OFICINA TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES TIC´S

POLITICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SISTEMA GESTIÓN DE CALIDAD

SANATORIO DE AGUA DE DIOS E.S.E.

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración del Sanatorio de Agua de Dios E.S.E con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

El Sanatorio de Agua de Dios E.S.E, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del Sanatorio de Agua de Dios E.S.E.
- Garantizar la continuidad del negocio frente a incidentes.

2. OBJETIVO

Definir los lineamientos que deben cumplir los servidores públicos del Sanatorio de Agua de Dios E.S.E sin importar el tipo de vinculación (funcionarios, contratistas, terceros, etc), en cuanto a la protección de los activos de información generados y/o procesados por la entidad para la prestación de sus servicios y que sirven como base para la toma estratégica de decisiones, lo anterior soportado en los tres (3) principios del sistema de seguridad de información como son la **confidencialidad**, **integridad** y **disponibilidad**.

3. MARCO NORMATIVO

- **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 1581 de 2012.** Por la cual se dictan disposiciones generales para la protección de datos personales.
- **Decreto Reglamentario 1377 de 2013.** Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- **Ley 1712 de 2014.** Por la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

- **Resolución 1519 del 2020.** Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.

- **ISO/IEC 27002 (ANTERIORMENTE DENOMINADA ESTÁNDAR 17799:2005), NORMA INTERNACIONAL QUE ESTABLECE EL CÓDIGO DE MEJORES PRÁCTICAS PARA APOYAR LA IMPLANTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN LAS ORGANIZACIONES:** Establecer directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Esto también incluye la selección, implementación y administración de controles, teniendo en cuenta los entornos de riesgo encontrados en la empresa. (Ostec, 2022)

- **Decreto 2693 del 21 de diciembre de 2012.** Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.

4. GLOSARIO

- **POLÍTICA:** Es el conjunto de actividades que se asocian con la toma de decisiones en grupo, u otras formas de relaciones de poder entre individuos, como la distribución de recursos o el estatus. También es el arte, doctrina o práctica referente al gobierno de los Estados,2 promoviendo la participación ciudadana al poseer la capacidad de distribuir y ejecutar el poder según sea necesario para garantizar el bien común en la sociedad. (es.wikipedia, 2022)

- **SEGURIDAD DE LA INFORMACIÓN:** es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos. (Wikipedia, 2022)

- **SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI):** Es un conjunto de políticas de administración de la información. El término se denomina en inglés “Information Security Management System” (ISMS). (Wikipedia, 2022)

- **TERCERO (Derecho Civil):** Es aquél que no ha sido parte en un contrato, y por lo tanto no le es oponible. Ello, no obstante, ese tercero lo puede ser en términos absolutos, es decir, que sea totalmente ajeno al contrato, o por el contrario que se trate de un tercero que posteriormente entrará en relación con los contratantes. (Loya, 2022)

- **ACTIVOS DE INFORMACIÓN:** Los activos los podemos separar en dos grandes grupos **TANGIBLES E INTANGIBLES**. Los activos **TANGIBLES** son aquellos activos materiales que contienen información, y sobre los que tomaremos medidas preventivas para protegerlos principalmente de riesgos físicos: golpes, agua, fuego, etc. Los activos **INTANGIBLES** son aquellos que soportan la información dentro de un activo material, y pueden inutilizar la información, pese a que el activo físico no haya sufrido daño alguno. (S.L, 2022)

- ✓ **ACTIVO:** Un activo es un recurso con valor que alguien posee con la intención de que genere un beneficio futuro (sea económico o no). En contabilidad, representa todos los bienes y derechos de una empresa, adquiridos en el pasado y con los que esperan obtener beneficios futuros. (Economipedia, 2022)

- ✓ **CULTURA DE SEGURIDAD:** La cultura de seguridad es un término que abarca diferentes actitudes y valores de las personas y de la organización en cuanto a los aspectos relativos a la seguridad, tanto en su forma de entenderla como el comportamiento diario que deben tener los trabajadores. (Nueva-iso-45001, 2022)

- ✓ **SISTEMA DE GESTION:** El Sistema de Gestión se define como **"un conjunto de elementos y actividades relacionados y coordinados que interactúan, y que, estableciendo Políticas y Objetivos, dirigen y controlan la organización con el fin de lograr dichas metas"**. Luego, según se trate de garantizar la Calidad de los productos, la correcta gestión Ambiental o la Seguridad, se centrará en las actividades más relacionadas con dichas áreas. (S.L., 2022)

- ✓ **LINEAMIENTO:** Es una orientación de carácter general, corresponde a una disposición o directriz que debe ser implementada en las entidades del Estado colombiano. (Mintic, 2022)

