AEXION

SEGURANÇA

Plano de Resposta a Incidentes de Segurança

PRI — LGPD Art. 48

DECISÕES INVISÍVEIS, RESULTADOS REAIS

aexion.com.br · uma plataforma aM Soluções

Plano de Resposta a Incidentes de Segurança

AEXION

S E G U R A N Ç A

Plano de Resposta a Incidentes de Segurança PRI — LGPD Art. 48 Documento elaborado pela AM Soluções Estratégicas LTDA, controladora da plataforma AEXION Finanças, em conformidade com o Art. 48 da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018). u 10 SEÇÕES u DETECÇÃO · CONTENÇÃO · NOTIFICAÇÃO · RECUPERAÇÃO u AEXION (cid:127) Espelho financeiro de PF e PJ AEXIONfinanceiro.com fi

AEXION

PRI — LGPD Art. 48 AEXIONfinanceiro.com Sumário u u u 01 Objetivo e Escopo 02 Definições 03 Equipe de Resposta a Incidentes 04 Classificação de Incidentes 05 Fluxo de Resposta 06 Notificação à ANPD 07 Comunicação aos Titulares 08 Modelos de Comunicação 09 Contatos de Emergência 10 Pós-Incidente e Lições Aprendidas AEXION (cid:127) PRI LGPD Art. 48 (cid:127) Confidencial Página 2 AEXIONfinanceiro.com

AEXION

PRI — LGPD Art. 48 AEXIONfinanceiro.com 01 SEÇÃO Objetivo e Escopo Por que esse plano existe e quando ele se aplica. Este Plano de Resposta a Incidentes de Segurança da Informação (PRI) estabelece o conjunto de procedimentos a serem adotados pela AM Soluções Estratégicas LTDA em caso de ocorrência de incidente de segurança envolvendo dados pessoais tratados na plataforma AEXION Finanças, em conformidade com o Art. 48 da Lei nº 13.709/2018 (LGPD). Objetivo: garantir que a empresa esteja preparada pra detectar, conter, mitigar, comunicar e aprender com qualquer incidente de segurança que possa expor dados pessoais de seus titulares — clientes pessoa física e pessoa jurídica. Escopo: aplica-se a TODOS os ambientes operados pela controladora — produção (Vercel + Supabase), repositórios de código (GitHub), infraestrutura de borda (Cloudflare), serviços de email (Resend, Hostinger), provedores integrados (Anthropic, Pluggy, Asaas, Hotmart) — bem como aos colaboradores, prestadores de serviço e quaisquer terceiros que tenham acesso a dados pessoais. “Art. 48 LGPD — O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.” AEXION (cid:127) PRI LGPD Art. 48 (cid:127) Confidencial Página 3 AEXIONfinanceiro.com

AEXION

PRI — LGPD Art. 48 AEXIONfinanceiro.com 02 SEÇÃO Definições Conceitos-chave usados ao longo deste plano. Incidente de segurança: qualquer evento confirmado ou suspeito que comprometa a confidencialidade, integridade ou disponibilidade de dados pessoais. Vazamento de dados: incidente de segurança no qual há acesso, divulgação ou exfiltração não autorizados de dados pessoais. Risco ou dano relevante: incidente que possa resultar em discriminação, fraude

financeira, dano material ou moral aos titulares — caracterizando obrigatoriedade de notificação à ANPD e aos titulares afetados. Dado sensível: conforme Art. 5º, II da LGPD — origem racial, convicção religiosa, opinião política, dados genéticos ou biométricos, dados referentes à saúde ou à vida sexual. Equipe de Resposta a Incidentes (ERI): grupo formal designado para coordenar a resposta — composto pela DPO, equipe técnica e responsável pela comunicação. RPO (Recovery Point Objective): tempo máximo de perda de dados aceitável. RTO (Recovery Time Objective): tempo máximo de indisponibilidade aceitável. Ambos definidos por categoria de dado. AEXION (cid:127) PRI LGPD Art. 48 (cid:127) Confidencial Página 4 AEXIONfinanceiro.com

AEXION

PRI — LGPD Art. 48 AEXIONfinanceiro.com 03 SEÇÃO Equipe de Resposta a Incidentes Quem faz o quê quando o alarme dispara. A Equipe de Resposta a Incidentes (ERI) da AEXION Finanças é estruturada da seguinte forma: u DPO — Encarregada de Proteção de Dados Aline Morellis de Quadros — sócia-administradora e Encarregada formal indicada por Ato de Indicação datado de abril/2026. Coordena toda a resposta. Responsável por: (i) classificar a gravidade do incidente; (ii) decidir se é caso de notificação à ANPD e aos titulares; (iii) ser o ponto de contato oficial com a autoridade; (iv) aprovar comunicações públicas. Email: dpo@AEXIONfinanceiro.com. u Coordenação Técnica Equipe técnica (Aline e/ou Victor) — responsável por: (i) detecção e diagnóstico; (ii) contenção (isolamento, revogação de credenciais, bloqueio de IPs); (iii) investigação forense (logs, audit_log, traces); (iv) restauração (restore Supabase PITR, deploy rollback Vercel); (v) implementação de medidas pós-incidente. u Comunicação Aline (DPO) assume a comunicação externa. Em incidentes de alta visibilidade, contratar provisoriamente assessoria jurídica especializada em LGPD (sugestão: escritório com prática em direito digital). Email institucional pra resposta: contato@AEXIONfinanceiro.com. u Auxílio externo (sob demanda) Suporte de operadores em caso de incidente que envolva o subsistema deles: Anthropic (security@anthropic.com), Pluggy (suporte@pluggy.ai), Vercel (security.vercel.com), Supabase (security@supabase.io), Cloudflare (abuse@cloudflare.com), Resend (security@resend.com). AEXION (cid:127) PRI LGPD Art. 48 (cid:127) Confidencial Página 5 AEXIONfinanceiro.com

AEXION

PRI — LGPD Art. 48 AEXIONfinanceiro.com 04 SEÇÃO Classificação de Incidentes Como medir a gravidade pra acionar a resposta certa. Cada incidente é classificado em três níveis de severidade que determinam o tempo de resposta, o nível de escalonamento e a obrigatoriedade de notificação. u n Severidade ALTA — Crítico Vazamento de dados sensíveis · acesso não autorizado a dados financeiros · comprometimento de credenciais administrativas · indisponibilidade total da plataforma > 4 horas · ransomware · exfiltração massiva de dados (>1.000 titulares). Notificação obrigatória à ANPD em até 2 dias úteis. Tempo de resposta inicial: imediato (até 1 hora). u n Severidade MÉDIA — Relevante Acesso não autorizado a dados não sensíveis · falha de configuração que expôs dados a ambiente público · phishing direcionado bem-sucedido · ataque DDoS de média intensidade · indisponibilidade parcial 1-4 horas. Avaliação caso-a-caso pra notificação à ANPD. Tempo de resposta: até 4 horas. u n Severidade BAIXA — Operacional Tentativas de login bloqueadas pelo Cloudflare Rate Limit · phishing genérico não-direcionado · vulnerabilidade em dependência sem exploração ativa · indisponibilidade < 1 hora. Sem obrigatoriedade de notificação. Tempo de resposta: até 24 horas. Registro em audit_log obrigatório pra histórico. AEXION (cid:127) PRI LGPD

Art. 48 (cid:127) Confidencial Página 6 AEXIONfinanceiro.com

AEXION

PRI — LGPD Art. 48 AEXIONfinanceiro.com 05 SEÇÃO Fluxo de Resposta Os 6 passos que sempre acontecem nessa ordem. u Etapa 1 — Detecção Fontes de detecção: (i) alertas automáticos do BetterStack (Status Page), Cloudflare WAF, error_log Supabase; (ii) reports de clientes via dpo@/suporte@; (iii) descobertas durante revisões internas; (iv) divulgação por terceiros (operadores, pesquisadores). DPO é notificada IMEDIATAMENTE por qualquer canal. u Etapa 2 — Contenção Ações imediatas pra IMPEDIR PIORA: (i) revogar tokens/sessões comprometidos (UPDATE auth_sessions SET revoked=true); (ii) rotacionar JWT_SECRET e env vars sensíveis; (iii) bloquear IPs no Cloudflare WAF; (iv) desativar endpoints comprometidos via Vercel; (v) snapshot Supabase PITR pra preservar evidência forense. u Etapa 3 — Investigação Apuração da causa raiz: (i) auditar audit_log Supabase (5 anos retenção); (ii) revisar logs Vercel + Cloudflare Analytics; (iii) revisar GitHub Audit Log; (iv) determinar quais titulares foram afetados, quais dados, por quanto tempo, qual operador envolvido; (v) registrar tudo em laudo formal. u Etapa 4 — Notificação à ANPD Se severidade ALTA ou risco relevante confirmado: DPO comunica via Sistema Eletrônico de Informações (SEI) da ANPD em até 2 dias úteis a contar do conhecimento do incidente. Conteúdo obrigatório do Art. 48 §1º — descrição, dados afetados, titulares envolvidos, medidas adotadas, riscos. u Etapa 5 — Comunicação aos Titulares Quando o risco aos titulares é relevante, comunicar individualmente por email no prazo determinado pela ANPD. Caso individual seja inviável, comunicação pública por meios proporcionais (banner no app, post na landing, email broadcast). u Etapa 6 — Recuperação e Pós-Incidente AEXION (cid:127) PRI LGPD Art. 48 (cid:127) Confidencial Página 7 AE

XIONfinanceiro.com

AEXION

PRI — LGPD Art. 48 AEXIONfinanceiro.com Restauração do serviço · validação de que a vulnerabilidade foi corrigida · análise de causa-raiz formal · atualização do PRI com lições aprendidas · revisão das medidas técnicas e organizacionais (RIPD pode precisar atualização). AEXION (cid:127) PRI LGPD Art. 48 (cid:127) Confidencial Página 8 AEXIONfinanceiro.com

AEXION

PRI — LGPD Art. 48 AEXIONfinanceiro.com 06 SEÇÃO Notificação à ANPD Conteúdo obrigatório, prazo e canal oficial. Conforme Art. 48 §1º da LGPD, a comunicação à ANPD deve conter: (cid:127) Descrição da natureza dos dados pessoais afetados; (cid:127) Informações sobre os titulares envolvidos (quantidade aproximada, perfil); (cid:127) Indicação das medidas técnicas e de segurança utilizadas para proteção dos dados, observados os segredos comercial e industrial; (cid:127) Riscos relacionados ao incidente; (cid:127) Motivos da demora, no caso de a comunicação não ter sido imediata; (cid:127) Medidas que foram ou serão adotadas para reverter ou mitigar os efeitos do prejuízo. u Canal oficial — SEI da ANPD Toda comunicação à ANPD é feita via Sistema Eletrônico de Informações (SEI) — sei.anpd.gov.br. A AM Soluções precisa estar previamente cadastrada como Usuário Externo (P0.1 do roadmap interno). O processo eletrônico é registrado e fica disponível pra consulta posterior. u Prazo legal Até 2 dias úteis a contar do conhecimento do

incidente, conforme prazo recomendado pela ANPD. A demora deve ser justificada documentalmente. AEXION (cid:127) PRI LGPD Art. 48 (cid:127) Confidencial Página 9 AEXIONfinanceiro.com

AEXION

PRI — LGPD Art. 48 AEXIONfinanceiro.com 07 SEÇÃO Comunicação aos Titulares Como avisar quem foi afetado. A comunicação aos titulares acontece após a notificação à ANPD ou simultaneamente, dependendo da orientação da autoridade. Linguagem clara, sem juridiquês, em português acessível. u Conteúdo da comunicação A comunicação deve informar (i) o que aconteceu em linguagem simples; (ii) quais dados foram afetados; (iii) quais riscos isso pode trazer; (iv) quais medidas a empresa tomou; (v) quais ações o titular pode tomar (trocar senha, monitorar conta bancária, etc.); (vi) canal de contato pra dúvidas. u Canal de envio Email transacional via Resend (mesma infra usada para emails do produto). Em incidentes que afetem >100 titulares, considerar comunicado público adicional na landing. AEXION (cid:127) PRI LGPD Art. 48 (cid:127) Confidencial Página 10 AEXIONfinanceiro.com

AEXION

PRI — LGPD Art. 48 AEXIONfinanceiro.com 08 SEÇÃO Modelos de Comunicação Templates prontos pra usar no momento crítico. u Modelo 01 — Notificação à ANPD (preencher e enviar via SEI) “À Autoridade Nacional de Proteção de Dados — ANPD. Em cumprimento ao Art. 48 da Lei nº 13.709/2018, a AM Soluções Estratégicas LTDA, controladora da plataforma AEXION Finanças, comunica a ocorrência de incidente de segurança em [DATA] envolvendo [QTD] titulares. Natureza dos dados afetados: [DESCRIÇÃO]. Medidas técnicas em vigor: [LISTAR]. Medidas mitigadoras adotadas: [LISTAR]. Riscos identificados: [DESCRIÇÃO]. Aline Morellis de Quadros — DPO — dpo@AEXIONfinanceiro.com.” u Modelo 02 — Email aos Titulares Afetados “Olá, [NOME]. Estamos te escrevendo pra informar que identificamos um incidente de segurança em [DATA] que afetou seus dados na plataforma AEXION Finanças. Os dados afetados foram: [LISTAR]. Já tomamos as seguintes medidas: [LISTAR]. Te recomendamos: trocar sua senha agora; ativar 2FA; ficar atento a tentativas de phishing; monitorar movimentações financeiras. Se tiver dúvidas, responda este email ou escreva pra dpo@AEXIONfinanceiro.com. Lamentamos sinceramente o ocorrido.” u Modelo 03 — Comunicado Público (landing + status page) “Em [DATA] identificamos um incidente de segurança em nossa plataforma. Tomamos as seguintes medidas imediatas: [LISTAR]. Os clientes afetados foram comunicados individualmente. A ANPD foi informada conforme Art. 48 da LGPD. Pra dúvidas, escreva pra dpo@AEXIONfinanceiro.com. Continuaremos atualizando esta página conforme novas informações estiverem disponíveis.” AEXION (cid:127) PRI LGPD Art. 48 (cid:127) Confidencial Página 11 AEXIONfinanceiro.com

