NORMAS DE GESTÃO DE INCIDENTES DE VIOLAÇÃO DE DADOS PESSOAIS

SUMÁRIO

1. OBJETIVO

Esta Norma de Gestão de Incidentes de Violação de Dados Pessoais tem por objetivo estabelecer as regras e restrições relativas à gestão dos Incidentes de Violação de Dados da **PiMA SERVICES** e mitigar os riscos ao negócio e aos ativos da empresa.

2. APLICAÇÃO

Esta Norma se aplica às seguintes Áreas: Responsável pela Segurança da Informação, Tecnologia da Informação, Encarregado pelo Tratamento de Dados Pessoais, e demais Áreas de Negócio.

Consiste ainda em identificar, prever e descrever possíveis situações de violação de dados, bem como as respectivas ações que deverão ser tomadas, os prazos e as formas de registro. O planejamento deverá conter, no mínimo, a previsão de possíveis situações de sinistros bem como as formas de monitoramento e a decisão que deverá ser tomada em caso desse tipo de ocorrência; a definição da área que deverá ser informada em situação de sinistro e de como reportá-lo. O grau de detalhamento das ações necessárias deve levar em conta a criticidade do evento.

3. DEFINIÇÕES

Ameaça: risco ou potencial perigo de um incidente, que pode resultar em dano a **PiMA SERVICES** ;

Ativo: é qualquer coisa que tenha valor para a **PiMA SERVICES** e precisa ser adequadamente protegida.

Evento: é qualquer ocorrência visível em uma rede ou sistema de informação. Exemplos: um usuário que acessa um arquivo compartilhado, um servidor que recebe uma solicitação para uma página da Web, um usuário que envia um e-mail ou um *firewall* que faz um bloqueio de uma tentativa de conexão, entre outros.

Evento adverso (ou ofensivo): é um evento com consequências negativas. Exemplos: falhas do sistema de informação, uso não autorizado de privilégios de sistema de informação, acesso não autorizado a dados confidenciais ou execução de *malware* que destrói dados, entre outros;

Incidente de Segurança da Informação: é um evento adverso identificado que indica possível violação à política de segurança da informação ou documentos complementares, falha de controles ou situação previamente desconhecida e que possa ser relevante à segurança da informação.

Informação: conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato.

Risco: Combinação da probabilidade da concretização de uma ameaça e seus potenciais impactos.

4. RESPOSTA A INCIDENTES

4.1. PREVENÇÃO A VIOLAÇÕES DE DADOS

A **PiMA SERVICES** realizará avaliações de impacto dos dados antes de iniciar qualquer projeto ou implementar qualquer tecnologia que processe Dados Pessoais. As análises de impacto nos dados avaliarão se os dados pessoais têm riscos associados.
Após determinar se existe um alto risco, a **PiMA SERVICES** tomará as medidas técnicas e organizacionais apropriadas para proteger os Dados Pessoais contra destruição acidental ou ilegal ou perda acidental, alteração, divulgação ou acesso não autorizado.

4.2. IDENTIFICAÇÃO DO INCIDENTE

Todos os colaboradores da **PiMA SERVICES** devem ser capazes de identificar um incidente de violação de dados pessoais, bem como estar atentos para reportar a ocorrência ao gerente responsável, área de segurança da informação ou Encarregado pelo Tratamento de Dados Pessoais. Incidentes ocorridos por ação ou omissão de agentes de tratamento que realizem essa tarefa específica em nome da **PiMA SERVICES** também devem notificar o Encarregado pelo Tratamento de Dados Pessoais.

O Encarregado pelo Tratamento de Dados Pessoais deve ser notificado quanto ao incidente e e deve analisar previamente se, de fato, a informação recebida configura um incidente de violação de dados pessoais.

Em caso positivo, o Encarregado pelo Tratamento de Dados Pessoais deve preencher o **"Formulário de Incidente de Violação de Dados Pessoais"** para incidentes ocorridos dentro da própria infraestrutura da **PiMA SERVICES** e, se necessário, envolver a área de Segurança da Informação.

