Ataques cibernéticos no setor de saúde

6 ações essenciais para planos e sistemas de saúde, redes de farmácias e outros segmentos impactados

pwc

Conteúdo

Impactos

O setor de saúde está enfrentando o impacto de ataques cibernéticos em um ecossistema de ameaças cada vez mais interconectado. As operações têm sido significativamente afetadas por diversos eventos de terceiros.

No Brasil, o setor de saúde se destaca como um dos principais alvos de cibercrimes. Em 2023, observou-se um aumento substancial no número de ataques a hospitais, clínicas e outras instituições em comparação com o ano anterior. Esses ataques comprometem a segurança e privacidade dos dados dos pacientes, expondo informações sensíveis de alto valor no mercado paralelo.

Além de ameaçar diretamente a segurança dos dados dos pacientes, os cibercrimes têm impactos negativos significativos na eficiência operacional e sustentabilidade financeira das instituições de saúde.

Uma vez vítimas desse tipo de incidente, organizações e prestadores de serviços enfrentam elevados custos tanto para resolver as instabilidades e os danos operacionais causados pelos ataques quanto para lidar com os processos judiciais decorrentes desses episódios, considerando que, segundo a Lei Geral de Proteção de Dados Pessoais (LGPD) vigente no país, é dever dessas instituições garantir a proteção dos dados sensíveis dos pacientes.

Seis ações essenciais

As empresas que se preparam, respondem com eficiência e emergem mais fortes de uma crise cibernética seguem um conjunto de seis ações essenciais:

- O estabelecimento de uma estrutura de gestão multifuncional de crise.
- A avaliação dos potenciais impactos para as operações e os clientes.
- O desenvolvimento de soluções táticas e abordagens alternativas para manter os processos operacionais críticos no curto e médio prazo.
- A consideração cuidadosa dos passos necessários para retomar as operações normais.
- O desenvolvimento de protocolos claros de comunicação interna e externa.
- O aperfeiçoamento de medidas internas de cibersegurança e a avaliação de riscos cibernéticos adicionais de terceiros.

“A indústria da saúde não está imune ao multiverso de riscos que enfrentamos na era da disrupção tecnológica. O ritmo da transformação digital torna desafiador o entendimento do que é mais crítico na hora de gerenciar riscos cibernéticos. À medida que o setor se digitaliza, a tendência é de que as ameaças sejam mais agressivas. Essa nova jornada será cheia de desafios, e as lideranças precisarão de resiliência para superar os obstáculos”.

