Resumen de validación del software

Axiospec, gestión de calibraciones Preparado para el responsable de calidad, el responsable de validación o el revisor de TI que evalúa Axiospec como sistema de registro oficial de calibraciones.

Versión del documento 1.0. Última revisión: 19-08-2026. Publicado por CaliTech LLC, Knoxville, Tennessee (Estados Unidos). Preguntas: support@axiospec.com, con respuesta en un día hábil.

Lee esto primero

Este documento es **una aportación a tu registro de validación. No es un registro de validación.**

Axiospec no valida tu instancia, no certifica tu cumplimiento y no realiza tu cualificación. La validación es una determinación que haces tú sobre tu propio uso previsto, tu configuración, tus procedimientos y tu personal. Tu entidad de certificación, tu evaluador o tu inspector deciden si la cumpliste.

Lo que te da este documento: una declaración de uso previsto, una descripción de los controles de integridad de datos que existen en el producto y de cómo se imponen, una lista de comprobación que puedes ejecutar y firmar en tu propio espacio de trabajo, nuestra práctica de gestión de cambios y una lista clara de lo que el software no hace.

Según la categorización de GAMP 5, un registro SaaS multiinquilino configurado de este tipo suele tratarse como Categoría 4 (producto configurado). Eso significa que tu esfuerzo de validación se basa en el riesgo y se apoya en la documentación del proveedor más tus propias pruebas de configuración y de proceso. Confirma esa categorización con tu propio procedimiento.

1. Declaración de uso previsto

Axiospec es un sistema de registro documental para equipos de medición y ensayo. Su uso previsto es:

- Mantener un registro de instrumentos, con su identificación, fabricante, modelo, número de serie, ubicación, sede y los campos personalizados definidos en el espacio de trabajo.
- Registrar eventos de calibración y verificación sobre esos instrumentos, incluidas las lecturas como se encontró y como se dejó, el valor nominal, la tolerancia, el resultado, las condiciones ambientales, el patrón de referencia utilizado, el número de certificado, el proveedor del servicio y la referencia de trazabilidad.
- Registrar los campos metrológicos que se usan en los flujos de trabajo de ISO/IEC 17025: incertidumbre de medida, factor de cobertura, nivel de confianza, regla de decisión, declaración de conformidad y el número de certificado del propio patrón de referencia.
- Identificar el estado de calibración de cada instrumento y su fecha de próximo vencimiento, y destacar los instrumentos vencidos y los próximos a vencer.
- Conservar esos registros de forma de solo anexión y con detección de manipulaciones, con autoría y marcas de tiempo.

- Enviar los registros de calibración a una aprobación opcional por dos personas antes de que tengan efecto.
- Producir una exportación completa, legible por personas y por máquinas, del registro y de su historial para auditoría.

Axiospec **no** es un laboratorio de calibración acreditado y no realiza mediciones. Cada documento que produce el sistema lleva textualmente esta declaración:

> "Datos de calibración registrados por personal del espacio de trabajo. Axiospec es un sistema de registro documental, no un laboratorio de calibración acreditado, y no realizó esta medición."

Axiospec no es software de dispositivo médico y no se afirma ni se da a entender ninguna relación con IEC 62304. IEC 62304 regula el software que es un dispositivo médico o forma parte de uno. Un registro de calibraciones es una herramienta del sistema de calidad.

Qué cláusulas determinan lo que se espera de un sistema como este

El texto de las cláusulas de las normas ISO está protegido por derechos de autor, así que lo que sigue son referencias a cláusulas con paráfrasis, no citas. Compruébalo con tu propio ejemplar con licencia.

