

Privacidade de dados e Riscos Cibernéticos

AGORA É LEI!

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



Clovis Ampuero

contato@impactusseg.com.br • (71) 98826-0216 • (71) 4103-8203



Súmario

Você sabia?.....	03
Como a Lei afeta meu negócio?.....	04
O que eu preciso fazer par estar em conformidade com a nova lei?.....	05
A quais riscos o meu negócio está exposto?.....	06
Ameaças digitais.....	07
Conte com um Seguro de Riscos Cibernéticos.....	08
Conheça as principais situações e as coberturas AIG.....	09
Quer saber mais?.....	10



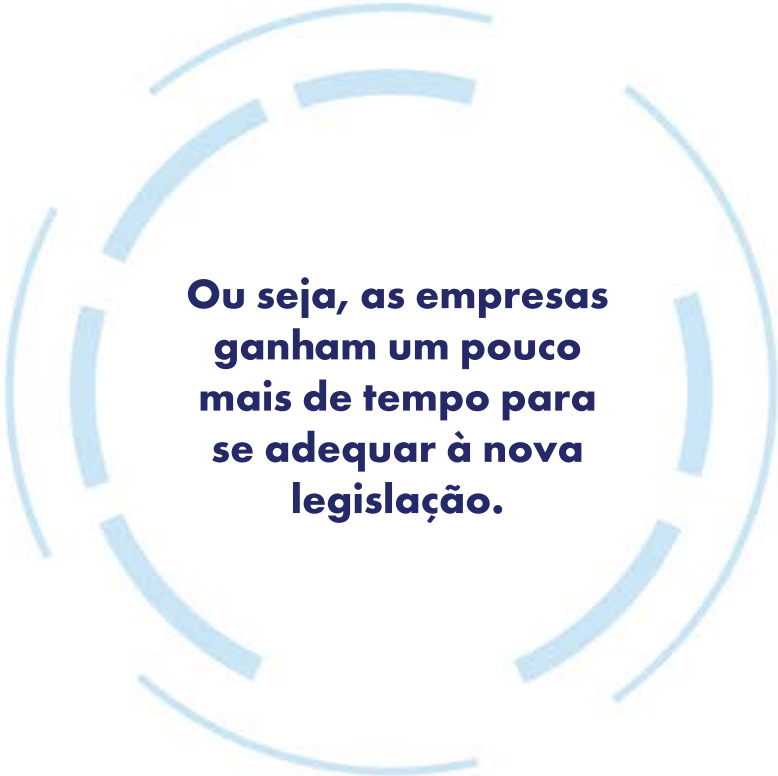
VOCÊ SABIA?

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 seguir:

- 1 Procure identificar onde, como e quando sua empresa faz a coleta de dados de seus clientes.
- 2 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.
- 3 Como é o armazenamento desses dados? Estão seguros?
- 4 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.
- 5 Quem acessa os dados de seus clientes? Qualifique sua equipe para que todos estejam inteirados sobre os procedimentos de segurança.
- 6 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 fisgado (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 entrada 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 proteção, 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



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 (2ª A 6ª-FEIRA, DAS 9H ÀS 18H): 0800 724 02 19 / OUVIDORIA - ATENDIMENTO A DEFICIENTES AUDITIVOS E DE FALA (2ª A 6ª-FEIRA, DAS 9H ÀS 18H): 0800 200 1244 | I – “A ACEITAÇÃO DO SEGURO ESTARÁ SUJEITA À ANÁLISE DO RISCO”; II – “O REGISTRO DESTES PLANOS 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)