

Antes das ferramentas, vem o diagnóstico: por que a maioria das empresas inverte esta ordem?

Boa parte das empresas brasileiras trata cibersegurança como uma lista de compras: firewall, antivírus, backup, autenticação multifator

Daniel Tieppo (*)

O problema é que nenhuma dessas ferramentas responde a uma pergunta anterior e mais importante, que é onde exatamente estão as vulnerabilidades daquela organização específica. Sem essa resposta, o investimento em proteção vira um exercício de tentativa e erro, caro e frequentemente ineficaz.

Os números confirmam esse descompasso. Segundo o Cybersecurity Readiness Index 2025, da Cisco, apenas 5% das empresas brasileiras atingiram o patamar considerado maduro em cibersegurança, o mesmo percentual registrado na edição anterior do estudo. Não houve avanço. As organizações seguem comprando tecnologia sem antes mapear onde ela precisa ser aplicada com mais urgência.

O dado incomoda menos pelo valor em si e mais pelo que ele revela. O mercado aumentou gastos em segurança nos últimos anos, mas essa curva de investimento não se traduziu em curva equivalente de maturidade, o que só acontece quando o dinheiro entra no lugar errado do processo: na compra de tecnologia antes do mapeamento de risco que deveria orientar essa compra.

O exemplo mais claro dessa desconexão está nas empresas de capital aberto, que, em tese, reúnem as melhores condições para fazer esse dever de casa. Um levantamento da Abrasca com o Security Design Lab atribuiu nota média de 4,9, numa escala de 0 a 10, à maturidade em cibersegurança das companhias listadas na B3.

Se organizações com orçamento robusto e obrigações regulatórias rigorosas ainda tiram nota mediana, o problema não é falta de recurso. É a ausência de um processo estruturado que diga a essas empresas, com precisão, onde elas estão vulneráveis antes de decidirem onde investir.

Diagnóstico é dado, não intuição

Esse processo estruturado não se resume a uma prática isolada. Ele combina diferentes frentes de diagnóstico, cada uma respondendo a uma parte do problema: o risk assessment, que mapeia e prioriza riscos a partir do contexto real do negócio; o ASM (Attack Surface Management), que monitora de forma contínua tudo o que está exposto na internet e pode virar porta de entrada; e o teste de invasão, ou pentest, que simula um ataque real para revelar falhas antes que um criminoso as explore.

Um levantamento recente da Pesquisa de Maturidade da Indústria em Cibersegurança mostrou que apenas 11,6% das empresas realizam pentest com regularidade, enquanto 63,3% simplesmente não o fazem — um



retrato que tende a se repetir quando se olha para as demais práticas de diagnóstico.

O motivo não costuma ser resistência a essas práticas, e sim a crença de que a tecnologia já instalada dá conta do trabalho sozinha. Essa crença é o verdadeiro ponto cego do setor.

Um firewall bem configurado impede acessos não autorizados que ele reconhece como ameaça, mas não avalia se uma senha fraca de um fornecedor terceirizado abre uma porta lateral para o sistema, ou se um processo de concessão de acesso ficou desatualizado depois da saída de um funcionário.

Esse tipo de falha só aparece quando alguém testa ativamente a estrutura, não quando alguém presume que ela está protegida porque o produto certo foi comprado. O diagnóstico é o que diferencia gasto de investimento: sem ele, a empresa paga por segurança sem necessariamente comprar redução de risco.

O tempo perdido tem preço

Se o diagnóstico já é raro na etapa de prevenção, sua falta fica ainda mais evidente quando um ataque de fato acontece. O Cost of a Data Breach Report 2025, da IBM, mostra que o ciclo médio entre identificação e contenção de uma violação de dados foi de 241 dias em 2025, o menor patamar em nove anos e, ainda assim, quase oito meses de exposição.

Esse número existe porque a maioria das empresas não tem um retrato atualizado do que é "normal" dentro da própria rede. Sem esse parâmetro, não há como distinguir uma atividade legítima de uma anomalia, e o ataque segue circulando disfarçado de rotina. O impacto financeiro dessa demora confirma a lógica: segundo o mesmo relatório, empresas que sofrem um incidente em até 200 dias registram custo médio de US\$ 3,87 milhões, contra US\$ 5,01 milhões nas que ultrapassam esse prazo.

O tripé que sustenta a decisão

No fundo, todas essas práticas de diagnóstico convergem para o mesmo objetivo, que pode ser resumido em três pilares. O primeiro é a visibilidade:

de saber, a qualquer momento, o que está acontecendo dentro do ambiente digital da empresa. O segundo é a observabilidade: entender por que e como aquilo está acontecendo, o que permite distinguir uma anomalia real de um ruído qualquer. O terceiro é a governança: transformar esse entendimento em processo, com responsáveis, critérios e continuidade — o que garante que a segurança se mantenha ao longo do tempo, e não apenas no dia em que a ferramenta foi instalada.

É esse tripé que deveria orientar qualquer decisão de investimento. Sem visibilidade, a empresa não sabe o que precisa proteger. Sem observabilidade, não consegue interpretar o que vê. E, sem governança, mesmo enxergando e entendendo os riscos, não sustenta a resposta a eles no tempo. Com essa base estabelecida, a escolha de quais serviços e ferramentas adotar deixa de ser tentativa e erro e passa a ser consequência direta do diagnóstico.

A diferença não nasce de uma tecnologia mais cara, nasce da capacidade de enxergar o problema mais cedo. E enxergar cedo é, por definição, uma função de diagnóstico contínuo — sustentado por visibilidade, observabilidade e governança —, não de uma ferramenta isolada.

O diagnóstico deveria ser processo e não um evento isolado. Uma avaliação de risco feita há dois anos descreve uma empresa que já não existe mais, com fornecedores diferentes, funcionários diferentes e superfície de ataque diferente. O mercado brasileiro amadureceu na hora de comprar tecnologia de segurança, mas segue tratando o mapeamento de risco como etapa dispensável, quando, na verdade, é ela que determina se o resto do investimento vai proteger o que precisa ser protegido.

Toda estratégia de cibersegurança que funciona começa pela mesma pergunta, que é conhecer com precisão os próprios riscos antes de tentar resolvê-los.

(*) Especialista em tecnologia e telecomunicações, com mais de 20 anos de experiência no setor. Formado em Ciência da Computação e Gestão Comercial, construiu sua carreira em empresas como Olitel Telecom, Vocalcom e Alcatel-Lucent Enterprise.



Quando o próprio piloto pede a torre de controle

Dario Amodei, CEO da Anthropic, fez algo raro para um executivo do Vale do Silício: pediu, de novo, para ser regulado

Em publicação nas redes, defendeu a criação de um órgão nos moldes da FINRA — a autorregulação supervisionada do mercado financeiro americano — para fiscalizar os grandes modelos de inteligência artificial. Não foi um lapso. Em junho, no ensaio “Policy on the AI Exponential”, ele já havia proposto que modelos de fronteira passem por testes obrigatórios e independentes, como aviões antes de decolar, e que o governo dos EUA tenha poder de barrar o lançamento dos que apresentarem riscos inaceitáveis.

A mesma Anthropic, aliás, já aposentou o Claude 2 e, em junho deste ano, tirou do ar mais dois modelos da família Claude 4. Hoje, quem decide quando um sistema de IA nasce, muda ou morre é a empresa que o criou — segundo critérios que ela mesma define. É exatamente esse o incômodo: a companhia age como reguladora de fato da própria tecnologia e, ao mesmo tempo, admite que esse arranjo não se sustenta.

Ceticismo é saudável. Regulação também interessa às big techs: dá previsibilidade, legitima o negócio às vésperas de um IPO bilionário e ergue barreiras de entrada que pequenos concorrentes não conseguem pagar. A tensão pode ser resumida: empresas devem participar da regulação, porque conhecem a tecnologia como ninguém — mas não devem dominá-la, sob risco de captura regulatória. Entre a expertise privada e a legitimidade pública, alguém precisa segurar a caneta.

E o Brasil? Em dezembro, o governo enviou ao Congresso o projeto que

institui o SIA — Sistema Nacional de Desenvolvimento, Regulação e Governança de IA: um Conselho Brasileiro de IA no topo, a ANPD como autoridade residual para normatizar, fiscalizar e sancionar, e os reguladores setoriais, como Banco Central e Anatel, cuidando de seus domínios. No papel, a torre de controle brasileira. Na prática, mais uma peça à espera do tabuleiro: o PL 2338, aprovado no Senado em 2024, segue parado na comissão especial da Câmara, com votação empurrada para depois das eleições.

O resultado é o pior dos mundos: incerteza jurídica. Sem marco legal, quem responde pelo dano causado por um algoritmo? O Judiciário decide caso a caso, sem parâmetros uniformes. A ANPD já anunciou fiscalizações de IA para 2026 e 2027 mesmo sem a lei geral. O TSE regulou deepfakes eleitorais por resolução. Cada lacuna vem sendo preenchida por improviso — e improviso, para quem investe, contrata e desenvolve, tem nome: risco. Regular sob incerteza radical já é difícil; deixar de regular é apenas transferir a conta para os tribunais.

Por isso, a lição não é esperar. Quando até quem constrói a tecnologia pede fiscalização, empresas que a utilizam não podem tratar governança de IA como agenda futura. Inventariar sistemas, avaliar impacto algorítmico, revisar contratos, garantir supervisão humana: nada disso depende de lei publicada — e tudo isso será cobrado, pelo regulador de amanhã ou pelo juiz de hoje. Advogados que dominarem esse vocabulário sairão na frente; os demais lerão o marco legal quando ele já estiver em vigor. Se o próprio piloto está pedindo torre de controle, seguir voando sem plano de voo não é ousadia. É negligência.

(*) - Sócia do Araujo Advs - advogada especializada em Governança de Inteligência Artificial

Brazil Hub leva empresas brasileiras ao ITC Vegas 2026

O mercado brasileiro de seguros terá um espaço próprio no ITC Vegas 2026 (InsureTech Connect). O Brazil Hub, organizado pelo Insurtech Brasil, será um ponto de encontro para empresas e executivos do país durante o maior evento mundial dedicado à inovação em seguros, realizado entre os dias 29 de setembro e 1º de outubro, no Mandalay Bay Convention Center, em Las Vegas (EUA).

A iniciativa foi criada para fortalecer a presença brasileira no evento e proporcionar às empresas um ambiente de visibilidade, relacionamento e geração de negócios dentro do ecossistema internacional de seguros. Além de conectar os próprios participantes brasileiros, o Brazil Hub permitirá apresentar empresas, soluções e iniciativas desenvolvidas no país a executivos, parceiros e potenciais

clientes de diferentes mercados. O espaço contará com quiosques exclusivos para empresas brasileiras, que poderão utilizar a estrutura como base para exposição da marca, apresentação de soluções, reuniões e desenvolvimento de novos contatos durante o ITC Vegas. Cada espaço inclui ainda duas inscrições para o evento, permitindo aos representantes das empresas acesso à programação e

às oportunidades de networking proporcionadas pelo encontro. Para José Prado, CEO do Insurtech Brasil, a proposta é ampliar a visibilidade e as possibilidades de conexão das empresas brasileiras em um dos ambientes mais relevantes da indústria mundial de seguros. “O ITC Vegas reúne algumas das principais lideranças e empresas do mercado global. O Brazil Hub nasce para dar mais visibilidade ao

Brasil dentro desse ambiente e, ao mesmo tempo, criar um ponto de conexão para os nossos executivos. Queremos que as empresas tenham uma referência no evento, possam apresentar o que estão desenvolvendo no país e aproveitem melhor as oportunidades de relacionamento e negócios que uma concentração tão grande de tomadores de decisão proporciona”, afirma (<https://itc.insurtechbrasil.com/>).