ARANIS

Security Posture Document

Descrição pública dos controles de segurança, privacidade e continuidade da plataforma Aranis

VERSÃO	2.1	CLASSIFICAÇÃO	Público
DATA DE EMISSÃO	19 de novembro de 2026	PRÓXIMA REVISÃO	Maio de 2027 (ou após mudança material)
RESPONSÁVEL	Paulo Nascimento — Fundador / Security Owner / DPO	CONTATO	security@aranis.ai

1. Identificação e escopo

A **Aranis** (aranis.ai) é uma plataforma SaaS B2B de gestão de risco de terceiros (TPRM) e risco cibernético, operada pela **Aranis Tecnologia em Desenvolvimento de Software Não Customizável Ltda** (Brasil). Este documento descreve os controles técnicos, organizacionais e de privacidade aplicados ao ambiente de produção da plataforma.

O escopo abrange as aplicações `aranis.ai`, `app.aranis.ai`, `tools.aranis.ai`, `docs.aranis.ai` e `trust.aranis.ai`, a infraestrutura de nuvem que as sustenta, e os dados de clientes nelas processados.

Este documento não é um relatório de auditoria independente. Ele descreve controles autodeclarados, sustentados por políticas internas formalizadas, registro de riscos e evidências operacionais disponíveis mediante solicitação sob NDA.

2. Certificações e atestações

Atestação	Status	Detalhe
CSA STAR Level 1	VIGENTE	Autoavaliação CAIQ v4.0.3 publicada no CSA STAR Registry em 06/07/2026. Verificável publicamente em `cloudsecurityalliance.org/star/registry/aranis`.
Conformidade LGPD	IMPLEMENTADA	Lei 13.709/2018. DPA, política de privacidade, base legal mapeada por finalidade e processo de resposta a titulares.
Crosswalk SOC 2 (TSC)	MAPEADO	Catálogo interno de controles mapeado às cinco categorias dos Trust Services Criteria. Preparatório para auditoria formal.
Crosswalk GDPR	MAPEADO	Mapeamento do catálogo de controles aos artigos aplicáveis do Regulamento (UE) 2016/679.
Pentest externo independente	PLANEJADO	Contratação prevista conforme evolução da base de clientes. Hoje a cobertura é de varredura automatizada contínua.
SOC 2 Type I	PLANEJADO	Próximo marco formal de certificação após o CSA STAR.

> **Transparência sobre maturidade.** A Aranis não possui, nesta data, certificação de terceira parte auditada (SOC 2, ISO 27001). Os controles descritos a seguir são reais e documentados internamente, e a empresa se compromete a não representar controles planejados como implementados.

3. Arquitetura e stack de produção

A plataforma é cloud-native e roda integralmente na Amazon Web Services (AWS), na região **us-east-1** (Estados Unidos). Não há infraestrutura on-premises sob gestão da Aranis, e o modelo de responsabilidade compartilhada dos provedores é considerado explicitamente no desenho dos controles.

Camada	Tecnologia	Função
Aplicação	Next.js (App Router)	Frontend e API routes
Hospedagem / rede / perímetro	Amazon Web Services (us-east-1), Cloudflare	Computação, balanceamento de carga, terminação TLS, proteção de perímetro, DNS
Banco de dados / Auth	Supabase self-hosted na AWS (PostgreSQL)	Persistência, autenticação, Row Level Security
Armazenamento de objetos	Amazon S3	Evidências e anexos de avaliações
Orquestração de jobs	Inngest	Execução assíncrona e workflows
Camada de IA	Amazon Bedrock (primário); Anthropic, OpenAI (contingência)	Agentes de avaliação, evidência e relatório
Pagamentos	Stripe	Cobrança; dados de cartão tokenizados, nunca trafegam pela Aranis
E-mail transacional	Resend / Amazon SES	Notificações e convites
Observabilidade	Amazon CloudWatch, BetterStack	Logs, métricas, alertas e página pública de status
DevSecOps	GitHub, Semgrep, Gitleaks, Dependabot	SAST, secret scanning, análise de composição de dependências

4. Governança de segurança

A Aranis mantém um conjunto de políticas de segurança formalizadas, versionadas e revisadas periodicamente, com aprovação do Security Owner:

- Política de Segurança da Informação
- Política de Controle de Acesso e Identidade
- Política de Criptografia e Proteção de Dados
- Política de Desenvolvimento Seguro (SSDLC)
- Política de Gestão de Vulnerabilidades
- Política de Resposta a Incidentes de Segurança
- Política de Gestão de Terceiros e Subprocessadores
- Política de Retenção e Descarte de Dados
- Política de Uso Aceitável e Confidencialidade
- Definição formal de RTO e RPO
- Runbook de Recuperação de Desastres

A gestão de riscos corporativos é conduzida por meio de um **Risk Register** formal, com riscos classificados por probabilidade e impacto, tratamento definido (mitigar, aceitar, transferir, evitar) e responsável nomeado. O registro é revisado trimestralmente.

5. Criptografia e proteção de dados

- **Em trânsito:** apenas TLS 1.2 e TLS 1.3 são aceitos em todos os endpoints públicos; TLS 1.0 e 1.1 são recusados, e HTTP sem criptografia é redirecionado para HTTPS. Headers obrigatórios: `Strict-Transport-Security`, `X-Content-Type-Options`, `X-Frame-Options`.
- **Em repouso:** AES-256 no armazenamento do banco de dados de produção, nos backups e no armazenamento de objetos, com chaves de criptografia gerenciadas pela AWS (AWS KMS nos volumes do banco de dados).
- **Gestão de chaves e segredos:** segredos armazenados no AWS Secrets Manager e em configuração de ambiente protegida, nunca em código. Varredura contínua de segredos expostos em commits e histórico Git.
- **Isolamento multi-tenant:** segregação lógica por tenant, com Row Level Security (RLS) ativo em todas as tabelas que contêm dados de clientes como segunda camada de defesa após o controle de aplicação.
- **Dados de pagamento:** processados integralmente pelo Stripe. A Aranis não armazena, transmite nem processa dados primários de cartão.

6. Controle de acesso e identidade

- Autenticação multifator (MFA) obrigatória em todas as contas administrativas de provedores críticos.
- Modelo RBAC dentro de cada tenant, com os papéis `owner`, `admin`, `member` e `viewer`.
- Princípio do menor privilégio aplicado a chaves de API, tokens de serviço, papéis IAM e integrações OAuth, com escopo restrito por função.
- Rotação programada de chaves de API e revogação imediata em caso de exposição ou encerramento de relacionamento com terceiros.
- Revisão periódica (trimestral) de acessos, permissões e credenciais ativas.

7. Desenvolvimento seguro e gestão de vulnerabilidades

Toda alteração de código passa por varredura antes de chegar à produção. Análise estática de código (Semgrep, incluindo regras específicas de segurança de IA) e detecção de segredos expostos em todo o histórico Git (Gitleaks) rodam a cada pull request e bloqueiam o merge em achados críticos. A análise de composição de dependências roda continuamente via Dependabot e auditoria de dependências.

SLAs de remediação

Severidade	CVSS	Prazo máximo	Tratamento
Crítico	9.0 – 10.0	24 horas	Isolamento imediato do componente se necessário; notificação a clientes impactados em até 72h
Alto	7.0 – 8.9	7 dias	Remediação iniciada de imediato, rastreada como P1
Médio	4.0 – 6.9	30 dias	Rastreado como P2, incluído no ciclo de desenvolvimento seguinte
Baixo	0.1 – 3.9	90 dias	Backlog priorizado por capacidade

Segredos expostos são sempre tratados como **críticos**, independentemente do CVSS, com revogação e rotação imediatas da credencial afetada e auditoria dos acessos dos 30 dias anteriores. Toda vulnerabilidade é triada em até 48 horas após a detecção. Exceções e aceitações formais de risco exigem justificativa documentada, controles compensatórios e data de reavaliação em no máximo 90 dias.

8. Segurança e governança de Inteligência Artificial

- Os controles de IA da plataforma são desenhados sob o **NIST AI RMF**, também presente no catálogo de controles do produto.
- A inferência de modelos roda principalmente no **Amazon Bedrock**, na região us-east-1 da AWS, onde prompts e respostas ficam dentro da AWS e não são compartilhados com os desenvolvedores dos modelos. As APIs da Anthropic e da OpenAI estão configuradas como provedores de contingência e podem ser usadas para garantir a continuidade.
- Dados de clientes não são utilizados para treinamento de modelos, conforme os termos comerciais de todos os provedores de IA em uso.
- Um modelo só pode ser ativado após revisão de compliance e de subprocessador; modelos não revisados ficam bloqueados no roteamento de modelos da plataforma.
- Aplicação de guardrails e tokenização/minimização de conteúdo antes das chamadas aos modelos, reduzindo a exposição de dados pessoais desnecessários ao processamento.
- Registro de auditoria das operações de IA, armazenando hashes das entradas em vez do conteúdo original, evitando a persistência de dados pessoais em logs.
- Toda saída de agente que impacte decisões de risco é rastreável ao controle e à evidência que a originou.

9. Continuidade de negócio e resiliência

Parâmetro	Compromisso
Disponibilidade alvo (SLA)	99,5% mensal
RTO — Recovery Time Objective	Inferior a 4 horas
RPO — Recovery Point Objective	Inferior a 24 horas
Backup	Backups diários automatizados do banco de dados de produção, criptografados em repouso
Página de status pública	status.aranis.ai — monitoramento externo independente
Runbook de recuperação	Documentado e revisado após todo incidente P0/P1

10. Resposta a incidentes

A Aranis mantém processo formal de resposta a incidentes cobrindo detecção, triagem, contenção, erradicação, recuperação e comunicação, alinhado ao Art. 48 da LGPD.

