Axiospec: seguridad y tratamiento de datos

Para responsables de TI y revisores de seguridad. Axiospec es un sistema de registros de calibración y de activos desarrollado por CaliTech LLC, Knoxville, Tennessee (Estados Unidos). Esta página describe cómo trata los datos de los clientes el servicio en producción. Todo lo que sigue es una afirmación sobre producción. Última revisión: 21 de septiembre de 2026.

Dos cosas que conviene saber antes de seguir leyendo. Axiospec no tiene hoy ninguna certificación de seguridad, y en la última sección decimos exactamente qué tenemos y qué no, en lugar de obligarte a buscarlo. Axiospec es un sistema de registro documental. Respalda y documenta tu programa de calibración y lo mantiene listo para auditoría. No certifica, asegura ni garantiza tu cumplimiento de ninguna norma.

Dónde están tus datos

Amazon Web Services, una sola cuenta, región **us-east-1 (Norte de Virginia, Estados Unidos)**. Todos los recursos de producción con estado están declarados en esa única región: la base de datos PostgreSQL 16, el bucket de almacenamiento de documentos, el bucket de registros de auditoría, el almacén de secretos y el cómputo de la aplicación.

La red de distribución de contenido que hay delante de la aplicación (Amazon CloudFront) es una red perimetral global. Termina TLS en una ubicación perimetral que puede estar fuera de Estados Unidos y reenvía la solicitud a us-east-1. Las respuestas de la API están configuradas expresamente para **no** almacenarse en caché en el perímetro. Solo se almacenan en caché los recursos estáticos de la aplicación y del sitio web. Los subencargados que se indican más abajo tratan los datos en sus propias ubicaciones.

Cifrado

En tránsito. La aplicación y la API se sirven solo por HTTPS. El HTTP sin cifrar se redirige. La versión mínima de TLS es la 1.2. La conexión desde la CDN hasta la aplicación también usa TLS 1.2. Las conexiones a la base de datos exigen TLS (`sslmode=require`), y el servicio de autenticación se niega a arrancar con una URL de base de datos que no lo exija.

En reposo. La base de datos de producción tiene activado el cifrado del almacenamiento. El bucket de registros de auditoría de la infraestructura se cifra con SSE-S3 (AES-256). Los secretos de la aplicación se guardan en AWS Secrets Manager y se cargan en tiempo de ejecución, en lugar de estar en texto plano en variables de entorno. La cola de mensajes que se usa para las tareas en segundo plano fallidas utiliza el cifrado gestionado por SQS.

Los archivos de evidencia subidos (certificados de calibración, fotos) se almacenan en Amazon S3, que cifra los objetos en reposo por defecto con SSE-S3. Hoy no declaramos ese ajuste de forma explícita en nuestro código de infraestructura, así que lo describimos como el comportamiento por defecto de la

plataforma y no como un control que podamos evidenciar. Todo el cifrado usa claves gestionadas por AWS. No existe la opción de claves gestionadas por el cliente (BYOK).

Aislamiento de red

La base de datos de producción **no es accesible públicamente**. Su única regla de entrada es PostgreSQL desde el propio grupo de seguridad de la aplicación. No se permite ningún rango de IP. La protección contra borrado está activada.

La aplicación se ejecuta dentro de una VPC, en dos zonas de disponibilidad, en subredes privadas sin direcciones IP públicas. El tráfico saliente pasa por una pasarela NAT; el tráfico hacia S3 usa un punto de enlace de pasarela de la VPC y no atraviesa internet. El grupo de seguridad de la aplicación no tiene ninguna regla de entrada.

Todos los buckets de S3 tienen el acceso público bloqueado por completo en los cuatro ajustes. El bucket de la aplicación de página única solo puede leerlo nuestra distribución de CloudFront, lo que se impone con Origin Access Control y una política de bucket limitada a esa distribución. El acceso de escritura de la aplicación al bucket de documentos se limita a `PutObject` y `GetObject` sobre ese bucket.

