



**E.S.E. Salud
del Tundama**



**MUNICIPIO DE DUITAMA
EMPRESA SOCIAL DEL ESTADO SALUD DEL TUNDAMA**

Resolución 396 del 26 de junio de 2025

“Por medio de la cual se crea la Política de Tratamiento de Datos Personales de la E.S.E. Salud del Tundama”

**LA GERENTE DE LA EMPRESA SOCIAL DEL ESTADO SALUD DEL
TUNDAMA**

En uso de sus facultades Constitucionales, legales y estatutarias y,

CONSIDERANDO:

Que la Constitución Política, en su artículo 15, consagra el derecho a la intimidad, al buen nombre y al habeas data, principios esenciales para la protección de datos personales en Colombia, imponiendo a las entidades públicas la obligación de asegurar la confidencialidad, integridad y disponibilidad de la información.

Que la Ley 1581 de 2012 establece un régimen general para la protección de datos personales, imponiendo responsabilidades al responsable y al encargado del tratamiento para garantizar la seguridad y el correcto tratamiento de los datos, y que el Decreto 1377 de 2013 reglamenta parcialmente dicha ley, especialmente en lo relativo a medidas técnicas, organizativas, derechos de los titulares y mecanismos de autorización.

Que la Ley 1712 de 2014 (“Ley de Transparencia y del Derecho de Acceso a la Información Pública”) define los procesos y límites para el acceso a la información institucional, de modo que la política de datos personales debe armonizar con las obligaciones de transparencia y reserva legal.

Que la Ley 1273 de 2009 tipifica conductas punibles relacionadas con el acceso no autorizado, la alteración, la pérdida o la destrucción de datos informáticos, reforzando la necesidad de implementar controles robustos para la protección de la información institucional.

Que el CONPES 3995 de 2020, en su política nacional para la confianza y seguridad digital, impulsa a las entidades del Estado a fortalecer los esquemas de protección de datos, fomentar la ciberseguridad y promover la cultura del buen uso de la información digital.

Que la Política de Gobierno Digital requiere que las entidades públicas adopten estándares de seguridad de la información y de protección de datos, con el fin de asegurar la confianza de los ciudadanos en los sistemas digitales estatales.

Que la E.S.E. Salud del Tundama ha desarrollado una política de confidencialidad mediante la Resolución 1034 de 2020, que definió medidas de seguridad para

Resolución 396 del 26 de junio de 2025**“Por medio de la cual se crea la Política de Tratamiento de Datos Personales de la E.S.E. Salud del Tundama”**

proteger las bases de datos institucionales, incluyendo datos de usuarios, colaboradores, proveedores y contratistas.

Que la Resolución N.º 003 de 2021 implementa en la E.S.E. un Programa de Seguridad de la Información, con mecanismos de monitoreo, evaluación y mejora continua, lo cual exige una política formalizada de tratamiento de datos personales que garantice su alineación con este programa de seguridad.

Que mediante Acuerdo N.º 05 del 4 de junio de 2024, la Junta Directiva adoptó el Plan de Gestión y Desarrollo institucional para 2024-2028, en el que se prioriza la innovación tecnológica, la protección de la información y la mejora continua de los procesos, objetivos que requieren consolidar una política de tratamiento de datos sólida y coherente con los retos del sector salud.

Que la información institucional es un activo estratégico para la entidad, por lo cual debe ser gestionada, protegida y usada de manera responsable para asegurar su disponibilidad, integridad y confidencialidad, en consonancia con los objetivos misionales, la seguridad del paciente y las obligaciones legales.

Que es necesario definir roles claros, mecanismos de control, procesos de aceptación y consentimiento, procedimientos para la gestión de riesgos de datos, así como medidas técnicas y organizativas para prevenir el uso no autorizado o indebido de la información.

Que, para garantizar el cumplimiento normativo, la confianza de los titulares de los datos y la responsabilidad institucional, la E.S.E. Salud del Tundama debe adoptar formalmente una Política de Tratamiento de Datos Personales, que oriente a todos sus colaboradores, contratistas y terceros, en el tratamiento seguro, legal y ético de los datos.

Que en mérito de lo anterior y con el propósito de proteger la privacidad, la seguridad y los derechos de los titulares de datos,

RESUELVE:

ARTÍCULO PRIMERO. CREACIÓN DE LA POLÍTICA DE TRATAMIENTO DE DATOS. Créase la **Política de Tratamiento de Datos Personales** de la E.S.E. Salud del Tundama, que tiene por objeto establecer las directrices para la recolección, almacenamiento, uso, acceso, custodia, transmisión, conservación, modificación, supresión y disposición final de los datos personales bajo la responsabilidad de la entidad, asegurando la protección, integridad, disponibilidad y legalidad del tratamiento.

