Resumo da validação do software

Axiospec, gestão de calibrações Preparado para o gestor da qualidade, o responsável pela validação ou o revisor de TI que avalia o Axiospec como sistema de registo oficial das calibrações.

Versão do documento 1.0. Última revisão a 19-08-2026. Publicado pela CaliTech LLC, Knoxville, Tennessee (Estados Unidos). Questões: support@axiospec.com, com resposta no prazo de um dia útil.

Leia isto primeiro

Este documento é **um contributo para o seu registo de validação. Não é um registo 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 a sua organização faz sobre a própria utilização prevista, a configuração, os procedimentos e as pessoas. O seu organismo de certificação, o seu avaliador ou o seu inspetor decide se foi cumprida.

O que este documento lhe dá: uma declaração de utilização prevista, uma descrição dos controlos de integridade de dados que existem no produto e da forma como são impostos, uma lista de verificação que pode executar e assinar no seu próprio espaço de trabalho, a nossa prática de gestão de alterações e uma lista clara do que o software não faz.

Segundo a categorização do GAMP 5, um registo SaaS multi-inquilino configurado deste tipo é normalmente tratado como Categoria 4 (produto configurado). Isso significa que o seu esforço de validação é baseado no 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 utilização prevista

O Axiospec é um sistema de guarda de registos para equipamento de medição e ensaio. A utilização prevista é:

- Manter um registo de instrumentos, incluindo a identificação, o fabricante, o modelo, o número de série, a localização, a instalação e os campos personalizados definidos no espaço de trabalho.
- Registar 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 do serviço e a referência de rastreabilidade.
- Registar os campos metrológicos utilizados nos fluxos de trabalho da ISO/IEC 17025: incerteza de medição, fator de expansão, nível de confiança, regra de decisão, declaração de conformidade e o número do certificado do próprio padrão de referência.
- Identificar o estado de calibração de cada instrumento e a data do próximo vencimento, e destacar os instrumentos vencidos e os que vencem em breve.

- Conservar esses registos de forma apenas de acréscimo e com deteção de adulteração, com autoria e marcas temporais.
- Encaminhar os registos de calibração para uma aprovação opcional por duas pessoas antes de produzirem efeitos.
- Produzir uma exportação completa, legível por pessoas e por máquinas, do registo e do respetivo histórico para auditoria.

O Axiospec **não** é um laboratório de calibração acreditado e não realiza medições. Todos os documentos que o sistema produz trazem esta declaração, palavra por palavra:

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

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

Que cláusulas determinam o que se espera de um sistema como este

O texto das cláusulas das normas ISO está protegido por direitos de autor, pelo que o que se segue são referências a cláusulas com paráfrase, e não citações. Confirme com o seu próprio exemplar licenciado.

- **ISO 9001:2015, cláusula 7.1.5.2** (rastreabilidade das medições): equipamento calibrado ou verificado a intervalos especificados face a padrões rastreáveis, identificável quanto ao estado de calibração, protegido contra ajustes que invalidem o resultado, e uma avaliação dos resultados anteriores quando se verifica que um equipamento não está apto.
- **ISO 9001:2015, cláusula 7.5.3** (controlo da informação documentada): disponibilidade, proteção contra a perda de integridade, controlo do acesso, armazenamento e preservação, controlo de alterações e de versões, retenção e eliminação.
- **ISO 9001:2015, cláusula 8.4** e **ISO/IEC 17025:2017, cláusula 6.6** (produtos e serviços de fornecedores externos): tem de avaliar e registar a qualificação do Axiospec como fornecedor. Este documento destina-se a servir de evidência nesse registo.
- **ISO/IEC 17025:2017, cláusula 6.4** (equipamento), em especial 6.4.6 (calibração quando a exatidão ou a incerteza afetam a validade), 6.4.8 (etiquetagem ou codificação do estado para que o utilizador identifique facilmente o estado de calibração ou o período de validade) e 6.4.13 (o conteúdo obrigatório dos registos do equipamento).
- **ISO/IEC 17025:2017, cláusula 7.11** (controlo dos 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 de acordo com a especificação, mantido de forma a assegurar a integridade dos dados, com as falhas e as ações corretivas registadas).
- **ISO 13485:2016, cláusula 4.1.6**: procedimentos para validar o software informático usado no SGQ, antes da primeira utilização e após alterações, com uma abordagem proporcional ao risco e com registos mantidos.

