



DOCUMENTO LEGAL Y DE CUMPLIMIENTO

Política de Privacidad

Versión	1.1
Vigencia	20 de septiembre de 2026

1. Alcance y respuesta clara sobre la recolección

Esta política explica el tratamiento asociado al sitio web, la plataforma web y la aplicación Android MASJ Community para residentes (Mobile). Debe leerse junto con la política de tratamiento del Responsable de cada copropiedad.

Sí: MASJ Community recopila y trata los datos personales y técnicos necesarios para autenticar usuarios, operar los módulos solicitados, proteger el servicio y cumplir instrucciones de la copropiedad. MASJ no vende datos personales ni usa datos personales para publicidad comportamental por defecto en V1. Las finalidades propias de un proveedor, cuando existan, se evalúan y transparentan según la operación concreta.

2. Roles en el tratamiento

La copropiedad normalmente actúa como Responsable cuando define por qué y cómo se tratan los datos de su comunidad. MASJ actúa como Encargado tecnológico siguiendo instrucciones documentadas y el contrato aplicable.

MASJ puede actuar como Responsable respecto de representantes de clientes, prospectos, proveedores, facturación, seguridad propia, soporte corporativo y contactos de su sitio.

La razón social, NIT, domicilio, dirección y existencia mercantil se contrastaron con el RUT y el certificado aportados. La aprobación interna deberá completarse antes de publicar.

3. Datos de cuenta, contacto y residencia

Puede tratarse documento y tipo de documento, nombres, apellidos, rol, estado de cuenta, correo, teléfonos, copropiedad, unidad, relación con la residencia y fechas relevantes. Se usan para identificar al usuario, autenticarlo, aplicar permisos, prestar el servicio y enviar comunicaciones operativas.

Las cuentas Mobile son aprovisionadas por Administración fuera de la aplicación; Mobile v1 no recopila datos para crear cuentas dentro de la app.

4. Datos de dispositivo, sesión y seguridad

Al iniciar sesión en Mobile se trata un UUID aleatorio de instalación, nombre o modelo del dispositivo, plataforma y versión de la aplicación. El servicio también puede tratar IP, User-Agent, fechas, resultado de acceso, identificadores y eventos de sesión, revocación, recuperación, aceptación legal y antiabuso.

La finalidad es autenticar, identificar sesiones, permitir su revocación, prevenir abuso, investigar incidentes y conservar trazabilidad razonable. El UUID no es un identificador publicitario.

Si el residente autoriza notificaciones push, Mobile registra un token de notificación, identificador de instalación, plataforma, nombre o modelo del dispositivo y versión de la aplicación, vinculados a su cuenta y sesión para entregar avisos operativos y gestionar su desactivación.

5. Información funcional de la comunidad

Según los módulos habilitados pueden tratarse visitantes e ingresos; vehículos y parqueaderos; paquetes y códigos de retiro; zonas comunes y reservas; pagos, saldos, conceptos y registros contables; votaciones; notificaciones; reportes; y solicitudes de mantenimiento.

En mantenimiento el residente puede aportar nombre, documento, teléfono, empresa y datos de visita de un técnico. Debe contar con autorización y limitarse a información necesaria.

En Mobile v1 los reportes contienen descripción, categoría, estado y seguimiento; el flujo auditado no permite adjuntar archivos a reportes o solicitudes de mantenimiento.

6. Comprobantes seleccionados por el usuario

Pagos permite seleccionar una imagen o PDF mediante el selector de archivos del sistema. La selección es voluntaria y limitada al archivo elegido; este puede copiarse temporalmente a la caché privada de la app antes de cargarse al almacenamiento autorizado del tenant.

El soporte se usa para revisión administrativa y conciliación interna. Su carga no equivale por sí sola a aceptación o confirmación del pago.

7. Almacenamiento local en Mobile

Los tokens de sesión, el UUID de instalación y la preferencia visual se guardan mediante almacenamiento seguro del sistema. La contraseña no se persiste en la app.

Cerrar sesión o revocar una sesión elimina sus tokens. El identificador de instalación y la preferencia pueden permanecer hasta borrar los datos de la app, desinstalarla o cambiar el identificador por una acción técnica válida. Los archivos temporales dependen del ciclo de caché.

En Android, para permitir la consulta sin internet de información ya cargada, Mobile puede conservar temporalmente respuestas de ciertas consultas del residente en una base cifrada dentro del almacenamiento privado de la aplicación. La clave de esa base se conserva por separado en el almacenamiento seguro del sistema. La copia se vincula a la sesión y comunidad correspondientes y puede contener datos personales presentes en las consultas permitidas; no almacena contraseñas, tokens de sesión, formularios pendientes, comprobantes ni archivos dentro de esa base de consultas.