Bruno Porto, sócio e líder do setor de Saúde da PwC Brasil

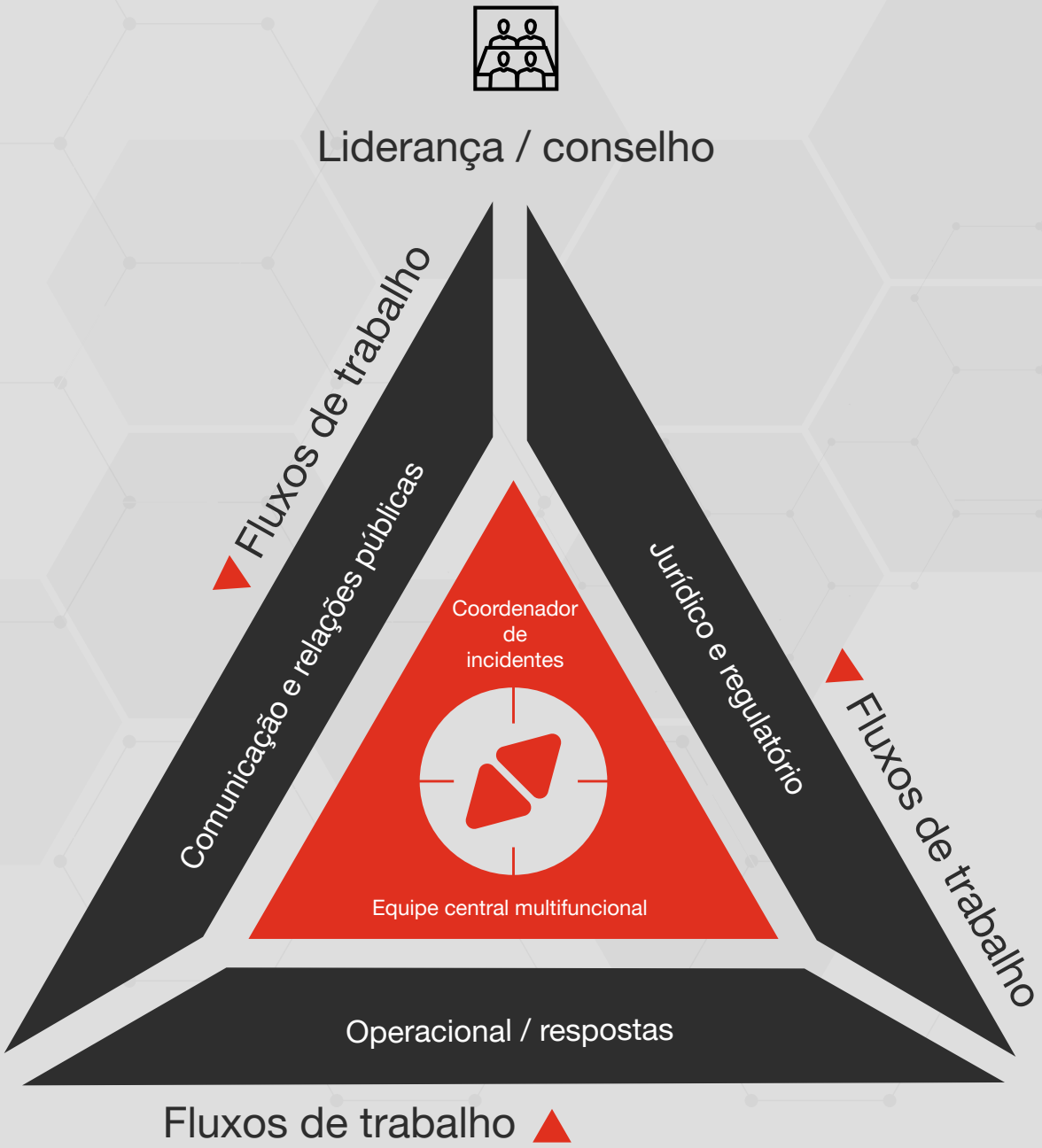
Considere estas questões-chave

Execução de respostas a crises

- Foi ativada uma equipe multifuncional de respostas a crises com um *project management office* (PMO) de apoio para gerenciar uma resposta holística em toda a empresa?
- Foram definidos fluxos de trabalho nas atividades de respostas com responsáveis claros e periodicidade de ações de divulgação?
- Foi implementada uma equipe de comunicação de crises para desenvolver uma mensagem central consistente, com uma unidade específica para triagem de clientes e *stakeholders* voltada a rastrear, gerenciar e responder rapidamente as consultas recebidas, de forma personalizada?

Avaliação da resiliência e do risco cibernético

- Foram realizadas atividades de busca por ameaças e avaliações de violação e comprometimento para assegurar que o ambiente permaneça seguro?
  - » Foram consideradas tanto as conexões com o ecossistema de saúde mais amplo quanto as vulnerabilidades *zero-day* das quais estados-nações e agentes criminosos procuram se aproveitar?
- Existe um plano definido para testar sua conexão com a entidade ou entidades impactadas quando estiverem operacionais novamente?
- Foi ativado um programa de gestão de riscos de terceiros para entender o impacto potencial das vulnerabilidades identificadas e quaisquer outros impactos potenciais de terceiros em seu ecossistema?