Con la presente política, la entidad busca prevenir eventuales riesgos y conflictos legales asociados al uso inadecuado de la información, garantizando la custodia y protección de los datos personales de los ciudadanos mediante la implementación de procedimientos, controles y medidas técnicas y administrativas orientadas al cumplimiento del régimen legal vigente. Esta obligación se articula con la misión y visión institucional, reafirmando el compromiso de la E.S.E. Salud del Tundama de

Resolución 396 del 26 de junio de 2025**“Por medio de la cual se crea la Política de Tratamiento de Datos Personales de la E.S.E. Salud del Tundama”**

brindar servicios con calidad, transparencia y plena garantía de seguridad sobre la información confiada por los usuarios.

ARTÍCULO SEGUNDO: ALCANCE: La presente política aplica a todos los colaboradores, servidores públicos, contratistas y terceros autorizados que manejen datos personales para la E.S.E. Salud del Tundama, y comprende todos los datos institucionales, sin importar su formato (físico o digital), incluyendo información sensible, reservada o clasificada, a lo largo de todo su ciclo de vida.

ARTICULO TERCERO. PRINCIPIOS Y DIRECTRICES. El tratamiento de datos personales en la entidad se rige por los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad, confidencialidad, integridad, minimización y responsabilidad demostrada, los cuales orientan todas las actuaciones institucionales frente a la gestión de la información.

En desarrollo de estos principios, la E.S.E. Salud del Tundama deberá garantizar que los datos sean recolectados únicamente para fines legítimos, explícitos y autorizados; que su uso sea proporcional y pertinente; y que su acceso se limite estrictamente al personal autorizado.

ARTÍCULO CUARTO. – MEDIDAS TÉCNICAS, ADMINISTRATIVAS Y ORGANIZACIONALES: la entidad adoptará entre otras, las siguientes medidas técnicas, administrativas y organizacionales adecuadas, incluyendo controles de seguridad, gestión de riesgos, protocolos de custodia y mecanismos de trazabilidad, para prevenir el acceso no autorizado, la alteración, pérdida, uso indebido o destrucción de la información, en cumplimiento de la Constitución Política, la Ley 1581 de 2012, sus decretos reglamentarios y los estándares nacionales de seguridad de la información:

1. Medidas Técnicas:

- **Controles de acceso lógico:** autenticación de usuarios mediante contraseña robusta, doble factor de autenticación (2FA), perfiles y roles de acceso diferenciados.
- **Encriptación:** cifrado de bases de datos, discos duros, copias de seguridad y transmisión de datos vía SSL/TLS.
- **Copias de seguridad automáticas:** respaldos periódicos, almacenados en entornos seguros y con pruebas de restauración.
- **Firewalls y antivirus corporativos:** protección frente a accesos no autorizados, malware y amenazas cibernéticas.
- **Registros de auditoría (logs):** monitoreo y trazabilidad de accesos, modificaciones y descargas de información.
- **Actualización y parcheo de sistemas:** instalación oportuna de actualizaciones de seguridad.
- **Control de impresión y bloqueo de dispositivos externos:** restricción de impresiones, desactivación de puertos USB para proteger información sensible como historias clínicas.
- **Seguridad física digital:** servidores en cuartos de TI con acceso restringido, sensores, cámaras y controles biométricos si existen.

Resolución 396 del 26 de junio de 2025**“Por medio de la cual se crea la Política de Tratamiento de Datos Personales de la E.S.E. Salud del Tundama”****2. Medidas Administrativas**

- **Políticas internas formales:** política de tratamiento de datos personales, política de seguridad de la información, manual de custodia de historias clínicas, protocolo de incidentes de seguridad y plan de continuidad del negocio.
- **Autorizaciones e instructivos:** formatos de autorización de tratamiento de datos, consentimiento informado, cláusulas contractuales de confidencialidad.
- **Acuerdos de confidencialidad:** para empleados, contratistas, practicantes, proveedores y auditores externos.
- **Gestión de incidentes:** procedimientos para reportar, registrar, analizar y mitigar incidentes de fuga o pérdida de información.
- **Evaluaciones y auditorías periódicas:** revisión del cumplimiento de la política de protección de datos y controles de seguridad.
- **Matriz de riesgos de seguridad de la información:** identificación, valoración y tratamiento de riesgos.
- **Clasificación de la información:** categorización de datos según su nivel de sensibilidad (públicos, reservados, confidenciales, sensibles).
- **Restricción de acceso a historias clínicas:** conforme a la Ley 23 de 1981, Resolución 1995 de 1999 y jurisprudencia constitucional.

