

Cómo protege PIPELINE-OS su información: 3 niveles de respaldo y cifrado de extremo a extremo

Su operación vive dentro de **PIPELINE-OS**: los **registros de la base de datos** (KPIs, usuarios, notas, actividad) y los **archivos que usted adjunta** (PDF, imágenes, vídeos, Excel, documentos). Este documento explica, en lenguaje claro, cómo blindamos toda esa información con **3 niveles de respaldo independientes y cifrado de extremo a extremo**, de modo que un borrado accidental, un hackeo o incluso la caída total de un proveedor no puedan dejarlo sin sus datos.

01

¿Qué información suya protegemos?

Tres cosas se respaldan en cada ciclo. Las dos primeras son **su información**; la tercera es el propio PIPELINE-OS, para poder reconstruir el servicio completo si hiciera falta.

Su base de datos

Registros del sistema: KPIs, usuarios, notas, actividad y toda la información estructurada que genera su operación.

Sus archivos adjuntos

PDF, imágenes, vídeos, hojas de Excel y documentos que usted carga y almacena dentro de PIPELINE-OS.

La aplicación PIPELINE-OS

El código del propio software. Se respalda en los **tres niveles** (Supabase, GitHub y Backblaze), para poder reconstruir el servicio completo —no solo los datos— ante cualquier imprevisto.

02

¿Qué pasa si sus datos se pierden, se dañan o los atacan?

Cada nivel es una copia adicional, guardada en un lugar distinto y con una protección distinta. Así, para cada tipo de incidente hay siempre una copia intacta lista para restaurar. Junto a cada nivel encontrará **qué tipo de cifrado lo protege**.



¿Cómo funciona cada nivel por dentro?

Cada nivel con sus datos clave. **Recuperación (RPO)** = cuánta información podría perderse, como máximo, entre el incidente y la última copia buena.

1
Supabase se respalda a sí mismo, todos los días

La plataforma donde vive PIPELINE-OS ya protege sus datos

POR ACTIVAR

FRECUENCIA Diaria automática	RETENCIÓN 7 días	RECUPERACIÓN ≤ 24 h la noche anterior	DÓNDE VIVE Supabase la app misma	CIFRADO AES-256 en reposo
---	-----------------------------------	--	---	--

QUÉ PROTEGE
 Su base de datos completa y una copia del código de **PIPELINE-OS**. Supabase —la infraestructura de nivel empresarial sobre la que corre PIPELINE-OS, usada por miles de compañías y con cumplimiento SOC 2— genera automáticamente un **respaldo diario dentro de la misma plataforma**. Es decir: el sistema donde viven sus datos ya se protege a sí mismo.

SU GRAN VENTAJA
 Es el **más rápido de restaurar**: devuelve la base al estado de la noche anterior en minutos, sin salir del proveedor. Sus datos viajan cifrados (TLS) y se guardan cifrados en reposo (AES-256). Se complementa con las copias externas de los niveles 2 y 3 para cubrir también un fallo del propio Supabase.

Por qué importa: ante el incidente más común —alguien borra o sobrescribe un dato hoy— este nivel lo resuelve solo, en minutos, sin depender de nada más. Es la primera línea de defensa.

2
Una copia cifrada, fuera de Supabase, en GitHub

Su información completa, sellada, en otra empresa

ACTIVO · PROBADO 04-AGO-2026

FRECUENCIA Diaria ~06:00 Bogotá	RETENCIÓN 30 días	RECUPERACIÓN ≤ 24 h	DÓNDE VIVE GitHub otra empresa	CIFRADO age extremo a extremo
--	------------------------------------	--------------------------------------	---	--

QUÉ PROTEGE
 Base de datos + archivos adjuntos + el código de **PIPELINE-OS**. Cada día se empaqueta TODO, se cifra con **nuestra propia llave** y se sube a GitHub como un paquete sellado que el proveedor no puede abrir. Incluir el código permite reconstruir el servicio entero, no solo los datos.

