

IT Insight



#63 SETEMBRO 2026

**media
NEXT**
STAY AHEAD · STAY RELEVANT



PARA ALÉM DA NUVEM: NO CAMINHO DO EDGE

claranet®

Shift Happens

22 de setembro, Lisboa

TOMORROW
BECOMES
CLEAR

Inscrições abertas ●

Código: SHIFT26_GUEST



IT Insight



#63 SETEMBRO 2026

IN DEEP

**PARÁ ALÉM DA NUVEM:
NO CAMINHO DO EDGE**

d_Al_gest por Henrique Carreiro

WISHLIST

Samsung Galaxy Z Fold8 Ultra: o dobrável que merece estar na secretária de um executivo?

BEST OF BREED | CYBERSECURITY RESILIENCE & ZERO TRUST

Zero Trust: a segurança que começa onde o perímetro acabou

360° VIEW | RUI OLIVEIRA, SALSA JEANS

“O CIO será um agente de transformação”

IN DEEP | BEYOND CLOUD: THE RISE OF EDGE AND DISTRIBUTED COMPUTING

A cloud deixou de ser o único destino

ROUND TABLE | FUTURE OF WORK & DIGITAL LEADERSHIP

Enterprise mobility: a mobilidade passou a ser uma questão de arquitetura

FACE 2 FACE

SOFIA TENREIRO, SIEMENS PORTUGAL

“Precisamos de garantir que a base está sólida para a IA poder retirar valor do mundo real”

ROUND TABLE

FUTURE OF WORK & DIGITAL
LEADERSHIP

FACE 2 FACE

**SOFIA TENREIRO,
SIEMENS PORTUGAL**



ZERO TRUST + AI

Acelere a inovação
com a segurança
que a era da IA exige

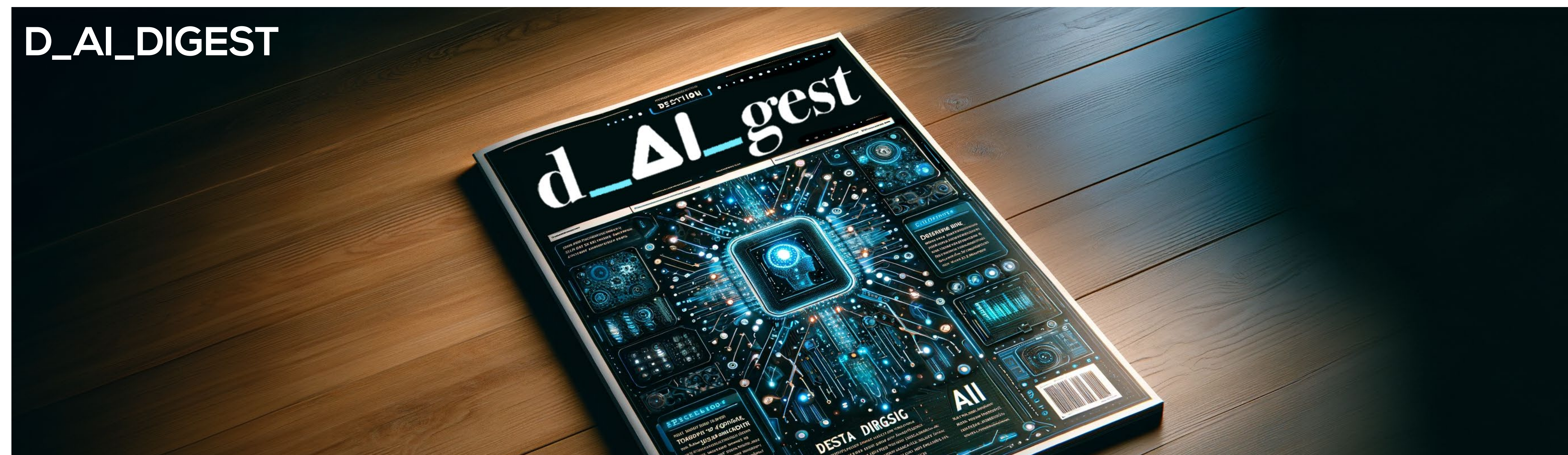


IT Insight



#63 SETEMBRO 2026

D_AI_DIGEST



IN DEEP

BEYOND CLOUD: THE RISE OF EDGE AND DISTRIBUTED COMPUTING

claranet Na tecnologia, a periferia ainda é uma escolha

BEST OF BREED

CYBERSECURITY RESILIENCE & ZERO TRUST

 **EXCLUSIVE NETWORKS** Cibersegurança industrial: quatro tensões que vão definir a proteção da operação até 2027

 **NetApp** Best of Breed: Ciber-Resiliência e Zero Trust na Era da Complexidade Digital

 **oramix** Quem comprou Zero Trust, comprou autenticação

 **zscaler** Zscaler posiciona o Zero Trust como resposta decisiva para proteger a IA nas empresas

BRANDED CONTENT

 **avanade** A governance como ponto de partida para escalar a IA nas organizações

 **Red Hat** Red Hat: “A maioria das organizações ainda está a acumular dívida técnica”

WISHLIST

SAMSUNG GALAXY Z FOLD8 ULTRA



BEST OF BREED

CYBERSECURITY RESILIENCE & ZERO TRUST



360° VIEW
RUI OLIVEIRA





netapp.com/artificial-intelligence/aipod/ | netapp.ecs.pt@arrow.com

SOLUÇÃO IA CHAVÉ NA MÃO

IA EMPRESARIAL PARA
IMPLEMENTAÇÃO RÁPIDA



A SOLUÇÃO COMPLETA PARA OS INTEGRADORES DE TECNOLOGIA EM PORTUGAL

PRONTO A FUNCIONAR
EM MINUTOS

INCLUI HW GPU POTENTE
E SW AVANÇADO

TOTALMENTE
ON-PREMISES

ROI IMEDIATO E
SEGURANÇA DE DADOS



HENRIQUE CARREIRO

E, no entanto, o novo “edge” move-se

NOS PRIMEIROS QUATRO DIAS após ter sido posto à venda por 399 dólares, a Hugging Face vendeu mais de dez mil unidades do Microduck, criado pela sua subsidiária Pollen Robotics, um pequeno robô bípede de 25 centímetros. O preço de venda e o facto de o robô se assemelhar muito a um “*cartoon*” ajudam naturalmente a explicar o entusiasmo em torno do lançamento mas, provavelmente, o maior interesse estará no que os compradores farão com o seu novo brinquedo. O Microduck chega com sete comportamentos treinados, entre andar, sentar-se, pontapear uma bola ou levantar-se depois de cair. Cada um desses comportamentos é uma “*policy*”, um modelo que transforma aquilo que o robô observa numa

decisão sobre o que deve fazer a seguir. O comportamento do robô é inteiramente extensível pelo utilizador — dentro, naturalmente, das limitações físicas de um robô deste tamanho e preço.

A proposta da Hugging Face é particularmente interessante nesse aspeto, como seria de esperar pelo histórico da empresa como repositório de modelos e *datasets*. O utilizador pode treinar um comportamento em simulação, colocá-lo no robô, observar onde falha, alterar o ambiente ou os dados de treino, repetir o processo e finalmente publicar a nova “*policy*” para que outros a possam utilizar. O simulador, o software e a *stack* de “*reinforcement learning*” são abertos. O que se partilha deixa, portanto, de ser apenas código:

pode ser uma forma de andar, agarrar um objeto ou reagir a determinada situação física. Passados poucos dias do lançamento, já é possível encontrar online todo um novo conjunto de “*policies*” — até um “*moonwalk*” ao estilo de Michael Jackson. Esta é uma extensão bastante natural das bases que têm vindo a sustentar o crescimento da empresa, de origem francesa, que foi recentemente adquirida pela Nvidia. O *Hub* da Hugging Face permitiu que modelos e “*datasets*” fossem publicados, reutilizados e modificados por terceiros. A nova plataforma pretende levar uma lógica semelhante à robótica: tornar comportamentos físicos partilháveis, juntamente com os ambientes e os métodos usados para os treinar. A diferença é que, agora, o resultado acaba por ter consequências no mundo físico e não apenas no virtual.

Muda, igualmente, quem pode “treinar” a máquina. No LeRobot, a plataforma de robótica da Hugging Face, uma “*policy*” pode ser executada no robô e interrompida quando começa a fazer algo errado. O utilizador assume então o controlo, demonstra a correção e devolve-o à máquina. Essa intervenção fica registada como novos dados e pode entrar diretamente na ronda seguinte de treino. Utilizar o robô passa a ser também uma forma de o treinar.

Isto pode constituir, claramente, a base de um conjunto de novas competências, para utilizadores sem qualquer experiência anterior em robótica. Um operador numa fábrica pode não saber programar um robô, mas sabe como uma peça deve ser apanhada, em que posição deve ser colocada ou que movimento denuncia uma

operação incorreta. Demonstrar e corrigir essas ações passa, assim, a ser uma forma de transferir conhecimento operacional para o robô.

Naturalmente, a dialética “edge”/“cloud” mantém-se. O treino pode ser feito numa máquina local ou em GPU remotas; simulações extensas e modelos maiores continuarão a beneficiar da infraestrutura centralizada. Mas o comportamento aprendido é depois colocado numa máquina que vê, decide e age no local onde o problema existe. Durante anos, o “edge” foi apresentado como um modelo onde a computação acontece perto de onde os dados são gerados. A robótica acrescenta-lhe agora pessoas que treinam comportamentos, comunidades que os partilham e máquinas que os levam consigo. O “edge” não pára: agora, ganhou uma capacidade nova — aprendeu a andar. ■



ZERO TRUST

VALIDAÇÃO, SEGMENTAÇÃO E VISIBILIDADE

Na Oramix ajudamos a transformar os princípios de Zero Trust numa arquitetura orientada à resiliência, não apenas à conformidade.



Avaliar

Identificamos ativos críticos, acessos, privilégios e os principais gaps de segurança.



Definir

Desenhamos a arquitetura e um roadmap faseado, alinhado com o risco e as prioridades do negócio.



Implementar

Garantimos a integração dos controlos definidos, com validação contínua em cada fase.

IA NO TRABALHO JÁ É UTILIZADA POR 84% DOS TRABALHADORES PORTUGUESES

A utilização de IA está a consolidar-se entre os trabalhadores portugueses, mas a integração nas organizações continua mais limitada e levanta desafios na utilização de ferramentas externas.



A utilização de Inteligência Artificial (IA) no contexto profissional chegou aos 84% entre os trabalhadores portugueses, acima dos 65% registados em 2025. Os dados constam da primeira parte do

estudo “*O momento da verdade da IA nas empresas*”, publicado pela Cegid e conduzido pela OpinionWay. O estudo ouviu 2.006 trabalhadores de escritório em Portugal, Espanha, França e Alemanha, entre 22 de maio e 4 de junho de 2026. A amostra portuguesa incluiu 502 profissionais. A IA está também a assumir maior peso na tomada de decisão. Entre os profissionais portugueses, 44% afirmam utilizar estas ferramentas frequentemente ou de forma sistemática para apoiar decisões importantes no trabalho. ■

IT LIDERA PREPARAÇÃO, MAS BURNOUT ATINGE 70%

Os profissionais de tecnologias de informação estão entre os mais preparados para o futuro do trabalho, mas 70% sentem ou sentiram recentemente burnout, revela o ManpowerGroup.



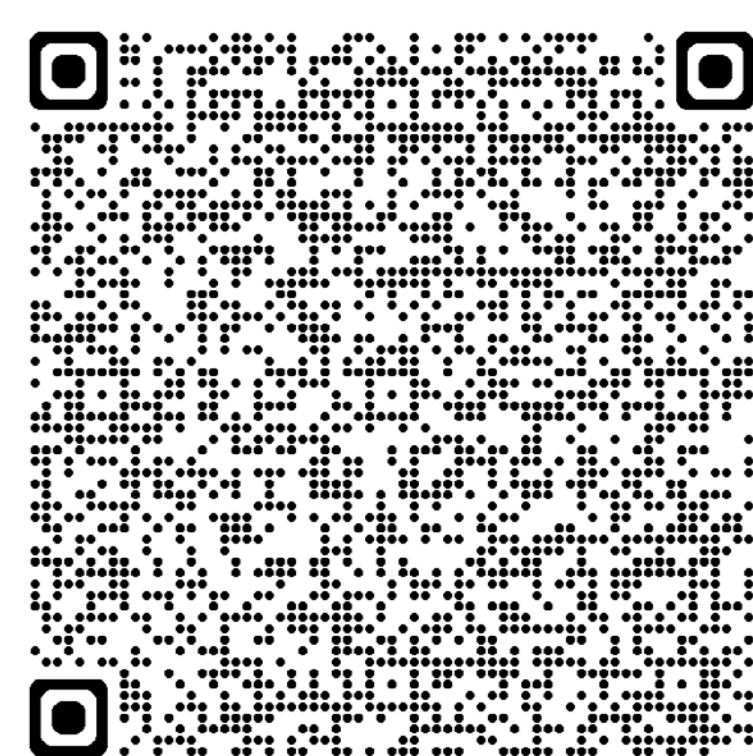
Os profissionais de Tecnologias de Informação destacam-se pela confiança nas suas competências, empregabilidade e preparação para a transformação tecnológica, mas apresentam simultaneamente elevados níveis de stress e *burnout* e uma menor intenção de permanecer

nas atuais empresas. As conclusões são do “*Global Talent Barometer 2026*”, do ManpowerGroup, realizado junto de 13.918 trabalhadores em 19 países. O índice de confiança dos profissionais de IT atinge 84%, mantendo-se estável face a 2025. Cerca de 91% dizem confiar nas competências necessárias para desempenhar a atual função e 85% consideram ter oportunidades para desenvolver novas competências e adquirir experiência para atingir os seus objetivos profissionais, o valor mais elevado entre os setores analisados. ■

Refrigeração líquida preparada para o futuro, **desenvolvida para IA**

Soluções de Refrigeração Líquida

Gestão térmica escalável,
desenhado para data centers de
elevada exigência.



Leia o código para explorar
soluções de refrigeração
líquida

se.com/pt



FALHAS BÁSICAS DE SEGURANÇA AINDA PERSISTEM NAS PME

A Eset alerta que a inteligência artificial está a acelerar a atividade dos cibercriminosos, mas as principais causas dos incidentes nas PME continuam a ser phishing, vulnerabilidades por corrigir e palavras-passe fracas.



A Inteligência Artificial (IA) está a transformar as ferramentas utilizadas pelos cibercriminosos, permitindo criar campanhas de phishing mais convincentes, automatizar tarefas de reconhecimento e reduzir a

barreira de entrada para atacantes menos experientes. No entanto, segundo a Eset, a preparação das PME para enfrentar ciberameaças continua a depender sobretudo da correção de falhas de segurança já conhecidas.

De acordo com o “*Eset SMB Cyber Readiness Index 2026*”, o malware alimentado por IA é apontado como a principal preocupação das PME para os próximos 12 meses. Ainda assim, a fabricante refere que os casos de malware verdadeiramente baseado em IA continuam a ser raros. ■

EMPRESAS AINDA TÊM DIFICULDADE EM ESCALAR IA

Apenas 22% das organizações conseguiram alargar a utilização de inteligência artificial a várias áreas do negócio, apesar de o investimento continuar a aumentar, segundo a Gartner.



A adoção de Inteligência Artificial (IA) continua a aumentar nas empresas, mas poucas organizações conseguiram escalar a tecnologia. Um inquérito da Gartner revela que apenas 22% conseguiram expandir a IA a várias unidades de negócio

ou adotaram uma abordagem *AI-first*.

Apesar das dificuldades, o investimento continua a acelerar, segundo os resultados que se baseiam neste inquérito realizado pela Gartner entre janeiro e abril de 2026 a 1.303 profissionais de organizações que registaram receitas anuais de pelo menos 50 milhões de dólares no exercício de 2025.

Entre os responsáveis funcionais inquiridos, 85% planeiam aumentar os gastos com IA em 2026, depois de terem dedicado, em média, 12% dos respetivos orçamentos à tecnologia em 2025. ■

Exclusive Training Center

Formação especializada em cibersegurança e creditações



Formação certificada
pelos fabricantes



Sessões práticas
e laboratórios



Opções de formação
personalizadas



Descubra o nosso catálogo de formações

IA MUDA O PAPEL DAS EQUIPAS DE IT NAS EMPRESAS

A disseminação da inteligência artificial está a levar as empresas a repensar a liderança tecnológica, com maior foco na autonomia das equipas, governação e avaliação de competências.



A maior facilidade de acesso a ferramentas de Inteligência Artificial (IA) está a permitir que profissionais fora das áreas tecnológicas realizem tarefas anteriormente dependentes de competências especializadas.

Para a Zühlke, esta evolução está a alterar não apenas a forma como a tecnologia é utilizada nas empresas, mas também o papel das equipas de IT e dos responsáveis tecnológicos.

A consultora identifica três tendências associadas a esta transformação, desde a democratização da criação tecnológica, a passagem das equipas de IT de uma função de controlo para uma de capacitação e uma maior valorização da capacidade de utilizar criticamente a IA na avaliação de competências profissionais. ■

TRANSPARÊNCIA E FLEXIBILIDADE GANHAM PESO NA ATRAÇÃO DE TALENTO

A Adecco defende que transparência, flexibilidade e oportunidades de desenvolvimento assumem um peso crescente na decisão dos candidatos ao escolher um novo empregador.



O salário continua a ser um fator importante na atração de talento, mas deixou de ser suficiente para convencer os candidatos. A conclusão é da Adecco, que aponta a transparência, a flexibilidade, as oportunidades de desenvolvimento e a confiança na organização como critérios cada vez

mais determinantes na escolha de um novo projeto profissional.

Segundo a empresa, a crescente escassez de competências e um mercado de trabalho marcado por profissionais mais informados estão a obrigar as organizações a rever as suas estratégias de atração.

A Adecco considera que a decisão de aceitar uma oferta de emprego deixou de assentar apenas na componente financeira, passando a refletir também a confiança que os candidatos depositam na organização e na sua capacidade para investir no desenvolvimento das pessoas. ■



Business Continuity & Resilience

IT Insight
talks

Da continuidade à resiliência: preparar o negócio para a disrupção

15 de outubro | Lispólis, Auditório Veiga Simão | 10h00

A continuidade do negócio exige hoje mais do que planos de recuperação. Num contexto de maior dependência tecnológica, ciberameaças, serviços críticos e cadeias de fornecimento cada vez mais interligadas, a resiliência passa pela capacidade de antecipar riscos, responder a incidentes e recuperar com rapidez.

Nesta IT Insight Talk, especialistas e decisores vão discutir estratégias, tecnologias e boas práticas para reforçar essa capacidade, incluindo o enquadramento criado pela NIS2 e pelo Cyber Resilience Act.

Lispólis, Auditório Veiga Simão | A partir das 9h30 | Participação presencial ou online.

Escolha a sua forma de participar:

QUERO ESTAR PRESENTE

QUERO ASSISTIR POR ZOOM

Patrocinado por:



IP Telecom

NetApp

RICOH
imagine. change.

VisionWare
since 2006

zscalerTM

Com o apoio de:

LISPOLIS
POLO TECNOLÓGICO DE LISBOA



A GOVERNANCE COMO PONTO DE PARTIDA PARA ESCALAR A IA NAS ORGANIZAÇÕES

Depois de uma fase marcada pela experimentação, as organizações começam agora a olhar para a inteligência artificial com outro nível de exigência. Escalar a tecnologia implica definir modelos de governance, assegurar a qualidade dos dados, gerir riscos e demonstrar impacto real no negócio.

A GOVERNANCE DA INTELIGÊNCIA ARTIFICIAL (IA) esteve em debate no Business Breakfast promovido pela IT Insight, em parceria com a Avanade, no Pestana Palace Hotel, em Lisboa. Sob o tema “AI Governance: Como transformar IA em valor”, a sessão reuniu decisores e especialistas para discutir como as organizações estão a estruturar a adoção da IA.

Na abertura da sessão, Hugo Gonçalves, da Avanade, enquadrou o debate a partir da necessidade de cruzar diferentes visões dentro das organizações, desde o negócio à segurança. O responsável sublinhou a importância de existir uma base comum para que as organizações consigam testar e escalar soluções de IA de forma estruturada. “O desafio é explorar





- Hugo Gonçalves -
Avanade



- Fábio de Pasquale -
Avanade



- Sandro Zeineddin -
Portway

aquilo que pode ser a *framework* principal e a *baseline* dentro de uma organização, com políticas de governance que permitam que todas as pessoas, independentemente do departamento ou do objetivo específico, tenham regras claras para escolher, aplicar, testar e, depois, escalar soluções dentro da própria organização”, afirmou.

Na apresentação inicial, Fábio de Pasquale, da Avanade, defendeu que o mercado está a passar

de uma fase de experimentação para uma fase de escala. Depois do *boom* da IA generativa, iniciado com o lançamento do Chat GPT, as empresas começam agora a procurar modelos de governance capazes de suportar a transformação. “Agora, para 2026, entramos numa fase em que as empresas estão a escalar a IA. E, para escalar a IA, aquilo de que precisam é de governance”, explicou, acrescentando que esta governance deve

incluir segurança, dados, informação e a forma como se conduz um processo de transformação baseado em IA.

Sandro Zeineddin, CTO, Portway: “Com perto de quatro mil colaboradores distribuídos por vários aeroportos e diferentes operações aeroportuárias, um dos nossos maiores desafios era garantir que a informação operacional chegava à gestão



- Henrique Carreiro -
Diretor da IT Insight

de forma estruturada, sem se perder ao longo das diferentes hierarquias. Com a implementação de uma plataforma de comunicação por voz suportada por AI, substituímos o sistema tradicional de rádio e passámos a gerar automaticamente resumos e os principais destaques de cada turno, dando à gestão operacional e à administração uma visão clara do que aconteceu ao longo do dia. Estamos agora a evoluir esta solução, inte-



- Marta Cabrita -
Vieira de Almeida

grando-a com outras aplicações e desenvolvendo novas capacidades de interação com os colaboradores, para que a AI funcione cada vez mais como um suporte operacional.”

