Da virtualização à IA: 20 anos de evolução na proteção de dados

Mauricio González (*)

Quando revisito os últimos 20 anos e lembro de como a indústria de tecnologia discutia seus principais desafios, fica evidente o quanto esse cenário se transformou. Naquele momento, a virtualização começava a redefinir os data centers, as empresas buscavam ganhar eficiência em suas infraestruturas e a disponibilidade dos ambientes se consolidava como uma prioridade para garantir a continuidade dos negócios.

Foi nesse contexto que a Veeam nasceu, em 2006, com o propósito de acompanhar a evolução dos ambientes virtualizados e ajudar as organizações a proteger seus dados de maneira mais ágil, eficiente e confiável.

Duas décadas depois, o cenário é completamente diferente. Hoje, os dados estão distribuídos por diferentes ambientes. As empresas operam em estruturas híbridas e multinuvem, dependem cada vez mais de aplicações SaaS, enfrentam ameaças como o ransomware e aceleram a adoção da inteligência artificial para transformar a forma como trabalham, tomam decisões e inovam.

Essa evolução traz uma conclusão importante. A proteção de dados já não pode ser tratada apenas como uma responsabilidade técnica. Ela se consolidou como uma prioridade estratégica para organizações que precisam operar com confiança em um ambiente cada vez mais distribuído, dinâmico e sujeito a novos riscos.

De backup à resiliência

A virtualização representou um ponto de inflexão para a indústria. Permitiu que as empresas otimizassem recursos, reduzissem custos e ganhassem flexibilidade, mas também trouxe novos desafios. Os modelos tradicionais de backup nem sempre estavam preparados para responder à velocidade e ao dinamismo desses novos ambientes.

Com o avanço da transformação digital, o desafio cresceu ainda mais. As organizações começaram a transferir cargas de trabalho para a nuvem, adotar aplicações SaaS e distribuir suas informações entre múltiplas plataformas. O desafio passou a ser proteger os dados críticos de forma consistente, independentemente do ambiente em que estejam.

Hoje, uma empresa pode ter informações em data centers locais, nuvens públicas, plataformas SaaS, dispositivos distribuídos, ambientes Kubernetes e aplicações impulsionadas por IA. Essa dispersão torna a proteção de dados mais complexa, mas também mais necessária do que nunca.

E então o ransomware mudou definitivamente essa perspectiva. Durante anos, o backup foi tratado principalmente como um recurso de recuperação diante de falhas, erros operacionais ou perdas acidentais de informação. As ameaças atuais, porém, elevaram a recuperação de dados a um componente estratégico de qualquer abordagem de cibersegurança.

Na minha perspectiva, as organizações precisam ir além da capacidade de prevenir um ataque e avaliar se estão realmente preparadas para se recuperar rapidamente, com dados limpos, confiáveis e validados. Em um ambiente no qual uma interrupção pode comprometer operações, receitas, reputação e a confiança dos clientes, a resiliência de dados passou a ter a mesma relevância estratégica que a prevenção.

A nova etapa: confiança em dados e IA

Agora estamos diante de um novo ponto de inflexão: a inteligência artificial. As empresas querem usar IA para automatizar processos, melhorar a tomada de decisões, otimizar operações e criar novas experiências. Mas há algo que não devemos perder de vista. A IA só pode gerar valor se for alimentada por dados confiáveis.

Isso abre uma conversa muito mais ampla. Já não basta proteger os dados. As organizações precisam saber onde eles estão, quem tem acesso a eles, como são governados, se estão em conformidade com as regulamentações aplicáveis e se podem ser recuperados de forma segura diante de um incidente.

Nesta nova era, marcada pela automação e pelos agentes de IA, a confiança nos dados será uma condição indispensável para inovar com responsabilidade. Essa confiança começa na qualidade e na integridade das informações e, nesse novo cenário, exige uma abordagem capaz de integrar governança, privacidade, conformidade, segurança e resiliência em uma camada unificada de confiança para dados e IA.

Nesses 20 anos, essa evolução levou a proteção de dados de uma abordagem centrada em backup para uma visão baseada em disponibilidade, resiliência e, agora, confiança. Os dados deixaram de ser apenas um recurso operacional, passando a ocupar uma posição central na continuidade dos negócios, na experiência do cliente, na inovação, na conformidade regulatória e na adoção de novas tecnologias.

