# LGPD e Ameaças Cibernéticas - Seus Custos, Efeitos e Seguro

Por Armandir Maciel Silveira e Calisto Mattia

10 de Outubro, 2020

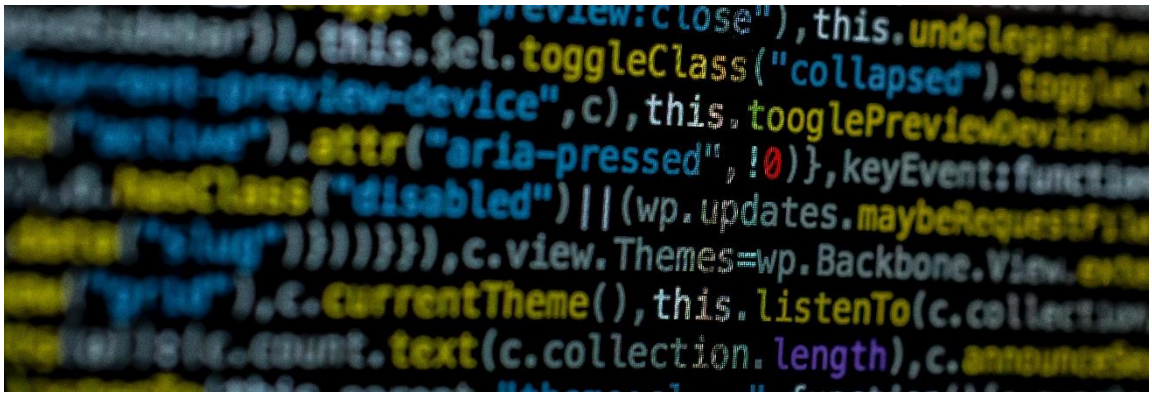



Foto de fauxels no Pexels

> "A visão de fora e a política de risco são remédios contra dois vieses distintos: o otimismo exagerado da falácia do planejamento e a precaução exagerada induzida pela aversão à perda."
>
> Daniel Kahneman – Rápido e Devagar

Nestes tempos de pandemia, o "novo normal" amplificou algumas tendências de comportamento da sociedade. Estas tendências foram proporcionadas pela necessidade de preservação à vida e à saúde, reduzindo-se o risco de contágio através do distanciamento físico. Estamos experimentando um processo de transformação digital no qual os sistemas de informação e de comunicação contribuem significativamente para termos ambientes e relações mais seguros. O trabalho em home-office, o e-commerce, as vídeo-reuniões são alguns dos exemplos do cotidiano que atualmente desafiam pessoas e organizações.

O crescente uso de tecnologia, dados, aplicativos, sua complexidade e a integração de sistemas de informação com smartphones e computadores em novos processos induz a uma maior exposição a riscos cibernéticos. A dependência destes processos, seja no nível operacional ou estratégico da organização, gera novos riscos com a violação dos sistemas de segurança à informação e crimes cibernéticos.

Ataques cibernéticos estão cada vez mais difundidos e representam ameaças possíveis às empresas e conselhos de administração. Os CEOs precisam criar eventos para avaliá-los, mesmo que não possam compreender muitos dos detalhes técnicos.

Quando falamos sobre riscos cibernéticos estamos falando de qualquer risco financeiro com o uso da tecnologia da informação e comunicação (TIC) que comprometa a confidencialidade, disponibilidade ou integridade de dados ou

serviços. O comprometimento da tecnologia associada às operações eventualmente leva à interrupção dos negócios, danos às propriedades de organizações e pessoais. São diversas as modalidades de ameaças cibernéticas que podem afetar os negócios das organizações e dados pessoais.