Se os dados pessoais envolvidos no incidente estiverem anonimizados, não serão dados pessoais. Nesse contexto, deverá ser seguido o processo normal de gestão de incidentes de segurança da informação e o caso em questão deixará de ser tratado como violação de dados pessoais.

4.3. REGISTRO DO INCIDENTE

Qualquer pessoa que primeiro detectar um possível incidente de segurança, poderá preencher o formulário de incidentes **disponibilizado no site em ambiente destinado à Privacidade e Proteção de Dados Pessoais**. A partir do envio desse formulário, o Encarregado pelo Tratamento de Dados Pessoais fará a avaliação do tipo e do nível de risco criado pela violação.

O Encarregado pelo Tratamento de Dados Pessoais determinará se existe um risco para os direitos e liberdades dos titulares dos dados. Os riscos a direitos e liberdades incluem, entre outros, perda de controle ou confidencialidade dos Dados Pessoais, reversão não autorizada de pseudonimização, danos à reputação, discriminação, roubo ou fraude de identidade, perda financeira e outras desvantagens econômicas ou sociais.

O Encarregado pelo Tratamento de Dados Pessoais avaliará se a probabilidade e a gravidade dos riscos potenciais criam um risco alto. Essa avaliação deve envolver uma análise do tipo de violação; da natureza dessa violação; da sensibilidade e do volume de dados pessoais afetados; da gravidade das possíveis consequências para os titulares dos dados; do número de dados afetados e das características dos titulares desses dados; das características do destinatário dos dados pessoais e da facilidade de identificação dos titulares dos dados.

Há riscos elevados no processamento que utiliza novas tecnologias ou métodos de processamento em que nenhuma avaliação de impacto na proteção de dados foi realizada antes da violação pelo controlador, ou quando uma avaliação de impacto nos dados se tornou necessária à luz do tempo decorrido desde o processamento inicial.

O risco deve ser avaliado com base em uma **avaliação objetiva.**

O Encarregado pelo Tratamento de Dados Pessoais facilitará a notificação para a ANPD e aos Titulares dos Dados Pessoais, conforme, e se necessário, o **nível de risco.**

4.4. CONTENÇÃO DO INCIDENTE

O Encarregado pelo Tratamento de Dados Pessoais deverá orientar os gestores e áreas responsáveis/afetadas pela violação de dados pessoais quanto às medidas corretivas a serem tomadas.

O Gerente da Área originária do incidente de violação de dados deve tentar, junto com sua equipe, **recuperar** qualquer dado que tenha sido comprometido, de forma a **mitigar o risco** ao máximo possível, com o apoio do Encarregado pelo Tratamento de Dados Pessoais e da Área de Segurança da Informação.

O Encarregado pelo Tratamento de Dados Pessoais deverá estabelecer quem precisa ser informado internamente acerca da violação de dados pessoais e quais ações devem ser tomadas por quem foi informado.

O Responsável pela Segurança da Informação deverá apoiar, com as medidas técnicas necessárias para contenção/recuperação do incidente, a exemplo de efetuar coleta de evidências de forma legal ou isolar recursos de tecnologia de modo a não perder informações do incidente.

4.5. ANÁLISE DE RISCOS

De forma a analisar os riscos envolvidos no incidente de violação de dados, deverá ser feita análise de riscos pelo Encarregado pelo Tratamento de Dados Pessoais, com apoio do gerente da área originária do incidente de violação de dados, considerando as informações que **constarem no formulário de incidente:**

- Que tipo de dados pessoais estão envolvidos?
- Há dados pessoais sensíveis nesta violação?
- Quais medidas de segurança são aplicáveis à área/recurso originário do incidente?
- Quantos indivíduos foram afetados pela violação?
- Em caso de compartilhamento indevido, quais informações um terceiro pode extrair da informação à qual teve acesso?
- Foi possível identificar todos os envolvidos na violação de dados ocorrida?
- Há informações de cadastro/contato de todos os envolvidos na violação de dados ocorrida?
- A violação de dados ocorrida afeta algum direito do titular de dados pessoais garantido por legislação de proteção de dados nos territórios onde ocorreu a violação?

