

## OPINIÃO

## Brasil volta ao pódio das maiores economias de TI, mas os desafios ainda continuam

Milton Ribeiro (\*)

Segundo dados da *International Data Corporation (IDC)*, o Brasil reassumiu seu lugar entre as dez maiores economias globais de TI, com um investimento de US\$ 50 bilhões.

Ainda de acordo com o levantamento analisado pela Associação Brasileira das Empresas de Software (ABES), o país superou a Coreia do Sul e Itália, e lidera na América Latina, em que os investimentos somaram US\$ 134 bilhões.

Não há como negar que o setor de Tecnologia da Informação vivencia um período de grande potencial. Esse resultado vem em resposta ao impulsionamento da crescente adoção da transformação digital nos últimos anos, o que coloca o nosso país em posição de destaque no cenário tecnológico global, reforçando sua capacidade de inovação liderada, especialmente, por fintechs, agritechs e healthtechs – além do amplo mercado consumidor digitalmente engajado.

Ainda que o atual momento deva ser encarado com otimismo, dado que o desempenho no ranking favorece a atração de investidores para o país, o setor ainda enfrenta desafios significativos que podem limitar seu crescimento. Dentre eles, é importante chamar a atenção para a escassez de mão de obra qualificada e necessidade de investimento em infraestrutura tecnológica.

De acordo com o levantamento global feito pela Gi Group Holding, em parceria com a universidade tecnológica italiana Politecnico di Milano, no Brasil, apenas 10,9% apontam que não tem dificuldade de encontrar mão de obra qualificada no setor, enquanto 43,7% afirmam que sofrem “um pouco” ou “em grande medida” para encontrar colaboradores com habilidades digitais avançadas.

Por outro lado, à medida que novas tendências tecnológicas, como a Inteligência Artificial, ganham força, cresce a ne-

cessidade de democratizar o acesso à tecnologia. Segundo estudo realizado pela ABES em 2024, a projeção é que, até 2027, haja um crescimento de 67% na adoção de soluções de IA, o que reforça a importância das empresas investirem em iniciativas que tornem essas inovações mais acessíveis.

Além disso, mais do que olhar novas tecnologias, é fundamental fazer o básico e bem feito. Ou seja, além da IA, recursos como *cloud computing* e cibersegurança continuarão tendo impacto e relevância para garantir a aceleração das operações, bem como ajudarão a favorecer o acompanhamento frente aos novos avanços que, certamente, virão ao longo dos próximos anos.

Mesmo o nosso país tendo um reconhecimento global no mercado de TI, para que o setor continue avançando, é fundamental que as empresas estabeleçam um olhar estratégico que garanta constância e consistência das operações. Isso é, ao analisar o mercado e enxergar a dificuldade de encontrar mão de obra qualificada, é imprescindível que as organizações alinhem ações de treinamento da equipe, a fim de capacitá-los e reter esses profissionais.

Os resultados obtidos até aqui mostram que o Brasil é um polo estratégico de outsourcing, startups e inovações tecnológicas, além de também se destacar na criação de soluções locais. Deste modo, para favorecer ainda mais o seu posicionamento frente a outras nações, é importante que sejam alinhadas estratégias que visem potencializar sua competitividade e expansão para novos mercados.

Mais do que celebrar o retorno do Brasil ao ranking das maiores economias de TI, esse é o momento de líderes e gestores tirarem as ideias do papel, estarem atentos aos movimentos do mercado, fazerem avaliações rápidas e estabelecerem as operações em concordância com os pilares da transformação digital. Afinal, sabemos que muito já foi feito até aqui, mas é importante se preparar para o que há de vir.

(\*) Co-Geo da SPS-Group.

## Trump manda cessar home office

Todos os órgãos do governo federal americano receberam instruções do Office of Personnel Management (OPM) para que tomem medidas extinguindo a possibilidade de trabalho na modalidade home office.

Vivaldo José Breternitz (\*)

Na nota, Charles Ezell, chefe interino do OPM, disse que a determinação é dada em função de determinação baixada por Donald Trump e que o trabalho deve voltar a ser presencial em tempo integral, ressalvadas algumas exceções.

Segundo Ezell, citando um recente relatório do Congresso, o home office praticamente irrestrito tornou os serviços governamentais menos eficientes e dificultou a supervisão e o treinamento dos funcionários do governo. Esse relatório acusou o governo Biden de “não ter feito nenhum esforço real para determinar os efeitos do home office generalizado”.

Ainda segundo o relatório, embora o governo Biden tenha falado em benefícios do home office, não existem dados concretos que justifiquem essa afirmação, trazendo ainda acusações aos sindicatos no sentido de terem abusado do processo de negociação coletiva para garantir o home office em tempo integral indefinidamente, impedindo qualquer



Yan\_Krukau\_de\_Pexoto\_CANVA

exigência de retorno aos escritórios.

O relatório conclui dizendo que há evidências de que o home office generalizado está prejudicando os serviços voltados ao cidadão, e recomenda que qualquer trabalho na modalidade home office deve

ser rastreado por meio de sistemas automatizados.

Enquanto isso, aqui no Brasil...

(\*) Doutor em Ciências pela Universidade de São Paulo, é professor, consultor e diretor do Fórum Brasileiro de Internet das Coisas – vjntz@gmail.com.

## Apenas dizer “não clique em links suspeitos” não está funcionando

Vamos começar com uma pergunta básica: o que é um link suspeito, afinal? Essa pergunta, aparentemente simples, revela uma das grandes fragilidades das estratégias de segurança digital. À medida que as fraudes cibernéticas se tornam mais sofisticadas, identificar um link malicioso a olho nu se tornou uma tarefa quase impossível. E, muitas vezes, usuários precisam clicar em links de domínios desconhecidos para realizar suas atividades diárias.

Essa realidade torna evidente que pedir para os usuários “não clicarem em links suspeitos” é uma solução insuficiente e desconectada do cenário atual. O phishing, por exemplo, continua sendo a arma preferida dos cibercriminosos, aparecendo em 41% dos ataques registrados. Isso acontece porque, apesar dos avanços tecnológicos, essa abordagem ainda funciona — e muito bem por sinal.

## Estratégias realistas para enfrentar o phishing

Para mitigar os danos do phishing, precisamos partir do princípio de que, em algum momento, um usuário vai clicar em um link malicioso, seja por descuido, ou por falta de conhecimento. Quando isso acontece, os criminosos exploram duas vias principais: persuadir o usuário a inserir informações em uma página falsa (roubo de credenciais) ou induzi-lo a baixar arquivos maliciosos, como executáveis ou scripts.

No caso do roubo de credenciais, a resposta está em fortalecer políticas de autenticação. Ferramentas como autenticação multifator (MFA) e logon único (SSO) são fundamentais para proteger acessos corporativos. Além disso, incentivar o uso de gerenciadores de senhas e restringir o acesso a dispositivos corporativos são medidas práticas que podem reduzir significativamente os riscos.



Já para prevenir ataques baseados em downloads maliciosos, a solução exige um enfoque técnico e mais robusto. Isso inclui bloquear a execução de arquivos suspeitos, desabilitar a montagem de arquivos .iso. A atualização constante de softwares e a adoção de soluções como monitoramento de endpoints (EDR) e bloqueio automático de ameaças também são estratégias indispensáveis.

## Treinamento ainda é essencial

Embora medidas técnicas avancem na redução de vulnerabilidades, elas não substituem a necessidade de treinar usuários para identificar links suspeitos. Esse treinamento tem um impacto duplo: fortalece a defesa da organização e protege os usuários em suas contas pessoais, que também podem ser alvos de criminosos determinados.

Além disso, capacitar os usuários para reportar e-mails suspeitos transforma cada colaborador em uma fonte potencial de inteligência para a organização. Saber onde e como os ataques estão acontecendo pode fornecer informações valiosas para ajustar e aprimorar as defesas.

## Segurança e usabilidade podem andar juntas

Há quem acredite que é preciso escolher entre segurança e usabilidade. Porém, alcançar o equilíbrio entre esses dois aspectos é a verdadeira chave para uma estratégia realmente eficaz. Com soluções práticas e realistas, é possível permitir que as pessoas realizem suas tarefas com eficiência e, ao mesmo tempo, manter um plano robusto para lidar com as inevitáveis tentativas de ataque.

As fraudes cibernéticas não serão eliminadas, mas a maneira como lidamos com elas pode ser transformada. Investir em tecnologia, fortalecer políticas de autenticação e, sobretudo, educar usuários, cria um ecossistema de defesa muito mais resiliente. A segurança cibernética não é apenas sobre prevenir cliques em links suspeitos, mas sobre construir uma rede de proteção integrada, em que tecnologia e conscientização trabalham lado a lado para enfrentar as ameaças modernas.

(Fonte: Leonel Conti é Diretor de tecnologia da Redbelt Security).

## Investir R\$ 30 milhões em solução de antifraude para expandir no Brasil

Em um mercado em expansão globalmente, a Koin, fintech especializada em simplificar o comércio digital, vai investir cerca de R\$ 30 milhões para avançar em suas soluções de antifraude no Brasil e na América Latina em 2025. Impulsionada pelo aumento das transações digitais e

pela sofisticação das tentativas de fraude, a fintech quer ampliar seu portfólio e trazer novas tecnologias para garantir transações cada vez mais seguras no e-commerce.

“Nosso objetivo é que os lojistas tenham acesso a soluções de antifraude de qualidade com funcionalidades como biometria

e 3DS, protocolo de autenticação de e-commerce, que aumenta a segurança da transação e gera uma melhor experiência de compra, para prevenir perdas em compras online”, explica Dieter Spangenberg, Chief Payments and Fraud (www.koin.com.br).

## News @TI

## App desenvolvido pela Eitri em parceria com a Wicomm alavanca vendas da ToyMania

A Eitri, plataforma para o desenvolvimento de aplicativos que está transformando o varejo brasileiro, continua focada em criar soluções móveis que oferecem três vezes mais produtividade por um terço do custo para as empresas. Exemplo disso foi o trabalho desenvolvido em parceria com a Wicomm para a ToyMania, loja que disponibiliza ampla gama de produtos para todas as idades, incluindo brinquedos educativos e colecionáveis de marcas renomadas como Fisher-Price e Barbie. Durante a semana do Dia das Crianças, a data mais importante do ano para o setor, houve crescimento de 12,5% nas vendas. Além disso, os usuários que navegaram pelo aplicativo registraram um ticket médio de R\$ 247, enquanto a conversão média do app foi de 6%. Segundo o relatório anual da Adjust, empresa de análise de dados e analytics, só em 2023 houve um aumento de 34% na receita das empresas que utilizaram aplicativos, o que acelerou o crescimento desse mercado. Com essa perspectiva, a ToyMania queria oferecer ainda mais praticidade para os seus consumidores (https://www.eitri.tech).

Empresas & Negócios José Hamilton Mancuso (1936/2017)

Laurinda Machado Lobato (1941-2021)

Responsável: Lilian Mancuso

**Editórias**  
Economia/Política: J. L. Lobato (lobato@netjen.com.br); Ciência/Tecnologia: Ricardo Souza (ricardosouza@netjen.com.br); Livros: Ralph Peter (ralphpeter@agenteliterarioph.com.br);  
Comercial: comercial@netjen.com.br  
Publicidade Legal: lilian@netjen.com.br

Webmaster/TI: Fabio Nader; Edição Eletrônica: Ricardo Souza.  
Revisão: Maria Cecília Camargo; Serviço informativo: Agências Brasil, Senado, Câmara, EBC, ANSA.

Artigos e colunas são de inteira responsabilidade de seus autores, que não recebem remuneração direta do jornal.

## Jornal Empresas &amp; Negócios Ltda

Administração, Publicidade e Redação: Rua Joel Jorge de Melo, 468, cj. 71 – Vila Mariana – São Paulo – SP – CEP: 04128-080  
Telefone: (11) 3106-4171 – E-mail: (netjen@netjen.com.br)  
Site: (www.netjen.com.br). CNPJ: 05.687.343/0001-90  
JUCESP, Nire 35218211731 (6/6/2003)  
Matriculado no 3º Registro Civil de Pessoa Jurídica sob nº 103.

Colaboradores: Claudia Lazzarotto, Eduardo Moisés, Geraldo Nunes e Heródoto Barbeiro.

ISSN 2595-8410