



Mercado Digital

Patricia Knebel

patricia.knebel@jornaldocomercio.com.br

Confira, diariamente, no blog Mercado Digital, conteúdos sobre tecnologia e inovação. Para acessar, aponte a câmera do seu celular para o QR Code.



jornaldocomercio.com/mercadodigital



‘Dívida de resiliência’ impacta segurança nas organizações

Qual o impacto nas empresas da chamada resilience debt, a dívida de resiliência? Muitas organizações acumulam, ao longo do tempo, uma falsa sensação de preparo ao priorizar estratégias formais e investimentos em prevenção, enquanto negligenciam a capacidade real de recuperação após um ataque cibernético.

Estudo encomendado pela Dell Technologies sobre o momento da resiliência cibernética nas empresas mostra que, no Brasil, essa dívida se torna ainda mais evidente quando se observa que 68% dos respondentes discordam que os testes de cibersegurança de suas organizações simulem de forma realista as técnicas modernas de ataque, revelando uma lacuna crítica entre os cenários testados e as ameaças reais.

O estudo, que ouviu 850 líderes globais de grandes empresas, sendo 50 deles no Brasil, mostra que, à medida que a inteligência artificial passa a ser percebida como um fator de risco estratégico, as organizações brasileiras começam a responder com maior automação nos processos de resposta a incidentes.

Outro dado interessante é que, apesar do movimento cres-



Empresas brasileiras incorporam ciber-resiliência, afirma Caroline

cente de investimento em tecnologias avançadas, os dados do estudo mostram que a percepção da liderança nem sempre reflete a realidade operacional.

No Brasil, 48% dos respondentes afirmam que a alta gestão superestima a prontidão da empresa para um grande incidente cibernético, enquanto apenas 36% discordam dessa percepção.

Isso demonstra que, embora as organizações estejam investindo fortemente em automação, IA/ML e aprimoramento de backups,

a percepção de segurança por parte da liderança pode gerar uma falsa sensação de proteção, destacando a importância de alinhar investimentos tecnológicos com avaliações objetivas de capacidade de resposta e resiliência frente a ameaças complexas.

Por outro lado, a pesquisa da Dell aponta que, na prática, a alta gestão das empresas brasileiras discute métricas de resiliência cibernética com frequência significativa: 32% semanalmente e 42% mensalmente, somando 74% das empresas com acompanhamento regular. Isso reflete o grau de prioridade atribuído à resiliência cibernética, corroborado por 90% dos respondentes que afirmam que o planejamento de resiliência é tratado como uma prioridade crítica para os negócios.

“Esses dados mostram que, mesmo em um cenário de ameaças complexas, as empresas brasileiras estão incorporando a ciber-resiliência à agenda estratégica, com monitoramento frequente e reconhecimento da importância de proteger dados, sistemas e operações essenciais”, pontua a líder de Plataforma de Segurança da Dell Technologies no Brasil, Caroline Maneta.

IA é principal motor de investimentos

O avanço das plataformas de Inteligência Artificial (IA) desponta como a principal preocupação em cibersegurança das empresas brasileiras, influenciando diretamente as decisões de investimento.

De acordo com o levantamento, 48% das organizações no Brasil afirmam que o principal motivador para o próximo grande investimento em segurança é a evolução do cenário de ameaças, com destaque explícito para ataques habilitados por IA e riscos na cadeia de suprimentos.

No País, 46% das empresas afirmam ter alto nível de automação, com a maioria das respostas a incidentes já automatizadas, enquanto outros 50% utilizam automação de forma moderada, especialmente para ataques recorrentes como phishing e malware.

A pesquisa mostrou que, embora a automação já esteja relativamente disseminada na resposta a incidentes, o uso efetivo de IA para detecção avançada ainda está em fase de consolidação, especialmente quando o foco são os backups – último recurso em casos de ransomware.

No Brasil, 54% das empresas afirmam utilizar IA ou machine learning de forma ampla para escanear dados de backup em busca de sinais de comprometimento, enquanto 34% restringem essa prática a conjuntos específicos de dados.

Por outro lado, 12% ainda não utilizam IA nesse contexto, seja por

ainda estarem em fase de planejamento (10%) ou por dependerem de métodos tradicionais (2%). Caroline Maneta diz que esse contraste evidencia um ponto crítico: embora as empresas reconheçam a inteligência artificial como um risco estratégico e avancem na automação da resposta a incidentes, nem todas aplicam essa tecnologia de forma consistente na proteção de backups.

“Quando observamos que 36% das organizações brasileiras reconhecem fragilidades na proteção de seus backups, fica claro que ainda existe um desafio relevante na jornada de resiliência cibernética. Os ataques modernos não se limitam à indisponibilidade de sistemas, mas miram diretamente os dados, que são o ativo mais valioso das empresas”, diz. Sem uma estratégia robusta de proteção e validação contínua dos backups, alerta, o risco deixa de ser apenas o ataque em si e passa a ser a incapacidade de recuperação após o incidente.

Ao mesmo tempo em que a IA é reconhecida pelos líderes de TI como uma ameaça crescente no cenário de segurança, também é encarada como uma oportunidade para guiar os investimentos das empresas em resiliência cibernética.

Nesse sentido, 84% das organizações brasileiras planejam priorizar, nos próximos 12 meses, investimentos em automação e detecção de ameaças impulsionadas por IA e machine learning.

Dell Technologies World 2026 acontece essa semana em Las Vegas

Essa semana estou em Las Vegas (EUA) acompanhando o Dell Technologies World 2026, um dos principais eventos globais de tecnologia corporativa, infraestrutura e inteligência artificial.

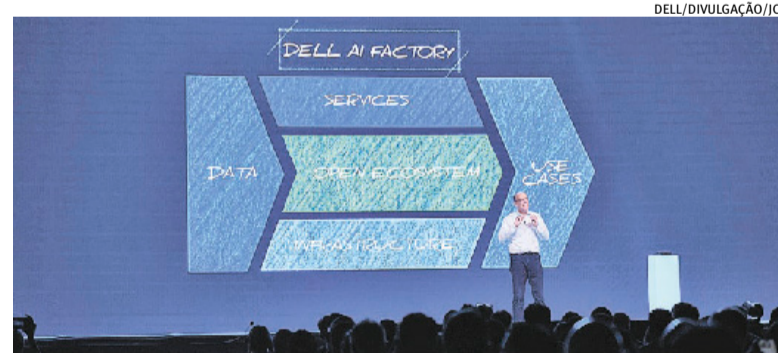
A grande expectativa para esta edição é aprofundar debates sobre como acelerar a transformação de ideias em ações e, especialmente, entender como liderar em um

cenário em que a Inteligência Artificial deixou de ser apenas uma ferramenta e passou a pressionar toda a infraestrutura corporativa.

Depois de reinventar boa parte dos negócios como costumávamos conhecer, agora a IA obriga lideranças a irem além da implementação. Já sabemos o que a inteligência artificial é capaz de fazer, mas qual é a melhor maneira?

Como? A que custo? Essas questões devem guiar muitos dos painéis por aqui.

Sobem ao palco do DTW 2026 nomes como o chairman e CEO da Dell Technologies, Michael Dell; o chairman da VaynerX e empreendedor, Gary Vaynerchuk; o fundador e CEO da Nvidia, Jensen Huang, e o CEO da McLaren, Zak Brown.



SUAS GRANDES IDEIAS, MERECEM O PAPEL PRINCIPAL!

A diferença entre o bom e o inesquecível, está na precisão.



contato@datacertagrafica.com.br
(51) 3365.0383 | (51) 3785.7342
@datacertagrafica