# 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

# Empresas ainda são reativas em segurança

O cenário de cibersegurança nas organizações brasileiras revela uma aparente contradição. Ao mesmo tempo em que há confiança nos investimentos atuais, cresce de forma significativa o direcionamento de recursos para resposta a incidentes, indicando um modelo ainda reativo diante de ameaças cada vez mais sofisticadas.

Dados do CIO Report 2026, realizado pela Logicalis, empresa global de soluções e serviços de tecnologia da informação e comunicação, em parceria com a Vanson Bourne, mostram que 72% das empresas brasileiras aumentaram o orçamento para remediação pós-incidente ou pagamentos relacionados a ataques, enquanto 28% não observaram essa elevação.

Mundialmente, o movimento se repete, com 68% confirmando o aumento do orçamento para remediação.

"O retrato da cibersegurança no Brasil e no mundo é, acima de tudo, paradoxal. Há avanço, investimento e conscientização. Mas também há sinais de que muitas organizações ainda são orientadas pela resposta ao incidente e não pela antecipação da ameaça", analisa o líder de cibersegurança da Logicalis Brasil, Tiago Matias. "Em um ambiente onde ataques são cada vez mais automatizados, sofisticados e imprevisíveis, essa diferença deixa de ser operacional e passa a ser estratégica", acrescenta.

Paradoxalmente, 66% das organizações afirmam que seus orçamentos são suficientes para atender às necessidades críticas de cibersegurança. A leitura combinada desses dados expõe um desalinhamento estrutural. Há recursos, mas sua alocação ainda parece privilegiar o pós-ataque.

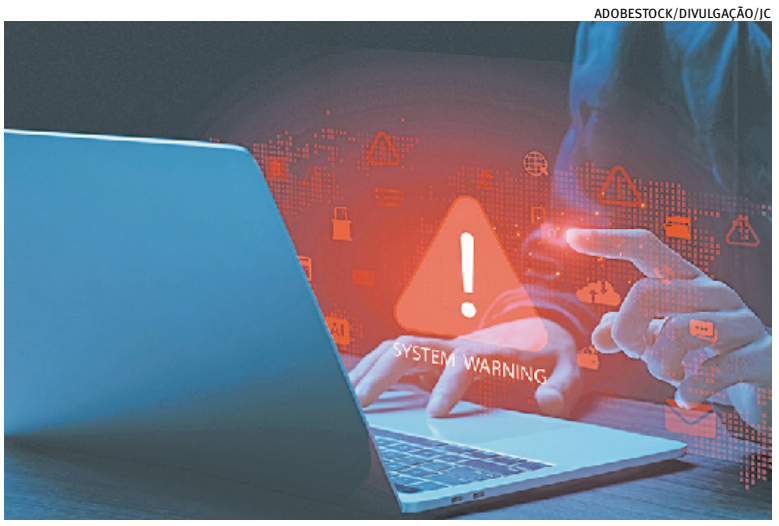
No campo operacional, o Brasil demonstra evolução relevante, embora com lacunas importantes. 58% das empresas realizam pentests regularmente, reforçando uma cultura de validação contínua de prevenção de vulnerabilidades.

No entanto, 40% ainda não executam testes de intrusão de forma consistente e 2% não souberam responder, abrindo espaço para riscos evitáveis. Essa assimetria evidencia que, apesar da conscientização crescente, a disciplina operacional ainda não é homogênea, fator crítico em um ambiente onde ameaças evoluem em velocidade exponencial.

A escassez de profissionais especializados segue como um dos principais gargalos. Em resposta, 94% das organizações no Brasil já adotaram medidas para mitigar o problema, priorizando contratação baseada em habilidades, treinamentos e certificações. O dado revela uma mudança estrutural no mercado. Mais do que tecnologia, cibersegurança tornou-se uma disputa por capital humano qualificado.

Essa transformação também se reflete nas estratégias de contratação. Empresas ampliam o funil de talentos e revisitam paradigmas tradicionais: 58% apostam no desenvolvimento de programas de reentrada profissional e na criação de trajetórias para profissionais que buscam uma segunda carreira em cibersegurança. Outras 56% recorrem à oferta de incentivos financeiros para colaboradores que identificam e evitam proativamente ataques cibernéticos e apenas 6% não possuem planos estruturados, indicando que a pauta de talentos já é consenso no setor.

ADOBESTOCK/DIVULGAÇÃO/JC




CIO Report foi realizado pela Logicalis e Vanson Bourne

Olhando para o futuro, no campo da computação quântica aplicada à cibersegurança, o Brasil ainda apresenta um nível de preparação limitado. 47% das companhias dizem que possuem estratégias mais maduras, 44% estão em estágio parcial e 9% ainda não abordaram o tema. Na prática, 52% das organizações não estão totalmente preparadas para esse cenário, o que pode representar um risco relevante no médio prazo.

Apesar das tensões estruturais, a percepção geral sobre a eficiência dos investimentos é positiva: 66% discordam de que não extraem valor das soluções, 63% discordam de que os sistemas de aplicação de patches de segurança são complexos demais e 58% rejeitam a ideia de que há um investimento exagerado em soluções subutilizadas.

O estudo entrevistou 1 mil profissionais de negócios e TI na EMEA (Europa, Oriente Médio e África), APAC (Ásia-Pacífico) e Américas. Foram ouvidos 100 executivos no Brasil.

## Eve avança na estratégia global de certificação do Eve 100

A brasileira Eve Air Mobility anunciou mais dois avanços no processo de certificação do Eve 100, aeronave elétrica de decolagem e pouso vertical (eVTOL).

A Agência Nacional de Aviação Civil (Anac) abriu uma consulta setorial com revisão dos critérios de aeronavegabilidade da aeronave, enquanto a Eve protocolou junto à Agência Europeia para a Segurança da Aviação (EASA, na sigla em inglês) o pedido para iniciar o processo de validação do Certificado de Tipo.

Os dois marcos reforçam o avanço da estratégia global de certificação da Eve e revelam a atuação coordenada que a empresa vem tendo junto às principais autoridades aeronáuticas, incluindo Brasil, Estados Unidos e Europa, com o objetivo de apoiar futuras operações internacionais.

A publicação dos critérios revisados representa mais uma etapa relevante rumo à certificação de tipo do Eve 100. A consulta permanecerá aberta para contribuições até 18 de agosto. Após isso, a ANAC analisará as contribuições recebidas e avaliará possíveis aperfeiçoamentos dos critérios propostos.

Os critérios revisados sucedem a primeira versão publicada pela ANAC em novembro de 2024 e incorporam o alinhamento com abordagens internacionais de certificação, incluindo as diretrizes da Administração Federal de Aviação dos Estados Unidos para aeronaves de sustentação por potência.

"Esses passos fortalecem ainda mais nossa trajetória rumo à certificação de tipo e apoiam nossa estratégia de levar o Eve 100 aos principais mercados globais", afirma Johann Bordais, CEO da Eve.

A Eve formalizou o pedido de certificação de tipo do eVTOL junto à ANAC em fevereiro de 2022, dando início ao processo de certificação da aeronave.

EVE/DIVULGAÇÃO/JC


Empresa atua de forma coordenada com autoridades aeronáuticas

## AMD e Anthropic anunciam parceria estratégica

A AMD e a Anthropic anunciaram uma parceria estratégica para implantar até 2 gigawatts de GPUs AMD Instinct da MI450 Series em soluções em escala de rack AMD Helios, com a implantação do primeiro gigawatt começando no primeiro semestre de 2027.

A Anthropic está expandindo sua infraestrutura de computação para atender a demanda pelo Claude, e sua adoção do AMD Helios em escala de gigawatts representa mais um passo importante nesse movimento.

Além disso, a AMD e a Anthropic estão iniciando uma colaboração de engenharia para usar o Claude no desenvolvimento acelerado do software da AMD. Especificamente, as equipes usarão o Claude para otimizar cargas de trabalho para as GPUs AMD Instinct e acelerar o desenvolvimento do software ROCm. A AMD também adotará o Claude de forma ampla em suas equipes de engenharia e desenvolvimento de produtos.

A AMD se comprometeu a realizar um investimento estratégico de capital (equity) de até US$ 5 bilhões na Anthropic no futuro.

"Esta colaboração une a liderança da Anthropic em IA de fronteira com toda a força da computação de alto desempenho da AMD. Juntos, aceleraremos a adoção da IA em escala e estabeleceremos o Helios como uma das principais plataformas para a próxima geração de infraestrutura", projeta a Dra. Lisa Su, presidente e CEO da AMD.

Ao combinar uma implantação em escala de gigawatts e a colaboração de engenharia, a meta é construir uma base de longo prazo para acelerar o desenvolvimento e a implementação da infraestrutura de IA de próxima geração.

"O acesso à computação é fundamental para manter o Claude na fronteira da tecnologia", afirma Tom Brown, Chief Compute Officer da Anthropic.