- **ISO 9001:2015, cláusula 7.1.5.2** (trazabilidad de las mediciones): equipos calibrados o verificados a intervalos especificados frente a patrones trazables, identificables en cuanto a su estado de calibración, protegidos contra ajustes que invaliden el resultado, y una evaluación de los resultados anteriores cuando se detecta que un equipo no es apto.
- **ISO 9001:2015, cláusula 7.5.3** (control de la información documentada): disponibilidad, protección contra la pérdida de integridad, control del acceso, almacenamiento y conservación, control de cambios y de versiones, conservación y disposición.
- **ISO 9001:2015, cláusula 8.4** e **ISO/IEC 17025:2017, cláusula 6.6** (productos y servicios suministrados externamente): debes evaluar y registrar tu cualificación de Axiospec como proveedor. Este documento está pensado para servir de evidencia en ese registro.
- **ISO/IEC 17025:2017, cláusula 6.4** (equipamiento), en concreto 6.4.6 (calibración cuando la exactitud o la incertidumbre afectan a la validez), 6.4.8 (etiquetado o codificación del estado para que el usuario pueda identificar fácilmente el estado de calibración o el periodo de validez) y 6.4.13 (el contenido obligatorio de los registros de los equipos).
- **ISO/IEC 17025:2017, cláusula 7.11** (control de los datos y gestión de la información), en concreto 7.11.2 (el sistema de gestión de la información se valida en cuanto a su funcionalidad, incluidas las interfaces) y 7.11.3 (protegido contra el acceso no autorizado, salvaguardado contra manipulaciones y pérdidas, operado según su especificación, mantenido para asegurar la integridad de los datos, y con registro de los fallos y de las acciones correctivas).
- **ISO 13485:2016, cláusula 4.1.6**: procedimientos para validar el software informático que se usa en el SGC, antes del primer uso y tras los cambios, con un enfoque proporcional al riesgo y con registros conservados.
- **21 CFR Part 11**, cuando los registros de calibración son tus registros regulados oficiales: 11.10(a) validación, 11.10(b) copias exactas y completas en formato legible por personas y en formato electrónico,

11.10(c) protección y recuperación rápida, 11.10(d) acceso limitado a personas autorizadas, 11.10(e) pistas de auditoría seguras, generadas por ordenador y con marca de tiempo, en las que "los cambios en los registros no ocultarán la información registrada previamente", 11.10(g) comprobaciones de autoridad, 11.50 manifestaciones de la firma, 11.70 vinculación entre firma y registro.

Ten en cuenta que ISO 9001 no tiene una cláusula explícita de validación del software. Para una empresa que solo aplica 9001, la obligación es el control de la información documentada, no un protocolo de validación. Dimensiona tu esfuerzo en consecuencia.

2. Controles de integridad de datos que existen

2.1 Libro de registros de calibración de solo anexión y con detección de manipulaciones

Cada evento de calibración se escribe en un libro de registros. En cuanto una entrada se confirma (es decir, en cuanto sale del estado de borrador, DRAFT), no puede editarse ni borrarse.

Cómo funciona la detección de manipulaciones. Cada entrada confirmada guarda un `record_hash`: un resumen SHA-256 calculado sobre una serialización JSON canónica, con las claves ordenadas, de los campos de esa entrada, que incluye el `record_hash` de la entrada anterior como `prev_hash`. Las entradas se encadenan por espacio de trabajo en orden de inserción, con `created_at` forzado a ser estrictamente creciente, de modo que el orden es una reproducción determinista. Cualquier alteración, inserción o eliminación de un registro cambia su hash y rompe la cadena desde ese punto en adelante, y la rotura se puede detectar.

Los campos incluidos en el hash son: el activo, el tipo de evento, la marca de tiempo de realización, el usuario que la realizó, el resultado de la calibración, el valor nominal, la tolerancia, las lecturas como se encontró y como se dejó, la temperatura, la humedad, el patrón de referencia, las mediciones, las notas, la referencia del adjunto, el número de certificado, el proveedor del servicio, la referencia de trazabilidad, el motivo de la corrección y los campos metrológicos enumerados en la sección 1.

Los archivos de evidencia se incorporan al hash por su contenido, no solo por su referencia. El SHA-256 del certificado o la foto subidos se calcula en el servidor y se incorpora al hash del registro. Cambiar el archivo que hay detrás de un enlace sin modificar rompe la cadena.

La inmutabilidad la impone la base de datos, no el código de la aplicación. Un trigger de PostgreSQL en la tabla del libro de registros bloquea, a nivel de base de datos: el borrado de una entrada confirmada, la vuelta de una entrada confirmada al estado de borrador y la modificación de cualquier columna de identidad o incluida en el hash de una entrada confirmada. Esto significa que una sesión SQL directa contra la base de datos de producción no puede reescribir en silencio un registro de calibración. Es un control más fuerte que una comprobación en la capa de aplicación, y es precisamente el punto que merece la pena demostrar a un evaluador.

Los cambios se representan añadiendo, nunca sobrescribiendo. Esta es la respuesta directa al requisito de Part 11 de que los cambios en los registros no oculten la información registrada previamente.

- Una **corrección** es una nueva entrada añadida que hace referencia a la entrada que sustituye y lleva un motivo de corrección en texto libre. El motivo es obligatorio (la API rechaza una corrección sin él) y forma parte del hash. La entrada sustituida permanece en el historial, legible por completo.

