

TÍTULO: GESTÃO DE INCIDENTES DE VIOLAÇÃO DE DADOS PESSOAIS

1. OBJETIVOS

Estabelecer diretrizes e princípios que nortearão a Gestão de Incidentes de Violação de Dados Pessoais na Âmbar Energia Amazonas, bem como mitigar os riscos ao negócio e aos ativos da Companhia.

2. ABRANGÊNCIA

Esta norma se aplica no âmbito da Âmbar Energia Amazonas S.A.

3. REFERÊNCIAS

- Lei nº. 13.709/2018, de 14/08/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);
- Lei nº. 13.853/2019, de 08/07/2019, que altera a Lei nº. 13.709/2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados – ANPD;
- Decreto nº 20.777/2020, de 28/10/2020 - Institui o Comitê Gestor de Proteção de Dados (CGPD);
- Código de Conduta e Ética da Âmbar Energia Amazonas S.A.

4. CONCEITOS

- 4.1 Agentes de Tratamento:** são figuras centrais na aplicação da LGPD, pois representam os atores envolvidos (Controlador e Operador) no processo de coleta, processamento e gerenciamento de dados pessoais;
- 4.2 Ameaça:** risco ou potencial perigo de um incidente, que pode resultar em dano a companhia;
- 4.3 Ativo:** é qualquer bem que tenha valor para a companhia e precisa ser adequadamente protegido;
- 4.4 Controlador:** pessoa natural ou jurídica que toma as decisões relacionadas ao tratamento de dados pessoais;
- 4.5 Data Protection Officer - DPO:** é a sigla para Data Protection Officer, que em português significa Oficial de Proteção de Dados. No Brasil, o DPO é também conhecido como **Encarregado pelo Tratamento de Dados Pessoais**;
- 4.6 Dado anonimizado:** é aquele que, originariamente, era relativo a uma pessoa, mas que passou por etapas que garantiram a desvinculação dele a essa pessoa. Se um dado for anonimizado, então a Lei de Geral de Proteção de Dados - LGPD não se aplicará;
- 4.7 Evento:** é qualquer ocorrência visível em uma rede ou sistema de informação. Exemplos: um usuário que acessa um arquivo compartilhado, um servidor que

Código: PR-DRC-02/N-004	Página: 2/16
Versão: 00	Vigência: 17/10/2026
Doc. Aprovação: RES n.º 056/2024, 16/10/2024	

TÍTULO: GESTÃO DE INCIDENTES DE VIOLAÇÃO DE DADOS PESSOAIS

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;

- 4.8 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;
- 4.9 Encarregado pelo Tratamento de Dados Pessoais:** pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
- 4.10 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;
- 4.11 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;
- 4.12 Operador:** pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do controlador.
- 4.13 Risco:** combinação da probabilidade da concretização de uma ameaça e seus potenciais impactos;
- 4.14 Violação de Dados:** é a liberação de informações confidenciais, privadas ou sensíveis em um ambiente não seguro.

5. RESPONSABILIDADES**5.1 Encarregado pelo Tratamento de Dados Pessoais**

- 5.1.1 Receber o "Formulário de Incidente de Violação de Dados", anexo III e prosseguir com as providências necessárias;
- 5.1.2 Avaliar a necessidade de comunicação do Incidente de Violação de Dados para a Autoridade Nacional de Proteção de Dados - ANPD e titulares de dados pessoais;
- 5.1.3 Iniciar processos de investigação do Incidente de Violação de Dados e indicar áreas envolvidas que deverão participar do processo.