**CATEGORIAS DE AMEAÇAS CIBERNÉTICAS**

| CATEGORIA | SUB-CATEGORIA | EXEMPLO |
|---|---|---|
| **INTEGRIDADE**<br><br>Ataques cibernéticos podem usar técnicas de hacking para moficar, destruir ou comprometer a integridade dos dados. | Propaganda/Desinformação | Modificação ou manipulação de dados ou introdução de dados contraditórios para influenciar um resultado político ou empresarial ou desestabilizar um regime estrangeiro. |
| | Intimidação | Ataques a sites para coagir seus proprietários (público ou privado) em remover ou modificar conteúdo, ou a seguir algum outro caminho. |
| | Destruição | Destruição permanente de dados para prejudicar concorrentes ou atacar governos estrangeiros. Isso pode, por exemplo, fazer parte de um conflito mais amplo. |
| **DISPONIBILIDADE**<br><br>Ataques de negação de serviço (Denial of Service - DoS) por botnets, por exemplo, pode ser usado para impedir o acesso de usuários a dados que estariam disponíveis. | Informação externa | Negação de serviço, etc. ataques ao governo ou serviços privados disponíveis ao público, tais como, meios de comunicação, sites de informações do governo, etc. |
| | Informação interna | Ataques a intranets privadas ou governamentais, redes de serviços de emergência, energia e infraestrutura de controle de transportes, sites de e-banking, sistemas de e-mail, sistemas de gestão da empresa. |
| **CONFIDENCIALIDADE**<br><br>Ataques cibernéticos podem ter como alvo vários tipos de informações confidenciais, normalmente para ganho criminoso. | Espionagem | Empresas que buscam informações sobre seus concorrentes; governos envolvidos em atividades de espionagem (contra governos e indivíduos estrangeiros). |
| | Roubo de dados pessoais | Ataques de phishing (ou similares) destinados a enganar usuários para revelar dados pessoais, como conta bancária; vírus que carregam e gravam os dados da máquina de um usuário. |
| | Roubo de identidade | Cavalos de Tróia e outros mecanismos usados para roubar informações de identidade e para cometer crimes. |
| | Data mining | Técnicas de código aberto empregadas para descobrir, por exemplo, informações pessoais de dados públicos disponíveis. |
| | Fraude | Muitas vezes enviados através de spam por e-mail, a fraude inclui o popular *Nigerian "419"* ou fraude de antecipação de recursos, na qual um golpista procura induzir uma pessoa a realizar um pagamento adiantado, com a promessa de futuramente receber algum tipo de benefício, bem como tentativas de convencer os destinatários a comprar um gama de bens ou serviços fraudulentos. |

Tabela: Categoria de Ameaças Cibernéticas - Adaptada de "Cyber Risk Resources for Practioners", IRM - Institute of Risk Management

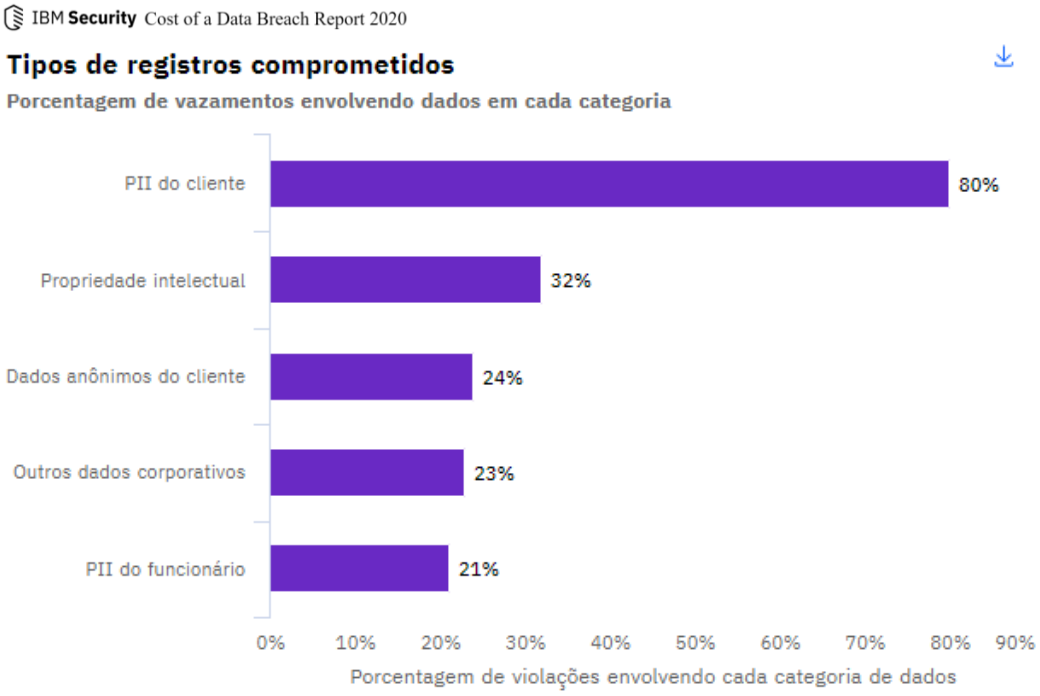
## Quais os custos e efeitos causados pelas ameaças cibernéticas?

Os dados e estudos sobre custos envolvendo risco cibernético ainda são escassos. As organizações que foram vítimas de ataques costumam ser relutantes em relatar e detalhar os eventos. Algumas das informações disponíveis são empíricas, referindo-se à violação de dados ou obtidas através de pesquisas com a garantia de preservação da identidade da empresa afetada.

A edição **2020 do "Relatório sobre o prejuízo de um vazamento de dados"** produzido pela IBM Security associada ao **Ponemon Institute** entrevistou mais de 3.200 pessoas. Os entrevistados foram executivos de 524 organizações que sofreram com vazamento de dados entre agosto de 2019 e abril de 2020 em 17 países distintos e em 17 setores da economia.

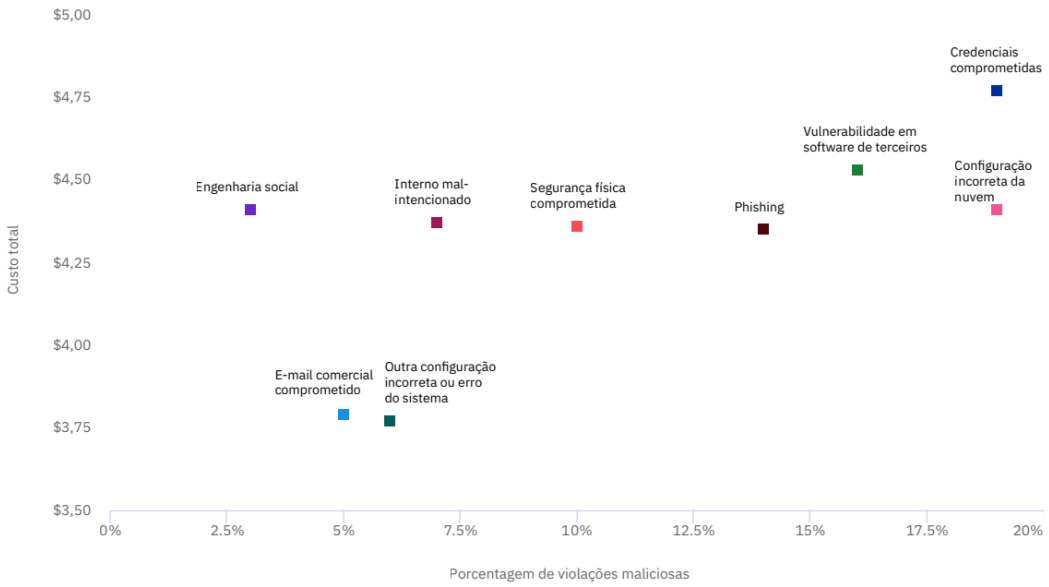
O Relatório nos apresenta dados globais sobre crimes cibernéticos, resultado da pesquisa, e que merecem uma reflexão.

- U$ 3,86 milhões é o prejuízo total médio das empresas.
- 280 dias é o tempo médio para identificar e conter o vazamento de dados.
- U$ 150 é o prejuízo médio por PII (informações de identificação pessoal) por registro.
- U$ 1,52 milhão de prejuízo total médio por perda de negócios devido à paralisação do sistema e aumento do custo de aquisição de novos clientes por dano à reputação da organização.



IBM Security Cost of a Data Breach Report 2020

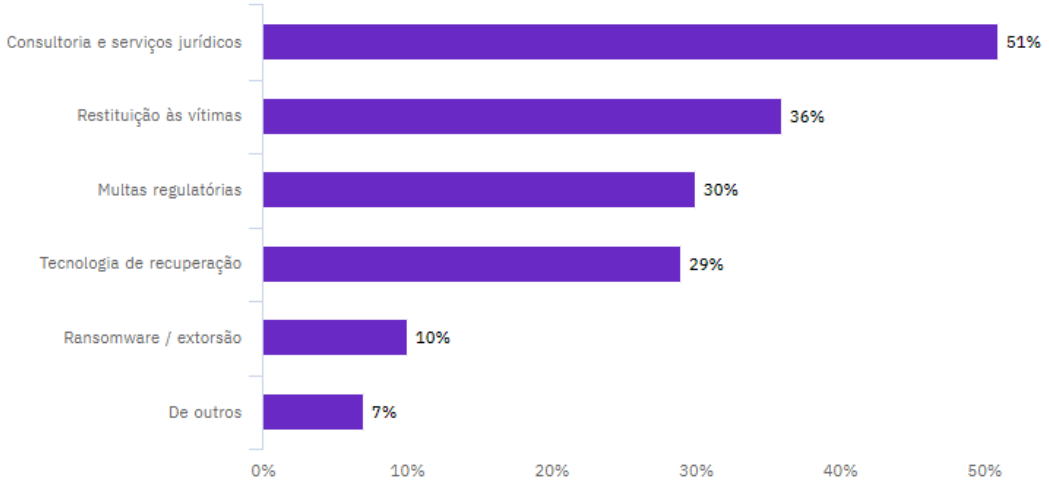
Prejuízo e frequência médios de vazamentos mal-intencionados de dados por vetor de causa principal




IBM Security Cost of a Data Breach Report 2020

**Tipos de prejuízos recuperados com sinistros de seguros de segurança virtual**

**Porcentagem de respostas, mais de uma resposta permitida**




## LGPD – O que é e por que é importante

O artigo 12 da Declaração Universal dos Direito Humanos menciona: "Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques à sua honra e reputação. Toda pessoa tem direito à proteção da lei contra tais interferências ou ataques". O próprio Código Civil também destaca os direitos da personalidade. Portanto, os dados pessoais fazem parte de um conjunto de atributos essenciais à constituição da pessoa e que requerem proteção e amparo.

A LGPD – Lei Geral de Proteção de Dados Pessoais é a Lei Federal 13.709 de 14 de agosto de 2018, regulamentada e implementada a partir de 14 de agosto de 2020, em que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Todas as empresas privadas e públicas de todos os setores da economia e a administração pública que realizem o tratamento de dados pessoais, independentemente do meio (físico ou digital), do país de sua sede ou do país onde estejam localizados os dados, estão sujeitas às determinações da LGPD.

As empresas devem se adequar à lei se, por exemplo:

- coletam dados de clientes para envio de ações promocionais ou de negócios;
- coletam dados através de site e aplicativos para vender produtos ou serviços;
- analisam comportamento dos clientes para sugerir conteúdo específico;
- mantêm dados de colaboradores e utilizam para pagamentos de salários;
- ou terceirizam a coleta, armazenamento e/ou tratamento de dados pessoais.

Eventual descumprimento das normas estabelecidas pela LGPD resultará na aplicação das penalidades previstas no artigo 52, destacando-se:

I. advertência, com indicação de prazo para adoção de medidas corretivas;
II. multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
III. multa diária, observado o limite total a que se refere o inciso II;
IV. publicização da infração após devidamente apurada e confirmada a sua ocorrência;
V. bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
VI. eliminação dos dados pessoais a que se refere a infração;

## Seguro para Riscos Cibernéticos

A aplicação dos processos da gestão de riscos, a partir de uma visão holística e abrangente, deve considerar todos os recursos de uma organização. As pessoas, a tecnologia e o capital precisam estar envolvidos e integrados nas soluções para tratar as ameaças que possam restringir o alcance dos objetivos.

O seguro é uma importante alternativa na gestão de riscos para a transferência de eventos cibernéticos não desejados. É praticamente impossível assegurar que se esteja totalmente protegido, mesmo implementando-se todas as recomendações

técnicas e as melhores práticas em *cibersegurança*. Neste sentido, o seguro fornece às organizações assistência, indeniza e auxilia em momentos críticos a superar as consequências danosas de uma violação aos seus sistemas e dados e que podem afetar os negócios e a imagem no longo prazo.