- Una **anulación** es un evento marcador añadido al libro de registros. El original anulado permanece en el historial con la etiqueta de anulado, y el instrumento vuelve a su calibración anterior o a sin calibrar. Una anulación nunca puede contar como una calibración.

Verificación en un clic. Cualquier usuario autenticado del espacio de trabajo puede ejecutar una verificación completa de la cadena, que recorre cada entrada confirmada, vuelve a calcular cada hash, comprueba la continuidad e informa de un resultado limpio con el número de entradas verificadas o de la primera entrada que no coincide, con la etiqueta de su instrumento. Se registran el resultado y el usuario que verificó.

Verificación independiente fuera de la plataforma. La exportación de auditoría incluye los valores `record_hash` y `prev_hash` en el CSV del manifiesto, más un README con un procedimiento paso a paso para verificar sin conexión el **encadenamiento** de la cadena sin Axiospec: el `prev_hash_hex` de cada fila debe ser igual al `record_hash_hex` de la fila anterior, de modo que cualquier registro eliminado, insertado o reordenado aparece como un enlace roto. Conviene ser preciso sobre el límite. El manifiesto no incluye todos los campos que alimentan la función de hash, por lo que no es posible recalcular el hash de un registro solo a partir del CSV. El nuevo cálculo del hash de un registro individual se hace en el servidor, en la aplicación y en el momento de exportar. El encadenamiento es lo que puedes demostrar tú, sin nosotros, para siempre.

2.2 Pista de auditoría

Registros de calibración. Cada entrada guarda el identificador del usuario que la realizó más una instantánea fija de su nombre, la marca de tiempo de realización y la marca de tiempo de creación en el servidor. Cuando la entrada pasa por revisión, guarda también el identificador y la instantánea del nombre del revisor, la marca de tiempo de la revisión, las notas de revisión y el motivo de rechazo, si lo hay. Los valores anteriores se conservan por construcción: nada se sobrescribe, así que el "valor anterior" es la entrada sustituida, que sigue siendo legible.

Administración del espacio de trabajo. Un registro de actividad aparte guarda las acciones de equipo y de configuración con el usuario que actúa, el objetivo, un registro JSON de lo que cambió, la IP de origen y una marca de tiempo. Entre las acciones cubiertas están las invitaciones y revocaciones de usuarios, los cambios de rol, el archivado de usuarios, 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 en las suscripciones de webhooks y el inicio de periodos de prueba de facturación. Los administradores del espacio de trabajo pueden leerlo en la aplicación, estrictamente limitado al espacio de trabajo de la sesión autenticada y no a un parámetro de la solicitud.

Carencia conocida, declarada. Los cambios en el registro maestro de un instrumento (por ejemplo, su intervalo de calibración) no se recogen hoy en el registro de auditoría del sistema. Los eventos de calibración en sí son inmutables y están totalmente atribuidos. Lo mismo se aplica a la etiqueta, el número de serie y la ubicación de un instrumento. Si tu procedimiento necesita saber "quién cambió el intervalo de este instrumento y cuándo", debes cubrirlo con tu propio control hasta que esto se resuelva. Consulta la sección 6.

2.3 Aprobaciones (quien registra y quien revisa)

La revisión por dos personas está disponible por instrumento o para todo el espacio de trabajo. Es **opcional y está desactivada por defecto.**

Cuando la revisión es obligatoria, el sistema no permite que quien envía un registro lo apruebe. La comprobación es incondicional al principio tanto de la vía de aprobación como de la de rechazo, y también falla de forma cerrada si no se puede resolver la identidad del aprobador. Aprobar exige el rol de responsable o de administrador, comprobado tanto a nivel de toda la organización como en la sede concreta a la que pertenece el instrumento, de modo que a un responsable de toda la organización al que se le ha rebajado el rol en esa sede se le deniega ahí. La ruta genérica de actualización de registros se niega a fijar un estado de aprobado o rechazado, así que el flujo de trabajo no se puede eludir. Las anulaciones siguen el mismo flujo, y una anulación pendiente o rechazada no oculta el original.

Cuando la revisión **no** es obligatoria, el envío se aprueba automáticamente y quien lo envía queda registrado como aprobador. Una persona registra y el registro tiene efecto de inmediato. Dilo con claridad en tu propia evaluación de riesgos, y activa la revisión en los instrumentos en los que tu evaluación de riesgos lo exija.

