PLANO DE RESPOSTA A INCIDENTES COM DADOS PESSOAIS

Última atualização: 09/08/23.

SUMÁRIO

1. INTRODUÇÃO:

Este Plano de Resposta a Incidentes com Dados Pessoais foi elaborado de acordo com a Lei nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD) e estabelece o procedimento para a gestão de situações após a identificação da ocorrência, ou mera suspeita, de um incidente de segurança da informação que envolva dados de pessoa natural identificada ou identificável, visando combater os riscos e minimizar os eventuais efeitos relacionados aos incidentes desta natureza.

2. OBJETIVOS:

O Plano de Resposta a Incidentes com Dados Pessoais tem o objetivo geral de orientar o Grupo A. Cândido Transportes a responder as situações de emergência e exceção, de forma documentada, formalizada, ágil e confiável, além de resguardar as evidências que possam auxiliar na prevenção de novos incidentes e no atendimento às exigências legais de comunicação e transparência.

Serão estabelecidas funções e responsabilidades individuais e de equipes, bem como, as medidas a serem adotadas para que o Grupo responda adequadamente a um incidente, sempre prezando pela integridade dos sistemas, processos, proteção de informações e privacidade dos seus titulares, possibilitando manter a confiabilidade dos seus produtos e serviços.

O presente Plano de Resposta a Incidentes com Dados Pessoais se aplica em qualquer caso de incidente envolvendo dados pessoais e deverá ser observado em conjunto com as demais políticas do Grupo por todos os colaboradores, estagiários, jovens aprendizes, prestadores de serviços, gestores, diretores e demais terceiros que por qualquer motivo tenham acesso ou venham a realizar operações de tratamento de dados pessoais, por força das atividades desempenhadas junto ao Grupo.

Este documento poderá sofrer atualizações de modo a refletir as melhores práticas em matéria de privacidade, proteção de dados pessoais e segurança da informação.

3. O QUE É UM INCIDENTE COM DADO PESSOAL?

Entende-se por incidente com dado pessoal toda e qualquer violação de segurança que, de forma acidental ou dolosa, enseje ou seja capaz de dar ensejo a destruição, perda, alteração, divulgação ou ao uso ou acesso não autorizados aos dados pessoais tratados pelo Grupo.

Um incidente pode ocorrer de forma maliciosa, ser o resultado de um erro humano, de falha nos sistemas que processam dados pessoais ou nos seus mecanismos de segurança. Isto pode incluir, por exemplo, o furto de um documento, o envio de um e-mail contendo dados pessoais para destinatários indesejados, tentativas de invasão a sistemas do Grupo ou outras ações, culposas ou dolosas.

Os incidentes podem ser de vários tipos, como por exemplo:

- **Vazamento de Dados Pessoais:** é o incidente no qual dados pessoais são indevidamente expostos e disponibilizados, por meios físicos ou digitais, para um número indeterminado de pessoas, no Brasil ou em qualquer país.

- **Negação de Serviço:** é o incidente no qual o acesso (lógico ou físico) a um sistema que armazene dados pessoais é prejudicado ou impossibilitado, de forma que a integridade dos dados pessoais (existência e/ou veracidade) pode ser comprometida permanentemente, dada a indisponibilidade do acesso.

- **Acesso não Autorizado:** é o incidente no qual o acesso (lógico ou físico) a um sistema que possua dados pessoais é tentado ou obtido, sem que se tenha a devida autorização. Ou seja, considera-se acesso não autorizado qualquer acesso cuja permissão para conexão, leitura, gravação, autenticação, modificação, eliminação ou criação não tenha sido concedida.

- **Uso Inapropriado:** é o incidente no qual há a violação das políticas de uso de dados, informações e sistemas do Grupo.

4. PAPÉIS E RESPONSABILIDADES:

Cada setor do Grupo tem responsabilidades quando da ocorrência ou mera suspeita de um incidente com dados pessoais, conforme descrito a seguir.

4.1 OBRIGAÇÕES DE TODOS OS SETORES:

- Comunicar imediatamente ao Comitê de Privacidade e Proteção de Dados Pessoais sobre a ocorrência ou a mera suspeita de um incidente com dados pessoais;

- Cumprir rigorosamente a Política de Privacidade Interna e este Plano de Resposta a Incidentes com Dados Pessoais, contribuindo para a mitigação dos riscos;

- Participar de treinamentos e programas de conscientização oferecidos pelo Grupo.

4.2 OBRIGAÇÕES DO COMITÊ DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS:

- Atuar para detectar e corrigir os eventuais incidentes com dados pessoais;

- Buscar estabelecer uma cultura organizacional preocupada com a segurança da informação e com o sigilo dos dados pessoais;

- Adotar as medidas necessárias para prevenir incidentes e minimizar o impacto de seus efeitos.

Cumpre citar com detalhes as formas como alguns setores estratégicos irão colaborar:

- **Diretoria:** Avalia a situação decorrente do incidente, sendo responsável pela tomada de decisão final.

- **LGPD e Compliance:** Avalia a situação decorrente do incidente, auxiliando e indicando a diretoria as medidas apropriadas que deverão ser tomadas, com base nas evidências apresentadas pelos responsáveis diretamente ligados ao caso.

- **Jurídico:** Avalia a situação decorrente do incidente e elabora parecer sobre o caso, a fim de auxiliar o DPO do Grupo.

- **Gestor:** Avalia a situação decorrente do incidente que envolver o seu setor respectivo, disponibilizando as evidências necessárias para elucidar o caso e o DPO do Grupo.

- **Tecnologia da Informação (TI):** Auxilia na resolução das questões técnicas relacionadas ao incidente e na investigação da origem e das razões para a ocorrência.

- **Recursos Humanos:** Auxilia na comunicação do Grupo com os seus colaboradores e/ou clientes sobre o incidente, incluindo o esclarecimento sobre o ocorrido e as ações tomadas para mitigar os efeitos e prevenir novos incidentes semelhantes no futuro, sempre de acordo com as orientações repassadas pelo Comitê de Privacidade e Proteção de Dados Pessoais.

5. DETECÇÃO DO INCIDENTE:

Detectar o incidente de forma rápida e eficiente é essencial. Desta forma, todos devem atentar-se, principalmente aos sinais mais comuns, como invasões de rede, perda ou furto de documentos, arquivos ou dispositivos, phishing (técnica de engenharia - tentativa de fraude), malware (software malicioso), instabilidades sistêmicas, entre outros.

Uma vez detectado o incidente ou detectada a mera suspeita de um incidente, deve-se comunicar imediatamente ao Comitê de Privacidade e Proteção de Dados Pessoais, através do endereço de e-mail do Encarregado pelo Tratamento de Dados Pessoais (DPO) do Grupo: dporn@acandidotransportes.com.br.

Na medida do possível, esta comunicação inicial deverá conter: a hora e a data em que a suspeita do incidente foi descoberta, os tipos de informações/dados envolvidos, a causa e a extensão do incidente (se souber), o contexto do ocorrido, bem como qualquer informação adicional que sirva para facilitar o entendimento do incidente, suas causas e possíveis consequências.

A comunicação sobre o incidente ou a mera suspeita é vital para o Grupo. Assim, caso um colaborador suspeite ou tenha conhecimento de um incidente e não o comunique, estará sujeito as sanções disciplinares, sendo avaliada a gravidade do incidente e a comprovação de eventual negligência.

5.1 PRIORIZAÇÃO DO INCIDENTE E PROCEDIMENTO PARA RESPOSTA:

Identificado o incidente, é necessário priorizá-lo conforme o nível de risco oferecido aos titulares dos dados pessoais eventualmente afetados e a gravidade da ocorrência.

O impacto do incidente deve ser aferido da seguinte forma:

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		

VOLUME DE DADOS PESSOAIS EXPOSTOS	
Criticidade	Descrição
Alto	Volume de dados pessoais afetado superior a 10% da base de dados do controlador.
Médio	Volume de dados pessoais afetado inferior a 10% e superior a 2% da base de dados do controlador.
Baixo	Volume de dados pessoais afetado inferior a 2% da base de dados do controlador.

SENSIBILIDADE DOS DADOS PESSOAIS AFETADOS	
Criticidade	Descrição
Alta	Dados pessoais de crianças/adolescentes, dados pessoais sensíveis ou que possam gerar discriminação ao titular.
Média	Dados pessoais imediatamente identificáveis (exemplos: nome, e-mail, CPF, endereço), combinados, ou não, com informações comportamentais (exemplos: histórico de atividades, preferências).
Baixa	Dados anonimizados, dados pessoais pseudonimizados (desde que a chave de desanonimização também não tenha sido comprometida), dados pessoais de difícil identificação (exemplo: IP).

De acordo com os parâmetros definidos acima, o Comitê de Privacidade e Proteção de Dados Pessoais deverá tomar as seguintes ações, simultaneamente ou, quando não for possível, em rápida sucessão:

1º: Comunicação formal a todos os membros do Comitê de Privacidade e Proteção de Dados Pessoais, que irão trabalhar na resolução do incidente;

2º: Tomar as medidas imediatas para minimizar os efeitos causados pelo incidente, promovendo a sua rápida correção e, se a correção não for possível de forma imediata, deve adotar as medidas temporárias para minimização de riscos;

3º: Comunicar aos setores envolvidos no incidente, que deverão estar à disposição do Comitê de Privacidade e Proteção de Dados Pessoais, devendo atender prontamente a qualquer solicitação;

4º: Uma vez que as medidas de resolução sejam tomadas, o incidente deverá ser documentado, conforme modelos disponibilizados no Anexo I deste Plano de Resposta a Incidentes com Dados Pessoais;

5º: O Comitê de Privacidade e Proteção de Dados Pessoais deverá reunir-se para analisar o incidente, discutir melhorias de processos e aperfeiçoar as ações, evitando reincidência semelhante no futuro, devendo esta reunião ser transcrita em ata que será devidamente arquivada;

6º: Após a resolução do incidente, poderá ser realizado um treinamento interno de conscientização, destacando as medidas preventivas que deverão ser adotadas pelo Grupo para evitar a reincidência.

5.2 COMUNICAÇÃO DO INCIDENTE À ANPD:

Em cumprimento à LGPD e ao Decreto nº 9.936/2019, o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. A avaliação sobre quais incidentes são materialmente relevantes deverá ser realizada pelo Comitê de Privacidade e Proteção de Dados Pessoais.

Caso o incidente possa acarretar risco ou dano relevante aos titulares e a comunicação à Autoridade Nacional de Proteção de Dados (ANPD) seja determinada pela diretoria do Grupo, o Encarregado pelo Tratamento de Dados Pessoais (DPO), irá elaborar a documentação aplicável, de acordo com o §1º do Art. 48 da LGPD, contendo:

- A descrição da natureza dos dados pessoais afetados (dados sensíveis, dados de criança, dados cadastrais, etc);
- As informações sobre os titulares envolvidos (número total, a relação dos titulares afetados e o país de residência de cada um deles);
- 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.

Na hipótese de o Comitê de Privacidade e Proteção de Dados Pessoais entender como necessária a comunicação sobre o incidente aos titulares dos dados pessoais afetados, após a autorização da diretoria, o Encarregado pelo Tratamento de Dados Pessoais (DPO), irá desenvolver a mensagem de comunicação, priorizando: a descrição dos fatos ocorridos, as medidas já tomadas pelo Grupo para minimizar os impactos, as eventuais medidas que possam ser adotadas pelos próprios titulares dos dados pessoais para mitigar riscos e os canais de comunicação para sanar dúvidas. Antes de ser veiculada pelo setor de Recursos Humanos, a mensagem deverá ser devidamente revisada e aprovada pela diretoria do Grupo.

6. DISPOSIÇÕES FINAIS:

Em caso de dúvidas, comentários e/ou sugestões relacionadas a este Plano de Respostas a Incidentes com Dados Pessoais, entre em contato com o Encarregado pelo Tratamento de Dados Pessoais (DPO) do Grupo, através do seguinte endereço de e-mail: dporn@acandidotransportes.com.br.

ANEXO I

Estão disponíveis abaixo os modelos que deverão ser utilizados pelo Grupo com o objetivo de documentar um eventual incidente com dados pessoais, auxiliando no esclarecimento e nos registros das informações.

- **DESCRIÇÃO DO INCIDENTE:**

DESCRIÇÃO DO INCIDENTE		
EMPRESA:		
RESPONSÁVEL PELO PREENCHIMENTO:		
DOCUMENTO Nº:		
DATA: _____/_____/_____.		
Nº	**PERGUNTA**	**RESPOSTA**
1	Em qual data o incidente foi descoberto?	
2	Qual o nome e o e-mail da pessoa que reportou o incidente?	
3	Breve descrição do incidente.	
4	O incidente ainda está ocorrendo?	
5	O que foi ou está sendo feito para cessar o incidente?	
6	Setor em que ocorreu ou está ocorrendo o incidente?	
7	No incidente, houve o comprometimento de dados pessoais e/ou dados pessoais sensíveis?	
8	Há possibilidade deste incidente comprometer a confidencialidade, integridade ou disponibilidade de dados pessoais e/ou sensíveis?	
9	Quais os dados pessoais envolvidos? Detalhar.	
10	Quais os dados pessoais sensíveis envolvidos? Detalhar.	

11	Quem são os titulares envolvidos? Se possível, anexar lista com o nome e meio de comunicação (e-mail ou número de celular).	
12	Há dados pessoais e/ou sensíveis de menores de idade?	
13	Quantos titulares estão envolvidos no incidente?	
14	Há algum indício de que estes dados pessoais e/ou sensíveis foram ou podem ser utilizados ilegalmente ou inadequadamente por terceiros?	
15	Estes dados pessoais e/ou sensíveis ficaram ou estão disponíveis para terceiros em algum lugar? Quais? Por quanto tempo?	
16	É possível rastrear estes dados pessoais e/ou sensíveis?	
17	Ainda é possível reverter o incidente?	
18	Qual a causa do incidente? Detalhe.	
19	Foi identificado algum responsável pelo incidente?	
20	Informações Adicionais	

- **CONCLUSÃO DO INCIDENTE:**

CONCLUSÃO DO INCIDENTE		
EMPRESA:		
RESPONSÁVEL PELO PREENCHIMENTO:		
DOCUMENTO Nº:		
DATA: _____/_____/_____.		
Nº	**PERGUNTA**	**RESPOSTA**
1	O incidente foi sanado/resolvido?	
2	Os dados foram recuperados? Todos?	
3	Houve a identificação do responsável?	
4	Houve a identificação da causa do incidente?	
5	Quais medidas internas foram tomadas para que novos incidentes deste tipo não voltem a ocorrer?	
6	O incidente foi reportado para a autoridade cível e/ou criminal? Em caso positivo, informe a data e o número do processo.	
7	O incidente foi reportado para os titulares dos dados?	
8	O incidente foi reportado para a Autoridade Nacional de Proteção de Dados (ANPD)? Em caso positivo, informe a data e o número do processo.	
9	O incidente foi reportado para outra entidade/órgão? Qual?	
10	Quais foram os efeitos do incidente para o Grupo?	
11	As políticas internas referentes ao gerenciamento do incidente foram eficazes?	

12	As políticas internas referentes ao gerenciamento do incidente demandam alguma alteração? Qual?	
13	Informações Adicionais	