Análise de mais de 500 grandes empresas mostra redução nas vulnerabilidades digitais e destaca os principais pontos de atenção em segurança da informação

Um estudo inédito da Zurich, realizado entre 2020 e 2024, revelou uma evolução significativa na maturidade das grandes empresas brasileiras em relação à gestão de riscos cibernéticos. O percentual de organizações com classificação de risco considerada insatisfatória ou ruim caiu de 93% para 55% no período, evidenciando um avanço gradual, mas consistente, na forma como empresas de diferentes setores vêm se preparando para enfrentar ameaças digitais.

As análises abrangeram um total de 577 empresas ao longo de 4 anos, todas com faturamento superior a US$ 10 milhões e pertencentes a uma ampla variedade de setores da economia, como indústria de base, energia, tecnologia, saúde, ensino, transporte, varejo e serviços jurídicos. O número de empresas avaliadas variou ao longo dos anos, incluindo companhias seguradas e não seguradas.

Foram avaliados 23 fatores de riscos de segurança da informação, desde a gestão de ativos, governança, controle de acessos e monitoramento, até planos de resposta a incidentes e recuperação de desastres. O estudo foi construído com base em entrevistas técnicas estruturadas, conduzidas por profissionais do time de Engenharia de Riscos da Zurich, que também entregaram recomendações de melhoria personalizadas às empresas avaliadas.

“Em 2024, 45% das empresas foram avaliadas com uma gestão de risco boa ou excelente, em comparação a 7% em 2020. A evolução na maturidade de riscos das empresas brasileiras é evidente, impulsionada por fatores como o aumento da frequência e da sofisticação dos ataques, a adoção de regulamentações como a LGPD, que impuseram novas responsabilidades às organizações, e o crescimento da conscientização por parte da alta liderança sobre os impactos dos riscos cibernéticos nos negócios”, explica José Bailone, diretor executivo de Seguros Corporativos e Subscrição de Ramos Elementares da Zurich Seguros.

O executivo ainda pontua que, a partir de 2022, é possível observar uma curva ascendente contínua na melhoria da gestão de risco nas empresas. “Os anos anteriores foram marcados pelo pico da pandemia, que necessariamente acelerou a digitalização das empresas brasileiras, muitas vezes de forma desordenada. É natural que a ampliação da exposição e os aprendizados tenham levado, nos anos seguintes, a uma melhora da gestão do risco”, aponta Bailone.

No entanto, o executivo chama a atenção para o fato de que, apesar da melhora substancial, a maioria das empresas ainda está em um nível considerado insatisfatório ou ruim de maturidade. “Ainda há um grande caminho pela frente. Esse estudo nos permite compreender, com base em dados concretos, quais são os principais desafios de segurança da informação hoje para as grandes empresas no Brasil”, destaca.

Onde estão os principais gaps

Além de mapear os avanços, o estudo também identificou quais são os principais pontos de atenção que ainda comprometem a maturidade cibernética das empresas brasileiras.

Segundo Hellen Fernandes, gerente de Linhas Financeiras da Zurich Seguros, as deficiências observadas não estão necessariamente ligadas à ausência de grandes investimentos. “Existem, sim, riscos associados a deficiências tecnológicas, como equipamentos e sistemas, que demandam um investimento maior. Mas as principais lacunas podem ser corrigidas com governança, processos bem definidos e capacitação técnica”, pontua a executiva.

Abaixo, os principais aspectos mais recorrentes entre as organizações avaliadas:

- **Ausência de um plano estruturado para lidar com incidentes cibernéticos:** ou, quando o têm, as empresas deixam de testá-lo regularmente ou de registrar os aprendizados obtidos. Isso compromete a capacidade de reagir de forma ágil e coordenada a um ataque digital, o que pode gerar prejuízos operacionais e reputacionais significativos.
- **Falta de preparo para a recuperação em caso de falhas ou ataques:** muitas empresas não possuem um plano de recuperação de desastres, com estrutura adequada e testes periódicos, há maior risco de paralisação prolongada das operações e perda de dados críticos.
- **Dificuldade em identificar comportamentos suspeitos dentro do ambiente digital:** inexistência de sistemas robustos de monitoramento contínuo, que permitem detectar rapidamente atividades anômalas — como acessos indevidos ou movimentações incomuns de dados — e agir antes que um ataque cause danos maiores.
- **Controles de acesso pouco eficazes:** falta de autenticação de dois fatores (2FA), um recurso básico que adiciona uma camada extra de proteção além da senha. Isso aumenta o risco de acessos não autorizados a sistemas e informações sensíveis, especialmente em contextos de ataques por phishing ou engenharia social.
- **Uso limitado ou inadequado de ferramentas de proteção digital:** mesmo soluções conhecidas, como firewall, segmentação de rede ou filtros de conteúdo e e-mail, muitas vezes estão ausentes ou mal configuradas. Essas ferramentas são fundamentais para bloquear ameaças, limitar movimentações maliciosas na rede e proteger dispositivos e dados contra vazamentos ou invasões.

O papel do mercado segurador

O levantamento teve como base a metodologia da Zurich, aplicada por engenheiros especializados em segurança da informação e baseada no framework internacional NIST — referência global em boas práticas de cibersegurança.

Além do nível de maturidade das empresas e dos principais gaps, o estudo também mostra que as empresas que contaram com o acompanhamento das recomendações pela equipe de engenheiros da Zurich melhoraram a qualificação do risco cibernético em 22%, em média.

“O trabalho de avaliação de risco e recomendações qualificadas da engenharia de riscos da Zurich foi fundamental para redução das fragilidades das empresas, mesmo que não tenham contratado o seguro”, pontua Tiago Santana, Superintendente de Engenharia de Riscos da Zurich. “Isso reforça o papel deste mercado, que vai muito além da oferta do seguro e valoriza a prevenção, com acompanhamento técnico contínuo e adoção de medidas estruturadas para a elevação do nível de proteção”, defende a executivo.

Segundo Tiago, ao consolidar essas análises, é possível orientar os clientes com mais assertividade na definição de prioridades e no fortalecimento de seus processos. “Proteger uma empresa contra riscos cibernéticos envolve, sobretudo, clareza sobre os próprios pontos frágeis e disposição para evoluir continuamente. Nosso papel é contribuir tecnicamente com esse processo, apoiando o mercado na construção de ambientes mais resilientes”, defende.

Segundo o executivo, a Zurich tem buscado ampliar seu apoio técnico às empresas, reforçando o papel do setor como aliado na construção de ambientes mais preparados. A empresa acaba de lançar uma novidade: o programa +Resiliência, um conjunto de serviços especializados em segurança da informação para clientes do produto Zurich Cyber Solutions.

Os serviços do +Resiliência foram cuidadosamente desenvolvidos com base nesse estudo, garantindo que as soluções atendam de forma direcionada às principais necessidades dos clientes. Ao contratar o seguro cibernético, a empresa recebe créditos que podem ser trocados por diferentes benefícios como treinamentos, avaliações e serviços técnicos, de forma flexível e personalizada.

“Os serviços que estamos disponibilizando se somam à proposta de valor do seguro. Como os

clientes podem escolher quais serviços usar, estamos aliando proteção e prevenção de maneira personalizada, fazendo jus ao nosso produto, que, muito mais do que um seguro, se propõe a ser um conjunto de soluções de gestão de riscos cibernéticos para o cliente", conclui Hellen Fernandes, gerente de Linhas Financeiras da Zurich Seguros

Fonte: Zurich/Fato Relevante, em 19.08.2025.