3. Medidas Organizacionales

- **Asignación de roles y responsabilidades:** responsable y encargados del tratamiento; custodios de bases de datos; responsables de archivo; oficiales de protección de datos.
- **Capacitaciones periódicas:** formación en protección de datos, seguridad de la información, ética en el manejo de historias clínicas y prevención de riesgos informáticos.
- **Comités institucionales:**
 - ✓ Comité de Seguridad de la Información.
 - ✓ Comité de Gestión y Desempeño.
 - ✓ Comité de Archivo e Historias Clínicas.
- **Protocolos de custodia y archivo:** control de préstamo, consulta, traslado y disposición final de documentos físicos y digitales.
- **Procedimientos de ingreso y salida del talento humano:** activación y desactivación de usuarios, devolución de equipos y acceso a sistemas, revocación de permisos.
- **Gestión de proveedores y terceros:** verificación de cumplimiento de estándares de seguridad y protección de datos antes de contratar.
- **Plan de continuidad y recuperación:** procedimientos para garantizar la disponibilidad de la información ante fallas, desastres o ataques cibernéticos.

*Adicional a lo anterior, téngase en cuenta la **MATRIZ DE CONTROLES PARA LA PROTECCIÓN DE DATOS PERSONALES**, adjunta y que hace parte integral de la presente política.*

ARTÍCULO QUINTO. – MEDIDAS TÉCNICAS, ADMINISTRATIVAS Y ORGANIZACIONALES: RESPONSABLES DEL TRATAMIENTO.

✓

Resolución 396 del 26 de junio de 2025**“Por medio de la cual se crea la Política de Tratamiento de Datos Personales de la E.S.E. Salud del Tundama”**

1. **Responsable del Tratamiento:** La E.S.E. Salud del Tundama, como entidad que define propósitos y medios del tratamiento de los datos personales.
2. **Encargados del Tratamiento:** Todas las áreas internas, procesos o terceros (como proveedores de software) que realizan operaciones sobre datos por cuenta de la entidad, bajo instrucciones definidas.
3. **Delegado de Protección de Datos:** El (la) líder de Gestión de la Información y Comunicación Organizacional, quien coordinará la implementación y seguimiento de esta política, gestionará el cumplimiento y reportará incidentes de seguridad.

ARTÍCULO SEXTO. – RESPONSABILIDADES ESPECÍFICAS. Se asignan responsabilidades a los distintos actores:

1. Gerencia: como autoridad administrativa y responsable de la dirección estratégica de la entidad, asume la responsabilidad superior en la implementación y sostenibilidad del Sistema de Protección de Datos Personales. En virtud de los principios de dirección y control previstos en el Modelo Integrado de Planeación y Gestión – MIPG, le corresponde:

- Aprobar, adoptar y promover la presente política, asegurando su alineación con la Ley 1581 de 2012, el Decreto 1377 de 2013 y las directrices de la SIC.
- Asignar los recursos técnicos, tecnológicos, humanos y financieros necesarios para la adecuada gestión de datos personales.
- Fomentar una cultura organizacional de privacidad y seguridad de la información, conforme a la jurisprudencia de la Corte Constitucional, que exige especial diligencia en el manejo de datos sensibles y datos relativos a la salud (Sent. T-043/2023 y T-158/2022).
- Incorporar la gestión del riesgo de privacidad dentro del mapa institucional de riesgo, siguiendo los lineamientos jurisprudenciales del Consejo de Estado sobre deber de previsión, control y vigilancia frente a actividades que comprometen derechos fundamentales (CE, Secc. Tercera, Sent. 2021 y 2023).
- Dirigir acciones de mejora continua y control interno, asegurando que los procesos internos mantengan trazabilidad, evidencia documental y cumplimiento regulatorio.

2. Gestión de la Información: como responsable operativo del aseguramiento de la calidad, integridad y seguridad de la información institucional, asume las siguientes funciones:

- Diseñar, implementar, evaluar y actualizar los estándares, protocolos y controles en materia de seguridad de la información, tratamiento de datos y administración de riesgos asociados.
- Desarrollar y mantener el inventario de bases de datos, clasificándolas según tipo de dato, nivel de riesgo y medidas de control exigidas por la normativa.
- Incorporar controles de seguridad (lógicos, físicos y administrativos) acordes con el principio de responsabilidad demostrada (accountability), conforme a la doctrina de la Superintendencia de Industria y Comercio.
- Monitorear incidentes de seguridad, activar los procedimientos de respuesta y reportar a las instancias correspondientes, con fundamento en la obligación constitucional de proteger la intimidad y el habeas data (Art. 15 CP y jurisprudencia T-414/2021).

