

- **Oportunidades estratégicas**
  - ✓ La creciente digitalización en el sector salud colombiano (telemedicina, interoperabilidad, historia clínica electrónica) abre una oportunidad para modernizar los servicios del Sanatorio.
  - ✓ El fortalecimiento de las TIC puede contribuir a mejorar la atención de pacientes con enfermedad de Hansen, optimizando procesos clínicos, logísticos y de seguimiento.
  - ✓ Existen líneas de apoyo técnico y financiero del MinTIC, Ministerio de Salud y entes internacionales para proyectos de gobierno digital.

9.2 Acciones Estratégicas para el Fortalecimiento de la Seguridad Digital.

Acción Estratégica	Descripción
1. Implementación de un SGSI	Diseñar e implementar un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001, con políticas internas claras y gestión de riesgos.
2. Evaluación de riesgos digitales	Realizar un análisis institucional de riesgos digitales, identificando activos críticos, amenazas y vulnerabilidades. Mantener actualizada la matriz de riesgos TIC.
3. Plan de gestión de incidentes	Establecer protocolos para la identificación, análisis, respuesta y documentación de incidentes de seguridad digital. Crear un equipo básico de respuesta.
4. Formación y sensibilización	Capacitar continuamente al personal en temas como ciberseguridad, protección de datos, buenas prácticas digitales y respuesta ante incidentes.
5. Fortalecimiento de controles de acceso	Aplicar políticas de contraseñas seguras, limitar privilegios según roles, y usar mecanismos de autenticación fuertes para accesos sensibles.
6. Optimización de la infraestructura tecnológica	Actualizar antivirus, firewall y sistemas de seguridad. Realizar revisiones periódicas de vulnerabilidades y asegurar respaldos cifrados.
7. Cumplimiento normativo	Asegurar la aplicación de la Ley 1581 de 2012, la Política de Gobierno Digital, y el Modelo de Seguridad y Privacidad de la Información (MSPI).
8. Plan de continuidad del negocio	Formular e implementar un plan de continuidad para asegurar la recuperación de la operación ante incidentes o desastres tecnológicos.

Tabla 1: Acciones Estratégicas para el Fortalecimiento de la Seguridad Digital.

10 RESPONSABILIDADES

Dirección General:

- Aprobar y liderar la implementación de la Política de Gobierno Digital y Seguridad Digital.
- Designar al responsable de Gobierno Digital y conformar el grupo interdisciplinario de Gobierno Digital.
- Asignar los recursos humanos, técnicos y financieros necesarios para la ejecución del plan de acción.
- Garantizar que la política esté integrada al direccionamiento estratégico institucional.

Comité de Gestión y Desempeño:

- Hacer seguimiento a la ejecución del plan de acción.
- Revisar, actualizar y proponer mejoras a la política, conforme a los cambios normativos y tecnológicos.
- Evaluar avances en la transformación digital y promover decisiones basadas en evidencia.
- Articular a las áreas misionales y de apoyo en la implementación de acciones tecnológicas.

Responsable de Gobierno Digital (Coordinador TIC o quien haga sus veces)

- Coordinar el desarrollo e implementación del Plan Estratégico de Tecnologías de la Información (PETI).
- Liderar la adopción de estándares de interoperabilidad, accesibilidad, ciberseguridad y arquitectura empresarial.

- Supervisar la ejecución de actividades en materia de servicios digitales, protección de datos y seguridad de la información.
- Presentar informes periódicos al Comité de Gestión y Desempeño y/o a la Dirección General.

Oficina Asesora Jurídica y/o administrativa

- Asesorar en la aplicación de la Ley 1581 de 2012 (protección de datos personales), Ley 1266 de 2008 y demás normas relacionadas.
- Elaborar y mantener actualizados los documentos legales asociados al tratamiento de la información digital.
- Realizar el registro de bases de datos ante la SIC y revisar los contratos que involucren servicios tecnológicos.
- Implementar, diseñar e incluir cláusulas de confidencialidad en los contratos bajo cualquier modalidad que realice la entidad.

Área de Talento Humano

- Incluir en el plan institucional de capacitación los temas relacionados con Gobierno Digital, ciberseguridad y uso responsable de las TIC.
- Sensibilizar a los servidores públicos sobre el cumplimiento de esta política y sus implicaciones disciplinarias en caso de incumplimiento.
- Promover una cultura organizacional basada en la transformación digital y la gestión del conocimiento.

Áreas Misionales y de Apoyo

- Colaborar en la digitalización de trámites y servicios institucionales bajo los principios de usabilidad, seguridad y enfoque ciudadano.

- Aplicar controles sobre la información y activos digitales que gestionan, conforme a los lineamientos de seguridad establecidos.
- Reportar incidentes de seguridad o vulneraciones a la privacidad al área TIC o al Comité de Gestión y Desempeño.

Contratistas y Terceros

- Cumplir estrictamente con los lineamientos establecidos en esta política durante el desarrollo de sus actividades.
- Garantizar la confidencialidad, integridad y disponibilidad de la información que procesen en nombre de la entidad.
- Firmar cláusulas de confidencialidad y compromisos de protección de datos personales, según lo definido por la entidad.

Oficina de Control Interno

- Verificar el cumplimiento de la Política de Gobierno Digital y Seguridad Digital mediante auditorías internas programadas.
- Evaluar la eficacia de los controles establecidos para la gestión de riesgos digitales, protección de datos personales y seguridad de la información.
- Emitir recomendaciones para la mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI) y del cumplimiento normativo en materia TIC.
- Realizar seguimiento a los planes de mejora derivados de hallazgos relacionados con el uso de tecnologías de la información.
- Coordinar con los entes de control externo las visitas o auditorías relacionadas con gobierno digital y seguridad digital.

11 MONITOREO Y EVALUACIÓN

Con el fin de garantizar la efectividad y sostenibilidad de la presente política, el **Sanatorio de Agua de Dios E.S.E.** implementará un sistema de **monitoreo y evaluación continua**, que permita verificar su nivel de cumplimiento, detectar oportunidades de mejora y medir el impacto institucional de la transformación digital y la seguridad de la información.

11.1 Mecanismos de Seguimiento y Evaluación

- **Revisión periódica del Comité de Gestión y Desempeño**
  El comité realizará reuniones trimestrales para hacer seguimiento al cumplimiento del plan de acción, revisar indicadores de gestión y formular recomendaciones para mejorar la implementación de la política.
- **Indicadores de gestión y resultado**
  Se establecerán indicadores cuantitativos y cualitativos en las siguientes dimensiones:
  - ✓ Nivel de digitalización de trámites y servicios institucionales.
  - ✓ Porcentaje de servidores capacitados en Gobierno Digital y Seguridad Digital.
  - ✓ Incidentes de seguridad digital reportados y gestionados.
  - ✓ Nivel de cumplimiento del PETI y del plan de seguridad de la información.
  - ✓ Grado de satisfacción del usuario frente a los servicios digitales.

11.1.1 Indicador

Nombre del indicador:

Índice de Cumplimiento Integral de la Política de Gobierno Digital y Seguridad Digital (ICIP-GDSD)

Fórmula:

$$\text{ICIP-GDSD (\%)} = \frac{\sum \text{Puntajes de cumplimiento por componente}}{\text{Puntaje total esperado}} \times 100$$

Componentes evaluados (ejemplo):

Componente	Peso (%)	Fuente de verificación
Implementación del PETI	20%	Documentos, cronograma, evidencias de ejecución
Nivel de digitalización de trámites/servicios	20%	SUIT, páginas web, encuestas de satisfacción
SGSI implementado y operando	20%	Informes, auditorías, matriz de riesgos actualizada
Formación del talento humano	15%	Registros de capacitación, evaluaciones, asistencia
Interoperabilidad y arquitectura empresarial	10%	Mapas de procesos, modelos arquitectónicos, informes
Protección de datos personales	10%	Registro SIC, reportes jurídicos, contratos revisados
Participación ciudadana digital	5%	Encuestas, buzones virtuales, estadísticas de uso

Meta anual sugerida:

≥ 85% de cumplimiento global.

Frecuencia de medición:

Semestral.

Responsable:

Coordinador GIT Planeación, Gestión Documental y Tics / Responsable de Gobierno Digital, con validación del Comité de Gestión y Desempeño.

11.2 Informes de Avance Semestrales

El responsable de Gobierno Digital elaborará un informe semestral, que será presentado a la Dirección General y al Comité de Gestión y Desempeño, el cual incluirá:

- Logros alcanzados.
- Cumplimiento de metas del plan de acción.
- Riesgos identificados y medidas correctivas adoptadas.
- Recomendaciones para ajustes estratégicos.

11.3 Auditorías internas y externas

Se incluirán actividades de verificación en los planes de auditoría interna y se fomentará la revisión por parte de organismos externos (ej. entes de control, MinTIC, Supersalud) cuando sea pertinente.

11.4 Gestión del riesgo digital

Se mantendrá actualizada una matriz de riesgos TIC que permita anticipar vulnerabilidades y establecer planes de contingencia, fortaleciendo el control preventivo en la seguridad digital institucional.

12 REVISIÓN Y ACTUALIZACIÓN

Para garantizar la vigencia, pertinencia y efectividad de la Política de Gobierno Digital y Seguridad Digital del Sanatorio de Agua de Dios E.S.E., se establece el siguiente mecanismo de revisión y actualización:

- La política será revisada de manera formal al menos una vez al año.
- Podrá adelantarse una revisión extraordinaria cuando:
  - ✓ Se promulguen nuevas leyes, decretos o normas que afecten el gobierno digital o la seguridad de la información.

- ✓ Se identifiquen cambios tecnológicos significativos que impacten la gestión institucional.
- ✓ Se presenten resultados de auditorías, evaluaciones o incidentes que requieran ajustes inmediatos

12.1 Criterios para la revisión

- Adecuación a la normatividad vigente en materia de TIC, protección de datos y seguridad digital.
- Resultados de los informes de seguimiento y evaluación.
- Cambios en el entorno tecnológico y de riesgos digitales.
- Recomendaciones y aprendizajes derivados de la gestión interna y externa.
- Necesidades institucionales y expectativas de los usuarios y servidores públicos.

12.2 Proceso de actualización

- La revisión será coordinada por el responsable de Gobierno Digital, con el apoyo del Comité de Gestión y Desempeño.
- Las propuestas de actualización serán sometidas a aprobación por la Dirección General del Sanatorio.
- Las modificaciones aprobadas serán socializadas y difundidas entre todos los servidores públicos, contratistas y usuarios relacionados.

13 REFERENCIAS

- Congreso de la República de Colombia. (2012). Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial No. 48.598.
- https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=51209

- Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC. (2019). Política de Gobierno Digital de Colombia.
- https://www.mintic.gov.co/portal/604/w3-article-9517.html
- Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC. (2020). Política Nacional de Seguridad Digital.
- https://www.mintic.gov.co/portal/604/w3-article-13312.html
- Superintendencia de Industria y Comercio. (2019). Guía para el cumplimiento de la Ley de Protección de Datos Personales en Colombia.
- https://www.sic.gov.co/sites/default/files/normatividad/guia_tratamiento_datos_personales.pdf
- ISO. (2013). ISO/IEC 27001:2013. Information technology — Security techniques — Information security management systems — Requirements.
- https://www.iso.org/standard/54534.html

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