POLÍTICA DE REPORTE E GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO E ESCOPO

A presente Política de Reporte e Gestão de Incidentes de Segurança da Informação estabelece diretrizes, procedimentos e responsabilidades para identificação, comunicação, investigação, contenção e resposta a incidentes de segurança que possam afetar a confidencialidade, integridade, disponibilidade ou privacidade de dados pessoais tratados pela **Aizen Tecnologia Ltda**., sociedade empresária inscrita no CNPJ sob o nº 63.740.359/0001-15, com sede na Rua Henri Dunant, 792, Apt 2306, Santo Amaro, São Paulo/SP, CEP 04709-110 ("**Aizen**"), em cumprimento ao disposto no artigo 48 da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) e às melhores práticas de segurança da informação.

Esta política aplica-se a todos os colaboradores, prestadores de serviço, parceiros e terceiros que, em razão de suas atividades, tenham acesso a sistemas, dados ou informações da Aizen, estabelecendo procedimentos uniformes para tratamento de eventos que comprometam ou possam comprometer a segurança da informação e a proteção de dados pessoais de usuários da plataforma.

2. DEFINIÇÕES

Para fins desta política, considera-se incidente de segurança da informação qualquer evento confirmado ou suspeito que resulte em acesso não autorizado, alteração indevida, destruição, perda, vazamento, divulgação não autorizada ou qualquer outra forma de tratamento inadequado de dados pessoais ou informações sensíveis da Aizen, incluindo comprometimento de sistemas, infraestrutura tecnológica, redes ou processos que possam afetar a segurança de dados.

Incidente de segurança envolvendo dados pessoais, para efeitos da LGPD, caracteriza-se quando há comprometimento da segurança que possa acarretar risco ou dano relevante aos titulares de dados, especialmente situações que envolvam acesso não autorizado a dados financeiros, credenciais de acesso, informações bancárias ou qualquer dado que, se exposto, possa resultar em prejuízos financeiros, discriminação, danos à reputação ou outros impactos adversos significativos.

Vulnerabilidade consiste em fragilidade ou falha em sistema, processo, controle de segurança ou infraestrutura que possa ser explorada para causar incidente de segurança, mesmo que ainda não tenha resultado em comprometimento efetivo de dados. A identificação e correção tempestiva de vulnerabilidades constitui medida preventiva essencial para evitar incidentes.

3. CLASSIFICAÇÃO DE INCIDENTES

Os incidentes de segurança são classificados em níveis de severidade conforme o impacto potencial ou confirmado sobre dados pessoais, sistemas, operações e titulares de dados,

determinando os procedimentos de resposta, prazos de comunicação e nível de escalação apropriados.

Incidentes de severidade crítica são aqueles que envolvem acesso não autorizado, vazamento, perda ou exposição de grande volume de dados pessoais, especialmente dados financeiros ou bancários de usuários, comprometimento de sistemas essenciais da plataforma que impeçam ou limitem significativamente a prestação de serviços, ou qualquer situação que apresente alto risco de dano relevante aos titulares. Esses incidentes exigem resposta imediata, comunicação urgente à alta administração e possível notificação à Agência Nacional de Proteção de Dados (ANPD) e aos titulares afetados.

Incidentes de severidade alta caracterizam-se por acesso não autorizado a dados pessoais de número limitado de usuários, comprometimento de sistemas não essenciais, tentativas confirmadas de invasão ou ataque que tenham sido parcialmente bem-sucedidas, ou vulnerabilidades críticas descobertas que apresentem risco iminente mas ainda não explorado. Requerem investigação prioritária e comunicação à liderança de segurança e ao Encarregado de Proteção de Dados.

Incidentes de severidade média incluem tentativas fracassadas de acesso não autorizado, identificação de vulnerabilidades moderadas, comprometimento de dados não sensíveis ou internos que não afetem diretamente usuários, indisponibilidade temporária de funcionalidades não críticas ou eventos que não apresentem risco relevante aos titulares mas demandem correção. Devem ser documentados, investigados e tratados conforme cronograma definido pela equipe de segurança.

