

REPORTE EJECUTIVO

Infraestructura de datos Tribyte

Un resumen ejecutivo de cómo se almacena, respalda y protege la información de su operación fiscal y contable.

Este documento describe, en términos generales, la arquitectura de datos, los protocolos de respaldo y los estándares de seguridad que resguardan la información de la empresa dentro de la plataforma.

— RESUMEN EJECUTIVO

La operación de datos se procesa sobre recursos designados para esta cuenta, con una persona asignada de forma permanente a su seguimiento. Antes de guardarse, la información se organiza por tipo —fiscal, contable y administrativa—, de modo que cada categoría se consulta y se controla por separado. Cada noche se genera una copia de respaldo distinta a la del día anterior, fuera del horario de operación, y se valida antes de darse por concluida. Ese respaldo se ejecuta bajo Acronis Cyber Protect, un proveedor sujeto a auditorías externas periódicas, y la información se cifra tanto al guardarse como al transmitirse.

CONTENIDO

- 02 Infraestructura dedicada
- 03 Pilares de administración de datos
- 04 Flujo de la información
- 05 Cómo funciona el respaldo
- 06 Certificaciones de seguridad
- 07 Qué garantiza este esquema

SECCIÓN 02

Infraestructura dedicada

La información de la empresa se procesa dentro de un entorno designado para esta cuenta, con recursos y responsables propios.

**Documentos fiscales**

Información de su operación fiscal y contable

**INFRAESTRUCTURA DE DATOS****Servidor dedicado**

Recursos designados específicamente para esta operación

**Personal asignado**

Seguimiento y atención continua

**Disponibilidad continua**

El servicio opera las 24 horas, los 7 días de la semana, sin ventanas de indisponibilidad para la consulta.

— QUÉ SIGNIFICA PARA SU OPERACIÓN

La información de la empresa se administra dentro de una infraestructura con recursos designados. Esto significa que el servidor y la capacidad de procesamiento son exclusivos para su operación, incluso en momentos de alta demanda, y no se comparten con otras cuentas. Esto permite que el procesamiento de la información no dependa de la carga de trabajo de terceros, y que cualquier ajuste, mantenimiento o mejora se realice de forma controlada. Adicionalmente, existe una persona asignada de forma permanente al seguimiento de estos datos, responsable de supervisar que los procesos de captura, almacenamiento y disponibilidad de la información se ejecuten correctamente día a día, ofreciendo un punto de contacto directo ante cualquier necesidad.

SECCIÓN 03

Pilares de administración de datos

Cuatro prácticas sostienen el manejo diario de la información: cómo se organiza, dónde se resguarda, cómo se copia y quién puede consultarla.



Almacenamiento

La información se organiza por tipo —fiscal, contable, administrativa—, evitando mezclar distintas categorías de datos en un mismo repositorio. Esto facilita la trazabilidad y reduce el riesgo de errores al consultar información específica.



Bases de datos

La información se resguarda en un motor de datos empresarial designado para esta cuenta, capaz de soportar altos volúmenes con tiempos de respuesta consistentes, incluso en periodos de alta demanda como cierres mensuales o declaraciones anuales.



Respaldos

Se generan copias completas de la información de forma diaria, en un horario que no interfiere con la operación. Esto asegura que, ante cualquier eventualidad, la información pueda restaurarse desde un punto reciente.



Seguridad

El acceso a la información está sujeto a controles estrictos: solo el personal autorizado puede consultar o modificar los datos, y cada acceso queda registrado como parte de las prácticas de control interno.

Estos cuatro pilares operan de forma coordinada: la organización por tipo facilita el respaldo, el respaldo se apoya en el motor de datos designado, y los controles de acceso aplican en cada uno de los puntos anteriores.

SECCIÓN 04

Flujo de la información

Antes de almacenarse y respaldarse, la información recorre un proceso claro y controlado, desde su origen hasta su consulta por el equipo autorizado.

**Obtención de información fiscal**

La plataforma se conecta de forma automática y segura a los portales oficiales (SAT e IMSS) para descargar la documentación fiscal vigente de la empresa.

**Procesamiento de comprobantes**

Los comprobantes fiscales (facturas) se reciben, se validan y se preparan para su uso contable.

**Organización por tipo de información**

Toda la información se clasifica y almacena por categoría —fiscal, de facturación, administrativa—, cada una en su propio repositorio, para mantener el control y la trazabilidad.

**Consulta desde la plataforma**

El equipo autorizado accede a la información ya organizada y validada a través del portal, sin tocar directamente ninguna base de datos.

SECCIÓN 05

Cómo funciona el respaldo

El respaldo de la información se realiza mediante **Acronis Cyber Protect**, proveedor utilizado por instituciones financieras y gubernamentales a nivel mundial, sujeto a auditorías externas independientes.



Proceso y frecuencia

- Copia de respaldo cada noche, fuera del horario de operación.
- Validación automática al finalizar cada copia, antes de darla por concluida.
- Almacenamiento separado del sistema original, con redundancia entre componentes.



Seguridad física

- Los centros de datos cuentan con vigilancia permanente y acceso restringido mediante verificación biométrica.
- Infraestructura con energía y componentes redundantes, para operar sin interrupciones ante fallas puntuales.



Seguridad digital

- Cifrado AES-256 en almacenamiento y en tránsito — el mismo estándar usado por instituciones bancarias.
- El personal del proveedor no tiene acceso al contenido de la información, solo a metadatos operativos de soporte.
- Acceso administrativo con doble verificación de identidad.

SECCIÓN 06

Certificaciones de seguridad

Estas certificaciones respaldan que el proveedor de respaldo —no solo la plataforma— cumple estándares internacionales verificados por auditores externos. No son declaraciones propias: cada una implica revisiones periódicas realizadas por firmas independientes, cuyos resultados condicionan la vigencia de la certificación.



ISO/IEC 27001

La certificación de seguridad de la información más reconocida a nivel internacional.



SOC 2 Type II

Auditorías externas independientes que verifican el manejo seguro de la información de forma continua.



Cumplimiento de privacidad — GDPR / HIPAA

Cumple con normativas internacionales estrictas de protección de datos y privacidad, incluyendo el marco europeo (GDPR) y el de salud en Estados Unidos (HIPAA). Esto garantiza que ni siquiera el personal del propio proveedor tiene acceso al contenido de la base de datos.

Las tres certificaciones se encuentran vigentes y se renuevan mediante auditorías periódicas.

SECCIÓN 07

Qué garantiza este esquema

En conjunto, la infraestructura designada, los pilares de administración y el esquema de respaldo se traducen en tres compromisos concretos hacia su operación.



Continuidad operativa

Ante fallas técnicas, errores humanos o eventos imprevistos, la información puede recuperarse desde una copia reciente sin depender de un único punto de falla. La operación diaria de la empresa no queda condicionada a un solo componente.



Trazabilidad y control

Cada acceso, cambio o proceso queda documentado, lo que permite auditar el manejo de la información en cualquier momento. Ante una revisión interna o externa, es posible reconstruir quién consultó qué y cuándo.



Respaldo con estándares internacionales

El proveedor de respaldo cumple con marcos normativos reconocidos globalmente, lo cual da una capa adicional de confianza sobre cómo se resguarda la información, incluso frente al propio proveedor del servicio.