POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

Versión borrador para revisión y aprobación de gerencia

Versión	1.0
Responsable	Delegado/a de Protección de Datos Personales (DPD)
Aprobado por	Dirección General
Vigencia	Desde su aprobación formal y hasta su actualización o reemplazo
Sensibilidad	Público (Para ser comunicado a titulares de derechos, asociados interesados y autoridades competentes)

Este documento será reemplazado por la versión aprobada y se integra con los procedimientos internos de accesos, auditoría, gestión de incidentes y atención de derechos del titular.

Control documental

Código	Propietario del documento	Revisión mínima	Documentos relacionados
CLP-PDP-POL-PDP-001	DPD, con apoyo de Dirección, TI, Talento Humano, Admisión, Facturación y áreas asistenciales	Anual o antes si hay cambios legales, tecnológicos, organizacionales o incidentes relevantes	Política de control de accesos y autenticación; procedimiento de alta/modificación/revocación; procedimiento de registro y auditoría de accesos; procedimiento de gestión de incidentes; procedimiento de atención de derechos del titular

1. Objeto

Establecer las reglas, responsabilidades, controles y evidencias mínimas que debe observar Clínica Los Pinos para tratar datos personales de manera lícita, leal, transparente, segura y demostrable, con especial protección de los datos de salud, de conformidad con la Ley Orgánica de Protección de Datos Personales, su Reglamento, la normativa y guías aplicables emitidas por la autoridad competente, y los deberes de confidencialidad propios de la actividad sanitaria.

2. Alcance

Esta política aplica a todo tratamiento de datos personales realizado por Clínica Los Pinos, en medios físicos o digitales, por personal propio, directivos, médicos con acceso autorizado a infraestructura o sistemas institucionales, prestadores externos, proveedores, encargados del tratamiento y cualquier tercero que trate datos por cuenta de la clínica o acceda a información bajo su custodia.

- Cubre datos de pacientes, familiares o representantes, médicos, personal administrativo y asistencial, postulantes, proveedores, visitantes y cualquier otra persona cuyos datos sean tratados por la clínica.
- Aplica a expedientes clínicos, formularios, consentimiento informado, imágenes, exámenes, correos electrónicos, archivos en Microsoft 365, sistemas administrativos, sistemas clínicos, respaldos, bitácoras y cualquier repositorio asociado.
- Incluye operaciones de recolección, registro, organización, conservación, uso, consulta, acceso, transmisión, comunicación, transferencia, respaldo, bloqueo, eliminación y destrucción.

3. Marco normativo y documental

La presente política se interpreta y aplica, entre otras referencias, con base en la LOPDP, su Reglamento, la normativa sectorial aplicable al ámbito sanitario, los deberes de secreto profesional, la normativa ecuatoriana sobre mensajes de datos y firmas electrónicas cuando corresponda, y la documentación interna de la clínica relacionada con accesos, incidentes, conservación documental, continuidad y atención de derechos del titular.

Referencia	Uso dentro de la política
LOPDP	Principios, bases legitimadoras, derechos del titular, categorías especiales de datos, seguridad y responsabilidad proactiva.

Referencia	Uso dentro de la política
Reglamento de la LOPDP	Conservación, roles, gestión de riesgos, protección desde el diseño y por defecto, evaluación de impacto y notificación de vulneraciones.
Guías y normativa emitidas por la SPDP	Orientación y criterios de implementación sobre gestión de riesgos, protección desde el diseño, evaluación de impacto y evidencia de cumplimiento.
Normativa sanitaria y documental aplicable	Conservación, custodia, acceso y reserva de documentación clínica y administrativa.
Políticas y procedimientos internos de Clínica Los Pinos	Operativizan esta política mediante flujos, formularios, matrices de control y registros de evidencia.