Las copias de consulta vencen como máximo a las 24 horas desde la última respuesta exitosa del servicio y pueden eliminarse antes por límites de almacenamiento o por el sistema operativo. La aplicación elimina la base cifrada y su clave al cerrar sesión, cambiar de cuenta o comunidad, o invalidarse la sesión. Los datos mostrados sin conexión pueden estar desactualizados y no permiten crear ni modificar registros hasta recuperar internet.

8. Datos que Mobile v1 no solicita

La versión auditada no solicita ubicación precisa o aproximada, contactos, calendario, SMS, llamadas, micrófono, audio, datos de salud, sensores o identificadores publicitarios.

Tampoco integra publicidad, analítica de producto ni SDK de crashes. Las notificaciones push operativas de Mobile son opcionales: se solicita permiso del dispositivo y denegarlo no impide usar la aplicación. Una capacidad futura que cambie este alcance exige evaluación previa y actualización coherente de permisos, política y declaración de Google Play.

9. Inteligencia artificial y decisiones automatizadas

La versión Web/Mobile auditada no utiliza inteligencia artificial generativa, reconocimiento facial, perfilado algorítmico ni decisiones exclusivamente automatizadas con efectos jurídicos o similares sobre las personas.

Los datos de las copropiedades no se envían a servicios de IA ni se usan para entrenar modelos de terceros. Antes de incorporar IA, MASJ deberá evaluar impacto, proveedor, datos, finalidad, intervención humana y transferencias; actualizar esta política, contratos y Data Safety; e informar y obtener la autorización que resulte aplicable.

10. Finalidades y autorización

Los datos se usan para prestar funciones solicitadas, aplicar autorizaciones, comunicar eventos, atender soporte, proteger el servicio, cumplir instrucciones del Responsable y obligaciones legales.

El Responsable debe contar con la autorización o fundamento aplicable y proporcionar avisos claros. Los datos no deben reutilizarse para finalidades incompatibles sin informar y obtener la autorización que legalmente corresponda.

11. Proveedores, transmisiones y autoridades

Cuando un proveedor actúe como Encargado o subencargado, tratará los datos conforme al alcance e instrucciones aplicables. Si una operación implica una finalidad propia distinta de la prestación por cuenta de MASJ o de la copropiedad, se evaluarán y transparentarán separadamente el rol, la finalidad y la base aplicable. MASJ no vende datos personales ni concede una autorización general para explotar bases de residentes. Deben limitarse a la finalidad contratada, mantener confidencialidad y aplicar seguridad. La arquitectura auditada identifica DigitalOcean para infraestructura o almacenamiento, Brevo para correo transaccional y Cloudflare Turnstile para protección antiabuso en determinados flujos Web. Antes de activar esta versión se confirmarán servicio contratado, entidad, región y flujo productivo real.

Brevo puede recibir destinatario, nombre, contenido y eventos de entrega. Turnstile puede tratar IP, User-Agent, token y señales técnicas del desafío. La infraestructura puede alojar los datos necesarios para prestar el servicio bajo acceso restringido.

Google Play distribuye la aplicación y trata datos propios de la tienda conforme a su política. Cuando se habilitan notificaciones push, el servicio de Expo recibe el token del dispositivo, un título y mensaje genéricos y datos técnicos de navegación para entregar el aviso; no se envía el detalle completo de la notificación ni la base tenant. Expo/EAS también puede intervenir en compilación y entrega, pero no se identificó como SDK de analítica de producto en Mobile v1.

Mercado Pago existe como integración Web condicional y está deshabilitada por defecto en la configuración productiva auditada. Solo recibirá los datos necesarios si una copropiedad la habilita después de informar condiciones y completar los controles contractuales y de privacidad.

MASJ no vende datos personales ni entrega la base de una copropiedad a otra. Podrá comunicar datos a autoridades ante obligación legal, orden o requerimiento válido dentro de sus competencias.

12. Seguridad

MASJ aplica medidas administrativas, contractuales y técnicas razonables, como HTTPS en producción, aislamiento por tenant, control de acceso, almacenamiento seguro de tokens, validación de archivos, revocación y auditoría. Ningún sistema ofrece riesgo cero.

13. Conservación, supresión y cuenta

Los datos se conservan durante el tiempo necesario para la finalidad, las instrucciones válidas del Responsable y obligaciones contractuales, contables, fiscales, de seguridad o legales. Durante el servicio los datos necesarios permanecen disponibles para la operación; una suspensión temporal restringe el acceso, pero no equivale a terminación ni supresión.

