OPINIÃO

Data center: como a localização influencia o desempenho da sua operação

Julio Dezan (*)

A escolha da localização de um data center sempre foi importante, mas hoje ela pesa mais do que nunca.

A localização influencia diretamente todo o ecossistema de TI: da velocidade de resposta ao suporte técnico, à segurança dos dados, aos custos e à capacidade de crescimento.

Nos últimos anos, muitas empresas apostaram nas grandes clouds globais como caminho natural. No entanto, em determinadas realidades de operação, esse modelo começou a apresentar desafios, como custos imprevisíveis, suporte distante, contratos menos flexíveis e entraves com legislações internacionais. Esses fatores têm levado cada vez mais organizações a repensar o equilíbrio entre centralização e regionalização da sua infraestrutura digital.

Esse movimento já é visível nos números. Segundo a IDC, em 2024, dois terços das empresas brasileiras sinalizaram a intenção de trazer suas operações digitais de volta para estruturas mais próximas, em busca de mais controle, agilidade no suporte e conformidade com a realidade local. Mesmo que tudo pareça acontecer "na nuvem", os dados trafegam por caminhos físicos. E, quanto mais distante estiver o data center, maior o tempo que essa informação leva para ir e voltar. Esses milissegundos se acumulam e podem atrapalhar o funcionamento de sistemas, integrações e ferramentas essenciais no dia a dia.

Quando o data center está fisicamente próximo do usuário final, especialmente com boa conexão local, a história muda. O acesso ao dado é mais estável, trafega de forma mais fluida e a performance melhora consideravelmente. Isso é essencial para aplicações que precisam de respostas rápidas, como ERPs, e-commerces ou plataformas SaaS, que não podem falhar justamente nos momentos de maior demanda.

Ter o data center na mesma região traz vantagens práticas. O suporte técnico está no mesmo fuso horário, fala a mesma língua e, se for preciso, pode agir presencialmente com rapidez. Isso reduz ruídos na comunicação e acelera a solução de problemas, um diferencial enorme em ambientes que não podem parar.

Além disso, manter os dados hospedados no Brasil facilita muito a conformidade com a LGPD. As informações ficam protegidas por leis locais, sem depender de normas internacionais, que muitas vezes são complexas e desalinhadas com o contexto local. E mais: os contratos são feitos em real, o que evita sustos com o câmbio, facilita o planejamento financeiro e torna tudo mais simples do ponto de vista tributário e jurídico.

Quando o data center está posicionado estrategicamente, ele vira uma base sólida para o crescimento. Isso significa mais rotas de rede disponíveis, espaço para expandir a operação e suporte para tecnologias como replicação entre regiões e virtualização. Tudo pronto para acompanhar o ritmo da sua empresa. Com essa estrutura, é possível crescer sem precisar parar tudo ou reinventar a infraestrutura. A empresa pode escalar com segurança, de forma planejada e sustentável.

Em resumo, escolher onde sua infraestrutura vai rodar não é só uma decisão técnica. É estratégica. Afeta diretamente a qualidade do serviço, o controle sobre os dados, os custos da operação e até o ritmo de inovação do negócio. Em um cenário onde a tecnologia está no centro de tudo, a localização do data center precisa estar no centro da sua estratégia digital.

(*) Diretor de Operações da EVEO.

Ciberataques podem gerar tragédias

Autoridades norueguesas atribuíram oficialmente à Rússia um recente ciberataque contra uma barragem em Bremanger, no oeste do país, levantando preocupações sobre possíveis ações de sabotagem contra infraestruturas críticas de toda a Europa.

Vivaldo José Breternitz (*)

É a primeira vez que Oslo estabelece um vínculo formal entre esse tipo de ataque e atores pró-Rússia.

O incidente ocorreu em abril, quando hackers conseguiram acessar remotamente os sistemas de computador da barragem e abriram uma válvula. Segundo a agência Reuters, o ataque liberou cerca de 600 litros de água por segundo, durante quatro horas seguidas, antes de ser detectado e interrompido pelos operadores da barragem.

Embora não tenham sido registradas vítimas ou danos materiais após o despejo de aproximadamente 9 milhões de litros de água, serviços de inteligência afirmam que a ação integra uma campanha mais ampla destinada a intimidar e desestabilizar a população.

Durante uma coletiva à imprensa, Beate Gangås, a chefe do Politiets sikkerhetstjeneste, Serviço de Segurança da Polícia da Noruega, principal agência de inteligência doméstica do país e responsável por contrainteligência e contraterrorismo, disse que "O nosso vizinho russo se tornou mais perigoso e eu quero que nossos compatriotas estejam preparados".

A Noruega e a Rússia têm uma fronteira comum de 198 quilômetros, no extremo norte da Europa, na região do Círculo Polar Ártico.

Provas do ataque surgiram em um vídeo de três minutos publicado no Telegram, com marca d'água de um grupo cibercriminoso pró-Rússia. Fontes da polícia norueguesa confirmaram a autenticidade do material à emissora NRK, observando que, embora conteúdos semelhantes já tenham circulado em redes sociais, este caso representa a primeira invasão confirmada à infraestrutura hídrica norueguesa desde 2022.