5.2 Departamento de Tecnologia da Informação - DAT

- 5.2.1 Aprovar e empreender ações ou investimentos que promovam a melhoria contínua do processo, com o apoio da Alta Direção;

Código: PR-DRC-02/N-004	Página: 3/16
Versão: 00	Vigência: 17/10/2026
Doc. Aprovação: RES n.º 056/2024, 16/10/2024	

TÍTULO: GESTÃO DE INCIDENTES DE VIOLAÇÃO DE DADOS PESSOAIS

- 5.2.2 Auxiliar na análise dos incidentes de violação de dados pessoais por meio da apresentação das trilhas de auditoria dos sistemas sob sua gestão;
- 5.2.3 Auxiliar nos processos de investigação do incidente, quando solicitado;
- 5.2.4 Apoiar com as medidas técnicas necessárias para contenção/recuperação do incidente;
- 5.2.5 Apoiar sempre que necessário na interação e no escalonamento com as demais áreas, a fim de prover um atendimento mais rápido sobre o incidente;
- 5.2.6 Monitorar continuamente o ambiente tecnológico do ponto de vista de segurança da informação, visando identificar eventos que possam causar impacto na disponibilidade, integridade e confidencialidade de dados pessoais que sejam tratados pela Companhia.

5.3 Departamento de Compliance

- 5.3.1 Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- 5.3.2 Receber comunicações da autoridade nacional e adotar providências;
- 5.3.3 Orientar os colaboradores e os contratados, acerca das práticas a serem tomadas em relação à proteção de dados pessoais;
- 5.3.4 Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

5.4 Gerente ou Coordenador

- 5.4.1 Observar o cumprimento deste normativo e demais documentos complementares de seus colaboradores;
- 5.4.2 Receber comunicação de incidentes de violação de dados por parte de colaboradores de sua área;
- 5.4.3 Reportar imediatamente os incidentes de violação de dados ao Encarregado pelo Tratamento de Dados Pessoais;
- 5.4.4 Preencher o "Formulário de Incidente de Violação de Dados Pessoais", anexo III e o encaminhar ao Encarregado pelo Tratamento de Dados Pessoais;
- 5.4.5 Auxiliar nos processos de investigação do incidente de dados pessoais, quando solicitado.

5.5 Colaboradores

- 5.5.1 Observar e cumprir as diretrizes contidas neste normativo, bem como reportar os incidentes de violação de dados à sua gerência imediata;

Código: PR-DRC-02/N-004	Página: 4/16
Versão: 00	Vigência: 17/10/2026
Doc. Aprovação: RES n.º 056/2024, 16/10/2024	

TÍTULO: GESTÃO DE INCIDENTES DE VIOLAÇÃO DE DADOS PESSOAIS

- 5.5.2 Auxiliar no preenchimento do Formulário de Incidente de Violação de Dados”, anexo III, quando solicitado;
- 5.5.3 Auxiliar nos processos de investigação do incidente de violação de dados, quando solicitado.

6. DIRETRIZES

6.1 Prevenção a violação de dados pessoais

- 6.1.1** As avaliações de impacto dos dados pessoais, deverá ser realizadas antes de iniciar qualquer projeto ou implementar qualquer tecnologia relacionada aos dados pessoais;
- 6.1.2** Para os casos que for determinado um alto risco, o Encarregado pelo Tratamento de Dados Pessoais, deverá adotar as medidas técnicas e organizacionais apropriadas para proteger os dados pessoais contra destruição acidental ou ilegal e/ou perda acidental, alteração, divulgação ou acesso não autorizado;
- 6.1.3** Para os incidentes de violação de dados pessoais que envolvam indícios de fraude ou vazamento de informação, deverá ser encaminhado imeditamente para o Encarregado de Dados, para as devidas providências e aprofundamento na investigação;
- 6.1.4** Para os incidentes de violação de dados pessoais que envolvam desvio de conduta do colaborador ou em desacordo com o Código de Conduta e Ética, deverá ser encaminhado imeditamente para o Departamento de *Compliance*, para as devidas providências e aprofundamento na investigação.

