

REPORTE EJECUTIVO

Seguridad y continuidad del servicio

Tribyte

Un resumen ejecutivo de los controles de seguridad, privacidad y disponibilidad que protegen la operación de su plataforma.

RESUMEN

Este documento describe, en términos claros y no técnicos, cómo protegemos su información y garantiza la continuidad de su operación: el control de accesos a los datos, el cumplimiento de la normativa mexicana de privacidad, el monitoreo continuo de los procesos automáticos, los mecanismos de respaldo a nivel aplicación, y las certificaciones de seguridad que resguardan tanto la infraestructura como el procesamiento de pagos.

CONTENIDO

- 01** Seguridad y control de accesos
- 02** Privacidad de la información
- 03** Disponibilidad y monitoreo
- 04** Respaldo a nivel aplicación
- 05** Certificaciones y seguridad de pagos

SECCIÓN 01

Seguridad y control de accesos

Cómo Tribyte protege la información almacenada frente a manipulaciones no autorizadas y controla quién puede ver o modificar cada dato.



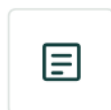
Consultas parametrizadas

Toda interacción con las bases de datos se realiza mediante consultas parametrizadas, nunca mediante construcción directa de texto con datos ingresados por el usuario. Esto elimina la posibilidad de que una entrada malintencionada altere el comportamiento de una consulta a la base de datos.



Acceso segmentado por roles

El acceso a la información está segmentado por roles: cada usuario solo puede consultar o modificar la información correspondiente a sus permisos asignados, y cada acceso queda registrado para su trazabilidad.



Trazabilidad de accesos

Cada acceso a la información queda registrado, permitiendo reconstruir en todo momento quién consultó o modificó un dato y cuándo, como respaldo ante cualquier revisión de seguridad.

SECCIÓN 02

Privacidad de la información

Cómo se resguardan los datos personales tratados dentro de la plataforma, conforme al marco legal mexicano de protección de datos.



Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP)

El tratamiento de la información personal dentro de la plataforma se apega a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), el marco legal mexicano que regula cómo las empresas privadas deben recolectar, usar, almacenar y resguardar datos personales. Esto incluye el reconocimiento de los derechos ARCO (acceso, rectificación, cancelación y oposición) de los titulares de la información, así como la aplicación de medidas de seguridad organizacionales —como políticas internas y capacitación del personal—, físicas y tecnológicas, acordes al nivel de sensibilidad de los datos tratados.

DERECHOS ARCO

A Acceso — conocer qué datos personales se tienen y cómo se utilizan.

R Rectificación — corregir datos inexactos o incompletos.

C Cancelación — solicitar la eliminación de los datos cuando corresponda.

O Oposición — oponerse al uso de sus datos para un fin específico.



Medidas de seguridad acordes al riesgo

Se aplican medidas de seguridad administrativas, técnicas y físicas acordes al nivel de sensibilidad de los datos tratados, reduciendo el riesgo de uso indebido o acceso no autorizado.

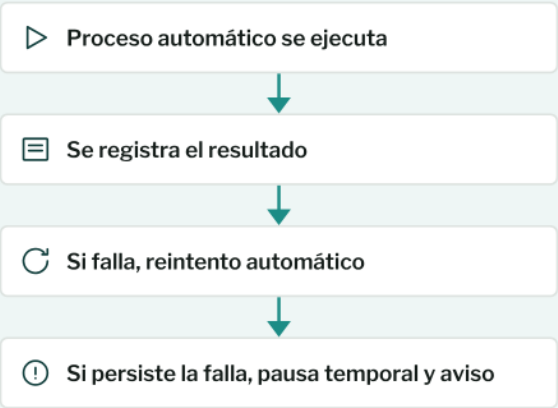
SECCIÓN 03

Disponibilidad y monitoreo

Cómo se supervisa la operación continua de la plataforma y cómo se contienen las fallas antes de que afecten el servicio.

- Los procesos automáticos se supervisan de forma constante, y cada operación queda registrada con su resultado: éxito, advertencia o error.
- Ante fallas, se generan reintentos automáticos antes de requerir intervención manual.
- Mecanismos de contención automática pausan temporalmente un proceso si detectan fallas repetidas, evitando que un problema puntual escale y afecte la disponibilidad general del servicio.

FLUJO DE CONTENCIÓN



SECCIÓN 04

Respaldo a nivel aplicación

Una capa adicional de consistencia, propia del software, que complementa el respaldo de la infraestructura.



Integridad de datos ante reprocesos

Además del respaldo de la infraestructura donde se aloja la información, la propia aplicación mantiene mecanismos de integridad a nivel de datos: cada documento procesado queda registrado de forma que el sistema puede identificar si ya fue guardado previamente, evitando duplicados o pérdidas ante reprocesos.



Identificación de documentos

Cada documento procesado se identifica de forma única, permitiendo saber si ya fue guardado.



Sin duplicados ni pérdidas

Ante un reproceso, la información existente se preserva sin generar registros duplicados.

Esto da una capa adicional de consistencia propia del software, complementaria a la del respaldo de infraestructura.

SECCIÓN 05

Certificaciones y seguridad de pagos

Los estándares internacionales que auditan la infraestructura de la plataforma y el procesamiento seguro de pagos.

CERTIFICACIONES DE LA PLATAFORMA

La infraestructura que resguarda la información de la operación cuenta con las siguientes certificaciones, auditadas de forma periódica por terceros independientes.



ISO/IEC 27001

Sistema de gestión de seguridad de la información, con estándares internacionales de control.



SOC 2 Type II

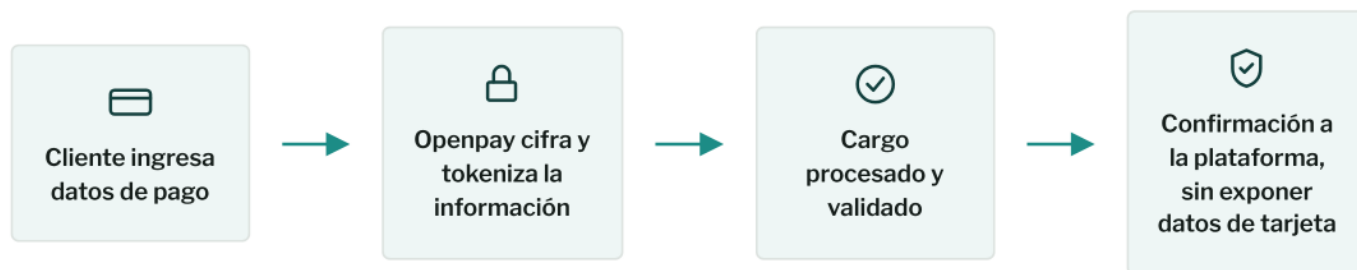
Auditoría periódica e independiente de los controles de seguridad a lo largo del tiempo.

SEGURIDAD EN PAGOS



Para el procesamiento de pagos y cobros recurrentes, la plataforma se apoya en **Openpay**, respaldada por BBVA, que cuenta con certificación **PCI DSS Nivel 1** — el estándar internacional más alto en seguridad de datos de tarjetas de pago. La información de tarjetas viaja cifrada mediante certificados SSL y nunca se almacena en los servidores propios: es tokenizada por el proveedor, de forma que ni siquiera Tribyte tiene acceso directo a los datos completos de la tarjeta. Openpay cuenta además con un sistema antifraude que analiza cada transacción y permite establecer límites máximos por cargo y por periodo, como capa adicional de control sobre los cobros recurrentes.

SECCIÓN 05 · FLUJO DE UN PAGO

De la tarjeta del cliente a la confirmación del cargo

CIERRE

Qué garantiza este esquema**Control y trazabilidad de accesos**

Cada acceso a la información queda registrado y limitado a los permisos de cada usuario.

**Cumplimiento normativo de privacidad**

El tratamiento de datos personales se apeg a la LFPDPPP y respeta los derechos ARCO.

**Continuidad operativa ante fallas**

El monitoreo continuo y la contención automática limitan el impacto de cualquier falla.

**Integridad de datos y pagos**

Los documentos procesados y los cargos realizados se validan y resguardan de forma consistente.

Documento de carácter informativo — Seguridad y continuidad del servicio.