ARANIS

Security Posture Document

Descripción pública de los controles de seguridad, privacidad y continuidad de la plataforma Aranis

VERSIÓN	2.1	CLASIFICACIÓN	Público
FECHA DE EMISIÓN	19 de noviembre de 2026	PRÓXIMA REVISIÓN	Mayo de 2027 (o ante cambio material)
RESPONSABLE	Paulo Nascimento — Fundador / Security Owner / DPO	CONTACTO	security@aranis.ai

1. Identificación y alcance

Aranis (aranis.ai) es una plataforma SaaS B2B de gestión de riesgo de terceros (TPRM) y riesgo cibernético, operada por **Aranis Tecnologia em Desenvolvimento de Software Não Customizável Ltda** (Brasil). Este documento describe los controles técnicos, organizativos y de privacidad aplicados al entorno de producción de la plataforma.

El alcance comprende las aplicaciones `aranis.ai`, `app.aranis.ai`, `tools.aranis.ai`, `docs.aranis.ai` y `trust.aranis.ai`, la infraestructura en la nube que las sostiene, y los datos de clientes procesados en ellas.

Este documento no constituye un informe de auditoría independiente. Describe controles autodeclarados, respaldados por políticas internas formalizadas, un registro de riesgos y evidencias operativas disponibles bajo solicitud y acuerdo de confidencialidad.

2. Certificaciones y atestaciones

Atestación	Estado	Detalle
CSA STAR Nivel 1	VIGENTE	Autoevaluación CAIQ v4.0.3 publicada en el CSA STAR Registry el 6 de julio de 2026. Verificable públicamente en `cloudsecurityalliance.org/star/registry/aranis`.
Cumplimiento LGPD	IMPLEMENTADO	Ley brasileña 13.709/2018. DPA, política de privacidad, base legal mapeada por finalidad y proceso documentado de atención a titulares.
Crosswalk SOC 2 (TSC)	MAPEADO	Catálogo interno de controles mapeado a las cinco categorías de los Trust Services Criteria. Preparatorio para auditoría formal.
Crosswalk GDPR	MAPEADO	Catálogo de controles mapeado a los artículos aplicables del Reglamento (UE) 2016/679.
Pentest externo independiente	PLANIFICADO	Contratación prevista conforme crezca la base de clientes. La cobertura actual es de escaneo automatizado continuo.
SOC 2 Tipo I	PLANIFICADO	Siguiente hito formal de certificación tras CSA STAR.

> **Transparencia sobre la madurez.** A esta fecha, Aranis no cuenta con una certificación auditada por tercera parte (SOC 2, ISO 27001). Los controles descritos a continuación son reales y están documentados internamente, y la empresa se compromete a no presentar controles planificados como implementados.

3. Arquitectura y stack de producción

La plataforma es cloud-native y opera íntegramente en Amazon Web Services (AWS), en la región **us-east-1** (Estados Unidos). Aranis no gestiona infraestructura on-premises, y el modelo de responsabilidad compartida de sus proveedores se considera explícitamente en el diseño de los controles.

Capa	Tecnología	Función
Aplicación	Next.js (App Router)	Frontend y rutas de API
Hospedaje / red / perímetro	Amazon Web Services (us-east-1), Cloudflare	Cómputo, balanceo de carga, terminación TLS, protección perimetral, DNS
Base de datos / Auth	Supabase autoalojado en AWS (PostgreSQL)	Persistencia, autenticación, Row Level Security
Almacenamiento de objetos	Amazon S3	Evidencias y adjuntos de evaluaciones
Orquestación de tareas	Inngest	Ejecución asíncrona y flujos de trabajo
Capa de IA	Amazon Bedrock (primario); Anthropic, OpenAI (contingencia)	Agentes de evaluación, evidencia e informes
Pagos	Stripe	Facturación; datos de tarjeta tokenizados, nunca transitan por Aranis
Correo transaccional	Resend / Amazon SES	Notificaciones e invitaciones
Observabilidad	Amazon CloudWatch, BetterStack	Logs, métricas, alertas y página pública de estado
DevSecOps	GitHub, Semgrep, Gitleaks, Dependabot	SAST, detección de secretos, análisis de composición de dependencias

4. Gobernanza de seguridad

Aranis mantiene un conjunto de políticas de seguridad formalizadas, versionadas y revisadas periódicamente, aprobadas por el Security Owner:

- Política de Seguridad de la Información
- Política de Control de Acceso e Identidad
- Política de Cifrado y Protección de Datos
- Política de Desarrollo Seguro (SSDLC)
- Política de Gestión de Vulnerabilidades
- Política de Respuesta a Incidentes de Seguridad
- Política de Gestión de Terceros y Subencargados
- Política de Retención y Eliminación de Datos
- Política de Uso Aceptable y Confidencialidad
- Definición formal de RTO y RPO
- Runbook de Recuperación ante Desastres

La gestión de riesgos corporativos se conduce mediante un **Risk Register** formal, con riesgos clasificados por probabilidad e impacto, tratamiento definido (mitigar, aceptar, transferir, evitar) y responsable designado. El registro se revisa trimestralmente.

5. Cifrado y protección de datos

- **En tránsito:** solo se aceptan TLS 1.2 y TLS 1.3 en todos los endpoints públicos; TLS 1.0 y 1.1 se rechazan, y el HTTP sin cifrar se redirige a HTTPS. Cabeceras obligatorias: `Strict-Transport-Security`, `X-Content-Type-Options`, `X-Frame-Options`.
- **En reposo:** AES-256 en el almacenamiento de la base de datos de producción, los respaldos y el almacenamiento de objetos, con claves de cifrado gestionadas por AWS (AWS KMS en los volúmenes de la base de datos).
- **Gestión de claves y secretos:** los secretos se almacenan en AWS Secrets Manager y en configuración de entorno protegida, nunca en código. Escaneo continuo de secretos expuestos en commits e historial de Git.
- **Aislamiento multi-tenant:** segregación lógica por tenant, con Row Level Security (RLS) activo en todas las tablas que contienen datos de clientes, como segunda línea de defensa tras el control de aplicación.
- **Datos de pago:** procesados íntegramente por Stripe. Aranis no almacena, transmite ni procesa datos primarios de tarjeta.

6. Control de acceso e identidad

- Autenticación multifactor (MFA) obligatoria en todas las cuentas administrativas de proveedores críticos.
- Modelo RBAC dentro de cada tenant, con los roles `owner`, `admin`, `member` y `viewer`.
- Principio de mínimo privilegio aplicado a claves de API, tokens de servicio, roles IAM e integraciones OAuth, con alcance restringido por función.
- Rotación programada de claves de API y revocación inmediata ante exposición o término de la relación con un tercero.
- Revisión periódica (trimestral) de accesos, permisos y credenciales activas.

7. Desarrollo seguro y gestión de vulnerabilidades

Todo cambio de código se escanea antes de llegar a producción. El análisis estático de código (Semgrep, con reglas específicas de seguridad de IA) y la detección de secretos expuestos en todo el historial de Git (Gitleaks) se ejecutan en cada pull request y bloquean el merge ante hallazgos críticos. El análisis de composición de dependencias se ejecuta de forma continua mediante Dependabot y auditorías de dependencias.

SLA de remediación

Severidad	CVSS	Plazo máximo	Tratamiento
Crítica	9.0 – 10.0	24 horas	Aislamiento inmediato del componente afectado si es necesario; notificación a clientes impactados en hasta 72 horas
Alta	7.0 – 8.9	7 días	Remediación iniciada de inmediato, rastreada como P1
Media	4.0 – 6.9	30 días	Rastreada como P2, incluida en el siguiente ciclo de desarrollo
Baja	0.1 – 3.9	90 días	Backlog, priorizado según capacidad

Los secretos expuestos se tratan siempre como **críticos**, con independencia del CVSS, exigiendo revocación y rotación inmediatas de la credencial afectada y auditoría de los accesos de los 30 días previos. Toda vulnerabilidad se tría en un plazo de 48 horas desde su detección. Las excepciones y aceptaciones formales de riesgo requieren justificación documentada, controles compensatorios y fecha de reevaluación en un máximo de 90 días.

8. Seguridad y gobernanza de Inteligencia Artificial

- Los controles de IA de la plataforma están diseñados conforme al **NIST AI RMF**, presente también en el catálogo de controles del producto.
- La inferencia de modelos se ejecuta principalmente en **Amazon Bedrock**, en la región us-east-1 de AWS, donde los prompts y las respuestas permanecen dentro de AWS y no se comparten con los desarrolladores de los modelos. Las API de Anthropic y OpenAI están configuradas como proveedores de contingencia y pueden utilizarse para garantizar la continuidad.
- Los datos de clientes no se utilizan para el entrenamiento de modelos, conforme a los términos comerciales de todos los proveedores de IA en uso.
- Un modelo solo puede activarse tras una revisión de cumplimiento y de subencargado; los modelos no revisados permanecen bloqueados en el enrutamiento de modelos de la plataforma.
- Se aplican guardrails y tokenización/minimización de contenido antes de las llamadas a los modelos, reduciendo la exposición innecesaria de datos personales al procesamiento.
- Las operaciones de IA se registran en un log de auditoría que almacena hashes de las entradas en lugar del contenido original, evitando la persistencia de datos personales en logs.
- Toda salida de agente que influya en una decisión de riesgo es trazable hasta el control y la evidencia que la originaron.

9. Continuidad de negocio y resiliencia

Parámetro	Compromiso
Disponibilidad objetivo (SLA)	99,5 % mensual
RTO — Recovery Time Objective	Inferior a 4 horas
RPO — Recovery Point Objective	Inferior a 24 horas
Respaldo	Respaldos diarios automatizados de la base de datos de producción, cifrados en reposo
Página pública de estado	status.aranis.ai — monitoreo externo independiente
Runbook de recuperación	Documentado y revisado tras cada incidente P0/P1

10. Respuesta a incidentes

Aranis mantiene un proceso formal de respuesta a incidentes que cubre detección, triaje, contención, erradicación, recuperación y comunicación, alineado con el Art. 48 de la LGPD.

- **Fuentes de detección:** escaneo de seguridad continuo, logs y alarmas de infraestructura y aplicación (Amazon CloudWatch), monitoreo externo de disponibilidad, boletines de seguridad de subencargados y reportes de clientes.
- **Clasificación:** severidades P0 a P3, con escalamiento automático a crítico cuando existe riesgo para datos de clientes.
- **Comunicación:** los clientes afectados son notificados dentro de los plazos regulatorios aplicables; la autoridad nacional (ANPD) es comunicada cuando corresponde.
- **Registro:** todo incidente se registra con fecha de detección y resolución, severidad, sistemas afectados, causa raíz y acciones correctivas.
- **Post-incidente:** revisión obligatoria del runbook y del Risk Register tras incidentes P0/P1.

11. Privacidad y protección de datos personales

- Base legal mapeada por finalidad de tratamiento, conforme a la LGPD.
- DPA (Data Processing Agreement) puesto a disposición de los clientes, incluyendo cláusulas de subencargo y transferencia internacional.
- Los datos de clientes se alojan en Estados Unidos (AWS us-east-1). Las transferencias internacionales se amparan en cláusulas contractuales tipo (SCC) de los DPA de los proveedores y en la evaluación de adecuación del país receptor.
- Los derechos de los titulares (acceso, corrección, eliminación, portabilidad) se atienden mediante un proceso documentado.
- El cliente puede eliminar sus datos y su cuenta en cualquier momento, directamente en la plataforma. La retención y eliminación se rigen por la Política de Retención y Eliminación de Datos.
- Se notifica a los clientes con 30 días de antelación la incorporación de cualquier nuevo subencargado.

12. Subencargados

Subencargados activos a la fecha de emisión de este documento. La lista completa y actualizada se mantiene en trust.aranis.ai.

Subencargado	Categoría	Datos procesados	Ubicación
Amazon Web Services	Hospedaje, base de datos, almacenamiento, IA (Bedrock), correo (SES)	Datos de clientes, usuarios y evaluaciones; evidencias; contenido de prompts de IA	EE. UU. (us-east-1)
Cloudflare	DNS / CDN / perímetro	Datos en tránsito, tráfico	Global
Anthropic	IA / LLM (contingencia)	Contenido de prompts de IA, cuando se enruta	EE. UU.
OpenAI	IA / LLM (contingencia)	Contenido de prompts de IA, cuando se enruta	EE. UU.
Stripe	Pagos	Datos de facturación; tarjeta tokenizada	EE. UU.
Resend	Correo transaccional	Direcciones de correo y contenido de mensajes	EE. UU.
Inngest	Orquestación de tareas	Payloads de eventos	EE. UU.
BetterStack	Monitoreo de disponibilidad / página de estado	Telemetría de disponibilidad (sin datos de clientes)	UE / EE. UU.
GitHub / Microsoft	Control de versiones y seguridad de código	Código fuente (sin datos de clientes)	EE. UU.
Atlassian	Documentación / gestión	Documentación interna (sin datos de clientes)	EE. UU. / AU

13. Marcos de referencia

Los controles de Aranis — tanto los aplicados internamente como los ofrecidos por el producto — se anclan en los siguientes marcos:

- **NIST CSF 2.0** — funciones Govern, Identify, Protect, Detect, Respond, Recover
- **ISO/IEC 27001:2022** — cláusulas de control aplicables a un entorno cloud-native
- **ISO 22301** — continuidad de negocio
- **NIST AI RMF** — gobernanza de sistemas de IA
- **CSA CCM / CAIQ v4** — base de la autoevaluación CSA STAR Nivel 1
- **LGPD** (Ley brasileña 13.709/2018) y **GDPR** (Reglamento UE 2016/679)
- **AICPA Trust Services Criteria** — crosswalk preparatorio para SOC 2
- **MITRE ATT&CK** — mapeo de técnicas adversarias a controles

14. Contacto y verificación

Finalidad	Canal
Consultas de seguridad y due diligence	security@aranis.ai
Privacidad y derechos de titulares (DPO)	privacy@aranis.ai
Reporte de vulnerabilidades	security@aranis.ai
Trust Center y documentación pública	trust.aranis.ai
Estado operativo en tiempo real	status.aranis.ai

Las evidencias detalladas de controles, el CAIQ completo y las políticas internas pueden ponerse a disposición de clientes y prospectos mediante acuerdo de confidencialidad.

15. Historial de revisiones

Versión	Fecha	Cambios
2.1	19/11/2026	Producción migrada a AWS (us-east-1): base de datos (Supabase autoalojado), almacenamiento en Amazon S3 e IA en Amazon Bedrock, con Anthropic y OpenAI como proveedores de contingencia. Actualizadas las herramientas de DevSecOps, la observabilidad, la descripción de respaldos, la eliminación de datos y la lista de subencargados. Entidad operadora actualizada. Fecha del registro CSA STAR corregida al 6 de julio de 2026.
2.0	08/07/2026	Versión pública inicial en PT/EN/ES.