Política de Resposta à Incidente de Segurança

(Plano de Resposta)

I – Apresentação:

A Contabilidade Waltrick Ltda ratifica perante a todos que a segurança da informação e programa de governança são prioridade entre seus trabalhadores, no entanto, mesmo com a adoção de inúmeras medidas preventivas cabíveis, todos sabemos que existe um risco residual, ou seja, apesar de todas as ações preventivas, o Escritório está sujeito a um incidente de segurança em dados pessoais.

Através desta Política de Incidente, tornaremos publica quais serão as nossas ações caso este evento ocorra.

II – O que é um incidente de segurança para a LGPD?

Para fins legais, o incidente de segurança é o "o acontecimento indesejado ou inesperado que seja hábil a comprometer a segurança dos dados pessoais, de modo a expô-los a acessos não autorizados e a situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito" (JIMENE; TAMER, 2020).

A perda de um *pen drive*, o furto de um *notebook*, a interrupção de acesso a um sistema são situações, do ponto de vista técnico, podem ser consideradas incidentes de segurança, uma vez que a informação corporativa estará exposta a uma ameaça.

II - Diante de algum incidente, as ações serão:

1 - Cumprindo a regra prevista no artigo 48 da Lei 13709, o Controlador comunicará a ocorrência de incidente de segurança para a ANPD (Agencia Nacional de Proteção de Dados). Esta comunicação também será feita ao titular dos dados pessoais;

2 - Elaboração e aplicação imediata de medidas técnicas e jurídicas que visem conter os riscos legais, iniciando com a identificação dos dados vinculados ao incidente.

3 - Analisar, cautelosa e detalhadamente, quais foram as informações envolvidas no episódio;

4 – Elaborar uma reunião com o Grupo de Trabalho, para a apuração da gravidade dos danos, e número de titulares envolvidos.

5 – Elaborar um estudo técnico e de investigação detalhada que aponte as falhas de segurança que permitiram ou contribuíram com a ocorrência do incidente";

6 – Pesquisar e identificar algum elemento de prova importante para certificar a origem do episódio ou sua autoria.

7 **-** Descobrir as causas do incidente e seus responsáveis, renovando o seu compromisso em tratar o este incidente e minimizar que novos incidentes ocorram.

8 - Uma vez localizado algum registro eletrônico (números de *IP*, datas e horas) o Escritório ajuizará medidas judiciais cabíveis.

9 - Registrar a ocorrência, através da lavratura de um Boletim de Ocorrência ou pedir a Instauração de Inquérito Policial.

10 - Elaboração de um relatório circunstanciado que detalhe os resultados identificados, a fim de que a empresa adote as medidas necessárias para a prevenção de novos episódios envolvendo vulnerabilidades tecnológicas.

Esse documento tem como objetivos:

- Permitir que o incidente e as providências adotadas fiquem registrados. Com isso, poderá a organização demonstrar, sobretudo para a fiscalização administrativa ou de procedimento extrajudicial (inquérito civil público) ou judicial (coletivo ou individual do titular do dado pessoal) que respondeu ao incidente;
- Gerar um documento para a organização no sentido de viabilizar, futuramente, que essa consiga avaliar os episódios que teve no passado e traçar uma linha evolutiva ou gráfica em direção aos altos níveis de maturidade em privacidade ou, se não for o caso, para que a organização identifique as possíveis causas de estagnação ou queda nos patamares de privacidade. Essas linhas históricas documentadas também serão importantes como provas positivas no caso de fiscalização, mencionado acima; e,
- A documentação do incidente e das providências adotadas permite e facilita, no caso de apuração de falhas, que o programa de privacidade seja revisado e alterado, se for o caso.

Última Atualização: 14/12/2021.