Optinsure SEGUROS

Risco Cibernético

- O que toda empresa precisa saber sobre segurança digital.

Ataques Cibernéticos em destaque

Este e-book foi produzido pela **Optinsure** para empresários, gestores e profissionais de TI, Segurança da Informação, Jurídico/Compliance e finanças que precisam entender, de forma clara e objetiva, **o que está em jogo quando o assunto é risco cibernético.**

Se a sua empresa usa tecnologia para operar, armazena dados de clientes ou colaboradores, realiza transações digitais ou tem equipes em home office, este guia é para você.

Boa leitura!

O Brasil no centro do risco digital

Somos o segundo país do mundo com mais ataques cibernéticos.
Em 2024 e 2025, registramos cerca de R$ 700 bilhões em tentativas de ataques.
São 1.379 tentativas por minuto, todos os dias.

O dado mais revelador é este: 40% das empresas já sofreram algum incidente cibernético.
Se você tem dez clientes ou parceiros de negócio, estatisticamente quatro deles já foram vítimas,
e a maioria não tinha seguro.

Por que as PMEs são o alvo favorito?
Nos últimos anos, as pequenas e médias empresas se digitalizaram em velocidade acelerada: adotaram nuvem, Pix, e-commerce e sistemas integrados. Mas a maturidade em segurança não acompanhou o ritmo.

- Ausência de autenticação multifator
- Senhas fracas e sem rotação periódica
- Backups não isolados do ambiente
- Equipes sem treinamento contínuo
- Nenhum plano formal de resposta a incidentes
- Home Office: cada funcionário em lugar diferente
- Falsa sensação de “Não sou alvo”

Alta conectividade e baixa proteção

O que acontece quando o ataque chega

0h — Invasão acontece de forma silenciosa.

2h — Dados já estão criptografados.

6h — A notícia vaza na mídia ou nas redes sociais.

24h — Obrigação legal de notificar a ANPD (Autoridade Nacional de Proteção de Dados).

72h — Prazo formal de comunicação aos titulares dos dados expira.

30 dias — Primeiras ações judiciais. Reclamações no PROCON, no Consumidor.gov e no Reclame Aqui.

6 meses — 60% das PMEs encerram as atividades.

Em média, as empresas brasileiras levam 204 dias para detectar uma violação.
Sem seguro cibernético, cada etapa vira uma fatura separada: advogados, peritos, marketing, multa, indenizações.

O peso jurídico que poucos calculam

A Lei Geral de Proteção de Dados (LGPD) estabelece responsabilidade para o tratamento de dados pessoais. Isso significa que a empresa não precisa ter agido com má-fé para ser responsabilizada: basta ter falhado na proteção.

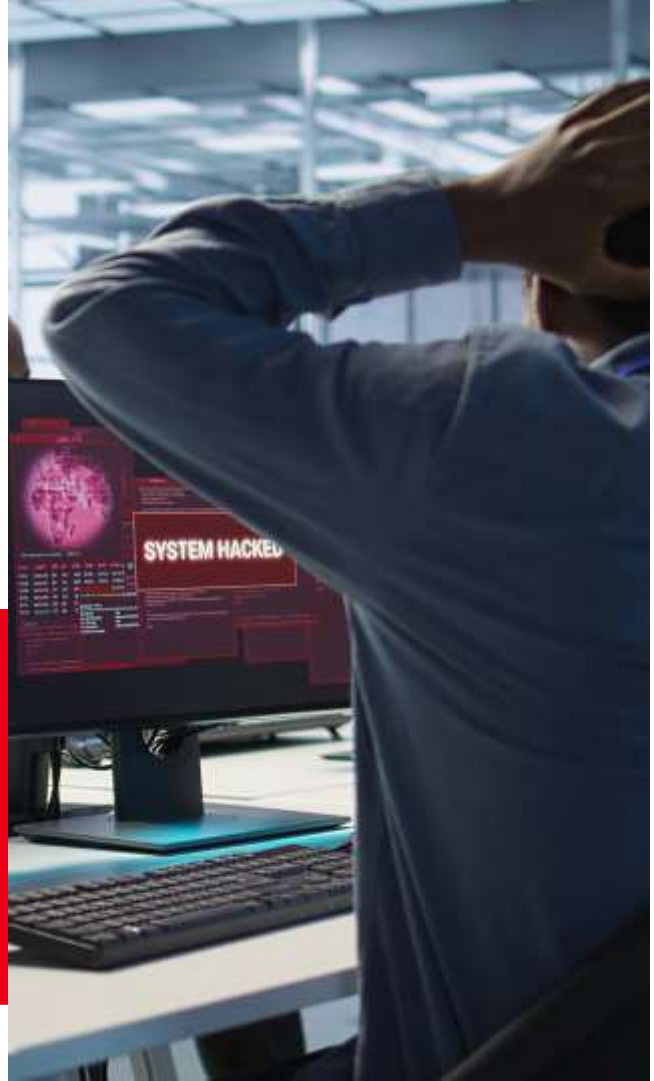
As consequências jurídicas de um ataque envolvem múltiplas frentes simultâneas.