6.2 Identificação do Incidente

- 6.2.1** Todos os colaboradores da Âmbar Energia Amazonas deverão ser capazes de identificar um incidente de violação de dados, bem como estar atentos em reportar a ocorrência ao Superior imediato;
- 6.2.2** O gerente responsável pela área/recurso do qual foi originado o incidente de violação deve ser notificado quanto ao incidente de violação de dados, devendo fazer uma análise prévia se a informação recebida realmente configura um incidente de violação de dados;
- 6.2.3** Em caso positivo deve preencher o “Formulário de Incidente de Violação de Dados”, anexo III para incidentes ocorridos dentro da própria infraestrutura da Âmbar Energia Amazonas e enviar para o Encarregado pelo Tratamento de Dados Pessoais;
- 6.2.4** Incidentes ocorridos por ação ou omissão de agentes de tratamento que atuem em nome da Âmbar Energia Amazonas devem ter o formulário “Formulário de Incidente de Violação de Dados” preenchidos pelo próprio

Código: PR-DRC-02/N-004	Página: 5/16
Versão: 00	Vigência: 17/10/2026
Doc. Aprovação: RES n.º 056/2024, 16/10/2024	

TÍTULO: GESTÃO DE INCIDENTES DE VIOLAÇÃO DE DADOS PESSOAIS

agente de tratamento e enviar para o Encarregado pelo Tratamento de Dados Pessoais;

6.2.5 A Âmbor Energia Amazonas manterá nos contratos de processamento de dados com terceiros, a obrigatoriedade da notificação imediata por parte do operador à Âmbor Energia Amazonas em caso de uma violação;

6.2.6 O "Formulário de Incidente de Violação de Dados", anexo III deve ser recebido e avaliado pelo Encarregado pelo tratamento dos dados pessoais, se a ocorrência realmente configurar um incidente de violação de dados pessoais;

6.2.7 Caso os dados pessoais envolvidos no incidente estiverem anonimizados, não serão considerados dados pessoais, devendo seguir o processo normal de gestão de incidentes de segurança da informação.

6.2.7.1 Nesses casos, a Lei Geral de Proteção de Dados - LGPD não se aplicará.

6.3 Registro do Incidente

6.3.1 O Encarregado pelo tratamento de dados pessoais deverá:

6.3.1.1 Avaliar o tipo e o nível de risco criado pela violação;

6.3.1.2 Registrar o incidente na ferramenta de gestão de incidentes utilizada pela Companhia;

6.3.1.3 Determinar se existe um risco para os direitos e liberdades dos titulares dos dados, o qual inclui:

- a) Perda de controle ou confidencialidade dos Dados Pessoais;
- b) Reversão não autorizada de pseudonimização;
- c) Danos à reputação;
- d) Discriminação;
- e) Roubo ou fraude de identidade, perda financeira e outras desvantagens econômicas ou sociais.

6.3.1.4 Avaliar se a probabilidade e a gravidade dos riscos potenciais criam um risco alto, devendo conter:

- a) Uma análise do tipo de violação;
- b) Natureza;
- c) Sensibilidade e volume de dados pessoais afetados;
- d) A gravidade das possíveis consequências para os titulares dos dados;
- e) O número e as características dos titulares de dados afetados;
- f) As características do destinatário dos dados pessoais e a facilidade de identificação dos titulares dos dados.

Código: PR-DRC-02/N-004	Página: 6/16
Versão: 00	Vigência: 17/10/2026
Doc. Aprovação: RES n.º 056/2024, 16/10/2024	

TÍTULO: GESTÃO DE INCIDENTES DE VIOLAÇÃO DE DADOS PESSOAIS

6.3.1.5 O risco deve ser analisado com base em uma avaliação objetiva;

6.3.1.6 Notificar a Autoridade Nacional de Proteção de Dados (ANPD) e aos Titulares dos Dados Pessoais caso necessário e conforme o nível de risco.

6.4 Contenção do Incidente

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

6.4.2 Nos casos de incidente de violação de dados, a área originária deverá tentar recuperar qualquer dado que tenha sido comprometido, de forma a mitigar o risco ao máximo possível, como o apoio do Encarregado pelo Tratamento de Dados Pessoais e o Departamento de Tecnologia da Informação - DAT.

6.4.3 O Encarregado pelo Tratamento de Dados Pessoais deverá estabelecer quem precisará ser informado internamente acerca da violação de dados e quais ações deverão ser tomadas;

6.4.4 O Departamento de Tecnologia da Informação deverá apoiar com as medidas técnicas necessárias para contenção/recuperação do incidente.