O mercado de seguros cibernéticos está se desenvolvendo rapidamente, principalmente neste momento de enfretamento à pandemia da COVID-19. Observou-se um crescimento da sinistralidade na carteira de seguros cibernéticos no 1° semestre de 2020, por força da maior exposição consequente da utilização dos meios digitais, atingindo 73% sobre os prêmios conforme dados obtidos no SES – Sistema de Estatística da SUSEP. O aumento da sinistralidade provocado pela maior incidência de ataques digitais e a implantação da LGPD (tendo no seguro uma garantia adicional contra eventuais perdas) resultaram em uma corrida para a contratação de novos seguros. Os prêmios tiveram um crescimento na ordem de 150% em comparação a igual período de 2019.

Para a contratação de seguros tradicionais de *property* (danos à propriedade) a organização mantém itens protecionais e programas de prevenção a incêndio, à explosão, roubos e furtos. Responde a questionários onde informa os locais e os itens protecionais para que a seguradora possa realizar a subscrição, definindo a aceitação e precificação do risco ou sua recusa. No seguro para riscos cibernéticos esta prática é similar. É através do questionário que as seguradoras poderão conhecer qual a política existente e as formas de tratamento para a *cibersegurança* e quais os efeitos em eventual ataque.

Alguns cuidados têm de ser adotados ao se contratar seguros, e o seguro contra riscos cibernéticos não é exceção. Pelo contrário! A maioria das empresas ainda não está familiarizada com o risco cibernético. É uma modalidade em que a organização tem que contar com o auxílio de consultores especializados em gestão de riscos e seguros, além dos colaboradores envolvidos como as áreas de gestão de riscos, financeira, jurídica, gestão de pessoas, tecnologia da informação, compliance, dentre outras. É um seguro novo e complexo. As tecnologias digitais estão em constante evolução, com mercado e condições em formação. Há escassez de dados estatísticos para a subscrição e merece especial atenção por parte dos segurados, consultores de riscos e seguros, seguradoras, resseguradores e instituições reguladoras.

O planejamento para o enfrentamento das ameaças inicia pela apuração por parte de especialistas para o potencial de risco (frequência/severidade) através da aplicação das técnicas de gerenciamento de riscos. Obtendo-se a visibilidade da exposição aos riscos e estando alinhada com a política de *cibersegurança*, define-se quais as ações adotar.

Se uma das alternativas for pela contratação de seguros, atuar com o consultor de riscos e seguros para a seleção das coberturas e seguradoras disponíveis no mercado que possam atender às expectativas. A pesquisa pelo produto de seguro procurará avaliar as condições contratuais com as coberturas oferecidas (básicas e

adicionais), esclarecer outros aspectos como as definições e glossário, limites segurados, riscos excluídos e a perda de direitos à Indenização. Os termos e condições têm de ser perfeitamente entendidos e discutidos com os consultores de riscos e seguros.

As coberturas do seguro cibernético não são padronizadas. São distintas entre as seguradoras e merecem aprofundada leitura e entendimento das cláusulas de definições e glossário. As empresas poderão contratar coberturas básicas, adicionais e prejuízos indenizáveis que as protejam contra as ameaças cibernéticas.

Destacamos as principais, atualmente disponíveis:

- Responsabilidade civil por violação de dados e confidencialidade.
- Responsabilidade por processos regulatórios e por força de legislação (inclui LGPD).
- Ameaça e extorsão cibernética e sequestro de dados.
- Responsabilidade por publicação em mídia e internet.
- Custos com gerenciamento de crise decorrente de evento cibernético.
- Lucros cessantes
- Fraude cibernética e engenharia social.
- Custos de defesa.
- Multas e penalidades.
- Custos de call center.
- Consultoria jurídica.

Tornar-se conhecedor em risco cibernético não significa que todos os executivos precisam se tornar especialistas em tecnologia da informação. Mas por certo é que precisam ser capazes de estabelecer qual o grau de tolerância de sua empresa ao risco cibernético, de definir os resultados que são mais importantes para o direcionamento do investimento em segurança e seus efeitos sobre as ameaças, e de promover uma cultura organizacional.

Quer saber mais sobre seguro cibernético?

Consulte-nos.

**www.hmo.com.br**

---

Armandir M. Silveira, MBA em Gerenciamento de Projetos e Inteligência Empresarial e 30 anos de experiência no mercado Segurador.

Calisto Mattia, MBA em Gestão Empresarial e Marketing de Serviços. 36 anos de experiência no mercado financeiro e Cooperativas.