Por isso, acredito que a proteção de dados já não pode ser vista como uma tarefa isolada da área de TI. Ela deve fazer parte de uma estratégia integral de resiliência empresarial, na qual tecnologia, processos, governança corporativa e cultura organizacional trabalham em conjunto.

Os próximos 20 anos serão definidos pela inteligência artificial, pela automação e pela necessidade de confiança contínua nos dados. O desafio para as organizações será proteger, governar, validar e recuperar suas informações em escala, com a certeza de que podem operar e inovar com segurança.

Porque, na era da IA, a inovação não começa com um algoritmo. Começa com dados seguros, governados, disponíveis e confiáveis.

(*) Vice-presidente da Veeam para a América Latina.





A Outra Sala

Ana Luisa Winckler

Ameaçaram uma vida. Estamos julgando a biografia

Uma pessoa está sendo ameaçada de morte.

Qual é a sua primeira pergunta?

"O que estão fazendo para protegê-la?"

Ou: "Mas o que ela fez?"

A segunda pergunta pode buscar contexto. Mas merece atenção quando a resposta serve para tornar a ameaça mais aceitável.

Ana Elisa Santos Silva, deputada federal eleita, denunciou ameaças de morte, de violência sexual e ataques racistas. A Polícia Federal investiga o caso. Medidas de proteção estão em execução.

Antes de qualquer consideração sobre o que ela pensa, diz ou representa, há uma pessoa ameaçada.

Isso deveria bastar para que sua segurança fosse uma preocupação comum.

Deveria.

Quero propor um exame menos confortável do que condenar a violência em público: observar o instante em que descobrimos quem é a pessoa ameaçada.

A gravidade permanece a mesma? Ou começamos a procurar na biografia alguma coisa que torne nosso desconforto menor?

Pense em frases como estas:

"Também, ela provoca."

"Quem se expõe precisa estar preparado."

O raciocínio merece ser confrontado: transformar a exposição de alguém em autorização para violentá-lo.

Desde quando ocupar um espaço significa consentir em viver sob ameaça?

A psicologia oferece uma lente para examinar esse deslocamento. A crença em um mundo justo pode nos levar a procurar na conduta da vítima uma justificativa para o que ela sofre. É uma tentativa de preservar alguma sensação de ordem: se acreditarmos que a pessoa sofreu violência porque fez algo errado, podemos imaginar que estaremos seguros fazendo tudo certo.

Essa interpretação pode confortar quem observa. Para quem está ameaçado, acrescenta outra exigência: além de enfrentar o medo, precisa demonstrar que não fez nada para merecê-lo.

Como se uma biografia irrepreensível fosse requisito para receber proteção.

Perguntar sobre circunstâncias é necessário para investigar. Usá-las para relativizar uma ameaça é uma escolha que precisa ser nomeada.

No caso de Ana Elisa, também precisamos nomear o racismo e a violência dirigida a ela como mulher. Quando as ameaças incluem conteúdo racista e violência sexual, tratá-las como hostilidade genérica apaga dimensões centrais do que foi denunciado.

E os efeitos podem ultrapassar sua vida individual. Outras mulheres negras podem olhar para essa violência e calcular o custo de também ocupar espaços de visibilidade e poder.

A ameaça pode começar a cumprir seu objetivo antes de qualquer agressão física: quando restringe uma saída, interrompe o sono, altera um caminho ou faz alguém pensar em desistir. A pessoa continua viva, mas sua liberdade já está sendo reduzida.

Então pedimos coragem.

Mas quanto da coragem que celebramos nas mulheres corresponde à proteção que deixamos de garantir?

Tenho resistência a transformar toda mulher ameaçada em exemplo de força. Ela pode estar apavorada. Pode querer parar. Pode não encontrar nenhuma lição bonita no que está vivendo.

Sua segurança não pode depender da capacidade de nos inspirar.

Também não deveria ser necessário dizer que ela poderia ser nossa filha. Ela já é alguém. Essa condição deveria ser suficiente.

Podemos discutir a adequação das medidas de segurança, com critérios e avaliação de risco. **O que não podemos usar como critério é o quanto gostamos da pessoa que precisa delas.**

Onde erramos enquanto sociedade?

Uma parte do erro está em exigir identificação antes de reconhecer um direito. Outra está em imaginar que nossa responsabilidade termina porque não fomos nós que ameaçamos.

Há responsabilidade também na conversa em que a violência vai se tornando aceitável. No comentário que transfere a culpa. Na cobrança de prudência dirigida apenas a quem está com medo.