- **21 CFR Part 11**, quando os registos de calibração são os seus registos regulamentados oficiais: 11.10(a) validação, 11.10(b) cópias exatas e completas em forma legível por pessoas e em forma eletrónica, 11.10(c) proteção e recuperação rápida, 11.10(d) acesso limitado a pessoas autorizadas, 11.10(e) pistas de auditoria seguras, geradas por computador e com marca temporal, em que "as alterações aos registos não devem ocultar informação registada anteriormente", 11.10(g) verificações de autoridade, 11.50 manifestações da assinatura, 11.70 ligação entre assinatura e registo.

Note que a ISO 9001 não tem uma cláusula explícita de validação de software. Para uma empresa que aplica apenas a 9001, a obrigação é o controlo da informação documentada, e não um protocolo de validação. Dimensione o seu esforço em conformidade.

2. Controlos de integridade de dados que existem

2.1 Livro de registos de calibração apenas de acréscimo e com deteção de adulteração

Cada evento de calibração é escrito num livro de registos. Assim que uma entrada é confirmada (ou seja, assim que sai do estado de rascunho, DRAFT), deixa de poder ser editada ou eliminada.

Como funciona a deteção de adulteração. Cada entrada confirmada guarda um `record_hash`: um resumo SHA-256 calculado sobre uma serialização JSON canónica, com as chaves ordenadas, dos campos dessa entrada, que inclui o `record_hash` da entrada anterior como `prev_hash`. As entradas são encadeadas por espaço de trabalho pela 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 registo muda o respetivo hash e quebra a cadeia a partir desse ponto, e a quebra pode ser detetada.

Os campos incluídos no hash são: o ativo, o tipo de evento, a marca temporal da realização, o utilizador que a realizou, o resultado da calibração, o valor nominal, a tolerância, as leituras antes do ajuste e após o ajuste, a temperatura, a humidade, o padrão de referência, as medições, as notas, a referência do anexo, o número do certificado, o prestador do serviço, a referência de rastreabilidade, o motivo da correção e os campos metrológicos enumerados na secção 1.

Os ficheiros de evidência entram no hash pelo conteúdo, não apenas pela referência. O SHA-256 do certificado ou da fotografia carregados é calculado no servidor e incorporado no hash do registo. Trocar o ficheiro por trás de uma ligação inalterada quebra a cadeia.

A imutabilidade é imposta pela base de dados, não pelo código da aplicação. Um trigger do PostgreSQL na tabela do livro de registos bloqueia, ao nível da base de dados: a eliminação de uma entrada confirmada, o regresso de uma entrada confirmada ao estado de rascunho e a alteração de qualquer coluna de identificação ou incluída no hash de uma entrada confirmada. Isto significa que uma sessão SQL direta na base de dados de produção não consegue reescrever em silêncio um registo de calibração. É um controlo mais forte do que uma verificação na camada da aplicação, e é precisamente o ponto que vale a pena demonstrar a um avaliador.

As alterações são representadas por acréscimo, nunca por escrita por cima. Esta é a resposta direta ao requisito da Part 11 de que as alterações aos registos não ocultem a informação registada anteriormente.

- Uma **correção** é uma nova entrada acrescentada que faz referência à entrada que substitui e tem um motivo de correção em texto livre. O motivo é obrigatório (a API rejeita uma correção sem motivo) e faz

parte do hash. A entrada substituída continua no histórico, legível na íntegra.

- Uma **anulação** é um evento marcador acrescentado ao livro de registos. O original anulado continua no histórico com a etiqueta de anulado, e o instrumento regressa à calibração anterior ou a não calibrado. Uma anulação nunca pode contar como calibração.

