# Iara Melo: Incidente de segurança com dados pessoais

18/10/2023

Um incidente de segurança é sempre um momento delicado para qualquer organização, dada a ameaça de impactos nos negócios. Com o advento da Lei Geral de Proteção de Dados (LGPD) — Lei 13.709/2018 —, a dinâmica desses incidentes, especialmente quando envolvem dados pessoais, tornou-se ainda mais complexa.


É crucial envolver o encarregado para uma análise focada na proteção de dados pessoais e avaliar a necessidade de notificar a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares afetados. Medidas mitigatórias dos riscos aos quais os titulares possam estar expostos também devem ser implementadas, além de outras ações.

Ao optar por notificar a ANPD, é preciso analisar uma série de consequências administrativas e jurídicas em um espaço de tempo reduzido. Até a data de redação deste artigo, a ANPD recomendava que a comunicação fosse feita em até dois dias úteis da ciência do fato.

Nosso objetivo ao redigir este artigo é auxiliar aqueles que nunca passaram por uma situação de incidente de segurança envolvendo dados pessoais, a se imaginar nos cenários normalmente vivenciados. É claro que cada empresa possui sua própria estrutura, processos e ferramentas. Por isso, rogamos ao leitor que não se apegue a detalhes específicos aqui narrados, mas realize o exercício de se imaginar na situação com o objetivo de identificar eventuais pontos de melhoria em seus próprios processos de resposta a incidentes.

**Terça-feira – 20h**
O encarregado de dados entra em contato com o escritório jurídico pelo WhatsApp, informando sobre um incidente em sua infraestrutura detectado por meio da ferramenta DLP *(Data Loss Prevention)*. O incidente possivelmente comprometeu uma base de dados com informações de clientes pessoa física da empresa. Embora a equipe de SOC tenha contido rapidamente o incidente, alguns dados parecem ter sido afetados.

**Terça-feira – 20h45**
Uma videoconferência é realizada com a equipe de TI, Jurídico, Operações, Encarregado e o escritório de advocacia, resultando em um plano de ação:

— *TI:* Continuar a investigação para determinar quais dados foram afetados. A base de dados comprometida parece conter informações cadastrais e de saúde de clientes, mas a extensão do incidente ainda não é clara.

— *Jurídico:* Antecipar-se ao pior cenário possível, solicitando pareceres sobre possíveis impactos legais nos âmbitos do direito do consumidor, direito civil e direito criminal.

— *Operações:* Apesar dos backups terem sido estabelecidos rapidamente, a política da empresa preconiza que se conduza um diagnóstico de impacto para avaliar os efeitos do vazamento de informações confidenciais de cunho operacional da empresa (*impact assessment*).

— *Comunicação:* Envolvimento da equipe de comunicação para redigir um comunicado interno, destinado aos colaboradores, informando sobre o incidente.

— *Encarregado:* Início da redação de um relatório detalhado sobre o incidente e uma análise de riscos aos titulares afetados, considerando o pior cenário possível.

**Quarta-feira – 8h**
As equipes iniciam a execução do plano de ação acordado na noite anterior; O encarregado fica responsável por preparar uma apresentação executiva para o CEO, agendada para as 17:00 deste mesmo dia.

**Quarta-feira – 9h20**
A equipe de comunicação compartilha com o jurídico o primeiro rascunho da comunicação interna. O documento tem como objetivo informar os colaboradores superficialmente sobre o incidente e esclarecer que a equipe técnica está apurando o ocorrido. No comunicado, os colaboradores são orientados a não comentar o incidente com pessoas externas à organização e a buscar a equipe de comunicação em caso de dúvidas. O documento é revisado pelo jurídico e compartilhado com o encarregado às 10:30 da quarta-feira para inclusão na apresentação ao CEO.

**Quarta-feira – 12h30**
A equipe de TI confirma que aproximadamente 4.000 titulares tiveram seus dados pessoais afetados, representando 10% da base de dados da empresa. Dados de saúde e dados cadastrais de clientes pessoa física foram comprometidos.

**Quarta-feira – 14h**
O jurídico recebe os pareceres sobre riscos de responsabilidade civis, consumeristas e criminais. O encarregado conclui a análise de risco aos titulares e verifica os aspectos regulatórios (probabilidade de sanção administrativa).

**Quarta-feira – 15h**
Uma reunião entre jurídico e encarregado é realizada para discutir cenários possíveis e suas consequências (notificar ou não a ANPD e os titulares). A recomendação de ambos é prosseguir

com a notificação à ANPD. Todos estes dados e recomendações são incluídos na apresentação executiva para o CEO.

**Quarta-feira – 17h**
De acordo com as informações apresentadas, após a reunião com a diretoria, o CEO decide notificar a ANPD e os titulares. A equipe começa a preparar um novo plano de ação, incluindo:

— *TI:* Coleta de evidências técnicas, documentação técnica para a ANPD e apuração da lista de titulares afetados.

— *Encarregado:* Redação da comunicação à ANPD e aos titulares.

— *Comunicação:* Veiculação do comunicado interno destinado aos colaboradores (aprovado em reunião). Planejamento para atender a solicitações de informações adicionais de titulares (criação de canal próprio, com e-mail *call center* para atender titulares afetados).

**Quinta-feira – 9h – 16h**
O dia acaba sendo completamente dedicado ao refinamento da comunicação à ANPD. Encarregado e jurídico trabalham em conjunto, enquanto TI fornece a documentação técnica que será acostada ao processo administrativo. Devido à complexidade em apurar a lista de titulares afetados com granularidade, as equipes optam por protocolizar uma comunicação parcial com as informações disponíveis até a referida data.

**Quinta-feira – 17h35**
Protocolo da comunicação de incidente no sistema da ANPD dentro do prazo sugerido de dois dias úteis.

Apesar do progresso até o momento, o trabalho ainda não acabou: as informações devem ser apuradas pela equipe de TI com maior granularidade para que a comunicação complementar seja apresentada à ANPD em até 30 dias. A comunicação aos titulares também deve ser realizada o mais breve possível, de forma a mitigar riscos.

As equipes decidem complementar o plano de ação e realizar reuniões semanais para acompanhar o progresso.

Depois de dois dias altamente dedicados ao incidente, as equipes finalmente conseguem voltar às suas atividades cotidianas. Contudo, ainda é necessário guardar o foco nas tarefas relacionadas ao incidente que ainda continuam no plano de ação.

Diversas lições foram aprendidas durante este período intenso, como a importância de um plano de resposta a incidentes bem estruturado e a importância de manter contratos guarda-chuva com empresas pré-selecionadas para atuar em situações de incidente com maior agilidade. Devido à repercussão do ocorrido na diretoria, a empresa passou a considerar a contratação de um seguro cibernético para o próximo exercício financeiro.

Esses são apenas alguns aprendizados valiosos que uma empresa pode ter em situações de incidente, reforçando a necessidade de preparação prévia. Ressaltamos que o verdadeiro valor de um plano de resposta a incidentes somente será apurado pela quantidade de informações e

processos relevantes que ele fornecerá à equipe em momentos de crise.

Por fim, lembramos que o cenário apresentado neste artigo é fictício, embora possa se assemelhar com diversas situações da vida real.

Fonte: https://conjur.jumps.com.br/2023-out-18/iara-melo-incidente-seguranca-dados-pessoais2/