AEXION

PRI — LGPD Art. 48 AEXIONfinanceiro.com AEXION (cid:127) PRI LGPD Art. 48 (cid:127) Confidencial Página 12 AEXIONfinanceiro.com

AEXION

PRI — LGPD Art. 48 AEXIONfinanceiro.com 09 SEÇÃO Contatos de Emergência Quem ligar e em que ordem. u Internos DPO — Aline Morellis de Quadros — dpo@AEXIONfinanceiro.com — celular pessoal (uso restrito ERI) Coordenação Técnica — Aline + Victor — contato@amsolucoesestrategicas.com u Operadores (security contacts) Anthropic (Claude IA) — security@anthropic.com Pluggy (Open Finance) — suporte@pluggy.ai Vercel (hosting) — security.vercel.com Supabase (banco) — security@supabase.io Cloudflare (edge/CDN) — abuse@cloudflare.com Resend (email) — security@resend.com Hostinger (email corporativo) — abuse@hostinger.com u Autoridades ANPD — sei.anpd.gov.br (canal oficial via Sistema Eletrônico de Informações) Polícia Civil — em caso de crime cibernético — registrar BO online no estado da Aline (RS) u Suporte jurídico Contratar sob demanda escritório com prática em LGPD (sugestão: avaliar 2-3 escritórios em Porto Alegre/RS antes do primeiro incidente — manter contato pré-aprovado). AEXION (cid:127) PRI LGPD Art. 48 (cid:127) Confidencial Página 13 AEXIONfinanceiro.com

AEXION

PRI — LGPD Art. 48 AEXIONfinanceiro.com 10 SEÇÃO Pós-Incidente e Lições Aprendidas Como transformar incidente em aprendizado permanente. Após cada incidente — independente da severidade — a DPO conduz uma revisão formal documentada em até 7 dias úteis após o encerramento do incidente. u Conteúdo do laudo pós-incidente (i) cronologia completa (detecção fi contenção fi resolução); (ii) análise de causa-raiz; (iii) impacto real (titulares, dados, financeiro, reputação); (iv) eficácia da resposta — o que funcionou, o que falhou; (v) ações corretivas planejadas com responsável e prazo; (vi) atualizações no PRI, RIPD, Política de Privacidade ou Termos de Uso, se necessário. u Frequência de revisão do PRI Revisão obrigatória do PRI: (i) após cada incidente de severidade ALTA; (ii) trimestralmente em rotina de auditoria interna; (iii) quando houver mudança significativa de tratamento (novo operador, novo dado coletado, mudança de infraestrutura). u Treinamento da equipe A DPO realiza simulação anual de incidente (tabletop exercise) com a equipe técnica pra testar o fluxo do PRI sem incidente real. Resultados documentados e usados pra atualizar o plano. AEXION (cid:127) PRI LGPD Art. 48 (cid:127) Confidencial Página 14 AEXIONfinanceiro.com

AEXION

PRI — LGPD Art. 48 AEXIONfinanceiro.com Aprovação Eu, Aline Morellis de Quadros, na qualidade de sócia-administradora da AM Soluções Estratégicas LTDA e Encarregada de Proteção de Dados (DPO) da plataforma AEXION Finanças, aprovo o presente Plano de Resposta a Incidentes de Segurança da Informação e me comprometo a coordenar sua aplicação em conformidade com o Art. 48 da Lei Geral de Proteção de Dados Pessoais. Passo Fundo - RS, _____ de _____ de 2026. _____ Aline Morellis de Quadros Sócia-administradora e DPO AM Soluções Estratégicas LTDA (cid:127) CNPJ 43.691.802/0001-06 AEXION (cid:127) PRI LGPD Art. 48 (cid:127) Confidencial Página 15 AEXIONfinanceiro.com