Axiospec: segurança e tratamento de dados

Para equipas de TI e revisores de segurança. O Axiospec é um sistema de registos de calibração e de ativos desenvolvido pela CaliTech LLC, Knoxville, Tennessee (Estados Unidos). Esta página descreve a forma como o serviço em produção trata os dados dos clientes. Tudo o que se segue é uma afirmação sobre a produção. Última revisão: 21 de setembro de 2026.

Duas coisas a saber antes de continuar a leitura. O Axiospec não tem hoje nenhuma certificação de segurança, e dizemos exatamente o que temos e o que não temos na última secção, em vez de o obrigar a procurar. O Axiospec é um sistema de guarda de registos. Apoia e documenta o seu programa de calibração e mantém-no pronto para auditoria. Não certifica, assegura nem garante a sua conformidade com qualquer norma.

Onde ficam os seus dados

Amazon Web Services, uma única conta, região **us-east-1 (Norte da Virgínia, Estados Unidos)**. Todos os recursos de produção com estado estão declarados nessa única região: a base de dados PostgreSQL 16, o bucket de armazenamento de documentos, o bucket de registos de auditoria, o armazenamento de segredos e a computação da aplicação.

A rede de distribuição de conteúdos à frente da aplicação (Amazon CloudFront) é uma rede periférica global. Termina o TLS numa localização periférica que pode ficar fora dos Estados Unidos e reencaminha o pedido para us-east-1. As respostas da API estão configuradas explicitamente para **não** ficarem em cache na periferia. Só os recursos estáticos da aplicação e do sítio web ficam em cache. Os subcontratantes indicados abaixo tratam os dados nas suas próprias localizações.

Cifragem

Em trânsito. A aplicação e a API são servidas apenas por HTTPS. O HTTP simples é redirecionado. A versão mínima do TLS é a 1.2. A ligação da CDN de volta à aplicação também usa TLS 1.2. As ligações à base de dados exigem TLS (`sslmode=require`), e o serviço de autenticação recusa-se a arrancar com um URL de base de dados que não o exija.

Em repouso. A base de dados de produção tem a cifragem do armazenamento ativada. O bucket de registos de auditoria da infraestrutura é cifrado com SSE-S3 (AES-256). Os segredos da aplicação são guardados no AWS Secrets Manager e carregados em tempo de execução, em vez de ficarem em texto simples em variáveis de ambiente. A fila de mensagens usada para as tarefas em segundo plano que falharam utiliza a cifragem gerida pelo SQS.

Os ficheiros de evidência carregados (certificados de calibração, fotografias) são guardados no Amazon S3, que cifra os objetos em repouso por predefinição com SSE-S3. Não declaramos hoje essa definição de forma explícita no nosso código de infraestrutura, pelo que a descrevemos como a predefinição da

plataforma e não como um controlo que evidenciamos. Toda a cifragem usa chaves geridas pela AWS. Não existe a opção de chaves geridas pelo cliente (BYOK).

Isolamento de rede

A base de dados de produção **não é acessível publicamente**. A sua única regra de entrada é PostgreSQL a partir do próprio grupo de segurança da aplicação. Não é permitido nenhum intervalo de IP. A proteção contra eliminação está ativada.

A aplicação corre dentro de uma VPC, em duas zonas de disponibilidade, em sub-redes privadas sem endereços IP públicos. O tráfego de saída passa por um gateway NAT; o tráfego para o S3 usa um endpoint de gateway da VPC e não atravessa a internet pública. O grupo de segurança da aplicação não tem nenhuma regra de entrada.

Todos os buckets do S3 têm o acesso público totalmente bloqueado nas quatro definições. O bucket da aplicação de página única só pode ser lido pela nossa distribuição do CloudFront, o que é imposto pelo Origin Access Control e por uma política de bucket limitada a essa distribuição. O acesso de escrita da aplicação ao bucket de documentos está limitado a `PutObject` e `GetObject` nesse bucket.

