Empresas & Negócios

Matéria de capa

Ionut_Dabijas_Images_CANVA

LGPD

PROTEÇÃO DE DADOS VIROU DIFERENCIAL COMPETITIVO, MAS MATURIDADE AINDA É BAIXA

Proteção de dados virou diferencial competitivo, mas maturidade ainda é baixa no Brasil. Especialistas alertam que segurança da informação segue desconectada da estratégia corporativa e defendem mudança urgente para gestão de risco e resiliência

Apesar dos avanços trazidos pela Lei Geral de Proteção de Dados (LGPD) e do aumento expressivo dos incidentes de segurança no país, a proteção de dados ainda não figura como prioridade estratégica na agenda de muitas empresas brasileiras. Na prática, grande parte das organizações mantém uma postura reativa, direcionando investimentos apenas após episódios críticos, como vazamentos de informações, interrupções operacionais ou a aplicação de sanções regulatórias.

Esse descompasso entre regulação, risco e prioridade estratégica tem impacto direto nos resultados das companhias. De acordo com o Cost of a Data Breach Report 2025, estudo global da IBM em parceria com o Ponemon Institute, o custo médio mundial de uma violação de dados atingiu US$4,44 milhões em 2025. O levantamento aponta uma leve retração em relação ao ano anterior, atribuída principalmente à adoção mais ampla de ferramentas de detecção e resposta a incidentes. No Brasil, no entanto, o cenário segue em direção oposta.

No país, o prejuízo médio por incidente chegou a R$7,19 milhões em 2025, alta de aproximadamente 6,5% na comparação com 2024. Setores como saúde, finanças e serviços estão entre os mais afetados, com perdas que podem ultrapassar R$11 milhões por ocorrência, considerando impactos como paralisações operacionais, danos à reputação e custos associados a sanções e exigências regulatórias.

Para Rodolfo Almeida, CRO da ViperX, empresa especialista em cibersegurança, esse cenário está menos relacionado à ausência de tecnologia e mais à falta de governança estruturada e contínua.“A segurança de dados ainda é acionada, em muitos casos, apenas após um incidente ou auditoria. Falta transformar a proteção de dados em um processo permanente de gestão, com métricas claras, liderança definida e alinhamento aos objetivos de negócio”, afirma.

Afio_Images_CANVA

Pequenas e médias empresas no centro do risco digital

A ideia de que pequenas e médias empresas não figuram entre os principais alvos do crime digital não encontra respaldo no atual cenário de ameaças. Os ataques cibernéticos operam em larga escala, apoiados por processos automatizados que varrem a internet em busca de falhas de segurança, independentemente do porte da organização. Nesse contexto, empresas que operam com e-mails corporativos, dados de clientes ou integrações financeiras passam a integrar o mesmo mapa de risco de grandes companhias.

Além disso, PMEs costumam representar o elo mais frágil das cadeias de fornecimento, ao manterem acessos a sistemas de organizações maiores por meio de credenciais de terceiros, VPNs mal configuradas ou contas sem autenticação multifator. “Do ponto de vista econômico, a PME também é um alvo conveniente para ransomware, já que muitas dependem da operação contínua e não possuem backups testados ou equipes dedicadas de segurança”, destaca Almeida.

> “A segurança de dados ainda é acionada, em muitos casos, apenas após um incidente ou auditoria. Falta transformar a proteção de dados em um processo permanente de gestão, com métricas claras, liderança definida e alinhamento aos objetivos de negócio.

Segundo o executivo, grande parte desse risco pode ser mitigada com medidas básicas, como autenticação multifator, gestão de acessos, atualizações regulares, backups offline, restrição de privilégios e treinamentos contra phishing. “A eficácia da segurança, nesse contexto, está menos na complexidade das soluções e mais na consistência dos controles”, completa.

alexsl_CANVA

Inteligência artificial amplia a escala dos ataques

O avanço da inteligência artificial tem ampliado a escala e a sofisticação dos ataques cibernéticos, especialmente em campanhas de engenharia social e no uso intensivo de automações para explorar vulnerabilidades. No Brasil, fraudes envolvendo deepfakes e identidades sintéticas cresceram 126% entre 2024 e 2025, com o país respondendo por quase 39% desse tipo de caso na América Latina, segundo o Identity Fraud Report 2025-2026 da Sumsub — e ataques considerados “sofisticados” subiram cerca de 180% no mesmo período, reforçando o uso de IA como vetor central nas fraudes digitais.

Diante desse cenário, o especialista recomenda três frentes centrais para as empresas se atentarem em 2026: a identidade digital como novo perímetro de proteção, a capacidade de detecção e resposta contínuas a incidentes e o aumento da resiliência operacional, com políticas de backup e recuperação efetivamente testadas.

“O maior erro é acreditar que a IA resolve tudo sozinha. Os ganhos reais surgem quando tecnologia, processos e pessoas atuam de forma integrada”, conclui o executivo.