Después de la terminación efectiva de una copropiedad, MASJ podrá mantener una custodia restringida hasta por un máximo ordinario de cinco (5) años, contado desde esa terminación, únicamente mientras exista una necesidad legítima y documentada. Este máximo no es un periodo mínimo, no autoriza conservar todas las categorías durante cinco años y no reemplaza los plazos especiales que exija la ley.

Cuando MASJ actúe como Encargado del Tratamiento, la custodia posterior a la terminación se realizará conforme al contrato, al anexo de transmisión y a las instrucciones válidas del Responsable. MASJ no ampliará unilateralmente el periodo de conservación de los datos del tenant por fuera de esas instrucciones, las finalidades legítimas aplicables o las obligaciones legales y contractuales correspondientes.

Durante esa custodia no habrá operación ordinaria, publicidad, marketing, perfilado comercial, venta, entrenamiento de inteligencia artificial ni usos incompatibles. El acceso se limitará a custodia, continuidad, recuperación, una eventual reactivación válidamente solicitada, obligaciones legales o contractuales, seguridad, auditoría, atención de reclamaciones y defensa jurídica.

La devolución, supresión o anonimización podrá realizarse antes cuando ya no exista una finalidad o base que justifique la custodia. Vencido el máximo ordinario se aplicará disposición segura, salvo deber legal o contractual, litigio, investigación, reclamación abierta, orden de autoridad, instrucción válida del Responsable o necesidad de defensa debidamente documentada.

Las copias de respaldo tienen un ciclo técnico separado: actualmente se gestionan manualmente y esta política no promete periodicidad, rotación, archivo automático, ubicación, cifrado ni recuperación instantánea no demostrados. Una restauración deberá respetar las restricciones y supresiones pendientes.

Desactivar una cuenta o cerrar sesión no equivale a borrar inmediatamente sus registros.

Mobile v1 no permite crear cuentas dentro de la app. Las solicitudes de consulta, corrección, revocatoria o supresión pueden dirigirse a Administración o al canal de privacidad, y se atenderán cuando procedan.

14. Derechos y trámite

La persona puede conocer, actualizar, rectificar y acceder a sus datos; solicitar prueba de autorización; pedir información sobre su uso; y solicitar revocatoria o supresión cuando legalmente proceda.

Puede presentar queja ante la Superintendencia de Industria y Comercio después de agotar el trámite correspondiente. Consultas y reclamos se atenderán dentro de los términos de la Ley 1581 de 2012.

15. Menores y datos sensibles

El tratamiento de datos de niños, niñas y adolescentes exige interés superior, respeto de sus derechos y las reglas especiales aplicables. Mobile v1 no usa reconocimiento facial ni identificación biométrica. Una función futura sobre datos sensibles requiere evaluación y autorizaciones previas.

16. Cambios, contacto y vigencia

Los cambios sustanciales se identificarán, comunicarán y, cuando creen una finalidad que requiera autorización, no se aplicarán antes de obtenerla. Cada versión publicada permanecerá identificable.

Sitio web: <https://masjcommunity.com>

Correo de privacidad actualmente publicado: contacto@masjcommunity.com

Teléfono / WhatsApp actualmente publicado: +57 314 2541060

Esta versión entra en vigencia el 20 de septiembre de 2026. La revisión de la misma v1.1 incorpora las aclaraciones de consulta sin conexión y notificaciones push aprobadas el 1 de octubre de 2026.

Fuentes oficiales de referencia

Ley 1581 de 2012: <https://www1.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>

Decreto 1074 de 2015: <https://www1.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=76608>

Guía SIC para propiedad horizontal: [https://sedeelectronica.sic.gov.co/noticias/superindustria-lanza-la-guia-para-e](https://sedeelectronica.sic.gov.co/noticias/superindustria-lanza-la-guia-para-el-tratamiento-de-datos-personales-en-la-propiedad-horizontal)
l-tratamiento-de-datos-personales-en-la-propiedad-horizontal

Política de datos de Google Play: <https://support.google.com/googleplay/android-developer/answer/10144311>

Cloudflare Turnstile y finalidad específica

Cloudflare trata determinadas señales técnicas necesarias para prestar Turnstile y prevenir abuso. Respecto de ciertas señales utilizadas para mejorar sus capacidades de detección, Cloudflare puede actuar bajo responsabilidad propia conforme a sus términos y aviso de privacidad aplicables. No se afirma acceso a la base de residentes ni acceso universal a campos de formularios.