Incidentes de severidade baixa compreendem eventos de segurança com impacto mínimo ou inexistente, como tentativas de phishing bloqueadas automaticamente, varreduras de porta ou tentativas de acesso claramente automatizadas e sem sucesso, identificação de vulnerabilidades menores sem exploração conhecida, ou outras ocorrências que não representem risco material à segurança de dados ou sistemas. São registrados para fins estatísticos e monitoramento de tendências.

4. IDENTIFICAÇÃO E REPORTE INTERNO

Qualquer pessoa que identifique ou suspeite de incidente de segurança da informação possui o dever de reportá-lo imediatamente, independentemente de sua posição hierárquica, função ou vínculo com a Aizen. O reporte tempestivo constitui responsabilidade fundamental de todos que acessam sistemas ou dados da empresa, sendo a demora na comunicação considerada infração disciplinar grave quando resultar em agravamento do incidente ou impedimento de medidas de contenção eficazes.

O reporte de incidentes deve ser realizado prioritariamente ao superior imediato e simultaneamente ao Encarregado de Proteção de Dados por meio do endereço eletrônico dpo@bonuz.it, disponível permanentemente para recebimento de comunicações relacionadas a incidentes. Na impossibilidade de contato com o superior imediato ou em situações de urgência extrema, especialmente fora do horário comercial, o reporte pode ser feito diretamente ao Encarregado de Proteção de Dados ou à alta administração.

A comunicação de incidente deve conter, sempre que possível e conforme informações disponíveis no momento do reporte, descrição detalhada do evento observado ou

suspeito, data e horário aproximados de ocorrência ou identificação, sistemas, dados ou informações potencialmente afetados, evidências disponíveis (logs, capturas de tela, mensagens suspeitas), identificação de pessoas que possam ter conhecimento adicional sobre o incidente e quaisquer medidas preliminares já adotadas para contenção ou preservação de evidências.

A Aizen garante proteção contra retaliação a qualquer pessoa que, de boa-fé, reporte incidente de segurança, mesmo que a investigação posterior conclua pela inexistência de incidente real ou que o evento tenha decorrido de erro não intencional do próprio reportante. A cultura de transparência e reporte tempestivo é incentivada como elemento fundamental da postura de segurança da organização.

5; RESPOSTA E INVESTIGAÇÃO DE INCIDENTES

Ao receber comunicação de incidente, o Encarregado de Proteção de Dados realiza avaliação preliminar para classificar a severidade, determinar a necessidade de acionamento imediato da equipe de resposta a incidentes e definir o nível de escalação apropriado. Para incidentes críticos ou altos, o acionamento da equipe de resposta ocorre imediatamente, a qualquer hora do dia ou da noite, enquanto incidentes médios e baixos podem ser endereçados durante horário comercial conforme cronograma de prioridades.

A equipe de resposta a incidentes, coordenada pelo Encarregado de Proteção de Dados e composta por profissionais de tecnologia da informação, segurança da informação, jurídico e outras áreas conforme necessário, conduz investigação técnica para determinar a extensão do comprometimento, identificar dados ou sistemas afetados, compreender o vetor de ataque ou causa raiz, identificar vulnerabilidades exploradas e avaliar riscos aos titulares de dados. A investigação segue metodologia estruturada que preserva evidências, documenta todas as descobertas e mantém cadeia de custódia adequada para eventual utilização em processos administrativos ou judiciais.

Simultaneamente à investigação, são implementadas medidas imediatas de contenção destinadas a interromper o incidente em curso, prevenir propagação para outros sistemas ou dados, proteger evidências contra destruição ou adulteração e mitigar riscos aos titulares. Medidas de contenção podem incluir isolamento de sistemas comprometidos, bloqueio de contas de usuário suspeitas, revogação de credenciais de acesso, implementação de regras de firewall adicionais, desativação temporária de funcionalidades ou serviços afetados e outras ações tecnicamente apropriadas conforme natureza do incidente.

Após contenção do incidente, procede-se à erradicação da causa raiz, eliminando malware, fechando vulnerabilidades exploradas, revogando acessos indevidos e implementando correções necessárias para prevenir recorrência. A fase de recuperação restabelece sistemas e serviços ao estado normal de operação, restaura dados de backups quando necessário, valida integridade de sistemas recuperados e monitora atividades para garantir que o incidente foi completamente eliminado.