4. Definiciones esenciales

- Dato personal: información que identifica o hace identificable a una persona natural.
- Datos de salud: datos personales relativos al estado físico o mental pasado, presente o futuro, prestaciones de salud, diagnósticos, tratamientos, resultados, antecedentes y demás información clínica asociada.
- Responsable del tratamiento: Clínica Los Pinos, cuando decide sobre la finalidad y medios del tratamiento.
- Encargado del tratamiento: persona natural o jurídica que trata datos por cuenta de la clínica, conforme a instrucciones documentadas.
- Delegado/a de Protección de Datos Personales (DPD): figura interna encargada de asesorar, supervisar, impulsar cumplimiento y coordinar controles de protección de datos.
- RAT: Registro de Actividades de Tratamiento.
- Incidente de seguridad y privacidad: evento que afecta o puede afectar la confidencialidad, integridad, disponibilidad, trazabilidad o uso legítimo de datos personales.
- Violación o vulneración de seguridad: incidente que compromete datos personales y puede generar riesgo para derechos y libertades de los titulares.
- Necesidad de conocer: criterio por el cual solo acceden a la información quienes requieren verla para cumplir una función autorizada.

- Privacidad desde el diseño y por defecto: obligación de incorporar controles de protección de datos desde la concepción de procesos, sistemas y cambios, y de tratar por defecto solo los datos necesarios.

5. Principios rectores y reglas generales

Todo tratamiento debe responder a una finalidad determinada, explícita y legítima, ser proporcional, limitado a lo necesario, exacto, seguro, conservado solo por el tiempo requerido y sustentado en una base legitimadora documentada. La clínica aplicará el criterio más favorable al titular cuando exista duda razonable sobre el alcance de una operación de tratamiento.

- Se prohíbe recolectar o usar datos por comodidad operativa, costumbre o "por si acaso".
- Los datos de salud se tratarán con nivel reforzado de confidencialidad, acceso restringido y trazabilidad reforzada.
- Toda área deberá poder demostrar qué datos trata, para qué, con qué base legitimadora, quién accede, dónde se almacenan y cuánto tiempo se conservan.
- La información compartida con aseguradoras, laboratorios, médicos tratantes, proveedores o autoridades deberá limitarse al mínimo necesario y contar con base jurídica o instrucción válida.
- Se prohíbe el uso de cuentas personales de correo, mensajería personal o repositorios no autorizados para almacenar o compartir datos personales de pacientes o personal.

6. Gobierno, roles y responsabilidades

La protección de datos personales es una responsabilidad institucional y no exclusiva del DPD o del área de TI. Cada rol responde por el tratamiento que controla o ejecuta.

Rol	Nivel	Responsabilidades principales
Dirección General	A	Aprueba la política, asigna recursos, resuelve excepciones de alto impacto y exige evidencia de cumplimiento.
DPD	R/C	Asesora, supervisa, verifica cumplimiento, impulsa el RAT, coordina derechos del titular, incidentes, riesgos, DPIA y mejora continua.

Rol	Nivel	Responsabilidades principales
TI / soporte tecnológico	R	Implementa controles técnicos, administración de accesos, bitácoras, respaldos, hardening, revisiones y evidencias técnicas.
Líderes de proceso	R	Definen finalidades, bases, flujos, roles de acceso, retención y validan necesidad/legitimidad del tratamiento.
Talento Humano	R	Gestiona accesos del personal, confidencialidad, inducción, cambios de rol y bajas.
Áreas asistenciales y administrativas	R	Tratan datos conforme a mínimo necesario, necesidad de conocer, deber de reserva y procedimientos vigentes.
Encargados y proveedores	R	Tratan datos solo por cuenta de la clínica, con instrucciones documentadas, medidas de seguridad y deber contractual de confidencialidad.

7. Inventario de tratamientos, categorías de datos y base legitimadora

Antes de iniciar o modificar un tratamiento, el área responsable deberá registrarlo o actualizarlo en el RAT. Ningún tratamiento relevante podrá operar de forma indefinida sin identificación de finalidad, base legitimadora, responsable, sistemas involucrados, encargados, categorías de titulares, categorías de datos, plazo de conservación y riesgos principales.