- **Fontes de detecção:** varredura de segurança contínua, logs e alarmes de infraestrutura e aplicação (Amazon CloudWatch), monitoramento externo de disponibilidade, boletins de segurança de subprocessadores e relatos de clientes.
- **Classificação:** severidades P0 a P3, com escalonamento automático para crítico quando há risco a dados de clientes.
- **Comunicação:** clientes afetados são notificados dentro dos prazos regulatórios aplicáveis; a ANPD é comunicada quando exigido.
- **Registro:** todo incidente é registrado com data de detecção e resolução, severidade, sistemas afetados, causa raiz e ações corretivas.
- **Pós-incidente:** revisão obrigatória do runbook e do Risk Register após incidentes P0/P1.

11. Privacidade e proteção de dados pessoais

- Base legal mapeada por finalidade de tratamento, conforme LGPD.
- DPA (Data Processing Agreement) disponibilizado a clientes, incluindo cláusulas de subprocessamento e transferência internacional.
- Os dados de clientes ficam hospedados nos Estados Unidos (AWS us-east-1). Transferências internacionais amparadas por cláusulas contratuais padrão (SCCs) nos DPAs dos provedores e avaliação de adequação do país receptor.
- Direitos dos titulares (acesso, correção, eliminação, portabilidade) atendidos por processo documentado.
- O cliente pode excluir seus dados e sua conta a qualquer momento, diretamente na plataforma. Retenção e descarte são regidos pela Política de Retenção e Descarte de Dados.
- Notificação a clientes com 30 dias de antecedência sobre a inclusão de novos subprocessadores.

12. Subprocessadores

Lista de subprocessadores ativos na data de emissão deste documento. A lista completa e atualizada é mantida em trust.aranis.ai.

Subprocessador	Categoria	Dados processados	Localização
Amazon Web Services	Hospedagem, banco de dados, armazenamento, IA (Bedrock), e-mail (SES)	Dados de clientes, usuários e avaliações; evidências; conteúdo de prompts de IA	EUA (us-east-1)
Cloudflare	DNS / CDN / perímetro	Dados em trânsito, tráfego	Global
Anthropic	IA / LLM (contingência)	Conteúdo de prompts de IA, quando roteado	EUA
OpenAI	IA / LLM (contingência)	Conteúdo de prompts de IA, quando roteado	EUA
Stripe	Pagamentos	Dados de cobrança; cartão tokenizado	EUA
Resend	E-mail transacional	Endereços de e-mail e conteúdo de mensagens	EUA
Inngest	Orquestração de jobs	Payloads de eventos	EUA
BetterStack	Monitoramento de disponibilidade / página de status	Telemetria de disponibilidade (sem dados de clientes)	UE / EUA
GitHub / Microsoft	Controle de versão e segurança de código	Código-fonte (sem dados de clientes)	EUA
Atlassian	Documentação / gestão	Documentação interna (sem dados de clientes)	EUA / AU

13. Frameworks de referência

Os controles da Aranis — tanto os aplicados internamente quanto os oferecidos pelo produto — são ancorados nos seguintes frameworks:

- **NIST CSF 2.0** — funções Govern, Identify, Protect, Detect, Respond, Recover
- **ISO/IEC 27001:2022** — cláusulas de controle aplicáveis a ambiente cloud-native
- **ISO 22301** — continuidade de negócios
- **NIST AI RMF** — governança de sistemas de IA
- **CSA CCM / CAIQ v4** — base da autoavaliação CSA STAR Level 1
- **LGPD** (Lei 13.709/2018) e **GDPR** (Regulamento UE 2016/679)
- **AICPA Trust Services Criteria** — crosswalk preparatório para SOC 2
- **MITRE ATT&CK** — mapeamento de técnicas adversárias a controles

14. Contato e verificação

Finalidade	Canal
Questões de segurança e due diligence	security@aranis.ai
Privacidade e direitos de titulares (DPO)	privacy@aranis.ai
Reporte de vulnerabilidade	security@aranis.ai
Trust Center e documentação pública	trust.aranis.ai
Status operacional em tempo real	status.aranis.ai

Evidências detalhadas de controles, o CAIQ completo e políticas internas podem ser disponibilizados a clientes e prospects mediante acordo de confidencialidade.

15. Histórico de revisões

Versão	Data	Alterações
2.1	19/11/2026	Produção migrada para a AWS (us-east-1): banco de dados (Supabase self-hosted), armazenamento em Amazon S3 e IA no Amazon Bedrock, com Anthropic e OpenAI como provedores de contingência. Atualizados ferramentas de DevSecOps, observabilidade, descrição de backup, exclusão de dados e lista de subprocessadores. Entidade operadora atualizada. Data do registro CSA STAR corrigida para 06/07/2026.
2.0	08/07/2026	Versão pública inicial em PT/EN/ES.