

DeBiens — Política de Seguridad

Versión 1.0 · Generado el 3 de agosto de 2026 desde debiens.com.mx/legal

Manejamos el dinero y el padrón de comunidades enteras. Esta política dice, sin humo, qué hacemos para protegerlos — y también qué no tenemos todavía.

01 · Nuestra postura

1.1 Somos una empresa joven: **aún no contamos con certificaciones como SOC 2 o ISO 27001**, y no vamos a presumirlas antes de tenerlas. Lo que sí hay es ingeniería concreta —descrita abajo— y una regla de la ley que hacemos propia: nuestras medidas nunca serán menores que las que usamos para nuestra propia información (artículo 18, LFPDPPP).

02 · Aislamiento por diseño

2.1 Cada propiedad vive aislada mediante **seguridad a nivel de fila (RLS) en la base de datos**: la separación entre clientes no depende de que el código «se porte bien», la impone la propia base en cada consulta. Un usuario de una propiedad no puede leer datos de otra ni aunque la aplicación tuviera un error.

2.2 Los permisos se resuelven **en el servidor**, nunca en el navegador: el rol de cada perfil (administrador, operativo, condómino) se verifica en cada petición.

03 · Cifrado

3.1 Todo el tráfico viaja cifrado con **TLS** (HTTPS obligatorio, sin excepciones). Los datos en reposo se almacenan cifrados por nuestro proveedor de base de datos **[CONFIRMAR AES-256 EN PLAN VIGENTE]**. Las contraseñas se guardan con hash criptográfico; nunca en claro, y nadie de DeBiens puede leerlas.

04 · Control de acceso

4.1 Acceso por **SSO de Google o Microsoft** o por credenciales propias; roles con mínimo privilegio; los accesos administrativos a la infraestructura están limitados a personal autorizado con autenticación de dos factores, y las acciones sensibles quedan en bitácora.

05 · RespalDOS y continuidad

5.1 Respaldo **diario y automático** de la base de datos, con retención de **[N DÍAS]** y pruebas periódicas de restauración. La exportación completa de datos está disponible para el Cliente en todo momento: la continuidad de tu operación no depende de nosotros para siempre.

06 · Subencargados de infraestructura

6.1 Proveedores sobre los que opera DeBiens, todos con servidores en Estados Unidos:

Proveedor	Función	Datos que toca
Vercel	Hosting de la aplicación	Tráfico cifrado de la app
Supabase	Base de datos y almacenamiento	Todos los datos de la plataforma
Resend	Correo transaccional	Direcciones y contenido de correos
Anthropic	Modelo de lenguaje de Obed	Fragmentos necesarios por consulta

Cambios a esta lista se avisan con **30 días de anticipación** a los clientes.

07 · Obed y la IA

7.1 Obed consulta la base **con los mismos permisos del usuario que pregunta** — no ve nada que ese usuario no pueda ver. Los fragmentos enviados al modelo de lenguaje se procesan bajo contrato que prohíbe usarlos para entrenamiento **[CONFIRMAR CONTRATO DEL PROVEEDOR]**, y no se conservan más allá del procesamiento de la consulta.

08 · Llaves de conexión (MCP)

8.1 Las llaves de conexión externas nunca se guardan en claro: almacenamos únicamente su huella **SHA-256**, así que ni nosotros podemos recuperar una llave perdida. Cada llave hereda los permisos del perfil que la creó y pasa por el mismo RLS de la sección 02: **identifica, no autoriza**. Se pueden crear de solo lectura, caducan automáticamente a los 90 días, se revocan al instante — y se reactivan o borran—, y el administrador de la cuenta puede cortar las de todo su equipo. Cada alta, revocación y borrado queda en bitácora, junto con la fecha de último uso.

8.2 Lo que no tenemos todavía, dicho sin humo: **no hay limitador de peticiones sobre esta interfaz ni un segundo factor sobre la llave**; hoy la defensa operativa es la revocación inmediata. Y lo que ocurra en el programa donde pegues la llave —lo que conserve, muestre o reenvíe— queda fuera de nuestro alcance técnico: se rige por tu contrato con ese proveedor. **[DECISIÓN DEL ABOGADO: validar que estas ausencias se declaren así de expresas, al estilo de la sección 01]**

09 · Vulneraciones

9.1 Si una vulneración de seguridad afecta de forma significativa derechos patrimoniales o morales de personas titulares, **informaremos de forma inmediata** a los titulares (artículo 19, LFPDPPP) y a las administradoras responsables, con lo que sepamos: qué pasó, qué datos, qué hicimos y qué recomendamos hacer.

10 · Reporte responsable

10.1 ¿Encontraste una vulnerabilidad? Escríbenos a contacto@debiens.com.mx [**ALIAS seguridad@ PENDIENTE**]. Nos comprometemos a responder en **72 horas**, a no emprender acciones legales contra la investigación de buena fe, y a dar crédito si lo deseas.

Referencias

Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Diario Oficial de la Federación, 20 de marzo de 2025; última reforma del 14 de noviembre de 2025. Cámara de Diputados. <https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>