Por Marcelo Oliveira (*)

A tecnologia conectou o mundo e, junto com as oportunidades, trouxe a urgência de proteger tudo o que está interligado. Isso porque, na atualidade, não é apenas a eficiência que move as empresas, mas a confiança que elas são capazes de transmitir em cada dado trafegado, em cada conexão estabelecida.

Com isso, a segurança deixou de ser um item de bastidor e passou a ocupar o centro da estratégia corporativa. Ou, em outras palavras, uma falha pode custar não só dinheiro, mas também reputação e credibilidade ao negócio. Nesse cenário, conquistar e manter a conformidade com padrões rigorosos de cibersegurança tornou-se um diferencial competitivo tão importante quanto inovar.

De acordo com a IBM, em 2025, o custo médio de uma violação de dados no Brasil alcançou R$7,19 milhões, contra os R$6,75 milhões registrados em 2024. Esse dado demonstra a escalada dos riscos nas organizações, além da crescente pressão sobre as equipes de segurança cibernética, que precisam lidar com ameaças cada vez mais sofisticadas e ambientes digitais em constante transformação.

Essa pesquisa evidencia que a infraestrutura de conectividade, quando desprovida de padrões

rígidos de compliance e auditoria, pode ser o elo mais frágil de toda a operação. Em vista disso, a busca por certificações reconhecidas de segurança e conformidade deixou de ser um diferencial e se tornou uma exigência básica para empresas que desejam permanecer competitivas em um ecossistema digital cada vez mais regulado e exigente.

Desse modo, as empresas que quiserem alcançar esse novo patamar de compliance devem estar cientes de que isso requer soluções robustas e compromisso contínuo com boas práticas, testes de vulnerabilidade, governança de dados e auditorias independentes. Trata-se de um processo que envolve cultura organizacional, investimento em inovação e alinhamento com padrões internacionais de cibersegurança.

A partir desse caminho, as organizações podem reduzir riscos e fortalecer a reputação e a confiança de clientes e parceiros. Isso ocorre porque, em um mercado em que a conectividade é o alicerce de quase todos os processos corporativos, a segurança se torna o principal elo de credibilidade.

Nesse prisma, parceiros que operam dentro de ecossistemas certificados ganham respaldo para oferecer soluções mais confiáveis e aderentes às exigências legais. Já os clientes finais passam a usufruir de redes mais estáveis, com mais privacidade e menos exposição a incidentes.

Ou seja, toda a cadeia de valor se beneficia, da indústria ao usuário. Por outro lado, empresas que ainda enxergam a segurança como custo e não como investimento, correm o risco de ver seus avanços tecnológicos anulados por falhas básicas de proteção.

Portanto, atingir a conformidade total em cibersegurança não é um ponto de chegada, mas um processo evolutivo que reflete maturidade e responsabilidade digital. Nesse sistema, o verdadeiro diferencial competitivo está na capacidade de transformar segurança em valor percebido, ampliando não apenas a eficiência operacional, como também a confiança que sustenta relações de longo prazo.

No fim, cada camada de proteção instalada é também uma camada de confiança construída. Em tempos em que tudo se conecta, o diferencial não está em ter mais dados, mas em saber guardá-los com responsabilidade, pois é na segurança que a inovação encontra solo fértil para crescer.

(*) **Marcelo Oliveira** é diretor de vendas corporativas da TP-Link, líder global em conectividade que oferece soluções B2B em redes e vigilância com gestão em nuvem.

Fonte: IMAGE, em 19.01.2026