Ameaçaram Ana Elisa. É a conduta de quem ameaça que precisa ser interrompida.

Uma sociedade precisa sustentar proteção também onde não existe afeto. Para a pessoa difícil. Para quem nos decepcionou. Para quem jamais convidaríamos à nossa mesa.

Talvez a pergunta seja menos "onde erramos?" e mais: **o que continuamos aceitando quando a vida ameaçada não nos comove?**

Não controlamos sentir a mesma proximidade por todas as pessoas. Podemos, porém, assumir a responsabilidade de não transformar essa diferença em uma hierarquia de direitos.

Se descobrir quem é a pessoa muda a gravidade da ameaça para você, o que, exatamente, você está avaliando?



(*) - Psicóloga por formação e inconformada por vocação. Há mais de 25 anos atua na transformação de culturas organizacionais, desenvolvimento de lideranças e reinvenção de modelos que aproximem empresas das pessoas — e não o contrário. Já esteve à frente de áreas estratégicas de RH em grandes corporações nacionais e multinacionais, do chão de fábrica ao boardroom, do Norte ao Sul do Brasil.

Fim da escala 6x1: a produtividade da logística precisa vir da eficiência, não do esforço humano

Flávio Piccinin (*)

O fim da escala 6x1 e a redução gradual da jornada de trabalho colocam um desafio importante para o setor logístico brasileiro: como manter a capacidade de atendimento com menos horas disponíveis, sem elevar os custos de forma desproporcional ou sobrecarregar os trabalhadores?

A resposta não está necessariamente em contratar mais pessoas, ampliar turnos ou acelerar o ritmo das operações. Antes disso, precisamos olhar para dentro dos centros de distribuição e identificar quanto tempo é desperdiçado por problemas que poderiam ser resolvidos com engenharia e planejamento.

Em muitos armazéns, os operadores percorrem distâncias excessivas, enfrentam corredores congestionados, aguardam equipamentos ou precisam realizar movimentações desnecessárias para acessar uma mercadoria. São atividades que consomem horas de trabalho sem acrescentar produtividade.

Um exemplo ajuda a dimensionar o problema: se uma operação perde apenas um minuto em cada movimentação, repetida 500 vezes por dia, são mais de oito horas de capacidade operacional consumidas diariamente.

Produtividade não é fazer o trabalhador se movimentar mais rápido. É fazer com que ele precise se movimentar menos para produzir o mesmo resultado.

É nesse contexto que a engenharia de armazenagem ganha ainda mais importância.

A revisão dos layouts, o reposicionamento de produtos de maior giro, a modernização das estruturas e a eliminação de cruzamentos de fluxo podem recuperar capacidade operacional sem exigir necessariamente a expansão das instalações.

Temos exemplos de projetos em que a substituição de sistemas drive-in por soluções com carros satélites melhorou o aproveitamento das posições-palete e reduziu deslocamentos. Em operações de carga fracionada, sistemas flow-rack também facilitaram o acesso aos produtos e diminuíram movimentações durante a separação de pedidos.

Dependendo das características da operação, reduções de 20% a 30% nos deslocamentos e manuseios podem representar um potencial de melhoria, embora cada projeto exija avaliação específica.

Outro cuidado é não confundir capacidade de armazenagem com produtividade. Aumentar a quantidade de posições-palete não significa necessariamente tornar uma operação mais eficiente. Se o ganho de densidade comprometer o acesso aos produtos ou gerar congestionamentos, o resultado pode ser exatamente o contrário.

O mesmo raciocínio vale para a automação. Investir em tecnologia sem antes revisar os processos significa correr o risco de automatizar ineficiências que já existem.

Por isso, diante das mudanças na jornada de trabalho, minha recomendação aos gestores é começar pelo diagnóstico. Medir deslocamentos, esperas, produtividade por hora, custo por movimentação e capacidade de expedição permite identificar onde estão as oportunidades reais de melhoria.

A redução da jornada pode acelerar a modernização da intralogística brasileira. Mas essa transformação precisa partir de uma mudança de mentalidade.

O futuro da produtividade nos armazéns não deve depender de exigir mais esforço das pessoas, mas de projetar operações que precisem de menos movimentos para entregar melhores resultados.

(*) Diretor executivo da ISMA, empresa especializada em soluções para armazenagem intralogística, com 56 anos de atuação no mercado brasileiro.