POLÍTICA DE GERENCIAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E DADOS PESSOAIS

Agente de Tratamento	Alphavia Transportes e Máquinas Ltda
Encarregado pelo Tratamento de Dados (DPO)	Harlei Ribeiro Miranda
Base normativa	Lei nº 13.709/2018 (LGPD), com ênfase no Capítulo VII, arts. 46, 48 e 50.
Finalidade	Estabelecer diretrizes, responsabilidades e procedimentos para prevenção, tratamento, comunicação e melhoria contínua relacionados a incidentes de segurança da informação e dados pessoais.
Natureza	Política corporativa de observância obrigatória por colaboradores, terceiros, prestadores de serviço e gestores.
Versão	1.0
Vigência	Imediata, após aprovação interna pela Alta Administração.

Documento técnico-jurídico voltado à governança, prevenção, resposta e comunicação de incidentes com potencial impacto à confidencialidade, integridade, disponibilidade e privacidade.

1. Objetivo, Escopo e Fundamentos

1.1. Esta Política de Gerenciamento de Incidentes de Segurança da Informação e Dados Pessoais estabelece diretrizes de prevenção, detecção, resposta, comunicação, recuperação e melhoria contínua aplicáveis a incidentes que possam comprometer a confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade de informações e dados pessoais tratados pela organização.

1.2. O documento observa, em especial, o Capítulo VII da Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), com ênfase no art. 46, relativo à adoção de medidas técnicas e administrativas aptas a proteger dados pessoais, no art. 48, relativo à comunicação de incidentes de segurança, e no art. 50, relativo à adoção de regras de boas práticas e governança.

1.3. O escopo desta política abrange todos os processos, sistemas, bases de dados, documentos físicos, serviços em nuvem, ativos tecnológicos, terceiros, operadores e ambientes corporativos que realizem tratamento de dados pessoais ou suportem operações críticas de negócio.

2. Diretrizes Gerais de Governança e Boas Práticas

2.1. A gestão de incidentes deve integrar o programa de governança em privacidade e segurança da informação, observando princípios de prevenção, responsabilização e prestação de contas, necessidade, minimização de impacto, tempestividade na resposta, documentação das decisões e melhoria contínua.

- manutenção de papéis e responsabilidades formalmente definidos para resposta a incidentes;
- registro centralizado de eventos, alertas, quase-incidentes e incidentes efetivos;
- integração entre Segurança da Informação, Privacidade, Jurídico, áreas de negócio, Comunicação e Alta Administração;
- capacitação periódica dos colaboradores e terceiros com acesso a dados pessoais e ativos críticos;
- revisão periódica dos controles técnicos e administrativos, com testes, exercícios simulados e lições aprendidas.

2.2. Comitê de Resposta a Incidentes (CRI)

Fica instituído o Comitê de Resposta a Incidentes – CRI, instância multidisciplinar responsável por coordenar o tratamento de incidentes relevantes e deliberar sobre medidas emergenciais, comunicação institucional e ações corretivas. O CRI poderá ser permanente ou convocado ad hoc, conforme a gravidade do caso.

- DPO / Encarregado pelo Tratamento de Dados Pessoais;
- Responsável por Segurança da Informação ou equipe equivalente;
- Representante do Jurídico/Compliance;
- Gestor da área afetada;
- Representante de Comunicação/Relacionamento, quando necessário;
- Membro da Alta Administração, nos incidentes de maior criticidade.

2.3. O CRI deverá manter fluxo formal de comunicação, matriz de escalonamento, critérios de classificação, atas ou registros decisórios, trilha de auditoria das deliberações e reporte executivo compatível com a materialidade do incidente.

3. Medidas Técnicas e Administrativas de Prevenção, Detecção e Mitigação

3.1. Em observância ao art. 46 da LGPD, a organização deve implementar e manter controles proporcionais à natureza das operações de tratamento, à sensibilidade dos dados, ao contexto do tratamento, ao estado da técnica e aos riscos identificados aos titulares de dados e ao negócio.

- controle de acesso baseado em necessidade de conhecimento e segregação de funções;
- gestão de identidades, credenciais, autenticação forte e revisão periódica de privilégios;
- proteção de endpoints, redes, backups, ambientes em nuvem e dispositivos móveis;
- registro e monitoramento de logs relevantes, com retenção compatível e rastreabilidade;
- gestão de vulnerabilidades, atualizações, correções de segurança e hardening;
- criptografia, pseudonimização, mascaramento ou técnicas equivalentes quando cabíveis;
- planos de continuidade de negócios, redundância e recuperação de desastres;
- cláusulas contratuais com operadores e fornecedores, incluindo cooperação em incidentes e reporte tempestivo;
- treinamento e conscientização periódicos sobre phishing, engenharia social, privacidade e resposta a incidentes.

