A importância da gestão de fornecedores para o cumprimento da LGPD

21/02/2024

De acordo com o relatório Global Cybersecurity Outlook 2024, publicado em janeiro pelo World Economic Forum [1], 41% das organizações que sofreram um incidente de segurança nos últimos 12 meses afirmam que ele foi causado por terceiros.

A pesquisa "*Close Encounters of the Third (and Fouth) Party Kind*", publicada em janeiro de 2023 pela *Security Scorecard*, por sua vez, aponta entre os seus achados que 98% das organizações têm relacionamento com pelo menos um terceiro que sofreu uma violação de segurança nos últimos dois anos; e que para cada fornecedor terceirizado em sua cadeia de suprimentos, as organizações normalmente têm relacionamentos indiretos com 60 a 90 vezes esse número de terceiros [2].

Os números apresentados são alarmantes e apontam para a necessidade de uma maior preocupação das organizações em relação aos seus fornecedores e parceiros. Sob a perspectiva da Lei Geral de Proteção de Dados (LGPD), os fornecedores com os quais a empresa se relaciona também atuam como agentes de tratamento dos dados pessoais, e caso, no exercício das atividades de tratamento, violem a legislação e/ou causem danos a titulares, a contratante pode vir a ser responsabilizada.

Por exemplo, caso a empresa A contrate uma empresa B para armazenar os dados pessoais de seus clientes, e a empresa B divulgue indevidamente os dados pessoais desses titulares e/ou não tome as medidas de segurança da informação necessárias para garantir a proteção dessas informações, a empresa A poderá ser sancionada pela Autoridade Nacional de Proteção de Dados Pessoais (ANPD) – a depender da sanção, pode, inclusive, inviabilizar a atividade-fim da empresa –, ou, por exemplo, ser condenada em âmbito judicial a indenizar os titulares envolvidos.

Vulnerabilidade do Brasil

Fato é que os incidentes de segurança têm sido cada vez mais comuns, principalmente no que concerne a ataques cibernéticos – como, por exemplo, o ataque de *ransomware,* que tem a capacidade de paralisar a operação da empresa e de seus parceiros por dias. A propósito, segundo relatório da Trend Micro, empresa multinacional de cibersegurança, divulgado em 2023, o Brasil é o segundo país mais vulnerável a ataques cibernéticos. Foram 85,6 bilhões de ameaças bloqueadas, somente no primeiro semestre daquele ano [3].

Esse cenário reflete os riscos relacionados à segurança dos dados e reforça a responsabilidade dos agentes envolvidos no tratamento de dados pessoais, que são legalmente responsáveis por garantir a privacidade e o correto tratamento dos dados pessoais.

Procedimentos

Nesse contexto, as empresas devem buscar a conformidade com a LGPD em todos os seus processos de tratamento de dados pessoais, bem como manter todas as suas documentações internas e contratos adequados. Porém, não basta olhar somente para dentro da empresa; é igualmente essencial assegurar que os seus parceiros e fornecedores também estejam em bom nível de maturidade em relação às medidas de proteção de dados.

Desse modo, a gestão eficaz dos riscos associados aos terceiros na cadeia de suprimentos torna-se uma prioridade incontestável para garantir a proteção dos dados e a segurança das operações empresariais.

A governança no processo de contratação de fornecedores deve perpassar por todas as etapas do relacionamento, desde o primeiro contato — que envolve a avaliação dos canais e sistemas utilizados, dos tipos de dados coletados e das atividades exercidas pela empresa —, passando pela análise apurada dos sistemas e medidas de segurança adotados durante a vigência do contrato, até a avaliação de condutas tomadas em caso de incidentes de segurança, em casos mais críticos.

O passo a passo da gestão

Então como fazer uma gestão eficaz dos fornecedores? É preciso que a organização estabeleça um processo de relacionamento com seus fornecedores que obedeça a três principais etapas:

1. Inicialmente, é necessário apurar e compreender os riscos que precisarão ser gerenciados nas atividades envolvidas na relação com o fornecedor. Compreendido isso, é essencial realizar uma diligência prévia (*due dilligence*) com o fornecedor em potencial, oportunidade em que será avaliado o nível de maturidade no que diz respeito à segurança da informação e proteção de dados pessoais. A título de exemplo, pode ser solicitado ao fornecedor que:

a. Apresente políticas de segurança e de tratamento de dados pessoais implementadas;

b. Indique os sistemas utilizados e se estes contam com as medidas de segurança necessárias para garantir a proteção dos dados pessoais tratados;

1. Indique as medidas de segurança da informação utilizadas pelo fornecedor para verificar se são satisfatórias.

2. Selecionado o fornecedor, é preciso estabelecer contratualmente as suas responsabilidades e obrigações, considerando o contexto da relação. Já durante a vigência do contrato, é importante monitorar a execução das atividades, acompanhar periodicamente as atualizações das

documentações e das medidas de segurança do fornecedor, além do cumprimento das novas exigências legais e regulatórias.

3. Por fim, ao final do contrato, é necessário garantir que a devolução ou o descarte dos dados pessoais tratados pelo fornecedor seja realizado de forma adequada e segura, bem como a remoção de acessos, se for o caso.

É importante destacar que para que todas as etapas mencionadas sejam devidamente implementadas é necessária a correta preparação da equipe, que, além de se conscientizar e se submeter a treinamentos sobre tratamento de dados pessoais, deve estar familiarizada com a gestão de contratos sob a ótica da proteção de dados e segurança da informação.

Conclusão
Em suma, a gestão do processo de contratação de fornecedores, o monitoramento e acompanhamento durante a vigência dos contratos contribuem significativamente para a mitigação de riscos de segurança da informação, para o cumprimento da legislação e para a preservação dos dados pessoais dos titulares, além de proporcionarem segurança jurídica a todos os envolvidos e, consequentemente, contribuírem para o sucesso empresarial.

Notas:

[1] Disponível em: https://cdn-conjur.s3.amazonaws.com/uploads/2024/02/WEF_Global_Cybersecurity_Outlook_2024.pdf

[2] Disponível em: https://cdn-conjur.s3.amazonaws.com/uploads/2024/02/Research-Close-Encounters-Of-The-Third-And-Fourth-Party-Kind.pdf

[3] Disponível em: https://abes.com.br/brasil-e-o-segundo-pais-mais-vulneravel-a-ataques-ciberneticos-segundo-relatorio-da-trend-micro

Fonte: https://conjur.jumps.com.br/2024-fev-21/a-importancia-da-gestao-de-fornecedores-para-o-cumprimento-da-lgpd/