4.6. NOTIFICAÇÃO PARA ANPD

Uma violação dos dados que provavelmente represente qualquer risco aos direitos e liberdades das pessoas físicas deve ser relatada à ANPD sem demora injustificada, quando possível, dentro de 72 horas depois que a **PiMA SERVICES** tomar conhecimento da violação. Uma violação que apresente alto risco deve ser relatada sem demora indevida. Quaisquer possíveis motivos para demora na comunicação devem ser informados à ANPD.

A **PiMA SERVICES** é considerada ciente de uma violação quando existe um grau razoável de certeza de que ocorreu um incidente de segurança que levou ao comprometimento dos dados pessoais. A **PiMA SERVICE** também é considerada ciente quando um operador é informado. Portanto, todos os contratos de processamento de dados devem exigir que o operador notifique imediatamente a **PiMA SERVICES** de uma violação.

Um aviso parcial e incompleto pode ser enviado para a ANPD ou, eventualmente, após 72 horas em circunstâncias específicas. Essas circunstâncias incluem violações complexas que requerem investigações detalhadas ou ocorrências de várias violações semelhantes em um curto período de tempo.

A **Comunicação Do Incidente De Segurança Para A Autoridade Nacional De Proteção De Dados** deverá ser protocolada por meio de Peticionamento Eletrônico - Usuário Externo no sistema SEI do Governo Federal. O formulário de incidentes disponibilizado no site em ambiente destinado à Privacidade e Proteção de Dados Pessoais da **PiMA SERVICES** é o conteúdo que deverá ser encaminhado por meio desse peticionamento eletrônico.

Para maiores informações sobre o cadastramento do usuário (DPO) para envio da Comunicação de Incidentes à ANPD, clique aqui.

4.7. AVISO AOS TITULARES DE DADOS PESSOAIS

Com o apoio do Jurídico, o Encarregado pelo Tratamento de Dados Pessoais comunicará violações de alto risco aos titulares de dados pessoais afetados, sem demora injustificada.
Uma comunicação com o Titular dos dados pessoais (no formato estabelecido no Anexo II) deve conter, no mínimo, em linguagem clara e simplificada:

- a descrição da natureza dos dados pessoais afetados;
- as informações sobre os titulares envolvidos;
- a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- os riscos relacionados ao incidente;
- os motivos da demora, no caso de a comunicação não ter sido imediata;
- as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo;
- a identificação dos pontos de contato para maiores detalhes;
- a descrição das possíveis consequências do incidente de violação de dados;

- a descrição de medidas para endereçar o incidente de violação de dados, incluindo medidas adotadas para mitigar possíveis efeitos adversos do incidente de violação de dados.

A comunicação com os titulares dos dados deve ser entregue em mensagens dedicadas por meios que maximizem as chances de comunicação das informações a todos os titulares dos dados afetados - isso pode exigir a utilização de vários métodos de comunicação e o fornecimento de informações em formatos e idiomas alternativos, quando apropriado.

Se a violação afetar um grande volume de registros de titulares de dados e dados pessoais, a **PiMA SERVICES** decidirá se uma notificação pública em massa é apropriada em vez de uma notificação personalizada individual. Essa decisão será tomada com base em uma avaliação da quantidade de recursos necessários para notificar cada titular de dados individualmente e sobre a capacidade da **PiMA SERVICES** de fornecer adequadamente aos titulares dos dados a notificação dentro do prazo especificado.

4.8. DECISÃO DE NÃO NOTIFICAÇÃO

A **PiMA SERVICES** está isenta do requisito de notificação obrigatória quando o risco para os titulares de dados é extremamente baixo. Alguns exemplos disso incluem, entre outros, violações de dados publicamente disponíveis, dados pessoais vazados, mas protegidos por uma chave que permanece confidencial e não pode ser verificada independentemente, perdas temporárias de acesso a dados pessoais e dados pessoais enviados acidentalmente para terceiros confiáveis em virtude de seu relacionamento com a **PiMA SERVICES** .

Se for tomada a decisão de não notificar, a justificativa para essa decisão deve ser documentada.

A **PiMA SERVICES** deve continuar a monitorar as circunstâncias e os efeitos de uma violação e pode precisar fazer ou atualizar notificações à ANPD ou comunicações do Titular dos Dados à medida que novas informações surgirem.