Separación entre clientes

Axiospec es multiinquilino: una base de datos compartida con un esquema compartido y **una delimitación por inquilino a nivel de fila impuesta en la aplicación**. Cada tabla con datos de clientes lleva un `tenant_id`. La identidad del inquilino se lee de una reclamación del token con firma verificada, nunca de una cabecera ni del cuerpo de una solicitud enviados por el cliente. Los tipos de registro principales (instrumentos, entradas del libro de registros, usuarios) se filtran además mediante un listener global de consultas que añade la condición del inquilino en cada lectura. Los archivos subidos se guardan con claves de objeto con el prefijo del inquilino.

Hay que ser exactos sobre lo que es: se trata de un aislamiento impuesto por la aplicación, no de la seguridad a nivel de fila de PostgreSQL, y no de una base de datos o un esquema separados por cliente.

Dentro de un espacio de trabajo hay un segundo límite. Los permisos por sede pueden restringir a un usuario a plantas o ubicaciones concretas, y el servidor comprueba el ámbito de sede en las operaciones de registrar, aprobar, anular y exportar.

Autenticación y control de acceso

Las contraseñas se guardan como hash PBKDF2-HMAC-SHA256 con 260.000 iteraciones y una sal aleatoria por contraseña, y se verifican en tiempo constante. El inicio de sesión usa un correo electrónico y una contraseña, o el inicio de sesión con Google, que funciona en producción. Las cuentas creadas con Google no tienen una contraseña utilizable.

La protección contra fuerza bruta es un retardo exponencial por cuenta, compartido entre todas las instancias de la aplicación a nivel de base de datos y basado en un hash del identificador, de modo que una cuenta inexistente se comporta exactamente igual que una real. Tiene un límite para que no pueda convertirse en una denegación de servicio contra tus usuarios.

La autenticación en dos factores está disponible y la activa cada usuario. Es una contraseña de un solo uso basada en el tiempo, generada por una aplicación de autenticación, con códigos de recuperación de un solo uso que se muestran una vez y se guardan con hash, y un token opcional de dispositivo de confianza que permite a un dispositivo elegido saltarse el segundo factor hasta que se revoca. No hay opción de WebAuthn, llave de seguridad ni SMS.

Las sesiones usan tokens firmados sin estado con una duración por defecto de 7 días, guardados en el almacenamiento local del navegador. Desactivar o eliminar un usuario tiene efecto inmediato: el estado de la cuenta se vuelve a comprobar en la base de datos en cada solicitud, así que un token existente deja de funcionar en la siguiente llamada de ese usuario. No hay una lista general de revocación, por lo que un token robado a un usuario que sigue activo es válido hasta que caduca.

El control de acceso basado en roles se impone en el servidor, no en el navegador. Cinco roles: superadministrador, administrador, responsable, técnico y auditor. El rol se vuelve a leer de la base de datos en cada solicitud en lugar de confiar en el token. El rol de auditor se impone como de solo lectura en todo el sistema, con una única excepción acotada para generar una exportación de auditoría. Los responsables no pueden ascender a usuarios por encima de su propia autoridad.

Dos controles de la aplicación que le importan a un revisor de calidad. Los registros de calibración confirmados no pueden editarse ni borrarse, algo que impone un trigger de la base de datos, así que se mantiene incluso frente al acceso SQL directo. Las correcciones se añaden como nuevos registros vinculados, con un motivo escrito obligatorio. Y cuando un espacio de trabajo activa la revisión entre quien registra y quien revisa, el sistema no permite que la persona que registró una calibración la apruebe.

Los controles de acceso a la consola de administración de nuestra cuenta de AWS se confirman por separado si se solicitan.

Copias de seguridad y recuperación

Copias de seguridad diarias automáticas de la base de datos con **un periodo de conservación de 14 días**, que permite la recuperación a un momento dado dentro de ese periodo. La protección contra borrado y una instantánea final obligatoria están activadas. En CloudWatch hay alarmas de infraestructura configuradas para la CPU, el almacenamiento y la presión de conexiones de la base de datos, los errores de la aplicación, la limitación de peticiones, la latencia, la tasa de errores 5xx de la CDN y las tareas en segundo plano fallidas, y se envían a una dirección de correo de guardia.