2.4 Firmas electrónicas

Lo que es real y está disponible. La firma electrónica es un ajuste por espacio de trabajo. Es opcional, no obligatoria. Cuando un espacio de trabajo la activa, la aprobación exige volver a verificar la contraseña de la propia cuenta del aprobador en el momento de firmar, en el servidor y frente al hash de contraseña almacenado, antes de que la aprobación siga adelante. Una contraseña incorrecta se rechaza siempre con un 403, sea cual sea cualquier indicador de configuración. La aplicación móvil pide la contraseña al registrar una calibración. Las contraseñas se guardan como PBKDF2-HMAC-SHA256 con 260.000 iteraciones y una sal aleatoria de 16 bytes por contraseña, y la verificación se hace en tiempo constante. Existe un endpoint de reautenticación independiente con el mismo fin. El usuario que aprueba y la marca de tiempo de la aprobación se registran en el registro inmutable del libro, fijados por el trigger de la base de datos descrito en la sección 2.1.

Dos límites que debes conocer antes de confiar en esto.

1. **Es opcional por espacio de trabajo y hoy no se impone de forma estricta.** Si el cliente no envía ninguna contraseña de firma, la aprobación se completa actualmente y registra una advertencia, en lugar de rechazarse. Solo se rechaza una contraseña incorrecta. El interruptor de imposición estricta existe en el código, pero no está activado en el entorno de producción.
2. **No existe un vínculo criptográfico de firma almacenado.** No esperes un artefacto de firma separado y recuperable en el registro de calibración, ni un indicador de firmado en la API. La evidencia duradera es el propio registro de aprobación: la identidad del aprobador, la instantánea de su nombre, la marca de tiempo de la aprobación y las notas de revisión, todo ello fijado por el trigger de inmutabilidad.

Por tanto, Axiospec **no** cumple hoy 21 CFR 11.50 y 11.70, y no puede cumplirse la expectativa de dos componentes de identificación distintos para sesiones no continuas, porque el producto no tiene autenticación multifactor. Si las firmas electrónicas de Part 11 son un requisito imprescindible para ti, trátalo como una carencia y plantéanoslo antes de comprar.

2.5 Control de acceso basado en roles

Cinco roles: superadministrador, administrador, responsable, técnico y auditor. La imposición se hace **en el servidor**, en cada ruta, mediante dependencias de FastAPI. El rol del usuario se vuelve a resolver desde la base de datos en el momento de la solicitud, en lugar de confiar en el token de sesión, de modo que un token antiguo no puede conservar privilegios elevados. En el cliente también hay restricciones, pero son cosméticas; el servidor es el punto de imposición.

Comportamientos relevantes para 11.10(d) y (g) y para ISO/IEC 17025 7.11.3:

- La autoridad para cambiar roles está acotada. Un responsable solo puede gestionar técnicos. Los permisos para invitar están limitados por rol.
- **El rol de auditor se impone como de solo lectura en todo el sistema.** Todos los métodos HTTP de escritura están bloqueados para los auditores, con exactamente dos excepciones permitidas: solicitar una exportación de la pista de auditoría y revocar su propio token de suscripción al calendario (lo que retira un acceso y nunca concede ninguno). Este es el rol que debes dar a tu entidad de certificación o a un evaluador externo.
- Sobre el rol se superpone un **límite de acceso por sede**. Un usuario puede tener un rol en toda la organización y aun así ver denegado el acceso en una sede concreta, y esto se comprueba al enviar, anular y aprobar calibraciones.
- Solo los responsables y los administradores pueden anular una calibración. Los técnicos solo pueden corregir sus propios registros; los responsables y administradores pueden corregir cualquiera.

Los registros se guardan con una delimitación por espacio de trabajo a nivel de fila impuesta en la capa de acceso a datos, y el espacio de trabajo se toma de una reclamación de sesión con firma verificada, nunca de una cabecera enviada por el cliente. Ten en cuenta la descripción honesta: se trata de una delimitación por espacio de trabajo **impuesta por la aplicación**, no de la seguridad a nivel de fila de PostgreSQL, y no de una base de datos separada por cliente. La inmutabilidad del libro de registros, en cambio, sí la impone la base de datos.

3. Lo que deberías verificar en tu propio entorno

Lo que sigue es un protocolo sugerido que ejecutas y registras tú. Nada de esto se ha ejecutado por ti. Para cada paso, registra la fecha, la persona que lo ejecutó, el resultado esperado, el resultado real, si es conforme o no, y adjunta una captura de pantalla. Según ISO/IEC 17025 7.11.2, esta es la verificación funcional que te corresponde.