Marta Cabrita, Head of Digital Acceleration, Vieira de Almeida: “Numa transação de M&A, que é tipicamente de grande complexidade e dimensão, conseguimos identificar onde é possível



introduzir IA. Isso obriga-nos a repensar a forma como determinados componentes do serviço são valorizados: a transação em si continuará a ser central, mas há tarefas cujo valor terá de ser justificado de outra forma. Por isso, temos de começar a pensar que novos produtos podemos desenvolver, onde existe espaço no mercado e em que nichos podemos atuar, a pensar no futuro e na sustentabilidade das sociedades de advogados.”



- Miguel Gonçalves -
Vinci Energies Portugal



- Rita Lopes -
Airbus

Miguel Gonçalves, Information Security Officer, Vinci Energies Portugal: “Criámos aquilo a que chamamos o AI Passport, ou seja, todos têm de passar por essa formação. Acima de tudo, criámos uma governance. Criámos um modelo de governo, uma estrutura, funções e responsabilidades, bem como peças que suportam esse modelo de governo e os respetivos *workflows*. Criámos, portanto,

uma estrutura, uma *framework* que, independentemente de hoje ser a solução A, B ou C, de ser o LLM A, B ou C, de ser uma solução interna ou vendável, encaixa dentro da nossa máquina.”

Rita Lopes, Security Officer for Sustainability and Communication, Airbus: “O futuro é IA, desde que encarada como uma ferramenta de

apoio ao ser humano. Isto exige uma ponderação, não apenas a nível de segurança, mas também na vertente analítica, para compreender como o sistema evolui. Além disso, talvez tenhamos, também, de equacionar a área da sustentabilidade na utilização da IA. Criar agentes e ter bons agentes implica, inicialmente, um investimento substancial de recursos para delinear a melhor estratégia



- Inês Condeço -
Fnac



- Nuno Silva -
Universidade Lusíada



de LLMs. A questão fundamental é avaliar se, a médio e longo prazo, esse esforço adicional trará o retorno esperado.”

Inês Condeço, Marketing and Communication Director, Fnac: “A Inteligência Artificial não substitui uma estratégia de cliente, mas pode amplifi-cá-la de uma forma sem precedentes. O verdadeiro desafio não está na tecnologia, está nos dados. Quando os dados estão dispersos por múltiplos

sistemas, a IA limita-se a replicar essa fragmen-tação. No retalho, o valor surge quando conse-guimos ligar todas as peças: compras, interações, preferências e contexto. Só assim é possível criar experiências verdadeiramente personalizadas, relevantes e úteis para cada cliente.”

Nuno Silva, CTO, Universidade Lusíada: “Na educação, a adoção está um pouco mais atra-sada, pelo menos relativamente às empresas.

As ferramentas deviam estar disponíveis para todos, e não apenas para as instituições muito grandes, deixando as mais pequenas para trás. Ainda assim, não causou grande preocupação. A primeira coisa que faço nas aulas é incentivar os alunos a abrirem a mente para a Inteligência Artificial. Em vez de lhes dizer para não usarem, digo o contrário: usem, experimentem. Por isso, foi finalizado um novo regulamento de avaliação. Vai ser um desafio.” ■

IT-SECURITY CONFERENCE

LISBOA

2026
OCT 08

conf.itsecurity.pt

#A VOZ DOS CISO

08 OUT 2026 | LISBOA

PARCEIROS

Diamond Partner



Platinum Partners



Golden Partners



Silver Partners



Silver Exhibition Partners



Bronze Partners



VAD Partners



Institutional Partners





RED HAT: "A MAIORIA DAS ORGANIZAÇÕES AINDA ESTÁ A ACUMULAR DÍVIDA TÉCNICA"



- Edgar Ivo -
Red Hat Portugal

A dívida técnica continua a crescer em muitas organizações portuguesas, pressionada agora pela adoção de Inteligência Artificial e pela crescente complexidade dos ambientes Hybrid Cloud. Para a Red Hat, o desafio passa por reduzir dependências e criar maior portabilidade entre plataformas.

À MEDIDA QUE AS ORGANIZAÇÕES procuram conciliar ambientes hybrid cloud, modernização aplicacional, virtualização e Inteligência Artificial, aumenta também a complexidade das infraestruturas de IT. A soberania digital, o controlo de custos e a dependência tecnológica ganharam, por isso, um peso nas decisões dos responsáveis.

Neste contexto, Edgar Ivo, Sales Leader da Red Hat em Portugal, considera que o mercado português evolui a duas velocidades: enquanto uma parte das organizações continua a acumular complexidade, outra começou já a normalizar tecnologias, plataformas e processos.

“Diria que a maioria ainda está a acumular dívida técnica e o mundo do IA só veio trazer ainda mais complexidade e uma maior velocidade a essa acumulação”, justifica.

O setor financeiro está, na sua perspetiva, um passo à frente neste percurso, fruto de uma modernização iniciada mais cedo e de uma pressão regulatória que obrigou as organizações a olharem de forma mais estruturada e sistematizada para a multiplicidade de tecnologias, plataformas e clouds. A banca começou, assim, a procura por uma maior normalização e portabilidade entre ambientes.

Edgar Ivo reconhece igualmente a evolução do setor público, que tem aproveitado as verbas associadas ao Plano de Recuperação e Resiliência (PRR) para fazer face a uma dívida técnica acumulada ao longo de vários anos.

VIRTUALIZAÇÃO ACELERA PROCURA POR ALTERNATIVAS

A necessidade de reduzir dependências tornou-se particularmente evidente no mercado de virtualização. Para Edgar Ivo, as alterações verificadas no mercado, nomeadamente em torno da VMware, expuseram as dificuldades



das organizações quando precisam de reagir rapidamente a uma mudança profunda num fornecedor.

“Se virmos o tema da virtualização, a incapacidade que as organizações tiveram de reagir a uma mudança abrupta no mercado trouxe-nos um impacto financeiro extremamente importante”, reforça.

Esta mudança resultou, segundo o responsável, em três momentos: um impacto inicial com uma reação negativa; uma expectativa de negociação

com o fornecedor, onde as organizações procuraram encontrar condições comercialmente aceitáveis; e, agora, por último, uma procura efetiva de alternativas.

“Neste momento, estamos ativamente a trabalhar com os clientes para encontrar essas alternativas. O custo e esta desconfiança de médio prazo são o grande acelerador das decisões. Depois, o risco operacional e a necessidade de ter que criar competências, obviamente, são aquilo que está a impedir que se acelere de forma mais rápida”, considera.

A quebra de confiança abriu espaço para a necessidade de encontrar uma tecnologia alternativa, adaptada aos processos operacionais existentes, assim como as competências para executar esta transição.

Um dos principais desafios para os próximos meses será, por isso, garantir a capacidade de executar, em tempo útil, projetos de migração e dar resposta a todos os pedidos de clientes, garantindo que

existe disponibilidade, capacidade e competências técnicas.

INTELIGÊNCIA ARTIFICIAL: DA EXPERIMENTAÇÃO À PRODUÇÃO

A dificuldade em passar da experimentação para ambientes de produção é igualmente visível na Inteligência Artificial. Edgar Ivo relativiza a ideia de que uma elevada percentagem dos projetos de IA generativa “falha”. Na sua leitura, muitas organizações conseguiram compreender que é simples obter resultados convincentes quando trabalham com um conjunto limitado de dados. No entanto, alerta para o problema que surge quando o piloto precisa de ser integrado nos sistemas, processos, dados e mecanismos de segurança da organização.

A complexidade aumenta especialmente quando as organizações deixam de trabalhar apenas com assistentes e avançam para agentes capazes de interagir com processos e tomar decisões.

Para Edgar Ivo, experimentar rapidamente continua a ser importante, mas a preparação da segunda fase deve começar em simultâneo porque, sem uma base sólida, a passagem à produção pode revelar-se mais demorada.

A IMPORTÂNCIA DOS DADOS PRÓPRIOS PARA A IA

A integração tecnológica traz consigo a questão económica, uma vez que, apesar de alguns pilotos realizados em cloud funcionarem tecnicamente bem, não conseguem escalar devido ao custo. A disponibilidade e o preço de recursos computacionais são, por isso, igualmente condicionantes. É também neste ponto que os dados internos ganham relevância. Os modelos generalistas têm capacidade de responder a questões de conhecimento geral, mas não conhecem os processos, a informação e o contexto específico das organizações. A abordagem defendida pela Red Hat passa, por isso, pela utilização de modelos mais específicos e

especializados, combinados com a informação própria de cada organização, em vez de recorrer sempre a modelos de grande dimensão.

“Aquilo que nós defendemos é definição de modelos muito mais específicos, definição de modelos muito mais especializados, agregados com a informação da organização, para que possamos, de forma eficiente, endereçar aquele objetivo de negócio.”

A questão deixa de ser apenas o que a tecnologia consegue fazer e passa também por perceber se o resultado pode ser obtido de forma financeiramente sustentável e com níveis de segurança e controlo adequados.

“Não nos basta ter respostas muito boas 90% do tempo. Temos que garantir que não há respostas erradas, não há respostas que nos criem um problema legal, que não nos criem um problema de segurança”, reitera o responsável.

A INFLUÊNCIA DA SOBERANIA DIGITAL

O controlo sobre a tecnologia e a informação tem em conta uma outra camada: a preocupação crescente em torno da soberania digital. Para Edgar Ivo, a soberania digital deixou de significar apenas saber onde estão alojados os dados. Banca, setor público, saúde e defesa são os setores portugueses onde a questão da soberania digital está mais presente.



“A soberania é garantir que tenho controlo sobre os dados, tenho controlo operacional sobre os dados, quem é que está a executar, as dependências que tenho de fornecedores, quer tecnológicos, quer de serviços”, afirma Edgar Ivo.

O caso da virtualização volta a ser de exemplo prático sobre o risco de dependência excessiva de um fornecedor: “Quando temos uma dependência de um



forneceador que, de repente, toma uma decisão que tem um impacto sério, tenho de conseguir reagir de forma ágil e a um custo que seja aceitável”.

A soberania digital surge, inclusivamente, como preocupação nos processos formais de contratação dos concursos públicos, onde o tema entra diretamente nos pedidos de proposta e concursos públicos, deixando de ser apenas um tema estratégico ou regulatório.

SETOR PÚBLICO CRUZA VIRTUALIZAÇÃO E MODERNIZAÇÃO

Atualmente, o setor público é uma das apostas fortes da Red Hat, que procura ajudar as organizações que se encontram a rever a infraestrutura de virtualização. O objetivo vai além da substituição da tecnologia e implica, sobretudo, preparar a modernização das aplicações.

Várias entidades têm combinado a saída de VMware com processos de modernização aplicacional, enquanto outras optaram por começar por modernizar antes de avançarem com a migração da virtualização.

A resposta da Red Hat a esta crescente diversidade passa por aproximar três áreas numa só plataforma: modernização aplicacional, virtualização e IA.

Para Edgar Ivo, esta convergência pode permitir às organizações reduzir a dívida técnica e uniformizar processos, independentemente das plataformas onde as cargas são executadas.

A própria Inteligência Artificial poderá assumir um papel na redução da distância entre as competências tradicionais das equipas de IT e as plataformas mais recentes. Contudo, a inferência é tida como uma das questões mais relevantes na próxima fase da adoção empresarial de IA.

No fundo, a estratégia pretende reduzir a complexidade e a dependência, sem nunca perder a capacidade sobre o local e a forma como cada carga é executada. ■



ΔI DIGEST, UM RESUMO DO QUE ESTÁ
Δ ΔCONTECER NAS FRONTEIRAS
DA INTELIGÊNCIA ΔRTIFICIAL

Coligido por Henrique Carreiro
Ilustrações de Teresa Rodrigues com o DALL-E

O software começa a trocar de estrutura

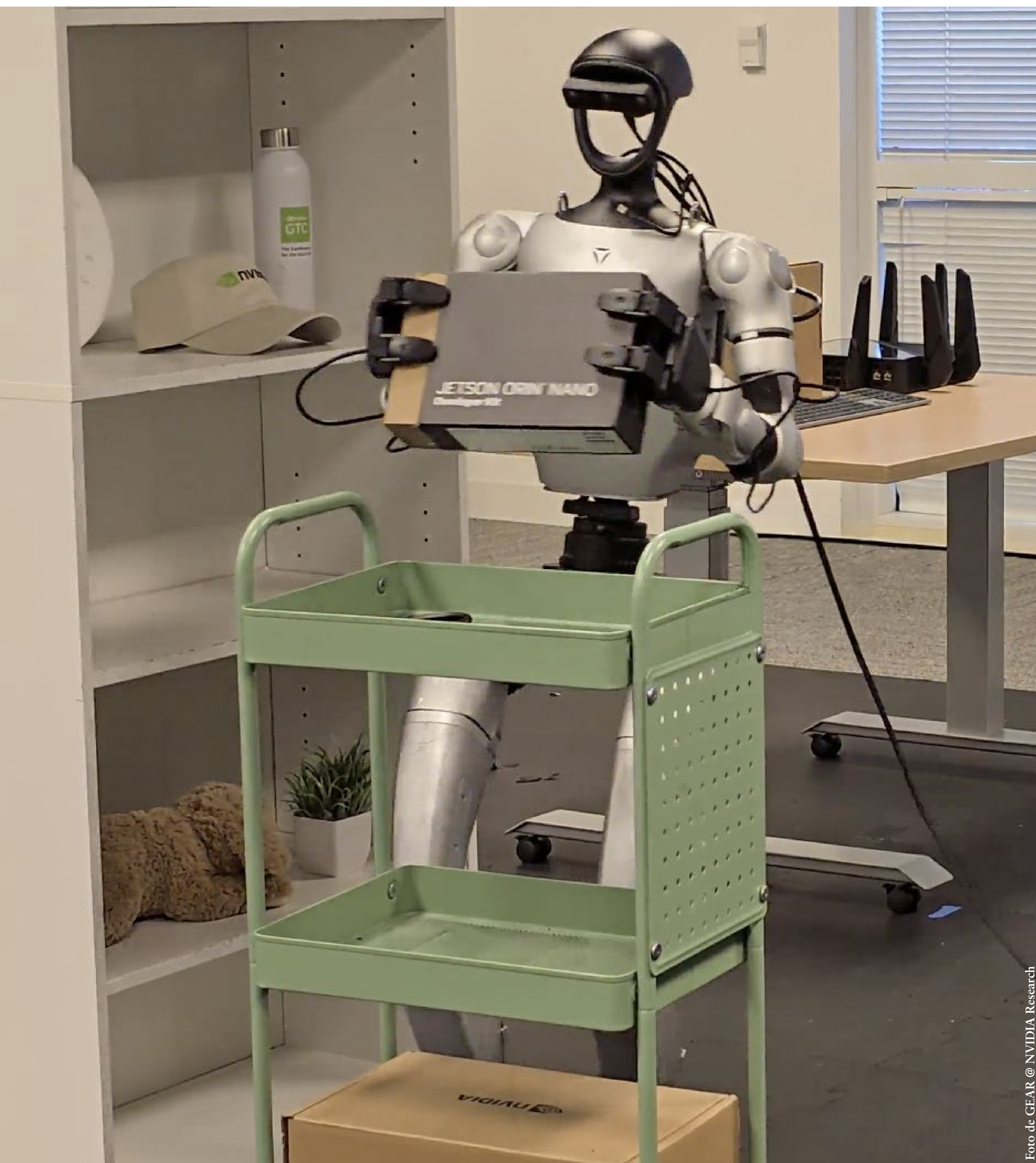


Foto de GEAR @ NVIDIA Research

NA ROBÓTICA, o software continua, em larga medida, preso à estrutura para que foi treinado: mudar o número de braços, articulações, câmaras ou mãos é suficiente para tornar difícil a transferência do comportamento aprendido. Mas os modelos mais recentes começam a reduzir tal dependência.

A Google DeepMind apresentou há pouco tempo o Gemini Robotics 2, um modelo que combina visão e linguagem para decidir que movimentos deve um *robot* executar. O mesmo modelo treinado conseguiu controlar configurações muito diferentes: o Apollo 2, um humanoide construído pela Apptronik, equipado com dois tipos de mãos, assim como uma plataforma formada por dois braços robóticos Franka. Uma versão concebida para correr directamente no *robot* pode, ainda, ser adaptada a máquinas com outras formas, sensores e articulações usando apenas algumas horas de recolha de dados adicionais.

A Nvidia está a seguir uma direção semelhante com o GR00T N1.6, um modelo para controlo de *robots* treinado com dados provenientes de humanoides, braços robóticos e outras configurações físicas, procurando que parte do comportamento aprendido sobreviva à mudança de máquina. As diferenças mecânicas, evidentemente, não desapareceram — um braço industrial continua sem pernas e um humanoide continua a ter o inconveniente de as possuir —, mas começam a deixar de determinar todo o software que existe acima delas. A mecânica continua a impor os limites, naturalmente. O que começa, entretanto, a desaparecer é a obrigação de ensinar tudo de novo ao software, de cada vez que muda o corpo onde aquele corre. ■

O cientista que treinou sem ocupar o laboratório

NUM SINCROTRÃO, o tempo de máquina é um recurso demasiado caro para ser usado a ensinar um agente por tentativa e erro. Estas instalações aceleram partículas para produzir feixes extremamente intensos destinados ao estudo da estrutura de materiais, e o acesso é limitado e disputado entre equipas de investigação.

Uma equipa do SLAC National Accelerator Laboratory, um centro de investigação norte-americano associado à Universidade de Stanford, construiu, por isso, uma cópia virtual de uma das suas estações experimentais. Neste simulador, um agente baseado num grande modelo de linguagem — capaz de observar o estado do equipamento, decidir a ação seguinte e emitir comandos para os instrumentos — aprendeu a orientar amostras de materiais perante um feixe de raios X. O agente interpretou as imagens produzidas pelo detetor, ajustou os motores que posicionavam a amostra e repetiu o processo até encontrar a orientação procurada.

Os investigadores transferiram depois o mesmo procedimento para o equipamento físico. O agente conseguiu orientar as amostras e reagiu ainda a problemas que não tinham sido incluídos no simulador, entre eles um erro de 1,5 graus na posição indicada por um dos motores. Por segurança, continuava a existir um investigador no circuito: recebia os comandos propostos pela IA e introduzia-os no sistema de controlo sem os alterar. É uma interface



humana bastante sofisticada para uma função próxima do copiar-e-colar, mas provavelmente razoável quando atrás do teclado existe um acelerador de partículas.

Neste caso, a réplica digital resolve uma limitação bastante material: permite treinar o operador sem ocupar, durante a aprendizagem, o equipamento científico que ele terá depois de operar. Imaginem-se as possibilidades quando tal tipo de simulação for generalizável. ■

IA entra na sala de operações



EM LONDRES, no National Hospital for Neurology and Neurosurgery, um neurocirurgião removeu um tumor da hipófise enquanto um sistema de inteligência artificial analisava, em tempo real, as imagens da câmara endoscópica. Desenvolvido pela University College London, o sistema identificava estruturas críticas na base do

cérebro e assinalava zonas de risco durante a intervenção. O doente, cuja visão estava seriamente comprometida, recuperou-a depois da operação. A expressão “*surgical ChatGPT*” apareceu entretanto na imprensa para caracterizar esta intervenção, como seria difícil evitar.

A comparação é boa para títulos de notícias, mas bastante menos útil para perceber o que aconteceu. O sistema vai reconhecendo a anatomia, os instrumentos e as interações com os tecidos enquanto a cirurgia decorre. Foi treinado e avaliado com centenas de vídeos de operações anteriores e corre numa plataforma Nvidia Clara IGX, destinada à execução de modelos de IA em dispositivos médicos. Enquanto a cirurgia decorre, o sistema acompanha o campo operatório fotograma a fotograma e assinala estruturas que importa não perder de vista.

Parte do trabalho da equipa consistiu precisamente em decidir o que mostrar ao cirurgião e

como indicar quando o modelo estava menos seguro. É um detalhe menos fotogénico do que a ideia de um ChatGPT a ajudar numa operação ao cérebro, mas provavelmente mais importante: não basta que o sistema reconheça corretamente uma estrutura se a forma como apresenta essa informação interferir com quem está a operar. A própria interface entra assim no problema da segurança clínica.

Este foi o primeiro doente de um ensaio ainda em curso. A recuperação da visão mostra que a operação correu bem; não demonstra que a IA a tornou mais segura ou mais eficaz. Isso exigirá outro tipo de medições. Para já, basta o que efetivamente aconteceu: foi usada visão computacional suficientemente rápida e precisa para acompanhar uma neurocirurgia em curso e apresentar informação utilizável ao especialista que continuava em controlo, a tomar as decisões. Só isto vale bem mais do que quaisquer títulos futuristas. ■



A CLOUD DEIXOU DE SER O ÚNICO DESTINO



DAS NEOCLOUDS AO “EDGE MÓVEL”

HENRIQUE CARREIRO

A CLOUD “TRADICIONAL” (se é que existe algo de tradicional na cloud) continua a crescer, mas o termo, encarado nas premissas habituais, já não é suficiente para descrever a infraestrutura que está a ser construída em torno dos *workloads* de Inteligência Artificial (IA). Atualmente, uma parte dessa infraestrutura, mais centralizada, concentra-se em instalações desenhadas para juntar dezenas ou centenas de milhares de aceleradores; paralelamente, no chamado “edge”, existe cada vez mais infraestrutura descentralizada em equipamentos industriais, automóveis e *robots*, onde os modelos trabalham junto dos dados e, em alguns casos, tomam decisões que não podem esperar por uma viagem a um data center remoto — ou trabalham em conjunto com a infraestrutura centralizada.

É neste contexto de mudança que têm vindo a surgir as chamadas “neoclouds”. Empresas como CoreWeave, Nebius, Lambda ou Crusoe não foram construídas para reproduzir de forma exata as centenas de serviços da Amazon Web Services, Microsoft Azure ou Google Cloud. **O negócio nasceu muito mais concentrado: fornecer grandes quantidades de GPU, redes de alto débito**

e armazenamento suficientemente rápido para as alimentar, sobretudo a empresas que treinam ou executam modelos de inteligência artificial. A IA é, neste momento, o motor de crescimento das neoclouds, com tudo o que isto tem de bom e, paralelamente, com o que tem de preocupante.

