Política de privacidad

Cómo se utilizan los datos personales en Lumez, quién responde por cada uso y cuáles son los límites actuales de conservación, comunicación y atención de derechos.

Versión: 2026-09-18.1
Actualizado el: 2026-09-18

Proveedor responsable

64.117.651 ARTHUR GOMES DE FREITAS CARDOZO

CNPJ 64.117.651/0001-49

10A RUA DOUTOR MONTEIRO, 864, CASA, CENTRO, ARROIO GRANDE/RS, CEP 96330-000 - Brasil

Dominio oficial: https://lumez.digital-directive.com

Privacidad y soporte: arthurgfcardozo@gmail.com

Mercado inicial: América del Sur

Infraestructura: AWS, Google Cloud, Vercel e infraestructura propia de Digital Directive

Digital Directive es el nombre comercial declarado por el titular. Lumez es el producto cubierto por estos documentos; los demás productos no se incluyen automáticamente.

1. Alcance y responsabilidad

Esta política se refiere a Lumez, ofrecido en lumez.digital-directive.com por el proveedor identificado en este documento bajo el nombre comercial Digital Directive. Lumez no es una persona jurídica independiente. El mercado inicial es América del Sur. Otros productos de Digital Directive pueden utilizar otros subdominios de digital-directive.com; compartir ese dominio no extiende esta política ni sus finalidades de tratamiento a esos productos.

El proveedor determina las finalidades de su propia administración de cuentas, consultas del sitio web, relaciones comerciales, soporte y seguridad del servicio, actuando como responsable en esas actividades. El cliente empresarial normalmente decide para qué se tratan sus contactos y conversaciones; el proveedor trata ese contenido operativo siguiendo instrucciones documentadas del cliente. Las funciones dependen de la actividad real y un acuerdo de tratamiento debe definir las instrucciones y responsabilidades pertinentes.

Como estándar común de protección, los derechos deben facilitarse gratuitamente, con verificación proporcionada de identidad, sin cuentas innecesarias, exigencias excesivas de documentos ni represalias. Toda tarifa o denegación permitida requiere fundamento jurídico individual y posibilidad de impugnación. Permanecen los derechos locales imperativos más favorables; una relación entre empresas no excluye los derechos sobre datos personales.

2. Categorías de datos y procedencia

La información puede proceder directamente de un usuario o interesado, de la empresa que administra un espacio de trabajo, de las personas que se comunican con ella o de una integración habilitada. La existencia de campos no significa que todos los clientes los utilicen. El modelo actual puede contener las siguientes categorías.

- Datos de cuenta y equipo: nombre, correo electrónico, imagen de perfil, registros de autenticación y verificación, función, invitaciones y pertenencia al espacio de trabajo. Las sesiones pueden incluir dirección IP, información del navegador y horas de acceso.
- Datos empresariales: nombres de la organización y sus unidades, datos registrales, dirección, zona horaria, idioma, configuración e identificadores de integraciones autorizadas.
- Datos de contactos y conversaciones: nombres, teléfonos, correos electrónicos, documentos, fecha de nacimiento, notas, etiquetas y campos personalizados; mensajes, archivos adjuntos, ubicación o contactos cuando se envían, estados de entrega y lectura, asignaciones y notas internas.
- Registros asociados a funciones habilitadas: pedidos, direcciones de entrega, citas, instrucciones de automatización y registros de ejecución. Su presencia en el software no demuestra que estén incluidos en una suscripción concreta.
- Datos de consultas del sitio: nombre, correo electrónico, WhatsApp, sector, tamaño del equipo, objetivo, canal de contacto preferido y opciones de consentimiento. La consulta puede incluir parámetros de campaña y una dirección reducida de la página de procedencia; se eliminan los parámetros de consulta y fragmentos de esa referencia.

3. Finalidades y bases del tratamiento

Una base jurídica debe vincularse a una finalidad concreta y a la relación con el interesado. Aceptar una política de privacidad no constituye consentimiento general. La siguiente correspondencia describe las finalidades y bases que deben aplicarse según el tratamiento real y la legislación pertinente.

- Crear una cuenta y prestar un servicio solicitado por una persona puede basarse en la ejecución contractual o en medidas precontractuales solicitadas. Para empleados o representantes del cliente empresarial que no sean partes del contrato, debe evaluarse otra base adecuada, incluidos intereses legítimos proporcionados cuando estén permitidos.
- La autenticación, el control de acceso, la prevención de abusos, el diagnóstico y la seguridad pueden basarse en intereses legítimos, sujetos a necesidad, proporcionalidad y derechos de las personas. Solo se invoca una obligación legal cuando una norma aplicable exige realmente el tratamiento.
- Responder a una solicitud de demostración atiende a la petición de la persona. El formulario actual registra la autorización de contacto sobre esa solicitud por separado del consentimiento opcional de marketing, con la versión y la fecha de esas elecciones.
- El marketing opcional debe utilizar la base y las autorizaciones de comunicación exigidas en la jurisdicción del destinatario. La persona puede retirar su consentimiento u oponerse al marketing directo escribiendo a arthurgfcardozo@gmail.com, indicando Digital Directive - Privacidad/Lumez, o

por correspondencia a la dirección identificada en este documento. Para el marketing controlado por un cliente empresarial, la solicitud puede dirigirse a esa empresa.

- Para el contenido controlado por el cliente, este debe establecer las bases aplicables, informar y emitir instrucciones lícitas. El acceso del proveedor para prestar el servicio contratado no le otorga un derecho independiente a reutilizarlo para publicidad ajena al servicio u otros productos.

4. Destinatarios, WhatsApp e integraciones del cliente

Cuando el cliente habilita WhatsApp, los mensajes, destinatarios, archivos, datos de entrega e identificadores de activos empresariales pasan por los servicios pertinentes de Meta o WhatsApp. El proveedor conserva los registros operativos necesarios para las funciones configuradas. Meta o WhatsApp pueden tener responsabilidades jurídicas y avisos propios; este documento no los sustituye ni promete la eliminación en sus sistemas.

La infraestructura utilizada por Lumez incluye AWS, Google Cloud, Vercel e infraestructura propia del proveedor. Esta identificación no significa que cada proveedor reciba todas las categorías de datos. El registro de subencargados y transferencias distingue esa infraestructura de Meta/WhatsApp y de las integraciones elegidas por el cliente. Los servicios específicos, entidades contratantes, regiones de tratamiento y garantías contractuales deben evaluarse para cada flujo real; no se atribuye aquí a un proveedor un país o contrato no verificado.

- Los miembros autorizados del espacio de trabajo acceden según sus permisos. Los proveedores de infraestructura, almacenamiento, correo y soporte pueden recibir únicamente los datos pertinentes para su servicio, mediante acuerdos adecuados a su función.
- Una automatización puede enviar un contenido JSON a un destino HTTPS público elegido por el cliente. Este debe evaluar al destinatario y sus instrucciones; un destino elegido por el cliente no es automáticamente un proveedor contratado por quien presta Lumez.
- La comunicación a autoridades u otros terceros debe tener fundamento jurídico válido y limitarse a la solicitud u obligación pertinente. Esta política no autoriza una comunicación ilimitada por el mero hecho de recibir una petición.

5. Cookies, almacenamiento del navegador e idioma

La aplicación examinada utiliza almacenamiento del navegador para autenticación, preferencia de idioma y continuación del registro. La revisión actual no identificó un píxel publicitario activo ni una integración externa de análisis de audiencia. Es una constatación de la implementación, no una afirmación sobre servicios de alojamiento no revisados o futuras integraciones.

El aviso de almacenamiento del navegador detalla estas funciones. Las nuevas tecnologías opcionales requieren actualizar el inventario y proporcionar los avisos, consentimientos u otros controles exigidos por la legislación local antes de activarlas. Bloquear el almacenamiento esencial de sesión puede impedir el acceso; borrar la preferencia de idioma puede restablecerla.

- La autenticación está configurada con sesiones de hasta 14 días, una caché cifrada de sesión de cinco minutos, un paso de doble factor de diez minutos y, cuando se elige, confianza en el dispositivo durante hasta 30 días. Una sesión concreta puede terminar antes.
- La cookie lumez_locale conserva el idioma elegido hasta un año. Sin una elección guardada, la aplicación considera las preferencias del navegador y después un encabezado de país disponible en la infraestructura; en otro caso utiliza inglés. Este flujo no solicita ubicación GPS precisa.
- La entrada lumez:pending-onboarding del almacenamiento local contiene el nombre de la empresa y el tamaño del equipo indicados al registrarse. Se elimina al terminar la incorporación o cuando no se puede interpretar el registro almacenado; no se identificó caducidad automática por tiempo.
- Cuando está activa la persistencia local de tablas, lumez:grid:{workspace}:{user}:{screen} guarda ordenación, búsquedas, filtros, columnas, densidad y paginación. Búsquedas y filtros pueden contener datos personales. Nuevas elecciones pueden sustituir el registro y restablecer la vista puede eliminarlo; esto no borra automáticamente una vista guardada en el servidor.

6. Información sensible, menores y funciones automatizadas

Los mensajes libres, notas y archivos pueden contener información que el servicio no solicitó específicamente, incluidos datos sensibles. Los clientes deben limitar la recogida a lo necesario y establecer la base específica, las protecciones y las instrucciones exigidas para datos sensibles o información de menores. El producto actual es una herramienta empresarial y no se presenta como un servicio dirigido a menores. La implementación examinada no ofrece verificación de edad ni controles de consentimiento parental.

El entorno de pruebas de IA examinado utiliza simulación local y no tiene habilitados motores externos de IA. Por ello, esta implementación no permite identificar a un proveedor específico de modelos como destinatario actual. Las automatizaciones basadas en reglas pueden ejecutar acciones configuradas; el cliente debe evaluar sus efectos y ofrecer revisión humana adecuada. Antes de introducir IA externa, perfiles o decisiones con efectos jurídicos o igualmente significativos, deben evaluarse los flujos reales, los requisitos legales y los procedimientos de revisión, y actualizarse los documentos.

7. Seguridad y gestión de incidentes

Los controles implementados incluyen permisos por espacio de trabajo y aislamiento en la base de datos, protección de credenciales de Meta en el servidor mediante cifrado autenticado, verificación de firmas de webhooks, límites de peticiones y eliminación de secretos reconocidos de ciertos registros de error. La autenticación ofrece verificación de correo y doble factor. Son controles específicos, no una certificación ni una garantía frente a cualquier incidente de seguridad.

La eficacia y cobertura del cifrado, alojamiento y protección de copias dependen de la configuración y los servicios realmente utilizados; esta política no afirma el cifrado de toda la información almacenada ni establece un nivel fijo de servicio para disponibilidad o comunicación de incidentes. Las obligaciones legales aplicables siguen siendo pertinentes. El responsable debe evaluar los incidentes, documentar decisiones y notificar a personas o autoridades cuando lo exijan las normas, con asistencia del encargado cuando corresponda.

8. Conservación y eliminación

La conservación depende de la finalidad, la configuración autorizada del cliente, las obligaciones aplicables y la categoría real de datos. La implementación actual no permite afirmar que todos los datos personales desaparezcan después de un único plazo. Deben considerarse los siguientes límites al atender solicitudes.

- Una rutina diaria utiliza un plazo predeterminado de 90 días por espacio de trabajo, según el límite configurado. Elimina archivos elegibles, limpia contenido y cargas de mensajes, cargas de webhooks y detalles de auditoría, y anonimiza campos de contactos inactivos que cumplan los criterios.
- La rutina no cubre toda identidad de contacto, nota interna, campo relacionado de pedido o cita, carga de automatización u otro registro asociado. Estas categorías requieren una decisión documentada de conservación y una actuación complementaria cuando sean pertinentes para la solicitud. Finalizar la rutina no demuestra una eliminación integral.
- Las solicitudes de demostración caducan a los 90 días en la base de datos, renovándose el plazo cuando una solicitud repetida actualiza el registro. Un proceso elimina los registros vencidos. Los correos de notificación y las copias en otros lugares no se eliminan mediante esa rutina.
- Los archivos de exportación generados pasan a ser elegibles para su eliminación 30 días después de finalizar. La eliminación es asíncrona; la implementación actual no establece un instante exacto de caducidad para todas las copias o descargas.
- Una medida de conservación registrada puede suspender la purga del espacio de trabajo. Toda conservación adicional debe justificarse, limitarse y revisarse. Esta política no establece un plazo uniforme verificado de conservación de copias de producción ni promete la eliminación inmediata de todas ellas. Las copias pertinentes deben considerarse al evaluar conservación y eliminación, incluidas las restricciones de acceso y los efectos de una restauración.

9. Tratamiento y transferencias internacionales

El enfoque inicial en América del Sur no significa que todo el tratamiento se realice allí. AWS, Google Cloud, Vercel, la infraestructura propia del proveedor, WhatsApp y las integraciones elegidas por el cliente pueden implicar distintas partes y ubicaciones. La configuración real determina cada flujo; aquí no se afirma un país exclusivo de almacenamiento ni una región de tratamiento no verificada.

Antes de activar cada flujo internacional pertinente, deben identificarse sus partes, países, funciones y normas aplicables. Una decisión válida de adecuación puede cubrir un flujo concreto; en otro caso debe evaluarse una garantía lícita disponible u otro mecanismo permitido. Un mecanismo europeo no satisface automáticamente los requisitos brasileños o británicos, y las transferencias posteriores requieren evaluación propia. Firmar o publicar esta política no crea por sí solo cláusulas contractuales tipo ni valida una transferencia.