6.5 Análise de Riscos

6.5.1 As análises dos riscos envolvidos no incidente de violação de dados, deverá ser conduzida pelo gerente da Área originária do incidente, juntamente com o apoio do Encarregado pelo Tratamento de Dados Pessoais, a considerar as seguintes informações:

- 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 a 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?

Código: PR-DRC-02/N-004	Página: 7/16
Versão: 00	Vigência: 17/10/2026
Doc. Aprovação: RES n.º 056/2024, 16/10/2024	

TÍTULO: GESTÃO DE INCIDENTES DE VIOLAÇÃO DE DADOS PESSOAIS

6.6 Notificação a Autoridade Nacional de Proteção de Dados - ANPD

6.6.1 Toda violação dos dados que represente qualquer risco aos direitos e liberdades das pessoas físicas, deverá ser relatada à Autoridade Nacional de Proteção de Dados – ANPD, sem demora injustificada, quando possível, no prazo de 02 (dois) dias úteis, após a constatação da violação.

6.6.1.1 Caso haja motivos para a demora na comunicação, deve ser informado a Autoridade Nacional de Proteção de Dados – ANPD;

6.6.1.2 Uma notificação parcial e incompleta pode ser enviada a Autoridade Nacional de Proteção de Dados - ANPD após as 48 horas, devido a violações complexas que requerem investigações detalhadas ou quando ocorrem várias violações semelhantes, em um curto período de tempo.

6.6.2 Será considerada uma violação, quando existir um grau razoável de certeza que ocorreu um incidente de segurança, o que levou ao comprometimento dos dados pessoais;

6.6.3 A notificação para a Autoridade Nacional de Proteção de Dados - ANPD deverá seguir no formato estabelecido, conforme o Anexo I, devendo ser incluído:

- a) A descrição da natureza dos dados pessoais afetados;
- b) As informações sobre os titulares envolvidos;
- c) A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comerciais e industriais;
- d) Os riscos relacionados ao incidente;
- e) Os motivos da demora, no caso de a comunicação não ter sido imediata ou no prazo de 02 (dois) dias úteis;
- f) As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo;
- g) Identificar pontos de contato para maiores detalhes;
- h) Descrever possíveis consequências do incidente de violação de dados;
- i) Descrever medidas para endereçar o incidente de violação de dados, incluindo medidas adotadas para mitigar possíveis efeitos adversos do incidente de violação de dados.

Código: PR-DRC-02/N-004	Página: 8/16
Versão: 00	Vigência: 17/10/2026
Doc. Aprovação: RES n.º 056/2024, 16/10/2024	

TÍTULO: GESTÃO DE INCIDENTES DE VIOLAÇÃO DE DADOS PESSOAIS

6.6.4 Independente do contato especificado pela Autoridade Nacional de Proteção de Dados - ANPD em relação a uma violação de dados, estes detalhes deverão constar no "Formulário de Incidente de Violação de Dados Pessoais", anexo III.

6.7 Aviso aos Titulares de Dados Pessoais

6.7.1 O Encarregado pelo tratamento de dados pessoais com o apoio do departamento jurídico, comunicará as violações de alto risco aos titulares de dados pessoais afetados, sem demora injustificada.

6.7.2 A comunicação com o Titular dos dados pessoais deve ser no formato estabelecido conforme o Anexo II, devendo conter no mínimo:

- a) A descrição da natureza dos dados pessoais afetados;
- b) As informações sobre os titulares envolvidos;
- c) A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comerciais e industriais;
- d) Os riscos relacionados ao incidente;
- e) Os motivos da demora, no caso de a comunicação não ter sido imediata;
- f) As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo;
- g) Identificar pontos de contato para maiores detalhes;
- h) Descrever possíveis consequências do incidente de violação de dados;
- i) Descrever medidas para endereçar o incidente de violação de dados, incluindo medidas adotadas para mitigar possíveis efeitos adversos do incidente de violação de dados.

