POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

ESTERIMED SERVICIOS DE ESTERILIZACIÓN CIA. LTDA.

Contenido

1. Presentación ... 3
1.1 Identificación detallada de la organización Responsable del Tratamiento de sus datos personales. ... 3
2. Objeto ... 3
3. Ámbito de Aplicación ... 3
4. Responsabilidades ... 4
5. Definiciones ... 6
6. Principios de Protección de Datos ... 7
7. Datos Personales ... 8
8. Limitación y Minimización de Datos ... 10
9. Transparencia y Finalidad del Tratamiento ... 10
10. Delegado de Protección de Datos personales ... 11
11. Obtención del consentimiento ... 12
12. Tratamiento de datos personales en apego a la LOPDP ... 12
12.1 Recolección de Datos ... 12
12.2 Almacenamiento y Conservación ... 13
12.3 Uso Interno de Datos ... 13
12.4 Transmisión Internacional de Datos ... 13
12.5 Comunicación y Acceso por Terceros ... 14
12.6 Procesos de Facturación ... 14
12.7 Tratamiento de Datos Sensibles ... 15
12.8 Monitoreo, Videovigilancia y Control de Accesos ... 15
12.9 Modificación y Actualización de Datos ... 15
12.10 Eliminación y anonimización ... 15
12.11 Atención de Derechos del Titular ... 16
12.11.1 Solicitudes incompletas o insuficientes ... 17
12.12 Gestión de Incidentes y Brechas de Seguridad ... 18
12.13 Auditorías, Supervisión y Mejora Continua ... 19

13. Seguridad de la información y confidencialidad de los Datos 19
14. Tratamiento por Terceros y Encargados 19
15. Derechos del Titular 19
16. Compromiso Institucional 21
17. Control de cambios 21
18. Firmas de responsabilidad 21

1. Presentación

ESTERIMED SERVICIOS DE ESTERILIZACIÓN CIA. LTDA. es una empresa ecuatoriana especializada en la prestación de servicios de esterilización y acondicionamiento de productos mediante procesos controlados orientados a preservar las condiciones requeridas para su posterior utilización por organizaciones de los sectores salud, industrial y comercial.

En cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP) y demás normativa aplicable, la organización establece la presente Política de Protección de Datos Personales con el propósito de informar los lineamientos que rigen el tratamiento de los datos personales dentro de sus actividades.

1.1 Identificación detallada de la organización Responsable del Tratamiento de sus datos personales.

- Razón social: ESTERIMED SERVICIOS DE ESTERILIZACIÓN CIA. LTDA.
- RUC: 1792738792001
- Actividades económicas:
  - C13130202 - SERVICIO DE APRESTO, SECADO, VAPORIZADO, ENCOGIMIENTO, REALIZADO POR TERCEROS A CAMBIO DE UNA RETRIBUCIÓN O POR CONTRATO.
  - S96090705 - ACTIVIDADES DE SERVICIOS DIVERSOS.
- Domicilio:
  PICHINCHA – QUITO. Parroquia: CONOCOTO; Dirección: Calle: FRANCISCO DE ORELLANA; Número: LT208; Intersección: FERNANDO DE MAGALLAN; Referencia: diagonal a la empresa A GAS CIA LTDA
- Teléfono: 022836032
- Página web: https://dhisve.com/
- Delegado de Protección de Datos personales (DPD): Byron Vásconez Martínez
- Correo electrónico para atención ciudadana: protecciondedatos.dhisve@outlook.com
- Formulario de derechos de titulares de datos personales: FORMULARIO - DERECHOS DE TITULARES DE DATOS PERSONALES: Rellenar formulario

2. Objeto

Esta Política establece los lineamientos obligatorios que debe aplicar Esterimed Servicios de Esterilización Cia. Ltda., para garantizar la protección de los datos personales en todas las fases del ciclo de vida del tratamiento, incorporando la LOPDP, su Reglamento General y la Guía de Protección de Datos desde el Diseño y por Defecto.

3. Ámbito de Aplicación

Este documento abarca a los datos personales recogidos de sus empleados, contratistas, aspirantes, clientes, usuarios, proveedores, aliados y/o terceros en general, sujetándose a lo dispuesto por la Ley ecuatoriana.

La LOPDP no protege los datos de las personas jurídicas, dado que estos no se consideran datos personales. Por lo tanto, quedan fuera del alcance de esta política:

- Razón social
- RUC de la empresa
- Dirección comercial
- Teléfonos institucionales
- Correos corporativos genéricos (p. ej., *contacto@empresa.com*)
- Información financiera, contractual o comercial referente únicamente a la persona jurídica
- Certificaciones, permisos, licencias, registros y documentación legal empresarial

Esta información podrá ser tratada sin requerir bases de licitud de tipo personal ni el ejercicio de derechos de titularidad, sin perjuicio de las obligaciones de confidencialidad, seguridad o contractual aplicables por otros marcos normativos.