Cualificación de la instalación (IQ), configuración registrada

N.º	Comprobación	Registro
IQ-1	Nombre del espacio de trabajo, URL de la aplicación y fecha del primer uso en producción	
IQ-2	Usuarios con nombre, sus roles y sus permisos por sede	

N.º	Comprobación	Registro
IQ-3	Ajustes del espacio de trabajo registrados: aprobaciones obligatorias sí/no, firma electrónica activada/desactivada, módulos activados, campos personalizados definidos	
IQ-4	Sedes y ubicaciones configuradas, coincidentes con tu lista de instalaciones	
IQ-5	Registro de instrumentos cargado, con el recuento conciliado con tu registro de origen	
IQ-6	Registro de cualificación de proveedor abierto para CaliTech LLC, con este documento adjunto	
IQ-7	Tu SOP controlado que designa a Axiospec como sistema de registro de calibraciones, emitido y aprobado dentro de tu control documental	

Cualificación operacional (OQ), pruebas funcionales

N.º	Prueba	Resultado esperado
OQ-1	Registrar una calibración en un instrumento de prueba	La entrada aparece en el historial de ese instrumento con tu nombre, la fecha de realización y las lecturas registradas
OQ-2	Intentar editar ese registro confirmado	El sistema lo rechaza y te indica que emitas una corrección
OQ-3	Intentar borrar ese registro confirmado	El sistema lo rechaza e indica que el libro de registros es de solo anexión
OQ-4	Emitir una corrección sin motivo y después con motivo	Rechazada sin motivo; aceptada con él; la entrada original sigue visible en el historial
OQ-5	Como responsable, anular una calibración	El original sigue en el historial con la etiqueta de anulado; el estado del instrumento vuelve a la calibración anterior o a sin calibrar
OQ-6	Como técnico, intentar anular una calibración	Rechazado
OQ-7	Activar la aprobación para un instrumento. Enviar una calibración como usuario A y después intentar aprobarla como usuario A	Rechazado, citando la separación entre quien registra y quien revisa
OQ-8	Aprobarla como usuario B	El nombre del aprobador y la marca de tiempo de la aprobación se registran en la entrada y se ven en el historial
OQ-9	Iniciar sesión como usuario con rol de auditor e intentar cualquier cambio	Todas las escrituras rechazadas

N.º	Prueba	Resultado esperado
OQ-10	Asignar un usuario solo a la Sede 1 y después intentar actuar sobre un instrumento de la Sede 2	Rechazado
OQ-11	Ejecutar la verificación de la cadena desde el área de auditoría	Informa de que está verificada, con el número de entradas verificadas. Registra la fecha, el número y el usuario que verificó
OQ-12	Generar una exportación de auditoría sin alcance	Se descarga un ZIP con audit_manifest.csv, audit_summary.pdf, la guía de verificación README y los archivos adjuntos
OQ-13	Seguir el procedimiento del README para verificar sin conexión el encadenamiento de la cadena	El `prev_hash_hex` de cada fila es igual al `record_hash_hex` de la fila anterior
OQ-14	Registrar un resultado fuera de tolerancia	El instrumento queda señalado; la evaluación del impacto fuera de tolerancia puede registrarse una vez y después queda bloqueada
OQ-15	Confirmar que el estado de calibración y la fecha de próximo vencimiento se muestran correctamente para un instrumento conocido (ISO/IEC 17025 6.4.8)	El estado y la fecha de vencimiento coinciden con lo esperado
OQ-16	Cambiar el rol de un usuario y después abrir el registro de actividad del espacio de trabajo	El cambio aparece con el usuario que actuó, el objetivo y la marca de tiempo
OQ-17	Editar el intervalo de calibración de un instrumento y después revisar el registro de actividad	**No aparece ninguna entrada. Es la carencia conocida de la sección 2.2.** Regístrala como carencia de control y documenta tu control compensatorio
OQ-18	Imprimir o exportar un certificado de calibración de un registro aprobado y después intentar lo mismo con un registro anulado	Se produce el certificado del registro aprobado; se rechaza para el anulado

Cualificación del desempeño (PQ), tu proceso con tu personal

N.º	Actividad
PQ-1	Definir el periodo (es preferible un ciclo de calibración completo; un mes es un mínimo habitual)
PQ-2	Trabajar en paralelo con tu registro actual durante ese periodo. Conciliar al final el número de instrumentos y las fechas de vencimiento
PQ-3	Confirmar que los avisos de próximos vencimientos y de vencidos llegan a las personas adecuadas en el calendario previsto
PQ-4	Confirmar que tus técnicos pueden completar un registro de calibración según tu SOP sin soluciones provisionales

N.º	Actividad
PQ-5	Hacer una auditoría simulada. Elegir un instrumento al azar y presentar: el historial completo, la referencia de trazabilidad, el patrón de referencia utilizado, los adjuntos de evidencia y la prueba de que el registro no se ha alterado
PQ-6	Gestionar de principio a fin un evento real fuera de tolerancia, incluida la evaluación del impacto en las mediciones anteriores (ISO 9001 7.1.5.2)
PQ-7	Verificar la vía de contingencia de tu SOP para cuando el sistema no esté disponible
PQ-8	Redactar y aprobar el informe resumen de validación. Firmarlo

Recualificación. Define qué desencadena una nueva prueba. Una regla práctica para un SaaS de Categoría 4: volver a ejecutar el subconjunto de la OQ que afecta a cualquier función de la que dependas siempre que cambies de forma sustancial tu configuración (ajustes de aprobación, roles, sedes, campos personalizados, adaptación a normas), y con un intervalo de revisión periódica que definas tú. Consulta en la sección 5 cómo funcionan los cambios por parte del proveedor.

4. Conservación y exportación de registros

La exportación es autoservicio, completa y no depende de un plan de pago ni de una solicitud de soporte. Pueden generarla los responsables, administradores y auditores. Los técnicos conservan el historial por instrumento en la aplicación, pero no la exportación de todo el espacio de trabajo.

La exportación es un único ZIP que contiene:

- `audit_manifest.csv`: una fila por registro de instrumento y después una fila por cada evento de calibración confirmado. Unas 45 columnas, entre ellas la identificación del instrumento, la sede y la ubicación, todos los campos de calibración, los campos metrológicos, los campos de aprobación y de revisor, el impacto fuera de tolerancia, los campos personalizados del espacio de trabajo como JSON y los valores `record_hash_hex` y `prev_hash_hex`. Las columnas de hash se excluyen a propósito de la protección contra la inyección de fórmulas en CSV, para que sean exactas byte a byte al comparar el encadenamiento.
- `audit_summary.pdf`: un informe legible con un panel de cumplimiento, una sección de verificación de integridad con detección de manipulaciones que indica el veredicto de la cadena, el número de entradas verificadas, el algoritmo de hash y los hashes del registro génesis y del más reciente, y después el historial de auditoría de calibraciones, el inventario de instrumentos y el detalle de lo que está fuera de tolerancia. La tabla de excepciones muestra los 20 eventos más recientes que cumplen el criterio; el conjunto completo está en `audit_manifest.csv`.
- `assets/<tag>/...`: los propios archivos de evidencia, en su formato original, agrupados por etiqueta de instrumento.
- Una guía de verificación README con el alcance de la exportación, los recuentos de cobertura, la explicación de la cadena de hashes y el procedimiento de verificación del encadenamiento sin conexión.

El archivo está pensado para apoyar tu determinación respecto a 11.10(b): proporciona los registros tanto en formato legible por personas (PDF) como en formato electrónico (CSV). Si cumple 11.10(b) para tus registros es una determinación tuya. También es la respuesta práctica a las preguntas sobre la continuidad del proveedor: el paquete es autónomo, está en formato abierto y su encadenamiento se puede comprobar sin nosotros.

Alcance y un límite importante. Las exportaciones pueden acotarse por sede, ubicación, instrumentos concretos, rango de fechas y estado, y el alcance siempre se cruza con los permisos de sede de quien la solicita, por lo que solo puede reducirse. **Una exportación acotada o limitada por fechas vuelve a verificar el hash propio de cada registro exportado, pero no afirma la continuidad de la cadena entre registros, porque un conjunto filtrado es un subconjunto deliberado de la cadena.** Solo una exportación sin alcance y con todo el historial recorre la cadena completa. Usa una exportación sin alcance cuando necesites la prueba de continuidad. El README también lo indica.

Conservación mientras la cuenta está activa: los registros se conservan durante toda la vida del espacio de trabajo. Nadie, ni siquiera nosotros, puede editar ni borrar un registro de calibración confirmado individual.

Conservación tras el cierre: cuando se cierra una cuenta, los datos se conservan **730 días (unos 24 meses)** para que puedas volver a iniciar sesión y exportar. La facturación se cancela de inmediato al solicitarlo, así que no se factura nada durante ese periodo. Pasado ese periodo, una purga definitiva borra los datos del espacio de trabajo en todas las tablas y elimina los archivos de evidencia almacenados. Esa purga es la **única** vía autorizada por la que se eliminan filas confirmadas del libro de registros, y es una operación sobre todo el espacio de trabajo, nunca un borrado por registro.

Copias de seguridad: la base de datos de producción tiene copias de seguridad diarias automáticas con un periodo de conservación de 14 días, protección contra borrado activada y una instantánea final ante cualquier desmantelamiento de la instancia. Consulta en la sección 6 lo que no afirmamos sobre la recuperación.

Alojamiento: la producción se ejecuta en Amazon Web Services, en us-east-1 (Estados Unidos). La base de datos está cifrada en reposo y no tiene acceso público desde internet. La aplicación y la API se sirven solo por HTTPS con TLS 1.2 como mínimo. AWS CloudTrail está activado en toda la cuenta con validación de la integridad de los archivos de registro y un periodo de conservación de 365 días. En axiospec.com/security se publica una descripción general de la seguridad aparte.

5. Gestión de cambios

Cómo se hacen y se controlan los cambios.

- Los despliegues en producción **solo se lanzan manualmente**. No hay ningún envío automático a producción.
- Un despliegue en producción se bloquea salvo que antes se superen tres tareas: el conjunto completo de pruebas del backend, una tarea de validación del esquema OpenAPI y una auditoría de vulnerabilidades de dependencias. Si el conjunto de pruebas falla, el despliegue se detiene.
- El conjunto de pruebas del backend consta de **2.465 funciones de prueba en 197 archivos de prueba**. Hay además 233 archivos de prueba en el frontend web. Son pruebas de regresión automatizadas que se

ejecutan con cada cambio.
- Cada compilación de producción se publica con una etiqueta de imagen inmutable por commit, de modo que hay un destino de reversión definido para cada versión.
- Staging y producción son entornos separados, con infraestructura separada. Los cambios llegan primero a staging.

Hay que tener claro lo que esto es y lo que no es. Un conjunto de pruebas automatizadas de ese tamaño es un control de desarrollo de software real y citable, y es buena materia prima para un argumento de cualificación operacional. **No** es un paquete de validación. No está escrito a partir de una especificación funcional formal, no hay matriz de trazabilidad de requisitos a pruebas y no hay registro de versión firmado. Un revisor de validación de sistemas informatizados no lo aceptará como tal, y nosotros no lo presentaremos como tal.

Cómo te enteras de que algo cambia.

Axiospec es software como servicio multiinquilino. Todos los clientes usan una única versión de producción. **No puedes fijar una versión, aplazar una actualización ni usar una versión anterior.** Es una restricción real para un entorno validado y deberías registrarla en tu evaluación de riesgos.

Hoy **no hay un registro de cambios publicado, ni una página de notas de versión, ni un compromiso escrito de notificación de cambios.** Si tu procedimiento exige aviso previo de los cambios en un sistema validado, pídenos ese compromiso por escrito antes de comprar, en support@axiospec.com. Preferimos decirte que no existe a que lo descubras durante una auditoría.

Lo que te sugerimos hacer al respecto, dado lo anterior: define en tu SOP un intervalo de reverificación periódica (por ejemplo, volver a ejecutar el subconjunto de la OQ cada trimestre y después de cualquier cambio que notes en una función de la que dependas), y vuelve a ejecutar la verificación de la cadena y a registrar el resultado con ese mismo intervalo. La verificación de la cadena se hace con un clic y produce un resultado fechado y atribuible.

6. Límites de lo que hace este software

Dichos con claridad, porque es más fácil cualificar a un proveedor pequeño que nombra sus límites que a uno que los esquiva.

Certificaciones y evaluaciones que no tenemos. Ningún SOC 2, ni Tipo I ni Tipo II. Ninguna ISO/IEC 27001. Ninguna prueba de penetración de terceros. Ningún acuerdo de asociado comercial de HIPAA, y no aceptamos información sanitaria protegida. Ningún FedRAMP, StateRAMP, CMMC, NIST 800-171, ITAR, EAR ni DFARS 252.204-7012. Si manejas información no clasificada controlada o datos sujetos a control de exportaciones, Axiospec no encaja hoy contigo. Ningún anexo de tratamiento de datos publicado, ninguna cláusula contractual tipo y ninguna residencia de datos en la UE; todos los datos están en Estados Unidos.

Ningún paquete de validación del proveedor. No hay ningún paquete IQ/OQ/PQ, ningún protocolo de validación, ninguna matriz de trazabilidad y ningún informe resumen de validación elaborado por nosotros. La sección 3 es una lista de comprobación para que la ejecutes tú, no una evidencia de que se haya ejecutado algo.

Ninguna declaración de cumplimiento. Axiospec no certifica, asegura ni garantiza tu cumplimiento de ninguna norma. Respalda y documenta los registros de calibración y los mantiene listos para auditoría. La conformidad la determinan tu unidad de calidad, tu entidad de certificación, tu organismo de acreditación o tu inspector.

No afirmamos la conformidad con 21 CFR Part 11. Las piezas que sostienen la integridad de los registros son realmente sólidas: inmutabilidad impuesta por la base de datos, una cadena de hashes SHA-256, entradas atribuidas y con marca de tiempo, correcciones de solo anexión que no ocultan la información anterior y revisión por dos personas. Los controles de firma todavía no están. Consulta la sección 2.4: la firma electrónica es opcional por espacio de trabajo en lugar de obligatoria, no hay un vínculo de firma almacenado en el registro, no hay un campo con el significado de la firma y no hay identificación multifactor. Publicamos una correspondencia de funciones con las carencias marcadas; no publicamos una declaración de cumplimiento.

Ninguna autenticación multifactor. No hay TOTP integrado, ni aplicación de autenticación, ni WebAuthn, ni SMS, ni códigos de respaldo. La única vía hoy hacia un segundo factor es iniciar sesión con Google, donde lo impone tu propio proveedor de identidad. El SSO empresarial por espacio de trabajo mediante OIDC y SAML está construido y probado en el backend, pero no está activado en producción y debe considerarse disponible bajo petición, no una función disponible. Si tu política de TI exige MFA obligatoria para todos los sistemas del SGC, hoy esto es un bloqueo total. Pregúntanos por el estado actual antes de comprar.

Los cambios en el registro maestro de los activos no se registran. Sección 2.2 y prueba OQ-17. Los eventos de calibración están totalmente cubiertos por el libro de registros. Los cambios en el registro descriptivo del instrumento, incluido su intervalo de calibración, no quedan atribuidos en el registro de actividad.

Las exportaciones filtradas no demuestran la continuidad de la cadena. Sección 4. Usa una exportación sin alcance para eso.

Ningún compromiso de disponibilidad. No hay SLA de disponibilidad, ni página de estado, ni historial de disponibilidad publicado. La base de datos de producción es una única instancia en una única zona de disponibilidad, así que un fallo de la zona de disponibilidad exige una restauración en lugar de una conmutación. No publicamos un objetivo de tiempo de recuperación ni de punto de recuperación, y no se ha documentado ningún simulacro de restauración. Las copias de seguridad están configuradas y se conservan 14 días; es una afirmación cierta sobre las copias de seguridad, no una afirmación probada sobre la recuperación. Tu SOP debería incluir una contingencia para cuando el sistema no esté disponible, algo que los evaluadores de ISO/IEC 17025 preguntan de todos modos.

Ningún plan documentado de respuesta a incidentes ni plazo contractual de notificación de brechas. En CloudWatch hay alarmas de infraestructura configuradas que se envían a una dirección de correo de guardia. Eso es monitorización, no un programa de respuesta a incidentes.

Ninguna clave de cifrado gestionada por el cliente. El cifrado usa claves gestionadas por AWS.

Los registros solo pueden borrarse de una manera. Nadie puede editar ni borrar un registro confirmado individual. La única vía de borrado es una purga de todo el espacio de trabajo solicitada por el cliente, tras el periodo de conservación de 730 días.

No realizamos calibraciones. Axiospec es un sistema de registro documental, no un laboratorio de calibración acreditado, y no realizó ninguna de las mediciones de tus registros.

Cómo usar este documento. Adjúntalo a tu registro de cualificación de proveedor para CaliTech LLC (ISO 9001, cláusula 8.4; ISO/IEC 17025, cláusula 6.6). Menciónalo en tu plan de validación como la descripción funcional y de controles del proveedor. Ejecuta la sección 3 en tu propio espacio de trabajo y conserva el resultado firmado como tu evidencia de cualificación. Registra los límites de la sección 6 en tu evaluación de riesgos junto con tus controles compensatorios.

Si una afirmación de este documento no coincide con lo que observas en el producto, dínoslo en support@axiospec.com y corregiremos el documento.
