## Opinião

# Se a identidade digital é a nova moeda – como protegê-la?

Jason Abbott (*)

*Nos últimos anos, a verificação de identidade digital baseada na captura de documentos e selfies conquistou espaço como símbolo de modernidade, conveniência e segurança.*

De bancos digitais a e-commerce, essa tecnologia promete agilizar o *onboarding*, reduzir atritos e oferecer uma experiência fluida aos clientes.

Mas há um ponto crucial que não podemos ignorar, ID&V, embora essencial, não é a solução definitiva contra as fraudes sofisticadas que enfrentamos hoje. A crença de que um documento digitalizado com perfeição e uma prova de vida convincente sejam suficientes para atestar a identidade de uma pessoa é uma simplificação perigosa.

**Aumento sensível de fraudes – de deepfakes a identidades sintéticas**

Estamos vendo que a identidade é a nova moeda, mas os sistemas de hoje estão quebrados. Somente em 2024, as perdas com fraudes dispararam para US$ 12,5 bilhões, um aumento de 25% em relação ao ano anterior, segundo a Federal Trade Commission (FTC) dos Estados Unidos. De deepfakes a identidades sintéticas, os fraudadores estão explorando brechas em documentos bancários, criptomoedas e até mesmo documentos de identidade emitidos por governos.

Em 2024, o Brasil enfrentou perdas significativas com fraudes online. O setor de e-commerce registrou prejuízos de aproximadamente R$ 7,5 bilhões, enquanto as fraudes envolvendo o sistema Pix aumentaram em 70%, totalizando R$ 4,9 bilhões. Além disso, o número de crimes digitais cresceu 45% em relação ao ano anterior, com cerca de 5 milhões de ocorrências. Esses dados são provenientes de estudos realizados pela Serasa Experian, Security Leaders e pela ADDP – Associação de Defesa de Dados Pessoais e do Consumidor.

Ainda de acordo com a Serasa Experian, em 2025, mais da metade dos brasileiros dizem ter sido vítima de algum tipo de fraude e 20% perderam até R$ 5 mil.

Nesse sentido, a verificação única no onboarding não garante proteção contínua, já que contas legítimas podem ser sequestradas ou usadas por terceiros. A ausência de inteligência contextual nos processos de ID&V agrava o problema, pois documentos e selfies são analisados isoladamente, sem considerar comportamentos, históricos de fraude ou conexões em rede.

O resultado é que muitos fraudadores "passam pela rede", deixando prejuízos financeiros, danos à reputação e perda de confiança.

**A importância de múltiplas camadas**

A resposta não está em descartar a verificação digital, mas em complementá-la com uma estratégia de múltiplas camadas:

**Orquestração de dados:** integra informações de diferentes fontes como crédito, dispositivos, comportamento e históricos internos.

**Modelos de machine learning avançados:** capazes de identificar padrões sutis de fraude, incluindo esquemas de identidades sintéticas e quadrilhas organizadas.

**Decisão em tempo real:** capaz de equilibrar experiência do cliente e mitigação de riscos em milissegundos.

**Análise contínua de clientes:** acompanha o comportamento ao longo do tempo - e não apenas no momento do cadastro.

**O futuro é abrangente, não complacente**

A verificação de identidade digital continua sendo uma peça importante do quebra-cabeça. Porém, diante da sofisticação dos fraudadores, tratá-la como solução única é insuficiente, pois é como verificar o passaporte de um passageiro no embarque, mas nunca escanear sua bagagem, você validou a identidade em um momento, mas não percebeu o risco contínuo.

A verdadeira defesa está em estratégias adaptáveis, inteligentes e integradas, que unem tecnologia, dados e contexto a fim de antecipar ameaças e capturar atividades suspeitas antes que causem impacto.

Só assim as empresas poderão proteger seus ativos, reduzir perdas e, principalmente, fortalecer a confiança na economia digital.

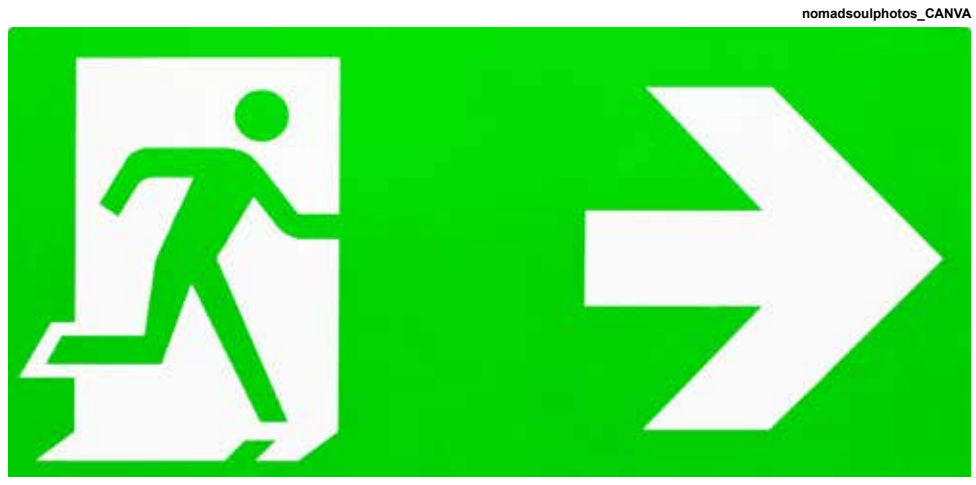
**(*) Diretor de Soluções de Fraude da Provenir.**

# Microsoft, Amazon e Google fogem da China

Com o aumento das tensões entre Estados Unidos e China, gigantes da tecnologia como Microsoft, Amazon e Google estão intensificando seus esforços para transferir a fabricação de seus produtos e seus data centers para fora do território chinês, informou o jornal japonês Nikkei, citando fontes do mercado.

**Vivaldo José Breternitz (*)**

nomadsoulphotos_CANVA



De acordo com o jornal, a Microsoft pretende que até 80% dos componentes de seus notebooks e tablets Surface, bem como dos consoles Xbox e do hardware usado em seus data centers, sejam produzidos fora da China até 2026. A empresa também pretende tirar do país as linhas de montagem de seus produtos.

A Amazon Web Services (AWS), por sua vez, estaria avaliando reduzir a compra de placas de circuitos impressos de sua parceira de longa data, a chinesa SYE - Shenzhen Yaxun Electronic; essas placas são essenciais para data centers de inteligência artificial.

Enquanto isso, o Google estaria pressionando seus fornecedores a aumentar a produção de servidores na Tailândia, onde a empresa já firmou diversas parcerias para o fornecimento de peças, componentes e montagem final, informou também o *Nikkei*.

Adicionalmente, o jornal observa que transferir a produção de forma tão rápida é um desafio, dada a ampla variedade de componentes envolvidos e a reconhecida competência tecnológica e industrial dos parceiros chineses.

O aumento da tensão entre Washington e Pequim tem gerado essas providências e também aumentos de tarifas, restrições à exportação de componentes estratégicos e outras medidas similares.

É provável que tudo isso leve a alterações ainda maiores nos cenários macroeconômico e geopolítico.

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

# A saúde como alvo estratégico de ataques cibernéticos

O setor de saúde vive um momento crítico em termos de cibersegurança. Com a digitalização crescente de prontuários, exames, telemedicina e dispositivos conectados, as instituições passam a lidar com dados extremamente sensíveis — cuja exposição pode trazer não apenas prejuízos financeiros, mas riscos reais à segurança do paciente.

Divulgação

*Denis Furtado*

De acordo com o IBM Security/Ponemon Institute Cost of a Data Breach Report 2023, a indústria da saúde teve o maior custo médio por violação de dados de todas as indústrias: cerca de US$ 10,93 milhões por incidente. Esse valor representa um aumento de mais de 53% desde 2020.

Além do custo financeiro direto, os prazos de detecção e contenção são elevados. O estudo aponta que, em média, leva 204 dias para identificar uma violação e mais 73 dias para contê-la, resultando num ciclo total de aproximadamente 277 dias de impacto.

No Brasil, o panorama também é preocupante. Um relatório recente identificou que o custo médio de uma violação de dados no país chega a R$ 7,19 milhões. Esse valor reflete compromissos legais, recuperação operacional, notificações, perda de confiança e impactos na reputação institucional.