A CoreWeave dá uma medida da escala que este mercado atingiu. No final do segundo trimestre deste ano operava 51 datacenters, com 1,5 GW de potência ativa, e tinha já cerca de 3,7 GW contratados. Estas instalações são construídas em torno de clusters extremamente densos de GPU, refrigeração líquida, redes especializadas e software cuja função é manter hardware muito caro ocupado durante o maior tempo possível. A própria rede começa a ter outro comportamento: **há transferências sustentadas entre armazenamento e *clusters* de computação que podem chegar a centenas de gigabits por segundo e, em alguns casos, à escala do terabit.**

No edge, parte da inferência começa a deslocar-se precisamente para junto dos dados. Numa fábrica, uma câmara pode ter de identificar imediatamente uma peça; um veículo autónomo dentro de um armazém tem de decidir



“A IA É, NESTE MOMENTO, O MOTOR DE CRESCIMENTO DAS NEOCLOUDS, COM TUDO O QUE ISTO TEM DE BOM E, PARALELAMENTE, COM O QUE TEM DE PREOCUPANTE”

se deve parar; um *robot* que está a agarrar um objeto precisa de corrigir o movimento enquanto o executa. Estas são tarefas em que quer a latência, quer a necessidade de autonomia e, até mesmo, o volume de dados e o custo de os transportar continuamente tornam pouco razoável depender permanentemente de um data center remoto.

A robótica torna particularmente visível esta separação entre o lugar onde um modelo é treinado e aquele onde é usado. A China tinha já, no final de 2024, mais de dois milhões de *robots* industriais em funcionamento e recebeu nesse ano 295 mil novas instalações, 54% do total mundial. Pela primeira vez, os fabricantes chineses venderam

mais *robots* no seu próprio mercado do que os fornecedores estrangeiros. Os humanoides ganharam entretanto enorme visibilidade — AgiBot, Unitree ou UBTech —, mas são apenas uma parte de um território muito maior, onde continuam a dominar braços industriais, plataformas móveis e máquinas desenhadas para funções específicas. A robótica atual, cada vez mais com mobilidade alargada, redefine o que era até agora a prevalência sobretudo estática do edge.

A expansão destes sistemas esbarra, contudo, numa escassez muito concreta: dados físicos. Os grandes modelos de linguagem foram treinados com quantidades imensas de texto, código, imagens

e vídeo já existentes. Um robot precisa também de aprender o que acontece quando um objeto escorrega, quando uma peça está ligeiramente fora do lugar, quando a superfície oferece mais resistência do que o previsto ou quando uma tentativa falha a meio. A simulação resolve parte do problema, mas não substitui toda a experiência do mundo real. Na Europa — que noutros aspetos parece tão afastada desta conversa — já está a aparecer infraestrutura dedicada precisamente a produzir essa experiência. A NEURA Robotics e a Universidade Técnica de Munique estão a criar junto ao aeroporto de Munique um RoboGym com 2.300 metros quadrados e um investimento inicial de



“UMA ORGANIZAÇÃO PRECISA DE SABER QUE VERSÃO DE UM MODELO ESTÁ EM PRODUÇÃO, ONDE CORRE, QUANDO FOI ATUALIZADA E QUE TELEMETRIA ESTÁ A DEVOLVER”

cerca de 17 milhões de euros. Uma frota de *robots* deverá executar tarefas em condições reais e produzir dados de treino que serão depois disponibilizados através do Neuraverse. A NEURA afirma estar a desenvolver dez centros deste tipo, cinco dos quais deverão estar operacionais até ao final do ano.

Instalações como estas transformam a experiência física em dados. Parte dessa informação será armazenada, outra combinada com simulação e enviada para *clusters* de GPU onde os modelos são treinados; quando uma nova versão fica pronta, regressa às máquinas que trabalham na fábrica, no armazém ou noutro ambiente real. Essa circulação exige, contudo, mais do que uma ligação

entre o data center e a máquina. Uma organização precisa de saber que versão de um modelo está em produção, onde corre, quando foi atualizada e que telemetria está a devolver. Em fábricas e armazéns, servidores locais e *gateways* podem assumir parte desse trabalho, distribuindo novas versões e recolhendo informação sem transformar cada robot ou câmara num sistema isolado.

Modelos e novas versões “descem” para as máquinas; vídeo, telemetria, trajetórias, demonstrações humanas, erros e correções regressam aos sistemas de armazenamento e treino. Quanto mais inteligência existir no terreno, maior pode ser também a procura de computação centralizada, porque cada máquina deixa de ser apenas um

ponto de execução e passa igualmente a produzir matéria-prima para a geração seguinte.

A nível empresarial, isto complica uma decisão que durante anos pareceu relativamente simples. Um mesmo sistema pode recolher dados num *robot*, guardá-los numa cloud empresarial, recorrer a uma neocloud para treino e executar localmente a decisão final. O custo, a latência ou a sensibilidade dos dados podem empurrar partes diferentes do mesmo *workload* para lugares diferentes; depois, alguém terá de manter coerentes as versões, as permissões e as atualizações ao longo dessa cadeia. Em boa verdade, já não basta decidir onde corre a aplicação: é preciso decidir onde corre cada parte do seu ciclo de vida. ■



A CLOUD DEIXOU DE SER O ÚNICO DESTINO

A cloud, o edge e a infraestrutura on-premises coexistem numa arquitetura cada vez mais distribuída. Fatores como a latência, os dados, a segurança e a IA contribuem cada vez mais para mudar a decisão sobre onde executar cada workload

MARTA QUARESMA FERREIRA

DEPOIS DE ANOS de concentração de *workloads* em cloud, as organizações estão hoje conscientes de que nem todos os dados, aplicações e processos devem ser executados no mesmo local.

Estará o conceito de *cloud-first* a evoluir para uma ideia de *workload-first*, onde a latência, o custo, a segurança, a soberania dos dados e o consumo energético assumem um papel central quando pensamos em arquiteturas distribuídas?

De forma a aproximar a computação do local onde os dados são produzidos, **o edge computing está a posicionar-se como uma arquitetura de eleição, especialmente em ambientes altamente distribuídos, como é o caso**

de ambientes industriais, telecomunicações, retalho ou saúde, onde determinados processos não podem ficar dependentes da disponibilidade da ligação ou sujeitos à latência associada ao processamento remoto.

“É uma mudança de paradigma, mas não do tipo que substitui a cloud”, começa por referir Hugo Rego, Senior Manager, Global Edge Solution Architects da Red Hat. Em setores como indústria, energia, *utilities* e logística, onde grande parte dos dados é gerada no edge, transportar toda essa informação para a cloud, garante Hugo Rego, “nunca foi sustentável”.

Mais do que deslocar para o edge *workloads* que anteriormente estavam na cloud, Hugo Rego distingue a existência de *workloads* nativos de edge,



- Hugo Rego -
Red Hat

que, pelas suas próprias características, precisam de operar junto da origem dos dados, ainda que necessitem de um modelo operacional semelhante ao da cloud. É o caso, exemplifica, de sistemas executados em subestações, PLC industriais, lojas ou mesmo ambientes de defesa sem conectividade. De acordo com o que observam no terreno, as organizações que começaram outrora com *cloud-first* “estão agora a perceber que precisam de uma estratégia de ‘operar em qualquer lugar’”. **A real mudança está, por isso, a acontecer numa**

vertente de “cloud como destino” para “cloud como modelo operacional, implementado em qualquer lugar”.

O WORKLOAD DITA A ARQUITETURA

Pedro Teixeira, Hybrid Solutions Manager da HPE Portugal, considera que depois de ter respondido “eficazmente às necessidades de transformação digital da última década”, o conceito de *cloud-first* precisa agora de “ser complementado por uma visão mais flexível”.

Na visão da empresa, a questão deixou de ser onde executar uma aplicação para passar a ser qual o ambiente que melhor se adequa a cada *workload*. “As organizações estão a evoluir de estratégias *cloud-first* para abordagens *cloud-smart* ou *hybrid-by-design*, onde cada aplicação é posicionada de acordo com critérios de negócio, desempenho, conformidade e eficiência operacional”, contextualiza Pedro Teixeira.

“SE TRATAMOS CADA LOCALIZAÇÃO EDGE COMO UM CASO ÚNICO, A COMPLEXIDADE ESCALA”



“

AS ORGANIZAÇÕES ESTÃO A EVOLUIR DE ESTRATÉGIAS CLOUD-FIRST PARA ABORDAGENS CLOUD-SMART OU HYBRID-BY-DESIGN, ONDE CADA APLICAÇÃO É POSICIONADA DE ACORDO COM CRITÉRIOS DE NEGÓCIO, DESEMPENHO, CONFORMIDADE E EFICIÊNCIA OPERACIONAL”



- Pedro Teixeira -
HPE Portugal

Com a centralização tradicional a dar lugar a ambientes distribuídos, Ricardo Silva, CTO & Leader, Sales and Solutions Engineering da Cisco Portugal, defende que as estratégias “devem ser mais abrangentes, integrando cloud, edge e ambientes híbridos”.

Victor Gago, Data Center & C&SP Sales Manager da Schneider Electric, afasta a ideia de

que esta evolução retire relevância aos grandes data centers. Mais do que uma descentralização da capacidade de computação, acredita que estamos perante uma “distribuição mais inteligente das cargas de trabalho”, em que data centers, cloud e edge desempenham funções complementares em função dos requisitos de cada aplicação.

A mesma ideia é defendida no estudo “*State of the Edge 2026*”, lançado pela The Linux Foundation Projects. Numa análise ao futuro do edge, Victor Lu, Independent Consultant e Former Senior Solution Specialist da Oracle, destaca a introdução do conceito *compute continuum* que pretende pensar nos dispositivos, no edge, na infraestrutura central e na cloud como “pontos da mesma arquitetura”, e não ambientes separados. A ideia não é criar uma dicotomia entre cloud e edge, mas centrar a questão sobre qual o melhor local para executar cada *workload*.



O EDGE PARA LÁ DA INTELIGÊNCIA ARTIFICIAL

A opinião dos responsáveis é unânime no que diz respeito à evolução da arquitetura empresarial: nos últimos cinco anos, **as arquiteturas progrediram de modelos centralizados para infraestruturas híbridas e distribuídas, onde o edge passou a fazer parte do argumento.**

De acordo com a Gartner, 40% das grandes organizações terão adotado edge computing nas infraestruturas IT até ao final de 2027. Dados da IDC mostram inclusivamente que a despesa mundial em edge computing poderá alcançar os 380 mil milhões de dólares em 2028.

Por detrás desta evolução estão fatores como a automatização de processos, a expansão do IoT e, mais recentemente, a crescente adoção da Inteligência Artificial (IA) que vai contribuir para alavancar o edge para uma plataforma capaz de suportar sistemas mais autónomos.



- Ricardo Silva -
Cisco Portugal

Esta evolução não significa, contudo, que o valor do edge dependa da atual vaga de IA. Victor Lu recorda que o edge computing respondia já a “problemas concretos”. Se numa primeira fase permitia recolher e processar informação localmente, **o recurso à IA acrescenta agora uma nova camada de capacidades, como a interpretação de informação que permite tomar decisões em tempo real.**

“ [ZERO TRUST] EXIGE POLÍTICAS DINÂMICAS E CONTEXTUAIS, QUE SE ADAPTAM AO RISCO E AO COMPORTAMENTO, SUPORTADAS POR AUTOMAÇÃO E VISIBILIDADE UNIFICADA ”



BEYOND CLOUD OR EDGE: A SEGURANÇA SEMPRE PRESENTE

Escritório, casa, cloud. Quando o tema é Zero Trust, a localização dos vários ambientes distribuídos torna-se num detalhe, uma vez que **a política de segurança “tem de acompanhar a identidade, o dispositivo, a aplicação e os dados”**, reforça Rui Duro.

O Country Manager para Portugal da Check Point Software detalha que o primeiro passo pressupõe a identificação de utilizadores, dispositivos, aplicações e *workloads*. “A organização deve depois aplicar acessos mínimos e específicos por aplicação, em vez de conceder acesso generalizado à rede. Cada pedido deve ser avaliado com base na identidade, no estado de segurança do dispositivo, no contexto da sessão, no risco e na sensibilidade do recurso”.

Para isso, Rui Duro destaca também a aposta numa arquitetura SASE porque “aproxima os controlos de segurança de utilizadores e aplicações”, permitindo a aplicação de regras por apli-

“

A ORGANIZAÇÃO DEVE APLICAR ACESSOS MÍNIMOS E ESPECÍFICOS POR APLICAÇÃO, EM VEZ DE CONCEDER ACESSO GENERALIZADO À REDE. CADA PEDIDO DEVE SER AVALIADO COM BASE NA IDENTIDADE, NO ESTADO DE SEGURANÇA DO DISPOSITIVO, NO CONTEXTO DA SESSÃO, NO RISCO E NA SENSIBILIDADE DO RECURSO”



- Rui Duro -
Check Point Software

cação e a verificação contínua do cumprimento dos requisitos de segurança.

Ricardo Marciano, Business Development Manager e SASE da Fortinet, reforça a ideia de que “é necessário verificar continuamente a postura de segurança do dispositivo, o contexto de acesso e o comportamento do utilizador ao longo da sessão”, garantindo que, em caso de incumprimento dos requisitos definidos, os privilégios de



determinado equipamento podem ser revistos. Na aplicação do Zero Trust, Ricardo Silva, da Cisco, está alinhado com a ideia de que o modelo “exige políticas dinâmicas e contextuais, que se adaptam ao risco e ao comportamento, suportadas por automação e visibilidade unificada”. Neste âmbito, a segurança deve estar, desde logo, integrada da infraestrutura até às aplicações, “com segmentação rigorosa e monitorização constante para mitigar ameaças em ambientes dispersos”.

ONDE FICA A COMPLIANCE?

A opinião é comum entre os responsáveis ouvidos pela IT Insight: o edge tanto pode facilitar como dificultar a *compliance*.

Por um lado, processar e proteger os dados mais perto do local onde são produzidos pode reduzir a circulação desnecessária de informação sensível, apoiar requisitos de residência dos dados e diminuir a exposição associada à transmissão de infor-



- Ricardo Marciano -
Fortinet

mação para data centers distantes. Por outro, a diversidade de localizações aumenta também o número de pontos onde é necessário garantir conformidade.

Segundo Hugo Rego, da Red Hat, a resposta “depende da abordagem”. “Se tratamos cada localização edge como um caso único, a complexidade escala; se adotamos uma abordagem de plataforma, com infraestrutura standardizada, ciclo de vida automatizado e configuração declarativa, o edge acaba por reduzir a complexidade

“ É NECESSÁRIO VERIFICAR CONTINUAMENTE A POSTURA DE SEGURANÇA DO DISPOSITIVO, O CONTEXTO DE ACESSO E O COMPORTAMENTO DO UTILIZADOR AO LONGO DA SESSÃO ”



ao eliminar processos manuais que nunca foram escaláveis”.

Para o responsável, esta distribuição obriga ainda as organizações a resolver problemas que a cloud permitiu adiar, entre os quais a operação *offline*, a limitação de recursos, a segurança física e a conformidade regulatória ao nível de cada localização. “Resolver estes problemas de forma adequada torna toda a operação mais resiliente, não mais complexa”, assegura o Senior Manager.

Na perspetiva de Ricardo Marciano, da Fortinet, este tema está muito dependente da forma como “a segurança é implementada e gerida ao longo da infraestrutura”, com a “falta de uniformidade” a abrir espaço para criar “lacunas de controlo”.

Na prática, é necessário garantir não só a proteção de utilizadores, mas sobretudo “assegurar que as mesmas regras de segurança são aplicadas de forma consistente, quer os recursos estejam na

cloud, num escritório remoto ou num ambiente operacional crítico”.

Rui Duro acredita que o desafio não reside propriamente no edge, mas sim nesta capacidade de alinhar “políticas, evidências e níveis de proteção consistentes” ao longo de toda a infraestrutura.

“O edge torna a *compliance* mais eficaz quando aproxima a aplicação dos controlos do risco real; torna a *compliance* mais difícil quando multiplica infraestruturas sem multiplicar a visibilidade e a capacidade de governação”, resume o Country Manager da Check Point em Portugal.

A GESTÃO DE AMBIENTES DISTRIBUÍDOS

Ricardo Silva, da Cisco Portugal, recorda que a atual arquitetura está a privilegiar a “orquestração e automação” na gestão de ambientes heterogêneos para garantir “consistência operacional”.

No entanto, esta gestão remota não está isenta de desafios. A garantia da consistência de confi-



gurações, a necessidade de operar em locais com recursos limitados e a resposta em caso de incidentes obriga a que estas plataformas sejam capazes de suportar “automação avançada, monitorização centralizada e capacidades de orquestração”, que permitam **a gestão eficiente de “milhares de pontos distribuídos, minimizando custos operacionais e riscos associados”**, explica Ricardo Silva, que aponta para este tópico como um dos “focos na evolução tecnológica da Cisco”.



- Victor Gago -
Schneider Electric

“MAIS DO QUE UMA DESCENTRALIZAÇÃO DA CAPACIDADE DE COMPUTAÇÃO, QUE ESTAMOS PERANTE UMA “DISTRIBUIÇÃO MAIS INTELIGENTE DAS CARGAS DE TRABALHO”, EM QUE DATA CENTERS, CLOUD E EDGE DESEMPENHAM FUNÇÕES COMPLEMENTARES EM FUNÇÃO DOS REQUISITOS DE CADA APLICAÇÃO”

Na hora de gerir eficazmente milhares de localizações distribuídas, Hugo Rego relembra que a automação e a standardização são as melhores aliadas. “Na Red Hat, ajudamos os nossos clientes a construir aquilo a que chamamos um *blueprint*: uma *golden image* que define todo o *stack* para um determinado tipo de localização”, explica o Senior Manager. A partir daqui as atualizações necessárias são distribuídas e as implementações acontecem de forma automática. A intervenção humana passa a ser uma exceção, e não a regra. Alguns dos exemplos práticos encontram-se nas *utilities*, nomeadamente na gestão de subestações, e na gestão de infraestrutura de lojas de retalhistas. **A distribuição da capacidade computacional traz também exigências ao nível da infraestrutura física.** Victor Gago, da Schneider Electric, lembra que cada nova localização precisa de assegurar alimentação elétrica, refrigeração e conectividade com níveis de disponibilidade e resiliência



adequados às aplicações. Neste contexto, o responsável da Schneider Electric destaca a normalização e a utilização de soluções modulares e replicáveis como formas de acelerar a implementação e manter padrões consistentes entre diferentes localizações.

A VISIBILIDADE NUM AMBIENTE SEM PERÍMETRO

Do ponto de vista da segurança, a multiplicidade das localizações adicionou uma camada de complexidade à gestão remota, com a visibilidade a surgir como um dos maiores desafios.

Rui Duro relembra que “uma equipa de segurança não consegue proteger adequadamente aquilo que não consegue identificar, classificar e monitorizar”, especialmente em ambientes distribuídos onde podem coexistir os mais diversos contextos.

No fim, o Country Manager resume aquelas que considera serem as três capacidades fundamentais: “visibilidade sobre todos os ativos, políticas consistentes em todos os ambientes e capacidade para responder sem depender da presença física de um especialista em cada localização”.

Ricardo Marciano, da Fortinet, acrescenta mais dois desafios: o primeiro

envolve a crescente utilização de aplicações cloud e dispositivos que nem sempre são geridos a partir da própria organização, o que obriga a “complementar os controlos tradicionais de acesso com mecanismos capazes de monitorizar a utilização das aplicações cloud, identificar comportamentos de risco e detetar possíveis configurações inseguras ou exposições indevidas de informação”; o segundo prende-se com a escassez de recursos especializados em cibersegurança.

A dificuldade de diagnóstico aumenta também à medida que a infraestrutura se distribui. Ricardo Marciano dá como exemplo uma situação de degradação do desempenho de uma aplicação: a organização precisa de conseguir determinar se a origem está no dispositivo, na rede local, no fornecedor de Internet, numa aplicação SaaS ou na própria infraestrutura empresarial, tornando a observabilidade de ponta a ponta particularmente relevante.

“O sucesso da gestão remota depende cada vez mais da combinação entre visibilidade operacional, controlo consistente sobre aplicações e dados, e capacidade de resposta contínua aos riscos de segurança, independentemente do local, dispositivo ou modelo de trabalho adotado”, conclui. ■

claranet®

POR PEDRO TEIXEIRA,
Cloud & Infra Senior Director, Claranet Portugal

NA TECNOLOGIA, A PERIFERIA AINDA É UMA ESCOLHA

A computação distribuída está a passar da experimentação para a infraestrutura – e a questão mais relevante para as organizações passa a ser o que deve, de facto, estar no Edge.

EM PORTUGAL habituámo-nos, nos últimos anos, a discutir tudo aquilo que está a ser empurrado para a periferia. Na tecnologia, felizmente, ainda podemos escolher.

Durante anos, a centralização da capacidade computacional na *Cloud* respondeu eficazmente às necessidades de escala, eficiência e flexibilidade das organizações, mas o aparecimento de *workloads* para os quais a distância passou a ser uma variável crítica desafia a validade desse modelo: sistemas que precisam de tomar decisões em milissegundos, operações em que transportar grandes volumes de dados custa mais do que processá-los localmente ou requisitos de soberania e resiliência que condicionam o local onde os dados podem ser tratados.



- Pedro Teixeira -

Cloud & Infra Senior Director, Claranet Portugal

CRIAR CAPACIDADE É, CONTUDO, APENAS UMA PARTE DA EQUAÇÃO. A DECISÃO FUNDAMENTAL CONTINUA DENTRO DAS ORGANIZAÇÕES. E AQUI IMPORTA RESISTIR À TENTAÇÃO DE TRATAR O EDGE COMO UMA ORIENTAÇÃO TECNOLÓGICA QUE DEVE SER ADOTADA POR INTEIRO.

É nestas situações que o Edge deixa de ser apenas uma opção arquitetural e passa a ser uma necessidade operacional, porque diferentes *workloads* devem correr nos ambientes mais adequados às suas características. É aqui que terminam as semelhanças entre “periferias”, porque no nosso cenário tecnológico, não se trata de substituir a *Cloud* ou deslocar indiscriminadamente a capacidade computacional para a periferia, mas sim de ampliar os recursos disponíveis para criar o modelo apropriado, gerindo as várias opções de acordo com as necessidades.