6. COMUNICAÇÃO EXTERNA E NOTIFICAÇÕES

Incidentes de segurança que acarretem risco ou dano relevante aos titulares de dados pessoais exigem comunicação à Autoridade Nacional de Proteção de Dados em prazo razoável, conforme determinado pelo artigo 48 da LGPD. A decisão sobre necessidade de comunicação à ANPD compete ao Encarregado de Proteção de Dados, com suporte jurídico e técnico, baseando-se em avaliação criteriosa do risco ou dano potencial aos titulares, considerando volume de dados afetados, sensibilidade das informações comprometidas, probabilidade de uso indevido dos dados, eficácia de medidas de segurança implementadas (como criptografia forte) e outros fatores relevantes.

A comunicação à ANPD contém, no mínimo, descrição da natureza dos dados pessoais afetados, informações sobre os titulares envolvidos (quantidade e categorias de titulares, sem identificação individual), indicação das medidas técnicas e de segurança utilizadas para proteção dos dados (incluindo criptografia, controles de acesso, logs de auditoria), descrição dos riscos relacionados ao incidente, motivação da eventual demora na comunicação caso não tenha sido possível comunicar imediatamente, e descrição detalhada das medidas adotadas para reverter ou mitigar efeitos do prejuízo causado ou potencial.

Paralelamente à comunicação à ANPD, quando aplicável, a Aizen comunica diretamente os titulares afetados pelo incidente, informando-os em linguagem clara e acessível sobre a natureza do incidente, os dados potencialmente comprometidos, as medidas que a Aizen está adotando para remediar a situação e investigar o ocorrido, as recomendações sobre ações que os titulares podem tomar para se proteger contra eventuais consequências adversas (como alteração de senhas, monitoramento de extratos bancários, ativação de alertas de crédito) e os canais de contato disponíveis para esclarecimentos adicionais.

A comunicação aos titulares é realizada por meio dos canais de contato cadastrados (preferencialmente correio eletrônico e notificação dentro da plataforma), sendo priorizadas formas diretas e pessoais de comunicação em detrimento de avisos genéricos. Em situações excepcionais onde comunicação individual seja impossível ou exija esforços desproporcionais, considerando-se o grande número de titulares afetados, a comunicação pode ser realizada por meio público de informação equivalente, como publicação em website com ampla divulgação.

7. DOCUMENTAÇÃO E REGISTRO

Todos os incidentes de segurança, independentemente de severidade, são registrados em sistema dedicado de gestão de incidentes que mantém histórico completo e rastreável de eventos, investigações, medidas adotadas e lições aprendidas. O registro de incidentes constitui importante fonte de informações para análise de tendências, identificação de vulnerabilidades recorrentes, avaliação da eficácia de controles de segurança e demonstração de conformidade regulatória perante autoridades competentes.

Para cada incidente, a documentação inclui identificação única do incidente, data e horário de ocorrência e de identificação, classificação de severidade, descrição detalhada do evento, sistemas e dados afetados, cronologia de ações tomadas desde a identificação até a resolução completa, evidências coletadas e preservadas, análise de causa raiz, impacto

estimado aos titulares e à organização, comunicações realizadas (internas e externas), medidas corretivas implementadas e recomendações para prevenção de incidentes similares.

Os registros de incidentes são preservados pelo prazo mínimo de cinco anos, podendo ser mantidos por período superior quando necessário para cumprimento de obrigações regulatórias específicas, defesa de direitos em processos judiciais ou administrativos, ou para fins de análise histórica de segurança. O acesso aos registros de incidentes é restrito ao Encarregado de Proteção de Dados, equipe de segurança da informação, alta administração e auditores internos ou externos devidamente autorizados, sendo vedada divulgação não autorizada de informações contidas nos registros.

8. ANÁLISE PÓS-INCIDENTE E MELHORIA CONTÍNUA

Após resolução de cada incidente classificado como médio, alto ou crítico, a equipe de resposta conduz reunião de análise pós-incidente destinada a revisar a eficácia da resposta, identificar falhas ou lacunas em processos, controles ou treinamentos, documentar lições aprendidas e propor melhorias nos procedimentos de segurança, prevenção ou resposta a incidentes. A análise pós-incidente examina tanto aspectos técnicos quanto processuais, incluindo tempestividade de identificação e reporte, adequação das medidas de contenção, eficácia da comunicação interna e externa, e suficiência dos controles preventivos existentes.