Todas as violações e as ações tomadas para responder às violações devem ser totalmente documentadas, mesmo que nenhuma notificação seja necessária, através do **“Formulário de Incidente de Violação de Dados”.**

4.9. NOTIFICAÇÃO AO CONTROLADOR - PiMA SERVICES NA CONDIÇÃO DE OPERADOR

Se os dados pessoais envolvidos no incidente estiverem sendo tratados pela **PiMA SERVICES** , na qualidade de operador, o controlador dos dados deverá ser notificado sem demora injustificada, conforme ANEXO III – NOTIFICAÇÃO AO CONTROLADOR, devendo a PiMA SERVICES cooperar com as informações necessárias, bem como com as autoridades fiscalizadoras, para a mais breve apuração, esclarecimento e solução do caso com total transparência.

4.10. PÓS INCIDENTE – PRÓXIMOS PASSOS

Após a correção de uma violação, a equipe de resposta à violação deve se reunir para discutir as medidas ou procedimentos de segurança que precisam ser implementados para melhorar a segurança dos dados com base nas lições aprendidas.

A equipe de resposta a violações também deve refletir sobre a resposta geral à violação e políticas ou protocolos atualizados, conforme necessário, para melhorar as reações futuras a eventuais novas violações.

5. PENALIDADES

Violações: descumprimento das diretrizes estabelecidas nesta Política e das obrigações de normas, regulamentos e leis em vigor à época da ocorrência de eventual incidente, deve ser considerado como uma violação e tratada pela **PiMA SERVICES** a fim de apurar as responsabilidades dos envolvidos, visando aplicação de sanções cabíveis.
Tentativa de Burla: A tentativa de burlar as diretrizes e controles estabelecidos, quando constatada, também deve ser tratada como uma violação.

6. RESPONSABILIDADES

6.1. Encarregado pelo Tratamento de Dados Pessoais

- Receber o incidente via “Formulário de Incidente de Violação de Dados” e prosseguir com o que for devido.
- Avaliar a necessidade de comunicação do Incidente de Violação de Dados para a Autoridade Nacional de Proteção de Dados e titulares de dados pessoais.
- Iniciar processos de investigação do Incidente de Violação de Dados e indicar áreas envolvidas que deverão participar do processo.

- Comunicar violações de alto risco aos titulares de dados afetados sem demora injustificada.

6.2. Tecnologia da Informação

- Aprovar e empreender ações ou investimentos que promovam a melhoria contínua do processo.
- Auxiliar na análise dos incidentes de violação de dados pessoais por meio da apresentação das trilhas de auditoria dos sistemas sob sua gestão.
- Comunicar a equipe de gerenciamento de mudanças a fim de que ela notifique os gestores e usuários do recurso em questão, caso o tratamento do incidente envolva impactos no ambiente de produção.
- Conduzir, em paralelo a este documento, os procedimentos indicados na Política de Gestão de Incidentes de Segurança da Informação.
- Auxiliar nos processos de investigação do incidente quando requerido.
- Apoiar, com as medidas técnicas necessárias, a contenção/recuperação do incidente.

6.3. Responsável pela Segurança da Informação

- Aprovar e empreender ações ou investimentos que promovam a melhoria contínua do processo.
- Apoiar, sempre que necessário, a interação e o escalonamento com as demais áreas a fim de prover um atendimento mais rápido ao processo.

6.4. Qualidade

- Os incidentes de violação de dados pessoais que envolvam indícios de fraude ou vazamento de informação serão encaminhados para área de auditoria, a qual poderá se aprofundar na investigação.

6.5. Jurídico

- Se o incidente tiver consequências legais, deve ser estabelecido um contato com os órgãos responsáveis pela apuração e aplicação de penalidades (Agências Reguladoras e/ou Delegacias, se for o caso) para relato dos fatos e a apresentação de indícios relativos ao incidente.

6.6. Pessoas e Cultura

- Para os incidentes de violação de dados pessoais que envolvam desvio de conduta do colaborador ou conduta em desacordo com o código de ética, esse colaborador será encaminhado para a área de recursos humanos, que poderá se aprofundar na investigação.

6.7. Comunicação

- Tomar as necessárias providências, em consonância com as diretrizes da Alta Direção, no caso de incidentes que tiverem desdobramentos para fora da PiMA SERVICES , e que envolvam a imprensa ou comunidade externa.

7. DISPOSIÇÕES FINAIS

O presente documento deve ser lido e interpretado sob a égide das leis brasileiras, no idioma português, em conjunto com as normas e procedimentos aplicáveis pela **PiMA SERVICES** ;
Esta Norma, bem como os demais documentos que a complementam, encontra-se disponível no *Sharepoint* ou, em caso de indisponibilidade, pode ser solicitada ao Encarregado pelo Tratamento de Dados Pessoais da **PiMA SERVICES** .

Qualquer dúvida relativa a esta Norma deve ser encaminhada ao Encarregado pelo Tratamento de Dados Pessoais da **PiMA SERVICES** , por meio do e-mail dpo@pimaservices.com.br.

Esta Norma entra em vigor na data de sua publicação.

ANEXO I – NOTIFICAÇÃO À AUTORIDADE **em caráter sugestivo*

Autoridade Nacional de Proteção de Dados
[ENDEREÇO]

Prezados Senhores,

Vimos pela presente comunicar a ocorrência de uma Violação de Dados Pessoais que consideramos uma grave violação de segurança de dados pessoais.

*[No caso de a violação já ter sido investigada]
[Investigamos a violação por [DETALHES DE COMO O INCIDENTE FOI INVESTIGADO] e apuramos as informações adiante descritas.]

*[No caso de a violação estar em investigação]
[Estamos investigando a violação e prevemos concluí-la até [DATA FINAL], quando forneceremos as informações adicionais necessárias. No estágio em que se encontra a investigação, podemos prestar os seguintes esclarecimentos [FORNECER PELO MENOS AS INFORMAÇÕES OBRIGATÓRIAS EXIGIDAS PELA ANPD].

*Detalhes da violação de segurança de dados
A PiMA SERVICES atua na qualidade de controlador de dados em relação à violação dos dados pessoais.

*[No caso de haver demora na comunicação. Neste ponto, a LGPD não fornece o prazo específico em horas, mas por analogia ao GDPR recomendamos que seja feita a notificação em até 72 horas.]

[Lamentamos a demora em relatar esse incidente, mas isso ocorreu por [RAZÕES]

A violação foi descoberta em [DATA] e provavelmente ocorreu em [DATA].

A informação foi [acidental ou ilegalmente destruída OU perdida OU alterada OU divulgada OU acessada sem autorização por [NOME OU DESCRIÇÃO DA ORGANIZAÇÃO]].

A violação ocorreu nas seguintes circunstâncias e pelas seguintes razões:
• [CIRCUNSTÂNCIAS] • [RAZÕES]

*Medidas em vigor:
Tínhamos as seguintes medidas em vigor para impedir que ocorresse um incidente dessa natureza:
• [MEDIDAS]
Existiam implementadas no momento da violação as seguintes políticas e procedimentos:
• [LISTA DE POLÍTICAS E PROCEDIMENTOS E DATA IMPLEMENTADA]

*Dados pessoais colocados em risco:
A violação afeta os seguintes tipos de informações:
• [TIPOS DE INFORMAÇÃO, POR EXEMPLO, DADOS PESSOAIS OU DADOS PESSOAIS SENSÍVEIS E DETALHES DA EXTENSÃO].

É provável que a violação afete cerca de [Número estimado] titulares de dados pessoais.

*[Aqui, listar a decisão de informar ou não informar os titulares]
[Não [informamos] os titulares de dados pessoais afetados pela violação porque [RAZÕES DA DECISÃO] OU Os titulares de dados pessoais estão [conscientes OU inconscientes] de que o incidente ocorreu].

A violação pode ter as seguintes consequências e efeitos adversos nos titulares de dados afetados:
• [CONSEQUÊNCIAS]
• [EFEITOS ADVERSOS]

*[Aqui, se houve reclamações ou não.]
Nós [recebemos [NÚMERO] de reclamações OU não recebemos nenhuma reclamação] dos titulares de dados pessoais afetados.