EL CIFRADO, EN DETALLE
Extremo a extremo con age (intercambio de claves X25519 + cifrado autenticado ChaCha20-Poly1305), aplicado **antes** de subir. Sobre eso, viaja por TLS 1.2+ y GitHub lo guarda además con AES-256 en reposo: **tres capas** sobre el mismo dato. GitHub nunca ve el contenido.

Por qué importa: es la primera copia **fuera** de Supabase, en una empresa distinta. Si Supabase entero fallara, fuera hackeado o se borrara, su negocio se reconstruye desde aquí. Ya está probado: la recuperación real del 04-ago-2026 salió de este nivel.

3
Un archivo imborrable de 2 años en Backblaze

La máquina del tiempo, a prueba de ransomware

POR IMPLEMENTAR

FRECUENCIA Diaria	RETENCIÓN 24 meses escalonada	RECUPERACIÓN ≤ 24 h	DÓNDE VIVE Backblaze otra empresa	CIFRADO age + candado WORM
------------------------------------	--	--------------------------------------	--	---

QUÉ PROTEGE
 El mismo paquete cifrado del nivel 2 (**datos + adjuntos + código**), pero guardado **hasta 24 meses de profundidad** y bajo candado inmutable. Cubre lo que ninguna otra capa: fraudes o daños que se descubren tarde, y obligaciones de historial de largo plazo.

POR QUÉ EL CANDADO SÍ ES INMUTABLE
 Usa **Object Lock en modo Cumplimiento (WORM)**: una copia escrita **no puede borrarse ni modificarse hasta que vence su plazo** — ni con las credenciales de administrador, ni por nosotros, ni por el soporte de Backblaze. El bloqueo lo impone el **propio proveedor a nivel de almacenamiento**, no nuestro software: por eso un ransomware que robara todas las claves no lograría cifrar ni borrar el archivo.

Por qué importa: es la única capa con años de historia y con candado anti-borrado. Aunque un atacante tomara el control de una cuenta, las copias de este nivel siguen intactas hasta su vencimiento. La retención escalonada se explica en la sección 04.

Cómo se cifra su información — y dónde está la llave que la abre 3 CAPAS DE CIFRADO

Su información está protegida por **tres capas de cifrado que se refuerzan**. Para leer un solo dato sin permiso, un atacante tendría que romper las tres a la vez — y aun así le faltaría la llave. Esto es lo que hay detrás:

Capa 1 En tránsito · TLS 1.2+

Los datos viajan cifrados entre usted, la app y los proveedores. **Frena** que alguien "escuche" la conexión (ataque *man-in-the-middle*).

Capa 2 En reposo · AES-256

Supabase, GitHub y Backblaze cifran los discos donde guardan la información. **Frena** que un disco robado del proveedor pueda leerse.

Capa 3 Propio, antes de subir · age

Sellamos el paquete con **nuestra llave** antes de que salga. **Frena** que el proveedor —o quien le robe— pueda leer sus datos: solo verían texto cifrado inservible. Este es nuestro diferencial.

La llave Custodiada fuera de línea

La llave que descifra **no vive en ningún servidor conectado a internet**: se guarda fuera de línea (en un vault), separada de las copias. Aunque robaran todas las cuentas en la nube, sin esa llave no abren nada.

La llave, explicada con una imagen simple: las copias en la nube son **cofres cerrados**; la única llave que los abre la guardamos en una **caja fuerte física, desconectada**, con una segunda copia de respaldo. Técnicamente usamos cifrado **asimétrico**: una llave *pública* solo sirve para cerrar (y puede vivir en el sistema sin riesgo) y una llave *privada* —la única que abre— permanece siempre fuera de línea. Datos y llave nunca están en el mismo lugar: por eso robar el almacenamiento no basta para leer nada.

04 ¿Hasta qué momento del pasado podemos recuperar?

"Respaldo diario durante 2 años" **no** significa guardar 730 copias. Detrás hay una idea muy simple:

Cuanto más viejo es un problema, menos precisión necesita para arreglarse.

Para un error de **ayer**, usted quiere volver a **ayer exacto** → guardamos una copia por día.

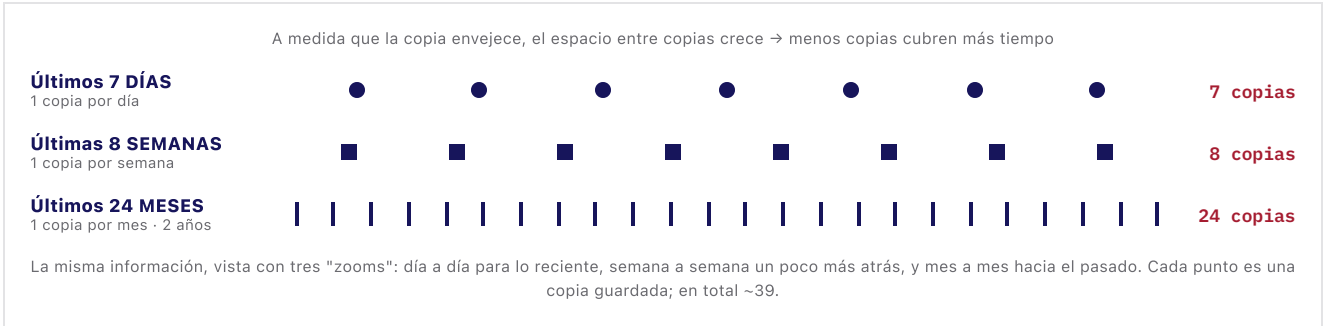
Para algo de **hace meses**, basta volver a "por esa época" → guardamos una por semana, y luego una por mes.

Así conservamos **mucho detalle en lo reciente y puntos de referencia en lo lejano**.

En números concretos, el archivo del nivel 3 conserva siempre estas tres franjas (y poda lo que sobra, automáticamente):

ANTIGÜEDAD DE LA COPIA	CADA CUÁNTO SE GUARDA	Nº DE COPIAS	PARA QUÉ LE SIRVE A USTED
Últimos 7 días	1 copia por día	7	Revertir un error reciente al día exacto
Últimas 8 semanas	1 copia por semana	8	Recuperar algo de "hace unas semanas"
Últimos 24 meses	1 copia por mes	24	Historial de largo plazo y hallazgos tardíos (fraude, corrupción de datos)

Total: ~39 copias, no 730. Detalle donde importa, historia donde hace falta — respaldando además sus obligaciones de conservación a largo plazo.



¿Y si falla —o hackean— un proveedor entero?

Aquí es donde su información se vuelve realmente indestructible. Seguimos la **regla 3-2-1**, el estándar de oro del respaldo, cuya idea de fondo es simple: **ningún evento único debe poder destruir todas sus copias a la vez**. Un detalle clave: incluso el sistema donde viven sus datos —Supabase— guarda **su propio respaldo interno**, así que ya hay protección antes de salir a cualquier otra empresa.



3

copias, como mínimo

Si una copia se corrompe o desaparece, todavía quedan otras para restaurar. Nunca un solo punto de fallo.

Usted tiene 4. Datos vivos + respaldo interno de Supabase + GitHub + Backblaze.

2

tecnologías distintas

Guardadas en soportes diferentes, para que un mismo fallo técnico no las tumbe todas a la vez.

Usted tiene 3. Nube gestionada (Supabase), repositorio (GitHub) y almacenamiento de objetos (Backblaze).

1

copia fuera del proveedor

Al menos una copia en una empresa distinta a la de producción. Si el proveedor principal desapareciera, usted sobrevive.

Usted tiene 2 fuera. GitHub y Backblaze, ambos fuera de Supabase y con accesos independientes.

En resumen: su información en PIPELINE-OS nunca depende de una sola copia ni de un solo proveedor. Se respalda todos los días, se cifra de extremo a extremo, se guarda también fuera del proveedor de producción y se archiva de forma imborrable hasta 2 años atrás. Un borrado accidental, un hackeo o la caída total de un proveedor: en todos los casos, **sus datos siguen recuperables**.