No obstante, cuando dichos documentos contengan datos personales de personas naturales (por ejemplo, nombres, firmas, números de identificación u otra información asociada a individuos), estos datos sí estarán sujetos a lo dispuesto en la LOPDP y a las medidas de protección establecidas en la presente política.

4. Responsabilidades

- Dirección: Aprobar y respaldar esta Política de Protección de Datos; Asignar los recursos necesarios (humanos, tecnológicos, financieros) para su implementación; Fomentar una cultura organizacional orientada a la privacidad, seguridad y responsabilidad en el tratamiento de datos personales; Asegurar que las decisiones estratégicas consideren el principio de protección de datos desde el diseño y por defecto; Supervisar el desempeño del Delegado de Protección de Datos (DPD), cuando aplique.
- Empresa Responsable del Tratamiento: Como responsable del tratamiento, Esterimed Servicios de Esterilización Cia. Ltda. debe:
  - ✓ Garantizar la licitud del tratamiento de datos personales.
  - ✓ Asegurar que las finalidades sean claras, legítimas y transparentes.
  - ✓ Implementar controles jurídicos, organizacionales y técnicos adecuados.
  - ✓ Mantener actualizado el Registro de Actividades de Tratamiento (RAT) cuando corresponda.
  - ✓ Realizar Evaluaciones de Impacto a la Protección de Datos (EIPD) cuando corresponda.
  - ✓ Supervisar la gestión de incidentes y, de ser necesario, efectuar notificaciones a la autoridad y titulares.
  - ✓ Documentar evidencias que demuestren cumplimiento.

- Delegado de Protección de Datos (DPO):
  - ✓ Actuar como punto de contacto entre la Empresa, los titulares y la Autoridad de Protección de Datos.

- ✓ Supervisar la correcta aplicación de esta Política.
- ✓ Asesorar en evaluaciones de impacto, gestión de riesgos y controles de privacidad.
- ✓ Emitir recomendaciones independientes y velar por su implementación.
- ✓ Revisar incidentes de seguridad y procesos de notificación.
- ✓ Coordinar auditorías internas.

- Encargados del Tratamiento

  Los proveedores o terceros que traten datos por cuenta de la Empresa deben:
  - ✓ Cumplir estrictamente las instrucciones documentadas emitidas por la Empresa.
  - ✓ Implementar medidas de seguridad equivalentes o superiores a las de la Empresa.
  - ✓ Garantizar la confidencialidad del personal involucrado.
  - ✓ Permitir auditorías y verificaciones.
  - ✓ Eliminar o devolver los datos al culminar la relación contractual.
  - ✓ Notificar incidentes de seguridad de forma inmediata y oportuna.
  - ✓ Asesoría preventiva en la elaboración de documentos contractuales que impliquen tratamiento de datos personales.

- Responsable de Seguridad de TICs

  - ✓ Implementar controles Zero Trust, autenticación fuerte, monitoreo continuo y segmentación de accesos.
  - ✓ Garantizar cifrado en tránsito y reposo.
  - ✓ Mantener inventario de activos tecnológicos, respaldos seguros.
  - ✓ Monitorear amenazas cibernéticas para implementar medidas de control y prevención.
  - ✓ Actualizar y parchear sistemas para evitar vulnerabilidades.
  - ✓ Colaborar activamente con el DPD y líderes de procesos.

- Líderes de Procesos

  - ✓ Asegurar que el tratamiento de datos en su área cumpla las finalidades declaradas.
  - ✓ Validar que la información recolectada sea pertinente y mínima.
  - ✓ Reportar incidentes o riesgos al DPD y a TICs.
  - ✓ Garantizar que su personal reciba capacitación sobre privacidad y seguridad.

- Colaboradores de la Empresa

  - ✓ Cumplir esta Política y las normas internas relacionadas.
  - ✓ Acceder y tratar los datos personales únicamente para fines autorizados por su rol.

- ✓ Mantener absoluta confidencialidad de la información a la que acceden.
- ✓ Proteger credenciales de acceso y evitar compartirlas.
- ✓ Reportar inmediatamente cualquier incidente o sospecha de vulneración.
- ✓ Participar en capacitaciones obligatorias.

