Axiospec: segurança e tratamento de dados

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

Duas coisas para saber antes de continuar a leitura. Hoje o Axiospec não tem nenhuma certificação de segurança, e dizemos exatamente o que temos e o que não temos na última seção, em vez de fazer você procurar. O Axiospec é um sistema de guarda de registros. Ele apoia e documenta o seu programa de calibração e o mantém pronto para auditoria. Ele não certifica, assegura nem garante a sua conformidade com nenhuma 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: o banco de dados PostgreSQL 16, o bucket de armazenamento de documentos, o bucket de logs de auditoria, o armazenamento de segredos e a computação do aplicativo.

A rede de distribuição de conteúdo na frente do aplicativo (Amazon CloudFront) é uma rede de borda global. Ela encerra o TLS em um ponto de presença que pode estar fora dos Estados Unidos e encaminha a solicitação para us-east-1. As respostas da API estão configuradas explicitamente para **não** ficar em cache na borda. Somente os recursos estáticos do aplicativo e do site ficam em cache. Os suboperadores listados abaixo tratam dados em seus próprios locais.

Criptografia

Em trânsito. O aplicativo e a API são servidos somente por HTTPS. O HTTP simples é redirecionado. A versão mínima do TLS é a 1.2. A conexão da CDN de volta ao aplicativo também usa TLS 1.2. As conexões com o banco de dados exigem TLS (`sslmode=require`), e o serviço de autenticação se recusa a iniciar com uma URL de banco de dados que não exija TLS.

Em repouso. O banco de dados de produção tem a criptografia de armazenamento ativada. O bucket de logs de auditoria da infraestrutura é criptografado com SSE-S3 (AES-256). Os segredos do aplicativo ficam no AWS Secrets Manager e são 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 usa a criptografia gerenciada pelo SQS.

Os arquivos de evidência enviados (certificados de calibração, fotos) ficam armazenados no Amazon S3, que criptografa os objetos em repouso por padrão com SSE-S3. Hoje não declaramos essa configuração de forma explícita no nosso código de infraestrutura, por isso a descrevemos como o padrão da plataforma, e

não como um controle que comprovamos. Toda a criptografia usa chaves gerenciadas pela AWS. Não há opção de chave gerenciada pelo cliente (BYOK).

Isolamento de rede

O banco de dados de produção **não é acessível publicamente**. A única regra de entrada dele é PostgreSQL a partir do próprio grupo de segurança do aplicativo. Nenhuma faixa de IP é permitida. A proteção contra exclusão está ativada.

O aplicativo roda 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 passa pela internet pública. O grupo de segurança do aplicativo não tem nenhuma regra de entrada.

Todos os buckets do S3 têm o acesso público totalmente bloqueado nas quatro configurações. O bucket do aplicativo 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 restrita a essa distribuição. O acesso de gravação do aplicativo ao bucket de documentos está limitado a `PutObject` e `GetObject` nesse bucket.

Separação entre clientes

O Axiospec é multilocatário: um banco de dados compartilhado com um esquema compartilhado e **um escopo por locatário no nível da linha imposto no aplicativo**. Toda tabela com dados de clientes tem um `tenant_id`. A identidade do locatário é lida de uma declaração do token com assinatura verificada, nunca de um cabeçalho ou do corpo de uma solicitação enviados pelo cliente. Os tipos de registro principais (instrumentos, lançamentos do livro-razão, usuários) também são filtrados por um listener global de consultas que injeta a condição do locatário em toda leitura. Os arquivos enviados são armazenados com chaves de objeto prefixadas pelo locatário.

É preciso ser exato sobre o que isso é: trata-se de isolamento imposto pelo aplicativo, não da segurança no nível da linha do PostgreSQL, e não de um banco de dados ou esquema separado por cliente.

Dentro de um espaço de trabalho existe um segundo limite. As permissões por unidade podem restringir um usuário a plantas ou locais específicos, e o servidor verifica o escopo da unidade nas operações de registrar, aprovar, anular e exportar.

Autenticação e controle de acesso

As senhas são armazenadas como hash PBKDF2-HMAC-SHA256 com 260.000 iterações e um salt aleatório por senha, e são verificadas em tempo constante. O login usa e-mail e senha ou o login com o Google, que está ativo em produção. As contas criadas pelo Google não têm uma senha utilizável.

