MARSH JLT SPECIALTY

RISCOS CIBERNÉTICOS

# Riscos cibernéticos no setor de saúde

Organizações do setor de saúde estão entre as mais suscetíveis a ciberataques. Isso é devido a manterem uma grande quantidade de dados de pacientes, porém, seus riscos de exposição são bem maiores que a perda dos dados.

Inteligência artificial, internet das coisas (IoT), prontuário eletrônico, armazenagem de dados de saúde e telemedicina, dispositivos móveis e aplicativos são algumas das novas tecnologias que têm auxiliado o setor a fim de melhorar o cuidado e a segurança dos pacientes, assim como melhorar a experiência de cuidados com a saúde.

Esse crescente uso da tecnologia cria novos focos de exposição a riscos e pontos de vulnerabilidade que provoquem o acesso ou desativação de sistemas decisivos, dispositivos médicos, redes, hardware e dados. Além disso, a dependência da tecnologia por parte de fornecedores, pagantes e comerciantes do setor de saúde, tais como os planos de saúde, estão mais suscetíveis a possíveis fraudes e também impactos operacionais fundamentais que possam resultar em perdas consideráveis de receita, gastos, responsabilidade e danos a reputação.

A entrada da LGPD impactará severamente a indústria de saúde, pois requer uma série de medidas a manipulação de dados e, consequentemente, na eventualidade de um incidente.

## Soluções Marsh para gestão de riscos de Cyber

O conjunto de análises da Marsh pode ajudar as organizações da área da saúde a compreender e quantificar seu nível de exposição cibernética e a avaliar suas necessidades específicas de seguros. Criamos as melhores soluções de gestão de riscos cibernéticos adaptadas ao perfil e requisitos próprios de cada cliente.

## Quantificar o risco de Cyber para otimizar os investimentos

Um tratamento correto do risco cibernético começa com um profundo conhecimento dos riscos a que uma organização está exposta, o que inclui a quantificação do possível impacto de incidentes de cyber. A quantificação expressa a ameaça em termos econômicos e permite uma comparação média de valores dos riscos cibernéticos com outros tipos de riscos críticos que sua organização esteja sujeita. Isso também permite medir a efetividade dos investimentos em segurança cibernética, o que resulta em otimização para alocar recursos de riscos cibernéticos e oferece informações para uma correta tomada de decisão sobre coberturas e limites de seu seguro de cyber.

### A QUEM SE DESTINA

Qualquer empresa da área de saúde que:

- use internet ou tecnologia em sua operação
- administre ou colete dados de pacientes

### O QUE É OFERECIDO

Soluções próprias e os melhores serviços de assessoria para ajudar sua empresa a:

- entender o universo do risco cibernético, suas próprias vulnerabilidades e as ameaças à companhia
- medir sua exposição cibernética através de ferramentas personalizadas de quantificação de risco
- administrar seus riscos cibernéticos por meio de:
  - soluções de seguros personalizadas que atendam suas exposições, com programas de treinamento e educação
  - ferramentas de mitigação de riscos e loss prevention
  - planos de resposta e recomendações de melhora no risco

MARSH

## Seguro cyber especializado em saúde

A Marsh pode desenhar uma cobertura de seguros personalizada a fim oferecer uma proteção ampla para qualquer perda e responsabilidade derivadas de uso de tecnologia e do tratamento de dados no setor de saúde, como:

### COBERTURAS DE CYBER E AMPLIAÇÕES OPCIONAIS

- **Parada operacional:** prejuízos diante de Interrupção/gastos adicionais: reembolso por perdas de receita e gastos em função de falha técnica, interrupção de sistema ou ciberataques, com a opção de incluir as seguintes coberturas:
  - contingências por interrupção derivadas de eventos envolvendo terceiros
  - equipamentos de IoT/dispositivos médicos e plataformas de telemedicina usadas no cuidado de pacientes e atenção ao cliente
- **Proteção de ativos de informações:** custos para recriar ou reconfigurar ativos de informação e dados eletrônicos, com a opção de incluir a substituição de hardware e custos para reconstruir sistemas
- **Gestão de vulnerabilidades/eventos:** custos para notificar e investigar vulnerabilidades de privacidade e segurança, incluindo serviços jurídicos, perícia forense e serviços de correção/reconstrução de arquivos
- **Ciberextorsão:** gastos com resgate e investigação associados a ameaças de roubo de informação confidencial, introdução de código malicioso, corrupção de sistemas ou restrição de acesso

### COBERTURA DE CYBER PARA TERCEIROS

- **Responsabilidade por privacidade:** falhas ao evitar vazamento de informações sigilosas – digitais e impressas
- Responsabilidade pela segurança das redes: falha computacional comprovada ou alegada para prevenir ou mitigar ataques relacionados a equipamentos de IoT ou sistemas computacionais operacionais
- **Custos de defesa para processos regulatórios:** custos para defesa em ações regulatórias e certas multas e penalizações, incluindo as avaliadas pelos departamentos de saúde e direitos civis
- **Erros e omissões (E&O) tecnológicas:** defesa e indenização em caso de erros ou suposta negligência quando do oferecimento de serviços a terceiros

## Os altos custos dos riscos cibernéticos para organizações de saúde

Acontecimentos recentes têm demonstrado os riscos relacionados a dados, tecnologia e responsabilidade aos fornecedores e empresas dentro do setor:

- Um fornecedor de um laboratório descobriu que hackers teriam invadido o sistema há meses, o que provocou um vazamento que afetou a mais de 20 milhões de pessoas e acarretou em sua falência nos EUA.
- Em uma importante seguradora de saúde, os hackers roubaram informação pessoal de mais de 80 milhões de pessoas, o que resultou em enormes gastos com a resposta aos vazamentos, investigações e litígios
- Uma grande empresa fornecedora de sistema de saúde sofreu com o vazamento de mais de 3 milhões de registros de pacientes e dados de cartão de crédito quando os hackers invadiram sua rede através de um fornecedor de pagamentos
- Uma ampla rede de saúde foi infectada por um ransomware, que alterou seus serviços por semanas. A empresa pagou o resgate, porém sofreu grandes perdas de receita
- Um hospital no Brasil deixou de realizar cerca de 3500 atendimentos em 4 dias frente a um ataque cibernético que impactou os sistemas computacionais e operacionais. 350 pacientes também tiveram seus tratamentos de radioterapia cancelados


Leader of
**25 year-old**
Cyber Insurance Market

**Broker Team of the Year ($500M+)**
Business Insurance US Awards 2019

**Cyber Broker of the Year**
Advisen 3 Time Winner

Para mais informações, visite marsh.com.br ou entre em contato com seu representante da Marsh no Brasil:

MARTA SCHUH
Líder de riscos cibernéticos
+55 11 998 857 118
marta_schuh@jltbrasil.com