



BlackJack3D_CANVA

LEI GERAL DE CIBERSEGURANÇA

A PRÓXIMA GRANDE EXIGÊNCIA REGULATÓRIA DO BRASIL NÃO É TRIBUTÁRIA, É CIBERNÉTICA

A recém-publicada minuta da futura Lei Geral de Cibersegurança pelo Comitê Nacional de Cibersegurança (CNCiber) representa um dos movimentos mais importantes já feitos pelo Brasil no intuito de estruturar a proteção digital do país. Mais do que uma nova regulamentação, trata-se de uma mudança de mentalidade. Nessa nova proposta, a segurança cibernética deixa de ser vista como uma preocupação técnica ou um centro de custo para assumir um papel estratégico na continuidade operacional das organizações.

Willy Andersen (*)

A urgência dessa discussão é evidente. Segundo o relatório Cost of a Data Breach 2025, desenvolvido pela IBM em parceria com o Ponemon Institute, o custo médio global de um incidente de segurança alcançou US\$ 4,4 milhões, valor que inclui interrupção operacional, recuperação de sistemas, perda de produtividade e danos reputacionais.

Nesse contexto, a nova legislação surge para preencher uma lacuna importante. Diferentemente da LGPD, que possui foco na proteção e privacidade de dados pessoais, a futura Lei Geral de Cibersegurança amplia o escopo à toda resiliência operacional das organizações, abrangendo infraestrutura, disponibilidade de serviços, cadeia de suprimentos e capacidade de resposta a incidentes.

Essa diferença é fundamental, porque a LGPD trouxe uma discussão importante sobre governança de dados, mas a Lei Geral de Cibersegurança tende ir muito além, exigindo maturidade operacional em segurança digital. Na prática, isso significa que as organizações precisarão demonstrar capacidade de prevenir, detectar, responder e se recuperar de incidentes cibernéticos que possam comprometer operações críticas.

O principal desafio do Brasil, no entanto, não está apenas na falta de investimento em tecnologia. O problema central é a baixa maturidade em cibersegurança observada tanto no setor público quanto no privado. Ainda existe uma percepção equivocada de que segurança é uma responsabilidade exclusiva da área de TI ou uma despesa que pode ser postergada. Muitas organizações ainda operam sob uma lógica reativa, investindo em segurança somente após um incidente relevante. Essa postura se torna cada vez mais arriscada em um cenário em que ataques são inevitáveis e a capacidade de resposta passa a ser tão importante quanto a prevenção. A nova legislação tende a acelerar a mudança dessa visão, tornando a cibersegurança um tema de governança corporativa e de continuidade dos negócios.

Essa deficiência de maturidade aparece de forma recorrente em estudos internacionais. Pesquisa global da Fortinet aponta que



Ricardo Hiraki

“Ferramentas de IA já estão sendo utilizadas para automatizar ataques, criar campanhas de engenharia social mais sofisticadas e acelerar a exploração de vulnerabilidades.

Divulgação

86% das organizações da América Latina sofreram ao menos uma violação cibernética em 2024, enquanto 63% dos entrevistados atribuíram os incidentes à falta de treinamento e qualificação em segurança da informação. O levantamento também mostra que 35% das empresas da região tiveram prejuízos superiores a US\$ 1 milhão decorrentes desses ataques.

Esse impacto será percebido de forma diferente entre os setores. O segmento financeiro, por exemplo, já possui um nível elevado de maturidade regulatória e operacional, impulsionado pelas exigências do Banco Central e de outras normas do setor. Já áreas como Saúde, Varejo e Agro ainda apresentam lacunas significativas em processos, monitoramento e capacidade de resposta, o que exigirá uma adaptação mais intensa.

No setor público, o impacto também deve ser relevante, principalmente porque os órgãos governamentais provavelmente passarão a exigir conformidade de toda a sua cadeia de fornecedores. Isso cria um efeito cascata no mercado. Empresas que prestam serviços a governos ou a setores críticos, precisarão elevar seus padrões de segurança a fim de continuar operando e participando de contratos estratégicos.

Nesse cenário, a adaptação das empresas não pode começar pela compra de ferramentas. O primeiro passo precisa ser o entendimento da própria maturidade operacional. É necessário identificar quais serviços e ativos são críticos ao negócio, estruturar processos de monitoramento, estabelecer planos de resposta a incidentes e, só então, investir em tecnologia de forma estratégica.

O avanço da inteligência artificial adiciona uma nova camada de complexidade a esse cenário. Ferramentas de IA já estão sendo utilizadas para automatizar ataques, criar campanhas de engenharia social mais sofisticadas e acelerar a exploração de vulnerabilidades. Isso reduz o tempo de reação das organizações e reforça a necessidade de monitoramento contínuo, governança e capacidade rápida de resposta.

Além disso, a nova lei traz um aspecto extremamente relevante ao incluir responsabilidade compartilhada na cadeia de suprimentos. Isso significa que fornecedores e parceiros também precisarão atender a requisitos mínimos de segurança, ampliando o nível de exigência em todo o ecossistema corporativo.

Particularmente, vejo essa movimentação como positiva para o mercado brasileiro. Pois, a construção de maturidade operacional sempre esteve no centro das estratégias. Mais do que implementar ferramentas, o foco deve estar na criação de processos, monitoramento contínuo e capacidade real de resposta. Segurança cibernética eficiente não é apenas tecnologia, é governança, preparo e resiliência.

A futura Lei Geral de Cibersegurança não impedirá que ataques aconteçam. Nenhuma legislação no mundo conseguiu fazer isso. O que ela pode fazer é criar um ambiente de maior preparação, responsabilidade e capacidade de resposta diante de ameaças que se tornam mais sofisticadas a cada ano.

Mais importante do que cumprir uma obrigação regulatória, as empresas terão de compreender que segurança digital passou a ser um fator de competitividade. Organizações capazes de demonstrar resiliência operacional, governança e controle de riscos tendem a conquistar maior confiança de clientes, investidores, parceiros e do próprio mercado.

O Brasil dá um passo importante ao reconhecer que cibersegurança não é apenas um tema tecnológico. É uma questão econômica, estratégica e de soberania nacional. A mensagem da futura legislação é clara, segurança digital deixou de ser uma escolha. Passa a ser um requisito de competitividade, continuidade operacional e confiança. As organizações que compreenderem isso primeiro estarão mais preparadas para crescer em uma economia cada vez mais digital.

(*) Chief Operation Officcer da iTProtect.



Jirak CANVA