Casos recentes ilustram como as vulnerabilidades se manifestam de forma prática. Na esfera global, foram expostas imagens médicas, raios-X e exames de diferentes hospitais por falhas em dispositivos conectados ou por configurações inseguras, como senhas fracas ou ausência de criptografia adequada.

Também no Brasil, ataques de ransomware e intrusões em provedores de software de saúde mostram que ameaças avançadas como o KillSec conseguem comprometer prontuários, exames de imagem e dados clínicos — ampliando o alcance do dano desde clínicas até grandes redes hospitalares.

Há vários fatores que explicam por que a saúde é tão visada:

**Valor elevado da informação:** dados de saúde pessoal (PHI) são os tipos mais procurados por criminosos, pois combinam informações pessoais e médicas com potencial de uso prolongado (identidade, histórico clínico, etc.).

**Sistemas legados e interoperabilidade:** muitos hospitais ainda dependem de sistemas antigos, pouco atualizados, com falhas conhecidas, dificultando a aplicação de patches ou modernizações seguras.

**Alta necessidade de disponibilidade:** interrupções de sistemas afetam diretamente o atendimento ao paciente — cirurgias, emergências, diagnósticos — o que cria pressões para manter sistemas operando a qualquer custo, por vezes em detrimento da segurança.

**Capilaridade de fornecedores:** provedores de software, equipamento médico conectado, serviços terceirizados etc., formam uma cadeia extensa. Uma falha em qualquer elo pode se propagar a muitas instituições.

Diante desse cenário, algumas medidas já demonstram eficácia real:

- adoção de políticas de autenticação forte (como autenticação multifator) para acesso a sistemas críticos;
- segmentação de rede para isolar ambientes clínicos dos administrativos ou externos;
- testes regulares de vulnerabilidades e auditorias de conformidade;
- planos de resposta a incidentes bem definidos, com simulações e exercícios práticos;
- governança de terceiros (fornecedores), com cláusulas contratuais claras de segurança e responsabilidade;
- proteção de dispositivos conectados, inclusive considerando sua segurança física, configuração, atualização de firmware.

Em resumo, a saúde precisa encarar a cibersegurança como parte integrante de sua missão, e não algo adicional ou opcional. Porque, no fim, não se trata apenas de dados — trata-se de manter instituições funcionando, pacientes seguros e a confiança pública intacta.

**(Fonte: Denis Furtado é engenheiro de sistemas e diretor da Smart Solutions, distribuidora brasileira de solução antifraude e de cibersegurança.**

## News @TI

*ricardosouza@netjen.com.br*

### Alper seleciona startups com foco em IA e automação

@A Alper Seguros, por meio da AlperTech, seu braço de inovação, selecionou cinco startups para a 7ª edição do seu Programa de Aceleração. O Pitch Day, evento que encerra o processo de seleção, consolidou a Inteligência Artificial (IA) como a força motriz do ecossistema de inovação, com todas as finalistas embarcando a tecnologia para resolver dores críticas de mercado. As escolhidas — Blue AI, ESGreen, Fluid, SuperDoc e Vibe Saúde — destacam-se por suas soluções disruptivas em healthtech, greentech e analytics.

### Futuro do varejo e inteligência artificial são destaques no CNC Tech Day 2025

@Na próxima terça-feira (28), o Rio de Janeiro sediará o Tech Day 2025, um encontro que conecta as maiores empresas de tecnologia do país ao varejo brasileiro para compartilhar conhecimento, experiências e soluções que estão transformando a economia. O evento acontece a partir das 8h30min no Auditório do Sesc, na Av. Ayrton Senna, 5.555, Barra da Tijuca, promovido pela Confederação Nacional do Comércio de Bens, Serviços e Turismo (CNC). Serão apresentadas tendências, estratégias e novas experiências de consumo que vão construir o futuro das relações entre marcas e consumidores (https://www.sympla.com.br/evento/tech-day-2025/3138489?utm_medium=email&utm_campaign=aviso_de_pauta__inscricoes_techday_-_outubro_2025&utm_source=RD+Station).

Empresas & Negócios **José Hamilton Mancuso (1936/2017)** **Laurinda Machado Lobato (1941-2021)** Responsável: **Lilian Mancuso**

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

*Webmaster/TI:* Fabio Nader; *Editoração 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.

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

ISSN 2595-8410

**Jornal Empresas & 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.