- **Considerações sobre resiliência**
- A empresa está preparada para fazer uma análise posterior à ação tomada e se preparar melhor para eventos similares no futuro?
- Foram realizadas avaliações de impacto nos negócios e identificados processos críticos que exigem capacidades de resiliência de alta disponibilidade?
- Foram identificados processos críticos para os quais as dependências de fornecedores criam um risco de concentração? Existe um processo de contingência? Foram consideradas estratégias de diversificação de fornecedores?
- Foram testados os processos de continuidade dos negócios e as capacidades de recuperação de desastres para saber o quanto a empresa conseguiria entregar serviços críticos durante outros tipos de eventos disruptivos?

Comunicação com beneficiários e outros *stakeholders*

- Existe uma estratégia de gestão de comunicação e canais? O que será comunicado e para quem? Qual será o formato e quais canais serão utilizados nessas comunicações (como beneficiários, pacientes, empregadores, prestadores de serviço, programa de benefícios em medicamentos (PBM), farmácias, corretores e agências estaduais e federais, entre outros)?
- Foi planejado o impacto na percepção/satisfação dos beneficiários (por exemplo, *Net Promoter Score* (NPS) e *Consumer Assessment of Healthcare Providers and Systems* (CAHPS))?
- Seus provedores de logística estão preparados para dar suporte à empresa?
- Existem previsões, contratações, treinamentos e FAQs atualizados para os centros de contato e fornecedores de *Business Process Outsourcing* (BPO)?

Considerações operacionais para prestadores

- A empresa tem processos vigentes caso não consiga completar as funções de acesso prévio, como verificação de seguro ou autorizações? Entre as implicações, encontramos:
  - » Atrasos que afetam as consultas, os procedimentos e a entrega de receitas e medicamentos aos pacientes, interrompendo o atendimento.
  - » Um aumento dos pedidos de reembolso negados devido à insuficiência de aprovações de seguros e autorizações necessárias.
  - » Impactos no fluxo de caixa do prestador, além de um aumento dos custos administrativos.
- Como a empresa priorizou a submissão de pedidos de reembolso com pagadores impactados no caso de atraso na codificação/faturamento inicial e envio desses pedidos?

- Existem acordos de pagamento provisório para preservar o fluxo de caixa no curto prazo?
  - » Foram coordenados os mecanismos de pagamento provisório tanto para remessas quanto para pagamentos em contas a receber?
  - » Foram estabelecidos procedimentos de reconciliação com os pagadores impactados individualmente para a gestão de pagamentos provisórios e o alívio de contas a receber ativas?
- Existem protocolos vigentes de processos de negação e contas a receber provisórias ativas junto aos pagadores/planos impactados? Entre eles, podem estar:
  - » O estabelecimento de prazos para contas ativas a receber e recursos de pedidos de reembolso negados para mitigar o "aumento do envelhecimento" – o aumento do tempo médio – das contas a receber, assim como a elevação das negativas e dos atrasos de pagamento.
  - » O alinhamento rápido dos mecanismos de processamento/reprocessamento de lotes para evitar a recuperação lenta/manual do estoque.
- Você está enfrentando tempo de inatividade de pessoal/recursos quando os fornecedores impactados são um prestador de serviços gerenciados ou oferecem suporte ao intercâmbio eletrônico de dados? Você assegurou recursos de *backup*/contingência que possam ser rapidamente dimensionados para atender às necessidades comerciais do provedor?

Considerações para o Programa de Benefícios em Medicamentos (PBM) e os planos de saúde

- A empresa tem processos provisórios para funções impactadas (por exemplo, elegibilidade e recebimento de pedidos)?
- A empresa tem processos provisórios para rastrear pré-autorizações que não foram processadas?
- A empresa tem estratégias de pagamento provisório para prestadores?

