POLÍTICA DE INCIDENTES DE SEGURANÇA DE DADOS PESSOAIS

PLANO DE RESPOSTAS A INCIDENTES DE SEGURANÇA EM DADOS PESSOAIS

Sumário

1. APRESENTAÇÃO

A Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, conhecida como LGPD, tem como principal objetivo a implementação de medidas de Segurança da Informação, visando trazer às entidades públicas e privadas uma cultura de maior conscientização aos Dados Pessoais.

Destrinchando a Lei, percebe-se que ela considera mais grave do que sofrer um ataque ou passar por um vazamento de dados, a não prevenção e/ou adoção de medidas e práticas necessárias e possíveis para a proteção dos seus dados e de todos os que são afetados por eventuais acessos não autorizados.

A adequação às regras da Lei Geral de Proteção de Dados Pessoais não se resume apenas ao emprego de medidas tecnológicas e padrões de segurança, mas também a necessidade de elaboração, manutenção e revisão de documentos que, além de garantir a adequação à citada Lei, também são medidas que podem trazer maior organização e otimização aos processos internos, além de proteger a reputação de empresas, entidades, escritórios, dentre outras, e seus colaboradores, usuários, parceiros e terceiros.

Diante disso, é que o escritório viu a necessidade de criação do referido documento.

2. OBJETIVO

Esta política tem como objetivo estabelecer diretrizes e procedimentos para a identificação, registro, tratamento e comunicação de incidentes de segurança relacionados a dados pessoais, garantindo conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD – Lei nº 13.709/2018).

Além disso, busca-se atingir os seguintes objetivos específicos:

1) Facilitar resposta coordenada e eficaz entre as áreas internas, em caso de incidente de segurança;
2) Priorizar a proteção de ativos do escritório, como dados sigilosos e sistemas para a operação das atividades;
3) Minimizar o impacto na reputação do escritório, comunicando-se de maneira eficaz com os titulares dos dados pessoais;
4) Melhorar as práticas de segurança.

3. DEFINIÇÕES

A Lei Geral de Proteção de Dados Pessoais nos traz conceitos específicos com relação às expressões mencionadas em seus artigos. Isto posto, seguem suas definições:

a. Conceitos em Relação aos Agentes

i. **Titular:** Pessoa Física a quem se referem os dados pessoais que serão tratados ao longo de todo o processo;
ii. **Controlador:** Pessoa física ou jurídica, de direito público ou privado, responsável por estipular como os dados serão tratados;
iii. **Operador:** Pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento dos dados pessoais em nome do controlador;
iv. **Encarregado de Dados Pessoais/Data Protection Officer (DPO):** Pessoa indicada pelo controlador para mediar a comunicação entre controlador, titular e a Autoridade Nacional de Proteção de Dados;
v. **Autoridade Nacional de Proteção de Dados:** Órgão da Administração Pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

b. Conceitos em Relação às Ações

i. **Consentimento:** Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

ii. **Eliminação:** Exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

iii. **Tratamento:** Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

iv. **Anonimização:** Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

v. **Uso compartilhado de dados:** Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

c. Conceitos em Relação aos Dados

i. **Dado Pessoal:** Informação relacionada a pessoa natural identificada ou identificável;

ii. **Dado Pessoal Sensível:** Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

iii. **Dado Anonimizado:** Dado relativo à titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

iv. **Banco de Dados:** Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

d. Conceito em Relação às Obrigações

i. **Mapeamento das atividades de dados:** documentação que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

e. Conceito em Relação às Ocorrências

i. Incidente: qualquer ato, suspeita, ameaça ou circunstância que comprometa a confidencialidade, integridade ou a disponibilidade de informações que estão em posse do escritório ou que ele venha a ter acesso;

ii. Vazamento de dados: qualquer quebra de sigilo ou disseminação de dados que possa resultar, criminosamente ou não, na perda, alteração, compartilhamento, acesso, transmissão, armazenamento ou processamento de dados não autorizado;

iii. Violação de privacidade: qualquer violação à legislação aplicável ou conduta e evento que resulte na destruição acidental ou ilícita dos dados, bem como sua perda, roubo, alteração, divulgação ou acesso não autorizado, danos ou desvio de finalidade em seu tratamento.

iv. Vírus: programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos.

4. PROCEDIMENTOS PARA TRATAMENTO DE INCIDENTES

4.1. Identificação e Registro do Incidente

Todo incidente deve ser reportado imediatamente ao Encarregado de Proteção de Dados.

O incidente deve ser registrado com as seguintes informações:

- Data e hora da ocorrência;
- Tipo de incidente;
- Natureza dos dados afetados;
- Consequências potenciais;
- Medidas tomadas para mitigar danos.

4.2. Avaliação do Impacto

É necessário determinar a gravidade do incidente e dos impactos aos titulares dos dados, onde será analisada pertinência de notificação a ANPD e os titulares.

A avaliação será feita através de um Mapa de Riscos

NÍVEL DE RISCO				
Volume de Dados Pessoais Expostos	Alto	**Alta Gravidade**	**Alta Gravidade**	**Alta Gravidade**
	Médio	**Média Gravidade**	**Alta Gravidade**	**Alta Gravidade**
	Baixo	**Baixa Gravidade**	**Média Gravidade**	**Média Gravidade**
		Baixa	Média	Alta
		Sensibilidade dos Dados Pessoais afetados		

Cada nível tem um valor de volume de dados para enquadramento de criticidade. No nível baixo, são Volumes de Dados Pessoais afetados inferior a 2% da base de dados; no nível médio, são Volumes de Dados Pessoais afetados inferior a

10% e superior a 2% da base de dados; no nível alto, são Volumes de Dados Pessoais afetados superiores a 10%. Já com relação a sensibilidade dos Dados Pessoais afetados, no nível baixo, são dados anonimizados, Dados Pessoais pseudonimizados (desde que a chave de desanonimização também não tenha sido comprometida), Dados Pessoais de difícil identificação (Ex.: IP); no nível médio, são Dados Pessoais imediatamente identificáveis (Ex.: nome, e-mail, CPF, endereço), combinados, ou não, com informações comportamentais (Ex.: histórico de atividades, preferências); no nível alto, são Dados Pessoais de crianças/ adolescentes, dados Pessoais Sensíveis ou que possam gerar discriminação ao titular.

Diante do exposto, deve-se procurar identificar a causa do incidente, atores e ações envolvidas, vulnerabilidades exploradas, visando determinar ações para as demais fases.

4.3. Preparação

A resposta a um incidente deve ser decisiva e executada de pronto. Neste caso, como existe pouco espaço para equívocos, é essencial que as práticas de emergência sejam exercitadas e os tempos de resposta medidos.

Isto posto, é possível desenvolver uma metodologia que estimule a agilidade e a exatidão, minimizando o impacto da indisponibilidade de recursos e os potenciais danos causados pelo comprometimento dos sistemas/processos.

4.4. Ações de Contenção e Remediação

Após a identificação de um incidente, faz-se necessário sua contenção. Sendo assim, necessário a implementação de medidas para interromper o incidente e proceder com a investigação, para identificar a causa e evitar recorrência.

4.5. Notificação de Incidentes

Caso o incidente represente risco ou dano relevante aos titulares, a ANPD e os titulares serão notificados conforme disposto na Lei Geral de Proteção de Dados Pessoais.

A notificação incluirá:

- Descrição do incidente;
- Medidas adotadas;
- Orientação aos titulares para mitigação de riscos.

4.6. Registro e Aprimoramento

Todos os incidentes deverão ser documentados, e o escritório deverá revisar periodicamente suas medidas de segurança para evitar novas ocorrências.

5. RESPONSABILIDADES

- Colaboradores: Reportar qualquer tipo de incidente imediatamente;
- Encarregado (DPO): Coordenar o tratamento do incidente e garantir a conformidade legal;
- Gestores: Implementar medidas preventivas e corretivas.

6. OBSERVAÇÕES COMPLEMENTARES

De forma paralela à execução desta Política, diversas ações devem ser desenvolvidas, antes, durante e depois da ocorrência de um incidente, conforme:

- Durante o incidente, como já fora dito, a etapa da identificação, coleta e preservação das evidências é essencial para demonstrar às autoridades que houve uma resposta adequada e que o incidente foi tratado com a seriedade necessária. De forma especial, no contexto da LGPD e da ANPD, as providências adotadas para conter o incidente e seus danos, podem ser definitivas para a minimização das sanções e multas, eventualmente, aplicadas ao caso concreto. Diante do exposto, necessário preservar as evidências do ocorrido;
- Necessário elaboração de um relatório final do incidente e revisão dos procedimentos, demonstrando uma função de comprovação das medidas levadas a efeito pelo escritório, compreendendo as causas do incidente, avaliando a aderência e efetividade da Política de Incidentes de Segurança de Dados e analisando a atuação dos responsáveis, seguindo disposto nos artigos da LGPD. Necessário mencionar, de forma clara e objetiva, e sem exagero de expressões técnicas, as condutas que foram e que serão implementadas para eliminar ou minimizar os efeitos do incidente, como o contato com as autoridades policiais, determinação de troca de senhas pelos usuários, a atualização de sistemas e servidores, dentre outros.

7. CANAIS DE ATENDIMENTO

- E-mail: atendimento@cenizeadvogados.com.br
- Site: www.cenizeadvogados.com.br
- Linkedin: @cenizesociedadeadvogados
- Telefones: (11) 2099-9417 – (11) 2506-2834
- Presencialmente: Rua Alferes Magalhães, nº 92, 1º andar – Sala 16 – Santana/SP, CEP: 02034-006

8. DISPOSIÇÕES FINAIS

Esta política deve ser revisada periodicamente para garantir sua eficácia e conformidade com as normas vigentes.