6.7.3 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, sendo decidida pelo Encarregado de Dados e Alta Direção.

6.7.3.1 Podendo ser utilizado vários métodos de comunicação e o fornecimento de informações em formatos e idiomas alternativos, quando apropriado.

6.7.4 Se a violação afetar um grande volume de registros de titulares de dados pessoais, será decidido se a notificação pública será coletiva ou individual personalizada, levando em consideração a quantidade de recursos necessários e o prazo de atendimento.

Código: PR-DRC-02/N-004	Página: 9/16
Versão: 00	Vigência: 17/10/2026
Doc. Aprovação: RES n.º 056/2024, 16/10/2024	

TÍTULO: GESTÃO DE INCIDENTES DE VIOLAÇÃO DE DADOS PESSOAIS

6.8 Decisão de Não Notificação

6.8.1 Para os casos em que o risco para os titulares de dados é extremamente baixo, a Âmbar Energia Amazonas ficará isenta de notificações obrigatórias, nos seguintes casos

6.8.1.1 Violações de dados publicamente disponíveis;

6.8.1.2 Dados pessoais vazados, porém protegidos por uma chave que permanece confidencial e não pode ser verificada independentemente;

6.8.1.3 Perdas temporárias de acesso a dados pessoais;

6.8.1.4 Dados pessoais enviados acidentalmente para terceiros confiáveis em virtude de seu relacionamento com a Âmbar Energia Amazonas S.A.

6.8.2 Em casos de tomada de decisão de **Não** Notificação, a justificativa para esta decisão deverá ser documentada;

6.8.3 As circunstâncias e os efeitos de uma violação precisam ser continuamente monitorados pela companhia, à medida que surgirem novas informações, sendo necessário:

6.8.3.1 Emitir à Autoridade Nacional de Proteção de Dados - ANPD novas notificações ou atualização das existentes;

6.8.3.2 Enviar ao Titular dos Dados novas comunicações;

6.8.4 Todas as violações e as ações tomadas para responder às violações devem ser documentadas, mesmo que nenhuma notificação seja necessária, devendo ser registrada no "Formulário de Incidente de Violação de Dados", anexo III.

6.9 Pós Incidente

6.9.1 Após a correção de uma violação, o encarregado de dados deve se reunir com o Departamento de Tecnologia da Informação e demais departamentos envolvidos para discutir as medidas ou procedimentos de segurança que precisam ser implementados, afim de melhorar a segurança dos dados com base nas lições aprendidas;

6.9.2 O Encarregado de dados deverá examinar com atenção e minúcia sobre a resposta geral à violação e políticas ou protocolos atualizados, conforme necessário, para melhorar as reações futuras à eventuais novas violações.

Código: PR-DRC-02/N-004	Página: 10/16
Versão: 00	Vigência: 17/10/2026
Doc. Aprovação: RES n.º 056/2024, 16/10/2024	

TÍTULO: GESTÃO DE INCIDENTES DE VIOLAÇÃO DE DADOS PESSOAIS

7. DISPOSIÇÕES GERAIS

- 7.1 Toda e qualquer situação que não esteja contemplada nesta norma será analisada pela área gestora do processo e submetida à Diretoria Executiva;
- 7.2 As eventuais necessidades de alterações desta norma, com o objetivo de otimização dos processos ou sua atualização face às novas legislações sobre o assunto, devem ser submetidas à Diretoria Executiva, com as devidas justificativas;
- 7.3 Esta Norma e seus respectivos documentos encontram-se disponíveis na intranet ou, em caso de indisponibilidade, podem ser solicitadas ao Encarregado pelo Tratamento de Dados Pessoais da Âmbar Energia Amazonas;
- 7.4 Qualquer dúvida relativa ao incidentes de violação de Dados Pessoais e/ou este normativo, deverá ser encaminhada ao Encarregado pelo Tratamento de Dados Pessoais da Âmbar Energia Amazonas, por meio do e-mail lgpd@ambarenergia-am.com.br
- 7.5 O não cumprimento dos termos desta norma, sujeita o colaborador infrator às penalidades previstas nas normas internas e legislação em vigor;
- 7.6 Esta norma deve ser reavaliada a cada 02 (dois) anos, ou quando houver necessidade de revisão pela Área gestora do normativo, sendo sua vigência considerada a partir da data de sua aprovação.

8. ANEXOS

- 8.1. Anexo I – Notificação à Autoridade;
- 8.2. Anexo II – Notificação ao Titular;
- 8.3. Anexo III – Formulário de Incidente de Violação de Dados Pessoais.

TÍTULO: GESTÃO DE INCIDENTES DE VIOLAÇÃO DE DADOS PESSOAIS

ANEXO I – NOTIFICAÇÃO À AUTORIDADE

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
O(a) <<NomeEmpresa>> atua na qualidade de controlador de dados em relação à violação dos dados pessoais.

*[No caso de haver demora na comunicação. Neste ponto, a Lei Geral de Proteção de Dados - LGPD não fornece o prazo específico em horas, mas por analogia ao Regulamento Geral sobre a Proteção de Dados-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:

TÍTULO: GESTÃO DE INCIDENTES DE VIOLAÇÃO DE DADOS PESSOAIS

- [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]].

Código: PR-DRC-02/N-004	Página: 13/16
Versão: 00	Vigência: 17/10/2026
Doc. Aprovação: RES n.º 056/2024, 16/10/2024	

TÍTULO: GESTÃO DE INCIDENTES DE VIOLAÇÃO DE DADOS PESSOAIS

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,

TÍTULO: GESTÃO DE INCIDENTES DE VIOLAÇÃO DE DADOS PESSOAIS

ANEXO II – NOTIFICAÇÃO AO TITULAR

[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 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 abaixo indicados:

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

Atenciosamente,

TÍTULO: GESTÃO DE INCIDENTES DE VIOLAÇÃO DE DADOS PESSOAIS

ANEXO III – FORMULÁRIO DE INCIDENTE DE VIOLAÇÃO DE DADOS PESSOAIS

Parte 1 - Notificação de incidente de violação de dados pessoais	
Informações	DADOS A SEREM PREENCHIDOS PELA ÁREA
Data do incidente	
Data de descoberta do incidente	
Local do incidente	
Países afetados	
Nome do colaborador responsável por identificar os incidentes	
Detalhes de contato do colaborador responsável por identificar o incidente	
Breve descrição do incidente	
Número de titulares de dados pessoais afetados	
Dados pessoais foram colocados em risco? Favor detalhar	
Breve descrição das medidas adotadas após descoberta do incidente	
Preenchimento pelo Encarregado pela Proteção de Dados Pessoais	
Recebido por:	
Data de recebimento:	
Áreas a serem envolvidas:	
Data de notificação de envolvimento das demais áreas:	

TÍTULO: GESTÃO DE INCIDENTES DE VIOLAÇÃO DE DADOS PESSOAIS**PARTE 2 – AVALIAÇÃO DE SEVERIDADE**

Detalhes de sistemas, equipamentos, registros envolvidos no incidente	
Detalhes de quais dados foram alvo de violação (destruição, alteração indevida, compartilhamento indevido, etc.)	
Natureza/categoria dos dados alvo do incidente	
Volume de dados afetado pelo incidente	
Há salvaguarda desta informação? Caso não haja, esta violação pode ter feitos operacionais, legais e reputacionais para a Empresa?	
Quantos indivíduos foram afetados?	
Há dados pessoais sensíveis envolvidos?	
Há dados pessoais de crianças e adolescentes envolvidos?	
A Informação caso acessada por terceiros pode ser utilizada para fins ilícitos? Ex.: abertura de contas em banco.	

PARTE 3 – MEDIDAS TOMADAS

Medidas técnicas e legais adotadas	
Planos de ação recomendados	
Necessário notificação para Autoridade Nacional de Proteção de dados? De quais países?	
Necessário notificação para Titulares de Dados Pessoais?	
Necessário notificação para outras partes interessadas?	