



OPINIÃO

A transformação dos ERPs com dados, IA e novas exigências de segurança digital

Décio Krakauer (*)

A transformação dos sistemas de gestão empresarial nas últimas duas décadas alterou profundamente a forma como as organizações operam e protegem seus dados.

Se os ERPs dos anos 2000 tinham como principal objetivo integrar processos internos e substituir controles fragmentados, as plataformas atuais assumiram um papel muito mais amplo, concentrando informações financeiras, operacionais, fiscais, comerciais e estratégicas em ambientes altamente conectados.

Essa evolução ocorreu paralelamente à expansão da computação em nuvem, da mobilidade corporativa, das integrações via APIs e da adoção crescente de modelos SaaS. Como resultado, os sistemas de gestão deixaram de ser aplicações isoladas dentro do datacenter corporativo para se tornarem plataformas centrais de ecossistemas digitais complexos, conectando fornecedores, clientes, instituições financeiras, marketplaces, sistemas fiscais e ferramentas analíticas.

Os números ajudam a dimensionar essa transformação, impulsionada principalmente pela migração para a nuvem, pela automação de processos e pela incorporação de novas tecnologias, ao mesmo tempo em que cresce a relevância da segurança digital diante do aumento dos riscos e do custo de incidentes cibernéticos. Nesse contexto, a centralização de informações, que antes representava um ganho de eficiência, passou a concentrar também uma parcela significativa do risco digital das empresas. O ERP tornou-se um dos repositórios mais valiosos para agentes maliciosos, não apenas pela quantidade de dados armazenados, mas pela capacidade de interromper processos críticos quando comprometido.

A mudança arquitetural dos sistemas também transformou a forma como a segurança é abordada. Em vez de depender exclusivamente de barreiras perimetrais, as organizações passaram a adotar modelos baseados em identidade, rastreabilidade e monitoramento contínuo, incorporando práticas como autenticação multifator, criptografia de dados e gestão de vulnerabilidades à própria

estrutura dos ambientes de gestão modernos. A migração para plataformas em nuvem acelerou esse movimento, ao mesmo tempo em que ampliou a superfície de ataque e elevou a necessidade de governança, visibilidade e controle.

Outro aspecto relevante é a crescente pressão regulatória. Leis de proteção de dados, como a LGPD no Brasil, transformaram os sistemas de gestão em elementos centrais da estratégia de compliance, tornando indispensável a capacidade de rastrear informações, controlar acessos e documentar operações.

Essa evolução aponta para uma mudança ainda mais profunda. O ERP deixa de ser apenas um sistema responsável por registrar transações para se consolidar como a principal base de dados corporativa. É nesse ambiente que passam a convergir informações provenientes das áreas financeira, operacional, comercial, fiscal e de relacionamento, formando um patrimônio de dados capaz de sustentar processos automatizados, análises avançadas e, cada vez mais, aplicações baseadas em inteligência artificial. Em outras palavras, o valor estratégico do ERP passa a estar na qualidade, abrangência e confiabilidade dos dados que concentra.

Da mesma forma, a inteligência artificial inaugura uma nova forma de interação com os sistemas de gestão. Em vez de navegar por menus, relatórios e múltiplas telas, os usuários passam a consultar o ERP por meio de linguagem natural, conversando com agentes inteligentes capazes de localizar informações, gerar análises, identificar tendências e executar processos. O resultado é uma transformação significativa na experiência de uso, tornando o acesso às informações mais simples, rápido e contextualizado, além de ampliar o potencial de automação e apoiar decisões com maior agilidade e precisão.

Essa transformação reforça que segurança, governança de dados e inteligência artificial deixaram de ser temas independentes. Quanto mais o ERP se consolida como a principal infraestrutura de dados das organizações e como plataforma para agentes inteligentes, maior é a responsabilidade das empresas em proteger esse ambiente crítico.

(*) CEO da Ramo.



News@TI

Tablet temático voltado para toda a família

@ A franquia Toy Story, da Disney/Pixar, volta a ocupar o centro das atenções de diferentes gerações de fãs. Aproveitando o momento de forte expectativa em torno da estreia de Toy Story 5 nos cinemas, a Positivo destaca o tablet Positivo Vision TAB 7 Toy Story como um dispositivo que leva os personagens da saga para o cotidiano das crianças e combina entretenimento, aprendizado e recursos voltados ao público infantil (<https://loja.meupositivo.com.br/>).