É preciso considerar:

  - » Pagamentos antecipados a serem reconciliados após a resolução de eventos disruptivos.
  - » Reconciliação (resolução posterior) para gerenciar solicitações duplicadas, pedidos enviados por diferentes fornecedores, pedidos em papel, etc.
  - » O que os prestadores consideram “suficientemente bom” após a resolução de eventos disruptivos.

- A empresa tem uma estratégia de comunicação com prestadores/farmácias e irá estratificar e priorizar seus fornecedores? É preciso considerar:
  - » Um nível apropriado de atendimento a prestadores responsáveis por maiores volumes/valor.
  - » A oportunidade de construção de relacionamento com prestadores com base no modo como as interações são administradas.
- Como será feita a reconciliação de prescrições realizadas de boa-fé?
- Como a empresa está gerenciando os impactos sobre a qualidade dos serviços de saúde e a adesão ao tratamento em relação a programas e indicadores de saúde no Brasil, como o Índice de Desempenho da Saúde Suplementar (IDSS) e as certificações de qualidade hospitalar?

- Existem processos de exceção para distribuir medicamentos críticos? Como serão tratadas as preocupações com adesão se os pacientes não puderem pagar o custo na ponta na farmácia?
- Se esta disrupção operacional persistir, a empresa tem alguma estratégia para lidar com o enorme acumulado de transações após o fim das interrupções? Ela considerou a criação de “ambientes de teste” para processar em lotes o grande volume de transações futuras?

Olhando para o futuro da resiliência

À medida que as operações comerciais voltam ao normal, é essencial considerar a resiliência tecnológica e operacional, além da concentração de fornecedores e dos processos de contingência. Construir uma organização verdadeiramente resiliente não acontece da noite para o dia. É um esforço de vários anos que precisa começar agora.

Desafios estratégicos para a resiliência

Custo e nível de esforço

Gerenciar custos exige a integração da expertise de negócios com a de tecnologia, usando as novas tecnologias para priorizar esforços com base em processos e ativos mais críticos.

Falta de visão para diversos tipos de evento

O planejamento de resiliência histórica tem se concentrado em redundância tecnológica e desastres naturais. Amplie sua abertura para outros eventos de disponibilidade, como riscos de concentração da cadeia de suprimentos.