- Usuarios, clientes y otras partes interesadas externas a la organización

Aunque no forman parte interna de la organización, se solicitará que:

- ✓ Brinden datos veraces y actualizados.
- ✓ Utilicen los canales adecuados para ejercer sus derechos.
- ✓ Respeten los mecanismos de seguridad establecidos por la Empresa.
- ✓ Conozcan y acepten la Política de Protección de datos

5. Definiciones

- **Dato Personal**: Cualquier información que identifique o permita identificar, directa o indirectamente, a una persona natural.
- **Dato Sensible**: Información cuya revelación pueda afectar derechos fundamentales del titular, como datos de salud, biométricos, origen étnico, creencias, orientación sexual, entre otros.
- **Titular de los Datos**: Persona natural a quien pertenecen los datos personales objeto de tratamiento.
- **Tratamiento de Datos**: Cualquier operación sobre datos personales, como recolección, almacenamiento, uso, modificación, transmisión, eliminación o consulta.
- **Responsable del Tratamiento**: Persona natural o jurídica que decide las finalidades y medios del tratamiento de datos personales.
- **Encargado del Tratamiento**: Persona natural o jurídica que realiza el tratamiento por cuenta del responsable, siguiendo sus instrucciones.
- **Delegado de Protección de Datos (DPO/DPD):** Persona encargada de supervisar, asesorar y verificar el cumplimiento de la normativa y de esta política en materia de protección de datos personales.
- **Consentimiento**: Manifestación libre, específica, informada e inequívoca mediante la cual el titular acepta el tratamiento de sus datos personales.
- **Finalidad del Tratamiento**: Propósito específico, explícito y legítimo para el cual se recopilan y procesan los datos personales.
- **Base de Licitud**: Fundamento jurídico que permite el tratamiento de datos, como consentimiento, obligación legal, contrato, interés legítimo o protección de intereses vitales.
- **Minimización de Datos**: Principio que exige recolectar únicamente los datos estrictamente necesarios para cumplir una finalidad legítima.

- **Privacidad desde el Diseño (Privacy by Design):** Obligación de incorporar medidas de protección de datos desde la concepción y planificación de un proyecto o proceso.
- **Privacidad por Defecto (Privacy by Default):** Configuración inicial de sistemas y procesos para que el nivel más alto de privacidad se aplique automáticamente.
- **Arquitectura Zero Trust:** Estrategia que asume que no existe confianza implícita y que todo acceso debe verificarse continuamente.
- **Evaluación de Impacto a la Protección de Datos (EIPD):** Análisis obligatorio cuando el tratamiento implique riesgos altos para los derechos del titular, especialmente en datos sensibles o monitoreo sistemático.
- **Registro de Actividades de Tratamiento (RAT):** Documento esencial donde se detallan todas las operaciones de tratamiento realizadas por la empresa.
- **Incidente de Seguridad**: Evento que compromete o puede comprometer la confidencialidad, integridad o disponibilidad de datos personales.
- **Brecha de Seguridad de Datos Personales**: Acceso no autorizado, pérdida, filtración o alteración de datos personales que afecta a los titulares.
- **Medidas Técnicas de Seguridad**: Controles tecnológicos como cifrado, autenticación multifactor, ofuscación, control de accesos y monitoreo continuo.
- **Medidas Organizacionales de Seguridad**: Políticas, procedimientos, entrenamiento y roles definidos para proteger los datos personales.
- **Seudonimización**: Proceso mediante el cual un dato personal no puede atribuirse a un titular sin información adicional.
- **Anonimización**: Transformación irreversible de datos personales para que no sea posible identificar al titular.
- **Tecnologías de Mejora de la Privacidad (PETs**): Herramientas como privacidad diferencial, encriptación, mascaramiento y agregación para reducir la exposición de datos.
- **Tercero Receptor**: Persona o entidad diferente del titular, responsable o encargado a quien se comunican o transfieren datos personales.
- **Transferencia Internacional de Datos**: Envío de datos personales a otro país o a organizaciones internacionales, sujeto a garantías especiales.
- **Derechos del Titular (ARCO y otros):** Derechos a acceso, rectificación, actualización, eliminación, oposición, portabilidad, suspensión y a no ser objeto de decisiones automatizadas.
- **Conflicto de Interés en Protección de Datos:** Situación en la que una función, rol o actividad compromete la independencia necesaria para supervisar adecuadamente el tratamiento.

6. Principios de Protección de Datos

La Empresa incorpora los siguientes principios, garantizando minimización, acceso limitado y seguridad por defecto.



7. Datos Personales

La organización, reconoce que los datos personales constituyen información esencial vinculada a la dignidad, autonomía y derechos de cada titular. Por ello, el tratamiento de esta información se realizará con estricta sujeción a la Ley Orgánica de Protección de Datos Personales (LOPDP), su Reglamento General y demás normativa aplicable.

Los datos personales pueden incluir, entre otros:

- Datos de identificación
- Datos de contacto
- Datos laborales
- Datos financieros
- Datos sensibles, especialmente relacionados con salud, biometría o información requerida para actividades sanitarias, regulatorias o logísticas
- Datos generados en contextos de transporte, distribución o comercialización de dispositivos médicos. Por ejemplo, firmas de recepción.
- Datos derivados del uso de sistemas, accesos o monitoreo para fines de seguridad
- Datos de menores de edad (Solo los necesarios para el cumplimiento de obligaciones contractuales como afiliación al seguro médico, pago de utilidades, entre otras).

Todos los datos serán tratados exclusivamente conforme a las finalidades previamente informadas al titular y autorizadas mediante las bases de licitud aplicables.

7.1. Datos Sensibles

En cumplimiento del Art. 4 y siguientes de la LOPDP, la Empresa reconoce que los datos sensibles requieren un nivel de protección reforzado debido al impacto que su divulgación podría tener en los derechos de los titulares.

Para este tipo de datos se adoptarán las siguientes consideraciones:

- Se recabarán únicamente cuando sean estrictamente necesarios.
- Su tratamiento requerirá consentimiento expreso, salvo excepciones legales.
- Se aplicarán medidas de seguridad adecuadas y proporcionales al riesgo
- Se evaluarán riesgos mediante Evaluaciones de Impacto (EIPD) cuando corresponda.
- Su acceso estará restringido al personal estrictamente autorizado.

7.2. Tratamiento de datos de personas en situación de vulnerabilidad

La organización reconoce que determinadas personas pueden encontrarse en situación de vulnerabilidad respecto del tratamiento de sus datos personales, ya sea por su edad, condición personal, relación de dependencia, contexto socioeconómico o por la naturaleza de los datos tratados.

En estos casos, la organización aplicará medidas reforzadas de protección, con el fin de salvaguardar los derechos y libertades de los titulares y garantizar un tratamiento justo, lícito, proporcional y transparente. Para menores de edad se exige consentimiento previo del representante legal con verificación de representación y tratamiento reforzado.

Se consideran, entre otros, como personas en situación de vulnerabilidad:

- niñas, niños y adolescentes;
- personas adultas mayores;
- personas con discapacidad;
- personas cuyos datos correspondan a categorías especiales o datos sensibles;
- personas que se encuentren en una relación de dependencia o subordinación frente a la organización;

Cuando el tratamiento involucre personas en situación de vulnerabilidad, la organización evaluará la necesidad de realizar una Evaluación de Impacto en la Protección de Datos Personales (EIPD) y documentará las medidas adoptadas para mitigar los riesgos identificados.

8. Limitación y Minimización de Datos

La Empresa asegura que:

- No se tratarán datos innecesarios, excesivos o no relacionados con la finalidad informada.
- Solo se recolectarán los datos mínimos indispensables para la operación, especialmente en procesos donde intervienen terceros, proveedores logísticos o autoridades sanitarias.
- Toda información no esencial será eliminada conforme a las políticas de retención y eliminación segura.

9. Transparencia y Finalidad del Tratamiento

La Empresa garantizará que todo tratamiento se rija por los principios de:

- Lealtad y legalidad
- Transparencia
- Limitación de la finalidad
- Minimización de datos
- Exactitud y actualización
- Limitación del plazo de conservación
- Integridad y confidencialidad

Antes de iniciar cualquier tratamiento, el titular será informado sobre:

- La identidad del responsable
- Las finalidades del tratamiento presentación y tratamiento reforzado.
- Las bases legales aplicables
- Las categorías de datos tratados
- Los derechos que le asisten

- La posible transferencia nacional o internacional de sus datos

La organización garantiza que todo tratamiento de datos personales se realiza sobre la base de una causa legítima prevista en la Ley Orgánica de Protección de Datos Personales. Para cada actividad de tratamiento, la organización identifica, documenta y conserva evidencia de la base de licitud aplicable, asegurando que dicha base sea adecuada, proporcional y coherente con la finalidad del tratamiento.

Las bases de licitud utilizadas incluyen, entre otras: el cumplimiento de una obligación legal; la ejecución de una relación contractual o precontractual; el consentimiento libre, específico, informado e inequívoco del titular; el interés legítimo del responsable, debidamente ponderado; la protección de intereses vitales del titular o de terceros.

Cuando exista una relación de dependencia o subordinación entre el titular y la organización, el consentimiento no será utilizado como base principal del tratamiento, salvo que se demuestre que ha sido otorgado de manera libre y sin condicionamiento.

La base de licitud correspondiente a cada actividad de tratamiento se encuentra documentada en los registros internos de tratamiento y es revisada periódicamente.

Actividad	Tipo de datos	Base de licitud	J6ustificación
Gestión de talento humano	Datos personales comunes y sensibles	Obligación legal, relación contractual	Cumplimiento de normativas laborales y contractuales.
Videovigilancia	Imagen / biométricos	Interés legítimo. Normativas sobre prevención de delitos	Seguridad de personas e instalaciones. Prevención de delitos
Gestión de clientes	Datos personales	Relación contractual.	Prestación del servicio. Emisión de comprobantes y obligaciones tributarias.
Gestión de proveedores	Datos personales	Relación contractual, interés legítimo	Transaccional: Ejecución de contratos, otorgamiento de crédito

10. Delegado de Protección de Datos personales

La organización designa un Delegado de Protección de Datos Personales (DPD) cuando así lo exija la Ley Orgánica de Protección de Datos Personales o cuando, por la naturaleza, alcance, contexto o fines del tratamiento, resulte necesario para garantizar una adecuada protección de los datos personales.

El DPD actuará con independencia funcional, sin recibir instrucciones respecto al ejercicio de sus funciones, y contará con acceso directo a la alta dirección de la organización.

La organización garantizará que el DPD no se encuentre en situación de conflicto de interés. En particular, no desempeñará funciones que impliquen la determinación de los fines o medios del tratamiento de datos personales.

El DPD contará con los recursos humanos, técnicos y financieros necesarios para el adecuado desempeño de sus funciones y será involucrado de manera oportuna en todas las cuestiones relativas a la protección de datos personales.

Los datos de contacto del DPD serán puestos a disposición de los titulares de los datos personales y de la Autoridad de Protección de Datos Personales, conforme a la normativa aplicable.

11. Obtención del consentimiento

Las condiciones de obtención del consentimiento son los requisitos legales, éticos y procedimentales que deben cumplirse para que la manifestación de voluntad del titular de los datos personales sea válida, legítima y verificable, previo al tratamiento de sus datos. El consentimiento debe obtenerse de forma:

- **Libre**: sin coacción, condicionamientos indebidos o consecuencias negativas por no otorgarlo.
- **Específica**: vinculada a finalidades concretas y claramente determinadas.
- **Informada**: previa entrega de información clara, completa y comprensible sobre el tratamiento de los datos.
- **Inequívoca**: expresada mediante una acción afirmativa clara que no dé lugar a dudas.
- **Previa**: otorgada antes de iniciar cualquier tratamiento de datos personales.
- **Revocable**: el titular puede retirarlo en cualquier momento, sin efectos retroactivos.

12. Tratamiento de datos personales en apego a la LOPDP

Con el fin de garantizar el estricto cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP), su Reglamento General y las buenas prácticas en privacidad, Esterimed Servicios de Esterilización Cia. Ltda. establece las directrices específicas que deben aplicarse según el tipo de tratamiento realizado en nuestras actividades operativas, administrativas, tecnológicas y comerciales.

12.1 Recolección de Datos

La Empresa puede recolectar datos personales en procesos de facturación, logística, seguridad, atención al cliente y actividades contractuales.

Obligaciones de cumplimiento:

- Informar al titular antes de la recolección (transparencia).
- Justificar la recolección con una base de licitud.
- Garantizar que los datos recolectados sean mínimos, necesarios y pertinentes.

- Evitar recopilar datos sensibles excepto cuando sea indispensable y legalmente permitido.

12.2 Almacenamiento y Conservación

Los datos serán almacenados en sistemas internos y plataformas tecnológicas como Microsoft Dynamics ERP, Zion, IVMS 4200 – HIKVISION, incluidos servidores internacionales.

Obligaciones de cumplimiento:

- Incorporar cifrado, control de accesos y auditorías de seguridad.
- Mantener el principio de privacidad por defecto (configuraciones restrictivas).
- Establecer periodos definidos de conservación según la finalidad.
- Eliminar, anonimizar o bloquear los datos una vez cumplida la finalidad o vencido el plazo legal.
- Documentar los plazos en el Registro de Actividades de Tratamiento (RAT).

12.3 Uso Interno de Datos

Incluye el tratamiento necesario para actividades administrativas, operativas, logísticas, comerciales y sanitarias asociadas a dispositivos médicos.

Obligaciones de cumplimiento:

- Usar los datos solo para la finalidad declarada.
- Restringir el acceso al personal autorizado.
- Mantener constancia documental de las finalidades y bases legales aplicables.
- Evitar tratamientos incompatibles o excesivos.

12.4 Transmisión Internacional de Datos

La organización podrá realizar transferencias de datos personales a terceros, nacionales o internacionales, únicamente cuando dichas transferencias se encuentren debidamente legitimadas conforme a la Ley Orgánica de Protección de Datos Personales y su Reglamento.

En el caso de transferencias internacionales de datos personales, la organización verificará previamente que el país, territorio u organización internacional receptora garantice un nivel adecuado de protección de datos personales.

Cuando el destinatario no ofrezca un nivel adecuado de protección, la transferencia solo se realizará si se implementan garantías apropiadas, tales como cláusulas contractuales, normas corporativas vinculantes u otros mecanismos reconocidos por la normativa aplicable.

La organización documentará las transferencias realizadas, las garantías adoptadas y la base de licitud correspondiente, como parte de su deber de responsabilidad proactiva.

Cuando sea legalmente exigible, el titular será informado sobre la transferencia internacional de sus datos personales, el país de destino y las garantías aplicadas.

Aplica a los datos almacenados y procesados en plataformas tecnológicas basadas fuera del Ecuador, como Microsoft Dynamics.

Obligaciones de cumplimiento:

- Verificar que el país receptor cuente con nivel adecuado de protección o aplicar garantías.
- Notificar claramente al titular sobre la transferencia.
- Mantener contratos, acuerdos o cláusulas modelo que obliguen a los proveedores a cumplir estándares de seguridad y confidencialidad.
- Registrar la transferencia en el RAT (Registro de actividades de tratamiento).

12.5 Comunicación y Acceso por Terceros

Incluye el acceso del técnico autorizado, proveedores tecnológicos, operadores logísticos y encargados del tratamiento.

Obligaciones de cumplimiento:

- Suscribir contratos con cláusulas específicas de protección de datos
- Supervisar el cumplimiento mediante auditorías o verificaciones.
- Asegurar que los terceros apliquen medidas equivalentes o superiores a las de la Empresa.
- Garantizar que los terceros solo traten los datos para el fin autorizado.

12.6 Procesos de Facturación

Incluyen la recolección y registro de datos para generar comprobantes tributarios.

Obligaciones de cumplimiento:

- Informar al cliente al momento de la recolección.
- Recolectar únicamente los datos exigidos por la normativa tributaria.
- Garantizar medidas de seguridad en el almacenamiento y transmisión internacional cuando aplique.

12.7 Tratamiento de Datos Sensibles

Aplica a datos biométricos, información de salud vinculada a servicios o dispositivos médicos, y datos de seguridad.

Obligaciones de cumplimiento:

- Obtener consentimiento expreso, salvo excepciones legales.
- Realizar una Evaluación de Impacto (EIPD) si el tratamiento puede implicar alto riesgo.
- Aplicar medidas reforzadas: cifrado robusto, segmentación, monitoreo, anonimización.
- Mantener registro documental del fundamento y necesidad.

12.8 Monitoreo, Videovigilancia y Control de Accesos

Incluye cámaras, registros de ingreso/salida, logs de sistemas y datos biométricos usados para seguridad física o digital y para control de asistencia.

Obligaciones de cumplimiento:

- Obtención de consentimiento de trabajadores para control de asistencia. Informar públicamente sobre la existencia de monitoreo.
- Usar datos solo para seguridad y prevención de incidentes.
- Limitar el tiempo de conservación según riesgos y normativa.
- Restringir el acceso a personal autorizado.
- Registrar estos tratamientos como actividades independientes en el RAT.

12.9 Modificación y Actualización de Datos

Realizada a solicitud del titular o por necesidades operativas.

Obligaciones de cumplimiento:

- Garantizar exactitud y actualización oportuna.
- Registrar las modificaciones cuando impacten información operativa crítica.
- Asegurar que los cambios no vulneren la integridad del sistema.

12.10 Eliminación y anonimización

Los datos serán eliminados o transformados cuando ya no sean necesarios. La eliminación busca la supresión definitiva del dato, sin posibilidad razonable de recuperación.

- **Obligaciones de cumplimiento:**

- Realizar eliminación segura (borrado irrecuperable).
- Anonimizar cuando la información sea útil para estadísticas o trazabilidad.
- Documentar el procedimiento en el RAT.
- Aplicar metodologías aceptadas internacionalmente.

12.11 Atención de Derechos del Titular

La organización garantiza a los titulares de datos personales el ejercicio de sus derechos reconocidos en la Ley Orgánica de Protección de Datos Personales. El ejercicio de los derechos será gratuito y podrá realizarse mediante los canales habilitados por la organización, los cuales aseguran accesibilidad, claridad y atención oportuna.

Las solicitudes serán atendidas dentro de los plazos establecidos en la normativa vigente, previa verificación de la identidad del solicitante.

La organización podrá limitar o negar el ejercicio de un derecho únicamente en los casos expresamente previstos en la ley, debiendo motivar su decisión y comunicarla al titular de forma clara y documentada.

Todas las solicitudes y respuestas serán registradas y conservadas como evidencia de cumplimiento del principio de responsabilidad proactiva.

A continuación, un cuadro informativo.

Nº	Derecho del titular	Descripción	Responsable	Posibles limitaciones legales
1	Acceso	Conocer si sus datos son tratados, cuáles, su origen, finalidad, base legal y destinatarios	DPD / Responsable del tratamiento	Afectación a derechos de terceros, información protegida
2	Rectificación	Solicitar la corrección de datos inexactos o incompletos	Proceso responsable del dato / DPD	Falta de sustento o verificación
3	Actualización	Solicitar la actualización de datos desactualizados	Proceso responsable del dato / DPD	Información no verificable
4	Eliminación (supresión)	Solicitar la supresión de datos innecesarios o ilícitos	Responsable del tratamiento / DPD	Obligación legal de conservación, defensa de derechos

5	Oposición	Oponerse al tratamiento basado en interés legítimo o fines no obligatorios	DPD	Interés legítimo prevalente debidamente justificado
6	Portabilidad	Recibir sus datos en formato estructurado y de uso común	TI / DPD	Imposibilidad técnica justificada
7	Suspensión del tratamiento	Solicitar la suspensión temporal del tratamiento en determinados casos	Responsable del tratamiento / DPD	Obligación legal o interés público
8	No ser objeto de decisiones automatizadas	Solicitar intervención humana y explicación de decisiones automatizadas	DPD / Área responsable	Tratamiento autorizado expresamente por ley
9	Información	Ser informado de forma clara sobre el tratamiento de sus datos	Responsable del tratamiento	Información sujeta a reserva legal
10	Revocatoria del consentimiento	Retirar el consentimiento otorgado previamente	Responsable del tratamiento / DPD	Tratamientos basados en obligación legal o contrato

El responsable debe responder en un plazo máximo de 15 días, contados desde la recepción de la solicitud válida del titular.

Obligaciones de cumplimiento:

- Establecer canales claros y accesibles para solicitudes.
- Responder dentro de los plazos legales.
- Registrar cada solicitud y la evidencia de gestión.
- No cobrar costos adicionales injustificados.

Para la atención de los derechos del titular o denuncias, se ha designado el correo del Delegado de Protección de Datos personales, es cual es: protecciondedatos.dhisve@outlook.com y el formulario de solicitud que puede encontrarse en el siguiente link: FORMULARIO - DERECHOS DE TITULARES DE DATOS PERSONALES: Rellenar formulario

12.11.1 Solicitudes incompletas o insuficientes

Cuando la solicitud presentada por el titular o su representante no contenga la información mínima necesaria para verificar su identidad, acreditar su legitimación o determinar con claridad el derecho ejercido, la organización podrá requerir información o documentación adicional para completar, aclarar o validar la solicitud.

El titular o su representante dispondrá de un plazo de cinco (5) días contados desde la notificación del requerimiento para remitir la información solicitada. Mientras no se reciba la información requerida, la atención de la solicitud quedará suspendida.

Si la información requerida no es proporcionada dentro de dicho plazo, la solicitud será archivada y el trámite se considerará concluido, sin perjuicio del derecho del titular a presentar una nueva solicitud posteriormente.

Los datos personales proporcionados en solicitudes incompletas serán tratados exclusivamente para la gestión, validación, documentación y trazabilidad del requerimiento presentado. Dichos datos serán conservados únicamente durante el tiempo necesario para acreditar el cumplimiento de las obligaciones legales y del principio de responsabilidad proactiva, procediéndose posteriormente a su eliminación con la normativa aplicable y las políticas o procedimientos internos de conservación de información.

La presentación de una solicitud incompleta no interrumpirá ni suspenderá los plazos legales de conservación que resulten aplicables a los datos personales tratados por la organización.

12.12 Gestión de Incidentes y Brechas de Seguridad

La organización implementa medidas técnicas y organizativas apropiadas para prevenir, detectar, gestionar y mitigar brechas de seguridad que afecten a datos personales.

Se considera brecha de seguridad de datos personales a todo incidente que ocasione la destrucción, pérdida, alteración, divulgación no autorizada o el acceso no autorizado a datos personales, ya sea de forma accidental o ilícita.

Ante la detección de una brecha de seguridad, la organización evaluará sin dilación indebida el riesgo que dicha brecha represente para los derechos y libertades de los titulares de los datos personales.

Cuando la brecha de seguridad represente un riesgo para los derechos y libertades de los titulares, la organización notificará el incidente a la Autoridad de Protección de Datos Personales, conforme a los plazos y condiciones establecidos en la normativa vigente.

Cuando la brecha represente un alto riesgo para los derechos y libertades de los titulares, la organización notificará adicionalmente a los titulares afectados, utilizando un lenguaje claro y comprensible.

Todas las brechas de seguridad, independientemente de que sean o no notificadas, serán documentadas, incluyendo su naturaleza, efectos, medidas adoptadas y acciones correctivas implementadas, como parte del principio de responsabilidad proactiva. Aplica a cualquier evento que afecte datos personales.

Obligaciones de cumplimiento:

- Activar de inmediato el protocolo interno de incidentes.

- Evaluar el nivel de riesgo para el titular.
- Notificar, cuando corresponda, a la Autoridad de Protección de Datos y a los titulares.
- Documentar el incidente, las causas y las medidas adoptadas.

12.13 Auditorías, Supervisión y Mejora Continua

La Empresa revisará periódicamente los tratamientos para garantizar cumplimiento y mitigación de riesgos

Obligaciones de cumplimiento:

- Realizar auditorías internas al menos una vez al año.
- Supervisar la actuación de terceros y proveedores tecnológicos.
- Mantener evidencia de cumplimiento (accountability).
- Actualizar medidas, controles y procedimientos conforme evolucionen los riesgos y la normativa.

13. Seguridad de la información y confidencialidad de los Datos

La Empresa se compromete a implementar medidas técnicas, organizativas y administrativas para garantizar la protección de los datos, tales como:

- Cifrado en tránsito y en reposo
- Controles de acceso basados en funciones
- Monitoreo continuo y detección de amenazas
- Auditorías internas periódicas

Todo el personal está sujeto a acuerdos de confidencialidad y capacitado regularmente sobre el adecuado manejo de la información.

14. Tratamiento por Terceros y Encargados

Cuando los datos personales sean tratados por terceros o encargados, la empresa:

- Suscribirá contratos de encargo de tratamiento que garanticen un nivel adecuado de protección
- Exigirá medidas equivalentes o superiores a las implementadas internamente
- Supervisará el cumplimiento mediante auditorías, controles documentados y/o verificación de prácticas
- El tercero deberá eliminar o devolver los datos al finalizar la relación contractual en un tiempo máximo de 15 días en formato legible, comprensible y estructurado.

15. Derechos del Titular

La Empresa garantiza el pleno ejercicio de los derechos reconocidos por la LOPDP, entre ellos:

Concepto	Significado
Derecho a la información	El titular tiene derecho a recibir información clara, previa y transparente sobre el tratamiento de sus datos personales, incluyendo la identidad del responsable, las finalidades, la base legal y los medios para ejercer sus derechos.
Derecho de acceso	Permite al titular conocer si sus datos personales están siendo tratados y, en caso afirmativo, acceder a dichos datos y a información sobre su tratamiento.
Derecho de rectificación y actualización	Faculta al titular a solicitar la corrección o actualización de sus datos personales cuando sean inexactos, incompletos o desactualizados.
Derecho de supresión (eliminación)	Permite solicitar la eliminación de los datos personales cuando hayan dejado de ser necesarios para la finalidad para la cual fueron recolectados o cuando el tratamiento sea ilícito.
Derecho de oposición	Autoriza al titular a oponerse al tratamiento de sus datos personales cuando existan motivos legítimos relacionados con su situación particular o cuando el tratamiento no sea obligatorio por ley.
Derecho a la limitación del tratamiento	Permite solicitar la restricción temporal del tratamiento de los datos personales en determinadas circunstancias, como mientras se verifica su exactitud o la legitimidad del tratamiento.
Derecho a la portabilidad	Faculta al titular a recibir sus datos personales en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento cuando sea técnicamente posible.
Derecho a no ser objeto de decisiones automatizadas	Garantiza que el titular no sea sometido a decisiones basadas únicamente en tratamientos automatizados, incluida la elaboración de perfiles, que produzcan efectos jurídicos o le afecten significativamente, salvo excepciones legales.
Derecho a la revocación del consentimiento	Permite retirar el consentimiento otorgado en cualquier momento, sin afectar la licitud del tratamiento realizado con anterioridad, cuando el tratamiento se base en dicho consentimiento.
Derecho a presentar reclamaciones	Faculta al titular a presentar reclamaciones ante el responsable del tratamiento y, de ser necesario, ante la Autoridad de Protección de Datos Personales del Ecuador.

Los titulares podrán ejercer estos derechos mediante los mecanismos informados públicamente por la Empresa.

16. Compromiso Institucional

Esterimed Servicios de Esterilización Cia. Ltda. reafirma su compromiso con la protección integral de los datos personales conforme a los requisitos de la LOPDP, implementando una cultura de privacidad, seguridad y cumplimiento normativo que abarque: Personas, procesos, tecnología, terceros, infraestructura y operaciones. El tratamiento de datos personales será siempre proporcional, legítimo y alineado a la misión y valores corporativos.

Esta política será revisada al menos una vez al año o antes si existen cambios en el contexto que lo ameriten

17. Control de cambios

Fecha	Descripción del cambio	Versión
25/03/2026	Creación del documento	01

18. Firmas de responsabilidad

Aprobado y autorizado por:	
Validar únicamente en FirmaEC. Firmado electrónicamente por: JUAN CARLOS MAJI MOZO Juan Carlos Maji Mozo Representante Legal	Validar únicamente en FirmaEC. Firmado electrónicamente por: BYRON XAVIER VASCONEZ MARTINEZ Byron Vásconez Martinez Delegado de Protección de Datos