Certificações e relatórios independentes

Código do Documento: DEC-CRT-022	Versão: 1.0
Data de Emissão: Janeiro de 2026	Classificação de Informação: Uso Interno / Clientes / Auditoria
Área Responsável: Governança de TI, Segurança & DevOps	Aplica-se a: Todos os Serviços e Infraestrutura em Nuvem

1. OBJETIVO

Esta declaração formal visa esclarecer o escopo de certificações e relatórios de auditoria independente aplicáveis ao serviço, garantindo o atendimento técnico.

2. ENQUADRAMENTO DA CONFORMIDADE (PARCIAL)

O enquadramento da conformidade do serviço é classificado formalmente como PARCIAL, fundamentado no Modelo de Responsabilidade Compartilhada em Nuvem (AWS Shared Responsibility Model). Esse modelo delimita com clareza as responsabilidades entre o provedor de infraestrutura de nuvem e a organização prestadora do serviço.

Camada / Âmbito	**Entidade Responsável**	**Status de Certificação / Auditoria**	**Descrição do Escopo do Atendimento**
Segurança DA Nuvem (Infraestrutura, Data Centers, Hardware e Hipervisores)	Amazon Web Services (AWS)	Totalmente Certificado	Cobertura integral por auditorias independentes mundiais e relatórios atestando a segurança física e lógica da infraestrutura base.
Segurança NA Nuvem (Aplicação, Código-Fonte, Regras de Negócio e Gestão de Dados)	Organização (Desenvolvimento e Operação)	Controles Internos Aplicados	Segurança assegurada por meio de políticas e controles internos de governança (DevSecOps, testes automatizados, auditoria de código e gestão de acessos).

3. CERTIFICAÇÕES VIGENTES DA INFRAESTRUTURA (AWS)

A infraestrutura de nuvem subjacente onde os serviços são hospedados e processados (AWS) possui as seguintes certificações e relatórios de conformidade independentes em vigor:

- ISO/IEC 27001:2013 / 27001:2022: Sistema de Gestão de Segurança da Informação (SGSI);
- ISO/IEC 27017:2015: Código de Prática para Controles de Segurança da Informação para Serviços em Nuvem;
- ISO/IEC 27018:2019: Código de Prática para Proteção de Dados Pessoais Identificáveis (PII) em Nuvens Públicas;
- SOC 1, SOC 2 (Type II) e SOC 3: Relatórios de auditoria independente cobrindo os critérios de Segurança, Disponibilidade, Integridade de Processamento, Confidencialidade e Privacidade;
- PCI-DSS Level 1: Padrão de Segurança de Dados do Setor de Cartões de Pagamento (camada de infraestrutura).

Nota: Cópias formais e vigentes dos certificados e relatórios SOC podem ser fornecidas ou validadas diretamente por meio do portal oficial AWS Artifact.

4. CONTROLES DE SEGURANÇA DA CAMADA DE APLICAÇÃO

Para garantir que a camada sob responsabilidade da organização permaneça alinhada às exigências da ISO 27001 e às boas práticas do mercado, adotam-se os seguintes controles de segurança complementares:

- Gestão de Alterações e Código: Versionamento em repositórios privados no GitHub com ramificações segregadas, aprovação por pares (Peer Review) e esteiras automatizadas de integração e entrega (CI/CD);
- Controle de Acessos e Identidade: Uso obrigatório de Autenticação Multi-Fator (MFA) e políticas do menor privilégio para todos os acessos administrativos;
- Continuidade e Recuperação: Plano formal de Recuperação de Desastres (DRP) com rotinas diárias de backup criptografado em repouso e em trânsito.

Revisão #2
Criado 2026-09-04 14:18:25 UTC por Marcio Klitzke
Atualizado: 2026-09-04 17:52:41 UTC por Marcio Klitzke