3.2. A área de Segurança da Informação deverá manter mecanismos de detecção e correlação de eventos, priorizando alertas relacionados a acesso indevido, exfiltração de dados, indisponibilidade relevante, malware, ransomware, falhas de configuração, uso indevido de credenciais e violações em ambientes terceirizados.

4. Fluxo de Resposta a Incidentes

4.1. Todo incidente ou suspeita de incidente deve ser imediatamente registrado e encaminhado ao fluxo corporativo de resposta, vedada a omissão, supressão de evidências ou tratamento informal fora dos canais institucionais.

4.2. Identificação e Classificação

A triagem inicial deverá verificar, no mínimo, a natureza do evento, ativos e processos afetados, categoria de dados envolvidos, volume estimado, quantidade de titulares potencialmente impactados, tempo de exposição, origem provável, existência de indícios de acesso indevido, impacto operacional, impacto reputacional e potencial risco ou dano relevante aos titulares.

Tabela 1 – Critérios mínimos de classificação do incidente

Nível	Critérios exemplificativos	Prazo interno de escalonamento	Atores mínimos envolvidos
Baixo risco	Evento sem evidência de vazamento ou indisponibilidade crítica; impacto limitado, reversível e sem dados sensíveis ou grande volume de titulares.	Até 4 horas úteis da identificação	Gestor da área, TI/SI e registro no sistema de incidentes.
Médio risco	Incidente com potencial de interrupção relevante, acesso indevido restrito, indícios de exposição moderada ou risco reputacional/operacional controlável.	Até 2 horas úteis da identificação	TI/SI, gestor da área, DPO/Privacidade e liderança responsável.
Alto risco	Incidente com alto potencial ou efetiva violação de dados pessoais, inclusive sensíveis, credenciais, grande volume de titulares, ransomware, indisponibilidade crítica ou risco substancial aos titulares.	Imediato, preferencialmente em até 1 hora	Comitê de Resposta a Incidentes, DPO, Jurídico, TI/SI, Comunicação e Alta Administração.

4.3. Contenção e Erradicação

Uma vez confirmada a materialidade do incidente, deverão ser adotadas medidas imediatas e proporcionais para limitar a propagação do evento, preservar evidências, reduzir danos e remover a causa raiz ou vetores de comprometimento, sem prejuízo da continuidade mínima dos serviços essenciais.

- isolamento de ativos, contas, credenciais, integrações ou segmentos de rede comprometidos;
- bloqueio de acessos indevidos, revogação de privilégios e rotação de senhas/chaves;
- aplicação de correções, restauração de configurações seguras e saneamento de artefatos maliciosos;
- coleta e preservação de evidências digitais, registros, imagens e logs para análise forense, quando pertinente;
- acionamento de fornecedores, operadoras, provedores de nuvem ou parceiros que detenham responsabilidade compartilhada.

4.4. Recuperação

A recuperação deverá observar critérios de segurança, integridade e validação antes do retorno à operação normal, de modo a evitar reincidência ou reintrodução da vulnerabilidade explorada. Backups, sistemas restaurados e fluxos de negócio deverão ser validados quanto à consistência e confiabilidade.

- restauração controlada de sistemas e dados a partir de cópias confiáveis;
- testes de integridade, disponibilidade e segurança antes da reabertura completa do ambiente;
- monitoramento reforçado após normalização, com período de observação compatível com a criticidade;
- registro formal da retomada, das restrições remanescentes e das aprovações necessárias.

5. Protocolo de Comunicação e Notificação

5.1. Nos termos do art. 48 da LGPD, a organização comunicará à Agência Nacional de Proteção de Dados (ANPD) e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. A decisão deverá ser motivada, documentada e baseada em análise de risco conduzida pelo DPO, pelo Jurídico e pelo CRI, sem prejuízo da autonomia decisória da Alta Administração quando necessária.

5.2. A comunicação externa deverá ocorrer sem atraso indevido e em prazo razoável, observando-se a legislação, a regulamentação vigente e o estágio de apuração do incidente, admitindo-se comunicação preliminar quando ainda houver elementos em investigação. Internamente, deverão ser observados prazos de escalonamento e decisão que viabilizem tempestividade, boa-fé, transparência e diligência demonstrável.

Tabela 2 – Protocolo de comunicação e notificação

Etapa	Prazo interno recomendado	Responsável primário	Saída mínima esperada
Registro inicial	Imediato	Qualquer colaborador / Service Desk / SI	Abertura do incidente, evidências iniciais e acionamento do fluxo.
Triagem e classificação	Até 24 horas	Segurança da Informação + gestor da área	Classificação preliminar, ativos afetados, hipótese de causa e risco aos titulares.