Separação entre clientes

O Axiospec é multi-inquilino: uma base de dados partilhada com um esquema partilhado e **uma delimitação por inquilino ao nível da linha imposta na aplicação**. Todas as tabelas com dados de clientes têm um `tenant_id`. A identidade do inquilino é lida de uma declaração do token com assinatura verificada, nunca de um cabeçalho ou do corpo de um pedido enviados pelo cliente. Os tipos de registo principais (instrumentos, entradas do livro de registos, utilizadores) são ainda filtrados por um listener global de consultas que injeta a condição do inquilino em cada leitura. Os ficheiros carregados são guardados com chaves de objeto prefixadas pelo inquilino.

É preciso ser rigoroso quanto ao que isto é: trata-se de isolamento imposto pela aplicação, não da segurança ao nível da linha do PostgreSQL, e não de uma base de dados ou esquema separado por cliente.

Dentro de um espaço de trabalho existe um segundo limite. As permissões por instalação podem restringir um utilizador a fábricas ou localizações específicas, e o servidor verifica o âmbito da instalação nas operações de registar, aprovar, anular e exportar.

Autenticação e controlo de acessos

As palavras-passe são guardadas como hash PBKDF2-HMAC-SHA256 com 260 000 iterações e um sal aleatório por palavra-passe, e são verificadas em tempo constante. O início de sessão usa um endereço de email e uma palavra-passe ou o início de sessão com a Google, que está ativo em produção. As contas criadas através da Google não têm uma palavra-passe utilizável.

A proteção contra força bruta é um atraso exponencial por conta, partilhado por todas as instâncias da aplicação ao nível da base de dados e baseado num hash do identificador, de modo que uma conta inexistente se comporta exatamente como uma real. Tem um limite para não poder ser transformado numa negação de serviço contra os seus utilizadores.

A autenticação de dois fatores está disponível e é ativada pelo próprio utilizador. É uma palavra-passe de utilização única baseada no tempo, gerada por uma aplicação de autenticação, com códigos de recuperação de utilização única que são apresentados uma vez e guardados como hash, e um token opcional de dispositivo de confiança que permite a um dispositivo escolhido dispensar o segundo fator até ser revogado. Não existe opção de WebAuthn, chave de segurança ou SMS.

As sessões usam tokens assinados sem estado, com uma validade predefinida de 7 dias, guardados no armazenamento local do navegador. Desativar ou eliminar um utilizador produz efeito imediato: o estado da conta é novamente verificado na base de dados em cada pedido, pelo que um token existente deixa de funcionar no pedido seguinte desse utilizador. Não existe uma lista geral de revogação, pelo que um token roubado a um utilizador que continua ativo é válido até expirar.

O controlo de acessos baseado em funções é imposto no servidor, não no navegador. Cinco funções: superadministrador, administrador, gestor, técnico e auditor. A função é novamente lida da base de dados em cada pedido, em vez de se confiar no token. A função de auditor é imposta como apenas de leitura em todo o sistema, com uma única exceção restrita para gerar uma exportação de auditoria. Os gestores não podem promover utilizadores acima da sua própria autoridade.

Dois controlos da aplicação que interessam a um revisor da qualidade. Os registos de calibração confirmados não podem ser editados nem eliminados, o que é imposto por um trigger da base de dados, pelo que isto se mantém mesmo perante acesso SQL direto. As correções são acrescentadas como novos registos ligados, com um motivo escrito obrigatório. E quando um espaço de trabalho ativa a aprovação por duas pessoas, o sistema não permite que a pessoa que registou uma calibração a aprove.

Os controlos de acesso à consola de administração da nossa conta da AWS são confirmados à parte, mediante pedido.