A Europa já traduz esta evolução em metas concretas. No âmbito da Década Digital, a União Europeia definiu o objetivo de ter 10 mil nós Edge climaticamente neutros e altamente seguros até 2030 e de 75% das empresas europeias utilizarem tecnologias *Cloud-Edge*. Em Portugal, o Plano Nacional de Nuvem Soberana e o Plano Nacional de Centros de Dados mostram também que capacidade computacional, resiliência e soberania digital passaram a fazer parte da discussão estratégica sobre as infraestruturas do país.

Criar capacidade é, contudo, apenas uma parte da equação. A decisão fundamental continua dentro das organizações. E aqui importa resistir à tentação de tratar o Edge como uma orientação tecnológica que deve ser adotada por inteiro. Insisto: *Cloud-Edge* são complementares e não mutuamente exclusivas.

Para cada caso, há que colocar, desde logo, quatro questões essenciais. A operação exige tempos de resposta que uma infraestrutura centralizada não consegue garantir? O custo ou a complexidade de transportar os dados justifica processá-los localmente? Existem requisitos de soberania, segurança ou residência dos dados que condicionam o local de processamento? O sistema tem de continuar a funcionar quando a ligação ao centro falha? Dependendo das respostas, uma plataforma centralizada pode continuar a ser a decisão técnica e economicamente mais racional. No Edge devem estar *workloads* que se justifiquem e é precisamente neste ponto que a arquitetura híbrida ganha importância, permitindo colocar cada *workload* no ambiente onde cria mais valor, e mantendo uma camada coerente de gestão,

AO CONTRÁRIO DO QUE ACONTECE NAS NOSSAS CIDADES, NA TECNOLOGIA A PERIFERIA CONTINUA A SER UMA ESCOLHA - E É ESSA ESCOLHA, FEITA COM CRITÉRIO, QUE SEPARA QUEM TIRA PARTIDO DO EDGE DE QUEM APENAS LHE CEDE ESPAÇO POR INÉRCIA.

segurança e governação. Neste cenário, *Cloud*, data center e Edge não são opções concorrentes, mas componentes de uma mesma arquitetura.

Esta lógica é particularmente importante quando falamos de soberania, que nos exige saber onde estão os nossos dados, quem os controla, sob que jurisdição são tratados e que nível de autonomia é necessário em função da sua criticidade. Portanto, o desafio não é, necessariamente, a obrigatoriedade desses dados permanecerem num determinado local; trata-se de classificar dados e *workloads* e aplicar a cada um os requisitos adequados de soberania, segurança e resiliência.

Mas decidir onde processar é apenas o início. Um piloto de Edge em poucas instalações pode ser relativamente simples de gerir e, mais tarde, quando se escala o projeto, manutenção, monitorização, atualizações e segurança tendem a revelar-se mais complexos. A automação passa então a ser indispensável, tal como as competências necessárias para operar sistemas distribuídos de forma segura e consistente.

Por isso, a capacidade para operar, automatizar, monitorizar e proteger uma infraestrutura distribuída tem de fazer parte da decisão de investimento desde o início, prevendo a possibilidade de evolução para um modelo de computação distribuída. E, sendo esse o caso, não se elimina a necessidade de controlo centralizado, porque quanto mais distribuída for a infraestrutura, mais coerentes terão de ser a sua governação, segurança e operação.

A pergunta a levar para a próxima decisão de investimento não é, portanto, se a organização já tem uma estratégia de Edge ou se está a caminho de empurrar tudo para a periferia. O essencial é perceber que *workloads* precisam efetivamente dela, onde devem correr e se a organização está preparada para os escalar e operar. Ao contrário do que acontece nas nossas cidades, na tecnologia a periferia continua a ser uma escolha - e é essa escolha, feita com critério, que separa quem tira partido do Edge de quem apenas lhe cede espaço por inércia. ■



ENTERPRISE MOBILITY: A MOBILIDADE PASSOU A SER UMA QUESTÃO DE ARQUITETURA

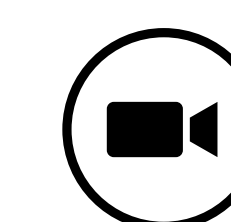


Há muito que a mobilidade empresarial deixou de significar apenas permitir que os colaboradores trabalhem fora do escritório. Num contexto em que utilizadores, dispositivos, aplicações e dados se distribuem por diferentes ambientes, garantir uma experiência simples, segura e consistente exige uma abordagem integrada. Arrow, em representação da HPE Networking, Asus, Claranet Portugal, DDC Group, Exclusive Networks, Konica Minolta, Ricoh e WatchGuard analisam os desafios e as prioridades das organizações na evolução das suas estratégias de enterprise mobility.

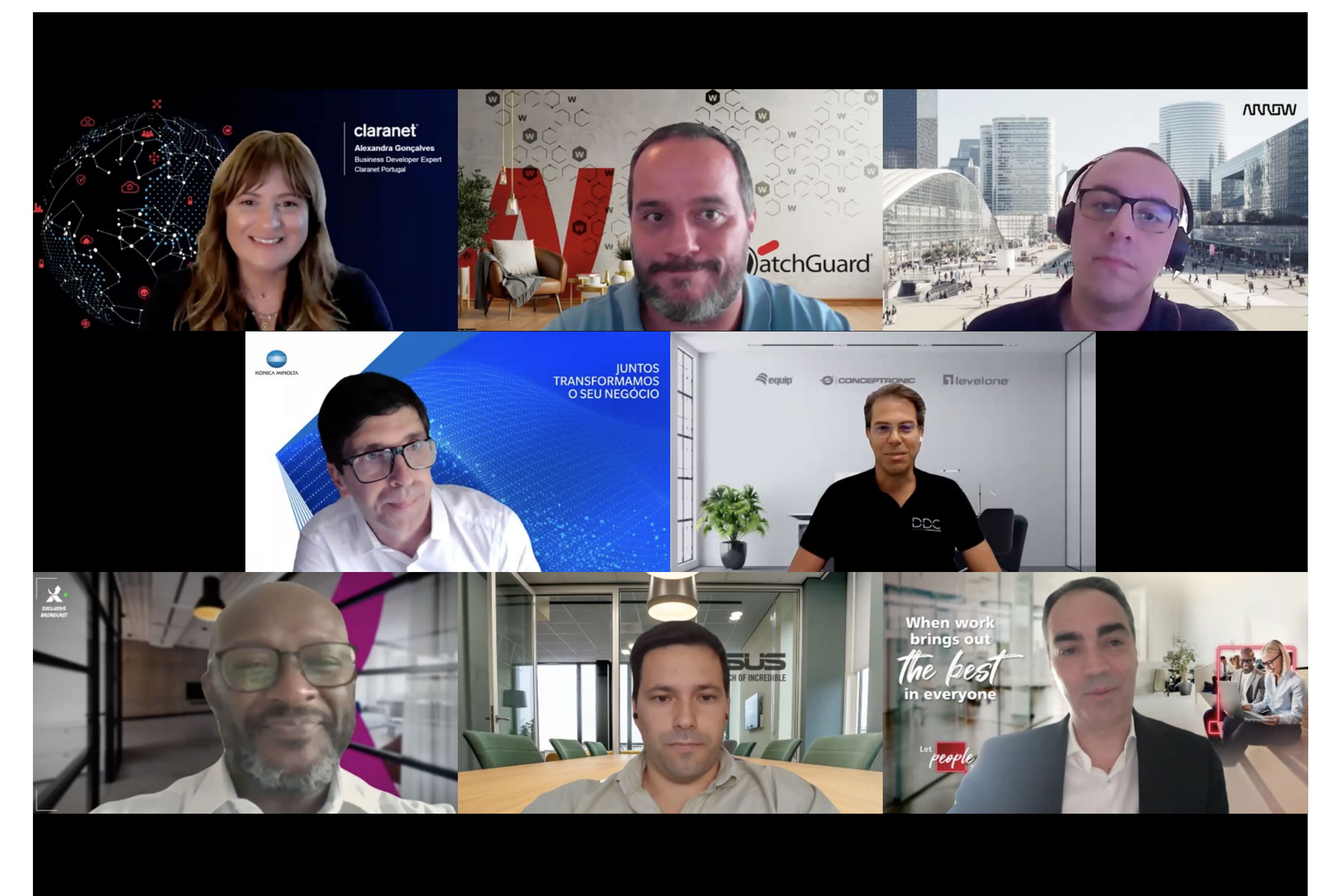
RUI DAMIÃO

O PERÍMETRO TRADICIONAL da empresa tornou-se cada vez mais difícil de definir. Os colaboradores acedem aos recursos corporativos a partir de diferentes localizações e equipamentos, as aplicações estão distribuídas entre ambientes locais e cloud e a conectividade deixou de estar confinada à rede do escritório. Ao mesmo tempo, as organizações procuram dar aos utilizadores maior flexibilidade sem comprometer a segurança, a capacidade de gestão ou a qualidade da experiência.

Neste cenário, a mobilidade empresarial já não pode ser encarada como a soma de iniciativas isoladas em torno dos dispositivos móveis ou do trabalho remoto. Rede, *endpoint*, identidade, segurança, colaboração e gestão têm de funcionar de forma articulada, enquanto as equipas de IT enfrentam ambientes cada vez mais heterogéneos e procuram reduzir complexidade. O desafio passa por encontrar o equilíbrio entre liberdade e controlo, simplificar a operação e garantir que a mobilidade contribui efetivamente para a produtividade e para o negócio.

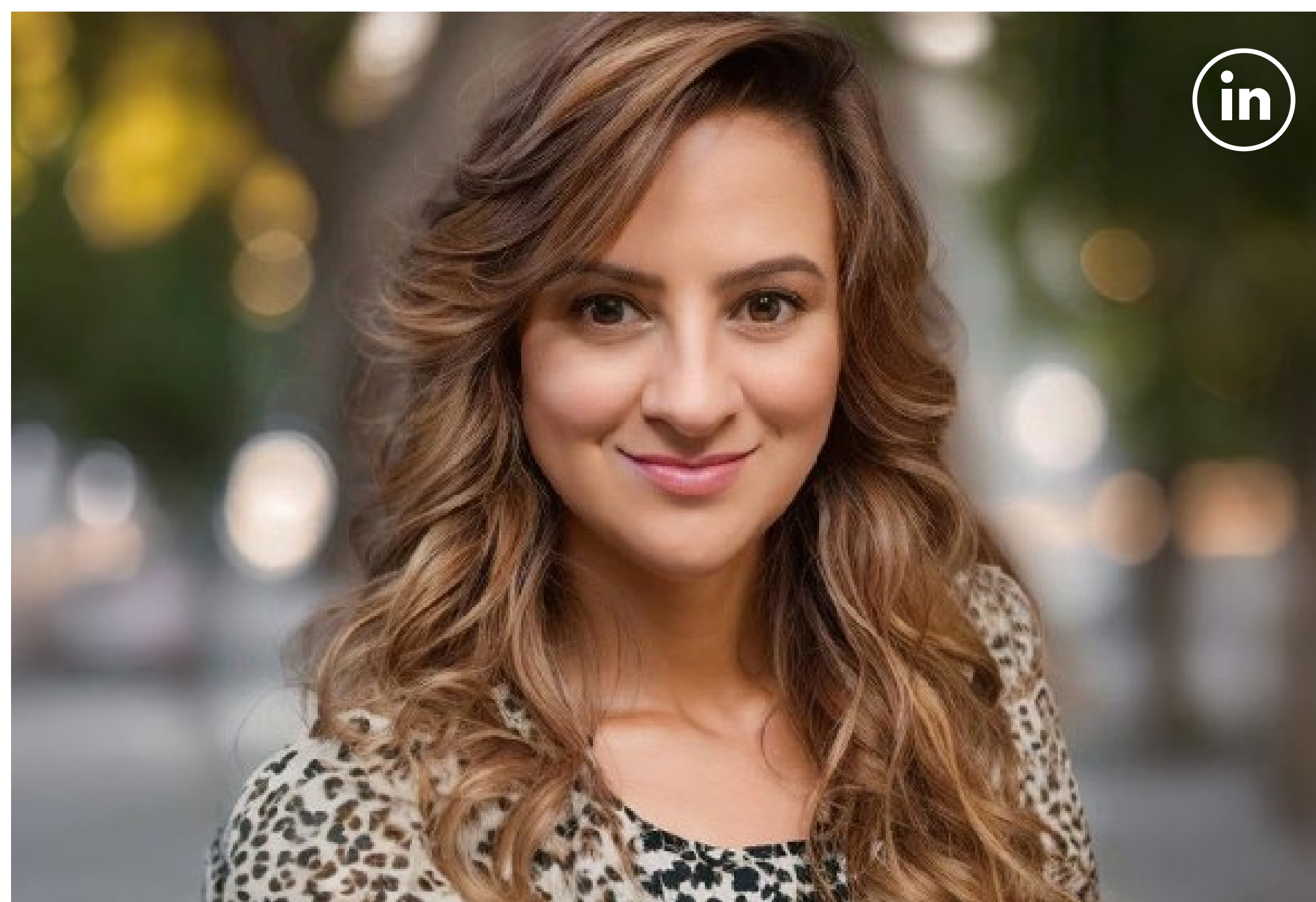


PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM





A INTELIGÊNCIA ARTIFICIAL (IA) GENERATIVA ESTÁ A MUDAR A FORMA COMO OS UTILIZADORES TRABALHAM, MAS TAMBÉM ESTÁ A MUDAR O QUE AS EMPRESAS VENDEM E COMO VENDEM. AS EMPRESAS PORTUGUESAS ESTÃO PREPARADAS PARA ESSA TRANSIÇÃO OU AINDA ESTÁ A MAIORITARIAMENTE A VENDER HARDWARE E LICENÇAS?



- Alexandra Gonçalves -
Claranet Portugal

Alexandra Gonçalves, Endpoint Solutions Business Developer Expert, Claranet Portugal: “Não há uma resposta simples e direta porque há uma desigualdade profunda no mercado português. O mercado transacional continua vivo e está tudo bem, não há um retrocesso porque essa é a base para o resto. **Se não tivermos equipamentos seguros, por exemplo, ninguém vai pensar em trabalho híbrido.** A grande viragem está no que acontece a essa aquisição e a IA generativa veio mudar esse foco: preocupamo-nos na experiência do utilizador, como é que vai utilizar o equipamento e as ferramentas de IA.”

“ A TECNOLOGIA FUNCIONA, MAS HÁ FALHAS NO ACOMPANHAMENTO DO PROJETO, DURANTE E DEPOIS DE ELE ACABAR ”

ALEXANDRA GONÇALVES, ENDPOINT SOLUTIONS BUSINESS DEVELOPER EXPERT, CLARANET PORTUGAL



João Gorgulho, Country Manager, DDC Group: “O mercado continua muito habituado a vender hardware e não há nada de errado nisto. Com a inteligência artificial parece que deixámos de precisar de hardware e infraestrutura e é exatamente o contrário. A infraestrutura é crítica para trabalhar em qualquer lado ou utilizar a cloud. O cliente já não quer comprar um *switch*, mas quer saber como é que isto vai tornar a empresa mais produtiva, como é que vai funcionar daqui a três anos. Ainda há uma transformação a fazer”

“ A QUESTÃO JÁ NÃO É SE O FUTURO É FÍSICO OU DIGITAL. SE TRABALHAMOS NO ESCRITÓRIO OU FORA DELE TAMBÉM NÃO É UM TEMA. NO ENTANTO, EXISTE ESTA DIGITALIZAÇÃO, MAS INTERAGIMOS COM PESSOAS E MÁQUINAS”

JOÃO GORGULHO, COUNTRY MANAGER, DDC GROUP



- João Gorgulho -
DDC Group

Ricardo Nascimento, Head of Sales, Ricoh: “Estamos numa fase de transição. Ainda existe o mercado de venda de hardware e licenças, tem de continuar a existir, mas já não é suficiente. Temos de perceber como é que podemos trazer valor. A inteligência artificial vai transformar o software numa *commodity*. É preciso perceber como é que o software traz valor para o negócio para trazer resultados. Hoje, o tema não é só o que vendemos, mas sim que valor é que trazemos para os clientes”



Nelson Martins, Key Account Manager, Asus: “Temos vindo a assistir a essa transição por parte das empresas a ritmos diferentes e de acordo com a dimensão de cada uma. Os grandes integradores vendem as licenças e o hardware, mas também vendem soluções completas desenhados à medida de cada cliente. Estas empresas tentam apresentar uma proposta de valor que vá de encontro às necessidades dos clientes, mas acrescentando valor para estarem preparados para o futuro”

O TRABALHO HÍBRIDO NORMALIZOU-SE, MAS OS MODELOS DE GESTÃO E DE SEGURANÇA AINDA NÃO ACOMPANHARAM. QUEM ESTÁ, NA PRÁTICA, A PAGAR ESSA FATURA? É O IT, O UTILIZADOR FINAL OU, EVENTUALMENTE, O PARCEIRO DE CANAL?

Emanuel Campos, Presales Consultant, Arrow, em representação da HPE Networking: “Na realidade, a fatura vai ser paga pelos três de formas diferentes. As equipas de IT têm de gerir utilizadores que estão por todo o lado, aplicações por todo o lado e requisitos de segurança cada vez mais exigentes. Os utilizadores finais esperam uma experiência simples, transparente e sem muitos problemas. Os parceiros de canal têm uma maior responsabilidade porque têm de desenhar arquiteturas que suportem tudo isto”

José Gonçalves, Solutions Engineering Manager, Exclusive Networks: “Aquilo que temos vindo a assistir é que o ambiente até ao COVID-19 as organizações trabalhavam num ambiente de ‘muralha da China’; com o ambiente híbrido isso desapareceu por completo. Existe uma componente muito importante que é o utilizador final, que é o foco da maior parte dos ataques e existe toda a necessidade de ele estar atento para a proteção de dados. **A IA – que toda a gente utiliza e toda a gente gosta – não costuma ter a sua utilização avaliada e não se percebe se é ou não utilizada da melhor forma”**



A PROLIFERAÇÃO DE DISPOSITIVOS E AMBIENTES FRAGMENTADOS CRIOU UMA SUPERFÍCIE DE ATAQUE MUITO MAIOR. A SEGURANÇA JÁ É UM ARGUMENTO DE VENDA OU CONTINUA A SER VISTA COMO UM CUSTO QUE O CLIENTE QUER MINIMIZAR?



- António Correia -
WatchGuard

António Correia, Area Sales Manager, WatchGuard: “O que é um facto é que tudo ganhou uma complexidade muito maior, sendo que as equipas de IT permanecem as mesmas ou até foram otimizadas com menos pessoas. **É muito fácil atirar tecnologia para os problemas, mas é preciso ter uma série de coisas por trás para que os problemas sejam resolvidos e cresçam seguras.** O que não falta é tecnologia e ofertas; é preciso escolher muito bem para poder escalar as soluções e fazê-lo de forma rentável para a organização”

“NOTA-SE UMA LIGAÇÃO ENTRE OS CLIENTES QUE ESTÃO MAIS SENSIBILIZADOS PARA A NECESSIDADE DE INVESTIR EM CIBERSEGURANÇA COM OS QUE ACEITAM MELHOR A AQUISIÇÃO DE SERVIÇOS”

ANTÓNIO CORREIA, AREA SALES MANAGER, WATCHGUARD



Emanuel Campos, Arrow, em representação da HPE Networking: “A segurança da solução já não é apenas um argumento de custo. Todos sabemos que uma falha de segurança pode ter impacto de várias ordens que, muitas vezes, pode ser superior ao investimento necessário para prevenir que o evento tivesse acontecido. A segurança deve ser integrada e deve estar em toda a infraestrutura. O modelo Zero Trust, segmentação dinâmica e visibilidade total, por exemplo, permite reduzir os custos e não aumentar a complexidade das suas soluções”

“TEM DE SE ACRESCENTAR VALOR AO NEGÓCIO DO CLIENTE. HÁ UMA TENDÊNCIA PARA INVESTIMENTOS HÍBRIDOS, OU SEJA, INVESTIMENTO NOS MODELOS TRADICIONAIS COM INVESTIMENTOS EM SERVIÇOS”

EMANUEL CAMPOS, PRESALES CONSULTANT, ARROW, EM REPRESENTAÇÃO DA HPE NETWORKING:



- Emanuel Campos -
Arrow, em representação da HPE Networking

Ricardo Nascimento, Ricoh: “Embora tenha vindo a mudar muito nos últimos anos e haja um *mindset* diferente nas empresas, depende muito da maturidade dos clientes. Há empresas que consideram, mas depois não investem. Há uns anos, quando se falava de cortar custos, a segurança era uma das primeiras; esse *mindset* mudou, mas por vezes, quando é preciso cortar, ainda se vai à segurança. Este tema tem de estar em todas as conversas para entregar mais valor para os clientes”



FALA-SE MUITO DE MODELOS DE SUBSCRIÇÃO E AS-A-SERVICE. NA REALIDADE DO MERCADO PORTUGUÊS, OS CLIENTES ESTÃO DISPOSTOS A PAGAR POR VALOR CONTÍNUO OU A PREFERÊNCIA É AINDA PELA COMPRA DIRETA?

Fernando Rodrigues, Workplace Business Development Manager, Konica Minolta: “O que notamos é que há cada vez mais uma migração para modelos as-a-Service, ainda que em diferentes ofertas na área do *workplace*. Se pegarmos na parte de *printing*, isso já está em as-a-Service; na parte do posto de trabalho, ainda há um caminho para percorrer; se formos para a área de *smart room* é praticamente todo transacionável. **Tem de haver um valor agregado aos equipamentos, saber o que está a acontecer, se está atualizada, se é segura e se é útil aos colaboradores**”





António Correia, WatchGuard: “Vemos cada vez mais uma adoção, mas é uma adoção muito tímida. Juntamente com o as-a-Service, os parceiros têm de ter verdadeiramente a componente do serviço, e especialmente na área de segurança, para dar um acompanhamento das soluções, afinação de políticas, por exemplo. Há um caminho a fazer de que o serviço está a ser feito e mostrar o que está a ser feito para dar visibilidade ao cliente. Nota-se uma ligação entre os clientes que estão mais sensibilizados para a necessidade de investir em cibersegurança com os que aceitam melhor esta forma de adquirir”

Emanuel Campos, Arrow, em representação da HPE Networking: “Tem de se acrescentar valor ao negócio do cliente. Há uma tendência para investimentos híbridos, ou seja, investimento nos modelos tradicionais com investimentos em serviços. **A conversa está cada vez mais centrada na capacidade de servir o negócio.** O mercado português tem um pouco de tudo que valoriza o modelo tradicional de aquisição, mas também vemos uma evolução para modelos de consumos flexíveis”

A IA NO POSTO DE TRABALHO VAI REDUZIR FRICÇÃO PARA O UTILIZADOR, MAS PODE AUMENTAR COMPLEXIDADE PARA O IT. O CANAL ESTÁ A POSICIONAR-SE COMO SIMPLIFICADOR NESSA EQUAÇÃO OU ESTÁ A TORNAR-SE EM MAIS UMA CAMADA DE COMPLEXIDADE?