10. Derechos previstos por la legislación brasileña

Cuando se aplica la LGPD, las personas pueden ejercer los derechos pertinentes a su situación, incluidos confirmación y acceso, corrección, información sobre comunicaciones y las medidas siguientes. La identidad y la representación deben verificarse proporcionalmente. El documento de derechos y eliminación explica las funciones existentes y sus límites.

- Solicitar anonimización, bloqueo o eliminación de datos innecesarios, excesivos o tratados ilícitamente, y eliminación de datos tratados con consentimiento cuando corresponda, sujetos a motivos legales de conservación.
- Retirar el consentimiento y obtener información sobre la posibilidad y las consecuencias de denegarlo; solicitar portabilidad en las condiciones reglamentarias aplicables; oponerse al tratamiento en los supuestos legales.
- Solicitar revisión de decisiones basadas exclusivamente en tratamiento automatizado que afecten a sus intereses, y la información exigida por ley sobre los criterios y procedimientos pertinentes.
- Dirigirse al cliente empresarial por el contenido que controla o al proveedor por sus actividades propias, y utilizar los procedimientos de reclamación de la autoridad competente cuando corresponda. La respuesta completa de confirmación o acceso y otros derechos pueden tener plazos distintos; la fecha objetivo de la cola técnica no los sustituye.

11. EEE y Reino Unido

El RGPD y las normas británicas de protección de datos se aplican según su ámbito territorial y material, incluido el establecimiento, la oferta dirigida o el seguimiento pertinentes. Disponer de páginas traducidas no significa que toda norma se aplique a cada actividad. Cuando correspondan, el responsable debe facilitar el aviso y la base exigidos, y las partes deben implementar los acuerdos de encargo y demás garantías requeridas por sus actividades.

Con sujeción a las condiciones aplicables, los derechos incluyen acceso, rectificación, supresión, limitación, portabilidad, oposición y retirada del consentimiento sin afectar al tratamiento lícito anterior. Las personas pueden reclamar ante la autoridad de control competente. Las exigencias de representantes, delegado de protección de datos o evaluaciones de impacto dependen de la actividad real; esta política no designa por sí sola a esas personas ni demuestra que se haya realizado una evaluación.

- Debe respetarse la oposición al marketing directo, incluida la elaboración de perfiles relacionada cuando esté cubierta por la ley.
- Cuando se apliquen normas sobre decisiones exclusivamente automatizadas con efectos jurídicos o igualmente significativos, deben existir las protecciones y vías de intervención o revisión exigidas.
- La parte responsable debe observar los plazos de respuesta aplicables y los procedimientos de prórroga lícita. Las funciones actuales de exportación y eliminación no implementan por sí mismas todos los derechos ni todas las obligaciones de comunicación.

12. California, vías de contacto y cambios

Los requisitos de California deben evaluarse según la actividad, la función jurídica y los umbrales legales. Si se aplica la CCPA, los derechos pertinentes pueden incluir conocer y acceder a información, corregir, eliminar, rechazar la venta y rechazar la comunicación para publicidad conductual entre contextos según la definición de la CCPA, limitar ciertos usos de información sensible y la protección contra discriminación ilícita por ejercer derechos. Los contratos con clientes también pueden imponer deberes de proveedor de servicios o contratista.

Identificar los proveedores de infraestructura no determina la clasificación jurídica de cada flujo como venta, comunicación o uso de información sensible. Esta política no afirma de forma general que no se venden datos ni que exista un mecanismo automatizado de oposición o de tratamiento de Global Privacy Control. Toda actividad cubierta por esas reglas debe respetar los derechos aplicables y ofrecer los avisos y controles exigidos; las solicitudes pueden dirigirse al proveedor por la vía de contacto siguiente.

Para los tratamientos propios del proveedor, envíe solicitudes de derechos o reconsideración a arthurgfcardozo@gmail.com, indicando Digital Directive - Privacidad/Lumez, o por correspondencia a la dirección identificada en este documento. Los controles autenticados de exportación y eliminación son vías adicionales para usuarios autorizados; no es necesario crear una cuenta únicamente para ejercer derechos. Para conversaciones controladas por el cliente, contacte con la empresa con la que interactuó. El dominio oficial para consultar esta política y sus cambios relevantes es lumez.digital-directive.com. Prevalecen los derechos locales imperativos más favorables, incluidos los aplicables en países de América del Sur; ni el enfoque geográfico ni las traducciones disponibles demuestran cumplimiento universal.