# Resumo de validação do software

**Axiospec, gestão de calibração** Preparado para o gerente da qualidade, o responsável pela validação ou o revisor de TI que avalia o Axiospec como sistema oficial de registro de calibrações.

Versão do documento 1.0. Última revisão em 19/08/2026. Publicado pela CaliTech LLC, Knoxville, Tennessee (Estados Unidos). Dúvidas: support@axiospec.com, com resposta em até um dia útil.

## Leia isto primeiro

Este documento é **uma entrada para o seu registro de validação. Ele não é um registro de validação.**

O Axiospec não valida a sua instância, não certifica a sua conformidade e não executa a sua qualificação. A validação é uma determinação que você faz sobre o seu próprio uso pretendido, a sua configuração, os seus procedimentos e as suas pessoas. O seu organismo certificador, o seu avaliador ou o seu inspetor decide se você a atendeu.

O que este documento oferece: uma declaração de uso pretendido, uma descrição dos controles de integridade de dados que existem no produto e de como são impostos, uma lista de verificação que você pode executar e assinar no seu próprio espaço de trabalho, a nossa prática de gestão de mudanças e uma lista clara do que o software não faz.

Pela categorização do GAMP 5, um cadastro SaaS multilocatário configurado desse tipo costuma ser tratado como Categoria 4 (produto configurado). Isso significa que o seu esforço de validação é baseado em risco e se apoia na documentação do fornecedor, mais os seus próprios testes de configuração e de processo. Confirme essa categorização com o seu próprio procedimento.

## 1. Declaração de uso pretendido

O Axiospec é um sistema de guarda de registros para equipamentos de medição e ensaio. O uso pretendido é:

- Manter um cadastro de instrumentos, incluindo identificação, fabricante, modelo, número de série, local, unidade e campos personalizados definidos no espaço de trabalho.
- Registrar eventos de calibração e de verificação desses instrumentos, incluindo as leituras antes do ajuste e após o ajuste, o valor nominal, a tolerância, o resultado, as condições ambientais, o padrão de referência utilizado, o número do certificado, o prestador de serviço e a referência de rastreabilidade.
- Registrar os campos metrológicos usados nos fluxos de trabalho da ISO/IEC 17025: incerteza de medição, fator de abrangência, nível de confiança, regra de decisão, declaração de conformidade e o número do certificado do próprio padrão de referência.
- Identificar a situação de calibração de cada instrumento e a data do próximo vencimento, e destacar os instrumentos vencidos e os que vão vencer em breve.

- Manter esses registros de forma somente de acréscimo e com detecção de adulteração, com autoria e carimbos de data e hora.
- Encaminhar os registros de calibração para uma aprovação opcional por duas pessoas antes que passem a valer.
- Gerar uma exportação completa, legível por pessoas e por máquinas, do cadastro e do seu histórico para auditoria.

O Axiospec **não** é um laboratório de calibração acreditado e não realiza medições. Todo documento que o sistema gera traz esta declaração, palavra por palavra:

> "Dados de calibração registrados por pessoal do espaço de trabalho. O Axiospec é um sistema de guarda de registros, não um laboratório de calibração acreditado, e não realizou esta medição."

O Axiospec não é software de dispositivo médico, e nenhuma relação com a IEC 62304 é afirmada ou sugerida. A IEC 62304 rege o software que é um dispositivo médico ou faz parte de um. Um cadastro de calibrações é uma ferramenta do sistema da qualidade.

### Quais cláusulas definem as expectativas para um sistema como este

O texto das cláusulas das normas ISO é protegido por direitos autorais, então o que segue são referências a cláusulas com paráfrase, e não citações. Confira com o seu próprio exemplar licenciado.

- **ISO 9001:2015, cláusula 7.1.5.2** (rastreabilidade de medição): equipamentos calibrados ou verificados em intervalos especificados contra padrões rastreáveis, identificáveis quanto à situação de calibração, protegidos contra ajustes que invalidem o resultado, e uma avaliação dos resultados anteriores quando um equipamento é considerado inadequado.
- **ISO 9001:2015, cláusula 7.5.3** (controle de informação documentada): disponibilidade, proteção contra perda de integridade, controle de acesso, armazenamento e preservação, controle de alterações e de versões, retenção e disposição.
- **ISO 9001:2015, cláusula 8.4** e **ISO/IEC 17025:2017, cláusula 6.6** (produtos e serviços providos externamente): você deve avaliar e registrar a sua qualificação do Axiospec como fornecedor. Este documento foi pensado para servir de evidência nesse registro.
- **ISO/IEC 17025:2017, cláusula 6.4** (equipamentos), em especial 6.4.6 (calibração quando a exatidão ou a incerteza afetam a validade), 6.4.8 (etiquetagem ou codificação da situação para que o usuário identifique facilmente a situação de calibração ou o período de validade) e 6.4.13 (o conteúdo exigido nos registros dos equipamentos).
- **ISO/IEC 17025:2017, cláusula 7.11** (controle de dados e gestão da informação), em especial 7.11.2 (o sistema de gestão da informação é validado quanto à funcionalidade, incluindo as interfaces) e 7.11.3 (protegido contra acesso não autorizado, salvaguardado contra adulteração e perda, operado conforme a especificação, mantido para assegurar a integridade dos dados, com falhas e ações corretivas registradas).
- **ISO 13485:2016, cláusula 4.1.6**: procedimentos para validar o software de computador usado no SGQ, antes do primeiro uso e após alterações, com abordagem proporcional ao risco e registros mantidos.

- **21 CFR Part 11**, quando os registros de calibração são os seus registros regulados oficiais: 11.10(a) validação, 11.10(b) cópias exatas e completas em forma legível por pessoas e em forma eletrônica, 11.10(c) proteção e recuperação rápida, 11.10(d) acesso limitado a pessoas autorizadas, 11.10(e) trilhas de auditoria seguras, geradas por computador e com carimbo de data e hora, em que "as alterações nos registros não devem ocultar informações registradas anteriormente", 11.10(g) verificações de autoridade, 11.50 manifestações de assinatura, 11.70 vinculação entre assinatura e registro.

Observe que a ISO 9001 não tem uma cláusula explícita de validação de software. Para uma empresa que segue apenas a 9001, a obrigação é o controle da informação documentada, e não um protocolo de validação. Dimensione o seu esforço de acordo.

## 2. Controles de integridade de dados que existem

### 2.1 Livro-razão de calibrações somente de acréscimo e com detecção de adulteração

Todo evento de calibração é gravado em um livro-razão. Depois que um lançamento é confirmado (ou seja, depois que sai do estado de rascunho, DRAFT), ele não pode ser editado nem excluído.

**Como funciona a detecção de adulteração.** Cada lançamento confirmado guarda um `record_hash`: um resumo SHA-256 calculado sobre uma serialização JSON canônica, com as chaves ordenadas, dos campos desse lançamento, que inclui o `record_hash` do lançamento anterior como `prev_hash`. Os lançamentos são encadeados por espaço de trabalho na ordem de inserção, com `created_at` forçado a ser estritamente crescente, de modo que a ordem é uma reprodução determinística. Qualquer alteração, inserção ou remoção de um registro muda o hash dele e quebra a cadeia daquele ponto em diante, e a quebra pode ser detectada.

Os campos incluídos no hash são: o ativo, o tipo de evento, o carimbo de data e hora da execução, o usuário que executou, o resultado da calibração, o valor nominal, a tolerância, as leituras antes do ajuste e após o ajuste, a temperatura, a umidade, o padrão de referência, as medições, as notas, a referência do anexo, o número do certificado, o prestador de serviço, a referência de rastreabilidade, o motivo da correção e os campos metrológicos listados na seção 1.

**Os arquivos de evidência entram no hash pelo conteúdo, não só pela referência.** O SHA-256 do certificado ou da foto enviados é calculado no servidor e incorporado ao hash do registro. Trocar o arquivo por trás de um link inalterado quebra a cadeia.

**A imutabilidade é imposta pelo banco de dados, não pelo código do aplicativo.** Um trigger do PostgreSQL na tabela do livro-razão bloqueia, no nível do banco de dados: a exclusão de um lançamento confirmado, a volta de um lançamento confirmado para rascunho e a alteração de qualquer coluna de identificação ou incluída no hash de um lançamento confirmado. Isso significa que uma sessão SQL direta no banco de dados de produção não consegue reescrever em silêncio um registro de calibração. É um controle mais forte do que uma verificação na camada de aplicação, e é justamente o ponto que vale a pena demonstrar a um avaliador.

**As mudanças são representadas por acréscimo, nunca por sobrescrita.** Essa é a resposta direta à exigência da Part 11 de que as alterações nos registros não ocultem informações registradas anteriormente.

- Uma **correção** é um novo lançamento acrescentado que faz referência ao lançamento que substitui e traz um motivo de correção em texto livre. O motivo é obrigatório (a API rejeita uma correção sem motivo) e faz parte do hash. O lançamento substituído continua no histórico, legível por inteiro.
- Uma **anulação** é um evento marcador acrescentado ao livro-razão. O original anulado continua no histórico com a etiqueta de anulado, e o instrumento volta para a calibração anterior ou para não calibrado. Uma anulação nunca pode ser contada como calibração.

**Verificação com um clique.** Qualquer usuário autenticado do espaço de trabalho pode executar uma verificação completa da cadeia, que percorre cada lançamento confirmado, recalcula cada hash, verifica a continuidade e informa um resultado limpo com o número de lançamentos verificados ou o primeiro lançamento divergente com a tag do instrumento. O resultado e o usuário que fez a verificação ficam registrados.

**Verificação independente fora da plataforma.** A exportação de auditoria inclui os valores `record_hash` e `prev_hash` no CSV do manifesto, mais um README com um procedimento passo a passo para verificar off-line o **encadeamento** da cadeia sem o Axiospec: o `prev_hash_hex` de cada linha deve ser igual ao `record_hash_hex` da linha anterior, de modo que qualquer registro removido, inserido ou reordenado aparece como um vínculo quebrado. É preciso ser exato sobre o limite. O manifesto não traz todos os campos que alimentam a função de hash, então não é possível recalcular o hash de um registro apenas a partir do CSV. O novo cálculo do hash de um registro individual acontece no servidor, no aplicativo e no momento da exportação. O encadeamento é o que você consegue provar sozinho, sem nós, para sempre.

### 2.2 Trilha de auditoria

**Registros de calibração.** Cada lançamento guarda o identificador do usuário que executou mais um instantâneo fixo do nome dele, o carimbo de data e hora da execução e o carimbo de data e hora de criação no servidor. Quando o lançamento passa por revisão, ele também guarda o identificador e o instantâneo do nome do revisor, o carimbo de data e hora da revisão, as notas de revisão e o motivo da rejeição, se houver. Os valores anteriores são preservados por construção: nada é sobrescrito, então o "valor anterior" é o lançamento substituído, que continua legível.

**Administração do espaço de trabalho.** Um log de atividade separado registra as ações de equipe e de configuração com o usuário que agiu, o alvo, um registro JSON do que mudou, o IP de origem e um carimbo de data e hora. As ações cobertas incluem convites e revogações de usuários, mudanças de função, arquivamento de usuários, mudanças de e-mail, emissão e revogação de chaves de API, mudanças na configuração de SSO e logins por SSO, mudanças nas assinaturas de webhooks e o início do período de teste do faturamento. Os administradores do espaço de trabalho podem lê-lo no aplicativo, com escopo rígido no espaço de trabalho da sessão autenticada, e não em um parâmetro da solicitação.

**Lacuna conhecida, declarada.** As alterações no cadastro mestre de um instrumento (por exemplo, o intervalo de calibração) ainda não são registradas no log de auditoria do sistema. Os eventos de calibração em si são imutáveis e totalmente atribuídos. O mesmo vale para a tag, o número de série e o local de um instrumento. Se o seu procedimento precisa saber "quem mudou o intervalo deste instrumento e quando", você deve cobrir isso com um controle próprio até que essa lacuna seja fechada. Veja a seção 6.

### 2.3 Aprovações (quem registra e quem aprova)

A revisão por duas pessoas está disponível por instrumento ou para todo o espaço de trabalho. Ela é **opcional e vem desativada por padrão.**

Quando a revisão é obrigatória, o sistema não deixa quem enviou aprovar o próprio registro. A verificação é incondicional logo no início tanto do caminho de aprovação quanto do de rejeição, e também falha de forma fechada se a identidade do aprovador não puder ser resolvida. Aprovar exige a função de gerente ou de administrador, verificada tanto em toda a organização quanto na unidade específica a que o instrumento pertence, de modo que um gerente de toda a organização que foi rebaixado naquela unidade tem o acesso negado ali. A rota genérica de atualização de registros se recusa a definir um status de aprovado ou rejeitado, então o fluxo de trabalho não pode ser contornado. As anulações seguem o mesmo fluxo, e uma anulação pendente ou rejeitada não oculta o original.

Quando a revisão **não** é obrigatória, o envio é aprovado automaticamente e quem enviou é registrado como aprovador. Uma pessoa registra e o registro passa a valer imediatamente. Deixe isso claro na sua própria avaliação de riscos e ative a revisão nos instrumentos em que a sua avaliação de riscos exigir.

### 2.4 Assinaturas eletrônicas

**O que é real e está disponível.** A assinatura eletrônica é uma configuração por espaço de trabalho. Ela é opcional, não obrigatória. Quando um espaço de trabalho a ativa, a aprovação exige que a senha da própria conta do aprovador seja verificada de novo no momento da assinatura, no servidor e contra o hash de senha armazenado, antes que a aprovação prossiga. Uma senha errada é sempre recusada com um 403, independentemente de qualquer indicador de configuração. O aplicativo móvel exige a senha quando uma calibração é registrada. As senhas são armazenadas como PBKDF2-HMAC-SHA256 com 260.000 iterações e um salt aleatório de 16 bytes por senha, e a verificação é feita em tempo constante. Existe um endpoint de reautenticação independente com a mesma finalidade. O usuário que aprova e o carimbo de data e hora da aprovação são gravados no registro imutável do livro-razão, fixados pelo trigger do banco de dados descrito na seção 2.1.

**Dois limites que você precisa conhecer antes de confiar nisso.**

1. **É opcional por espaço de trabalho e hoje não é imposto de forma rígida.** Se o cliente não enviar nenhuma senha de assinatura, a aprovação atualmente é concluída e registra um aviso, em vez de ser recusada. Só uma senha errada é recusada. A chave de imposição rígida existe no código, mas não está ativada no ambiente de produção.
2. **Não existe vínculo criptográfico de assinatura armazenado.** Não espere um artefato de assinatura separado e recuperável no registro de calibração, nem um indicador de assinado na API. A evidência duradoura é o próprio registro de aprovação: a identidade do aprovador, o instantâneo do nome do aprovador, o carimbo de data e hora da aprovação e as notas de revisão, tudo fixado pelo trigger de imutabilidade.

Portanto, hoje o Axiospec **não** atende ao 21 CFR 11.50 e 11.70, e a expectativa de dois componentes de identificação distintos para sessões não contínuas não pode ser atendida, porque o produto não tem autenticação multifator. Se as assinaturas eletrônicas da Part 11 forem um requisito obrigatório para você, trate isso como uma lacuna e fale conosco antes de comprar.

### 2.5 Controle de acesso baseado em funções

São cinco funções: superadministrador, administrador, gerente, técnico e auditor. A imposição é feita **no servidor**, em todas as rotas, por meio de dependências do FastAPI. A função do usuário é resolvida de novo a partir do banco de dados no momento da solicitação, em vez de se confiar no token de sessão, de modo que um token antigo não carrega privilégios elevados. Também existem restrições no cliente, mas elas são cosméticas; o servidor é o ponto de imposição.

Comportamentos relevantes para 11.10(d) e (g) e para a ISO/IEC 17025 7.11.3:

- A autoridade para mudar funções é limitada. Um gerente só pode gerenciar técnicos. As permissões para convidar são restritas por função.
- **A função de auditor é imposta como somente leitura em todo o sistema.** Todos os métodos HTTP de gravação são bloqueados para auditores, com exatamente duas exceções permitidas: solicitar uma exportação da trilha de auditoria e revogar o próprio token do feed de calendário (o que remove um acesso e nunca concede nenhum). Esta é a função a dar ao seu organismo certificador ou a um avaliador externo.
- Um **limite de acesso por unidade** se soma à função. Um usuário pode ter uma função em toda a organização e ainda assim ter o acesso negado em uma unidade específica, e isso é verificado no envio, na anulação e na aprovação de calibrações.
- Só gerentes e administradores podem anular uma calibração. Os técnicos só podem corrigir os próprios registros; gerentes e administradores podem corrigir qualquer um.

Os registros são armazenados com escopo por espaço de trabalho no nível da linha, imposto na camada de acesso a dados, e o espaço de trabalho é obtido de uma declaração de sessão com assinatura verificada, nunca de um cabeçalho enviado pelo cliente. Observe a descrição honesta: trata-se de escopo por espaço de trabalho **imposto pelo aplicativo**, não da segurança no nível da linha do PostgreSQL, e não de um banco de dados separado por cliente. A imutabilidade do livro-razão, ao contrário, é imposta pelo banco de dados.

## 3. O que você deve verificar no seu próprio ambiente

O que segue é um protocolo sugerido que você executa e registra. Nada aqui foi executado por você. Para cada passo, registre a data, a pessoa que executou, o resultado esperado, o resultado obtido, aprovado ou reprovado, e anexe uma captura de tela. Pela ISO/IEC 17025 7.11.2, esta é a verificação funcional que cabe a você.

#### Qualificação de instalação (IQ), configuração registrada

| Nº | Verificação | Registro |
|---|---|---|
| IQ-1 | Nome do espaço de trabalho, URL do aplicativo e data do primeiro uso em produção | |
| IQ-2 | Usuários nomeados, as funções deles e as permissões por unidade | |

| Nº | Verificação | Registro |
|---|---|---|
| IQ-3 | Configurações do espaço de trabalho registradas: aprovações obrigatórias sim/não, assinatura eletrônica ativada/desativada, módulos ativados, campos personalizados definidos | |
| IQ-4 | Unidades e locais configurados, de acordo com a sua lista de instalações | |
| IQ-5 | Cadastro de instrumentos carregado, com a contagem conciliada com o seu cadastro de origem | |
| IQ-6 | Registro de qualificação de fornecedor aberto para a CaliTech LLC, com este documento anexado | |
| IQ-7 | O seu POP controlado que designa o Axiospec como sistema de registro de calibrações, emitido e aprovado no seu controle de documentos | |

### Qualificação de operação (OQ), testes funcionais

| Nº | Teste | Resultado esperado |
|---|---|---|
| OQ-1 | Registrar uma calibração em um instrumento de teste | O lançamento aparece no histórico desse instrumento com o seu nome, a data de execução e as leituras registradas |
| OQ-2 | Tentar editar esse registro confirmado | O sistema recusa e orienta você a emitir uma correção |
| OQ-3 | Tentar excluir esse registro confirmado | O sistema recusa, informando que o livro-razão é somente de acréscimo |
| OQ-4 | Emitir uma correção sem motivo e depois com motivo | Recusada sem motivo; aceita com motivo; o lançamento original continua visível no histórico |
| OQ-5 | Como gerente, anular uma calibração | O original continua no histórico com a etiqueta de anulado; a situação do instrumento volta para a calibração anterior ou para não calibrado |
| OQ-6 | Como técnico, tentar anular uma calibração | Recusado |
| OQ-7 | Ativar a aprovação para um instrumento. Enviar uma calibração como usuário A e depois tentar aprová-la como usuário A | Recusado, citando a separação entre quem registra e quem aprova |
| OQ-8 | Aprová-la como usuário B | O nome do aprovador e o carimbo de data e hora da aprovação são gravados no lançamento e ficam visíveis no histórico |
| OQ-9 | Entrar como usuário com função de auditor e tentar qualquer alteração | Todas as gravações recusadas |

| Nº | Teste | Resultado esperado |
|---|---|---|
| OQ-10 | Atribuir um usuário somente à Unidade 1 e depois tentar agir sobre um instrumento da Unidade 2 | Recusado |
| OQ-11 | Executar a verificação da cadeia na área de auditoria | Informa que está verificada, com o número de lançamentos verificados. Registre a data, o número e o usuário que fez a verificação |
| OQ-12 | Gerar uma exportação de auditoria sem escopo | É baixado um ZIP com audit_manifest.csv, audit_summary.pdf, o guia de verificação README e os arquivos anexados |
| OQ-13 | Seguir o procedimento do README para verificar off-line o encadeamento da cadeia | O `prev_hash_hex` de cada linha é igual ao `record_hash_hex` da linha anterior |
| OQ-14 | Registrar um resultado fora da tolerância | O instrumento é sinalizado; a avaliação de impacto fora da tolerância pode ser registrada uma vez e depois fica bloqueada |
| OQ-15 | Confirmar que a situação de calibração e a data do próximo vencimento aparecem corretamente para um instrumento conhecido (ISO/IEC 17025 6.4.8) | A situação e a data de vencimento correspondem ao esperado |
| OQ-16 | Mudar a função de um usuário e depois abrir o log de atividade do espaço de trabalho | A mudança aparece com o usuário que agiu, o alvo e o carimbo de data e hora |
| OQ-17 | Editar o intervalo de calibração de um instrumento e depois consultar o log de atividade | **Nenhum lançamento aparece. Esta é a lacuna conhecida da seção 2.2.** Registre-a como lacuna de controle e documente o seu controle compensatório |
| OQ-18 | Imprimir ou exportar um certificado de calibração de um registro aprovado e depois tentar o mesmo com um registro anulado | O certificado é gerado para o registro aprovado; é recusado para o anulado |

### Qualificação de desempenho (PQ), o seu processo com as suas pessoas

| Nº | Atividade |
|---|---|
| PQ-1 | Definir o período (um ciclo completo de calibração é o ideal; um mês é um mínimo comum) |
| PQ-2 | Operar em paralelo com o seu cadastro atual durante esse período. Conciliar ao final a contagem de instrumentos e as datas de vencimento |
| PQ-3 | Confirmar que os avisos de vencimento e de atraso chegam às pessoas certas no cronograma esperado |
| PQ-4 | Confirmar que os seus técnicos conseguem concluir um registro de calibração conforme o seu POP, sem contornos |

| Nº | Atividade |
|---|---|
| PQ-5 | Fazer uma auditoria simulada. Escolher um instrumento ao acaso e apresentar: histórico completo, referência de rastreabilidade, padrão de referência utilizado, anexos de evidência e a prova de que o registro não foi alterado |
| PQ-6 | Tratar de ponta a ponta um evento real fora da tolerância, incluindo a avaliação do impacto nas medições anteriores (ISO 9001 7.1.5.2) |
| PQ-7 | Verificar o caminho de contingência do seu POP para quando o sistema estiver indisponível |
| PQ-8 | Redigir e aprovar o relatório resumo de validação. Assiná-lo |

**Requalificação.** Defina o que dispara um novo teste. Uma regra prática para um SaaS de Categoria 4: executar de novo o subconjunto da OQ que toca qualquer função de que você depende sempre que mudar de forma relevante a sua configuração (configurações de aprovação, funções, unidades, campos personalizados, adaptação a normas), e em um intervalo de revisão periódica que você definir. Veja na seção 5 como funcionam as mudanças do lado do fornecedor.

## 4. Retenção e exportação de registros

**A exportação é autosserviço, completa e não depende de um plano pago nem de um chamado de suporte.** Gerentes, administradores e auditores podem gerá-la. Os técnicos mantêm o histórico por instrumento no aplicativo, mas não a exportação de todo o espaço de trabalho.

A exportação é um único ZIP com:

- `audit_manifest.csv`: uma linha por registro de instrumento e depois uma linha por evento de calibração confirmado. Cerca de 45 colunas, incluindo a identificação do instrumento, a unidade e o local, todos os campos de calibração, os campos metrológicos, os campos de aprovação e de revisor, o impacto fora da tolerância, os campos personalizados do espaço de trabalho como JSON e os valores `record_hash_hex` e `prev_hash_hex`. As colunas de hash ficam fora, de propósito, da proteção contra injeção de fórmulas em CSV, para ficarem exatas byte a byte na comparação do encadeamento.
- `audit_summary.pdf`: um relatório legível com um painel de conformidade, uma seção de verificação de integridade com detecção de adulteração que informa o veredito da cadeia, o número de lançamentos verificados, o algoritmo de hash e os hashes do registro gênese e do mais recente, e depois a trilha de auditoria das calibrações, o cadastro de instrumentos e o detalhamento do que está fora da tolerância. A tabela de exceções lista os 20 eventos mais recentes que se enquadram; o conjunto completo está em `audit_manifest.csv`.
- `assets/<tag>/...`: os próprios arquivos de evidência, no formato original, agrupados por tag de instrumento.
- Um guia de verificação README com o escopo da exportação, as contagens de cobertura, a explicação da cadeia de hashes e o procedimento de verificação off-line do encadeamento.

O arquivo foi pensado para apoiar a sua determinação quanto ao 11.10(b): ele fornece os registros tanto em forma legível por pessoas (PDF) quanto em forma eletrônica (CSV). Se ele atende ao 11.10(b) para os seus registros é uma determinação sua. Ele também é a resposta prática às perguntas sobre continuidade do fornecedor: o pacote é autossuficiente, em formato aberto, e o encadeamento da cadeia pode ser conferido sem nós.

**Escopo e um limite importante.** As exportações podem ser restringidas por unidade, local, instrumentos específicos, período e status, e o escopo sempre se cruza com as permissões de unidade de quem solicita, então só pode ficar mais restrito. **Uma exportação com escopo ou por período verifica de novo o hash próprio de cada registro exportado, mas não afirma a continuidade da cadeia entre registros, porque um conjunto filtrado é um subconjunto proposital da cadeia.** Somente uma exportação sem escopo, com todo o histórico, percorre a cadeia completa. Use uma exportação sem escopo quando precisar da prova de continuidade. O README também informa isso.

**Retenção enquanto a conta está ativa:** os registros são mantidos durante toda a vida do espaço de trabalho. Nenhum registro de calibração confirmado individual pode ser editado ou excluído por ninguém, nem por nós.

**Retenção após o encerramento:** quando uma conta é encerrada, os dados são mantidos por **730 dias (cerca de 24 meses)** para que você possa entrar de novo e exportar. A cobrança é cancelada imediatamente no momento da solicitação, então nada é cobrado durante esse prazo. Depois do prazo, uma exclusão definitiva apaga os dados do espaço de trabalho em todas as tabelas e remove os arquivos de evidência armazenados. Essa exclusão é o **único** caminho autorizado pelo qual lançamentos confirmados do livro-razão são removidos, e é uma operação sobre o espaço de trabalho inteiro, nunca uma exclusão por registro.

**Backups:** o banco de dados de produção tem backups diários automáticos com uma janela de retenção de 14 dias, proteção contra exclusão ativada e um snapshot final em qualquer desativação da instância. Veja na seção 6 o que não afirmamos sobre a recuperação.

**Hospedagem:** a produção roda na Amazon Web Services, em us-east-1 (Estados Unidos). O banco de dados é criptografado em repouso e não tem acesso pela internet pública. O aplicativo e a API são servidos somente por HTTPS com TLS 1.2 no mínimo. O AWS CloudTrail está ativado em toda a conta com validação de integridade dos arquivos de log e uma janela de retenção de 365 dias. Uma visão geral de segurança separada está publicada em axiospec.com/security.

## 5. Gestão de mudanças

**Como as mudanças são feitas e controladas.**

- As implantações em produção são **disparadas somente de forma manual**. Não existe envio automático para produção.
- Uma implantação em produção fica bloqueada a menos que três tarefas passem antes: o conjunto completo de testes do backend, uma tarefa de validação do esquema OpenAPI e uma auditoria de vulnerabilidades de dependências. Se o conjunto de testes falhar, a implantação para.
- O conjunto de testes do backend tem **2.465 funções de teste em 197 arquivos de teste**. Há mais 233 arquivos de teste no front-end web. São testes de regressão automatizados que rodam a cada mudança.

- Cada build de produção é publicado com uma tag de imagem imutável por commit, de modo que há um alvo de reversão definido para cada versão.
- Homologação e produção são ambientes separados, com infraestrutura separada. As mudanças chegam primeiro à homologação.

**É preciso ser claro sobre o que isso é e o que não é.** Um conjunto de testes automatizados desse tamanho é um controle de desenvolvimento de software real e citável, e é uma boa matéria-prima para um argumento de qualificação de operação. Ele **não** é um pacote de validação. Não foi escrito contra uma especificação funcional formal, não há matriz de rastreabilidade de requisitos para testes e não há registro de versão assinado. Um revisor de validação de sistemas computadorizados não vai aceitá-lo como tal, e nós não vamos apresentá-lo como tal.

**Como você fica sabendo quando algo muda.**

O Axiospec é software como serviço multilocatário. Todos os clientes usam uma única versão de produção. **Você não pode fixar uma versão, adiar uma atualização nem usar uma versão anterior.** Essa é uma restrição real para um ambiente validado, e você deve registrá-la na sua avaliação de riscos.

Hoje **não existe changelog publicado, página de notas de versão nem compromisso escrito de notificação de mudanças.** Se o seu procedimento exige aviso prévio de mudanças em um sistema validado, peça esse compromisso por escrito antes de comprar, em support@axiospec.com. Preferimos dizer que ele não existe a deixar que você descubra isso durante uma auditoria.

**O que sugerimos que você faça a respeito,** diante do que foi dito: defina no seu POP um intervalo de reverificação periódica (por exemplo, executar de novo o subconjunto da OQ a cada trimestre e depois de qualquer mudança que você perceber em uma função de que depende), e execute de novo a verificação da cadeia e registre o resultado nesse mesmo intervalo. A verificação da cadeia leva um clique e gera um resultado datado e atribuível.

## 6. Limites do que este software faz

Ditos com clareza, porque um fornecedor pequeno que declara os próprios limites é mais fácil de qualificar do que um que se esquiva.

**Certificações e avaliações que não temos.** Nenhum SOC 2, nem Tipo I nem Tipo II. Nenhuma ISO/IEC 27001. Nenhum teste de invasão feito por terceiros. Nenhum acordo de associado comercial da HIPAA, e não aceitamos informações de saúde protegidas. Nenhum FedRAMP, StateRAMP, CMMC, NIST 800-171, ITAR, EAR ou DFARS 252.204-7012. Se você lida com informações não classificadas controladas ou dados sujeitos a controle de exportação, hoje o Axiospec não é adequado. Nenhum aditivo de tratamento de dados publicado, nenhuma cláusula contratual padrão e nenhuma residência de dados na UE; todos os dados estão nos Estados Unidos.

**Nenhum pacote de validação do fornecedor.** Não existe pacote de IQ/OQ/PQ, protocolo de validação, matriz de rastreabilidade nem relatório resumo de validação elaborado por nós. A seção 3 é uma lista de verificação para você executar, e não uma evidência de que algo foi executado.

**Nenhuma declaração de conformidade.** O Axiospec não certifica, assegura nem garante a sua conformidade com nenhuma norma. Ele apoia e documenta os registros de calibração e os mantém prontos

para auditoria. A conformidade é determinada pela sua área da qualidade, pelo seu organismo certificador, pelo seu organismo de acreditação ou pelo seu inspetor.

**Não afirmamos conformidade com o 21 CFR Part 11.** Os elementos de integridade dos registros são realmente sólidos: imutabilidade imposta pelo banco de dados, uma cadeia de hashes SHA-256, lançamentos atribuídos e com carimbo de data e hora, correções somente de acréscimo que não ocultam informações anteriores e revisão por duas pessoas. Os controles de assinatura ainda não estão lá. Veja a seção 2.4: a assinatura eletrônica é opcional por espaço de trabalho, e não obrigatória, não há vínculo de assinatura armazenado no registro, não há um campo com o significado da assinatura e não há identificação multifator. Publicamos um mapeamento de funcionalidades com as lacunas marcadas; não publicamos uma declaração de conformidade.

**Nenhuma autenticação multifator.** Não há TOTP integrado, aplicativo autenticador, WebAuthn, SMS nem códigos de backup. Hoje, o único caminho para um segundo fator é entrar pelo Google, onde o seu próprio provedor de identidade o impõe. O SSO corporativo por espaço de trabalho via OIDC e SAML está construído e testado no backend, mas não está ativado em produção e deve ser tratado como disponível sob solicitação, e não como uma funcionalidade disponível. Se a sua política de TI exige MFA obrigatória para todos os sistemas do SGQ, hoje isso é um impedimento total. Pergunte-nos a situação atual antes de comprar.

**As alterações no cadastro mestre dos ativos não são registradas.** Seção 2.2 e teste OQ-17. Os eventos de calibração são totalmente cobertos pelo livro-razão. As alterações no cadastro descritivo do instrumento, incluindo o intervalo de calibração, não são atribuídas no log de atividade.

**Exportações filtradas não provam a continuidade da cadeia.** Seção 4. Use uma exportação sem escopo para isso.

**Nenhum compromisso de disponibilidade.** Não há SLA de disponibilidade, página de status nem histórico de disponibilidade publicado. O banco de dados de produção é uma única instância em uma única zona de disponibilidade, então uma falha da zona de disponibilidade exige uma restauração, e não um failover. Não publicamos um objetivo de tempo de recuperação nem de ponto de recuperação, e nenhum teste de restauração foi documentado. Os backups estão configurados e são mantidos por 14 dias; essa é uma afirmação verdadeira sobre os backups, e não uma afirmação comprovada sobre a recuperação. O seu POP deve incluir uma contingência para quando o sistema estiver indisponível, o que os avaliadores da ISO/IEC 17025 perguntam de qualquer forma.

**Nenhum plano documentado de resposta a incidentes nem prazo contratual de notificação de violações.** Há alarmes de infraestrutura configurados no CloudWatch e enviados para um endereço de e-mail de plantão. Isso é monitoramento, e não um programa de resposta a incidentes.

**Nenhuma chave de criptografia gerenciada pelo cliente.** A criptografia usa chaves gerenciadas pela AWS.

**Os registros só podem ser excluídos de uma forma.** Nenhum registro confirmado individual pode ser editado ou excluído por ninguém. O único caminho de exclusão é uma exclusão definitiva de todo o espaço de trabalho, a pedido do cliente, após o período de retenção de 730 dias.

**Não realizamos calibrações.** O Axiospec é um sistema de guarda de registros, não um laboratório de calibração acreditado, e não realizou nenhuma das medições dos seus registros.

**Como usar este documento.** Anexe-o ao seu registro de qualificação de fornecedor da CaliTech LLC (ISO 9001, cláusula 8.4; ISO/IEC 17025, cláusula 6.6). Faça referência a ele no seu plano de validação como a descrição funcional e de controles do fornecedor. Execute a seção 3 no seu próprio espaço de trabalho e guarde o resultado assinado como a sua evidência de qualificação. Registre os limites da seção 6 na sua avaliação de riscos, junto com os seus controles compensatórios.

Se alguma afirmação deste documento não corresponder ao que você observa no produto, avise-nos em support@axiospec.com e corrigiremos o documento.

O Axiospec é publicado pela CaliTech LLC, Knoxville, Tennessee (Estados Unidos). O Axiospec apoia e documenta o seu programa de calibração e o mantém pronto para auditoria. Ele não certifica, assegura nem garante a conformidade com nenhuma norma; essa determinação cabe a você e ao seu auditor. Dúvidas: support@axiospec.com