- Los tratamientos vinculados a atención médica, historia clínica, diagnósticos, exámenes, imágenes, interconsultas y facturación asociada deben identificarse expresamente como tratamientos de alto impacto por involucrar datos de salud.
- Cuando el tratamiento se base en consentimiento, este deberá ser informado, específico, verificable y conservado como evidencia, sin sustituir otras bases legales cuando estas resulten aplicables.
- Cuando la clínica trate datos por obligación legal, ejecución contractual, protección de intereses vitales, cumplimiento de mandato judicial o ejercicio legítimo de competencias, la base deberá quedar documentada en el RAT y en los formularios o sistemas correspondientes.
- No se tratarán más categorías de datos de las necesarias para la finalidad declarada.

8. Reglas especiales para datos de salud y otros datos de categoría especial

Por la naturaleza de sus servicios, la clínica trata datos de salud y otra información especialmente sensible o reservada. Estos datos exigen controles reforzados, incluso cuando su tratamiento resulte necesario para la atención sanitaria, continuidad asistencial, facturación, auditoría médica o cumplimiento regulatorio.

- El acceso a información clínica se limita al personal asistencial o administrativo autorizado según rol, función, turno, sede y necesidad real de conocer.
- Los expedientes clínicos, resultados, diagnósticos, imágenes y reportes no podrán circular por canales informales ni quedar expuestos en escritorios, impresoras, pantallas abiertas o carpetas compartidas sin restricción.
- La entrega de información a familiares, aseguradoras, médicos externos, laboratorios, abogados o autoridades deberá pasar por validación de identidad, legitimidad, alcance y registro de entrega.
- La clínica adoptará medidas reforzadas respecto de niñas, niños y adolescentes, personas con discapacidad, adultos mayores y demás grupos de atención prioritaria, cuando corresponda.

9. Derecho a la información, consentimiento y atención de derechos del titular

La clínica informará a los titulares de manera clara y suficiente sobre la identidad del responsable, finalidades, bases legitimadoras, destinatarios, canales de ejercicio de derechos y demás extremos exigibles. El ejercicio de derechos se tramitará conforme al procedimiento específico vigente, con registro, validación de identidad, trazabilidad y respuesta documentada.

- La clínica habilitará canales formales para solicitudes de acceso, rectificación, actualización, eliminación, oposición, portabilidad, suspensión y demás derechos reconocidos por la normativa aplicable.
- Como regla interna de servicio, se acusará recibo de la solicitud en un plazo objetivo máximo de 48 horas hábiles, sin perjuicio de los plazos legales aplicables para resolver.
- Toda solicitud deberá quedar registrada con fecha, responsable, análisis, decisión, fundamento y evidencia de respuesta.
- Las áreas no podrán negar, retrasar o desatender solicitudes por criterio personal; cualquier controversia deberá escalarse al DPD.

10. Ciclo de vida del dato personal

10.1 Recolección

Solo se recolectarán datos adecuados, pertinentes y limitados a la finalidad correspondiente. Los formularios físicos y digitales deberán revisarse para eliminar campos innecesarios, ambiguos o carentes de base.

10.2 Uso y consulta

El uso interno de datos se realizará con segregación por perfil y registro de accesos cuando el sistema lo permita. Está prohibida la consulta por curiosidad, conveniencia, parentesco, notoriedad del paciente o motivos ajenos a la función.

10.3 Comunicación y transferencia

Toda entrega o acceso de terceros deberá estar documentado, sustentado y limitado. Se priorizarán mecanismos seguros de intercambio, confidencialidad contractual y trazabilidad de envíos.

10.4 Conservación, bloqueo y eliminación

Los datos se conservarán por el tiempo necesario para la finalidad y por los plazos que exija la normativa sanitaria, laboral, tributaria, contractual o de defensa jurídica que resulte aplicable. Cumplido el plazo, se procederá a su eliminación, anonimización o bloqueo seguro según corresponda, dejando evidencia cuando el tratamiento así lo requiera.