Verificação com um clique. Qualquer utilizador autenticado do espaço de trabalho pode executar uma verificação completa da cadeia, que percorre cada entrada confirmada, recalcula cada hash, verifica a continuidade e apresenta um resultado limpo com o número de entradas verificadas ou a primeira entrada divergente com a etiqueta do instrumento. O resultado e o utilizador que fez a verificação ficam registados.

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 offline o **encadeamento** da cadeia sem o Axiospec: o `prev_hash_hex` de cada linha tem de ser igual ao `record_hash_hex` da linha anterior, pelo que qualquer registo removido, inserido ou reordenado aparece como uma ligação quebrada. Convém ser preciso quanto ao limite. O manifesto não inclui todos os campos que alimentam a função de hash, pelo que não é possível recalcular o hash de um registo apenas a partir do CSV. O novo cálculo do hash de um registo individual é feito no servidor, na aplicação e no momento da exportação. O encadeamento é o que pode provar sozinho, sem nós, para sempre.

2.2 Pista de auditoria

Registos de calibração. Cada entrada guarda o identificador do utilizador que a realizou mais um instantâneo fixo do nome dele, a marca temporal da realização e a marca temporal de criação no servidor. Quando a entrada passa por revisão, guarda também o identificador e o instantâneo do nome do revisor, a marca temporal da revisão, as notas de revisão e o motivo da rejeição, se existir. Os valores anteriores são preservados por construção: nada é escrito por cima, pelo que o "valor anterior" é a entrada substituída, que continua legível.

Administração do espaço de trabalho. Um registo de atividade separado guarda as ações de equipa e de configuração com o utilizador que agiu, o alvo, um registo JSON do que mudou, o IP de origem e uma marca temporal. As ações abrangidas incluem os convites e revogações de utilizadores, as alterações de função, o arquivamento de utilizadores, as alterações de email, a emissão e revogação de chaves de API, as alterações à configuração de SSO e os inícios de sessão por SSO, as alterações às subscrições de webhooks e o início do período de avaliação da faturação. Pode ser lido na aplicação pelos administradores do espaço de trabalho, estritamente limitado ao espaço de trabalho da sessão autenticada e não a um parâmetro do pedido.

Lacuna conhecida, declarada. As alterações ao registo mestre de um instrumento (por exemplo, o intervalo de calibração) ainda não são captadas no registo de auditoria do sistema. Os eventos de calibração propriamente ditos são imutáveis e totalmente atribuídos. O mesmo se aplica à etiqueta, ao número de série e à localização de um instrumento. Se o seu procedimento precisa de saber "quem alterou o intervalo deste instrumento e quando", tem de o cobrir com um controlo próprio até esta lacuna ser fechada. Consulte a secção 6.

2.3 Aprovações (quem regista e quem verifica)

A revisão por duas pessoas está disponível por instrumento ou para todo o espaço de trabalho. É **opcional e está desativada por predefinição.**

Quando a revisão é obrigatória, o sistema não permite que quem submete aprove o próprio registo. A verificação é incondicional logo no início tanto da via de aprovação como da de rejeição, e também falha de forma fechada se a identidade do aprovador não puder ser resolvida. Aprovar exige a função de gestor ou de administrador, verificada tanto ao nível de toda a organização como na instalação específica a que o instrumento pertence, pelo que um gestor de toda a organização que foi despromovido nessa instalação vê o acesso recusado aí. A rota genérica de atualização de registos recusa-se a definir um estado de aprovado ou rejeitado, pelo que 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, a submissão é aprovada automaticamente e quem submete fica registado como aprovador. Uma pessoa regista e o registo produz efeitos de imediato. Indique isso com clareza na sua própria avaliação de riscos e ative a revisão nos instrumentos em que a sua avaliação de riscos o exija.

2.4 Assinaturas eletrónicas

O que é real e está disponível. A assinatura eletrónica é uma definição por espaço de trabalho. É opcional, não obrigatória. Quando um espaço de trabalho a ativa, a aprovação exige que a palavra-passe da própria conta do aprovador seja novamente verificada no momento da assinatura, no servidor e face ao hash da palavra-passe guardado, antes de a aprovação avançar. Uma palavra-passe errada é sempre recusada com um 403, independentemente de qualquer indicador de configuração. A aplicação móvel exige a palavra-passe quando uma calibração é registada. As palavras-passe são guardadas como PBKDF2-HMAC-SHA256 com 260 000 iterações e um sal aleatório de 16 bytes por palavra-passe, e a verificação é feita em tempo constante. Existe um endpoint de reautenticação autónomo com a mesma finalidade. O utilizador que aprova e a marca temporal da aprovação são registados no registo imutável do livro, fixados pelo trigger da base de dados descrito na secção 2.1.

Dois limites que deve conhecer antes de confiar nisto.

1. **É opcional por espaço de trabalho e hoje não é imposto de forma rígida.** Se o cliente não enviar nenhuma palavra-passe de assinatura, a aprovação é atualmente concluída e regista um aviso, em vez de ser recusada. Só uma palavra-passe errada é recusada. O interruptor de imposição rígida existe no código, mas não está ativado no ambiente de produção.
2. **Não existe uma ligação criptográfica de assinatura guardada.** Não espere um artefacto de assinatura separado e recuperável no registo de calibração, nem um indicador de assinado na API. A evidência duradoura é o próprio registo de aprovação: a identidade do aprovador, o instantâneo do nome do aprovador, a marca temporal da aprovação e as notas de revisão, tudo fixado pelo trigger de imutabilidade.

Por conseguinte, o Axiospec **não** cumpre hoje o 21 CFR 11.50 e 11.70, e a expectativa de dois componentes de identificação distintos para sessões não contínuas não pode ser cumprida, porque o produto não tem autenticação multifator. Se as assinaturas eletrónicas da Part 11 forem um requisito obrigatório para a sua organização, trate isto como uma lacuna e fale connosco antes de comprar.

2.5 Controlo de acessos baseado em funções

Cinco funções: superadministrador, administrador, gestor, técnico e auditor. A imposição é feita **no servidor**, em todas as rotas, através de dependências do FastAPI. A função do utilizador é novamente resolvida a partir da base de dados no momento do pedido, em vez de se confiar no token de sessão, pelo que um token antigo não pode transportar privilégios elevados. Também existem restrições no cliente, mas 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 alterar funções é limitada. Um gestor só pode gerir técnicos. As permissões para convidar estão restringidas por função.
- **A função de auditor é imposta como apenas de leitura em todo o sistema.** Todos os métodos HTTP de escrita estão bloqueados para os auditores, com exatamente duas exceções permitidas: pedir uma exportação da pista de auditoria e revogar o seu próprio token do feed de calendário (o que retira um acesso e nunca concede nenhum). Esta é a função a atribuir ao seu organismo de certificação ou a um avaliador externo.
- Um **limite de acesso por instalação** sobrepõe-se à função. Um utilizador pode ter uma função em toda a organização e mesmo assim ver o acesso recusado numa instalação específica, e isto é verificado na submissão, na anulação e na aprovação de calibrações.
- Só os gestores e os administradores podem anular uma calibração. Os técnicos só podem corrigir os seus próprios registos; os gestores e os administradores podem corrigir qualquer um.

Os registos são guardados com uma delimitação por espaço de trabalho ao nível da linha, imposta na camada de acesso aos dados, e o espaço de trabalho é obtido de uma declaração de sessão com assinatura verificada, nunca de um cabeçalho enviado pelo cliente. Note a descrição honesta: trata-se de uma delimitação por espaço de trabalho **imposta pela aplicação**, não da segurança ao nível da linha do PostgreSQL, e não de uma base de dados separada por cliente. A imutabilidade do livro de registos, pelo contrário, é imposta pela base de dados.

3. O que deve verificar no seu próprio ambiente

O que se segue é um protocolo sugerido que a sua organização executa e regista. Nada disto foi executado por si. Para cada passo, registe a data, a pessoa que o executou, o resultado esperado, o resultado obtido, conforme ou não conforme, e anexe uma captura de ecrã. Segundo a ISO/IEC 17025 7.11.2, esta é a verificação funcional que lhe cabe.

Qualificação da instalação (IQ), configuração registada

N.º	Verificação	Registo
IQ-1	Nome do espaço de trabalho, URL da aplicação e data da primeira utilização em produção	
IQ-2	Utilizadores identificados, as respetivas funções e as permissões por instalação	

N.º	Verificação	Registo
IQ-3	Definições do espaço de trabalho registadas: aprovações obrigatórias sim/não, assinatura eletrónica ativada/desativada, módulos ativados, campos personalizados definidos	
IQ-4	Instalações e localizações configuradas, de acordo com a sua lista de instalações físicas	
IQ-5	Registo de instrumentos carregado, com a contagem conciliada com o seu registo de origem	
IQ-6	Registo de qualificação de fornecedor aberto para a CaliTech LLC, com este documento anexado	
IQ-7	O seu procedimento controlado que designa o Axiospec como sistema de registo das calibrações, emitido e aprovado no âmbito do seu controlo documental	

Qualificação operacional (OQ), testes funcionais

N.º	Teste	Resultado esperado
OQ-1	Registar uma calibração num instrumento de teste	A entrada aparece no histórico desse instrumento com o seu nome, a data de realização e as leituras registadas
OQ-2	Tentar editar esse registo confirmado	O sistema recusa e indica que deve emitir uma correção
OQ-3	Tentar eliminar esse registo confirmado	O sistema recusa, indicando que o livro de registos é apenas de acréscimo
OQ-4	Emitir uma correção sem motivo e depois com motivo	Recusada sem motivo; aceite com motivo; a entrada original continua visível no histórico
OQ-5	Como gestor, anular uma calibração	O original continua no histórico com a etiqueta de anulado; o estado do instrumento regressa à calibração anterior ou a não calibrado
OQ-6	Como técnico, tentar anular uma calibração	Recusado
OQ-7	Ativar a aprovação para um instrumento. Submeter uma calibração como utilizador A e depois tentar aprová-la como utilizador A	Recusado, com referência à separação entre quem regista e quem verifica
OQ-8	Aprová-la como utilizador B	O nome do aprovador e a marca temporal da aprovação ficam registados na entrada e visíveis no histórico
OQ-9	Iniciar sessão como utilizador com função de auditor e tentar qualquer alteração	Todas as escritas recusadas

N.º	Teste	Resultado esperado
OQ-10	Atribuir um utilizador apenas à Instalação 1 e depois tentar atuar sobre um instrumento da Instalação 2	Recusado
OQ-11	Executar a verificação da cadeia a partir da área de auditoria	Indica que está verificada, com o número de entradas verificadas. Registe a data, o número e o utilizador que fez a verificação
OQ-12	Gerar uma exportação de auditoria sem âmbito	É descarregado um ZIP com audit_manifest.csv, audit_summary.pdf, o guia de verificação README e os ficheiros anexados
OQ-13	Seguir o procedimento do README para verificar offline o encadeamento da cadeia	O `prev_hash_hex` de cada linha é igual ao `record_hash_hex` da linha anterior
OQ-14	Registar um resultado fora da tolerância	O instrumento é assinalado; a avaliação de impacto fora da tolerância pode ser registada uma vez e fica depois bloqueada
OQ-15	Confirmar que o estado de calibração e a data do próximo vencimento são apresentados corretamente para um instrumento conhecido (ISO/IEC 17025 6.4.8)	O estado e a data de vencimento correspondem ao esperado
OQ-16	Alterar a função de um utilizador e depois abrir o registo de atividade do espaço de trabalho	A alteração aparece com o utilizador que agiu, o alvo e a marca temporal
OQ-17	Editar o intervalo de calibração de um instrumento e depois consultar o registo de atividade	**Não aparece nenhuma entrada. É a lacuna conhecida da secção 2.2.** Registe-a como lacuna de controlo e documente o seu controlo compensatório
OQ-18	Imprimir ou exportar um certificado de calibração de um registo aprovado e depois tentar o mesmo com um registo anulado	O certificado é produzido para o registo aprovado; é recusado para o anulado

