POLÍTICAS PARA EL TRATAMIENTO DE DATOS PERSONALES

1.PROPÓSITO

El propósito de la presente política es establecer los lineamientos institucionales, jurídicos, técnicos y administrativos que garanticen el cumplimiento del derecho fundamental al Hábeas Data y la adecuada protección de los datos personales que sean recolectados, almacenados, usados, circulados o suprimidos por CARDIOSALUD EJE CAFETERO S.A.S., en el desarrollo de su objeto social como institución prestadora de servicios de salud de tercer nivel.

Esta política busca:

- Asegurar que el tratamiento de los datos personales de pacientes, usuarios, colaboradores, proveedores, contratistas y demás titulares se realice conforme a los principios de legalidad, finalidad, libertad, seguridad y confidencialidad.

- Dar cumplimiento a las disposiciones de la Ley 1581 de 2012, su reglamentación y demás normas complementarias o las que la modifiquen.

- Establecer mecanismos institucionales que garanticen los derechos de los titulares frente a la recolección, almacenamiento, tratamiento y supresión de su información.

- Prevenir y mitigar riesgos derivados del tratamiento de datos personales, en especial de datos sensibles relativos a salud, historia clínica, información biométrica o laboral.

2. MARCO NORMATIVO

Esta política se enmarca en las siguientes normas nacionales e internacionales:

- Constitución Política de Colombia, artículo 15 (Derecho al Hábeas Data y a la intimidad personal y familiar).
- Ley 1266 de 2008: Disposiciones generales del hábeas data financiero.
- Ley 1273 de 2009: Delitos informáticos y protección de la información y los datos.
- Ley 1581 de 2012: Régimen general de protección de datos personales.
- Decreto 1377 de 2013: Reglamentario parcial de la Ley 1581 de 2012.

- Decreto 886 de 2014: Registro Nacional de Bases de Datos – RNBD.
- Ley 2300 de 2023: Protección del derecho a la intimidad de los consumidores frente a comunicaciones no deseadas.
- Resolución 1995 de 1999 (Ministerio de Salud): Regulación de la historia clínica.
- Decreto 1072 de 2015: Compilación normativa en materia laboral y de seguridad social.
- Circulares Externas 02 y 03 de 2018 (Superintendencia de Industria y Comercio): Buenas prácticas para el tratamiento de datos personales.

3. ALCANCE

Esta política aplica a:

- Todas las bases de datos físicas, electrónicas o mixtas bajo custodia de CARDIOSALUD.
- Todos los procesos y áreas de la organización: asistenciales, administrativos, financieros, comerciales, laborales y tecnológicos.
- Toda persona natural o jurídica, pública o privada, que actúe en calidad de responsable o encargado del tratamiento por cuenta de CARDIOSALUD.

Su cumplimiento es obligatorio para directivos, miembros de la asamblea general de accionistas, colaboradores, contratistas, estudiantes en práctica, proveedores y terceros que tengan acceso a datos personales de los cuales CARDIOSALUD sea responsable o custodio.

4. RESPONSABLE DEL TRATAMIENTO

CARDIOSALUD EJE CAFETERO S.A.S. es la responsable del tratamiento de la información personal que administra.
NIT: 900.346.953-4
Domicilio: Pereira, Risaralda
Dirección: Carrera 13 N.º 3B-12, Av. Circunvalar
Teléfonos: (606) 3419028 – 3218525751 – 3104649235
Correo electrónico institucional: citasmedicas@cardiosaludeje.com.co
Representante Legal: LORSIS ANTONIO MARULANDA DURANGO
Calidad institucional: Entidad de salud habilitada.

5. PRINCIPIOS RECTORES DEL TRATAMIENTO

De conformidad con el artículo 4 de la Ley 1581 de 2012 y el Decreto 1377 de 2013, CARDIOSALUD se compromete a observar los siguientes principios:

Legalidad: Ningún tratamiento podrá realizarse sin fundamento en una norma legal o reglamentaria.

Finalidad: El tratamiento debe obedecer a una finalidad legítima, explícita, informada y proporcional al objeto social.

Libertad: Solo se efectuará con consentimiento previo, expreso e informado del titular, salvo mandato legal.

Veracidad o calidad: Los datos serán veraces, completos, actualizados, comprobables y comprensibles.

Transparencia: Se garantizará al titular el derecho a obtener información sobre el tratamiento en cualquier momento.

Acceso y circulación restringida: Solo accederán las personas autorizadas por el titular o por la ley.

Seguridad: Se implementarán medidas técnicas, humanas y administrativas para proteger los datos.

Confidencialidad: Quienes intervengan en el tratamiento guardarán reserva incluso después de finalizada su relación.

Temporalidad: Los datos se conservarán por el tiempo necesario para cumplir la finalidad o las normas legales.

Responsabilidad demostrada: CARDIOSALUD evidenciará, mediante políticas, auditorías y registros, su cumplimiento normativo (principio de accountability).

Proporcionalidad: El tratamiento se limitará a los datos estrictamente necesarios para el fin perseguido.

Legalidad en la recolección: Los datos se obtendrán por medios legítimos y lícitos.

6. DEFINICIONES

A los efectos de esta política, se adoptan las siguientes definiciones:

Autorización: Consentimiento previo, expreso e informado del titular para el tratamiento de sus datos personales.

Aviso de privacidad: Comunicación verbal o escrita que informa al titular sobre la existencia de políticas de tratamiento.

Base de datos: Conjunto organizado de datos personales sometido a tratamiento.

Dato personal: Información vinculada o asociable a una persona natural determinada o determinable.

Dato sensible: Información que afecta la intimidad del titular o cuyo uso indebido puede generar discriminación (salud, creencias, orientación sexual, datos biométricos, etc.).

Dato público: Información considerada pública por mandato legal o constitucional (estado civil, profesión, condición de servidor público).

Encargado del tratamiento: Persona natural o jurídica que realiza el tratamiento por cuenta del responsable.

Responsable del tratamiento: Persona natural o jurídica que decide sobre la base de datos y su tratamiento.

Titular: Persona natural cuyos datos personales son objeto de tratamiento.

Tratamiento: Cualquier operación sobre datos personales: recolección, almacenamiento, uso, circulación, supresión o transferencia.

Transferencia: Envío de datos a otro responsable ubicado dentro o fuera del país.

Transmisión: Comunicación de datos personales a un encargado para su tratamiento por cuenta del responsable.

Anonimización: Proceso de eliminación o modificación de información que impida identificar al titular.

Datos biométricos: Características físicas o conductuales que permiten identificar a una persona (huellas, rostro, iris, voz).

7. CLASIFICACIÓN Y CATEGORÍAS DE DATOS PERSONALES RECOLECTADOS

CARDIOSALUD, en cumplimiento de su objeto social y funciones institucionales, podrá recolectar, almacenar y tratar las siguientes categorías de datos personales:

7.1 Datos de identificación

Nombre, apellidos, tipo y número de documento de identidad, fecha y lugar de nacimiento, edad, género, firma, estado civil, nacionalidad y ocupación.

7.2 Datos de contacto

Dirección de correspondencia, teléfonos fijos o móviles, correo electrónico personal o corporativo y lugar de residencia.

7.3 Datos laborales

Cargo, historia laboral, afiliaciones, desempeño, información de ingresos y egresos, antecedentes disciplinarios, evaluaciones de desempeño, control de asistencia, ausentismo, licencias, incapacidades y demás relacionados con el vínculo laboral.

7.4 Datos financieros y tributarios

Información bancaria, número de cuenta, ingresos, egresos, retenciones, RUT, información contable, tributaria y contractual.

7.5 Datos de salud

Información médica, historia clínica, diagnósticos, tratamientos, resultados de laboratorio, antecedentes médicos, incapacidades y datos requeridos para atención en salud conforme a la Resolución 1995 de 1999.

7.6 Datos biométricos

Imágenes, videos, voz, huellas dactilares, rostro, firma digital o electrónica y otros elementos que permitan la identificación física o electrónica de una persona.

7.7 Datos familiares y de emergencia

Nombres y contactos de familiares, beneficiarios o personas a notificar en caso de urgencia.

7.8 Datos académicos

Formación profesional, títulos obtenidos, certificaciones, calificaciones, constancias de estudios y antecedentes académicos.

8. FINALIDADES DEL TRATAMIENTO

CARDIOSALUD actuará como responsable del tratamiento de los datos personales, y usará la información recolectada exclusivamente para los fines legales, contractuales y administrativos descritos a continuación:

8.1 Pacientes y/o usuarios

- Prestar servicios médicos asistenciales, diagnósticos y terapéuticos[U1].
- Gestionar historias clínicas conforme a la Resolución 1995 de 1999 y demás normas del sector salud.
- Procesar autorizaciones, glosas y facturación.
- Coordinar citas, recordatorios y seguimiento a tratamientos.

- Realizar auditorías médicas y controles de calidad.
- Cumplir con obligaciones derivadas de convenios con EPS, ARL, IPS o entidades territoriales.
- Efectuar reportes al SISPRO, RIPS, Ministerio de Salud, INVIMA y demás autoridades competentes.
- Realizar estudios epidemiológicos, estadísticos y de mejoramiento del servicio.

8.2 Colaboradores, practicantes y contratistas

- Administración del personal, nómina, pagos y prestaciones.
- Afiliación a EPS, ARL, fondos de pensión y caja de compensación.
- Evaluación de desempeño, control de asistencia y bienestar laboral.
- Cumplimiento de obligaciones laborales y tributarias.
- Control de ingreso, videovigilancia y seguridad en las instalaciones.
- Prevención de fraude, lavado de activos y corrupción.
- Cumplimiento de políticas internas y del reglamento de trabajo.

- Atención de emergencias, incapacidades y procedimientos médicos.
- Implementación de planes de formación y capacitación.

8.3 Proveedores y clientes

- Gestión de compras, contratación, pagos, recepción de bienes y servicios.
- Cumplimiento de obligaciones comerciales, contables y tributarias.
- Evaluación de calidad, auditorías y control de cumplimiento contractual.
- Comunicación institucional y envío de información sobre servicios.
- Verificación de antecedentes financieros y comerciales.

8.4 Accionistas y miembros de junta

- Administración del libro de accionistas y convocatoria a asambleas.
- Cumplimiento de disposiciones mercantiles y contables.
- Envío de información societaria, estados financieros y actas.
- Registro de participación, votaciones y decisiones corporativas.

8.5 Visitantes y terceros

- Control de acceso físico y digital a las instalaciones.
- Protección de personas, bienes e información.
- Cumplimiento de protocolos de bioseguridad y vigilancia.

9. TRATAMIENTO DE DATOS SENSIBLES

Los datos sensibles —especialmente aquellos relacionados con la salud, la orientación sexual, la religión, las creencias, la vida familiar o los datos biométricos— tendrán un tratamiento restringido y reforzado, conforme a los artículos 5 y 6 de la Ley 1581 de 2012.

9.1 Requisitos para el tratamiento

Solo podrán ser tratados cuando:

- El titular otorgue autorización previa, expresa e informada.
- Sea necesario para salvaguardar el interés vital del titular o de un tercero.
- Sea indispensable para el reconocimiento o defensa de un derecho en proceso judicial o administrativo.
- Exista mandato legal o judicial que lo ordene.
- Tenga finalidad médica, científica o sanitaria, bajo obligación de confidencialidad.

9.2 Protección reforzada

CARDIOSALUD aplicará medidas especiales de seguridad, acceso restringido, control de perfiles y cifrado de información en bases de datos que contengan información sensible o médica.

10. TRATAMIENTO DE DATOS DE NIÑOS, NIÑAS Y ADOLESCENTES

CARDIOSALUD solo tratará datos personales de menores de edad cuando:

- Exista autorización expresa del representante legal.
- El tratamiento responda al interés superior del menor.
- Los datos sean necesarios para la prestación de servicios asistenciales o educativos.
- Se garantice la protección integral de sus derechos fundamentales.
- La información recolectada se usará exclusivamente con fines médicos, académicos o de bienestar social, prohibiéndose su uso con fines comerciales o de mercadeo.

11. DERECHOS DE LOS TITULARES

De conformidad con el artículo 8 de la Ley 1581 de 2012, los titulares tienen derecho a:

- Conocer, actualizar y rectificar sus datos personales frente a CARDIOSALUD.
- Solicitar prueba de la autorización otorgada.
- Ser informados del uso dado a sus datos personales.
- Presentar quejas ante la Superintendencia de Industria y Comercio por infracciones.
- Revocar la autorización o solicitar la supresión del dato.
- Acceder de manera gratuita a la información que repose en las bases de datos.
- Oponerse al tratamiento cuando no exista consentimiento o finalidad legítima.
- Solicitar corrección oficiosa cuando la información sea inexacta, incompleta o desactualizada.

12. AUTORIZACIÓN PARA EL TRATAMIENTO

Previo a cualquier tratamiento, CARDIOSALUD solicitará la autorización libre, previa, expresa e informada del titular, mediante medios escritos, físicos, electrónicos o

digitales.
La autorización incluirá:

- Finalidades del tratamiento.
- Derechos del titular.
- Mecanismos para ejercerlos.
- Identificación del responsable.
- La prueba de autorización será conservada física o digitalmente, garantizando su trazabilidad y custodia.

13. AVISO DE PRIVACIDAD

El aviso de privacidad es el documento mediante el cual CARDIOSALUD informa a los titulares sobre la existencia de esta política y las condiciones del tratamiento.
Debe contener:

Identificación del responsable.
Finalidades del tratamiento.
Derechos del titular.
Procedimiento para ejercerlos.
Canales de contacto.

14. DEBERES DE CARDIOSALUD COMO RESPONSABLE

De acuerdo con el artículo 17 de la Ley 1581 de 2012, CARDIOSALUD se compromete a:

- Garantizar al titular el ejercicio pleno de sus derechos.
- Solicitar y conservar copia de la autorización.
- Informar la finalidad del tratamiento.
- Conservar la información bajo condiciones de seguridad.
- Actualizar y rectificar los datos cuando sea necesario.
- Tramitar consultas y reclamos en los términos legales.
- Reportar incidentes de seguridad a la SIC.
- Cumplir las instrucciones de la autoridad de protección de datos.
- Implementar programas de capacitación interna.
- Mantener registro de auditorías y evidencias de cumplimiento.

15. DEBERES DEL ENCARGADO DEL TRATAMIENTO

De conformidad con el artículo 18 de la Ley 1581 de 2012, quien actúe como

encargado deberá:

- Tratar los datos conforme a las instrucciones del responsable.
- Garantizar la confidencialidad y seguridad de la información.
- Abstenerse de circular datos sin autorización del responsable.
- Permitir auditorías del responsable o de la SIC.
- Eliminar o devolver la información cuando finalice el encargo.
- Reportar incidentes o vulneraciones de seguridad inmediatamente.
- Colaborar con la atención de peticiones, consultas y reclamos.

16. MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN

CARDIOSALUD adopta medidas administrativas, humanas, físicas y tecnológicas para garantizar la seguridad e integridad de los datos personales:

- Control de acceso por roles y credenciales seguras.
- Políticas de contraseñas robustas.
- Cifrado de datos sensibles.
- Copias de seguridad automáticas y almacenamiento cifrado.
- Monitoreo y auditorías de acceso.
- Eliminación segura de información (borrado certificado o destrucción física).
- Prohibición de uso de dispositivos personales para almacenar información institucional.
- Protocolos de respuesta a incidentes y violaciones de seguridad.
- Protocolo para el reporte inmediato de incidentes a la SIC y a los titulares cuando se comprometan datos sensibles.

17. CONSERVACIÓN Y SUPRESIÓN DE DATOS

17.1 Conservación

- Historias clínicas: mínimo 10 años desde la última atención (Res. 1995/1999).
- Documentos laborales: mínimo 20 años (Decreto 1072/2015).
- Registros contables y fiscales: según los plazos establecidos por la DIAN.
- Información contractual: por la vigencia del contrato y cinco años adicionales.

17.2 Supresión

Los datos personales se eliminarán cuando:

- Haya sido alcanzada la finalidad para la cual fueron recolectados.
- Se revoque la autorización del titular.
- Exista orden de autoridad competente.
- La supresión se realizará mediante técnicas seguras y verificables.

18. PROCEDIMIENTO PARA EL EJERCICIO DE LOS DERECHOS DE LOS TITULARES

CARDIOSALUD EJE CAFETERO S.A.S. garantiza el ejercicio pleno de los derechos de los titulares mediante los siguientes mecanismos de atención:

18.1 Canales de atención

Correo electrónico: citasmedicas@cardiosaludeje.com.co[U2]

Dirección física: Carrera 13 N.º 3B-12, Av. Circunvalar – Pereira, Risaralda.

Teléfonos: (606) 3419028 – 3218525751 – 3104649235

Horario de atención: lunes a viernes de 8:00 a.m. a 5:00 p.m.

18.2 Consultas

Los titulares podrán consultar la información personal que repose en las bases de datos de CARDIOSALUD.

La respuesta se dará en un término máximo de diez (10) días hábiles, contados a partir de la fecha de recibo.

Si no fuere posible responder dentro del término, se informará al interesado el motivo de la demora y la fecha de respuesta, que no podrá superar cinco (5) días hábiles adicionales.

18.3 Reclamos

Los titulares podrán presentar reclamos cuando consideren que la información contenida en las bases de datos debe ser corregida, actualizada o suprimida, o

cuando adviertan incumplimiento de los deberes legales.
El reclamo deberá presentarse por escrito, con identificación del titular, descripción de los hechos y pruebas.
Si el reclamo está incompleto, se requerirá al interesado dentro de los cinco (5) días hábiles siguientes a su recepción.
Si transcurren dos (2) meses sin respuesta, se entenderá que desistió de su reclamo.
El término máximo para atender el reclamo será de quince (15) días hábiles, prorrogables por ocho (8) días hábiles adicionales, previa justificación.
Cuando el reclamo esté en trámite, CARDIOSALUD incluirá la leyenda "reclamo en trámite" en la base de datos correspondiente.