ANPD: multas de até R$ 50 milhões por infração ou até 2% do faturamento da empresa no Brasil. A Resolução ANPD nº 15/2024 tornou a obrigação de notificação ainda mais rigorosa.

Ações civis individuais: cada titular de dados afetado pode acionar a empresa. Um único ataque pode gerar centenas ou milhares de processos simultâneos.

Ações coletivas: associações de consumidores e o Ministério Público podem ajuizar ações coletivas com base no CDC combinado com a LGPD.

Responsabilidade pessoal: sócios e administradores podem responder civil e criminalmente em determinadas circunstâncias, especialmente quando houver omissão.



O custo real:
quanto vale uma hora parada?

Existe uma forma simples de tornar o risco cibernético concreto para qualquer gestor: **calcular o custo de uma hora de operação parada.**

Faturamento anual ÷ 365 dias ÷ 24 horas = custo por hora parada

A esse custo de interrupção, soma-se: honorários advocatícios de urgência, contratação de peritos forenses, custos de comunicação de crise, notificação aos titulares de dados, multas regulatórias e eventuais indenizações.

UMA CRISE MAL GERIDA CUSTA MUITO MAIS DO QUE O IMPACTO TÉCNICO DO ATAQUE.

Como estruturar sua proteção cibernética

A proteção cibernética pode ser desenvolvida de forma acessível e proporcional ao porte e ao perfil de risco de cada empresa.

Prevenção

Conhecer os riscos antes que se tornem incidentes. Isso inclui avaliar a maturidade digital da empresa, identificar vulnerabilidades e implementar controles básicos de segurança.

Resposta

Ter um plano claro para quando o ataque acontecer. Quem aciona? Em quanto tempo? Como notificar a ANPD e os titulares de dados? Quem cuida da comunicação externa?

Transferência de Risco

O seguro cibernético funciona como o último escudo, garantindo que, mesmo quando a prevenção falhe, a empresa tenha recursos para responder sem comprometer sua continuidade.

Investir em proteção cibernética é 20 a 50x mais barato do que arcar com as consequências.

O papel da Optinsure

Nossa visão é que risco cibernético é um risco de negócio que precisa ser gerenciado de forma integrada, assim como os demais riscos que afetam pessoas e resultados.

Para apoiar as empresas, desenvolvemos a análise do perfil de exposição, conexão com parceiros especializados em seguro cibernético e gestão de riscos digitais, além de apoio na estruturação de uma abordagem integrada de proteção.

Sua empresa está preparada para ataques?

Empresas que tratam o risco cibernético de forma reativa pagam muito mais, em dinheiro e em reputação.

Entre em contato com a Optinsure. Vamos entender juntos onde está a exposição da sua empresa e qual é o caminho mais inteligente de proteção.

FALAR COM ESPECIALISTA

Obrigado pela leitura.

optinsure.com.br
facebook.com/optinsure.br
instagram.com/optinsure.br
linkedin.com/company/optinsure-br

Optinsure SEGUROS