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

N.º	Atividade
PQ-1	Definir o período (é preferível um ciclo de calibração completo; um mês é um mínimo habitual)
PQ-2	Trabalhar em paralelo com o seu registo atual durante esse período. Conciliar no 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 calendário previsto
PQ-4	Confirmar que os seus técnicos conseguem concluir um registo de calibração de acordo com o seu procedimento, sem soluções alternativas

N.º	Atividade
PQ-5	Fazer uma auditoria simulada. Escolher um instrumento ao acaso e apresentar: o histórico completo, a referência de rastreabilidade, o padrão de referência utilizado, os anexos de evidência e a prova de que o registo 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 a via de contingência do seu procedimento para quando o sistema estiver indisponível
PQ-8	Redigir e aprovar o relatório de síntese da validação. Assiná-lo

Requalificação. Defina o que desencadeia um novo teste. Uma regra prática para um SaaS de Categoria 4: voltar a executar o subconjunto da OQ que toca em qualquer função de que dependa sempre que alterar de forma significativa a sua configuração (definições de aprovação, funções, instalações, campos personalizados, adaptação a normas), e com um intervalo de revisão periódica que defina. Consulte na secção 5 como funcionam as alterações do lado do fornecedor.

4. Conservação e exportação de registos

A exportação é feita pelo próprio cliente, é completa e não depende de um plano pago nem de um pedido ao suporte. Os gestores, administradores e auditores podem gerá-la. Os técnicos mantêm o histórico por instrumento na aplicação, mas não a exportação de todo o espaço de trabalho.

A exportação é um único ZIP com:

- `audit_manifest.csv`: uma linha por registo de instrumento e depois uma linha por cada evento de calibração confirmado. Cerca de 45 colunas, incluindo a identificação do instrumento, a instalação e a localização, 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 excluídas, de propósito, da proteção contra injeção de fórmulas em CSV, para serem exatas byte a byte na comparação do encadeamento.
- `audit_summary.pdf`: um relatório legível com um painel de conformidade, uma secção de verificação de integridade com deteção de adulteração que indica o veredicto da cadeia, o número de entradas verificadas, o algoritmo de hash e os hashes do registo génese e do mais recente, e depois o histórico de auditoria das calibrações, o inventário de instrumentos e o detalhe do que está fora da tolerância. A tabela de exceções lista os 20 eventos mais recentes que cumprem o critério; o conjunto completo está em `audit_manifest.csv`.
- `assets/<tag>/...`: os próprios ficheiros de evidência, no formato original, agrupados por etiqueta de instrumento.
- Um guia de verificação README com o âmbito da exportação, as contagens de cobertura, a explicação da cadeia de hashes e o procedimento de verificação offline do encadeamento.

O arquivo destina-se a apoiar a sua determinação quanto ao 11.10(b): fornece os registos tanto em forma legível por pessoas (PDF) como em forma eletrónica (CSV). Se cumpre o 11.10(b) para os seus registos é uma determinação sua. É também a resposta prática às perguntas sobre a continuidade do fornecedor: o pacote é autónomo, está em formato aberto e o encadeamento da cadeia pode ser verificado sem nós.

Âmbito e um limite importante. As exportações podem ser restringidas por instalação, localização, instrumentos específicos, intervalo de datas e estado, e o âmbito cruza-se sempre com as permissões de instalação de quem faz o pedido, pelo que só pode estreitar-se. **Uma exportação com âmbito ou limitada por datas volta a verificar o hash próprio de cada registo exportado, mas não afirma a continuidade da cadeia entre registos, porque um conjunto filtrado é um subconjunto deliberado da cadeia.** Só uma exportação sem âmbito, com todo o histórico, percorre a cadeia completa. Use uma exportação sem âmbito quando precisar da prova de continuidade. O README também o indica.

Conservação enquanto a conta está ativa: os registos são conservados durante toda a vida do espaço de trabalho. Nenhum registo de calibração confirmado individual pode ser editado ou eliminado por ninguém, incluindo nós.

Conservação após o encerramento: quando uma conta é encerrada, os dados são conservados durante **730 dias (cerca de 24 meses)** para que possa voltar a iniciar sessão e exportar. A faturação é cancelada de imediato quando é pedido o encerramento, pelo que nada é faturado durante esse período. Findo o período, uma purga definitiva elimina os dados do espaço de trabalho em todas as tabelas e remove os ficheiros de evidência guardados. Essa purga é a **única** via autorizada pela qual as linhas confirmadas do livro de registos são alguma vez removidas, e é uma operação sobre todo o espaço de trabalho, nunca uma eliminação por registo.

Cópias de segurança: a base de dados de produção tem cópias de segurança diárias automáticas com um período de conservação de 14 dias, proteção contra eliminação ativada e um instantâneo final em qualquer desmantelamento da instância. Consulte na secção 6 o que não afirmamos sobre a recuperação.

Alojamento: a produção corre na Amazon Web Services, em us-east-1 (Estados Unidos). A base de dados está cifrada em repouso e não tem acesso a partir da internet pública. A aplicação e a API são servidas apenas por HTTPS com TLS 1.2 no mínimo. O AWS CloudTrail está ativado em toda a conta com validação da integridade dos ficheiros de registo e um período de conservação de 365 dias. Está publicada uma descrição geral da segurança à parte em axiospec.com/security.

5. Gestão de alterações

Como as alterações são feitas e controladas.

- As implementações em produção são **lançadas apenas manualmente**. Não existe nenhum envio automático para produção.
- Uma implementação em produção fica bloqueada a menos que três tarefas passem primeiro: o conjunto completo de testes do backend, uma tarefa de validação do esquema OpenAPI e uma auditoria de vulnerabilidades das dependências. Se o conjunto de testes falhar, a implementação para.
- O conjunto de testes do backend tem **2465 funções de teste em 197 ficheiros de teste**. Há mais 233 ficheiros de teste no frontend web. São testes de regressão automatizados que correm a cada alteração.

- Cada compilação de produção é publicada com uma etiqueta de imagem imutável por commit, pelo que existe um alvo de reversão definido para cada versão.
- O ambiente de pré-produção e o de produção são separados, com infraestrutura separada. As alterações chegam primeiro à pré-produção.

É preciso ser claro quanto ao que isto é e não é. Um conjunto de testes automatizados desta dimensão é um controlo de desenvolvimento de software real e citável, e é uma boa matéria-prima para uma argumentação de qualificação operacional. **Não** é um pacote de validação. Não está escrito a partir de uma especificação funcional formal, não existe uma matriz de rastreabilidade de requisitos para testes e não existe um registo de versão assinado. Um revisor de validação de sistemas informatizados não o aceitará como tal, e nós não o apresentaremos como tal.

Como fica a saber quando algo muda.

O Axiospec é software como serviço multi-inquilino. Todos os clientes usam uma única versão de produção. **Não é possível fixar uma versão, adiar uma atualização nem usar uma versão anterior.** É uma restrição real para um ambiente validado e deve registá-la na sua avaliação de riscos.

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

O que sugerimos que faça a este respeito, tendo em conta o que ficou dito: defina no seu procedimento um intervalo de reverificação periódica (por exemplo, voltar a executar o subconjunto da OQ trimestralmente e depois de qualquer alteração que note numa função de que dependa), e volte a executar a verificação da cadeia e a registar o resultado com esse mesmo intervalo. A verificação da cadeia faz-se com um clique e produz um resultado datado e atribuível.