Cópias de segurança e recuperação

Cópias de segurança diárias automáticas da base de dados com **um período de conservação de 14 dias**, que permite a recuperação para um momento específico dentro desse período. A proteção contra eliminação e um instantâneo final obrigatório estão ativados. Existem alarmes de infraestrutura configurados no CloudWatch para a CPU, o armazenamento e a pressão de ligações da base de dados, os erros da aplicação, a limitação de pedidos, a latência, a taxa de erros 5xx da CDN e as tarefas em segundo plano que falharam, enviados para um endereço de email de piquete.

Limites, com honestidade: a base de dados de produção está numa única zona de disponibilidade. Uma falha da zona exige uma reposição, não uma comutação automática. Não publicamos nenhum SLA de disponibilidade, RPO ou RTO, e não realizámos nenhum exercício de reposição documentado.

Registos e auditoria

Três camadas separadas.

1. **Infraestrutura.** O AWS CloudTrail está ativado em toda a conta e em todas as regiões, com validação da integridade dos ficheiros de registo, e escreve num bucket bloqueado e cifrado com conservação de 365

dias. Abrange os eventos de gestão. Os eventos de acesso ao nível do objeto do S3 não estão ativados, pelo que não existe um rasto ao nível do armazenamento de "quem descarregou que ficheiro".

2. **Atividade do espaço de trabalho.** Os convites e revogações da equipa, as alterações de função, o arquivamento de utilizadores e 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 a webhooks e os inícios de períodos de avaliação da faturação são escritos num registo de auditoria com o autor, a data e a hora, os campos alterados e o endereço IP. Os administradores do espaço de trabalho podem ler o seu próprio registo na aplicação.
3. **Registos de calibração.** Cada calibração confirmada é escrita num livro de registos apenas de acréscimo, com o utilizador que a registou e a data e a hora, encadeado com SHA-256 de modo que o hash de cada registo abrange o hash do registo anterior. O conteúdo dos ficheiros anexados entra na cadeia por hash, não apenas o caminho do ficheiro. Qualquer utilizador autenticado pode verificar a cadeia completa a partir da aplicação.

Um limite de âmbito que convém indicar: as edições ao registo mestre de um instrumento (etiqueta, número de série, intervalo de calibração, localização) ainda não são escritas no registo de atividade do espaço de trabalho. Os eventos de calibração propriamente ditos estão totalmente cobertos pelo livro de registos.

A monitorização de erros da aplicação é feita através do Sentry, com as informações de identificação pessoal desativadas por predefinição e uma função de limpeza própria aplicada a cada evento.

Subcontratantes e o que cada um vê

Entidade	Função	O que pode ver
Amazon Web Services (us-east-1)	Alojamento, base de dados, armazenamento, email, segredos, registos	Todos os dados dos clientes
Stripe	Processamento de pagamentos	Email de faturação e um identificador do espaço de trabalho. Os dados do cartão são introduzidos diretamente no Stripe e nunca chegam aos servidores do Axiospec. Nenhum dado de calibração ou de instrumentos.
Sentry	Monitorização de erros e de desempenho	Rastreios de pilha e caminhos de pedido após a limpeza. Não há garantia de que nunca contenham um identificador que apareça numa mensagem de erro.
Google (Firebase)	Notificações push no telemóvel	Tokens push dos dispositivos e o conteúdo das notificações, como os alertas de calibração a vencer
Google (Firebase Analytics)	Análise de produto apenas dentro da aplicação Android	Eventos de utilização da aplicação e o identificador interno do utilizador definido no início de sessão. A aplicação iOS não integra o SDK.

Entidade	Função	O que pode ver
Google (Analytics 4)	Análise de produto e do sítio web	Caminhos de página e eventos de interação, incluindo dentro da aplicação com sessão iniciada. Não é transmitido nenhum dado de calibração. Está implementado o Consent Mode v2 com predefinições regionais. O Google Ads foi descontinuado a 15 de setembro de 2026 e não é publicada nenhuma etiqueta de anúncios, conversão de anúncios ou píxel de remarketing.
Google (OAuth)	Início de sessão com a Google	O evento de início de sessão dos utilizadores que escolhem essa opção
Google (reconhecimento de voz do Android)	Ditado por voz de leituras na aplicação Android	O áudio ditado. Sai do dispositivo; o reconhecimento não é feito no próprio dispositivo.
Apple (reconhecimento de voz do iOS)	Ditado por voz de leituras na aplicação iOS	O áudio ditado, nas mesmas condições que no Android.
GitHub	Controlo de código-fonte e pipeline de implementação	Código-fonte. Nenhum dado de clientes.

Se configurar webhooks de saída, os dados dos eventos de calibração são também enviados para o destino que **a sua organização** escolher, e esse conteúdo indica o nome do técnico que realizou a calibração. Esse destino é um subcontratante seu, não nosso.

A mesma lista está publicada para os clientes em axiospec.com/subprocessors, com o que cada entidade recebe e porquê. As duas são mantidas em sintonia.

Propriedade e exportação dos dados

Os seus registos são seus. A exportação é feita pelo próprio cliente, é ilimitada e não depende de nenhum plano de preços. Os gestores, administradores e auditores podem gerar um arquivo de auditoria completo em qualquer momento.

O arquivo é um único ZIP com:

- `audit_manifest.csv`, uma linha por instrumento e depois uma linha por cada evento de calibração confirmado, incluindo o hash de cada registo e o hash do registo anterior em hexadecimal
- `audit_summary.pdf`, um relatório legível com o painel de conformidade, o resultado da verificação de integridade, o histórico de auditoria completo, o inventário de ativos e o detalhe do que está fora da tolerância
- os ficheiros de evidência originais, agrupados por etiqueta de instrumento
- um README com o âmbito da exportação, o primeiro e o último hash de registo e um procedimento passo a passo para **voltar a verificar por conta própria o encadeamento da cadeia, offline e sem o Axiospec**

As exportações podem ser restringidas por instalação, localização, instrumento, intervalo de datas ou estado de conformidade, e o âmbito só pode estreitar-se dentro das suas próprias permissões, nunca alargar-se. Tenha em conta que uma exportação com âmbito verifica o hash próprio de cada registo exportado, mas não afirma a continuidade de toda a cadeia, porque é um subconjunto deliberado. Só uma exportação completa, sem âmbito, percorre a cadeia inteira.

Os dados do inventário de instrumentos também podem ser exportados para CSV a partir do navegador em qualquer momento.

Se deixar de usar o Axiospec

A faturação termina de imediato quando pede o encerramento da conta. Os seus dados são conservados durante **730 dias (cerca de 24 meses)** depois disso, para que possa voltar a iniciar sessão e exportá-los, e para que possa reativar a conta se mudar de ideias. Findo esse período, são eliminados de forma permanente, incluindo os ficheiros de evidência guardados.

Não existe pagamento para exportar nem formato proprietário. Como o arquivo de auditoria é CSV em formato aberto, mais PDF, mais os seus ficheiros originais, mais instruções escritas para verificar de forma independente o encadeamento da cadeia, o pacote de evidências continua a poder ser verificado por um terceiro mesmo que o Axiospec deixe de existir.

O que ainda não temos

Preferimos dizê-lo logo à partida a deixar que o descubra num questionário.

