Resumo de Segurança

Última atualização: 22 out 2025
Contato do DPO: security@alignio.tech

1. Escopo & Modelo de Operação

O que fazemos: Operamos o **financeiro**, **contabilidade** e **report ao investidor** de startups; padronizamos rotinas e KPIs, entregamos **Startup View** & **Investor View** no **AWS QuickSight** e estruturamos o Deal Room no **Investory**.

Papéis (LGPD):

- **Website e pré-venda: Controlador**.
- **Entrega dos serviços (Foundry/Operação):** atuamos **principalmente como Operador**, processando dados **por conta e sob instruções** do cliente (Controlador).
- **Sem software proprietário:** usamos **stack de terceiros auditáveis** (Omie, Thomson Reuters, AWS Quicksight e Investory).

2. Princípios de Proteção de Dados

Minimização e finalidade: coletamos e tratamos **apenas o necessário** para executar as rotinas contratadas.

Segregação por cliente: nenhum dado é cruzado entre clientes; datasets, credenciais e acessos são **isolados logicamente**.

"Mesmo número, menos ruído": o **IRA by alignio** evita múltiplas versões de planilhas; todo número tem **rastro de origem**.

3. Controles Técnicos (núcleo)

Criptografia

- **Em trânsito:** TLS 1.2+ nos canais sob nossa gestão e nos provedores.
- **Em repouso:** criptografia nativa dos provedores.

Gestão de acesso: RBAC e **princípio do menor privilégio**; **MFA** obrigatória em contas internas; **SSO** (SAML/OIDC) quando disponível.

Logs & trilhas: registros de acesso/alteração em provedores (ex.: AWS QuickSight, Omie) e nos fluxos operacionais; **auditoria rastreável**.

Segredos & credenciais: cofre de segredos, rotação periódica e acesso **just-in-time** quando aplicável.

Backups & restauração: backups fornecidos pelos provedores + políticas de retenção do cliente; **testes periódicos de restauração** documentados.

4. Controles Organizacionais

Governança: política de segurança, classificação de dados, gestão de riscos e **comitê de incidentes**.

Treinamento: segurança e privacidade no onboarding e reciclagens.

Due diligence de terceiros: avaliação de risco e **DPA** com subprocessadores; revisão contínua.

SLA operacional: calendário de **fechamento com prazos** e responsabilidades explícitas reduz falhas humanas e retrabalho.

5. Subprocessadores (serviços centrais)

- **Omie** — BPO financeiro (emissão, contas, conciliação).
- **Thomson Reuters** — contabilidade/fiscal.
- **AWS QuickSight** — armazenamento/visualização e reporting.
- **Investory** — armazenamento/visualização e reporting.

Ferramentas de site/analytics e agendamento aparecem separadamente na Política de Privacidade/Cookie Policy.

6. Retenção, Exclusão & Portabilidade

Retenção: conforme contrato, obrigações legais e necessidade operacional.

Exclusão/anonimização: ao término do contrato ou por solicitação do Controlador, seguindo os prazos legais aplicáveis.

Portabilidade: suporte ao Controlador para **exportar dados** em formatos estruturados.

7. Direitos do Titular (LGPD)

Apoiamos o **Controlador** no atendimento a solicitações de **acesso, correção, eliminação, portabilidade, informação sobre compartilhamento, revogação de consentimento** e **oposição**, conforme a LGPD.

8. Incidentes & Notificações

Resposta a incidentes: detecção, contenção, erradicação e lições aprendidas.

Notificação: comunicamos o **Controlador** sem atrasos injustificados; quando aplicável, o Controlador decide sobre comunicação a **ANPD** e titulares.

Forense: preservação de evidências e cronologia do evento; análise de causa raiz.

9. Continuidade & Resiliência

Planejamento: avaliação de impacto (BIA) dos processos críticos (fechamento, conciliação, reporting).

RTO/RPO: definidos contratualmente conforme estágio/escopo do cliente; testes em cenários de indisponibilidade de provedores.

Operação sem lock-in: como usamos stack de terceiros, migrações podem ser orquestradas com **baixo atrito**.

10. Conformidade & Documentos

- **LGPD** e boas práticas de proteção de dados.
- **DPA (Data Processing Addendum)**: define instruções, bases legais, subprocessadores, prazos e segurança.
- **Inventário de Cookies** e **Política de Privacidade** (site).
- **Lista atualizada de subprocessadores** e histórico de mudanças no Trust Center.

Compromissos-Chave (resumo executivo)

- **Dados segregados por cliente** e **governança de acesso** (RBAC/MFA/SSO).
- **Criptografia em trânsito e repouso** nos provedores.
- **Trilha de auditoria** ponta a ponta (do lançamento ao dashboard).
- **Backups e restauração testados** + **processo de resposta a incidentes**.
- **DPA contratual** e transparência de subprocessadores no Trust Center.

DPO | alignio — security@alignio.tech