A proteção contra força bruta é um atraso exponencial por conta, compartilhado entre todas as instâncias do aplicativo no nível do banco de dados e baseado em um hash do identificador, de modo que uma conta inexistente se comporta exatamente como uma real. Ele tem um limite para não poder ser transformado em uma negação de serviço contra os seus usuários.

A autenticação de dois fatores está disponível e cada usuário a ativa sozinho. É uma senha de uso único baseada em tempo, gerada por um aplicativo autenticador, com códigos de recuperação de uso único que são exibidos uma vez e armazenados como hash, e um token opcional de dispositivo confiável que permite a um dispositivo escolhido pular o segundo fator até ser revogado. Não há opção de WebAuthn, chave de segurança ou SMS.

As sessões usam tokens assinados sem estado, com validade padrão de 7 dias, guardados no armazenamento local do navegador. Desativar ou excluir um usuário tem efeito imediato: o estado da conta é verificado de novo no banco de dados a cada solicitação, então um token existente para de funcionar na próxima chamada desse usuário. Não há uma lista geral de revogação, então um token roubado de um usuário que continua ativo vale até expirar.

O controle de acesso baseado em funções é imposto no servidor, não no navegador. São cinco funções: superadministrador, administrador, gerente, técnico e auditor. A função é lida de novo do banco de dados a cada solicitação, em vez de se confiar no token. A função de auditor é imposta como somente leitura em todo o sistema, com uma única exceção restrita para gerar uma exportação de auditoria. Os gerentes não podem promover usuários acima da própria autoridade.

Dois controles do aplicativo que importam para um revisor da qualidade. Os registros de calibração confirmados não podem ser editados nem excluídos, o que é imposto por um trigger do banco de dados, então isso vale inclusive contra acesso SQL direto. As correções são acrescentadas como novos registros vinculados, com um motivo escrito obrigatório. E quando um espaço de trabalho ativa a revisão entre quem registra e quem aprova, o sistema não permite que a pessoa que registrou uma calibração a aprove.

Os controles de acesso ao console administrativo da nossa conta da AWS são confirmados separadamente, mediante solicitação.

Backups e recuperação

Backups diários automáticos do banco de dados com **uma janela de retenção de 14 dias**, que permite a recuperação para um ponto no tempo dentro dessa janela. A proteção contra exclusão e um snapshot final obrigatório estão ativados. Há alarmes de infraestrutura configurados no CloudWatch para CPU, armazenamento e pressão de conexões do banco de dados, erros do aplicativo, limitação de requisições, latência, taxa de erros 5xx da CDN e tarefas em segundo plano que falharam, enviados para um endereço de e-mail de plantão.

Limites, com honestidade: o banco de dados de produção fica em uma única zona de disponibilidade. Uma falha da zona exige uma restauração, não um failover automático. Não publicamos SLA de disponibilidade, RPO nem RTO, e não fizemos nenhum teste de restauração documentado.

Logs e auditoria

Três camadas separadas.

1. **Infraestrutura.** O AWS CloudTrail está ativado em toda a conta e em todas as regiões, com validação de integridade dos arquivos de log, gravando em um bucket bloqueado e criptografado com retenção de

365 dias. Isso cobre os eventos de gerenciamento. Os eventos de acesso no nível de objeto do S3 não estão ativados, então não existe uma trilha no nível do armazenamento de "quem baixou qual arquivo".

2. **Atividade do espaço de trabalho.** Convites e revogações da equipe, mudanças de função, arquivamento de usuários e mudanças de e-mail, emissão e revogação de chaves de API, mudanças na configuração de SSO e logins por SSO, mudanças em webhooks e inícios de período de teste do faturamento são gravados em um log 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 próprio log no aplicativo.
3. **Registros de calibração.** Cada calibração confirmada é gravada em um livro-razão somente de acréscimo, com o usuário que a registrou e a data e a hora, encadeado com SHA-256 de modo que o hash de cada registro cobre o hash do registro anterior. O conteúdo dos arquivos anexados entra na cadeia por hash, não apenas o caminho do arquivo. Qualquer usuário autenticado pode verificar a cadeia inteira pelo aplicativo.

Um limite de escopo que vale a pena dizer: as edições no cadastro mestre de um instrumento (tag, número de série, intervalo de calibração, local) ainda não são gravadas no log de atividade do espaço de trabalho. Os eventos de calibração em si são totalmente cobertos pelo livro-razão.

O monitoramento de erros do aplicativo é feito pelo Sentry, com as informações de identificação pessoal desativadas por padrão e uma função de limpeza própria aplicada a cada evento.

Suboperadores e o que cada um vê

Parte	Função	O que pode ver
Amazon Web Services (us-east-1)	Hospedagem, banco de dados, armazenamento, e-mail, segredos, logs	Todos os dados dos clientes
Stripe	Processamento de pagamentos	E-mail de cobrança e um identificador do espaço de trabalho. Os dados do cartão são digitados diretamente no Stripe e nunca chegam aos servidores do Axiospec. Nenhum dado de calibração ou de instrumentos.
Sentry	Monitoramento de erros e de desempenho	Rastreamentos de pilha e caminhos de solicitação após a limpeza. Não há garantia de que nunca contenham um identificador que apareça em uma mensagem de erro.
Google (Firebase)	Notificações push no celular	Tokens push dos dispositivos e o conteúdo das notificações, como os alertas de calibração a vencer
Google (Firebase Analytics)	Análise de produto somente dentro do aplicativo Android	Eventos de uso do aplicativo e o identificador interno do usuário definido no login. O aplicativo iOS não integra o SDK.

Parte	Função	O que pode ver
Google (Analytics 4)	Análise de produto e da web	Caminhos de página e eventos de interação, inclusive dentro do aplicativo com login. Nenhum dado de calibração é transmitido. O Consent Mode v2 com padrões regionais está implementado. O Google Ads foi descontinuado em 15 de setembro de 2026 e nenhuma tag de anúncio, conversão de anúncio ou pixel de remarketing é publicado.
Google (OAuth)	Login com o Google	O evento de login dos usuários que escolhem essa opção
Google (reconhecimento de voz do Android)	Ditado por voz de leituras no aplicativo Android	O áudio ditado. Ele sai do dispositivo; o reconhecimento não acontece no próprio aparelho.
Apple (reconhecimento de voz do iOS)	Ditado por voz de leituras no aplicativo iOS	O áudio ditado, nas mesmas condições do Android.
GitHub	Controle de código-fonte e pipeline de implantação	Código-fonte. Nenhum dado de clientes.

Se você configurar webhooks de saída, os dados dos eventos de calibração também são enviados ao destino que **você** escolher, e esse conteúdo inclui o nome do técnico que executou a calibração. Esse destino é o seu suboperador, não o nosso.

A mesma lista é publicada para os clientes em axiospec.com/subprocessors, com o que cada parte recebe e por quê. As duas são mantidas em sincronia.

Propriedade e exportação dos dados

Os seus registros são seus. A exportação é autosserviço, ilimitada e não depende de nenhum plano de preços. Gerentes, administradores e auditores podem gerar um arquivo de auditoria completo a qualquer momento.

O arquivo é um único ZIP com:

- `audit_manifest.csv`, uma linha por instrumento e depois uma linha por evento de calibração confirmado, incluindo o hash de cada registro e o hash do registro anterior em hexadecimal
- `audit_summary.pdf`, um relatório legível com o painel de conformidade, o resultado da verificação de integridade, a trilha de auditoria completa, o cadastro de ativos e o detalhamento do que está fora da tolerância
- os arquivos de evidência originais, agrupados por tag de instrumento
- um README com o escopo da exportação, o primeiro e o último hash de registro e um procedimento passo a passo para **verificar de novo, por conta própria, o encadeamento da cadeia, off-line e sem o Axiospec**

As exportações podem ser restringidas por unidade, local, instrumento, período ou status de conformidade, e o escopo só pode ficar mais restrito dentro das suas próprias permissões, nunca mais amplo. Observe que uma exportação com escopo verifica o hash próprio de cada registro exportado, mas não afirma a continuidade da cadeia inteira, porque é um subconjunto proposital. Somente uma exportação completa, sem escopo, percorre a cadeia inteira.

Os dados do cadastro de instrumentos também podem ser exportados para CSV pelo navegador a qualquer momento.

Se você parar de usar o Axiospec

A cobrança para imediatamente quando você solicita o encerramento da conta. Os seus dados são mantidos por **730 dias (cerca de 24 meses)** depois disso, para que você possa entrar de novo e exportá-los, e para que possa reativar a conta se mudar de ideia. Depois desse prazo, eles são apagados definitivamente, incluindo os arquivos de evidência armazenados.

Não existe cobrança para exportar nem formato proprietário. Como o arquivo de auditoria é CSV em formato aberto mais PDF mais os seus arquivos originais mais instruções escritas para verificar de forma independente o encadeamento da cadeia, um terceiro continua podendo conferir o pacote de evidências mesmo que o Axiospec deixe de existir.

O que ainda não temos

Preferimos contar isso logo de início a deixar que você descubra em um questionário.

- **Nenhum relatório SOC 2** (Tipo I ou Tipo II). Nenhuma auditoria foi feita e nenhum auditor foi contratado. O que oferecemos em vez disso: este documento, respostas diretas ao seu questionário e um contato nomeado que responde.
- **Nenhuma certificação ISO/IEC 27001.** Observe 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 misturamos as duas coisas.
- **Nenhum teste de invasão feito 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 informações de saúde protegidas nem informações não classificadas controladas no Axiospec.
- **Nenhum segundo fator por WebAuthn, chave de segurança ou SMS.** A autenticação de dois fatores do Axiospec é uma senha de uso único baseada em tempo, gerada por um aplicativo autenticador, com códigos de recuperação e um token opcional de dispositivo confiável. Esse é o único segundo fator oferecido. O SSO corporativo por locatário (OIDC e SAML 2.0) está ativado em produção. As solicitações de autenticação SAML não são assinadas nesta versão.
- **Nenhum DPA publicado, termos de GDPR, cláusulas contratuais padrão ou região de dados na UE.** Todos os dados estão nos Estados Unidos, em us-east-1. Existem minutas de um acordo de tratamento de dados e dos termos de transferência, e elas estão com os nossos advogados. Nada está em vigor, e não vamos descrever uma minuta como se estivesse.

- **Nenhum SLA de disponibilidade, página de status, RPO ou RTO**, e nenhum teste de restauração documentado. Os backups estão configurados; o tempo de recuperação não é garantido.
- **Nenhum versionamento de objetos no bucket de arquivos de evidência.** Um arquivo sobrescrito ou excluído não tem caminho de recuperação no nível do armazenamento. O registro da calibração no livro-razão sobrevive de qualquer forma.
- **Nenhum período definido de retenção dos logs do aplicativo.** Hoje os logs do aplicativo ficam guardados indefinidamente por padrão.
- **Nenhum pacote de validação de software (IQ/OQ/PQ) e nenhuma matriz de rastreabilidade de requisitos para testes.** O que temos: 2.465 funções de teste em 197 arquivos de teste que precisam passar antes de qualquer implantação em produção, uma verificação de vulnerabilidades de dependências que bloqueia a compilação, versões de produção disparadas somente de forma manual e imagens imutáveis por versão para reverter. Esse é um controle real de desenvolvimento de software. Não é um pacote de validação, e um revisor de validação de sistemas computadorizados não deve aceitá-lo como tal.
- **Ainda não há acesso de privilégio mínimo à infraestrutura.** A nossa função de implantação de CI tem o AWS AdministratorAccess. As implantações em produção são disparadas somente de forma manual e protegidas por um ambiente do GitHub, mas quem puder disparar 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 há programa documentado de segurança de pessoal, processo de verificação de antecedentes nem programa de treinamento em segurança.
- **Nenhum plano completo de resposta a incidentes e nenhuma apólice de seguro cibernético 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 avisado e em que ordem. É um documento interno e ainda não foi exercitado em uma simulação. Há alarmes de infraestrutura configurados no CloudWatch e enviados para um endereço de e-mail de plantão, o que é monitoramento, e não um processo de resposta.

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

Contato de segurança

Envie perguntas de segurança, questionários ou relatos de vulnerabilidades para **support@axiospec.com**. Respondemos em até 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, é só pedir. Você recebe os três pelo mesmo endereço.