Adoção tardia da nuvem

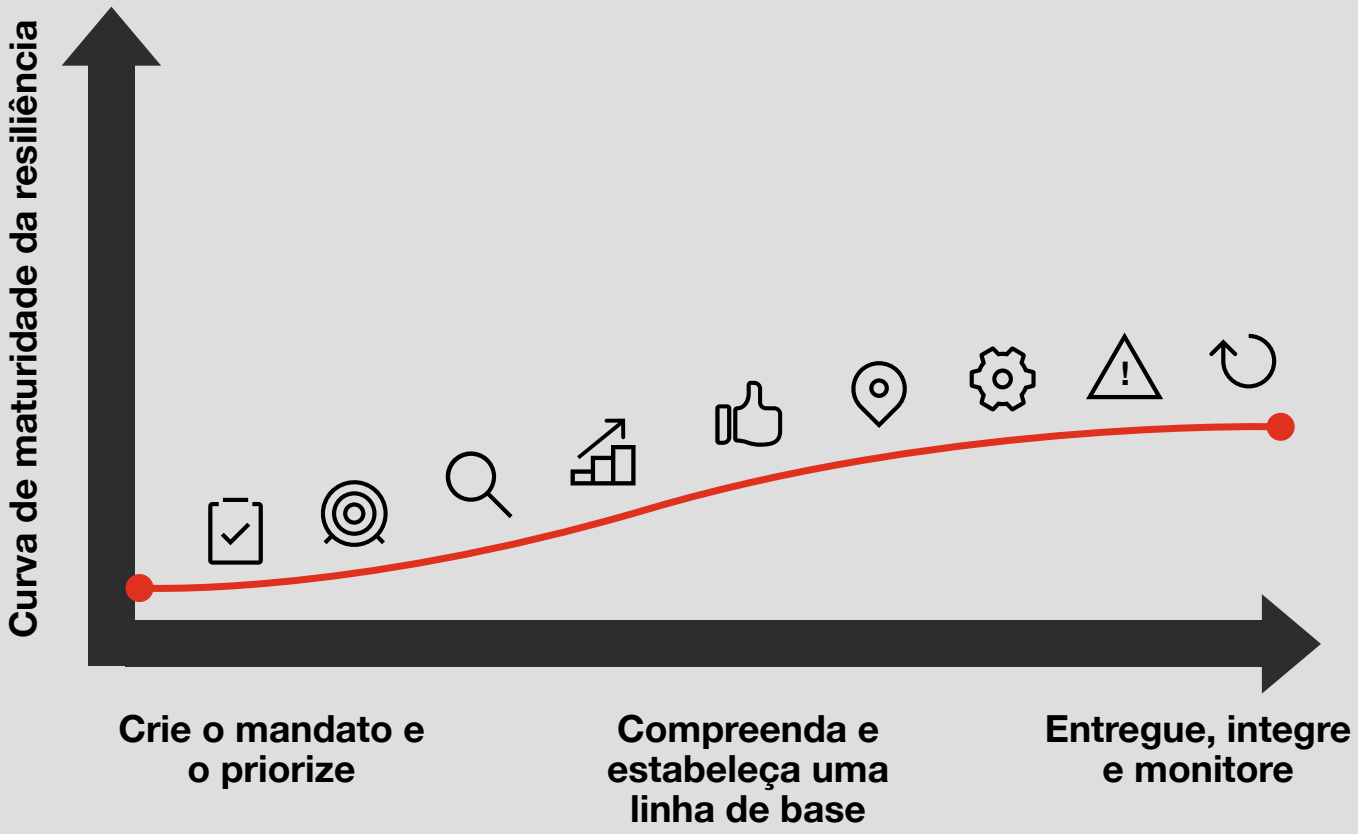
A computação em nuvem deve ser um componente crítico de qualquer estratégia de resiliência. Priorizar a nuvem para gerar crescimento deve ser balanceado com o uso da nuvem para resiliência geral.

Mentalidade antiquada

Focar no *compliance* com as regulações de Informações de Saúde Protegidas (*Protected Health Information*, ou PHI) e aceitar a noção de que o “PHI está em todos os lugares” prejudicam o planejamento estratégico.

Avalie seu nível de resiliência em relação a vários eventos

Invista estrategicamente para evoluir



Estabeleça um mandato de resiliência
Inclua de forma explícita a resiliência na agenda do conselho de administração.

Priorize
Identifique os serviços mais importantes que impactam pacientes, beneficiários e/ou a prestação dos serviços de saúde.

Mapeie os serviços críticos e visualize melhor a infraestrutura, as aplicações e as dependências da cadeia de suprimentos
Entenda como os serviços são entregues e apoiados.

Compreenda os impactos e estabeleça os limites da disrupção
Entenda como os impactos se manifestam em disrupções, na ausência da ação gerencial.

Desenvolva planos e manuais de procedimento
Desenvolva planos estratégicos e operacionais para responder e se recuperar de uma disrupção.

Pense em cenários e testes
Compreenda o impacto de cenários severos, mas plausíveis, nos serviços prioritários.

Tome decisões de investimentos
Use os insights de resiliência e aloque recursos para construir ou sustentar a resiliência.

Corrija as vulnerabilidades e construa resiliência
Realize a transformação necessária para ampliar a resiliência.

Sustente a resiliência por meio da melhoria contínua
Atualize, recalibre, revise e aprenda.

Contatos

Bruno Porto
Sócio e líder da indústria de Saúde
bruno.porto@pwc.com

Eduardo Batista
Sócio e líder de Cibersegurança e Privacidade
eduardo.batista@pwc.com

pwc

Acesse o site:

www.pwc.com.br

Siga a PwC nas redes sociais: