# PRACTICAS DE SEGURIDAD

Ago-2025

# PRÁCTICAS DE SEGURIDAD

En STS Group, la seguridad de los datos es una prioridad absoluta y nos esforzamos por mantener la transparencia como uno de nuestros principios fundamentales. Nos comprometemos a ser claros y directos sobre cómo gestionamos la seguridad. Si tienes más preguntas sobre nuestras prácticas de seguridad, estaremos encantados de responderlas. Puedes escribirnos a info@grupo-sts.com, y te responderemos lo más pronto posible.

Nuestra página de prácticas de seguridad describe los controles administrativos, técnicos y físicos aplicables a STS Group, que incluye nuestra plataforma, flujos de trabajo y aplicaciones ejecutadas en nuestra infraestructura.

## Controles de plataforma

### Arquitectura y segregación de datos

Operamos nuestros servicios en una arquitectura multiusuario tanto a nivel de plataforma como de infraestructura, diseñada para segregar y restringir el acceso a los datos que tú y otros usuarios proporcionan a través de nuestros servicios. Esta arquitectura garantiza una separación lógica de los datos de cada cliente mediante una ID única.

### Infraestructura de nube pública

Nuestros servicios están alojados en la nube pública, accesibles a través de proveedores externos, lo que permite un servicio escalable y disponible a cualquier persona que desee utilizarlo o comprarlo.

### Auditorías

Nuestras prácticas de seguridad son verificadas internamente ya que se realizan auditorías internas periódicas. Además, utilizamos análisis continuos y automatizados de nuestra plataforma web. Los informes de auditoría interna están disponibles para nuestros clientes.

### Certificaciones

Mantenemos certificaciones actualizadas en ambientes productivos.

## Controles de seguridad

### Registro de acceso

Proporcionamos registros de acceso detallados, disponibles para usuarios y administradores, que incluyen tipo de dispositivo utilizado y dirección IP.

**Administración de acceso**

Ofrecemos a los administradores la capacidad de terminar sesiones y cerrar dispositivos remotamente en cualquier momento.

**Conservación de datos**

Los propietarios de equipos pueden establecer políticas de retención de mensajes personalizadas que automáticamente eliminan mensajes y archivos que exceden la duración establecida.

**Administración de servidores**

Realizamos análisis de vulnerabilidad automáticos en nuestros servidores de producción y aplicamos medidas de seguridad física como el cifrado de disco completo.

**Protección de la red**

Implementamos autenticación de dos factores y utilizamos firewalls configurados según las mejores prácticas de la industria.

**Manejo de incidencias**

Mantenemos políticas y procedimientos robustos para el manejo de incidentes de seguridad, incluyendo notificación rápida a los clientes afectados y publicación de actualizaciones de estado.

**Cifrado de Datos**

Utilizamos cifrado estándar de la industria para proteger los datos del cliente durante la transmisión y en reposo.

**Fiabilidad y copias de seguridad**

Nuestra infraestructura está diseñada para ser altamente disponible y realizamos copias de seguridad regulares para garantizar la continuidad del negocio.

**Confidencialidad**

Controlamos estrictamente el acceso de nuestros empleados a los datos del cliente, con políticas de privacidad y confidencialidad y de acceso a datos para garantizar la seguridad y privacidad.

**Prácticas del personal**

Realizamos verificaciones de antecedentes a todos los empleados y proporcionamos capacitación continua en seguridad y privacidad.

**Infraestructura**

Utilizamos la infraestructura de Amazon Web Services (AWS) para alojar y procesar los datos del cliente, con acceso a información detallada sobre las prácticas y certificaciones de seguridad de AWS.

Para más detalles sobre nuestras políticas y para acceder a nuestros informes de seguridad, contáctanos directamente en info@grupo-sts.com.