Informe de Seguridad

Cómo Align protege los datos de su institución

Versión 1.0 · Abril 2026

RESUMEN EJECUTIVO

Align es una plataforma SaaS diseñada para instituciones educativas. Dado que gestiona información sensible sobre reuniones, acuerdos y equipos docentes, la seguridad no es una característica opcional sino un principio de diseño. Este documento describe las medidas técnicas y operativas que protegen los datos de cada institución.

1 Autenticación

Solo Google OAuth — sin contraseñas almacenadas

Align no gestiona ni almacena contraseñas. El acceso se realiza exclusivamente mediante Google OAuth 2.0, delegando la autenticación al proveedor de identidad más utilizado del mundo. Esto elimina los riesgos asociados a contraseñas débiles, reutilizadas o filtradas.

- Cada sesión genera un token JWT firmado con una clave secreta única del sistema
- Los tokens tienen expiración automática
- El administrador puede suspender usuarios con efecto inmediato

2 Aislamiento de datos entre instituciones

Cada escuela ve únicamente sus propios datos

La arquitectura garantiza separación completa entre instituciones. Cada consulta a la base de datos está filtrada por el identificador único de la escuela del usuario autenticado. No existe ninguna ruta — directa ni indirecta — que permita a un usuario de la institución A ver información de la institución B.

- **Nivel de aplicación:** todos los endpoints verifican la pertenencia del usuario a la escuela antes de devolver datos
- **Nivel de base de datos:** claves de servicio con permisos acotados; las operaciones siempre incluyen filtros de escuela

3 Control de acceso por roles

Align implementa un sistema granular de roles dentro de cada institución. Un detalle importante: el Director o Owner sabe que una reunión existe — puede ver su título, fecha y participantes — pero no puede acceder a la minuta ni a los acuerdos a menos que un participante se la comparta explícitamente. Esto protege la confidencialidad de los equipos y genera confianza interna. Ningún usuario puede escalar sus permisos por cuenta propia — los roles son asignados por el director y verificados en el servidor en cada operación.

Rol	Nivel de acceso
Director / Owner	Sabe que la reunión existe (título, fecha, participantes) pero no puede ver la minuta ni los acuerdos a menos que un participante se la comparta explícitamente
Vicedirector / Coordinador	Acceso completo a reuniones donde participa
Docente	Acceso a sus propias reuniones y resúmenes relevantes
Administrativo	Acceso restringido según configuración del director

4 Gestión de usuarios e invitaciones

El acceso siempre es por invitación explícita — no existe registro abierto ni acceso anónimo

- El director genera un link de invitación para un email específico con un rol predefinido
- El link tiene validez de 7 días y es de un solo uso
- El invitado debe autenticarse con Google antes de poder acceder
- Un usuario removido pierde el acceso en su siguiente sesión

5 Infraestructura y cifrado

- **Hosting:** Vercel — CDN global sobre infraestructura AWS
- **Base de datos:** Supabase (PostgreSQL gestionado, SOC 2 Type II)
- Todo el tráfico viaja cifrado con TLS 1.2/1.3 (HTTPS obligatorio)
- Los datos en reposo están cifrados en la infraestructura de Supabase
- Las claves de API nunca están incluidas en el código fuente
- El dominio aplica HSTS para forzar siempre conexiones seguras

6 Protecciones HTTP

Cada respuesta del servidor incluye headers de seguridad estándar de la industria:

- **X-Frame-Options: DENY** — protección contra clickjacking
- **X-Content-Type-Options: nosniff** — previene interpretación incorrecta de archivos
- **Referrer-Policy** — controla información compartida al navegar a sitios externos
- **Permissions-Policy** — deshabilita acceso a cámara, micrófono y geolocalización
- **Strict-Transport-Security** — fuerza HTTPS durante 1 año

7 Procesos automatizados

Align ejecuta tareas automáticas diarias y semanales (recordatorios, resúmenes, alertas). Estos procesos están protegidos mediante un token secreto rotable que solo conoce la infraestructura de Vercel. Cualquier intento de activarlos desde fuera es rechazado automáticamente.

8 Integraciones externas

Align se integra únicamente con proveedores con certificaciones de seguridad vigentes:

Servicio	Propósito	Certificaciones
Google OAuth	Autenticación	ISO 27001, SOC 2, SOC 3
Supabase (PostgreSQL)	Base de datos	SOC 2 Type II
Vercel	Hosting y CDN	SOC 2 Type II
Resend	Emails transaccionales	SOC 2
OpenAI / Anthropic	Procesamiento de IA	SOC 2

Las claves de acceso están almacenadas como variables de entorno cifradas en Vercel, nunca en el código fuente.

9 Privacidad de los datos

- Align no vende ni comparte datos de las instituciones con terceros
- Los datos de transcripción y reuniones son propiedad exclusiva de la institución
- Los modelos de IA no entrenan sobre los datos de los usuarios — OpenAI y Anthropic ofrecen garantías contractuales al respecto
- Cada institución puede solicitar la eliminación completa de sus datos en cualquier momento

10 Actualizaciones y monitoreo

- El código se actualiza de forma continua con validación de tipos (TypeScript) antes de cada deploy
- Los errores de servidor se registran para revisión del equipo técnico
- Las dependencias se mantienen actualizadas para incorporar parches de seguridad

¿PREGUNTAS SOBRE SEGURIDAD?

Si su institución requiere información adicional, una revisión técnica detallada o documentación específica para su área de sistemas, estamos disponibles para responder cualquier consulta antes, durante y después de la implementación.

align.frameops.net