- **Nenhum relatório SOC 2** (Tipo I ou Tipo II). Não foi realizada nenhuma auditoria e não há nenhum auditor contratado. O que oferecemos em alternativa: este documento, respostas diretas ao seu questionário e um contacto identificado que responde.
- **Nenhuma certificação ISO/IEC 27001.** Note que o Axiospec apoia os programas ISO 9001 e ISO/IEC 17025 dos clientes. Esse é o domínio do produto e não tem relação com a nossa própria certificação de segurança da informação. Não confundimos as duas coisas.
- **Nenhum teste de intrusão realizado por terceiros.** Apenas revisão interna.
- **Nenhum BAA da HIPAA, e nenhum programa FedRAMP, CMMC, NIST 800-171, ITAR ou DFARS 252.204-7012.** Não coloque informação de saúde protegida nem informação não classificada controlada no Axiospec.
- **Nenhum segundo fator por WebAuthn, chave de segurança ou SMS.** A autenticação de dois fatores do Axiospec é uma palavra-passe de utilização única baseada no tempo, gerada por uma aplicação de autenticação, com códigos de recuperação e um token opcional de dispositivo de confiança. É o único segundo fator disponível. O SSO empresarial por inquilino (OIDC e SAML 2.0) está ativado em produção. Os pedidos de autenticação SAML não são assinados nesta versão.
- **Nenhum DPA publicado, termos do RGPD, cláusulas contratuais-tipo ou região de dados na UE.** Todos os dados estão nos Estados Unidos, em us-east-1. Existem versões preliminares de um acordo de tratamento de dados e dos termos de transferência, que estão com os nossos advogados. Nada está em vigor, e não vamos descrever uma versão preliminar como se estivesse.

- **Nenhum SLA de disponibilidade, página de estado, RPO ou RTO**, e nenhum exercício de reposição documentado. As cópias de segurança estão configuradas; o tempo de recuperação não está garantido.
- **Nenhum controlo de versões de objetos no bucket de ficheiros de evidência.** Um ficheiro escrito por cima ou eliminado não tem via de recuperação ao nível do armazenamento. O registo da calibração no livro de registos mantém-se em qualquer caso.
- **Nenhum período definido de conservação dos registos da aplicação.** Hoje os registos da aplicação são conservados indefinidamente por predefinição.
- **Nenhum pacote de validação do software (IQ/OQ/PQ) e nenhuma matriz de rastreabilidade de requisitos para testes.** O que temos: 2465 funções de teste em 197 ficheiros de teste que têm de passar antes de qualquer implementação em produção, uma análise de vulnerabilidades das dependências que bloqueia a compilação, versões de produção lançadas apenas manualmente e imagens imutáveis por versão para reverter. É um controlo real de desenvolvimento de software. Não é um pacote de validação, e um revisor de validação de sistemas informatizados não o deve aceitar como tal.
- **Ainda não existe acesso de privilégio mínimo à infraestrutura.** A nossa função de implementação de CI tem o AWS AdministratorAccess. As implementações em produção são lançadas apenas manualmente e protegidas por um ambiente do GitHub, mas quem puder lançar esse fluxo de trabalho tem a administração completa da conta.
- **Nenhuma segregação de funções nem revisão formal de acessos.** A CaliTech LLC é uma empresa de uma só pessoa. Não existe um programa documentado de segurança do pessoal, um processo de verificação de antecedentes nem um programa de formação em segurança.
- **Nenhum plano completo de resposta a incidentes e nenhuma apólice de ciberseguro verificada.** O que existe, desde 21 de setembro de 2026, é um procedimento escrito de notificação de violações: o que conta como violação de dados pessoais, quem decide, o prazo de 72 horas e quem é informado e por que ordem. É um documento interno e ainda não foi testado num exercício. Existem alarmes de infraestrutura configurados no CloudWatch e enviados para um endereço de email de piquete, o que é monitorização e não um processo de resposta.

Não vamos descrever nada do que está acima como "em curso" nem como "alinhado com" algo que não temos.

Contacto de segurança

Envie questões de segurança, questionários ou comunicações de vulnerabilidades para **support@axiospec.com**. Respondemos no prazo de um dia útil. O Axiospec é desenvolvido pela CaliTech LLC, Knoxville, Tennessee (Estados Unidos).

Se a sua revisão precisar de um diagrama de arquitetura ou de fluxo de dados, de um questionário de segurança de fornecedores preenchido ou de uma chamada com a pessoa que escreveu o código, basta pedir. Recebe as três coisas a partir do mesmo endereço.