Samsung anuncia resultados extraordinários

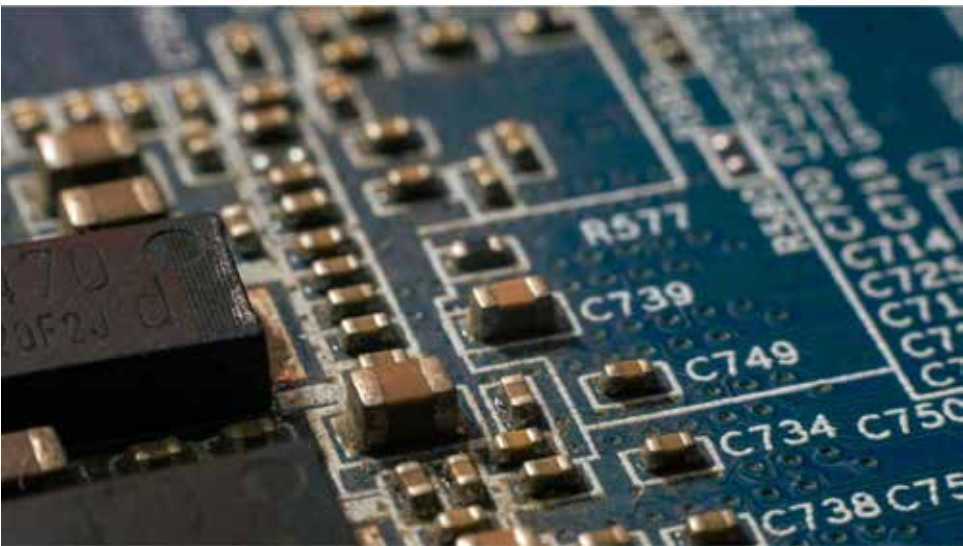
Kim Yong-Kwan, presidente da divisão Device Solutions (DS) da Samsung, afirmou que em 2026 o lucro da unidade de semicondutores da empresa superará todo o acumulado nos cerca de 40 anos de atuação da companhia nesse setor.

Vivaldo José Breternitz (*)

A afirmação foi feita no início desta semana, quando a empresa anunciou os resultados referentes ao segundo trimestre: um lucro operacional de US\$ 58,5 bilhões, acima das projeções do mercado e dos US\$ 53,54 bilhões da Nvidia. Vale lembrar que no mesmo período, os demais negócios da empresa, especialmente smartphones e eletrodomésticos renderam muito mais do que isso.

Os resultados são explicados pela forte demanda de memórias para inteligência artificial, que permitiu que os preços fossem elevados, garantindo margens recordes. A empresa prevê escassez de oferta até 2027 e já anuncia novos aumentos para o terceiro trimestre.

Segundo o jornal Korea JoongAng Daily, analistas projetam que a Samsung DS e sua concorrente SK hynix somem aproximadamente US\$ 97,5 bilhões em lucro operacional apenas no segundo



corelens_CANVA

trimestre, consolidando a liderança sul-coreana na indústria global de semicondutores.

Curiosamente, os ganhos recordes dos trabalhadores da indústria de chips na Coreia estão impactando diretamente a

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

IA generativa eleva sofisticação dos golpes e expõe limites dos modelos tradicionais de prevenção

Em uma realidade digital onde lutamos por 47 segundos de atenção de um cliente legítimo, uma inteligência artificial é capaz de clonar uma voz de forma convincente ou gerar dezenas de deepfakes realistas. Esse dinamismo ajuda a explicar por que 87% das empresas apontam a IA como o risco de segurança que mais cresceu no último ano.

Diante desse cenário, o paradigma de que a confiança no ambiente digital estava ancorada naquilo que era possível ver, ouvir ou validar de forma direta deixou de existir. A evolução tecnológica tornou obsoletos os critérios tradicionais de verificação e elevou o nível de sofisticação das fraudes a um patamar em que a percepção humana já não é suficiente para distinguir o real do manipulado.

O Brasil se tornou um dos principais campos de teste desse fenômeno. Com dimensões continentais, diversidade de documentos, diferentes níveis de digitalização e ampla base de usuários conectados, o país reúne as condições ideais para a experimentação de novas técnicas de fraude. O que funciona aqui tende a escalar globalmente. Nesse contexto, prevenir fraudes deixou de ser apenas uma questão de evitar prejuízo direto e passou a ser um fator determinante para proteger margem, sustentar crescimento e preservar ativos e reputação.

A transformação mais significativa está na qualidade das falsificações. Saímos de erros grosseiros para clones praticamente perfeitos. Deepfakes, identidades sintéticas e manipulação avançada de documentos digitais fazem parte do novo arsenal que desafia inclusive sistemas automatizados. A inteligência artificial superou a capacidade de detecção do olho humano, o que exige uma mudança estrutural no modo como organizações lidam com risco. Não é mais possível confiar apenas no que se vê ou se escuta.

Ao mesmo tempo, existe um paradoxo: as mesmas tecnologias que impulsionam a sofisticação das fraudes também são fundamentais para combatê-las. Sistemas baseados em dados conseguem prever cenários, identificar padrões e aprender com erros. No entanto, há um limite crítico que precisa ser compreendido. A fraude



Shutterstock_CANVA

não ocorre na média, ela está concentrada na exceção, muitas vezes naquele 0,1% que escapa das métricas de alta precisão. Modelos que operam com 99,9% de acurácia trazem uma falsa sensação de segurança e, quando considerados como única camada, ainda deixam espaço suficiente para ataques relevantes.

Isso ocorre porque o fraudador não ataca onde o sistema é forte, mas onde ele é cego e, a cada nova camada de proteção, surgem contra padrões desenhados especificamente para contorná-la. O conceito tradicional de criar barreiras cada vez mais rígidas se mostra insuficiente. É o equivalente a construir muros mais altos enquanto o adversário aprende a voar. O problema não é substituído ao longo do tempo, ele se acumula e se combina com novas técnicas, ampliando o nível de complexidade.

Tal cenário é reforçado pela profissionalização do ecossistema de fraude. Modelos como Fraud as a Service (FaaS), vazamentos de dados em larga escala, ataques de phishing mais sofisticados, uso de máscaras 2D e 3D, além de ataques por coerção e injeção de dados, mostram que não se trata mais de iniciativas isoladas. Existe uma indústria estruturada, com compartilhamento de metodologias e em evolução contínua.

O impacto financeiro é mais amplo do que aparenta. Para cada valor perdido diretamente em fraude, o custo real pode ser quase quatro vezes maior quando se consideram investigação, chargebacks, esforços de marketing e tempo operacional. A discussão deixa de ser apenas sobre perdas diretas e passa a envolver eficiência, experiência do usuário e sustentabilidade do negócio. O dilema entre fricção e segurança se torna central. Em um contexto com atenção cada vez mais escassa, exigir validações excessivas pode afastar clientes legítimos, enquanto flexibilizar demais abre espaço para ataques.

Insistir em modelos baseados em verificações pontuais ou em respostas isoladas não é mais suficiente. A construção de confiança precisa ser tratada como um processo contínuo e orientado por dados. Não se trata apenas de saber se uma imagem é real, mas de analisar contexto, comportamento, padrões de interação, velocidade de digitação, histórico e múltiplas variáveis simultaneamente. É na combinação dessas camadas que se reduz a probabilidade de pequenas falhas se transformarem em grandes prejuízos.

A nova lógica exige flexibilidade e orquestração. Em vez de soluções fragmentadas, é necessário integrar diferentes sinais e tecnologias em um sistema capaz de se adaptar em tempo real. A confiança deixa de ser subjetiva e passa a ser construída de forma mensurável, com base em evidências e aprendizado contínuo.

O avanço da inteligência artificial generativa vai além do desafio tecnológico, constituindo uma mudança de paradigma. Ele obriga empresas e instituições a abandonarem certezas antigas e a reconhecerem que segurança não é um estado fixo, mas um processo dinâmico. Em um ambiente onde não se pode mais confiar plenamente no que se vê ou se ouve, a única resposta viável é evoluir na mesma velocidade, usando dados, contexto e inteligência para reconstruir a confiança em novas bases.

(Fonte: Yolanda Gonçalves é Head de Segurança da idwall, empresa de tecnologia que disponibiliza plataforma de gestão de identidade digital e background check. E-mail: idwall@nbpress.com.br).

 José Hamilton Mancuso (1936/2017) Responsável: Lilian Mancuso	Laurinda Machado Lobato (1941-2021)	José Leonil Lobato (1939-2026)
Editorias <i>Economia:</i> Nelson Tucci (nelson.tucci@netjen.com.br) <i>Mercado/Negócios/Tecnologia/Agronegócios/ Espaço empresarial:</i> Ricardo Souza (ricardosouza@netjen.com.br); <i>Livros:</i> Ralph Peter (ralphpeter@agenteliterarioralph.com.br) <i>Comercial:</i> comercial@netjen.com.br <i>Publicidade Legal:</i> lilian@netjen.com.br	<i>Webmaster/TI:</i> Fabio Nader; <i>Editoração Eletrônica:</i> Ricardo Souza. <i>Revisão:</i> Maria Cecília Camargo; <i>Serviço informativo:</i> 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 & 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: Ana Luisa Winckler, Carol Olival, Claudia Lazzarotto, Denise Debiasi, Fabiana Monteiro, Geraldo Nunes, Heródoto Barbeiro e Neiva Mendes	ISSN 2595-8410	