A polícia informou ao jornal Aftenposten que o grupo responsável é composto por hackers que operam em parceria e que já desfecharam diversos ataques contra empresas ocidentais nos últimos anos.

Petra_Nesti_de_Pexels_CANVA

Demonstrando como ataques como esses vem se tornando comuns e perigosos, é oportuno lembrar que câmeras que controlam rodovias holandesas foram tiradas do ar recentemente, ao que parece também por hackers russos.

(*) Vivaldo José Breternitz, Doutor em Ciências pela Universidade de São Paulo, é professor e consultor – vjnitz@gmail.com.

Por que proteger dados virou questão de sobrevivência empresarial

Cada vez mais conectadas e dependentes da tecnologia para operar, empresas de todos os portes estão na mira de cibercriminosos. No Brasil, o setor de cibersegurança movimentou R$ 17 bilhões em 2024, de acordo com levantamento da consultoria Peers Consulting + Technology. A expectativa é de que esse número cresça 9% em 2025, impulsionado principalmente pela crescente demanda por soluções que protejam dados e sistemas contra ataques cada vez mais frequentes e sofisticados.

Ainda segundo o estudo, o país sofre, em média, 140 mil ataques cibernéticos por ano. São invasões, sequestros de dados, tentativas de fraudes e outras ações maliciosas que colocam em risco tanto as operações quanto a reputação das empresas.

Para o especialista em segurança digital Felipe Berneira, CEO da Pronnus Tecnologia — empresa do Grupo Sancon, de Santa Catarina — o aumento no número de ataques está diretamente ligado ao avanço tecnológico e à falta de atenção sobre as vulnerabilidades das empresas. "As ameaças se tornaram mais complexas e direcionadas. Hoje, os criminosos não atacam mais no escuro. Eles estudam as empresas, identificam vulnerabilidades específicas e exploram brechas com precisão", explica.

Grupo Sancon

Felipe Berneira é CEO da Pronnus Tecnologia e especialista em soluções de segurança da informação.

Segundo ele, é comum que pequenas e médias empresas subestimem os riscos, acreditando que não serão alvo de ataques. "Essa é uma percepção perigosa. Cibercriminosos muitas vezes veem essas empresas como alvos fáceis, justamente por não investirem o suficiente em proteção. E um único ataque pode comprometer toda a operação, causar prejuízos financeiros consideráveis e danos irreparáveis à imagem da marca", alerta.

O cenário atual também tem impulsionado a busca por soluções como backups criptografados, firewalls de última geração e resposta rápida a incidentes. De acordo com o especialista, não existe proteção absoluta, mas é possível dificultar a ação dos criminosos. Para Berneira, a segurança digital precisa deixar de ser vista como um custo e passar a ser encarada como investimento estratégico.

Além de manter sistemas e softwares atualizados, ele recomenda que as empresas invistam em uma cultura de segurança que envolva todos os colaboradores. "A conscientização é essencial. Muitas invasões começam com um simples clique em um link malicioso. Por isso, todos na empresa devem estar preparados para identificar e evitar esse tipo de armadilha", reforça.

News @TI

Câmeras corporais para o mercado corporativo

@O Oakmont Group anuncia o lançamento da Linha Enterprise da Axon, líder mundial em soluções para segurança, uma iniciativa que marca a entrada das avançadas câmeras corporais Axon Body 4 no universo corporativo. A nova linha é voltada para empresas que buscam elevar o nível de proteção, controle e qualidade operacional em segmentos como varejo supermercadista, saúde, logística e hotelaria. A Linha Enterprise representa uma expansão estratégica do Oakmont, em parceria com a Axon, e traz recursos como gravação em alta definição, transmissão em tempo real, integração com plataformas de armazenamento seguras, além de IA embarcada para acionamento automatizado e gestão remota de evidências (https://www.axon.com/).

Trela lança Concierge

@Quando o assunto é fazer mercado, na loja física ou no app, pouca coisa mudou desde os corredores dos anos 1980. A Trela quer mudar isso. E acaba de dar mais um passo nessa jornada com o lançamento do Concierge Trela, o primeiro assistente inteligente de compras do Brasil. A ferramenta usa inteligência artificial para entender as preferências de cada cliente e oferecer uma experiência de compra fluida, eficiente e sob medida. Pelo WhatsApp, o consumidor pode pedir sugestões específicas, como "lanches saudáveis pros meus filhos" ou "jantar leve para duas pessoas", ou apenas enviar sua lista da semana.

O primeiro centro da América Latina com foco na aplicação de IA na transição energética

O Centro Universitário ENIAC, em parceria estratégica com a Mind Source Brasil, anunciou o lançamento do CEPAITE, o primeiro centro da América Latina com foco dedicado na aplicação de Inteligência Artificial na Transição Energética. O projeto surge com forte atuação em inovação aplicada e formação de talentos, unindo pesquisa de ponta, conhecimento técnico e visão de mercado para gerar impacto positivo. Criado em um cenário de desafios relacionados às energias eólicas e solares no Brasil, o CEPAITE visa conectar ciência, tecnologia e setor produtivo para acelerar a transição energética brasileira com soluções em inteligência artificial aplicada, promovendo eficiência, sustentabilidade e inovação.

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.