- ✓ **CONFIDENCIALIDAD:** Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. La confidencialidad ha sido definida por la Organización Internacional de Estandarización (ISO) en la norma ISO/IEC 27002 como **"garantizar que la información es accesible sólo para aquellos autorizados a tener acceso"** y es una de las piedras angulares de la seguridad de la información. (wikipedia, 2022)

- ✓ **INTEGRIDAD (Dato):** La integridad de datos es un término usado para referirse a la exactitud y fiabilidad de los datos. Los datos deben estar completos, sin variaciones o compromisos del original, que se considera confiable y exacto. (Tecnologias-Informacion, 2022)

- ✓ **DISPONIBILIDAD (Dato):** Es la capacidad de garantizar que tanto el sistema como los datos van a estar disponibles al usuario en todo momento. (infosegur.wordpress, 2022)

- ✓ **REDES DE DATOS:** Las redes de datos son infraestructuras que han sido creadas para poder transmitir información a través del intercambio de datos. Es decir, son arquitecturas específicas para este fin, cuya base principal es la conmutación de paquetes y que atienden a una clasificación exclusiva, teniendo en cuenta la distancia que es capaz de cubrir su arquitectura física y, por supuesto, el tamaño que presentan. (Valencia, 2022)

- ✓ **SISTEMAS DE INFORMACIÓN:** Se llama sistema de información (**SI**) a un conjunto de datos y elementos que interaccionan entre sí y que tienen un fin específico que, en general, tiene que ver con satisfacer una necesidad. (Uriarte, 2022)

5. ALCANCE

Esta política aplica para todos los servidores públicos, contratistas, terceros y ciudadanía en general que por el cumplimiento de sus funciones y las del Sanatorio de Agua de Dios E.S.E, utilicen, procesen, intercambien, consulten o

compartan información que haya sido generada, procesada o utilizada en los procesos que se encuentren incorporados en el mapa de procesos institucional, y a su vez, en los procedimientos establecidos en cada uno de ellos.

6. POLÍTICAS INSTITUCIONALES DEL SGSI

A continuación, se describen los criterios de la política Institucional del Sanatorio de Agua de Dios E.S.E, que establecen el SGSI para el uso adecuado de los recursos tecnológicos, físicos y los activos de información.

- ✓ El Sanatorio de Agua de Dios E.S.E, ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
- ✓ Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
- ✓ El Sanatorio de Agua de Dios E.S.E, protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
- ✓ El Sanatorio de Agua de Dios E.S.E, protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- ✓ El Sanatorio de Agua de Dios E.S.E, protegerá su información de las amenazas originadas por parte del personal.
- ✓ El Sanatorio de Agua de Dios E.S.E, protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- ✓ El Sanatorio de Agua de Dios E.S.E, controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- ✓ El Sanatorio de Agua de Dios E.S.E, implementará control de acceso a la información, sistemas y recursos de red.
- ✓ El Sanatorio de Agua de Dios E.S.E, garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- ✓ El Sanatorio de Agua de Dios E.S.E, garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- ✓ El Sanatorio de Agua de Dios E.S.E, garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.
- ✓ El Sanatorio de Agua de Dios E.S.E, garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

7. GESTIÓN ACTIVOS DE INFORMACIÓN

La identificación, clasificación y valoración de activos de información estará a cargo de cada uno de los **centros de costos** que conforman el mapa de procesos institucional, la cual deberá mantener la relación de sus activos de información mediante la utilización de la herramienta que el Coordinador de TICs designe para este proceso, esta herramienta debe permitir identificar el tipo de Activo, Tipo de Dato, Propietario del Activo, ubicación, Valor y Clasificación.

La información generada o gestionada por la entidad puede encontrarse de muchas formas (Impresa, manuscrita, almacenada en disco o en medio magnético, en medios electrónicos, presentaciones, videos o conversaciones, etc.), cualquiera que sea la forma de existencia de la información, está siempre debe estar protegida adecuadamente, para preservar la confidencialidad, integridad y la disponibilidad de la misma.

Los activos de Información del Sanatorio de Agua de Dios E.S.E se pueden clasificar en:

7.1. ACTIVOS HUMANOS

- **Empleados:** Empleados públicos de planta (de carrera administrativa y los provisionales), funcionarios de libre nombramiento y remoción, trabajadores oficiales, contratistas.

- **Externos:** Consultores, contratistas, asesores, especialistas, trabajadores temporales, proveedores.