João Gorgulho, DDC Group: “Essa é uma das grandes oportunidades para o canal: ou simplificamos ou somos parte do problema. Para o utilizador, tudo parece mais simples. **Trabalhar em casa ou no escritório é cada vez mais simples para o utilizador, mas alguém teve de ter a certeza que tudo funciona da melhor maneira e mais simples possível.** O erro seria o canal responder a essa complexidade com mais tecnologia, com mais uma plataforma; isso não é simplificar, mas sim empilhar, atirar hardware para cima. O parceiro que ganha relevância é o que consegue olhar para tudo isto para tornar a vida do cliente mais simples”



Alexandra Gonçalves, Claranet Portugal: “A perceção que tenho é que o canal tem de assumir um papel de simplificador. Despejar licenças e ferramentas na mão do cliente não simplifica nada e só cria ruído. A inteligência artificial só facilita a vida de todos os utilizadores – IT incluído – se houver alguém que trate da complexidade, desta mão invisível que está sempre associada. Temos de ser agentes simplificadores e apoiamos o cliente desde a parte inicial até à gestão proativa, mas reforçando o papel de consultor, de trabalho invisível de suporte e segurança para que a IA liberte os utilizadores de alguma das funções que tinham de fazer, mas sem que isso asfixie o IT”

José Gonçalves, Exclusive Networks: “Nesta fase, a inteligência artificial ainda é muito recente. A componente do *shadow IT* pode ser qualquer um; com as ferramentas que temos, podemos utilizar muitas ferramentas para agilizar algum processo, estando a criar uma camada de *shadow IT*. Os fabricantes estão a tentar dar resposta a isto, com aquisições quase mensais, porque o utilizador tem acesso a ferramentas quase em exclusivo para ele e o IT não tem visibilidade. A visibilidade é a coisa mais importante do IT e a IA tem de vir para o IT para se ter essa visibilidade”

“É MUITO FÁCIL VENDER TECNOLOGIA AOS CLIENTES FINAIS, MAS SEM A COMPONENTE DE CONSULTORIA NÃO SE CONSEGUE COMPREENDER VERDADEIRAMENTE AS NECESSIDADES DO CLIENTE E DO NEGÓCIO”

JOSÉ GONÇALVES, SOLUTIONS ENGINEERING MANAGER, EXCLUSIVE NETWORKS



- José Gonçalves -
Exclusive Networks



COM A PROLIFERAÇÃO DE FORMATOS E ESPECIFICAÇÕES, COMO NPU INTEGRADAS, DISPOSITIVOS HÍBRIDOS E ULTRAPORTÁTEIS, COMO É QUE SE COMUNICA AO CLIENTE EMPRESARIAL O QUE REALMENTE IMPORTA, SEM SE PERDER EM ESPECIFICAÇÕES TÉCNICAS QUE O DECISOR NÃO CONSEGUE AVALIAR?



- Nelson Martins -
Asus

Nelson Martins, Asus: “O mercado oferece uma quantidade enorme de alternativas. Hoje, existem dispositivos para todos os gostos, quase para cada pessoa. Com tanta transição tecnológica de uma forma geral, o mercado torna-se um pouco confuso, até para os fabricantes que trabalham com isto todos os dias. Para o cliente final não é fácil tomar uma decisão. Ter várias opções é bom na teoria, mas na prática cria muita confusão. O desafio é perceber o que é que o cliente precisa, que se calhar precisa de mobilidade e fácil de transportar e com elevada autonomia”

“SE CONTINUARMOS A VENDER A SEGURANÇA DO HARDWARE COMO UMA ESPECIFICAÇÃO, MORRE NO PAPEL; SE FOR COMO ALGO INTEGRADO DO EQUIPAMENTO, A SEGURANÇA PASSA A SER VISTA COMO UM PESO E RELEVÂNCIA MAIOR”

NELSON MARTINS, KEY ACCOUNT MANAGER, ASUS



QUAIS SÃO AS FALHAS MAIS CRÍTICAS QUANDO SE TRATA DE VENDER SOLUÇÕES DE *WORKPLACE* MODERNO EM COMPARAÇÃO COM A VENDA DO PRODUTO?

Ricardo Nascimento, Ricoh: “Este tema depende de quem vende, mas também de quem compra. As empresas têm de estar disponíveis para esta conversa disruptiva. A maior falha é tentar vender, passe a expressão, a enciclopédia; vende especificações. **É preciso perceber a solução que traz mais valor para o negócio, que traz mais valor para as equipas, mas também é necessário que quem compra esteja disponível para essa conversa.** O posto de trabalho mudou muito, é muito mais misto, e tem de ser adaptado. É preciso um posto de trabalho mais inteligente, mais colaborativa”

José Gonçalves, Exclusive Networks: “Um dos temas passa pelo utilizador final. Estamos a falar de uma equipa que faz a aquisição e a análise das necessidades, mas, no fim do dia, o utilizador final tem uma palavra muito importante para dar. É fácil entrar num processo em que se faz uma aquisição de um tipo de computadores para responder a um conjunto de características, mas o utilizador vai sentir o impacto no seu dia a dia, até com o evoluir das soluções que vão aparecendo”



A SEGURANÇA AO NÍVEL DO HARDWARE É FREQUENTEMENTE UM ARGUMENTO NO PAPEL. NO TERRENO, ESSE ARGUMENTO CHEGA À CONVERSA COM O CLIENTE OU FICA PELA LISTA DE ESPECIFICAÇÕES TÉCNICAS?

Nelson Martins, Asus: “Falando concretamente dos computadores, a segurança não é o primeiro ponto que se refere. É algo que surge à medida que a venda vai avançando porque é mandatório em qualquer empresa, principalmente no contexto atual em que se acede a dados a partir de qualquer local. A questão da segurança também vai depender muito do grau de maturidade das empresas, como se aborda o tema junto dos clientes finais e dos envolvidos nesta conversa. Se continuarmos a vender a segurança do hardware como uma especificação, morre no papel; se for como algo integrado do equipamento, a segurança passa a ser vista como um peso e relevância maior”

Fernando Rodrigues, Konica Minolta: “É um tema relevante, mas depende do interlocutor. Ao final do dia, acaba por ser um conjunto de especificações que são pedidas e têm de ser cumpridas. É preciso garantir que a discussão é outra e vai mais além. É preciso garantir a segurança durante três, quatro ou cinco anos e uma solução tecnológica e aplicacional ajustada. O que faz diferença junto dos clientes é ter recursos com competências diferenciadas. Quando endereçamos este tema, se formos com um cardápio cheio de soluções só se cria confusão. É preciso gerar confiança”



A ABORDAGEM PASSOU DE EM VEZ DE ESTARMOS A FALAR DE MANAGED PRINT SERVICES PARA MANAGED DOCUMENT SERVICES E TRANSFORMARMOS DADOS EM INFORMAÇÃO. A DISCUSSÃO TORNA-SE MAIS AMPLA”



- Fernando Rodrigues -
Konica Minolta



NUM MERCADO ONDE O DOCUMENTO FÍSICO ESTÁ SOB PRESSÃO E O DIGITAL É NORMA, COMO É QUE SE JUSTIFICA RELEVÂNCIA NUMA CONVERSA SOBRE O FUTURO DO TRABALHO JUNTO DOS DECISORES DE IT?



- Ricardo Nascimento -
Ricoh

Ricardo Nascimento, Ricoh: “O papel é apenas uma fonte de dados. A relevância já não vem da fonte da informação e o mais importante são os dados. É importante perceber como se vai colocar a informação e os dados ao serviço do utilizador. O futuro do trabalho não é imprimir menos ou mais, mas garantir que a informação correta chega à pessoa certa de forma segura para acrescentar valor não só ao processo, mas também aos clientes e à organização para estar ao serviço do negócio”

“ O POSTO DE TRABALHO MUDOU MUITO, É MUITO MAIS MISTO, E TEM DE SER ADAPTADO. É PRECISO UM POSTO DE TRABALHO MAIS INTELIGENTE, MAIS COLABORATIVA ”

RICARDO NASCIMENTO, HEAD OF SALES, RICOH

Fernando Rodrigues, Konica Minolta: “Existe uma pressão sobre o documento físico, em que se mantém ou diminui, mas em compensação o número de documentos digitais cresce exponencialmente. A preocupação não é tanto o documento físico, que existe e vai continuar a existir, até por questões legais. A abordagem passou de em vez de estarmos a falar de *managed print services* para *managed document services* e transformarmos dados em informação. A discussão torna-se mais ampla”



João Gorgulho, DDC Group: “A questão já não é se o futuro é físico ou digital. Se trabalhamos no escritório ou fora dele também não é um tema. No entanto, existe esta digitalização, mas interagimos com pessoas e máquinas. **Vivemos num mundo físico. Para um decisor de IT não deve ser se vamos imprimir documentos, mas como é que a informação circula na organização, como a protegemos.** Existe uma rede e uma infraestrutura e, sem isso, não existe um *workplace* moderno. Não existe o futuro do trabalho sem uma infraestrutura preparada para o suportar”

O CANAL GENERALISTA TEM COMPETÊNCIA REAL PARA VENDER SEGURANÇA DE FORMA INTEGRADA NUM AMBIENTE HÍBRIDO OU O MODELO ATUAL FRAGMENTA DEMASIADO A PROPOSTA PARA SER EFICAZ?

António Correia, WatchGuard: “Ao entrar no mercado de *best-of-breed*, o canal generalista arrisca a não ter as competências necessárias e a não fornecer recursos e capacidade técnica. A área da cibersegurança evolui de forma muito rápida e é fácil ficar obsoleto. **Acreditamos que o caminho está na consolidação, na entrega de uma plataforma que inclua um serviço de SOC para olhar para os recursos do cliente.** Para conseguir fazer isto, tenho de dedicar muito tempo e se calhar esse é o maior custo”

Alexandra Gonçalves, Claranet Portugal: “Neste momento, o canal generalista não consegue vender segurança integrada. A segurança integrada exige especialização e operação contínua, que não está muito na génese do que é o canal generalista. É preciso um conceito de vender segurança integrada, não só uma ideia de vender licenças. Muitos dos nossos colaboradores trabalham fora do perímetro do escritório e que haja uma transição para um modelo de MSSP”



OS FORNECEDORES DE SERVIÇOS GERIDOS TÊM UMA VISÃO DO QUE FALHA NO TERRENO DEPOIS DE AS SOLUÇÕES SEREM IMPLEMENTADAS. QUAL É O PADRÃO DE FALHA MAIS COMUM E O QUE DIZ ISSO SOBRE COMO AS EMPRESAS ESTÃO A IMPLEMENTAR O LOCAL DE TRABALHO MODERNO?

José Gonçalves, Exclusive Networks: “Aqui passa muito pela capacidade de entregar aos clientes uma componente de consultoria. É muito fácil vender tecnologia aos clientes finais, mas sem a componente de consultoria não se consegue compreender verdadeiramente as necessidades do cliente e do negócio. **É preciso casar as necessidades do negócio com a venda das soluções e é aí que aparecem muitos *gaps* porque não faz *fit* com as necessidades da organização**”

Alexandra Gonçalves, Claranet Portugal: “A venda consultiva é muito importante. O que temos visto ao olhar para o terreno é que as falhas raramente são tecnológicas. A tecnologia funciona, mas há falhas no acompanhamento do projeto, durante e depois de ele acabar. Entrega-se o produto, as ferramentas, e assume-se que está tudo a funcionar. Os utilizadores acabam por voltar aos padrões antigos e é preciso existir um acompanhamento para utilizar as soluções. Sem isso, as soluções estão corretas, mas não são utilizadas da melhor maneira para a organização e para o trabalho dos utilizadores” ■



ZERO TRUST:
A SEGURANÇA QUE COMEÇA ONDE
O PERÍMETRO ACABOU

O perímetro de segurança não desapareceu de um dia para o outro; foi sendo contornado, credencial a credencial, sessão a sessão e exceção a exceção. O Zero Trust surgiu como resposta a essa erosão silenciosa, mas a distância entre o conceito e a implementação real continua a ser o maior risco que muitas organizações não conseguem ver.

RUI DAMIÃO

HÁ ANOS QUE O ZERO TRUST domina o vocabulário de cibersegurança, até porque num mundo onde os perímetros tradicionais desapareceram, ninguém deve ser automaticamente confiável. O problema é que a distância entre o conceito e a implementação real permanece enorme. A Gartner estima que 63% das organizações afirmam ter implementado Zero Trust de forma parcial ou total, mas, na prática, a história é diferente.

A DIFERENÇA ENTRE INTENÇÃO E EXECUÇÃO

“O *gap* mais comum é confundir Zero Trust com um conjunto de produtos. Muitas organiza-

ções comparam MFA, um *gateway* ZTNA [Zero Trust Network Access] e um EDR [Endpoint Detection and Response] e consideram o tema fechado”, explica David Silva, CEO da CyberX. “O que encontramos nos exercícios de *red team* é outra coisa: uma vez lá dentro – normalmente entramos, por um [ataque de] phishing ou por uma credencial reutilizada –, a rede continua plana e a confiança continua implícita. A maioria implementou autenticação forte à entrada e continua a não ter autorização granular lá dentro”, indica David Silva, que acrescenta, que “Zero Trust não é como se entra, é o que se consegue alcançar depois de entrar”.

O “Verizon Data Breach Investigations Report 2025”, que analisou mais de 22 mil incidentes e 12.195 brechas confirmadas, revelou que 22% de todas as brechas tiveram credenciais roubadas como vetor de entrada inicial, que 88% dos ataques a aplicações web básicas envolveram credenciais comprometidas e que o elemento humano esteve presente em 60% dos incidentes.

Sónia Casaca, Country Manager da Zscaler Portugal, identifica o mesmo problema. “Em Portugal, ainda vemos muitas organizações a comunicar o início da jornada como se já representasse o destino. Mas o verdadeiro teste do Zero Trust não é ter um projeto lançado, é conse-



- David Silva, CyberX -

guir reduzir a superfície de ataque e eliminar a confiança excessiva na rede”, afirma.

Para David Grave, Cyber Security Senior Director na Claranet Portugal, há três padrões que se repetem especificamente no mercado português: o Active Directory nunca limpo, com grupos herdados de reorganizações antigas; o acesso permanente de terceiros; e a confusão estrutural

“

A MAIORIA
IMPLEMENTOU
AUTENTICAÇÃO
FORTE À ENTRADA
E CONTINUA A NÃO
TER AUTORIZAÇÃO
GRANULAR LÁ
DENTRO”

entre comprar e desenhar. “Zero Trust não é uma decisão de arquitetura sobre quem confia em quem, para fazer o quê e durante quanto tempo. Não vem dentro de uma licença”, defende.

Carlos Caldeira, CISO & Cybersecurity Manager da Oramix, descreve um caso concreto. “Tivemos um caso recente num cliente do setor financeiro em que a política de acesso estava bem desenhada no papel, mas há mais de dois anos que ninguém revia as permissões das contas de serviço. Uma delas, de um projeto já terminado, ainda tinha acesso de administrador a três sistemas”, exemplifica.

O diagnóstico da CyberInspect mostra o problema. “Avaliámos mais de 50 mil empresas portuguesas, sempre com informação observável do exterior, sem qualquer acesso à infraestrutura interna”, explica Valter Silva Rodrigues, Responsável da CyberInspect. “Três em cada quatro organizações apresentam risco médio ou elevado, e quase um

terço desse grupo está no patamar mais crítico. Setores com mais intensidade digital, como programação informática e retalho tecnológico, têm em média uma pior postura do que setores tradicionais porque mais presença digital significa mais superfície exposta”.

Gonçalo Martins, Partner, Cyber & Telecom Networks da Deloitte, enquadra o estado da maturidade. “Muitas organizações encontram-se numa fase centrada na proteção da identidade, o que constitui um passo relevante. No entanto, a concretização de uma arquitetura Zero Trust exige estender os princípios de confiança mínima e verificação contínua a toda a infraestrutura, aplicações, dados e processos de negócio”.

A IDENTIDADE JÁ NÃO CHEGA

Se o primeiro problema é a implementação incompleta, o segundo é que as regras do jogo estão a



- Sónia Casaca, Zscaler Portugal -

mudar. A Inteligência Artificial (IA) está a transformar a economia dos ataques de identidade de formas que tornam os controlos clássicos de *Multifactor Authentication* (MFA) cada vez mais insuficientes.

Pedro Soares, National Security Officer da Microsoft Portugal, cita o “*Microsoft Digital Defense Report 2025*” e menciona que “o phishing gerado por IA é três vezes mais eficaz do que as

“EM PORTUGAL, AINDA VEMOS MUITAS ORGANIZAÇÕES A COMUNICAR O INÍCIO DA JORNADA COMO SE JÁ REPRESENTASSE O DESTINO. MAS O VERDADEIRO TESTE DO ZERO TRUST NÃO É TER UM PROJETO LANÇADO”

campanhas tradicionais. Técnicas de *Adversary-in-the-Middle* podem intercetar sessões e contornar algumas formas de MFA, confirmando que autenticar uma vez não é suficiente”.

David Grave faz uma distinção que muitas organizações ainda não interiorizaram, a de que “o MFA clássico foi desenhado para resolver o roubo de *password*, e com sucesso. Só que o ataque dominante já não é quebrar o segundo fator, é roubar a sessão depois de ele acontecer. Phishing em *Adversary-in-the-Middle*, *infostealers*, *tokens* exfiltrados de máquinas comprometidas: o atacante não precisa de enganar o MFA, basta esperar que o utilizador legítimo o faça por ele”.

Carlos Caldeira descreve um caso em que “houve uma tentativa de fraude de *deepfake* de voz do CFO num cliente nosso, detetada e bloqueada só porque o pedido de transferência saía do procedimento habitual. A deteção comportamental

“

ZERO TRUST NÃO É UMA DECISÃO DE ARQUITETURA SOBRE QUEM CONFIA EM QUEM, PARA FAZER O QUÊ E DURANTE QUANTO TEMPO. NÃO VEM DENTRO DE UMA LICENÇA”



- David Grave, Claranet Portugal -

ajuda a apanhar contas já comprometidas, mas só quando alguém age sobre os alertas – e isso nem sempre acontece”.

O consenso entre fabricantes e integradores aponta na mesma direção: autenticação resistente a phishing (como FIDO2, *passkeys* e certificados), avaliação contínua da sessão e extensão do modelo às identidades não-humanas. Contas de serviço, chaves de API e agentes de IA já são mais do que os utilizadores humanos na maioria



- Carlos Caldeira, Oramix -

dos ambientes, mas raramente têm controlos equivalentes. “A identidade só continua a ser um pilar se deixarmos de a tratar como um evento e passarmos a tratá-la como um estado contínuo e criptograficamente verificável”, sintetiza David Silva.

Rui Duro, Country Manager para Portugal da Check Point Software, descreve a evolução necessária da tomada de decisão e defende que “uma decisão de acesso deve combinar a identidade declarada como o estado do dispositivo, a loca-

lização, o comportamento da sessão, a sensibilidade do recurso, o nível de privilégio pedido e o risco da operação”.

PLATAFORMA ÚNICA OU BEST-OF-BREED

A Forrester, na edição Q3 2025 do Wave para plataformas de Zero Trust, explica que nenhum dos *vendors* avaliados deve ser visto como “*one-stop shop*”. A recomendação da consultora é uma abordagem híbrida, ou seja, plataformas para os controlos centrais e soluções especializadas para necessidade específicas, que evite complexidade excessiva ou *lock-in* a um fabricante.

Sónia Casaca explica que “este dilema está muitas vezes mal colocado, porque tende a ser tratado como uma escolha ideológica, quando na verdade é uma decisão operacional. Quando uma organização vive com demasiadas consolas, políticas fragmentadas, integrações frágeis e equipas sobrecarregadas, a consolidação pode criar valor real”.

“TIVEMOS UM CASO RECENTE NUM CLIENTE DO SETOR FINANCEIRO EM QUE A POLÍTICA DE ACESSO ESTAVA BEM DESENHADA NO PAPEL, MAS HÁ MAIS DE DOIS ANOS QUE NINGUÉM REVIA AS PERMISSÕES DAS CONTAS DE SERVIÇO”

Ricardo Marciano, Business Development Manager SASE da Fortinet, aponta o fator que, na sua opinião, é decisão: “não é o número de fabricantes envolvidos. É a capacidade de integrar informação, automatizar processos e aplicar políticas consistentes. Quando isso não acontece, a complexidade torna-se rapidamente um problema de segurança”.

A CyberX propõe uma regra prática. “Consolidar o plano de controlo, diversificar o plano de verificação. Quem impõe o controlo nunca deve ser a única entidade a confirmar que o controlo funciona”, defende David Silva, que também aponta um risco que é silencioso na maioria das organizações: “quando se aceita um módulo medíocre porque ‘já vem incluído’”.

Elizabeth Alves, Sales Manager da Exclusive Networks Portugal, identifica onde o canal de parceiros falha neste processo. “Um dos *gaps* que



- Valter Silva Rodrigues, CyberInspect -

identificamos está na componente de consultoria associada à componente tecnológica. Na maioria das organizações, estas duas vertentes são lideradas por equipas distintas e, quando se tenta implementar a tecnologia com base nos *outputs* da equipa de consultoria, encontramos *gaps* extensos: falta a ‘cola’”.