11. Controles mínimos de seguridad y privacidad

11.1 Controles organizacionales

- Compromisos de confidencialidad para personal y terceros con acceso a datos.
- Inducción obligatoria al ingreso y capacitación periódica, al menos anual, en protección de datos y manejo seguro de información.
- Clasificación de la información y definición de propietarios de procesos y repositorios.
- Gestión formal de cambios cuando se incorporen nuevas herramientas, formularios, integraciones o proveedores.

11.2 Controles de acceso y autenticación

- Modelo de acceso por rol y necesidad de conocer.
- Cuentas nominativas, prohibición de cuentas compartidas salvo excepción documentada y controlada.

- Autenticación reforzada, al menos para accesos remotos, privilegios administrativos y plataformas críticas donde la tecnología vigente lo permita.
- Revisión periódica de usuarios, perfiles y privilegios; mensual para privilegios altos y al menos trimestral para accesos estándar.
- Revocación o ajuste oportuno de accesos por ingreso, cambio de función, licencias prolongadas, desvinculación o pérdida de necesidad operativa.

11.3 Trazabilidad, bitácoras y monitoreo

- La clínica mantendrá registros de eventos de acceso, administración de identidades, cambios relevantes y actividades críticas en la medida que la plataforma y licenciamiento vigentes lo permitan.
- En Microsoft 365 y entornos asociados se aprovecharán, según disponibilidad, capacidades de Microsoft Entra para sign-in logs y audit logs, y capacidades de Microsoft Purview para auditoría de actividades.
- Las bitácoras deberán revisarse con una periodicidad definida según criticidad y conservarse conforme a la política de retención aplicable o a las limitaciones de la plataforma, procurando su exportación o resguardo cuando ello sea necesario y viable.

11.4 Herramientas autorizadas y comunicaciones

- Los datos personales y, especialmente, los datos de salud deberán tratarse únicamente en sistemas, repositorios y canales institucionales autorizados.
- Se prohíbe almacenar información de pacientes en dispositivos personales, nubes personales, memorias externas no cifradas o aplicaciones de mensajería no autorizadas.
- La impresión, copia, descarga, exportación o reenvío de información deberá obedecer a una necesidad legítima y quedar limitada al mínimo necesario.

11.5 Copias de seguridad, continuidad y recuperación

- Los sistemas y repositorios críticos con datos personales deberán contar con respaldo, capacidad de recuperación y pruebas periódicas proporcionales al riesgo.
- La restauración de información deberá quedar autorizada y documentada.
- Las copias de seguridad deben protegerse contra accesos indebidos y destrucción accidental o maliciosa.

11.6 Proveedores, encargados y transferencias internacionales

- Ningún proveedor tratará datos por cuenta de la clínica sin evaluación previa, contrato o cláusulas adecuadas, instrucciones documentadas, deber de confidencialidad y definición de medidas de seguridad.

- Cuando se utilicen servicios en la nube o exista almacenamiento o soporte fuera del territorio nacional, el área responsable y el DPD deberán revisar base legitimadora, riesgos, salvaguardas contractuales, ubicación del servicio, acceso remoto y medidas compensatorias.
- Los médicos independientes, prestadores externos o empresas aliadas que accedan a sistemas o información de la clínica deberán contar con perfil de acceso segregado y reglas documentadas de uso.

11.7 Privacidad desde el diseño, análisis de riesgos y DPIA

- Todo proyecto, integración, cambio relevante de proceso o nueva herramienta que implique tratamiento de datos deberá pasar por revisión temprana de privacidad.
- La clínica aplicará análisis de riesgos y, cuando corresponda, evaluación de impacto relativa a protección de datos antes de iniciar tratamientos que puedan implicar alto riesgo para derechos y libertades.
- No se admitirán despliegues tecnológicos relevantes sin definir responsable, finalidad, base legitimadora, flujo de datos, controles, riesgos y plan de tratamiento.