As recomendações resultantes da análise pós-incidente são formalizadas em plano de ação com responsáveis designados, prazos definidos e mecanismos de acompanhamento periódico. A implementação de melhorias identificadas possui prioridade elevada no planejamento de segurança da informação, sendo monitorada pelo Encarregado de Proteção de Dados e pela alta administração. Recomendações não implementadas dentro dos prazos estabelecidos devem ser formalmente justificadas com análise de riscos de aceitação.

Trimestralmente, o Encarregado de Proteção de Dados apresenta à alta administração relatório consolidado de incidentes de segurança ocorridos no período, incluindo estatísticas de incidentes por severidade e categoria, análise de tendências, status de implementação de melhorias recomendadas, avaliação da maturidade dos processos de resposta a incidentes e recomendações estratégicas para fortalecimento da postura de segurança organizacional.

9. TREINAMENTO E CONSCIENTIZAÇÃO

A Aizen conduz programa contínuo de treinamento e conscientização sobre segurança da informação e proteção de dados dirigido a todos os colaboradores, incluindo módulo específico sobre identificação e reporte de incidentes de segurança. O treinamento cobre tipologia de incidentes mais comuns (phishing, malware, acesso não autorizado, vazamentos acidentais), sinais de alerta que podem indicar comprometimento de segurança, procedimentos corretos de reporte, importância da tempestividade na comunicação e responsabilidades individuais na proteção de dados.

Novos colaboradores recebem treinamento sobre esta política como parte do processo de integração, antes de receberem acessos a sistemas ou dados sensíveis. Reciclagens anuais são realizadas para toda a organização, sendo atualizadas conforme evolução de ameaças, ocorrência de incidentes relevantes ou alterações nos procedimentos de resposta. A participação nos treinamentos é obrigatória e monitorada, sendo considerada requisito para manutenção de acessos a sistemas críticos.

10. RESPONSABILIDADES

O Encarregado de Proteção de Dados é responsável pela coordenação geral do processo de gestão de incidentes, incluindo classificação de severidade, acionamento da equipe de resposta, supervisão de investigações, decisão sobre comunicações externas à ANPD e titulares, manutenção de registros de incidentes e reporte à alta administração. Atua como ponto focal para comunicações relacionadas a incidentes tanto internamente quanto com autoridades e titulares.

A equipe de tecnologia da informação e segurança da informação é responsável pela resposta técnica a incidentes, incluindo investigação forense, implementação de medidas de contenção e erradicação, recuperação de sistemas, correção de vulnerabilidades e implementação de melhorias técnicas recomendadas. Colabora estreitamente com o Encarregado de Proteção de Dados fornecendo informações técnicas necessárias para avaliação de impacto e decisões sobre comunicações.

A alta administração é responsável por prover recursos adequados para implementação desta política, aprovar decisões estratégicas relacionadas a incidentes de alto impacto, supervisionar a eficácia do programa de gestão de incidentes e garantir cultura organizacional que valorize segurança da informação e reporte transparente de incidentes. Todos os colaboradores e prestadores de serviço são responsáveis por conhecer esta política, reportar prontamente incidentes identificados e cooperar com investigações quando solicitados.

11. DISPOSIÇÕES FINAIS

Esta política é revisada anualmente ou sempre que mudanças significativas na regulamentação, infraestrutura tecnológica, modelo de negócio ou ambiente de ameaças justifiquem atualização. Alterações substanciais são comunicadas a todos os colaboradores e terceiros relevantes, sendo promovidos treinamentos adicionais quando necessário para garantir compreensão das modificações.

O descumprimento desta política constitui infração disciplinar sujeita a medidas que podem incluir advertência, suspensão, rescisão contratual ou revogação de acessos, conforme gravidade da infração, sem prejuízo a eventuais responsabilidades civis e criminais decorrentes de condutas ilícitas. A avaliação de infrações considera tanto a materialidade do descumprimento quanto a boa-fé ou má-fé do infrator, sendo a recusa intencional em reportar incidente ou a tentativa de ocultação consideradas infrações de máxima gravidade.