A

Resolución 396 del 26 de junio de 2025**“Por medio de la cual se crea la Política de Tratamiento de Datos Personales de la E.S.E. Salud del Tundama”**

3. Gestión de Información y Atención al Usuario: como punto de contacto directo con el titular de datos, cumple funciones esenciales para asegurar el ejercicio de los derechos fundamentales a la intimidad y al habeas data:

- Verificar la recolección lícita, informada y proporcional de los datos personales, asegurando que exista autorización válida y que el titular conozca las finalidades del tratamiento.
- Gestionar, tramitar y responder de manera oportuna las solicitudes, peticiones, consultas y reclamos de los titulares, en cumplimiento del artículo 14 de la Ley 1581 de 2012.
- Garantizar la protección, reserva y confidencialidad de la información suministrada por los usuarios, especialmente cuando se trata de datos sensibles o datos relativos a la salud (resguardados bajo reserva legal y jurisprudencia consolidada: T-307/2023 y T-158/2022).
- Asegurar trazabilidad en el ciclo de vida de la información, desde su recolección hasta su eliminación segura.

4. Gestión del Talento Humano: Por su manejo de información personal y sensible de empleados, aspirantes y exservidores, esta dependencia deberá:

- Aplicar las medidas de protección de datos en los procesos de selección, contratación, inducción, desempeño y desvinculación, con observancia de los principios de finalidad, necesidad y proporcionalidad.
- Garantizar que los funcionarios reciban capacitación periódica en protección de datos, seguridad de la información y confidencialidad.
- Implementar cláusulas de confidencialidad y obligaciones de reserva en las relaciones laborales o contractuales.
- Custodiar adecuadamente las historias laborales y demás archivos, protegiendo la intimidad y reserva documental conforme a la Ley 1581 de 2012 y a la jurisprudencia de tutela sobre tratamiento de información laboral (T-095/2023).

5. Gestión Jurídica: La dependencia jurídica, como soporte normativo y garante de cumplimiento, deberá:

- Asesorar integralmente la aplicación de la normativa sobre protección de datos personales, privacidad, seguridad de la información y derecho de petición.
- Verificar la legalidad y suficiencia de las autorizaciones de tratamiento, así como la validez de las bases de datos institucionales.
- Responder solicitudes de autoridades, organismos de control, jueces y titulares, asegurando la observancia de la protección reforzada de datos sensibles.
- Promover acciones de responsabilidad y seguimiento frente a incumplimientos, incidentes de seguridad o vulneraciones de derechos.
- Incorporar los criterios jurisprudenciales recientes sobre responsabilidad administrativa por fallas en control interno y gestión del riesgo (Consejo de Estado 2022, 2023).

6. Contratistas, Proveedores y Terceros: Toda persona natural o jurídica que actúe como Encargado del Tratamiento deberá:

✓

Resolución 396 del 26 de junio de 2025**“Por medio de la cual se crea la Política de Tratamiento de Datos Personales de la E.S.E. Salud del Tundama”**

- Tratar los datos única y exclusivamente para las finalidades autorizadas, con apego estricto a las instrucciones del Responsable del Tratamiento.
- Adoptar medidas técnicas, organizacionales y jurídicas adecuadas, equivalentes o superiores a las exigidas por la entidad.
- Garantizar la confidencialidad, integridad y seguridad de la información administrada.
- Reportar oportunamente incidentes de seguridad y colaborar en las investigaciones internas.
- Suscribir acuerdos de confidencialidad, cláusulas contractuales y anexos de protección de datos, siguiendo la doctrina de la SIC sobre corresponsabilidad y estándares mínimos de seguridad.

ARTÍCULO SEPTIMO. – DEFINICIONES. Para los efectos de la presente Resolución y conforme a lo dispuesto en la Constitución Política, la Ley 1581 de 2012, el Decreto 1377 de 2013 y demás normas concordantes, se adoptan las siguientes definiciones:

Dato Personal: Toda información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. Comprende, entre otros, datos de identificación, localización, características personales, información socioeconómica, laboral y cualquier otra que permita identificar al titular.

Datos Sensibles: Aquellos datos que afectan la intimidad del titular o cuyo uso indebido puede generar riesgos de discriminación. Se consideran sensibles, entre otros, los relativos a la salud, orientación sexual, origen étnico, características biométricas, creencias religiosas o convicciones filosóficas. Su tratamiento está sujeto a restricciones especiales y a la autorización explícita del titular, salvo excepciones legales.