“

SETORES COM MAIS INTENSIDADE DIGITAL, COMO PROGRAMAÇÃO INFORMÁTICA E RETALHO TECNOLÓGICO, TÊM EM MÉDIA UMA PIOR POSTURA DO QUE SETORES TRADICIONAIS PORQUE MAIS PRESENÇA DIGITAL SIGNIFICA MAIS SUPERFÍCIE EXPOSTA”

“

A CONCRETIZAÇÃO DE UMA ARQUITETURA ZERO TRUST EXIGE ESTENDER OS PRINCÍPIOS DE CONFIANÇA MÍNIMA E VERIFICAÇÃO CONTÍNUA A TODA A INFRAESTRUTURA, APLICAÇÕES, DADOS E PROCESSOS DE NEGÓCIO”



- Gonçalo Martins, Deloitte -

O PROBLEMA DO LEGACY

Uma fatia significativa das infraestruturas críticas portuguesas corre em sistemas que nunca serão *compliant* com Zero Trust. O consenso sobre a estratégia é uniforme: não se transforma o sistema *legacy*; transforma-se tudo à volta dele.

“A pergunta certa não é como tornar confiável o AS/400 ou o autómato industrial; é como fazer

com que a confiança da organização deixe de depender deles”, explica David Silva. “Ninguém – utilizador, aplicação ou administrador – tem acesso direto àquele sistema. Tudo passa por um intermediário que sabe quem está a pedir, autoriza pedido a pedido e regista o que se passou”. Carlos Caldeira descreve um caso real, “num cliente de uma *utility*, onde um SCADA antigo não podia ser tocado sem parar a operação. A solução foi isolar a rede de controlo por trás de um *broker* de acesso dedicado, com sessão gravada e aprovação individual por ligação”.

A Deloitte formalizou esta abordagem sob o conceito de “*Compensating Zero Trust*”. Gonçalo Martins explica que, “em vez de procurar modernizar de imediato todas as aplicações, procura-se integrá-las numa arquitetura de segurança mais ampla, onde permanecem operacionalmente relevantes, mas devidamente isoladas e controladas”.

David Grave levanta a dimensão de *governance*

que normalmente não é abordada. “Cada exceção tem de ter um responsável, com o risco formalmente aceite ao nível certo e com um prazo. Uma exceção sem dono e sem prazo não é uma exceção, é uma decisão permanente que ninguém quis assumir”.

O CUSTO POR ORÇAMENTAR

O argumento financeiro para Zero Trust existe; o “*IBM Cost of a Data Breach Report 2025*” quantifica que as organizações com arquitetura Zero Trust madura poupam, em média, 1,76 milhões de dólares por incidente face a organizações sem este modelo. No entanto, o *Total Cost of Ownership* (TCO) real da implementação é raramente discutido.

“A licença é a parte barata”, refere David Grave, que acrescenta que “o custo que praticamente todas as organizações subestimam é a higiene

prévia – o inventário de utilizadores, grupos, contas de serviço e fluxos entre aplicações. Esse trabalho é ingrato, invisível e consome a maior fatia do esforço. Poucas o orçamentam e é ele que faz derrapar os prazos”.

Carlos Caldeira acrescenta que o custo de operação contínua. “Num projeto recente, a equipa tinha orçamentado um analista a meio-tempo; ao fim de três meses eram precisos dois a tempo inteiro”, diz.



- Pedro Soares, Microsoft Portugal -

“O PHISHING GERADO POR IA É TRÊS VEZES MAIS EFICAZ DO QUE AS CAMPANHAS TRADICIONAIS”

Rui Duro alerta para um custo que normalmente não aparece nas análises. “A proliferação de ferramentas cria redundância e complexidade, com muitas organizações a utilizarem mais de dez soluções distintas apenas para segurança da cloud”, explica. “Uma análise séria do TCO deve incluir custos diretos, como licenças e subscrições, custos indiretos, como integração, monitorização e formação, e custos de oportunidade, como inter-



- Rui Duro, Check Point Software -

rupções, perda de confiança ou atraso no lançamento de serviços”.

Para David Silva, o argumento certo junto da administração é fácil de encontrar. “Hoje, um incidente numa rede sem separação interna custa a empresa inteira; com separação, custa um departamento. Essa diferença é dinheiro que as seguradoras já calculam porque condicionam prémios a controlos concretos. Zero Trust não se vende como segurança. Vende-se como perda esperada mais baixa e seguro mais barato”.

“UMA DECISÃO DE ACESSO DEVE COMBINAR A IDENTIDADE DECLARADA COMO O ESTADO DO DISPOSITIVO, A LOCALIZAÇÃO, O COMPORTAMENTO DA SESSÃO, A SENSIBILIDADE DO RECURSO, O NÍVEL DE PRIVILÉGIO PEDIDO E O RISCO DA OPERAÇÃO”

NIS2 E DORA COMO ACELERADOR?

A transposição da NIS2 para a lei portuguesa (em vigor desde abril de 2026) e o DORA (aplicável ao setor financeiro desde janeiro de 2025) estão a criar uma procura real. De acordo com a Mordor Intelligence, o mercado de cibersegurança em Portugal atingiu os 1,2 mil milhões de dólares em



- Ricardo Marciano, Fortinet -

2025 e está projetado para crescer 6,7% ao ano até 2030, com o regulamento regulatório como motor principal. No entanto, a pressão regulatória traz um risco específico: transformar Zero Trust em mais uma caixa para marcar num relatório de conformidade.

Pedro Soares cita uma investigação da IDC e da Microsoft e indica que “77% das organizações

“

SE RETIRARMOS
A AUDITORIA
DA EQUAÇÃO,
CONTINUARÍAMOS
A INVESTIR NESTA
MEDIDA DE
SEGURANÇA? SE A
RESPOSTA FOR NÃO,
PROVAVELMENTE
ESTAMOS PERANTE
UM EXERCÍCIO DE
CONFORMIDADE”

na EMEA não está totalmente preparada para a NIS2. **Estar conforme no papel e operar com resiliência continuam a ser realidades distintas”.**

Valter Silva Rodrigues defende que **“a forma mais fácil de distinguir”** as organizações **“é olhar para o que acontece a um relatório de teste depois de ser entregue. Numa organização que testa para perceber o risco real, o relatório gera um plano de correção com responsáveis e prazos. Numa organização que testa para ter documentação, o relatório fica arquivado e os mesmos problemas aparecem no teste seguinte”.**

Elizabeth Alves confirma que “as organizações estão a contratar serviços de consultoria para alinhar processos e controlos às exigências normativas. Entre as tecnologias mais procuradas estão as soluções de controlo de identidade, como MFA e PAM [*Privileged Access Management*], e as soluções de sensibilização dos colaboradores”.

David Silva sintetiza que “quem constrói para o

auditor passa na auditoria e falha no incidente. Quem constrói para o atacante passa nos dois”. Por sua vez, Ricardo Marciano propõe um teste simples para qualquer organização. “Se retirarmos a auditoria da equação, continuaríamos a investir nesta medida de segurança? Se a resposta for não, provavelmente estamos perante um exercício de conformidade”, refere.

Para David Grave, o que distingue os programas que funcionam dos que falham raramente é técnico. “Basta perguntar quais são os ativos verdadeiramente críticos, quem lhes acede hoje e quem tem mandato para cortar esse acesso às três da manhã sem pedir autorização a ninguém. Se a resposta sai com clareza, o programa vai funcionar, mesmo que a maturidade técnica seja baixa”, defende.

Já Gonçalo Martins acrescenta o sinal de falha mais comum: as exceções. “Quando as exceções se tornam a norma e são sistematicamente aprovadas sob o argumento da urgência do negócio,



- Elizabeth Alves, Exclusive Networks Portugal -

a eficácia do programa degrada-se progressivamente”, indica.

Sónia Casaca encerra com a perspetiva que situa o momento atual. “O Zero Trust deixou de ser uma ambição teórica e passou a ser uma exigência prática de resiliência. A questão já não é se as organizações vão fazer esta transição, mas quão rapidamente conseguem fazê-la de forma operacional, sustentável e alinhada com o negócio”, conclui. ■

“UM DOS GAPS QUE IDENTIFICAMOS ESTÁ NA COMPONENTE DE CONSULTORIA ASSOCIADA À COMPONENTE TECNOLÓGICA. NA MAIORIA DAS ORGANIZAÇÕES, ESTAS DUAS VERTENTES SÃO LIDERADAS POR EQUIPAS DISTINTAS”



CIBERSEGURANÇA INDUSTRIAL: QUATRO TENSÕES QUE VÃO DEFINIR A PROTEÇÃO DA OPERAÇÃO ATÉ 2027

A rede da fábrica está cada vez mais próxima da rede do escritório, e é essa aproximação, mais do que qualquer ameaça nova, que está a redesenhar a segurança industrial.

SETE EM CADA DEZ organizações industriais reportaram entre um e nove ataques no último ano, mais do que os 47% do ano anterior, segundo o relatório State of Operational Technology and Cybersecurity 2026, da Fortinet, feito junto de mais de 700 profissionais de OT.

SABER O QUE ESTÁ LIGADO

O primeiro obstáculo é conhecer o que está ligado. Em ambientes OT, o inventário raramente é simples, coexistem equipamentos de gerações diferentes, sensores IoT e sistemas de controlo nunca pensados para estar permanentemente ligados em rede. A visibilidade é o fator mais crítico para a resiliência em cibersegurança, pois não se pode proteger o que não consegue ver. Segmentar sem parar a produção.



O segundo é segmentar sem criar um problema novo. Separar redes por lógica puramente tecnológica, sem perceber que equipamentos comunicam entre si e quais as ligações indispensáveis ao processo, arrisca bloquear uma comunicação legítima e parar a produção. O desafio não é segmentar mais, é segmentar com conhecimento do processo que se está a proteger.

NEM TODA A ANOMALIA É UM INCIDENTE

O terceiro é distinguir uma anomalia de uma alteração planeada. Em TI, um comportamento fora do padrão costuma ser um sinal relativamente claro. Em OT, pode ser apenas uma mudança normal no processo, e alertas a mais podem ter, na prática, o mesmo efeito de não ter alertas suficientemente úteis: dificultam a identificação do que merece intervenção. O problema, mostra um relatório de 2025 do SANS Institute sobre ICS/OT, já não está em detetar depressa, quase metade dos incidentes já são detetados em menos de 24 horas, mas em restabelecer a operação com segurança a seguir, quando quase 20% dos casos ainda demoram mais de um mês a normalizar.

QUEM ENTRA, E COM QUE ACESSO

O quarto desafio é controlar quem entra na infraestrutura. Fornecedores, equipas de manutenção, integradores e outros terceiros precisam frequentemente de acesso remoto a ambientes OT, mas cada ligação adicional cria

uma nova possibilidade de exposição. Saber quem acede, a quê, durante quanto tempo e com que privilégios tornou-se uma questão de segurança, não apenas de gestão operacional.

Esta preocupação estende-se à própria cadeia de fornecimento. Uma organização pode ter os seus sistemas protegidos e continuar exposta através de um fornecedor ou equipamento comprometido. A NIS2 veio reforçar precisamente esta responsabilidade, incluindo a segurança da cadeia de fornecimento entre as medidas de gestão de risco que as organizações abrangidas devem considerar.

O desafio é garantir que estes acessos são necessários, controlados e monitorizados, sem transformar a segurança num obstáculo à manutenção ou continuidade da operação.

Há ainda uma dificuldade que distingue particularmente os ambientes OT: nem todas as vulnerabilidades podem ser resolvidas com um patch.

Equipamentos antigos, sistemas que suportam processos críticos ou tecnologias que dependem de versões específicas de software podem não poder ser atualizados ou retirados de operação sem impacto. Nesses casos, reduzir o risco pode exigir outras medidas, como segmentação, controlo de acessos, monitorização e deteção.

O objetivo não é eliminar todos os riscos de uma vez, mas reduzir a exposição dos ativos que não podem ser alterados sem pôr em causa a operação.

“É ESTA CAPACIDADE DE MONTAR A COMBINAÇÃO CERTA PARA CADA OPERAÇÃO, E NÃO VENDER UM CATÁLOGO FECHADO, QUE TORNA A EXCLUSIVE NETWORKS UM PARCEIRO RELEVANTE PARA O CANAL NESTE MERCADO”

UMA MATURIDADE MAIS HONESTA

Estes quatro pontos pesam mais à luz da maturidade real do setor. Com critérios de avaliação mais rigorosos, a fatia de equipas de OT que se considerava no nível mais avançado caiu de 49% para 17% num só ano, ainda segundo a Fortinet.

Não é que a segurança tenha piorado, é que o setor está finalmente a ver a distância entre o que pensava ter e o que tem. A responsabilidade pela segurança OT também está em movimento, 60% das organizações atribuem-na hoje ao CISO, uma ligeira descida face aos 69% de 2025, ainda que 81% já planeiem formalizar essa transição no próximo ano. E isto com a pressão regulatória a apertar, quase nove em cada dez responsáveis de OT esperam nova regulação em cinco anos ou menos.

A RESPOSTA NÃO ESTÁ NUMA MARCA SÓ

Nenhum destes desafios se resolve com uma ferramenta isolada, e raramente com um único fabricante. Uma organização pode precisar de ganhar visibilidade sobre os ativos e as comunicações, reforçar a segmentação da rede, controlar políticas de acesso e, ao mesmo tempo, detetar comportamentos anómalos sem interferir com processos críticos.

Estas necessidades podem ser respondidas por diferentes tecnologias e fabricantes, mas o desafio está em fazê-las funcionar de forma coerente. É aqui que uma abordagem multivendor ganha relevância: em vez de partir de uma solução pré-definida, começa pelo ambiente que existe, pelos riscos identificados e pelas exigências da operação.

É também neste ponto que a Exclusive Networks pode acrescentar valor ao canal. Com um ecossistema que inclui especialistas em diferentes áreas da segurança OT e de rede, como a Nozomi Networks, a Fortinet e a Palo Alto Networks, a empresa pode ajudar os parceiros a avaliar diferentes opções e a construir, para cada cliente, uma combinação de tecnologias adequada ao seu contexto.

“É esta capacidade de montar a combinação certa para cada operação, e não vender um catálogo fechado, que torna a Exclusive Networks um parceiro relevante para o canal neste mercado. Não há duas infraestruturas OT iguais e, por isso, não faz sentido partir de uma solução pré-definida. O papel do canal é perceber o ambiente do cliente, identificar onde estão os riscos e construir a arquitetura que melhor responde a essas necessidades”, afirma Elizabeth Alves, Sales Manager, Exclusive Networks Portugal. ■



POR TIAGO ANDRADE,
Senior Client Executive, NetApp Portugal

BEST OF BREED: CIBER-RESILIÊNCIA E ZERO TRUST NA ERA DA COMPLEXIDADE DIGITAL

A transformação digital trouxe ganhos extraordinários para organizações públicas e privadas.

NO ENTANTO, também ampliou significativamente a superfície de ataque, multiplicando os riscos associados ao ransomware, à exfiltração de dados, à interrupção de serviços críticos e às ameaças à cadeia de abastecimento digital. Neste contexto, os conceitos de **Zero Trust** e **Ciber-Resiliência** deixaram de ser temas exclusivos das equipas de segurança para se tornarem prioridades estratégicas ao nível dos conselhos de administração.

A realidade é simples: nenhuma organização pode assumir que um utilizador, dispositivo, aplicação ou infraestrutura é confiável por defeito. O

modelo Zero Trust baseia-se precisamente neste princípio: verificar continuamente, conceder apenas os privilégios estritamente necessários e monitorizar permanentemente o comportamento dos ativos digitais.

Contudo, a implementação prática do **Zero Trust** continua a ser um desafio. Muitas iniciativas limitam-se à autenticação reforçada, sem abordar aspetos fundamentais como a proteção dos dados, a segmentação granular, a deteção de anomalias ou a capacidade de recuperação após um ataque bem-sucedido. É aqui que a **Ciber-Resiliência** assume um papel decisivo.



- Tiago Andrade -
Senior Client Executive, NetApp Portugal

A verdadeira medida da maturidade de uma organização não está apenas na sua capacidade de prevenir ataques, mas sobretudo na rapidez e eficácia com que consegue recuperar operações, proteger informação crítica e garantir continuidade de negócio.

É precisamente neste ponto que a **NetApp** oferece uma proposta diferenciadora no mercado.

Ao contrário de soluções focadas exclusivamente na camada de segurança, a NetApp integra a proteção dos dados diretamente na infraestrutura onde estes residem. Através da plataforma **ONTAP**, as organizações beneficiam de funcionalidades únicas de resiliência, incluindo snapshots imutáveis, proteção contra ransomware, deteção comportamental baseada em inteligência artificial, recuperação rápida de dados e mecanismos avançados de isolamento cibernético.

O conceito de **Cyber Vault**, desenvolvido pela NetApp, permite criar cofres digitais isolados e imutáveis, protegendo os ativos mais críticos contra ataques sofisticados, incluindo ransom-

ware de última geração. Esta abordagem está alinhada com as recomendações da NIST, da União Europeia e de diversos organismos nacionais de cibersegurança.

Paralelamente, a NetApp suporta estratégias Zero Trust através da integração com os principais fornecedores de identidade, segurança e cloud, permitindo uma abordagem aberta e verdadeiramente **Best of Breed**. Em vez de forçar dependências proprietárias, a plataforma integra-se com ecossistemas como Microsoft, VMware, Cisco, Palo Alto Networks, CrowdStrike, Splunk, Rubrik, Google Cloud, AWS e Microsoft Azure, permitindo às organizações escolher as melhores tecnologias para cada domínio de segurança.

Esta capacidade de integração é particularmente relevante para entidades públicas e infraestruturas críticas, onde coexistem ambientes legados, regulamentação exigente e necessidades rigorosas de soberania dos dados. A flexibilidade de uma arquitetura aberta reduz o risco de dependência

tecnológica, evita bloqueios futuros e acelera a adoção de novos controlos de segurança.

Num cenário marcado pela NIS2, pelo Cyber Resilience Act, pelo DORA e por requisitos crescentes de conformidade, a proteção dos dados tornou-se um elemento central da postura de segurança. Afinal, quando todas as outras camadas falham, são os dados que permanecem como o ativo mais valioso da organização.

A estratégia vencedora não passa por adquirir mais ferramentas isoladas. Passa por construir uma arquitetura integrada, resiliente e centrada nos dados. Uma arquitetura onde prevenção, deteção, resposta e recuperação trabalham de forma coordenada.

O futuro da segurança não pertence às organizações que acreditam que nunca serão atacadas. Pertence às que assumem que podem ser atacadas a qualquer momento e que, ainda assim, conseguem continuar a operar.

É essa a essência da Ciber-Resiliência. E é exatamente aí que a NetApp faz a diferença. ■

QUEM COMPROU ZERO TRUST, COMPROU AUTENTICAÇÃO

Quase todos os fornecedores de segurança falam hoje sobre Zero Trust, mas são poucas as organizações que de facto o adquiriram e o implementaram. O que a maioria comprou, foi um segundo fator de autenticação com um nome mais caro.

NUNCA CONFIAR, VERIFICAR SEMPRE

Há uma pergunta que faço de forma recorrente às equipas de gestão de topo: se a vossa arquitetura fosse testada amanhã, o que resistiria? Durante anos, bastou estar ligado à rede da organização para se ser considerado de confiança. Essa lógica acabou com a chegada do trabalho híbrido, da cloud e com o acesso a partir de qualquer dispositivo. O perímetro, tal como o conhecíamos, simplesmente deixou de existir. O Zero Trust responde com um princípio incómodo: nunca confiar implicitamente,

validar sempre. A identidade passa a ser o novo perímetro, quer isso agrade ou não aos donos das redes.

Na prática, isto obriga a responder em contínuo a um conjunto de perguntas: quem pede o acesso, a partir de onde, para quê e com que risco. Nenhuma resposta isolada chega, pois é a combinação que decide se o acesso é concedido, limitado ou negado. É também aqui que a maioria das organizações fica. O multifator e a autenticação adaptativa são o degrau mais fácil de vender e de comprar, por



- Carlos Caldeira -
Cybersecurity Manager & CISO, Oramix

isso aparecem em quase todas as apresentações comerciais como “Zero Trust completo”. Não são. São o primeiro degrau de um percurso bem mais longo.

PRIVILÉGIOS E DADOS: ONDE A IMPLEMENTAÇÃO FALHA

O princípio de least privilege devia garantir que cada utilizador tem apenas o acesso estritamente necessário, mas, na prática, é aqui que mais organizações falham. Numa auditoria que conduzimos recentemente, uma organização apresentava o seu programa de Zero Trust. Quando questionámos quem tinha acesso ao ERP financeiro, a resposta foi “praticamente todo o departamento, por hábito”.

Do ponto de vista do risco, o que interessa não é o número de controlos implementados, mas o que fica exposto quando um deles falha. Sem saber onde estão os dados críticos, quem lhes acede e como são usados, qualquer política de acesso é um

exercício de fé. Classificar e monitorizar os dados ao longo do seu ciclo de vida não é um extra, é o que torna tudo o resto possível.

A estes desafios juntam-se ainda sistemas legacy que nunca vão cumprir os requisitos, acessos mantidos por conveniência histórica e contas de serviço com privilégios permanentes que ninguém revê. Pela nossa experiência são a regra, não a exceção.

A NIS2 acelerou a procura por Zero Trust nos últimos dois anos; no entanto, resolveu poucos dos desafios estruturais. Quando um incidente acontece, é a segmentação e a redução de privilégios que limitam os danos.

VALIDAÇÃO, SEGMENTAÇÃO, VISIBILIDADE: O TESTE REAL

As avaliações de maturidade que a Oramix realiza no terreno mostram, ano após ano, um gap entre o que se apresenta como Zero Trust e o que resiste a um incidente real.

A validação acontece só no login ou ao longo de toda a sessão? A segmentação chega aos sistemas legacy ou só ao que é fácil e novo? Há visibilidade real sobre os dados mais críticos ou apenas um inventário de aplicações desatualizado?

São as respostas a estas questões, e não a lista de funcionalidades de um fabricante, que separam arquiteturas eficientes das que funcionam apenas como uma fachada. A monitorização contínua de comportamentos anómalos, como uma transferência de dados fora de padrão, é o que deteta uma ameaça real, interna ou externa. Já não interessa quem está dentro ou fora da rede, mas quem tenta aceder a quê, em que contexto e com que risco.

Bem feito, o Zero Trust liberta a organização para adotar cloud, trabalho híbrido e inteligência artificial com mais confiança. Mas essa maturidade não vem numa solução de MFA. Exige que a gestão de topo invista na segmentação, na visibilidade dos dados e na validação contínua, não apenas na porta de entrada, onde quase todos ficaram. ■



ZSCALER POSICIONA O ZERO TRUST COMO RESPOSTA DECISIVA PARA PROTEGER A IA NAS EMPRESAS

À medida que a inteligência artificial ganha escala nas operações, a segurança deixa de poder funcionar em atraso. Para a Zscaler, proteger agentes de IA, aplicações e dados exige uma abordagem Zero Trust capaz de reduzir risco, fechar superfície de ataque e impor visibilidade, controlo e governação de forma contínua.

À MEDIDA QUE A ADOÇÃO de copilotos, chatbots, modelos de IA e agentes autónomos acelera, cresce também a distância entre a velocidade da inovação e a capacidade real de proteção. Cada nova integração com dados empresariais, aplicações críticas e fluxos de trabalho sensíveis acrescenta identidades, permissões e pontos de acesso que os modelos tradicionais de segurança não foram desenhados para controlar com a granularidade exigida. O risco passa, assim, a estar na forma como esta tecnologia se liga ao negócio.

UMA NOVA SUPERFÍCIE DE ATAQUE EXIGE OUTRA DISCIPLINA

Os sinais de alerta descritos nos documentos de base são claros: as ferramentas corporativas de IA podem ficar expostas a potenciais ataques externos, enquanto a maturidade média em segurança específica para IA permanece reduzida. Em muitos casos, interfaces de IA, servidores MCP ou APIs de inferência são integrados sem mecanismos robustos de autenticação, controlo de acesso e governação. O resultado é uma super-

fície de ataque em expansão, onde a falta de visibilidade compromete o controlo sobre dados e aplicações.

AGENTES DE IA SEM CONTROLO NÃO SÃO AUTOMAÇÃO SEGURA

A pressão aumenta com a chamada IA agentic. Ao contrário dos assistentes tradicionais, os agentes autónomos não se limitam a responder: podem executar tarefas, consultar múltiplas fontes de dados, interagir com várias aplicações e tomar

decisões para cumprir objetivos. Esta autonomia reforça o valor da IA para o negócio, mas altera profundamente o problema de IT security. Já não basta proteger utilizadores humanos com identidades previsíveis; é necessário aplicar políticas consistentes a entidades dinâmicas, rápidas e altamente conectadas, que operam à velocidade da máquina e podem ampliar risco em segundos se não existirem limites claros.

ZERO TRUST É A BASE PARA ESCALAR IA COM CONFIANÇA

É aqui que a Zscaler assume um posicionamento forte e diferenciador. O modelo Zero Trust parte do princípio de que nenhum utilizador, dispositivo, aplicação ou agente deve ser confiado por defeito. Cada pedido de acesso tem de ser validado continuamente em função da identidade, do contexto, do nível de risco e do recurso solicitado. Aplicado à IA, este princípio permite reduzir privilégios, reforçar controlo, proteger dados e aplicações e impor governação contínua sobre interações que, sem este modelo, tenderiam a escapar à supervisão das equipas de segurança.

É nesta lógica que a evolução da plataforma Zscaler Zero Trust Exchange é apresentada como resposta concreta para este novo cenário. Entre as capacidades referidas nos textos de base estão o AI Broker, para proteger comunicações entre agentes e gerir permissões a partir de um registo centralizado; o Endpoint AI Security, focado na deteção de ameaças relacionadas com IA em dispositivos, navegadores, extensões e ferramentas locais; e o AI Access Graph, concebido para dar rastreabilidade às interações entre utilizadores, agentes, aplicações e dados. Somam-se ainda funções de descoberta de ativos de IA, controlos sobre aplicações de IA generativa e mecanismos de proteção dirigidos a infraestruturas e aplicações baseadas em inteligência artificial.

UM PASSO A FRENTE DO RISCO

Para as organizações, a mensagem é objetiva: adotar IA sem uma arquitetura de segurança alinhada com esta nova realidade é aumentar exposição sem garantir controlo. À medida que a IA se torna parte central das operações, a segurança tem de ser condição de escala e não camada

reativa. Nesse contexto, a Zscaler reforça o Zero Trust como resposta crítica para reduzir risco, melhorar visibilidade e sustentar uma adoção de IA mais segura, governada e preparada para proteger o negócio.

ACERCA DA ZSCALER

A Zscaler (NASDAQ:ZS) acelera a transformação digital para que os clientes possam ser mais ágeis, eficientes, resilientes e seguros. A plataforma Zscaler Zero Trust Exchange™ protege milhares de clientes contra ciberataques e perda de dados através da ligação segura de utilizadores, dispositivos e aplicações em qualquer localização. Distribuída em mais de 150 centros de dados em todo o mundo, a Zero Trust Exchange™ baseada em SASE é a maior plataforma de segurança na nuvem em linha do mundo. Mais informação em www.zscaler.com. ■

Informação de contacto:

Sónia Casaca | Country Lead | Zscaler, Inc.

Mobile +351 918 603 412

Email scasaca@zscaler.com

SOFIA TENREIRO, PRESIDENTE EXECUTIVA DA SIEMENS PORTUGAL

**“PRECISAMOS DE
GARANTIR QUE A BASE
ESTÁ SÓLIDA PARA A IA
PODER RETIRAR VALOR DO
MUNDO REAL”**



Para Sofia Tenreiro, Presidente Executiva da Siemens Portugal, o desafio da inteligência artificial já não assenta apenas na tecnologia, mas envolve também dados, processos e pessoas que são determinantes para transformar o potencial em impacto.

HENRIQUE CARREIRO E MARTA QUARESMA FERREIRA

A SOFIA ESTÁ HOJE À FRENTE DA SIEMENS PORTUGAL, MAS O SEU PERCURSO FALA POR SI: CARGOS DE LIDERANÇA EM SETORES MUITO DIFERENTES – TECNOLOGIA, ENERGIA, INDÚSTRIA – E EM ORGANIZAÇÕES COM ORIGENS MUITO VARIADAS, DESDE LOGO NORTE-AMERICANAS E EUROPEIAS. COM UMA EXPERIÊNCIA TÃO DIVERSIFICADA, QUAIS SÃO AS PRINCIPAIS DIFERENÇAS E ADAPTAÇÕES QUE SÃO NECESSÁRIAS NUMA LIDERANÇA?

O nosso estilo de liderança não só tem de se adaptar ao sítio onde estamos, à organização, à equipa, mas também ao desafio que temos em mãos e à fase que estamos a nível mundial.

Os líderes têm de ser muito camaleónicos. Há uma parte nossa de valores e de crenças que não muda, mas em termos de formato e até de energia tem

de mudar. Dependendo da maturidade das organizações, do grau de transformação que é pedido, do que está a acontecer à nossa volta, tudo impacta a forma como temos de liderar.

Primeiro procuro absorver a cultura da organização, sendo que é tudo rápido e quase imediato. Podemos influenciar a cultura da organização local, mas não vamos mudar os grandes princípios e valores da multinacional.

Temos também de perceber muito bem qual é a estratégia e o desafio que nos é pedido para depois adaptarmos o nosso estilo e a nossa estratégia também a esse momento.

Uma das grandes características que os líderes têm de ter é, por um lado, esta capacidade de adaptação muito rápida porque, muitas vezes, também temos de nos adaptar dentro da mesma organização e no mesmo contexto; por outro, temos de ter uma grande velocidade em tudo o que fazemos porque

o mundo está a mudar muito rapidamente. O cliente final é sempre muito mais rápido em termos de necessidades, de conhecimento, muitas vezes até dos nossos próprios produtos e dos produtos dos nossos concorrentes.

Se os líderes tiverem inerentes características como a mudança, a transformação, a reinvenção e a velocidade, será mais fácil adaptarem-se quando abraçam um novo desafio.

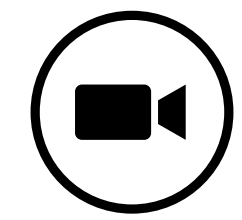
SE HÁ UNS ANOS FALÁVAMOS DA SIEMENS COMO UMA EMPRESA ESSENCIALMENTE INDUSTRIAL, HOJE TERMOS COMO *DIGITAL TWINS* E INTELIGÊNCIA ARTIFICIAL (IA) TAMBÉM FAZEM TAMBÉM PARTE DO ADN DA ORGANIZAÇÃO. COMO É QUE DEFINE ATUALMENTE A SIEMENS? QUAIS AS MUDANÇAS ESTRATÉGICAS QUE OCORRERAM NA ORGANIZAÇÃO COM A CHEGADA DA SOFIA, EM 2025?

A Siemens é um caso de sucesso porque é uma empresa tecnológica com 180 anos na Europa. Tem acompanhado as grandes revoluções que têm marcado a história da Humanidade – ajudámos na eletrificação, em toda a parte da industrialização – e agora estamos a ajudar na nova revolução da inteligência artificial.

A nossa estratégia é ligar o mundo real e digital, e acreditamos muito que é esta ligação que maximiza o valor dos clientes e das empresas. Estamos todos, a nível profissional e pessoal, a caminhar para o digital, mas a verdade é que o mundo real acontece, desde logo nas máquinas industriais, nas camas dos hospitais, nos transportes e na logística. Quando pensamos de forma consciente e criamos estas ligações entre o mundo digital e real, estamos a colocar a tecnologia ao serviço do real.

“

A JUNÇÃO DOS MOTORES MAIS AVANÇADOS DE IA COM O CONHECIMENTO E DADOS QUE TEMOS PERMITE-NOS AJUDAR OS CLIENTES NA APLICABILIDADE DA INTELIGÊNCIA ARTIFICIAL AO CORE DAS SUAS OPERAÇÕES”



PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM



Acreditamos que, ao focarmo-nos nesta componente tecnológica, alicerçada no que chamamos de inteligência artificial industrial, estamos a ser diferenciadores ao colocar a inteligência artificial em cima deste contexto que é único, com estes 180 anos de conhecimento e todos os dados que temos connosco. A junção dos motores mais avançados de IA com o conhecimento e dados que temos permite-nos ajudar os clientes na aplicabilidade da inteligência artificial ao *core* das suas operações.

A Siemens Portugal tem trabalhado para ajudar os clientes a adotarem esta inteligência artificial industrial, alicerçada em temas de simulação como os *digital twins*, que nos permite não só conceber, como também implementar, operacionalizar e manter fábricas, hospitais e sistemas de distribuição da água.

Também estamos a trabalhar com equipas internacionais através do nosso Portugal Tech Hub, onde temos cerca de 1.600 pessoas a produzir soluções digitais para o mundo, muitas que incorporamos na nossa forma de trabalhar, mas outras que são projetos em que estão a trabalhar com clientes a nível mundial.

Temos uma equipa muito grande de serviços partilhados em Portugal, também alicerçada em soluções digitais, a servir 60 Siemens a nível mundial desde Portugal, para termos estes ganhos de eficiência e conseguirmos uma maior homogeneização na forma como trabalhamos a nível global.

ONDE É QUE A SIEMENS SE ESTÁ A POSICIONAR NESTE ENABLEMENT DA IA PARA OS PRÓXIMOS ANOS?

A verdade é que os EUA, e especialmente a China, estão muito mais à frente do que a Europa – partiram claramente mais rapidamente e estão a conseguir ter um efeito de escala que nós não estamos a conseguir. Falamos de uma



SOMOS O SEXTO MAIOR PAÍS EM TERMOS DE ÁREA TECNOLÓGICA [NA SIEMENS], O QUE NÃO É MUITO COMUM DADA A DIMENSÃO DO PAÍS. A RAZÃO PARA ESTA RELEVÂNCIA A NÍVEL MUNDIAL ASSENTA NUMA ESTRATÉGIA DE VÁRIOS ANOS DE ATRAIR HEADQUARTERS PARA PORTUGAL, ALAVANCANDO ESSENCIALMENTE NO TALENTO”

Europa, mas nós não somos uma Europa, somos um conjunto de países. O continente europeu está um bocadinho atrás, mas acho que as pessoas têm a perceção de que está mais atrás do que está. Sem dúvida de que, como um todo, não está tão avançado, mas temos muita inovação a acontecer e acredito que temos um potencial enorme porque somos um continente industrial.

Portanto, se conseguirmos modernizar a nossa indústria rapidamente, se calhar conseguimos dar um salto quântico de aproximação aos outros dois países, que é o que queremos todos.

A REINDUSTRIALIZAÇÃO E A SOBERANIA TECNOLÓGICA MARCAM CADA VEZ MAIS A AGENDA ATUAL DO BLOCO EUROPEU. COMO É QUE PORTUGAL PODE BENEFICIAR DESTA MUDANÇA?

Portugal tem condições incríveis, não só de qualidade de vida, mas também por estarmos numa ponta da Europa, mais próximos de África, Estados Unidos e da América Latina, e por sermos um país pacificador.

Temos, acima de tudo, um talento incrível e reconhecido. Hoje, somos 4.300 pessoas no Grupo Siemens em Portugal. Somos o sexto maior país em termos de área tecnológica [na Siemens], o que não é muito comum dada a dimensão do país. A razão para esta relevância a nível mundial assenta numa estratégia de vários anos de atrair *headquarters* para Portugal, alavancando essencialmente no talento. Temos muitas empresas que exportam, a nível global, mas deveríamos conseguir ter esta atração de talento e de investimento para criarmos mais centros de competência de valor acrescentado no país.

As grandes tecnológicas têm grandes consultoras e grandes centros na Índia, mas acreditamos que Portugal é muito complementar. Somos muito bons a executar também, mas temos uma grande criatividade e capacidade de inovação, uma grande proatividade e, portanto, não só executamos o que nos é pedido, mas acrescentamos esta vontade de impactar e liderar os projetos. Não somos tão seguidores; lideramos.

E devemos pensar como é que conseguimos atrair mais este tipo de investimento para Portugal, sabendo que temos um ecossistema de *startups* incrível,

muitos empreendedores com reconhecimento a nível mundial e empresas de génese portuguesa que cresceram cá dentro e hoje são multinacionais. Temos empresas muito credíveis em Portugal.

No entanto, precisamos, por um lado, de ter mais exemplos de atração e de captação de investimento para Portugal; por outro lado, devíamos pensar em áreas como inteligência artificial, cibersegurança, dados, analítica, e como é que conseguimos utilizar o talento que temos para nos assumirmos como *hub* para o mundo inteiro.

Um terceiro ponto tem a ver com PME. Sabemos que têm menos recursos e, muitas vezes, menos capacidade de investimento, mas a transformação tecnológica pode começar a ser feita sem grande investimento porque qualquer pessoa pode experimentar e perceber qual o valor que consegue tirar da IA. No fundo, é capacitar as equipas das empresas, olhar para os processos, reinventá-los, olhar para os dados e limpar os mesmos.

Quando conseguirmos ter estas três *foundations*, já estamos a acrescentar valor à empresa e a permitir que possa dar depois outros saltos em termos de investimentos de IA. Tem de haver uma adoção muito mais rápida por parte das PME e, para isso, temos de partilhar mais conhecimento, dar mais confiança. Não é uma revolução que só está ao alcance de grandes empresas com um grande investimento; está ao alcance de todos e deveríamos estar a tirar partido e a criar impacto da sua utilização.



PARA QUEM TEM UMA VISÃO TRANSVERSAL DE MERCADOS E DE UM CONJUNTO GRANDE DE EMPRESAS, O QUE É QUE FALTA PARA, DE FACTO, ATINGIREM A TAL VELOCIDADE QUE REFERIA ANTERIORMENTE? ESTAMOS A FALAR DE TRANSFORMAÇÃO TECNOLÓGICA, MAS HÁ ALGO MAIS QUE TEM DE SER TRANSFORMADO?

A transformação tecnológica tem de existir, mas essa está ao alcance de todos; acho que a maior transformação é de *mindset*, e por vários motivos.

Para já, é uma questão de confiança de que estes sistemas vêm para ajudar e acho que ainda há, por falta de conhecimento, muitos líderes de PME com alguma desconfiança sobre qual é o real valor que estas ferramentas podem trazer à sua própria empresa e se vão ajudar mais do que trazer risco.

Depois há o tema de *mindset*. Há muitas pessoas e empresas que olham para trás e pensam ‘eu sempre tive sucesso sem inteligência artificial, porque é que eu tenho de investir tempo ou dinheiro com esta ferramenta se eu nunca precisei dela?’ Mais uma vez, **é preciso muito conhecimento, é preciso experimentar e partilhar casos de sucesso que estão a ser feitos noutras empresas porque esta transformação é muito invisível.**

Depois há um terceiro ponto que está também a impedir, e que tem a ver com as *foundations* que referi, sobre algumas pessoas dizerem que a IA ainda não está a criar impacto e se calhar é uma

“

A TRANSFORMAÇÃO
TECNOLÓGICA
TEM DE EXISTIR,
MAS ESSA ESTÁ
AO ALCANCE DE
TODOS; ACHO
QUE A MAIOR
TRANSFORMAÇÃO É
DE MINDSET”

bolha: precisamos de garantir que a base está sólida para a inteligência artificial poder retirar valor do mundo real. Temos de garantir que há uma estratégia forte de dados, que estão bem identificados e categorizados, bem estruturados e acessíveis, para que quando a inteligência artificial trabalhar em cima dos dados, o *output* seja bom.

Um segundo ponto tem a ver com os processos que existem hoje nas empresas e que sempre existiram. **Nunca houve urgência de os repensar, muitas vezes nem estão documentados. Temos de ter coragem de pensar que se construíssemos hoje a nossa própria empresa do zero, havia muitas coisas que não faríamos ou faríamos de forma diferente.**

Se tivermos processos complexos, muitas vezes nem conseguimos aplicar a inteligência artificial porque a complexidade é tão grande que não vamos conseguir ter impacto.

E o terceiro ponto, o mais importante, são as pessoas e o *mindset*. Temos de conseguir ajudar as nossas equipas para que ninguém fique para trás e para que as pessoas percebam qual o verdadeiro valor que podem tirar e o que é que podem fazer com a IA. É algo que tem de vir de cima, das chefias. No fundo, as empresas portuguesas têm de trabalhar primeiro nestes três pilares – processos, dados e pessoas –, e depois pedirem ajuda a empresas tecnológicas.

QUAL O TIPO DE PERFIL PROFISSIONAL QUE A SIEMENS PROCURA PARA OS PRÓXIMOS ANOS?

Recrutamos com base nas atitudes, no potencial, nas *skills* da pessoa, mais do que no histórico. Temos pessoas com as mais variadas experiências, também porque o nosso portfólio e atuação são muito variados. Apostamos muito na formação, por isso criámos em Portugal as academias Siemens, focadas em tecnologias específicas.

O espírito colaborativo nunca foi tão importante. Não só cada pessoa tem de trabalhar em ecossistema, mas as próprias empresas têm de trabalhar com os seus clientes, com a academia, com as próprias entidades governamentais. Nunca foi tão importante termos esta co-criação e aproveitarmos as mais-valias e as capacidades de cada uma das organizações – também é assim com o talento.



Na Siemens Portugal temos cerca de 600 estrangeiros, mais de 70 nacionalidades e, portanto, acreditamos também nesta riqueza, de ter pessoas de diferentes *backgrounds*, de todos os géneros e de diferentes nacionalidades.

QUAIS SERÃO OS PRINCIPAIS SETORES DE DESENVOLVIMENTO DA ECONOMIA PORTUGUESA NOS PRÓXIMOS DOIS, TRÊS ANOS? E NO CASO DA SIEMENS PORTUGAL?

Os dois estão ligados. Se pensarmos, as grandes atuações que temos como Siemens Portugal são na eletrificação, e temos inclusive uma fábrica em Corroios de *superchargers* e trabalhamos também com os grandes e pequenos



TEMOS TUDO PARA SER UM PAÍS COM CRESCIMENTO INCRÍVEL. ÀS VEZES PRECISAMOS DE UM POUCO MAIS DE AJUDA, NÃO SÓ NA DESBUROCRATIZAÇÃO, NA RAPIDEZ DE PROCESSOS, LICENCIAMENTO, MAS TAMBÉM MAIS CORAGEM”

clientes para os ajudar a fazer a eletrificação, para garantir uma melhor gestão das redes elétricas, muito mais eficiente e resiliente, também com cada vez mais incorporação de energias renováveis.

Trabalhamos na automação, ao ajudarmos as empresas a serem muito mais automatizadas, e também na transformação digital, desde a cibersegurança à inteligência artificial, trabalhamos com tudo. Um exemplo cada vez mais premente é como é que nós ajudamos os edifícios a serem não só inteligentes, mas autónomos e a gerirem-se a si próprios.

Portanto, trabalhamos estas três áreas que são as grandes áreas de investimento das empresas. Os verticais e as áreas de foco do país serão sempre as nossas porque as empresas acabam por nos pedir ajuda.

O OT, por exemplo, foi um bocadinho mais descurado e agora percebe-se que é muito importante porque representa muitas fragilidades para as empresas porque está todo interligado.

Em termos de verticais, temos o tema da energia, que tem vindo a ser muito importante e no qual vamos continuar a ser um *player* muito relevante; todo

o tema da indústria e da reindustrialização de Portugal que também tem de acontecer; setores como a defesa são muito importantes, não só pela nossa posição geográfica – todo o palco geopolítico –, mas também porque temos esta indústria muito forte.

Não posso deixar de referir a questão dos data centers e das *gigafactories*, onde nós estamos muito presentes e acreditamos que Portugal também tem aqui um papel muito relevante na Europa, por todos os motivos e mais alguns – renováveis, acesso à energia, cabos submarinos –, com variáveis que nos tornam únicos e onde a Siemens tem um portfólio muito abrangente.

Temos tudo para ser um país com crescimento incrível. Às vezes precisamos de um pouco mais de ajuda, não só na desburocratização, na rapidez de processos, licenciamento, mas também mais coragem no sentido de não acharmos que somos pequeninos. Temos de pensar “nós somos muito grandes” porque quando olhamos para o mundo, a verdade é que nós podemos ser muito, muito grandes. ■



“O CIO SERÁ UM AGENTE DE TRANSFORMAÇÃO”

Rui Oliveira, CIO da Salsa Jeans, explica como dados, cloud e IA estão a transformar o negócio e o próprio papel da liderança de IT.