Límites, dichos con honestidad: la base de datos de producción está en una sola zona de disponibilidad. Un fallo de la zona exige una restauración, no una conmutación automática. No publicamos ningún SLA de disponibilidad, ningún RPO ni ningún RTO, y no hemos hecho ningún simulacro de restauración documentado.

Registros y auditoría

Tres capas separadas.

1. **Infraestructura.** AWS CloudTrail está activado en toda la cuenta y en todas las regiones, con validación de la integridad de los archivos de registro, y escribe en un bucket bloqueado y cifrado con una

conservación de 365 días. Cubre los eventos de administración. Los eventos de acceso a nivel de objeto de S3 no están activados, por lo que no existe un rastro a nivel de almacenamiento de "quién descargó qué archivo".

2. **Actividad del espacio de trabajo.** Las invitaciones y revocaciones del equipo, los cambios de rol, el archivado de usuarios y los cambios de correo electrónico, la emisión y revocación de claves de API, los cambios de configuración de SSO y los inicios de sesión por SSO, los cambios de webhooks y los inicios de periodos de prueba de facturación se escriben en un registro de auditoría con el autor, la fecha y hora, los campos modificados y la dirección IP. Los administradores del espacio de trabajo pueden leer su propio registro en la aplicación.
3. **Registros de calibración.** Cada calibración confirmada se escribe en un libro de registros de solo anexión, con el usuario que la registró y la fecha y hora, encadenado con SHA-256 de modo que el hash de cada registro cubre el hash del registro anterior. El contenido de los archivos adjuntos se incorpora a la cadena mediante su hash, no solo la ruta del archivo. Cualquier usuario autenticado puede verificar la cadena completa desde la aplicación.

Un límite de alcance que conviene decir: las modificaciones del registro maestro de un instrumento (etiqueta, número de serie, intervalo de calibración, ubicación) no se escriben hoy en el registro de actividad del espacio de trabajo. Los eventos de calibración en sí están totalmente cubiertos por el libro de registros.

La monitorización de errores de la aplicación se hace con Sentry, con la información de identificación personal desactivada por defecto y una función de depuración propia aplicada a cada evento.

Subencargados y lo que ve cada uno

Tercero	Función	Lo que puede ver
Amazon Web Services (us-east-1)	Alojamiento, base de datos, almacenamiento, correo electrónico, secretos, registros	Todos los datos de los clientes
Stripe	Procesamiento de pagos	El correo electrónico de facturación y un identificador del espacio de trabajo. Los datos de la tarjeta se introducen directamente en Stripe y nunca llegan a los servidores de Axiospec. Ningún dato de calibración ni de instrumentos.
Sentry	Monitorización de errores y rendimiento	Trazas de pila y rutas de solicitud después de la depuración. No se garantiza que nunca contengan un identificador que aparezca en un mensaje de error.
Google (Firebase)	Notificaciones push en el móvil	Tokens push de los dispositivos y el contenido de las notificaciones, como los avisos de calibración próxima
Google (Firebase Analytics)	Analítica de producto solo dentro de la aplicación de Android	Eventos de uso de la aplicación y el identificador interno de usuario que se establece al iniciar sesión. La aplicación de iOS no integra el SDK.

Tercero	Función	Lo que puede ver
Google (Analytics 4)	Analítica de producto y web	Rutas de página y eventos de interacción, también dentro de la aplicación con sesión iniciada. No se transmite ningún dato de calibración. Está implementado Consent Mode v2 con valores por defecto regionales. Google Ads se dejó de usar el 15 de septiembre de 2026 y no se publica ninguna etiqueta publicitaria, conversión publicitaria ni píxel de remarketing.
Google (OAuth)	Inicio de sesión con Google	El evento de inicio de sesión de los usuarios que lo eligen
Google (reconocimiento de voz de Android)	Dictado por voz de lecturas en la aplicación de Android	El audio dictado. Sale del dispositivo; no se reconoce en el propio dispositivo.
Apple (reconocimiento de voz de iOS)	Dictado por voz de lecturas en la aplicación de iOS	El audio dictado, en las mismas condiciones que en Android.
GitHub	Control de código fuente y cadena de despliegue	Código fuente. Ningún dato de clientes.

Si configuras webhooks salientes, los datos de los eventos de calibración también se envían al destino que **tú** eliges, y esa carga útil incluye el nombre del técnico que realizó la calibración. Ese destino es tu subencargado, no el nuestro.

La misma lista está publicada para los clientes en axiospec.com/subprocessors, con lo que recibe cada tercero y por qué. Las dos se mantienen sincronizadas.

Propiedad y exportación de los datos

Tus registros son tuyos. La exportación es autoservicio, ilimitada y no depende de ningún plan de precios. Los responsables, administradores y auditores pueden generar un archivo de auditoría completo en cualquier momento.

El archivo es un único ZIP que contiene:

- `audit_manifest.csv`, una fila por instrumento y después una fila por cada evento de calibración confirmado, incluido el hash de cada registro y el hash del registro anterior en hexadecimal
- `audit_summary.pdf`, un informe legible con el panel de cumplimiento, el resultado de la verificación de integridad, el historial de auditoría completo, el inventario de activos y el detalle de lo que está fuera de tolerancia
- los archivos de evidencia originales, agrupados por etiqueta de instrumento
- un README con el alcance de la exportación, el primer y el último hash de registro, y un procedimiento paso a paso para **volver a verificar por tu cuenta el encadenamiento de la cadena, sin conexión y sin Axiospec**

Las exportaciones pueden acotarse por sede, ubicación, instrumento, rango de fechas o estado de cumplimiento, y el alcance solo puede reducirse dentro de tus propios permisos, nunca ampliarse. Ten en cuenta que una exportación acotada verifica el hash propio de cada registro exportado, pero no afirma la continuidad de toda la cadena, porque es un subconjunto deliberado. Solo una exportación completa, sin alcance, recorre la cadena entera.

Los datos del registro de instrumentos también pueden exportarse a CSV desde el navegador en cualquier momento.

Si dejas de usar Axiospec

La facturación se detiene de inmediato cuando solicitas el cierre de la cuenta. Tus datos se conservan **730 días (unos 24 meses)** después, para que puedas volver a iniciar sesión y exportarlos, y para que puedas reactivar la cuenta si cambias de opinión. Pasado ese periodo se eliminan de forma permanente, incluidos los archivos de evidencia almacenados.

No hay muro de pago para exportar ni formato propietario. Como el archivo de auditoría es CSV en formato abierto más PDF más tus archivos originales más instrucciones escritas para verificar de forma independiente el encadenamiento de la cadena, un tercero puede seguir comprobando el paquete de evidencias aunque Axiospec deje de existir.

Lo que todavía no tenemos

Preferimos decírtelo de entrada a que lo descubras en un cuestionario.

- **Ningún informe SOC 2** (Tipo I ni Tipo II). No se ha realizado ninguna auditoría y no hay ningún auditor contratado. Lo que ofrecemos a cambio: este documento, respuestas directas a tu cuestionario y un contacto con nombre que responde.
- **Ninguna certificación ISO/IEC 27001.** Ten en cuenta que Axiospec da soporte a los programas ISO 9001 e ISO/IEC 17025 de sus clientes. Ese es el ámbito del producto y no tiene relación con nuestra propia certificación de seguridad de la información. No mezclamos las dos cosas.
- **Ninguna prueba de penetración de terceros.** Solo revisión interna.
- **Ningún BAA de HIPAA, y ningún programa FedRAMP, CMMC, NIST 800-171, ITAR ni DFARS 252.204-7012.** No guardes información sanitaria protegida ni información no clasificada controlada en Axiospec.
- **Ningún segundo factor por WebAuthn, llave de seguridad ni SMS.** La autenticación en dos factores de Axiospec es una contraseña de un solo uso basada en el tiempo, generada por una aplicación de autenticación, con códigos de recuperación y un token opcional de dispositivo de confianza. Es el único segundo factor disponible. El SSO empresarial por inquilino (OIDC y SAML 2.0) está activado en producción. Las solicitudes de autenticación SAML no se firman en esta versión.
- **Ningún DPA publicado, condiciones del RGPD, cláusulas contractuales tipo ni región de datos en la UE.** Todos los datos están en Estados Unidos, en us-east-1. Existen borradores de un acuerdo de tratamiento de datos y de las condiciones de transferencia, y están en manos de nuestros abogados. Nada está en vigor, y no vamos a describir un borrador como si lo estuviera.

- **Ningún SLA de disponibilidad, página de estado, RPO ni RTO**, y ningún simulacro de restauración documentado. Las copias de seguridad están configuradas; el tiempo de recuperación no está comprometido.
- **Ningún control de versiones de objetos en el bucket de archivos de evidencia.** Un archivo sobrescrito o eliminado no tiene vía de recuperación a nivel de almacenamiento. El registro de la calibración en el libro de registros se conserva en cualquier caso.
- **Ningún periodo definido de conservación de los registros de la aplicación.** Hoy los registros de la aplicación se conservan indefinidamente por defecto.
- **Ningún paquete de validación del software (IQ/OQ/PQ) y ninguna matriz de trazabilidad de requisitos a pruebas.** Lo que sí tenemos: 2.465 funciones de prueba en 197 archivos de prueba que deben superarse antes de cualquier despliegue en producción, un análisis de vulnerabilidades de dependencias que bloquea la compilación, versiones de producción que solo se lanzan manualmente e imágenes inmutables por versión para poder revertir. Es un control real de desarrollo de software. No es un paquete de validación, y un revisor de validación de sistemas informatizados no debería aceptarlo como tal.
- **Todavía no hay acceso de mínimo privilegio a la infraestructura.** Nuestro rol de despliegue de CI tiene AWS AdministratorAccess. Los despliegues en producción solo se lanzan manualmente y están protegidos por un entorno de GitHub, pero quien pueda lanzar ese flujo de trabajo tiene la administración completa de la cuenta.
- **Ninguna separación de funciones ni revisión formal de accesos.** CaliTech LLC es una empresa de una sola persona. No hay un programa documentado de seguridad del personal, ni un proceso de verificación de antecedentes, ni un programa de formación en seguridad.
- **Ningún plan completo de respuesta a incidentes y ninguna póliza de ciberriesgo verificada.** Lo que sí existe, desde el 21 de septiembre de 2026, es un procedimiento escrito de notificación de brechas: qué cuenta como brecha de datos personales, quién decide, el plazo de 72 horas y a quién se avisa y en qué orden. Es un documento interno y no se ha puesto a prueba en ningún simulacro. En CloudWatch hay alarmas de infraestructura configuradas que se envían a una dirección de correo de guardia, lo que es monitorización y no un proceso de respuesta.

No vamos a describir nada de lo anterior como "en curso" ni como "alineado con" algo que no tenemos.

Contacto de seguridad

Envía las preguntas de seguridad, los cuestionarios o los informes de vulnerabilidades a **support@axiospec.com**. Respondemos en un día hábil. Axiospec es un producto de CaliTech LLC, Knoxville, Tennessee (Estados Unidos).

Si tu revisión necesita un diagrama de arquitectura o de flujo de datos, un cuestionario de seguridad de proveedores completado o una llamada con la persona que escribió el código, pídelo. Recibirás las tres cosas desde la misma dirección.

Axiospec es un producto de CaliTech LLC, Knoxville, Tennessee (Estados Unidos). Axiospec respalda y documenta tu programa de calibración y lo mantiene listo para auditoría. No certifica, asegura ni garantiza la conformidad con ninguna norma; esa determinación corresponde a ti y a tu auditor. Preguntas: support@axiospec.com