Titular: Persona natural cuyos datos personales son objeto de tratamiento. El titular tiene derecho a conocer, actualizar, rectificar, suprimir, oponerse y revocar la autorización del tratamiento, en los términos de la Ley 1581 de 2012.

Autorización: Consentimiento previo, expreso e informado otorgado por el titular para el tratamiento de sus datos personales. Este puede constar en medios físicos, electrónicos o cualquier mecanismo que permita su conservación y verificación, conforme al principio de demostrabilidad ("accountability").

Habeas Data: Derecho fundamental mediante el cual toda persona puede conocer, actualizar y rectificar la información que sobre ella se haya recogido en bases de datos o archivos de entidades públicas o privadas. Incluye la facultad de solicitar prueba de la autorización otorgada y de ser informado sobre el uso dado a los datos.

Base de Datos: Conjunto organizado de datos personales objeto de tratamiento, cualquiera sea su modalidad de creación, almacenamiento, procesamiento u organización. Podrá ser física, digital, automatizada o semiautomatizada.

Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros decide sobre la finalidad y los medios del

✍

Resolución 396 del 26 de junio de 2025
“Por medio de la cual se crea la Política de Tratamiento de Datos Personales de la E.S.E. Salud del Tundama”

tratamiento de datos personales. En el marco de esta Resolución, la E.S.E. Salud del Tundama actúa como Responsable del Tratamiento.

Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que realiza el tratamiento de datos personales por cuenta del Responsable del Tratamiento y siguiendo sus instrucciones. Debe garantizar la seguridad, confidencialidad e integridad de la información a su cargo.

Aviso de Privacidad: Comunicación verbal o escrita, física o digital, generada por el Responsable del Tratamiento y puesta a disposición del titular, mediante la cual se informa sobre la existencia de la política de tratamiento, las finalidades del tratamiento de sus datos personales y la manera de acceder a dicha política.

Tratamiento: Cualquier operación o conjunto de operaciones realizadas con datos personales, tales como recolección, almacenamiento, archivo, uso, circulación, transmisión, transferencia, actualización, consulta, supresión o disposición final.

Información Pública: Aquella que no está sujeta a reserva legal y puede ser conocida por cualquier persona, de conformidad con la Ley 1712 de 2014, sin perjuicio de la protección de datos personales que puedan encontrarse incluidos dentro de dicha información.

Información Pública Clasificada o Reservada: Información cuyo acceso puede ser negado legítimamente cuando su divulgación afecta derechos fundamentales, la seguridad nacional, la defensa, la investigación penal o cualquier otra categoría de reserva legal expresamente definida. Incluye información personal que pertenece al ámbito privado o semiprivado de una persona natural.

Seguridad de la Información: Conjunto de medidas técnicas, administrativas y organizativas adoptadas para garantizar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de los datos personales e información institucional.

Incidente de Seguridad: Cualquier evento, interno o externo, que afecte o pueda afectar la seguridad, confidencialidad, integridad, disponibilidad o legalidad del tratamiento de datos personales o bases de datos administradas por la entidad.

ARTÍCULO OCTAVO. – CAPACITACIÓN Y CULTURA. La entidad implementará programas de formación periódica para colaboradores, contratistas y terceros, con el fin de sensibilizar sobre la protección de datos, la política institucional y las obligaciones derivadas del régimen legal.

ARTÍCULO NOVENO. – MONITOREO, CUMPLIMIENTO Y REPORTE. La Gerencia de la Información establecerá mecanismos de auditoría interna, evaluación de riesgos y reporte de incidentes de seguridad, y presentará informes periódicos al Comité Institucional de Gestión y Desempeño para evaluar la efectividad de la política y promover su mejora continua.

ARTÍCULO DECIMO. – VIGENCIA. La presente resolución entra en vigencia a partir de su expedición y deroga cualquier disposición anterior que regule de forma

✍

Resolución 396 del 26 de junio de 2025
“Por medio de la cual se crea la Política de Tratamiento de Datos Personales de la E.S.E. Salud del Tundama”


contradictoria o parcial la protección de datos personales en la E.S.E. Salud del Tundama.


COMUNÍQUESE Y CÚMPLASE

Dada en Duitama a los veintiséis (26) días del mes de junio de 2025



ANDREA LILIANA ARIAS-PERDOMO
GERENTE
E.S.E SALUD DEL TUNDAMA

Proyectó: Edwin Romero Agudelo – Líder de Gerencia de la información y comunicación organizacional. 

Revisó: Sandra Avendaño Merchán - Líder Mejoramiento Continuo 

Yamile Buitrago Peralta- Líder Gestión Jurídica 