*Contenção e recuperação
Nós [adotamos OU propomos tomar] as seguintes medidas para solucionar a violação e minimizar e mitigar seus efeitos sobre os indivíduos afetados:
• [MEDIDAS]

As informações [não] foram recuperadas [e os detalhes são os seguintes:
• [DETALHES DE COMO E QUANDO FOI RECUPERADO]].

Também adotamos as seguintes etapas para evitar ocorrências futuras da violação:
• [AÇÃO PALIATIVA TOMADA]
• [Os fatos que cercam a violação, os efeitos dessa violação e as ações corretivas tomadas foram registrados em um formulário de violação de dados mantido pelo [controlador dos dados pessoais]

*Treinamento e orientação
Nós [não] fornecemos à equipe treinamento sobre os requisitos da Lei de Geral de Proteção de Dados Pessoais [e os detalhes são os seguintes:
• [DETALHES OU EXTRATOS DOS MANUAIS DE TREINAMENTO RELEVANTES PARA ESTE RELATÓRIO DE DADOS]].

Nós fornecemos orientações detalhadas para a equipe sobre o tratamento de dados pessoais em relação a este incidente e os detalhes são os seguintes:
• [DETALHES OU EXTRATOS DE QUALQUER ORIENTAÇÃO DETALHADA DADA AO PESSOAL NO TRATAMENTO DE DADOS PESSOAIS EM RELAÇÃO À VIOLAÇÃO DE DADOS].

Confirmamos que o treinamento sobre os requisitos da Lei Geral de Proteção de Dados Pessoais é obrigatório para todos os funcionários e que os funcionários envolvidos neste incidente receberam treinamento em [DATA].

*Diversos
Nós [não] notificamos outras autoridades de proteção de dados (no exterior) sobre essa violação de dados [e os detalhes são os seguintes:
• [DETALHES DAS AUTORIDADES DE PROTEÇÃO DE DADOS]].

Nós [não] informamos a polícia sobre essa violação de dados [e os detalhes são os seguintes:
• [DETALHES E NOME DA FORÇA POLICIAL]].

Nós [não] informamos outros órgãos reguladores sobre essa violação de dados [e os detalhes são os seguintes:
• [NOME E DETALHES DOS ORGANISMOS REGULAMENTARES]].

[Não] houve cobertura da mídia [e os detalhes são os seguintes:
• [DETALHES DA COBERTURA DA MÍDIA]].

Além disso, consideramos que as seguintes informações seriam do seu interesse:
• [DETALHES].
Eventuais esclarecimentos adicionais poderão ser obtidos por meio dos contatos abaixo indicados:

- [NOME DE CONTROLADOR DE DADOS]
- [NOME DO CONTATO DO ENCARREGADO PELO TRATAMENTO DE DADOS]
- [ENDEREÇO]
- [NÚMERO DE TELEFONE]
- [ENDEREÇO DE E-MAIL]
- [ENDEREÇO DO WEBSITE].

Atenciosamente,

ANEXO II – NOTIFICAÇÃO AO TITULAR **em caráter sugestivo*

[DESTINATÁRIO]
[ENDEREÇO]

Prezado [Titular dos Dados Pessoais],

Lamentamos informá-lo sobre uma violação da segurança que resultou na [destruição OU perda OU alteração OU divulgação acidental [ou ilegal] OU acesso não autorizado] de seus dados pessoais.

A violação foi descoberta em [DATA] e provavelmente ocorreu em [DATA].

Como resultado de nossa investigação, concluímos que a referida violação afeta os seguintes tipos de informações:
• [TIPOS DE INFORMAÇÃO. POR EXEMPLO, DADOS PESSOAIS E DADOS PESSOAIS SENSÍVEIS].

A violação ocorreu nas seguintes circunstâncias e pelas seguintes razões:
• [CIRCUNSTÂNCIAS].• [RAZÕES].

Tomamos as seguintes medidas para mitigar quaisquer efeitos adversos:
• [MEDIDAS].

Recomendamos que você tome as seguintes medidas para mitigar possíveis efeitos adversos:
• [MEDIDAS].

[Informamos a Autoridade de Proteção de Dados sobre a violação em [DATA].

Eventuais esclarecimentos adicionais poderão ser obtidos por meio dos contatos indicados a seguir:

- [NOME DO CONTROLADOR DE DADOS]
- [NOME DO ENCARREGADO PELO TRATAMENTO DE DADOS]
- [ENDEREÇO]
- [NÚMERO DE TELEFONE]
- [ENDEREÇO DE E-MAIL]
- [ENDEREÇO DO WEBSITE].

Atenciosamente,

ANEXO III – NOTIFICAÇÃO AO CONTROLADOR**em caráter sugestivo*

Prezado [NOME DO CONTROLADOR DOS DADOS],

Vimos pela presente, na qualidade de operador dos dados e em cumprimento das obrigações negociais firmadas, comunicar que, no dia [DD] de [MM] de [AAAA], identificamos o comprometimento de parte da nossa base de dados, que consideramos uma grave violação de segurança dos dados pessoais que tratamos conforme suas instruções.

* [No caso de a violação já ter sido investigada]
Imediatamente ao tomar ciência do incidente, abrimos uma investigação interna para apurar ocorrido e [DETALHAR COMO O INCIDENTE FOI INVESTIGADO], tendo sido apuradas as informações adiante descritas.

* [No caso de a violação estar em investigação]
Estamos investigando a violação e prevemos concluí-la até [DATA FINAL], quando forneceremos as informações adicionais necessárias. No estágio em que se encontra a investigação, podemos prestar os seguintes esclarecimentos

* [Detalhar a violação de segurança de dados]
A informação foi [acidental ou ilegalmente destruída OU perdida OU alterada OU divulgada OU acessada sem autorização da PiMA SERVICES].

A violação ocorreu nas seguintes circunstâncias e pelas seguintes razões:
• [CIRCUNSTÂNCIAS] • [RAZÕES]

* [Informar os dados pessoais colocados em risco]
A violação afeta os seguintes tipos de informações:
• [TIPOS DE INFORMAÇÃO, POR EXEMPLO, DADOS PESSOAIS OU DADOS PESSOAIS SENSÍVEIS E DETALHES DA EXTENSÃO].

É provável que a violação afete cerca de [Número estimado] titulares de dados pessoais.

Dessa forma, solicitamos que [NOME DO CONTROLADOR] comunique o ocorrido à Autoridade Nacional de Proteção de Dados – ANPD (recomendamos que seja feita a notificação em até 72 horas, por analogia ao GDPR, pois a LGPD não fornece o prazo específico).

*[Aqui, listar a decisão de informar ou não informar os titulares]
Entendemos que os titulares de dados pessoais afetados pela violação [DEVEM OU NÃO SER INFORMADOS] porque [RAZÕES DA DECISÃO].

* Contenção e recuperação
Nós [adotamos OU propomos tomar] as seguintes medidas para solucionar a violação e minimizar e mitigar seus efeitos sobre os indivíduos afetados:

• [MEDIDAS]

As informações [não] foram recuperadas [e os detalhes são os seguintes]:
• [DETALHES DE COMO E QUANDO FOI RECUPERADO].

Também adotamos as seguintes etapas para evitar ocorrências futuras da violação:
• [AÇÃO PALIATIVA TOMADA]
• [Os fatos que cercam a violação, os efeitos dessa violação e as ações corretivas tomadas foram registrados em um formulário de violação de dados mantido pelo [controlador dos dados pessoais]

Lamentamos profundamente o ocorrido e estamos à disposição para cooperar com as informações necessárias, bem como com as autoridades fiscalizadoras, para a mais breve apuração, esclarecimento e solução do caso com total transparência.

A PiMA SERVICES se coloca inteiramente à disposição para eventuais esclarecimentos adicionais, que poderão ser obtidos por meio dos contatos abaixo indicados:
- [NOME DO CONTATO DO ENCARREGADO PELO TRATAMENTO DE DADOS]
- [ENDEREÇO]
- [NÚMERO DE TELEFONE]
- [ENDEREÇO DE E-MAIL]

Atenciosamente,