6. Limites do que este software faz

Ditos com clareza, porque um fornecedor pequeno que declara os seus 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 intrusão realizado por terceiros. Nenhum acordo de parceiro comercial da HIPAA, e não aceitamos informação de saúde protegida. Nenhum FedRAMP, StateRAMP, CMMC, NIST 800-171, ITAR, EAR ou DFARS 252.204-7012. Se trata informação não classificada controlada ou dados sujeitos a controlo de exportações, o Axiospec não é hoje adequado. Nenhum aditamento de tratamento de dados publicado, nenhumas cláusulas contratuais-tipo e nenhuma residência de dados na UE; todos os dados estão nos Estados Unidos.

Nenhum pacote de validação do fornecedor. Não existe nenhum pacote IQ/OQ/PQ, nenhum protocolo de validação, nenhuma matriz de rastreabilidade e nenhum relatório de síntese da validação elaborado por nós. A secção 3 é uma lista de verificação para 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 qualquer norma. Apoia e documenta os registos de calibração e mantém-nos prontos

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

Não afirmamos a conformidade com o 21 CFR Part 11. Os elementos que sustentam a integridade dos registos são realmente sólidos: imutabilidade imposta pela base de dados, uma cadeia de hashes SHA-256, entradas atribuídas e com marca temporal, correções apenas de acréscimo que não ocultam a informação anterior e revisão por duas pessoas. Os controlos de assinatura ainda não existem. Consulte a secção 2.4: a assinatura eletrónica é opcional por espaço de trabalho, e não obrigatória, não existe uma ligação de assinatura guardada no registo, não existe um campo com o significado da assinatura e não existe identificação multifator. Publicamos um mapeamento de funcionalidades com as lacunas assinaladas; não publicamos uma declaração de conformidade.

Nenhuma autenticação multifator. Não existe TOTP integrado, aplicação de autenticação, WebAuthn, SMS nem códigos de reserva. Hoje, a única via para um segundo fator é iniciar sessão através da Google, onde o seu próprio fornecedor de identidade o impõe. O SSO empresarial por espaço de trabalho através de OIDC e SAML está construído e testado no backend, mas não está ativado em produção e deve ser tratado como disponível mediante pedido, e não como uma funcionalidade disponível. Se a sua política de TI exige MFA obrigatória para todos os sistemas do SGQ, isto é hoje um impedimento absoluto. Pergunte-nos qual é a situação atual antes de comprar.

As alterações ao registo mestre dos ativos não são registadas. Secção 2.2 e teste OQ-17. Os eventos de calibração estão totalmente cobertos pelo livro de registos. As alterações ao registo descritivo do instrumento, incluindo o intervalo de calibração, não são atribuídas no registo de atividade.

As exportações filtradas não provam a continuidade da cadeia. Secção 4. Use uma exportação sem âmbito para isso.

Nenhum compromisso de disponibilidade. Não existe SLA de disponibilidade, página de estado nem histórico de disponibilidade publicado. A base de dados de produção é uma única instância numa única zona de disponibilidade, pelo que uma falha da zona de disponibilidade exige uma reposição e não uma comutação. Não publicamos um objetivo de tempo de recuperação nem de ponto de recuperação, e não foi documentado nenhum exercício de reposição. As cópias de segurança estão configuradas e são conservadas durante 14 dias; é uma afirmação verdadeira sobre as cópias de segurança, e não uma afirmação comprovada sobre a recuperação. O seu procedimento deve incluir uma contingência para quando o sistema estiver indisponível, algo 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. Existem alarmes de infraestrutura configurados no CloudWatch e enviados para um endereço de email de piquete. Isso é monitorização, e não um programa de resposta a incidentes.

Nenhuma chave de cifragem gerida pelo cliente. A cifragem usa chaves geridas pela AWS.

Os registos só podem ser eliminados de uma forma. Nenhum registo confirmado individual pode ser editado ou eliminado por ninguém. A única via de eliminação é uma purga de todo o espaço de trabalho pedida pelo cliente, após o período de conservação de 730 dias.

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

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

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