7.2. ACTIVOS FÍSICOS

- **Infraestructura física y de TI:** Edificios, oficinas, centro de datos, cuartos de servidores y equipos, armarios de red (Racks), cableado, escritorios, cajones, archivadores, salas de almacenamiento de medios físicos, dispositivos de identificación y autentificación, control de acceso del personal y otros dispositivos de seguridad como por ejemplo las cámaras (circuito cerrado de TV, lectores biométricos...).
- **Controles del entorno de TI:** Alarmas, sistema de refrigeración, supresión contra incendio, sistemas de alimentación ininterrumpida (UPS), planta eléctrica, alimentación de potencia y de red.
- **Hardware de TI:** Computadores de escritorio y portátiles, dispositivos de almacenamiento, servidores, firewall, routers, dispositivos de comunicaciones, impresoras, scanners.
- **Documentación:** Procedimientos, programas, guías, formatos, manuales y demás documentación física de propiedad de la entidad.

7.3. ACTIVOS DE SERVICIOS DE TI

- Servicios de autenticación y administración de usuario, aplicaciones, servidores proxy, servicios de red, servicios web, servicios inalámbricos, antivirus, antispyware, antispam, detección y prevención de intrusiones, seguridad, FTP, bases de datos, correo electrónico y mensajería instantánea, herramientas de desarrollo, contratos de soporte y mantenimiento de software.

7.4. PRINCIPIOS DE LA SEGURIDAD DE LA INFORMACIÓN

- ✓ **Integridad:** Se refiere a la garantía de que una información no ha sido alterada, borrada, reordenada, copiada, etc., bien durante el proceso de transmisión o en su propio equipo de origen.
- ✓ **Confidencialidad:** Se refiere a que la información solo puede ser conocida por individuos autorizados.
- ✓ **Disponibilidad de la información:** Se refiere a la seguridad que la información puede ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

7.5. DATOS PERSONALES

- ✓ **Ley 1712 de 2014**
  - **Información Pública:** Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.
  - **Información Reservada:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

- ✓ **Ley 1581 de 2012**
  - **Contiene Datos Personales:** Los datos de carácter personal son cualquier tipo de datos que se pueden utilizar para identificar directa o indirectamente a una persona (sujeto de datos).
  - **NO Contiene Datos Personales:** No todos los datos de una persona física se consideran personales. Por ejemplo, los datos anonimizados no se consideran datos personales siempre y cuando no sea posible re identificar a la persona física a la que se refieren.

7.6. CLASIFICACION DE LA CONFIDENCIALIDAD

- ✓ **PÚBLICO:** Activos de información que se son de carácter público y están alcance de todos los interesados.
- ✓ **USO INTERNO:** Activos de información que por su naturaleza son para uso de los servidores públicos en las diferentes áreas de la entidad y entes de control.
- ✓ **CONFIDENCIAL:** Activos de información que son de uso exclusivo de la dirección estratégica de la entidad.

8. RESPONSABLES DE LA POLÍTICA

El Gerente del Sanatorio de Agua de Dios E.S.E garantizara el apoyo para el desarrollo, implementación, aplicación, seguimiento y mejora continua, de la Política del Sistema de Seguridad de Información. El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad,

incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

Los Coordinadores de área son responsables de adoptar e implementar en los diferentes procesos establecidos por la entidad en el mapa de procesos institucional deben adoptar y son responsables de su aplicación.

- **El Comité Institucional de Gestión y Desempeño**: Es la encargada de la revisión y ajustes a la política de seguridad de la información, sus funciones están descritas en la resolución No. 10.39.673 de 18 de noviembre de 2021, este comité es responsable de realizar la sensibilización y la adopción al interior de la entidad.

9. APROBACIÓN

ELABORO	REVISO	APROBO	Vo. Bo. SGC
JOSE GUILLERMO TRUJILLO Profesional de Apoyo Oficina de Planeación	EDGAR ANGELICO GAMBOA MUR Supervisor Código 4220 Grado 23	ANTONIO RUIZ FLOREZ Gerente	EDGAR ANGELICO GAMBOA MUR Supervisor Código 4220 Grado 23
FECHA DE CAMBIO (DD/MM/AAA)	**FECHA DE CAMBIO (DD/MM/AAA)**	**FECHA DE CAMBIO (DD/MM/AAA)**	**FECHA DE CAMBIO (DD/MM/AAA)**

10. CONTROL DE CAMBIOS

ASPECTO DE MODIFICACION	DETALLE DE LOS CAMBIOS	RESPONSABLE	FECHA DE CAMBIO (DD/MM/AAA)	VERSION
VERSIÓN INICIAL	ACTUALIZACIÓN E IMPLEMENTACIÓN	EDGAR ANGELICO GAMBOA MUR Supervisor Código 4220 Grado 23		UNO