12. Gestión de incidentes, vulneraciones y escalamiento

Todo incidente real o presunto deberá ser reportado de inmediato por el personal a través del canal interno definido. La clínica aplicará contención, análisis, preservación de evidencia, calificación de impacto, medidas correctivas y, cuando corresponda, notificación a la autoridad competente y a los titulares afectados, conforme al marco legal aplicable y al procedimiento específico de gestión de incidentes.

- El reporte interno inicial deberá realizarse de manera inmediata y, como regla operativa, no más tarde de 24 horas desde que el colaborador conozca el hecho.
- Los encargados o proveedores deberán notificar a la clínica cualquier incidente que afecte o pueda afectar datos personales tan pronto sea posible, sin esperar al cierre de su análisis interno.
- El DPD coordinará la evaluación jurídica y de riesgo; TI y el área afectada coordinarán la contención y remediación técnica y operativa.
- Toda decisión de no notificar externamente deberá quedar motivada y documentada.

13. Evidencia, registros y auditoría

La clínica debe poder demostrar cumplimiento. No basta con declarar controles; deben existir registros, responsables y revisiones verificables.

Evidencia mínima	Contenido esperado	Periodicidad / responsable
RAT	Finalidad, base, categorías, sistemas, responsables, encargados, retención y riesgos.	Actualización continua / dueño del proceso + DPD
Matriz de accesos	Perfiles, altas, cambios, bajas, privilegios y aprobaciones.	Continua y revisión periódica / TI + jefaturas
Registros de derechos	Solicitud, identidad, análisis, respuesta y cierre.	Continua / DPD
Registro de incidentes	Detección, impacto, acciones, notificaciones y lecciones aprendidas.	Continua / DPD + TI
Contratos con encargados	Cláusulas de tratamiento, confidencialidad, subencargados y seguridad.	Previo al servicio y revisión anual / Jurídico + DPD
Capacitación y confidencialidad	Listas, evidencias, compromisos firmados, evaluaciones.	Inducción + anual / Talento Humano
Revisiones de logs y controles	Resultados, hallazgos, excepciones y acciones correctivas.	Según criticidad / TI + DPD

14. Auditoría, mejora continua, incumplimientos y excepciones

La clínica realizará verificaciones internas y, cuando corresponda, auditorías específicas para comprobar el cumplimiento de esta política. Los hallazgos deberán transformarse en planes de acción con responsable y plazo.

- El incumplimiento de esta política podrá generar medidas disciplinarias internas, sin perjuicio de responsabilidades civiles, administrativas, profesionales o penales que resulten aplicables.
- Ninguna excepción podrá aprobarse verbalmente. Toda excepción deberá constar por escrito, indicar alcance, vigencia, controles compensatorios, riesgo residual y responsable aprobador.
- Las brechas recurrentes, hallazgos repetidos o incumplimientos de alto impacto deberán elevarse a Dirección General.

15. Cláusula de implementación y vigencia

Esta política entra en vigor desde su aprobación formal. Los controles no implementados a la fecha deberán incorporarse al plan de adecuación institucional con priorización basada en riesgo, sin que ello implique autorización para tratar datos sin base, sin control o fuera de los canales permitidos.

- La revisión ordinaria será anual.
- La revisión extraordinaria procederá ante cambios legales, incidentes significativos, nuevos sistemas, cambios de proveedor, apertura de nuevas sedes o cambios relevantes en el modelo de atención.
- Toda nueva versión deberá conservar trazabilidad de cambios y fecha de aprobación.

Firmas de aprobación

Elaborado por	DPD / Responsable designado
Revisado por	Asesoría jurídica / TI / Talento Humano
Aprobado por	Dirección General
Fecha	12-may-2026

Control de versionamiento

Versión	1.0	**Cambios significativos**	Versión inicial
Aprobado por	Patricio Guzman	**Firma**	Validar únicamente en FirmaEC. Firmado electrónicamente por: PATRICIO JAVIER GUZMAN BRAVO