18.4 Revocatoria y supresión

El titular podrá solicitar en cualquier momento la revocatoria de la autorización o la supresión de sus datos personales cuando no exista deber legal o contractual que lo impida.
En caso de persistir una obligación legal, la información será bloqueada o archivada bajo reserva.

19. TRANSFERENCIA Y TRANSMISIÓN DE DATOS PERSONALES

CARDIOSALUD podrá realizar transferencias y transmisiones nacionales o internacionales de datos personales, siempre que se cumplan los estándares previstos en los artículos 25 y 26 del Decreto 1377 de 2013.

19.1 Transferencia internacional

Se entenderá como la comunicación de datos personales a otro responsable ubicado fuera del territorio nacional.

CARDIOSALUD solo transferirá datos a países que proporcionen niveles adecuados de protección o cuenten con cláusulas contractuales que garanticen los mismos estándares exigidos por la Ley 1581 de 2012.

19.2 Transmisión internacional

Corresponde al tratamiento de datos personales por parte de un encargado ubicado fuera del país, que actúa por cuenta de CARDIOSALUD.
En estos casos, se suscribirá un contrato de transmisión internacional que establezca:

- Finalidades, obligaciones y duración del tratamiento.
- Niveles de seguridad.
- Medidas de confidencialidad.
- Restricciones sobre el uso de la información.

20. RESPONSABILIDAD DEMOSTRADA Y AUDITORÍA INTERNA

CARDIOSALUD implementará un sistema de responsabilidad demostrada (accountability) en materia de protección de datos, mediante:

- Políticas internas documentadas de seguridad y confidencialidad.
- Mapeo de riesgos asociados al tratamiento de datos personales.
- Capacitaciones periódicas a todos los empleados y contratistas.
- Designación de un delegado o responsable de protección de datos personales (DPO) dentro del área administrativa.
- Auditorías anuales para verificar cumplimiento normativo.
- Plan de mejora contínua basado en hallazgos de auditoría.
- Matriz de riesgos y controles conforme a los lineamientos ISO 27001 e ISO 27701.
- Registro de incidentes de seguridad y sus medidas correctivas.
- La coordinación de servicio[U3] y de sistemas será responsable de coordinar las auditorías y reportes de cumplimiento ante la dirección general y la SIC.

21. INCUMPLIMIENTOS Y SANCIONES

El incumplimiento de las disposiciones contenidas en esta política se considera falta grave, conforme al Reglamento Interno de Trabajo y a la Ley 1581 de 2012, artículo 23.

21.1 Sanciones internas

- Amonestaciones escritas.
- Suspensión o terminación del vínculo laboral o contractual.
- Reporte al área de cumplimiento y control interno.

Estas sanciones no excluyen la responsabilidad civil, penal o administrativa derivada del mal uso de información.

22. CONTROL DE CAMBIOS Y VIGILANCIA NORMATIVA

CARDIOSALUD establecerá un proceso permanente de vigilancia normativa para actualizar esta política cada vez que se expidan nuevas leyes o decretos en materia de protección de datos.

Toda modificación será informada a los titulares mediante los canales institucionales (página web, correo electrónico o carteleras internas).

El control documental será gestionado por la coordinación de servicio.[U4]

23. DIVULGACIÓN Y CUMPLIMIENTO

La política será divulgada a través de:

- Página web institucional.
- Inducciones y capacitaciones internas.
- Contratos laborales y comerciales (cláusula de protección de datos).
- Puntos de atención al usuario y recepción.

El desconocimiento de esta política no exime de su cumplimiento a ningún empleado o contratista.

24. MODIFICACIONES Y ACTUALIZACIONES

CARDIOSALUD podrá modificar unilateralmente esta política por razones normativas, tecnológicas o institucionales.

Toda actualización incluirá:

Fecha de modificación.
Versión y código documental.
Descripción de los cambios realizados.
Los cambios serán aprobados por la Dirección General y registrados en la tabla de control de cambios del formato PP-FO-003.

25. VIGENCIA

Esta política entra en vigor a partir del 6 de noviembre de 2025 y permanecerá vigente mientras CARDIOSALUD EJE CAFETERO S.A.S. desarrolle actividades que impliquen tratamiento de datos personales o hasta que sea sustituida por una nueva versión.

CONTROL DE CAMBIOS

Versión	Fecha	Descripción de cambios
1	10-11-2022	Creación de documento
2	26-08-2023	Ajuste a estructura y normatividad
3	06-11-2025	Ajuste de normatividad