Etapa	Prazo interno recomendado	Responsável primário	Saída mínima esperada
Decisão sobre notificação externa	Até 48 horas da confirmação material do incidente	DPO + Jurídico + CRI	Parecer formal sobre necessidade, escopo e conteúdo da comunicação à ANPD e/ou titulares.
Comunicação à ANPD e titulares, quando cabível	Sem atraso indevido e em prazo razoável, observada a regulamentação aplicável	DPO / representante indicado	Notificação formal com os elementos mínimos exigidos pela LGPD e normas complementares.
Relatório de encerramento	Até 10 dias úteis após contenção	Líder do incidente / CRI	Relatório final, lições aprendidas, plano de ação e atualização do inventário de riscos.

5.3. Conteúdo mínimo da notificação

Sem prejuízo de exigências regulatórias supervenientes ou específicas, a notificação à ANPD e/ou aos titulares deverá contemplar, na medida do possível e de forma objetiva, os seguintes elementos:

- descrição da natureza do incidente e da data ou período aproximado de ocorrência e detecção;
- categoria e natureza dos dados pessoais afetados, incluindo menção a dados pessoais sensíveis, quando houver;
- quantitativo estimado de titulares envolvidos e, se possível, o universo de registros impactados;
- indicação das medidas técnicas e administrativas de segurança utilizadas para a proteção dos dados, observados segredos comercial e industrial;
- riscos relacionados ao incidente e potenciais impactos aos titulares;
- medidas de contenção, mitigação, erradicação e recuperação já adotadas ou planejadas;
- orientações práticas aos titulares para proteção de seus interesses, quando aplicável;
- canais de contato do DPO ou área responsável para esclarecimentos adicionais.

5.4. A Comunicação Institucional deverá ser acionada apenas mediante alinhamento com o DPO, Jurídico e Alta Administração, a fim de assegurar consistência factual, linguagem adequada, proteção reputacional legítima e observância do dever de transparência, sem omissão de informações materialmente relevantes.

6. Registros, Evidências e Responsabilização

6.1. Todos os incidentes, independentemente da classificação, deverão possuir registro formal contendo data/hora, origem da comunicação, descrição inicial, ativos afetados, avaliação preliminar, responsáveis, medidas adotadas, deliberações, evidências preservadas, cronologia de eventos e status de encerramento.

6.2. Os registros e relatórios produzidos no âmbito desta política devem ser armazenados de forma íntegra, acessível e auditável pelo período definido nas normas internas de retenção, observados requisitos legais, regulatórios, contratuais e de defesa em processos administrativos ou judiciais.

6.3. O descumprimento desta política, a omissão deliberada de incidentes, a destruição indevida de evidências ou o tratamento negligente de dados pessoais poderão ensejar medidas disciplinares e contratuais cabíveis, sem prejuízo de eventual apuração de responsabilidade civil, administrativa e penal.

7. Melhoria Contínua, Pós-Incidente e Inventário de Riscos

7.1. Encerrado o tratamento do incidente, deverá ser conduzida revisão pós-incidente para identificação de causa raiz, controles falhos ou inexistentes, efetividade da resposta, oportunidades de automação, necessidades de treinamento e impactos residuais ao negócio e aos titulares.

1. elaborar relatório final com síntese executiva, linha do tempo, causa raiz, decisões tomadas e evidências relevantes;
2. atualizar o inventário de riscos, o registro de operações de tratamento, o inventário de ativos e a matriz de terceiros impactados, quando aplicável;
3. definir plano de ação corretivo com responsáveis, prazos e indicadores de acompanhamento;
4. reavaliar políticas, procedimentos, controles, cláusulas contratuais e necessidades de comunicação complementar;
5. promover reciclagem ou treinamento direcionado às áreas envolvidas e registrar as lições aprendidas.

7.2. A presente política deverá ser revisada periodicamente, ou sempre que houver mudança relevante no ambiente tecnológico, no perfil de riscos, no modelo de negócio, na regulamentação aplicável ou após incidentes de maior criticidade.

8. Disposições Finais

8.1. Esta política deve ser interpretada em conjunto com as demais normas internas de segurança da informação, privacidade, continuidade de negócios, gestão de acessos, classificação da informação, gestão de fornecedores e resposta a crises.

8.2. Casos omissos serão avaliados pelo DPO, pela área de Segurança da Informação, pelo Jurídico e pela Alta Administração, conforme a natureza do evento e a criticidade do impacto potencial.

8.3. A aprovação desta política representa manifestação formal de comprometimento institucional com a proteção de dados pessoais, a gestão responsável de incidentes e a adoção de boas práticas e governança compatíveis com a LGPD.

Anexo I – Fluxo Resumido de Atuação

1. Detectar, registrar e escalar imediatamente qualquer suspeita de incidente.
2. Classificar o incidente e avaliar o potencial impacto aos titulares e ao negócio.
3. Conter o evento, preservar evidências e erradicar a causa ou vetor de comprometimento.
4. Recuperar os serviços e validar a integridade do ambiente antes da retomada plena.
5. Deliberar e executar a comunicação à ANPD, aos titulares e a partes interessadas, quando cabível.
6. Encerrar formalmente, documentar lições aprendidas e atualizar o inventário de riscos e controles.