

Política de Privacidad y Tratamiento de Datos Personales

Versión 1.0 · Última actualización: 22 de octubre de 2026 · Ley 1581 de 2012 y Decreto 1377 de 2013 (Colombia)

1. Quién trata tus datos

El responsable de esta política es **Maycol Ruiz Zuluaga**, persona natural identificada con NIT **1088025510-4**, quien actúa a través de su establecimiento de comercio **Nexuring**, operador del software **Histoclinik**, con domicilio en Diagonal 26 #15-38, Dosquebradas – Risaralda, Colombia.

Canal de atención para consultas y reclamos: admin@nexuring.tech · Teléfono y WhatsApp: +57 319 505 2478.

2. A quién aplica esta política

Esta política aplica a las siguientes categorías de titulares:

- **Instituciones clientes** (hogares geriátricos y centros de cuidado): datos de contacto, facturación y de sus usuarios.
- **Usuarios de las instituciones** (personal administrativo, enfermería, cuidadores y profesionales): datos de identificación, credenciales y registros de actividad.
- **Residentes y sus familiares**: datos personales y de salud registrados por la institución cliente.

Respecto de los datos de residentes, **la institución clienta es la Responsable del tratamiento y Histoclinik es Encargada del tratamiento**: solo tratamos esa información siguiendo las instrucciones de la institución y para operar el servicio.

3. Datos que tratamos

De la institución cliente: nombre o razón social, NIT, dirección, teléfonos, correos, datos del representante, información de facturación y de medios de pago (procesados por la pasarela Wompi; no almacenamos números completos de tarjeta).

De los usuarios: nombre, documento, correo, teléfono, cargo, rol, credenciales de acceso y registros de auditoría (fecha, hora y acción realizada).

De los residentes: datos de identificación, contacto del acudiente o familiar, y datos de salud y cuidado (diagnósticos registrados, medicamentos, notas de enfermería, signos vitales y evolución) que la institución decide ingresar.

Datos técnicos: dirección IP, identificadores de sesión y registros de uso necesarios para la seguridad y el funcionamiento del servicio.

4. Para qué usamos la información

- Prestar, operar y dar soporte al servicio contratado.
- Administrar la cuenta, los usuarios, los roles y los permisos.
- Facturar, recaudar y gestionar pagos y cobros recurrentes.
- Atender consultas, requerimientos y reclamos.
- Generar reportes y estadísticas para la propia institución, no para terceros.
- Enviar comunicaciones del servicio (novedades, mantenimientos y avisos de seguridad).

- Prevenir fraudes, asegurar la plataforma y cumplir obligaciones legales.
- Con autorización previa y separada, enviar comunicaciones comerciales, autorización que el titular puede revocar en cualquier momento.

No vendemos, alquilamos ni cedemos datos personales a terceros con fines publicitarios.

5. Autorización y datos sensibles

Los datos de salud son **datos personales sensibles**. Los tratamos porque son necesarios para el cuidado de los residentes y en el marco de la operación de la institución, que es quien obtiene la **autorización previa, expresa e informada** de los titulares o de sus representantes legales. Si la institución no cuenta con esa autorización, no debe registrar la información en la Plataforma.

6. Encargados y terceros que intervienen

Para operar el servicio trabajamos con los siguientes terceros:

- **Proveedor de infraestructura en la nube (Oracle Cloud):** alojamiento de la aplicación y la base de datos, en servidores ubicados en Colombia.
- **Amazon Web Services (AWS), región us-east-1, Estados Unidos:** almacenamiento de archivos adjuntos y respaldos.
- **Wompi (Bancolombia):** procesamiento de pagos.
- **Meta Platforms / WhatsApp:** únicamente cuando la institución activa el agente de IA por WhatsApp.
- **Proveedor de correo electrónico:** para las notificaciones del servicio.

Estos terceros tratan la información por cuenta nuestra y bajo obligaciones de confidencialidad y seguridad.

7. Transferencia y transmisión internacional

Algunos de los terceros indicados se encuentran fuera de Colombia (almacenamiento de archivos y respaldos en Estados Unidos). El tratamiento de datos en el exterior se realiza conforme al artículo 26 de la Ley 1581 de 2012, en el marco del contrato de prestación del servicio y con la autorización del titular o de la institución responsable.

8. Cuánto tiempo conservamos los datos

- **Datos de la institución y de los usuarios:** mientras la relación esté vigente y, después, por los plazos legales de conservación de soportes contables y comerciales.
- **Datos de los residentes:** mientras la institución mantenga el servicio activo. Tras la terminación, la institución cuenta con sesenta (60) días para descargar la información; luego podrá eliminarse o anonimizarse, salvo que exista un deber legal de conservación o que la institución solicite por escrito su conservación por un plazo mayor.
- **Copias de seguridad (respaldos):** el Proveedor genera copias de seguridad diarias de la base de datos y las almacena en un servicio de almacenamiento externo (Amazon Web Services, región us-east-1, Estados Unidos). Se conservan por el tiempo que el Proveedor defina en su procedimiento de respaldos y luego se eliminan.

9. Tus derechos (habeas data)

Como titular, directamente o a través de la institución que representas, puedes:

- **Conocer** tus datos y solicitar prueba de la autorización otorgada.
- **Actualizar y rectificar** la información inexacta o incompleta.
- **Suprimir** los datos cuando no exista deber legal o contractual de conservación.
- **Revocar** la autorización, cuando sea procedente.

- **Presentar quejas** ante la Superintendencia de Industria y Comercio (SIC).
- **Acceder** gratuitamente a tus datos al menos una vez al mes calendario.

Cómo ejercerlos: escribe a admin@nexuring.tech indicando nombre, documento, dato o solicitud y el medio de respuesta. Para trámites relacionados con residentes, dirige la solicitud a la institución responsable; Histoclinik la apoyará como encargada.

Plazos de respuesta: las consultas se atienden dentro de los diez (10) días hábiles siguientes, prorrogables hasta por cinco (5) días hábiles más; los reclamos, dentro de los quince (15) días hábiles siguientes, prorrogables hasta por ocho (8) días hábiles más.

10. Seguridad de la información

Aplicamos medidas técnicas, humanas y administrativas razonables: cifrado en tránsito, control de acceso por roles, contraseñas con requisitos mínimos, registros de auditoría, copias de seguridad, gestión de vulnerabilidades y confidencialidad de nuestro personal. Ninguna medida es infalible, por lo que recomendamos a las instituciones no compartir credenciales y mantener sus propios respaldos.

11. Incidentes de seguridad

Si identificamos un incidente que comprometa datos personales, informaremos a la institución responsable sin dilación indebida, con la información disponible, para que esta cumpla sus deberes ante los titulares y la SIC.

12. Menores de edad y personas en situación de vulnerabilidad

Los datos de residentes menores de edad o de personas con discapacidad deben ser registrados por la institución bajo la autorización de sus representantes legales y respetando el interés superior del niño y la protección reforzada de las personas en situación de vulnerabilidad.

13. Cambios a esta política

Publicaremos cualquier cambio en esta página con la fecha de actualización y, cuando sea sustancial, lo notificaremos por los canales oficiales con al menos diez (10) días de antelación.

14. Vigencia

Esta política rige desde el 22 de octubre de 2026 y reemplaza cualquier versión anterior.