

Privacidade de dados e Riscos Cibernéticos

, AGORA E LEI!

Empresas são responsáveis pela proteção e privacidade dos dados de seus clientes





Súmario

Como a Lei afeta meu negócio?0
O que eu preciso fazer par estar em conformidade com a nova lei?
A quais riscos o meu negócio está exposto?
Ameaças digitais0
Conte com um Seguro de Riscos Cibernéticos0
Conheça as principais situações e as coberturas AIG0
Quer saber mais?1



VOCÊ SABIA?

A Lei Geral de Proteção de Dados Pessoais define regras para o uso, proteção e transferência de dados pessoais coletados pelas empresas.

O texto oferece ao cidadão brasileiro mais controle sobre suas informações pessoais: exige consentimento explícito para coleta e uso dos dados, tanto pelo poder público quanto pela iniciativa privada, e exige que as empresas apresentem opções para o usuário visualizar, corrigir e excluir esses dados.

Estão sujeitos às penalidades da lei – que variam de advertências a multas diárias de até R\$ 50 milhões – os negócios que registram informações dos clientes sem sua autorização, ou que os repassem, armazenem sem necessidade comprovada, ou que tenham esses dados vazados de alguma forma.

Apesar de ainda tramitar pela Câmara dos Deputados e passar pela sanção presidencial, a decisão estabelece que a legislação passará a vigorar em janeiro de 2021.

Ou seja, as empresas ganham um pouco mais de tempo para se adequar à nova legislação.

COMO A LEI AFETA MEU **NEGÓCIO?**

A Lei de Proteção de Dados Pessoais vale para todas as empresas que, de alguma forma, coletam, armazenam e tratam informações de clientes no Brasil, independente de seu segmento de atuação, porte ou faturamento.

Por isso, o nível de exposição da empresa e o eventual vazamento de dados podem comprometer a saúde financeira e continuidade de seus negócios, principalmente de PMEs.

Ou seja, das startups a grandes empresas já consolidadas, passando por pequenos comércios que armazenam informações de clientes como CPF, RG, Telefone, Endereço, etc., todas devem contar com medidas para proteção dos dados dos clientes.

O QUE EU PRECISO FAZER PARA **ESTAR EM CONFORMIDADE COM** A NOVA LEI?

É preciso que as empresas façam uma análise interna de seus processos, sistemas e ferramentas para avaliar como os dados pessoais de seus clientes/usuários são tratados, reforçando a proteção, com responsabilidade e transparência.

Os Especialistas em Riscos Cibernéticos da AIG Seguros indicam os passos a sequir:

- Procure identificar onde, como e quando sua empresa faz a coleta de dados de seus clientes.
- Seu negócio online possui Termo de Uso e Termo de Confidencialidade atualizados e transparentes? É importante que o cliente esteja ciente e aceite tais termos.
- Como é o armazenamento desses dados? Estão seguros?
- Conte com o apoio de profissionais especializados em Segurança da Informação para auxiliá-lo a verificar a atualização de seus programas de antivírus, firewall, navegador e outras plataformas digitais que utiliza.
- Quem acessa os dados de seus clientes? Qualifique sua equipe para que todos estejam inteirados sobre os procedimentos de segurança.
- Já tem mapeados os principais riscos de vazamentos de dados que sua empresa pode sofrer? Esteja preparado.



A QUAIS RISCOS O MEU **NEGÓCIO ESTÁ EXPOSTO?**

Mundialmente, os segurados AIG relatam os seguintes ataques cibernéticos como os mais frequentes:

- · Servidores externos com acesso remoto combinado a senhas frágeis. Isso oferece uma oportunidade para a entrada de programas maliciosos (malware) ou sequestro de dados (ransomware). O acesso remoto deve ser controlado cuidadosamente.
- · Falta de conscientização do usuário, permitindo o acesso de hacker por meio de phishing. Por desconhecimento, o usuário pode acessar um email contendo um link malicioso. Ao clicar, é fisaado (daí o termo phishing) ao ser direcionado a uma página falsa que pode coletar seus dados ou expor os dados de acessos do usuário ao hacker. O usuário deve estar sempre alerta e perguntar-se: "este email é de remetente confiável?". Caso contrário, ele deve informar a equipe de Segurança da Informação da empresa para que sejam tomadas as devidas medidas.
- Procedimentos frágeis de login. O risco de phishing é diminuído ao contar com processos mais robustos de acesso aos sistemas, como o uso de duplo fator de autenticação. Esse procedimento deve ser adotado como um padrão mínimo de segurança por usuários de empresas com acesso a informações sensíveis, como dados pessoais e bancários de funcionários e de clientes.



AMEAÇAS DIGITAIS

Outro dado preocupante é que, dos sinistros de riscos cibernéticos registrados pela AIG nos últimos cinco anos, 45% foram em 2018, mais que o dobro do registrado em 2016 e 2017, o que mostra o crescimento desse tipo de ocorrência.

A principal porta de entraga dos ataques são os emails empresariais, daí a importância de conscientizar todos os funcionários, não somente os especialistas em Tecnologia da Informação, sobre as melhores práticas de segurança.

Serviços financeiros, serviços profissionais e varejo são alguns dos segmentos mais afetados no mundo todo, assim como saúde e logística. No entanto, não há setor imune às ameaças digitais ou vazamento de dados, sejam eles intencionais ou causados por acidente. E essa realidade é no mundo todo, inclusive no Brasil. Estudo recente publicado pela empresa de segurança na rede Fortinet, registrou mais de 9,7 bilhões de tentativas de ataques cibernéticos na América Latina, só nos primeiros 4 meses de 2020, sendo 1,6 bilhão de ataques somente no Brasil.



CONTE COM UM SEGURO **DE RISCOS CIBERNÉTICOS**

Segundo a empresa especializada em Segurança da Informação, Kaspersky, o Brasil é hoje o quarto país mais atacado por hackers no mundo. Por isso, o Seguro de Riscos Cibernéticos atua hoje como uma camada extra de protecão, com coberturas específicas para diferentes situações em que os dados de sua empresa são expostos a terceiros.

Coberturas

O Seguro de Riscos Cibernéticos da AIG oferece ampla cobertura em caso de vazamento de dados armazenados por uma empresa, inclusive contempla o pagamento de multas, como será agora exigido pela nova legislação. Outras coberturas do Seguro de Riscos Cibernéticos AIG também são os custos de notificação da empresa a seus clientes, e responsabilidade pela segurança de dados, ato, erro ou omissão que resulte na divulgação dessas informações devido a uma violação de segurança, e ressarcimento por lucros cessantes.



[fonte: https://cybermap.kaspersky.com/stats/]

CONHEÇA AS PRINCIPAIS SITUAÇÕES E AS COBERTURAS AIG

DESTRUIÇÃO DE BASE DE DADOS

(Interno ou externo)

Consequências possíveis: Prejuízo operacional e financeiro da empresa

Transferência de risco e resposta da apólice: Custos e despesas para determinar se os dados eletrônicos podem ser ou não restaurados, restabelecidos ou recriados; ou restaurar, restabelecer ou recriar os dados eletrônicos, quando possível

VAZAMENTO DE INFORMAÇÕES (Interno ou externo)

Consequências: Perda de confiança dos clientes, impacto negativo na reputação da organização

Transferência para a Apólice: Gastos relacionados com a gestão da crise, custo de equipe de relações públicas que atuará na definição de estratégias, bem como o custeio das notificações a serem realizadas aos indivíduos que tiveram dados vazados

PERDAS CAUSADAS A TERCEIROS EM **DECORRÊNCIA DE ATAQUE CIBERNÉTICO** (Interno ou externo)

Consequências possíveis: Reclamação de terceiros por prejuízos sofridos em decorrência de um ataque cibernético, que podem envolver a violação de privacidade, roubo de código de acesso ou a contaminação por malware

Transferência de risco e resposta da apólice:

Pagamento das perdas devido a terceiros | Acordos e/ou indenizações | Custo de defesa

VIOLAÇÃO DE SEGURANÇA E **VAZAMENTO DE DADOS** (Interno ou externo)

Consequências possíveis Caso II: Investigação Administrativa

Transferência de risco e resposta da apólice: Honorário, custos e gastos que o segurado incorra, para o assessoramento legal e a representação relacionados a uma investigação

VIOLAÇÃO DE PRIVACIDADE (Interno ou externo)

Consequências possíveis: Danos à imagem da organização e à reputação dos responsáveis pela proteção de dados, investigações administrativas de órgãos reguladores, multas e penalidades previstas nas leis de proteção de dados

Transferência para a apólice: Os custos decorrentes de investigações administrativas e regulatórias, assim como o custo com peritos forenses computacionais e o pagamento de multas relacionadas à violação de leis de proteção de dados podem ser transferidos para a apólice de seguros

VIOLAÇÃO DE SEGURANÇA E VAZAMENTO DE DADOS

(Interno ou externo)

Consequências possíveis: Reclamação de terceiros por prejuízos sofridos

Transferência de risco e resposta da apólice: Pagamento das perdas devido a terceiros | Acordos e/ou indenizações | Custo de defesa

DESTRUIÇÃO OU CONTAMINAÇÃO DE BANCOS DE DADOS

(Interno ou externo)

Consequências: Destruição de bases de dados cadastrais ou transacionais em decorrência de ataque cibernético, causando prejuízos operacionais e/ou financeiros à organização

Transferência de risco: Os custos para restaurar ou recriar os bancos de dados danificados ou destruídos são pagos pela apólice do CyberEdge

EXTORSÃO OU RANSOMWARE

(Interno ou externo)

Consequências possíveis: Indisponibilidade de ativos e sistemas críticos da organização por conta de ataque cibernético em que o atacante exige pagamentos em dinheiro (ou criptomoedas ou outros ativos de valor) para cessar a ameaça

Transferência de risco: A seguradora pagará ao segurado o custo de realizar uma investigação pra determinar a causa de uma ameaça de segurança e/ou quantia paga em conformidade com os requisitos legais e com prévio consentimento da Seguradora para encerrar uma ameaça de segurança que poderia resultar em um dano ao Segurado

INTERRUPÇÃO DE REDE DECORRENTE DE VIOLAÇÃO DE SEGURANÇA

(Interno ou externo)

Consequências possíveis: Lucros cessantes do segurado

Transferência de risco e resposta da apólice: A seguradora pagará o lucro líquido que teria sido ganho; ou despesas operacionais contínuas incorridas durante a interrupção material, incluindo gastos com folhas de pagamento

Quer trocar experiências, conhecer riscos e soluções para diversos tipos de negócios?

Acesse www.negocioseguroaig.com.br



GARANTIDO POR AIG SEGUROS BRASIL S/A. CNPJ 33.040.981/0001-50 | CENTRAL DE ATENDIMENTO AIG 24 HORAS: 0800 726 6130 / ATENDIMENTO AIG A DEFICIENTES AUDITIVOS: 0800 724 0149 | OUVIDORIA (2° A 6°-FEIRA, DAS 9H ÀS 18H): 0800 724 02 19 / OUVIDORIA - ATENDIMENTO AIG ESCURIO DE FALA (2° A 6°-FEIRA, DAS 9H ÀS 18H): 0800 200 1244 | I – "A ACEITAÇÃO DO SEGURO ESTARÁ SUJEITA À ANÁLISE DO RISCO"; II – "O REGISTRO DESTE PLANO NA SUSEP NÃO IMPLICA, POR PARTE DA AUTARQUIA, INCENTIVO OU RECOMENDAÇÃO A SUA COMERCIALIZAÇÃO"; III – "O SEGURADO PODERÁ CONSULTAR A SITUAÇÃO CADASTRAL DE SEU CORRETOR DE SEGUROS, NO SITE WWW.SUSEP.GOV.BR, POR MEIO DO NÚMERO DE SEU REGISTRO NA SUSEP, NOME COMPLETO, CNPJ OU CPF". CYBER EDGE® (PROCESSO SUSEP Nº 15414.901341/2014-13)