POLÍTICA DE PRIVACIDAD – MI BIBLIOPASS

Última actualización: 30 de abril de 2026

En Mi BiblioPass, nuestra prioridad absoluta es la seguridad de su información sensible. Esta aplicación ha sido diseñada bajo el principio de "Privacidad por Defecto", lo que significa que sus datos nunca abandonan su dispositivo a menos que usted decida exportarlos manualmente.

1. FILOSOFÍA DE "CERO DATOS" (ZERO-KNOWLEDGE)

A diferencia de otros gestores de contraseñas, Mi BiblioPass no utiliza servidores en la nube.

No recopilamos sus nombres de usuario, correos electrónicos ni contraseñas.

No tenemos acceso a su Contraseña Maestra ni a su PIN de seguridad.

No rastreamos su actividad ni vendemos su información a terceros.

2. ¿QUÉ DATOS SE PROCESAN Y DÓNDE?

Toda la información que usted introduce se almacena exclusivamente en el almacenamiento local protegido de su teléfono móvil (AsyncStorage).

Contraseñas y Documentos: Se guardan cifrados localmente.

Biometría: La aplicación utiliza los servicios nativos de su sistema operativo (Huella dactilar o Reconocimiento facial). La app solo recibe la confirmación del sistema; nunca accede a su rastro biométrico real.

Validación de Email: El correo solicitado en el registro se utiliza únicamente para la configuración inicial del perfil dentro del dispositivo.

3. MEDIDAS DE SEGURIDAD ACTIVAS

Para garantizar que sus datos estén a salvo de miradas indiscretas, la aplicación incluye:

Bloqueo de Capturas: Impedimos técnicamente la realización de capturas de pantalla o grabaciones de video en secciones críticas.

Protección de Multitarea: El contenido de la app se oculta cuando usted cambia de aplicación para evitar que sea visible en el menú de aplicaciones abiertas.

Autoborrado de Portapapeles: Cualquier dato sensible que usted copie se eliminará automáticamente del portapapeles tras 30 segundos.

MFA de Memoria (15 días): El sistema le obligará a introducir su Contraseña Maestra cada 15 días para asegurar que no la olvide, dado que no existe un servidor para recuperarla.

4. COPIAS DE SEGURIDAD (BACKUP)

El usuario es el único responsable de la custodia de sus datos.

La función de Copia de Seguridad genera un archivo HTML cifrado con el algoritmo militar AES-256.

Este archivo solo puede ser descifrado mediante su Contraseña Maestra.

Al exportar este archivo (a Google Drive, WhatsApp, etc.), la seguridad del mismo pasa a ser responsabilidad del usuario y del servicio de almacenamiento elegido.

5. TU RESPONSABILIDAD

Dado que no tenemos acceso a tus datos, eres el único responsable de mantener tu Contraseña Maestra segura.

Si olvidas tu Contraseña Maestra, no podemos recuperar tus datos.

Si pierdes tu teléfono o borras la app sin una copia de seguridad, tus datos se pierden para siempre.

También se te pedirá aceptar un descargo de responsabilidad al iniciar por primera vez, reconociendo que el desarrollador no se hace responsable de ninguna pérdida de datos.

Mantén siempre copias de seguridad seguras en tu almacenamiento en la nube personal o ubicaciones externas.

6. DERECHOS DEL USUARIO (ARCO-POL)
Al ser una aplicación local, usted tiene el control total:
Acceso y Rectificación: Puede ver y editar sus datos en cualquier momento desde la app.
Eliminación: Puede realizar un "Borrado Masivo" desde los ajustes o simplemente desinstalar la aplicación. Esto eliminará permanentemente todos sus datos sin posibilidad de recuperación.
7. PROCESAMIENTO DE PAGOS Y SUSCRIPCIONES
Para gestionar las suscripciones Premium, utilizamos los servicios de Google Play Billing y RevenueCat.

- Datos recopilados: Al realizar una compra, estos servicios procesan un ID de usuario anónimo, el historial de transacciones y el estado de la suscripción.
- Finalidad: Estos datos se utilizan exclusivamente para validar su acceso a las funciones Pro y prevenir fraudes. No se recopila información personal identificable para fines de marketing.
- Eliminación de datos: Si desea solicitar la eliminación de los registros de facturación asociados a su ID anónimo en los servidores de RevenueCat, puede hacerlo enviando un correo electrónico a nuestro contacto de soporte.

8. PUBLICIDAD Y SERVICIOS DE TERCEROS

En la versión gratuita de la aplicación, podemos mostrar publicidad a través del servicio Google AdMob.

- Datos de Publicidad: Google AdMob puede recopilar y utilizar identificadores de publicidad anónimos de su dispositivo (como el ID de publicidad de Android) para mostrar anuncios relevantes y medir el rendimiento de los mismos.
- Control del usuario: Usted puede restablecer o limitar el uso de estos identificadores desde los ajustes de privacidad de su dispositivo Android. Al adquirir la versión Premium de Mi BiblioPass, la publicidad se desactiva por completo y cesa la recopilación de datos asociados a este fin.

9. ACTUALIZACIONES DE POLITICA

Podemos actualizar esta política de privacidad de vez en cuando.

La fecha "Última Actualización" se mostrará en la app. Los cambios significativos te serán notificados a través de notificaciones de la aplicación.

10. CONTACTO
Si tiene dudas sobre el funcionamiento de la seguridad de Mi BiblioPass, puede contactar con el desarrollador en:
Email: ecf.team.apps@gmail.com