MARTA QUARESMA FERREIRA

PARA UMA EMPRESA como a Salsa Jeans, estar na moda não é ‘apenas’ uma questão de produto; passa também pela evolução do papel da tecnologia e da transformação digital, com o propósito de responder às necessidades do presente e do futuro do negócio.

“Se anteriormente a área de IT era muitas vezes encarada como uma função de suporte operacional, hoje está claramente posicionada como um parceiro estratégico do negócio”, justifica Rui Oliveira, CIO da Salsa Jeans.

A marca portuguesa especializada em denim alcançou 200 milhões de euros em vendas globais em 2025, um crescimento superior a 11% face a 2024. O responsável tem acompanhado uma evolução tecnológica marcada, sobretudo, pela crescente adoção de cloud, pela democratização da análise de dados, pela integração de ecossistemas digitais mais complexos e, mais recentemente, pela aceleração proporcionada pela Inteligência Artificial (IA).

No retalho, os utilizadores passaram também a exigir “experiências digitais mais simples, intuitivas e personalizadas”, enquanto a velocidade se tornou um “fator crítico” para a gestão.

Neste contexto, o papel do CIO evoluiu, considera Rui Oliveira, “de gestor de infraestrutura para líder de transformação”, com responsabilidades que cruzam “tecnologia, negócio, pessoas, cultura e inovação”.

INOVAÇÃO ORIENTADA PARA O NEGÓCIO

Na perspetiva do especialista, a inovação já não pode ser vista como um “objetivo isolado”, mas sim como um “instrumento para resolver problemas concretos”.

Desta forma, o foco passa por “equilibrar inovação e sustentabilidade”, com a identificação de tendências que serão, efetivamente, capazes de gerar

valor para o negócio, garantindo, simultaneamente, escalabilidade, segurança e retorno do investimento.

“A estratégia tecnológica da Salsa Jeans está fortemente alinhada com os objetivos de crescimento, eficiência e diferenciação da marca”, explica Rui Oliveira, que traça o perfil de uma organização “cada vez mais orientada por dados, digitalmente integrada e capaz de responder rapidamente às necessidades de um mercado global”.

CLOUD, DADOS E IA ACELERAM A TRANSFORMAÇÃO

A par dos projetos de modernização aplicacional, da evolução das capacidades analíticas e do reforço da integração entre plataformas e canais, a transformação tecnológica da empresa tem-se traduzido em investimento na simplificação da experiência digital dos colaboradores, com ferramentas mais intuitivas e de colaboração.



- Rui Oliveira -
CIO, Salsa Jeans

A IA generativa representa igualmente “uma das áreas com maior potencial transformador”, frisa o CIO, uma vez que permite acelerar tarefas de análise, apoiar na tomada de decisão e aumentar a produtividade.

No caso da cloud, “continua a desempenhar um papel fundamental”, com ganhos de flexibilidade, escalabilidade e agilidade. “Paralelamente, a aposta em capacidades avançadas de análise de dados tem

“

UMA
TRANSFORMAÇÃO
BEM-SUCEDIDA
DEPENDE DE UMA
VISÃO CLARA,
PATROCINADA PELA
LIDERANÇA DE TOPO
E COMPREENDIDA
POR TODA A
ORGANIZAÇÃO”



permitido melhorar a previsão, identificar tendências, compreender melhor os comportamentos dos clientes e tomar decisões mais informadas em toda a cadeia de valor”, afirma o CIO.

A cibersegurança é outro dos pilares incorporados na estratégia tecnológica da Salsa Jeans, que segue uma abordagem *security by design*, com requisitos de segurança a serem considerados desde o início dos projetos.

Apesar do investimento em “proteção tecnológica, monitorização, gestão de identidades, controlo de acessos e reforço das capacidades de deteção e resposta”, Rui Oliveira sublinha que “a tecnologia, por si só, não é suficiente”, principalmente porque “as pessoas continuam a ser um elemento crítico da segurança”. O caminho passa, por isso, pela sensibilização e pela formação regular dos colaboradores.

Neste âmbito, o CIO defende que o principal fator de sucesso da transformação não está na tecnologia, mas sim pelas pessoas. “Uma transformação bem-sucedida depende de uma visão clara, patrocinada pela liderança de topo e compreendida por toda a organização”, garante.

Para isso, a Salsa Jeans tem apostado na capacitação das equipas e no desenvolvimento contínuo de competências técnicas e comportamentais, procurando “desenvolver profissionais capazes de compreender o negócio, identificar oportunidades e contribuir para a criação de valor”.

O DESAFIO, PARA ALÉM DA TECNOLOGIA

No processo de transformação digital, Rui Oliveira considera que o maior desafio está em “transformar, simultaneamente, processos, cultura e formas de trabalho num contexto de mudança permanente”.

Perante este cenário complexo, o responsável considera necessário “encontrar o equilíbrio entre inovação e execução” e explorar novas oportunidades tecnológicas, entre elas a IA: “será, certamente, a tecnologia com maior impacto transversal ao longo da próxima década”, a par da análise avançada de dados, da computação cloud e da automação inteligente.

No setor da moda e do retalho, em particular, as “tecnologias associadas à previsão da procura, otimização da cadeia de abastecimento, personalização da experiência do consumidor e sustentabilidade” vão assumir um “papel cada vez mais relevante”.

Quando combinadas com uma “forte orientação para o cliente”, estas capacidades tecnológicas podem, de acordo com o CIO, contribuir para que as organizações estejam mais bem posicionadas para competir.



UM PAPEL CADA VEZ MAIS PRÓXIMO DO NEGÓCIO

Para Rui Oliveira, o papel do CIO do futuro será cada vez mais híbrido. Para lá de uma “sólida compreensão tecnológica”, o fator diferenciador reside na “capacidade de ligar tecnologia, estratégia e negócio”. “Será um líder responsável por identificar oportunidades, impulsionar a inovação, promover a transformação organizacional e criar valor através da tecnologia”, antevê.

Com a integração da tecnologia na organização, Rui Oliveira acredita que as diferenças entre estratégia de negócio e estratégia tecnológica vão “desaparecer”.

Nesse cenário, o CIO será, sobretudo, “um agente de transformação, um facilitador da inovação e um parceiro fundamental na construção do futuro da empresa”. ■

SAMSUNG GALAXY Z FOLD8 ULTRA: O DOBRÁVEL QUE MERECE ESTAR NA SECRETÁRIA DE UM EXECUTIVO?



Sete gerações depois do primeiro Galaxy Fold, a Samsung lançou o dobrável que, finalmente, faz esquecer que é um dobrável.

HÁ SETE ANOS que a Samsung tenta convencer o mercado de que um smartphone que se dobra ao meio é uma proposta de valor para os utilizadores. Durante a maior parte desse tempo, a resistência era legítima; ecrãs frágeis, vincos que perturbavam a utilização, autonomia comprometida e um preço que tornava o argumento difícil de sustentar perante qualquer comité de aprovação de despesas. O Galaxy Z Fold 8 Ultra não resolve todos esses problemas, mas resolve os suficientes para que a conversa mude de tom.

Este é o primeiro ano em que a Samsung divide a gama Fold em dois dispositivos distintos. O Fold8 base aposta num formato mais curto e largo, pensado para consumo de conteúdos. O

Fold8 Ultra mantém a estrutura vertical que veio do Fold7 (ecrã exterior de 6,5 polegadas, ecrã interior de oito) e é sobre ele que importa falar se o critério de avaliação for produtividade real.

O QUE MUDOU E O QUE FICOU IGUAL

Afinal, quais são as mudanças da versão anterior para a nova. A resposta não está no design, até porque, no exterior, é praticamente indistinguível do Fold7. O mudou está dentro e, em alguns casos, de forma significativa.

A bateria passou de 4.400mAh para 5.000mAh através de uma célula de silicone-carbono que permite maior capacidade sem aumentar o volume do dispositivo. O resultado prático é uma auto-





nomia que, em testes de vídeo contínuo, chegou às 32 horas, substancialmente acima do modelo anterior. Para quem passa o dia entre reuniões, voos e deslocações, é a diferença entre carregar o telemóvel uma vez ao dia ou andar sempre à procura de uma tomada.

O processador Snapdragon 8 Elite Gen 5 for Galaxy garante desempenho sem hesitações na alternância entre aplicações e a velocidade de carrega-

mento por cabo subiu dos 25W do Fold7 para 45W, uma melhoria prática que reduz o tempo de paragem.

O ecrã interior atingiu os três mil nits de brilho máximo e ganhou um revestimento antirreflexo que torna a leitura ao ar livre significativamente mais confortável. O vinco, aquela dobra central que sempre foi o calcanhar de Aquiles dos dobráveis, recuou visivelmente graças a uma nova camada de liga de titânio sob o ecrã.

O ARGUMENTO DA PRODUTIVIDADE

A proposta do Fold8 Ultra para um decisor é mais simples do que parece: um ecrã de oito polegadas que cabe no bolso do casaco. Aberto, permite



ter duas aplicações lado a lado com espaço útil para ambas, seja um email e um calendário, documentos e videoconferência ou um dashboard e notas. Fechado, é um smartphone com um ecrã exterior perfeitamente funcional para comunicação rápida.

A altura extra do ecrã interior face ao modelo base, onde o formato mais largo favorece o consumo de vídeo, mas comprime espaço vertical, é determinante para quem trabalha com documentos, folhas de cálculo ou qualquer interface que beneficie de scroll vertical. A Galaxy AI integrada, com tradução, resumo e sugestão de respostas, entre outros, funciona com maior utilidade num ecrã deste tamanho, onde é possível ter o conteúdo e a ferramenta visíveis em simultâneo.



O sistema de câmara mantém as três lentes traseiras que o modelo base perdeu: 200MP na câmara principal, 50MP de ultra-grande angular e 10MP com zoom ótico de três vezes. Para os executivos que fazem da câmara do smartphone um instrumento de trabalho, seja para apresentações, registos ou videoconferências, a diferença é tangível.



QUANTO CUSTA E PARA QUEM FAZ SENTIDO.

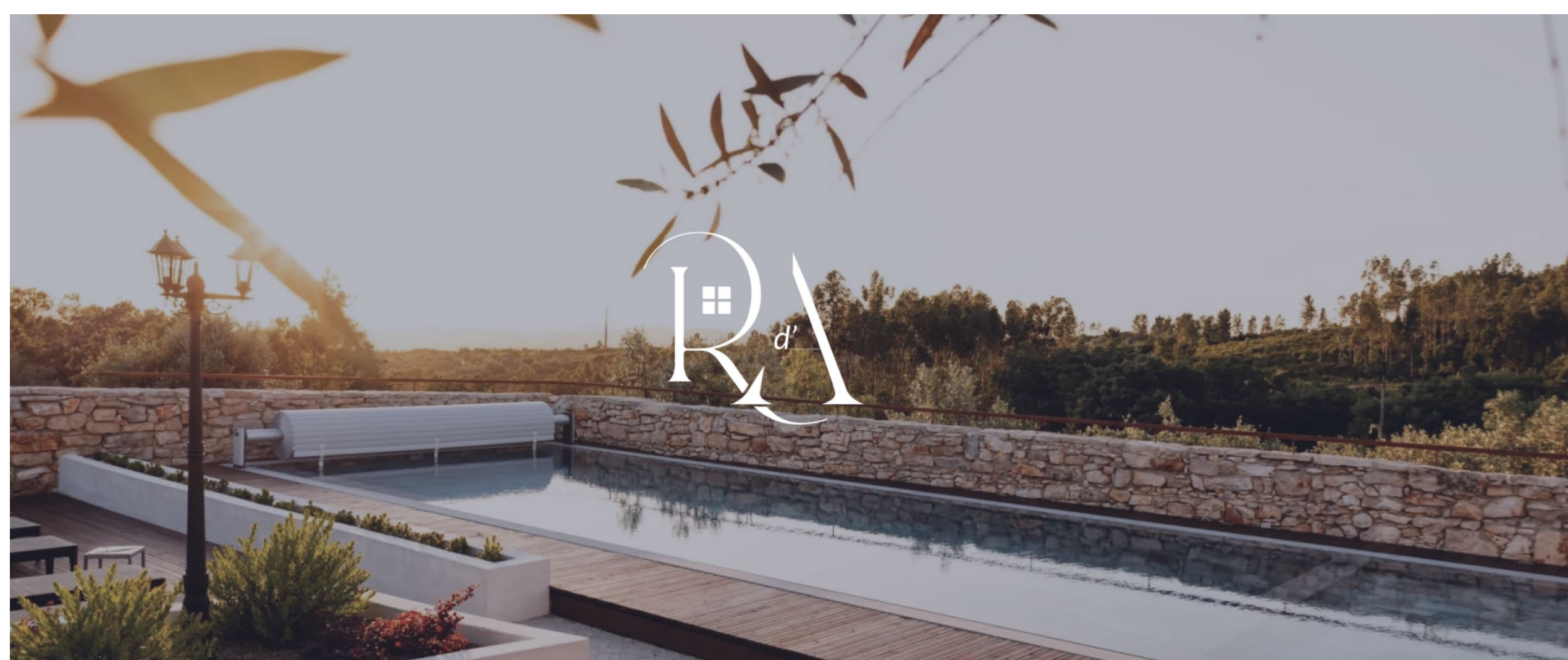
Em Portugal, o Galaxy Z Fold8 Ultra começa nos 2.269,90 euros na configuração de 256GB, chegando aos 2.869,90 euros no modelo de 1TB. É um valor alto, mais do que a maioria dos portáteis de gama média e suficiente para comprar um smartphone de topo e um tablet separados.



O argumento a favor não é, no entanto, o preço, mas a consolidação. Um único dispositivo que substitui o smartphone e o tablet, com autonomia para um dia completo de uso intensivo, desempenho sem compromissos e um ecrã que torna o trabalho em mobilidade genuinamente diferente. Para quem viaja com frequência e não quer gerir dois dispositivos, ou para quem já justificou um tablet de trabalho e procura uma alternativa que caiba no bolso, o Fold8 Ultra tem uma proposta coerente.

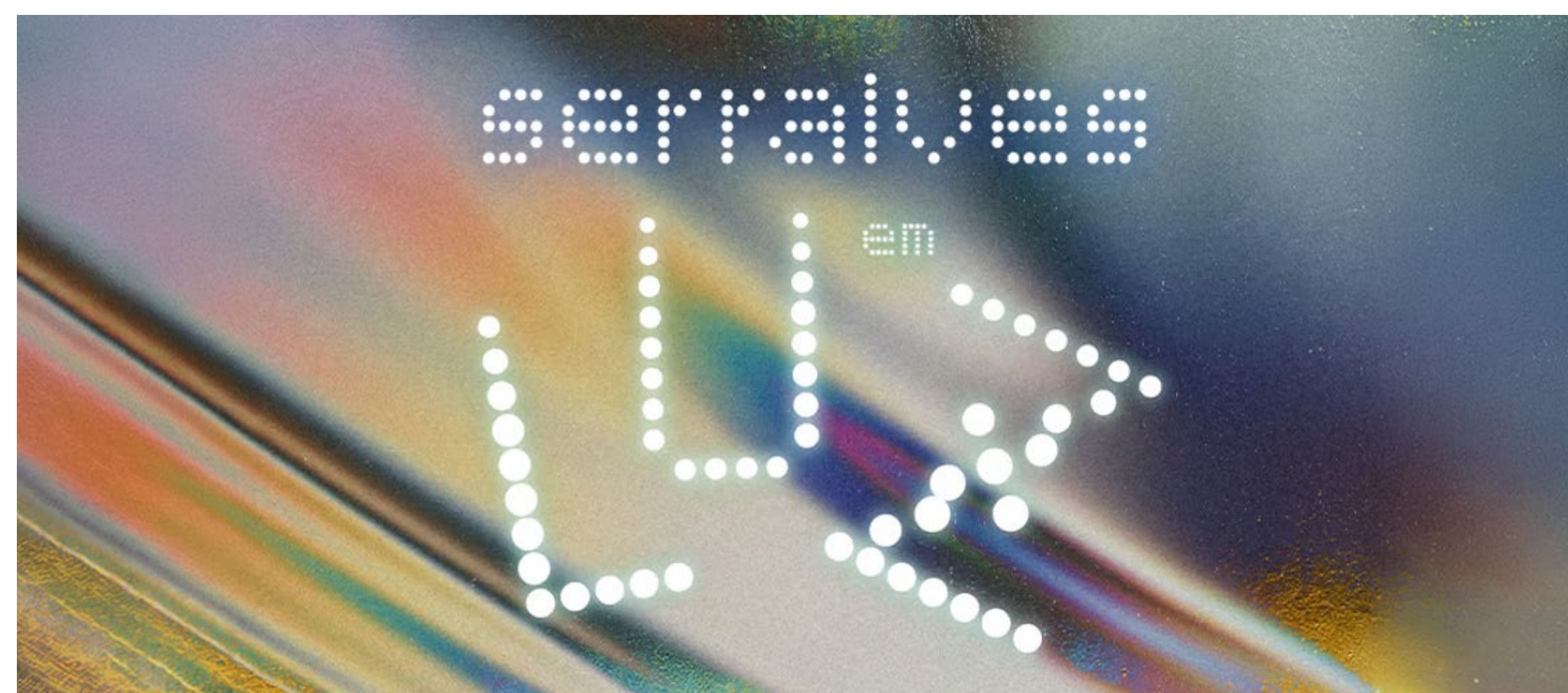
Para quem está satisfeito com o Fold7, a atualização não será, certamente, urgente. Para quem nunca experimentou um dobrável ou desistiu da categoria há uns anos, este é o momento certo para reavaliar. ■

PRÉMIO CINCO ESTRELAS REGIÕES DISTINGUEM TURISMO RURAL EM POMBAL



ORECANTOS D'ALMERINDA, no distrito de Leiria, foi consagrado vencedor do Prémio Cinco Estrelas Regiões 2026 na categoria de turismo rural, reforçando o reconhecimento da região no panorama do alojamento em meio natural. Integrado na Serra da Sicó, o projeto combina casas de pedra restauradas com conforto contemporâneo, piscinas de água salgada aquecidas e jacuzzis privados sob o céu aberto, num conceito que valoriza a tranquilidade, a privacidade e a ligação ao território. Mais do que um alojamento, propõe uma experiência de imersão na paisagem e no ritmo do interior. ■

SERRALVES À NOITE: ENTRE LUZ E NATUREZA



“SERRALVES EM LUZ” regressa ao Parque de Serralves com um percurso noturno de cerca de dois quilómetros, onde arte, natureza e tecnologia se cruzam através de 20 instalações luminosas. Sob o conceito *Light vs Darkness*, a quarta edição acrescenta uma dimensão sonora criada para os diferentes espaços, com composições de músicos como Rodrigo Leão, Noiserv e Maria João. A experiência, que pode ser visitada até 8 de novembro, prolonga-se por cerca de 90 minutos e propõe uma forma diferente de descobrir a paisagem e a arquitetura de Serralves depois do anoitecer. ■

SANTARÉM SERVE PORTUGAL À MESA



SANTARÉM é ponto de encontro dos sabores e tradições de várias regiões do país durante o Festival Nacional de Gastronomia durante os meses de outubro e novembro. À mesa juntam-se produtos, receitas e especialidades que atravessam o território português, numa celebração da diversidade gastronómica nacional e dos produtores que a mantêm viva. Entre provas, refeições e momentos dedicados à cozinha portuguesa, a Casa do Campino transforma-se numa viagem pelo país através dos sabores. ■



A IA ganhou corpo

Os robôs humanoides começam a sair dos laboratórios para entrar no mundo real. Na fábrica da BMW em Spartanburg, o Figure 03 já executa tarefas de logística que exigem percepção, destreza e coordenação de todo o corpo. O seu sistema Helix 02 permite-lhe manipular peças, ajustar a posição e adaptar os movimentos em tempo real. Depois de décadas de automação fixa, a indústria prepara-se para uma nova geração de máquinas capazes de trabalhar em ambientes concebidos para pessoas.

OBRIGADO POR TER LIDO A IT Insight

*Para continuar a receber regularmente a sua IT Insight, por favor atualize os seus dados profissionais **aqui***

*Conheça a política de privacidade da IT Insight **aqui***

IT Insight

PUBLISHER: Jorge Bento



DIRETOR: Henrique Carreiro

DIRETOR EDITORIAL: Rui Damião - rui.damiao@medianext.pt

COORDENADORA EDITORIAL: Marta Quaresma Ferreira

REDAÇÃO: Inês Garcia Martins e Flávia Gomes

GESTÃO DE PARCEIROS:

Catarina de Brito – catarina.brito@medianext.pt - (351)910 121 200

João Calvão – joao.calvao@medianext.pt- (351)910 788 413

MKT & EVENTS DIRECTOR: Rosa Bento – rosa.bento@medianext.pt

MARKETING & COMMUNICATIONS: Rita Rodrigues

ARTE E PAGINAÇÃO: Teresa Rodrigues

FOTOGRAFIA: Luciano Reis

ILUSTRAÇÕES E IMAGENS: Adobe Stock e DALL-E

DESENVOLVIMENTO WEB: Global Pixel

A REVISTA DIGITAL INTERATIVA IT INSIGHT É EDITADA POR:

MediaNext Professional Information Lda.

GERENTE: Pedro Botelho

SEDE E REDAÇÃO: Largo da Lagoa, 7c, 2795-116

Linda-a-Velha, Portugal

TEL: (+351) 214 147 300 | **FAX:** (+351) 214 147 301

PERIODICIDADE: Bimestral

IT INSIGHT está registada na Entidade Reguladora para a Comunicação Social nº12729

Consulte [aqui](#) o Estatuto Editorial

PROPRIEDADES E DIREITOS

A propriedade do título “IT Insight” é de MediaNext Lda., NIPC 510 551 866. Proprietários com mais de 5% de Capital Social: Margarida Bento e Pedro Botelho. Todos os direitos reservados. A reprodução do conteúdo (total ou parcial) sem permissão escrita do editor é proibida. O editor fará todos os esforços para que o material mantenha fidelidade ao original, não podendo ser responsabilizado por gralhas ou erros gráficos surgidos. As opiniões expressas em artigos assinados são da inteira responsabilidade dos seus autores.

A IT Insight utiliza as melhores práticas em privacidade de dados:

Editado por:

IT Insight é membro de:

