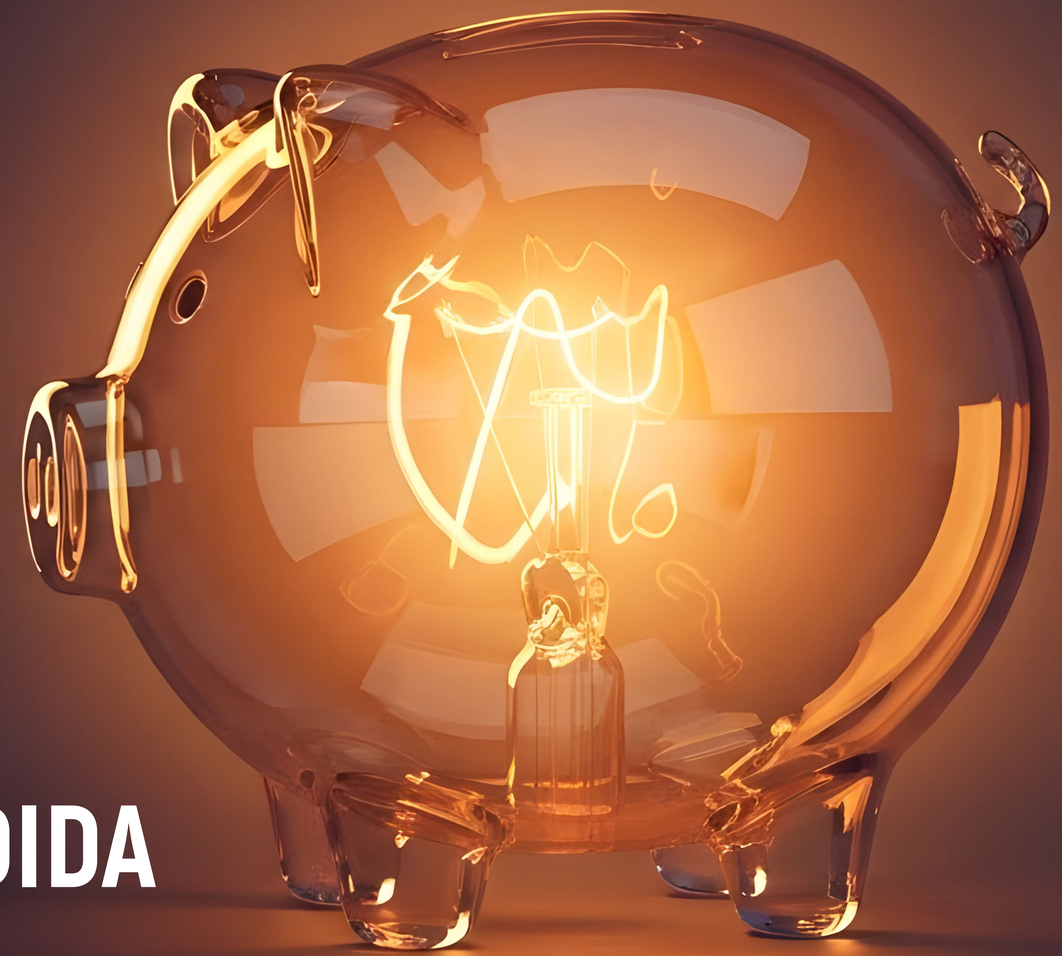
IT Insight

#64 NOVEMBRO 2026

media NEXT
STAY AHEAD • STAY RELEVANT

IT Insight talks

Business Continuity & Resilience



A FATURA (CADA VEZ MENOS) ESCONDIDA DA TRANSFORMAÇÃO DIGITAL

Empurrar limites para moldar o futuro

Cloud & Infra

Workplace

Applications

Data & AI

Cyber Security

claranet.pt

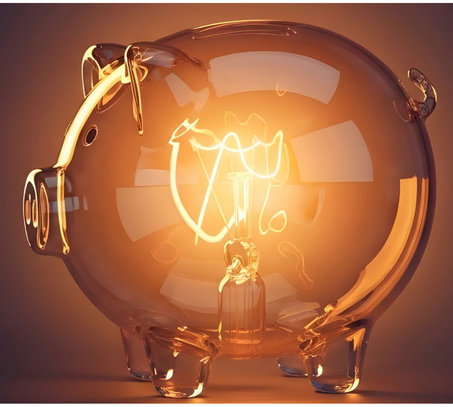
claranet®

IT·Insight

#64 NOVEMBRO 2026

IN DEEP

A FATURA (CADA VEZ MENOS) ESCONDIDA DA EFICIÊNCIA DIGITAL



d_AI_gest por Henrique Carreiro

COVERAGE
IT Security Conference 2026: Cibersegurança enfrenta uma nova era de riscos

WISHLIST
Asus Zenbook 14: quando o portátil também é um objeto de design

BEST OF BREED | CLOUD STRATEGY, STORAGE & BUSINESS CONTINUITY
Cloud, Storage e Resiliência: o desafio de modernizar sem comprometer o negócio

360º VIEW | MARCO BASTOS, CRÉDITO AGRÍCOLA
"A liderança será sempre feita através da escuta, da confiança e das pessoas"

IN DEEP | SUSTAINABILITY & IT EFFICIENCY IN THE DIGITAL ENTERPRISE
A fatura (cada vez menos) escondida da eficiência digital

IT INSIGHT TALKS | BUSINESS CONTINUITY & RESILIENCE
Continuidade de negócio: da prevenção à capacidade de resposta

FACE 2 FACE | CARLOS MIRANDA, ESTORIL-SOL
"Recuperar a confiança é um processo muito mais longo"

TRANSFORM
EAD digitaliza milhares de documentos no setor da saúde com contributo da Ricoh

IT INSIGHT TALKS



BUSINESS CONTINUITY & RESILIENCE

FACE 2 FACE



CARLOS MIRANDA, ESTORIL-SOL

Dados, IA e resiliência: o novo padrão da manutenção inteligente.

Anticipe falhas.
Proteja a sua operação.
Maximize os seus resultados.

A EcoCare transforma a manutenção numa vantagen competitiva baseada em dados.

-75%
de risco de paragens

+25%
de vida útil dos equipamentos

-40%
nos custos de manutenção

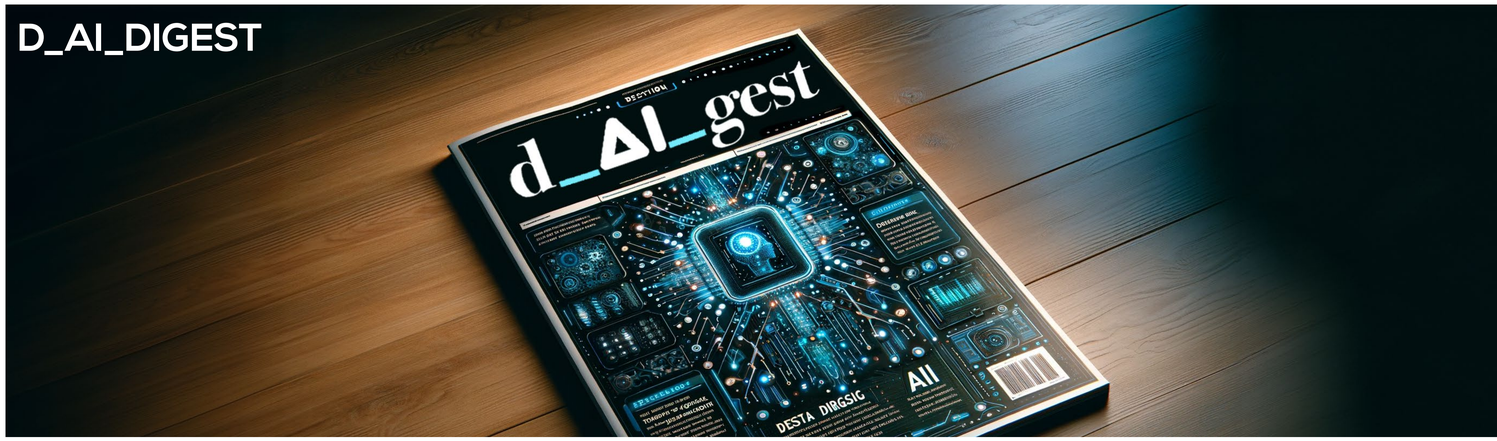
-66%
de intervenções no local

Digitalize e descubra como antecipar a próxima falha

Schneider Electric

IT·Insight

#64 NOVEMBRO **2026**



IN DEEP

SUSTAINABILITY & IT EFFICIENCY IN THE DIGITAL ENTERPRISE

claranet Sustentabilidade e Eficiência Tecnológica: uma questão de competitividade empresarial

Life Is On Schneider Electric Refrigeração líquida: a eficiência dos Data Centers para IA além do PUE

zaltor Software Distribution Sustentabilidade e eficiência de TI: duas prioridades da Zaltor para a empresa digital

BRANDED CONTENT

claranet A Inteligência Artificial acelera. As pessoas transformam

ManageEngine IT Pulse Portugal 2026 coloca a prevenção no centro da gestão de IT

Red Hat Fadiga de compliance? O problema não é a regulação

Life Is On Schneider Electric Data Centers para IA: da capacidade de refrigeração à inteligência do sistema

IT INSIGHT TALKS

BUSINESS CONTINUITY & RESILIENCE

IP Telecom Continuidade de Negócio no contexto de Soberania Digital

NetApp Continuidade de Negócio na Era Digital: Da Recuperação à Resiliência

VisionWare since 2005 A nossa segurança acaba onde começa a dependência?

zscaler Business Continuity sem fronteiras, a resiliência já não se decide apenas dentro da empresa

BEST OF BREED

CLOUD STRATEGY, STORAGE & BUSINESS CONTINUITY

NOESIS A resiliência vai muito além dos backups





Red Hat

Embed compliance into automated processes from the start

Explore more:





HENRIQUE CARREIRO

Dívida técnica: a hora do pagamento chegou

NO PASSADO dia 21 de outubro, o projeto PHP, a comunidade que mantém a linguagem usada, de acordo com o serviço de estatísticas W3Techs, em sessenta e nove por cento dos sites cuja tecnologia de servidor é identificável, publicou novas versões que eliminam duas vulnerabilidades críticas no seu motor; segundo a empresa de segurança Wiz, estas afetavam todas as versões publicadas até então ao longo da última década e permitiam, em certas configurações, executar código num servidor sem autenticação. A primeira-ministra do Japão, Sanae Takaichi, deixou no X, nesse mesmo dia, pouco antes das dez da noite em Tóquio, um invulgar "pedido urgente" às empresas nipónicas para atualizarem o PHP nessa noite ou, não o conseguindo, suspenderem temporariamente os seus sites.

Na véspera da divulgação, os códigos com que as duas falhas tinham sido registadas no catálogo internacional de vulnerabilidades (CVE) apareceram em fóruns e redes sociais, ainda sem pormenores técnicos e, nessa mesma noite, a Calif, uma das empresas que as tinham descoberto, publicou, aparentemente por engano, um vídeo em que demonstrava como as falhas podiam ser exploradas; o vídeo foi apagado, mas as cópias espalharam-se e, segundo a PHP Foundation, aceleraram o aparecimento de provas de conceito públicas. Por causa da fuga, a divulgação coordenada, prevista para dia 22, foi antecipada

em vinte e quatro horas e, na manhã de 21, a Chainguard, uma distribuidora de software já compilado, publicou as novas versões, mais de seis horas antes da hora prevista, o que, para um atacante, capaz de comparar o código novo com o anterior e chegar à falha, podia ser considerado um convite.

Não que o problema fosse novo. Em 2024, um dos programadores do *core* do PHP reparou num comportamento anómalo na forma como o PHP reagia quando um programa esgotava a memória que lhe estava atribuída, mas ninguém conseguiu demonstrar como explorá-lo, e o assunto ficou por resolver. No passado mês de agosto, a Calif, que trabalhou com um modelo da OpenAI, e uma equipa da própria OpenAI chegaram, cada uma por si, à mesma causa; a Wiz, com modelos da Google e da OpenAI, construiu ataques funcionais contra o WordPress, o Drupal e o Joomla. Foi a partir destas descobertas que o projeto preparou as versões de outubro.

O custo de passar da suspeita à demonstração mudou, e não apenas no PHP: em outubro, a Microsoft lançou *patches*, de uma só vez, para cerca de mil e quatrocentas vulnerabilidades — mais, segundo a Zero Day Initiative, do que em qualquer ano anterior, seja qual for a parte desse aumento que se fique a dever à IA. A dívida técnica acumulada em décadas de desenvolvimento de software é, há muito, tema de discussão nas conferências e nas reuniões empresariais, mas foi sendo empurrada de orçamento em orçamento, enquanto encontrar e explorar as falhas foi caro. Esse adiamento acabou: a IA trouxe a dívida a pagamento, e os juros capitalizam depressa, como mostram os ataques que a Cloudflare registou contra os seus clientes ainda antes das novas versões.

O caso de 2024 mostra onde está, de facto, o estrangulamento. Sem uma forma de exploração demonstrada, um problema identificado compete por tempo e recursos com tudo o resto que os responsáveis de um projeto têm em mãos, e raramente ganha.

A proposta de solução nipónica — desligar o que não se consegue atualizar a tempo — pressupõe que alguém saiba o que tem ligado. A percentagem de vulnerabilidades corrigidas dentro do prazo, a métrica durante muitos anos usada pelas comissões de avaliação de risco, mede, na verdade, o ritmo de quem as trata, mas diz pouco sobre o que fica, entretanto, exposto. Agora que a fatura chegou, mais útil será a lista do que fica por corrigir, ou desligado, durante quanto tempo e por decisão de quem. E essa lista deve começar pelas bibliotecas de código aberto de que cada organização depende e para cuja manutenção, muitas vezes, nunca contribuiu: é a parte da dívida que, até agora, foi paga por outros. ■

NetApp | intel | ARROW

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

INVESTIMENTO MUNDIAL EM IT DEVERÁ CRESCER 15% E ATINGIR 7,35 BILIÕES DE DÓLARES EM 2027

A Gartner prevê que a despesa mundial em tecnologias de informação ultrapasse os sete biliões de dólares pela primeira vez em 2027. A infraestrutura de IA será o principal motor de crescimento.



A despesa mundial em tecnologias de informação deverá atingir 7,35 biliões de dólares em 2027, o que representa um crescimento de 15% face a 2026, segundo a Gartner. A expansão será impulsionada sobretudo pelo investimento em infraestruturas de Inteligência Artificial (IA), plataformas de cloud e software. As previsões apontam para uma aceleração do crescimento do mercado global de IT, depois de uma subida estimada de 14,5% em 2026. O segmento de sistemas para data centers deverá registar a maior expansão, com um crescimento de 55,5% em 2027, atingindo 1,37 biliões de dólares. O investimento em servidores otimizados para IA, serviços de Infrastructure-as-a-Service e plataformas de software deverá continuar a aumentar à medida que as organizações procuram implementar a IA em maior escala. ■

PORTUGAL JUNTA-SE A 12 PAÍSES PARA SIMPLIFICAR LEGISLAÇÃO EUROPEIA

A iniciativa pretende reduzir a burocracia, eliminar obrigações duplicadas e avaliar o impacto das regras europeias na inovação e competitividade.



Portugal juntou-se a outros 12 Estados-Membros da União Europeia numa iniciativa que pretende promover uma revisão sistemática da legislação europeia, com o objetivo de reduzir os encargos administrativos, simplificar as regras existentes e reforçar a competitividade das empresas. A proposta defende uma abordagem regulatória mais orientada para a inovação, a interoperabilidade e a aplicação prática das normas.

A iniciativa, liderada pela Áustria, conta com o apoio de Portugal, Alemanha, República Checa, Dinamarca, Eslováquia, Eslovénia, Estónia, Hungria, Itália, Letónia, Lituânia e Polónia. Os 13 países subscreveram um documento informal que propõe uma revisão aprofundada do quadro legislativo europeu, avaliando quais as regras que continuam a ser necessárias, quais devem ser atualizadas e quais representam encargos desproporcionados para cidadãos e empresas. ■

NOESIS

Technology for real growth

Há **30 anos** que ajudamos organizações a utilizar a tecnologia para evoluir, crescer e explorar novas oportunidades de negócio.

Com uma equipa de mais de **1 300 profissionais e presença em 8 países**, desenvolvemos soluções que simplificam as operações do dia a dia, aumentam a eficiência e aceleram o crescimento sustentável. É assim que transformamos tecnologia em crescimento real.

Portugal | Espanha | Países Baixos
Irlanda | Reino Unido | Brasil | EUA | EAU

www.noesis-corporation.com

IT Operations & Infrastructure

Cloud & Security

Enterprise Application Integration

Application Development

Data Analytics & AI

DevOps & Automation

Quality Management

Professional Services

© Noesis. All rights reserved.

44% DOS CEO TÊM DIFICULDADES EM DEMONSTRAR RETORNO FINANCEIRO DA IA

Um estudo da Gartner revela que 44% dos CEO não conseguem demonstrar facilmente o retorno financeiro dos investimentos em inteligência artificial. Apesar disso, 75% pretendem aumentar o investimento em tecnologia.

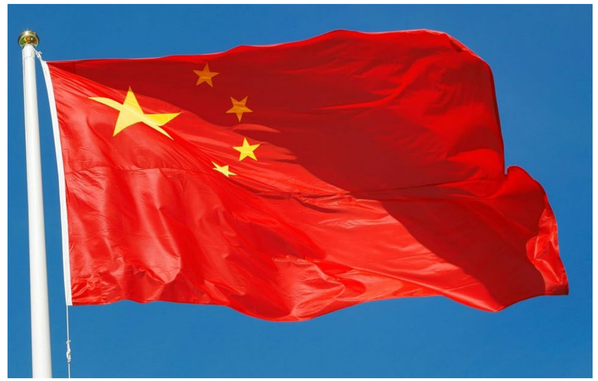


Quase metade dos CEO enfrenta dificuldades em demonstrar aos investidores e restantes partes interessadas os benefícios financeiros dos investimentos em Inteligência Artificial (IA). Segundo o estudo da Gartner, 44% dos líderes empresariais têm dificuldades em comprovar o retorno financeiro da IA, apesar de a tecnologia assumir um papel cada vez mais central nas estratégias de crescimento das organizações.

Os resultados do "*2027 Gartner CEO Survey*" mostram que estas dificuldades não estão a provocar uma redução das intenções de investimento. Pelo contrário, 75% dos inquiridos planeiam aumentar a despesa em tecnologia, enquanto 62% identificam o crescimento das receitas ou do negócio como uma das principais prioridades estratégicas. ■

CHINA PREPARA RESTRIÇÕES À EXPORTAÇÃO DE TECNOLOGIAS DE IA

Pequim quer acrescentar 40 tecnologias à lista de exportações proibidas ou sujeitas a restrições, incluindo 23 ligadas à inteligência artificial.



A China anunciou uma proposta de revisão da sua lista de tecnologias cuja exportação é proibida ou sujeita a restrições, com especial incidência na inteligência artificial, na biomedicina e na indústria fotovoltaica. A iniciativa, apresentada a 16 de outubro pelos ministérios do Comércio e da Ciência e Tecnologia, abrange 40 tecnologias e está em consulta pública até 15 de novembro de 2026.

Embora a revisão ainda não esteja concluída, as autoridades chinesas introduziram um mecanismo temporário de registo prévio para determinadas exportações tecnológicas abrangidas pela proposta. A medida aplica-se desde a publicação do anúncio e manter-se-á em vigor até à entrada em aplicação da versão revista do catálogo. ■

IP Telecom

Housing
IPT Cloud

CloudSolutions
Housing
Hosting

Nato Secret

EU Secret

Rede Nacional CSIRT

LIGAMOS NEGÓCIOS

Telecomunicações | Data Center | Cloud Computing



www.iptelecom.pt

comercial@iptelecom.pt

CIO REFORÇAM PAPEL ESTRATÉGICO, MAS ENFRENTAM DESAFIOS NA EXECUÇÃO

Estudo da Experis revela que 48% dos líderes tecnológicos consideram o alinhamento do IT com o negócio a principal responsabilidade dos CIO.



Os CIO estão a assumir um papel cada vez mais relevante na estratégia e no crescimento das organizações, mas continuam a enfrentar dificuldades para transformar os investimentos tecnológicos em resultados concretos. Segundo o estudo "*CIO 2026 Outlook*", da Experis, 48% dos líderes tecnológicos consideram que o alinhamento da estratégia do IT com os objetivos de negócio é atualmente a principal responsabilidade dos CIO, face aos 34% registados em 2025.

O relatório identifica uma evolução das prioridades da liderança de IT. A capacidade de demonstrar valor para o negócio está a ganhar importância, num contexto marcado pela adoção de inteligência artificial, modernização de sistemas antigos, riscos de cibersegurança e dificuldades na gestão da mudança. ■

EMPRESAS PORTUGUESAS PERDEM PRODUTIVIDADE COM FERRAMENTAS DESCONECTADAS

Estudo estima perdas anuais de 327 mil euros numa empresa com mil colaboradores. A fragmentação de informação e ferramentas dificulta a produtividade e a adoção de IA.

A falta de integração entre equipas, processos e ferramentas digitais está a gerar custos de produtividade nas empresas portuguesas. Segundo o estudo "*Business Facts Index 2026 – The Cost of Business Disconnection*", da Factorial, 57,3% dos líderes empresariais nacionais afirmam perder entre 20% e 30% do seu tempo à procura de informação, a reconciliar dados ou a repetir tarefas já realizadas.

A empresa estima que este tempo perdido represente um custo anual de 327.002 euros numa organização com mil colaboradores, considerando apenas o tempo dos gestores afetados. Para uma empresa com 500 trabalhadores, o custo estimado é de 163.501 euros por ano, enquanto numa organização com 250 colaboradores o valor se situa nos 81.750 euros. ■

VisionWare

since 2005

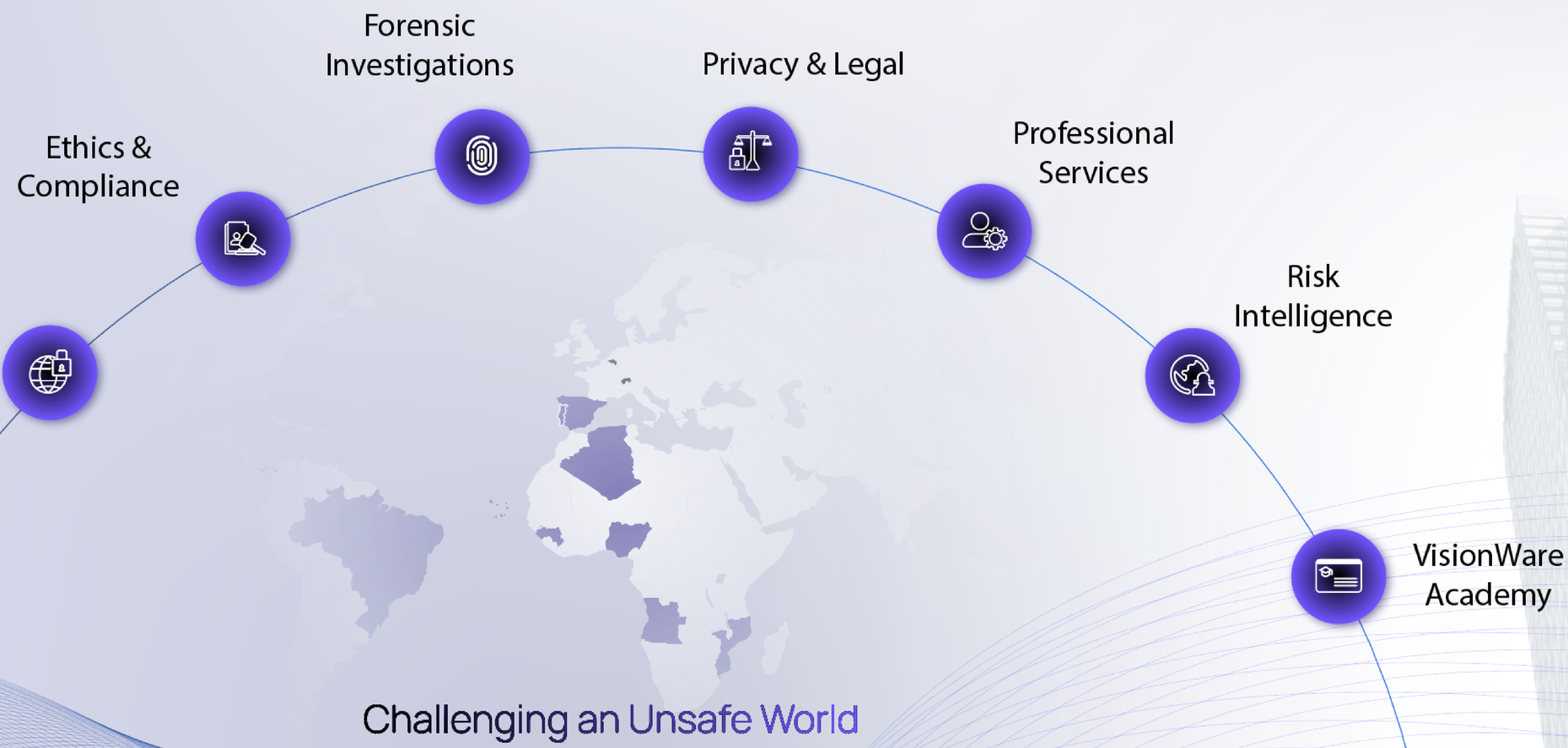
+5000 projetos desenvolvidos

+100 colaboradores

+200 clientes ativos

+10 geografias

A **missão da VisionWare** é contribuir para o Sucesso das organizações, aumentado a sua cultura e maturidade em Segurança da Informação.



Porto | Lisboa | Praia | Mindelo

geral@visionware.pt

+351 225 323 740

visionware.pt

IA REDEFINE ECONOMIA DO CONHECIMENTO E APONTA PARA AUTOMATIZAÇÃO DE 30% DAS TAREFAS ATÉ 2030

A Inteligência Artificial poderá automatizar até 30% das tarefas dos profissionais do conhecimento até 2030. Ainda assim, a falta de competências digitais ameaça limitar esta transformação.



A inteligência artificial generativa poderá automatizar até 30% das tarefas desempenhadas por profissionais do conhecimento até 2030, alterando a forma como são prestados serviços em várias áreas, segundo a Frost & Sullivan. A consultora considera que a combinação entre competências humanas, infraestruturas digitais e IA será um dos principais fatores de competitividade económica até 2035. No entanto, a escassez de profissionais qualificados e as desigualdades no acesso à tecnologia pode limitar a capacidade das organizações para aproveitar estas oportunidades. De acordo com os dados apresentados, 59% dos trabalhadores a nível mundial vão precisar de adquirir novas competências até 2030, enquanto apenas 28% da força de trabalho global possui formação superior ou competências digitais formais. ■

INFRAESTRUTURAS DE DATA CENTERS CRESCEM 27% NO SEGUNDO TRIMESTRE

O mercado mundial de infraestruturas físicas para data centers atingiu 14 mil milhões de dólares no segundo trimestre de 2026.



O mercado mundial de infraestruturas físicas para data centers cresceu 27% em termos homólogos no segundo trimestre de 2026, atingindo receitas de 14 mil milhões de dólares para os fabricantes, segundo o Dell'Oro Group.

O crescimento manteve-se acima dos 20%, impulsionado pela procura de capacidade para suportar cargas de trabalho de Inteligência Artificial (IA), que continua a superar a oferta disponível. A ligeira desaceleração face ao primeiro trimestre de 2026 resulta de uma base de comparação mais elevada e não de uma redução da procura, segundo a consultora.

O relatório introduz também uma nova segmentação dos clientes do mercado de infraestruturas físicas para data centers, dividida em cinco categorias: *hyperscalers*, outros fornecedores cloud, incluindo neoclouds, operadores de *colocation*, operadores de telecomunicações e empresas. ■

zscaler™

ZERO TRUST + AI

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

Zscaler.com



claranet®

POR CRISTINA FREIXO,
Innovation Labs Director, Claranet Portugal

A INTELIGÊNCIA ARTIFICIAL ACELERA. AS PESSOAS TRANSFORMAM

É fácil apresentar o potencial da Inteligência Artificial. Mais exigente é integrá-la numa operação real, onde existem compromissos com clientes, processos interdependentes e equipas que precisam de continuar a entregar todos os dias. É nesse contexto que uma organização testa a distância entre aquilo que a tecnologia promete e aquilo que consegue efetivamente transformar.

PARA UMA *empresa de serviços de IT*, este teste tem uma responsabilidade acrescida. A credibilidade para conduzir a transformação dos clientes também se constrói através da capacidade de transformar a própria organização. A adoção interna obriga-nos a enfrentar as mesmas perguntas que encontramos no mercado: assegurar a qualidade dos dados, integrar a *IA* nos processos, envolver as pessoas e demonstrar valor.

É necessário fazer essa jornada: criar iniciativas inovadoras, desenvolvê-las e acompanhá-las nos seus vários estados de maturidade, observar resultados e validar ambições novas. Distinguir estas dimensões é essencial para uma conversa séria sobre *IA*.

Iniciativas de automação aplicadas à operação revelam, em geral, reduções muito significativas no tempo entre a entrada de um pedido de suporte e a primeira intervenção da equipa responsável. Para o cliente, significa uma resposta mais rápida. Para a organização, demonstra que a integração de tecnologia num processo pode produzir uma melhoria mensurável.



- Cristina Freixo -
Innovation Labs Director

Mas o rigor exige que se explique o alcance desse resultado. Uma redução no tempo até à primeira intervenção não significa uma redução equivalente no tempo total de resolução, no esforço das equipas ou no custo do serviço. Cada benefício precisa da sua própria medição. A credibilidade também depende daquilo que escolhemos não extrapolar.

É a partir daqui que começa a transformação mais interessante: perceber o que podemos fazer com a capacidade que a automação possibilita libertar. Até porque permite, numa operação de serviços, tempo para as atividades mais complexas e que as pessoas têm tendência a adiar, quando a urgência consome os recursos disponíveis. Esta é a verdadeira eficiência ganha com a IA.

A montante, existe trabalho de prevenção, melhoria do conhecimento das pessoas e identificação de problemas recorrentes. A jusante, importa analisar causas, eliminar repetições e melhorar a experiência do cliente. Entre estes dois momentos, continuam a existir situações complexas que exigem julgamento, contexto e responsabilidade.

Reduzir tarefas repetitivas pode criar espaço para reforçar estas atividades. Pode também permitir absorver mais volume e complexidade sem aumentar os recursos na mesma proporção. Essa capacidade adicional tem valor económico e pode traduzir-se em melhor serviço, maior capacidade de crescimento e funções mais qualificadas.

Nada disto acontece automaticamente. Uma hora libertada só se transforma em valor quando existe uma decisão sobre como a utilizar. Cabe à gestão redesenhar responsabilidades, desenvolver competências e criar condições para que as equipas assumam trabalho de maior valor. Instalar tecnologia e esperar que a organização se reorganize por si própria é deixar a transformação a meio.

É também por isso que a *adoção* interna constitui um teste tão relevante. Obriga a trabalhar a integração com os sistemas existentes, a qualidade do conhecimento, os limites de atuação, o tratamento de exceções e a confiança das pessoas. Obriga, sobretudo, a verificar se a melhoria se mantém para além da demonstração inicial e se pode ser replicada noutros contextos.

Escalar exige essa aprendizagem. Multiplicar uma solução antes de compreender as condições do seu sucesso pode apenas multiplicar fragilidades.

Os resultados abrem também, cada vez mais, uma discussão sobre o próprio modelo de negócio. À medida que a *IA* aumenta a eficiência, é legítimo que os clientes esperem transparência sobre o investimento, os custos de operação e os benefícios efetivamente alcançados.

Quando conseguimos prevenir problemas e assegurar maior continuidade no serviço com a IA, o valor deste serviço torna-se menos dependente do esforço necessário para executar cada tarefa individualmente. Demonstrar esse valor e encontrar formas equilibradas de o partilhar pode reforçar a confiança na relação com o cliente.

Transformar primeiro significa assumir estas decisões dentro de casa. Medir com rigor, aprender com as limitações e dar um destino concreto à capacidade libertada. É essa experiência que torna a ambição de escalar mais sólida, e a promessa feita ao mercado mais credível. ■

zaltor
Software Distribution

PAESSLER
THE MONITORING EXPERTS

TrustBuilder

soluções para

Sustentabilidade e eficiência de TI

Contacte-nos →

www.zaltor.com

ManageEngine

IT PULSE PORTUGAL 2026 COLOCA A PREVENÇÃO NO CENTRO DA GESTÃO DE IT

A preparação para a NIS2, a integração de tecnologias de cibersegurança e a gestão proativa de endpoint estiveram em destaque no IT Pulse Portugal 2026, o roadshow da ManageEngine que percorreu três cidades portuguesas.

SETÚBAL foi a primeira paragem do IT Pulse Portugal 2026, o roadshow da ManageEngine que passou também por Aveiro e Braga. A iniciativa abordou os desafios atuais da gestão de IT e cibersegurança, com destaque para a preparação para a NIS2, a integração de tecnologias para apoiar a conformidade e a proteção proativa de endpoint.

José Fonseca, Technical Expert Iberia da ManageEngine, abriu a sessão com o tema "*Blueprint de Conformidade: Alavancar SIEM, SOAR e PAM para a Prontidão da NIS2*", centrado na preparação das organizações para os requisitos da diretiva europeia. "Controlar o acesso, responder com contexto e demonstrar o resultado" foram os três objetivos apresentados.

O primeiro passo passa por identificar quem acedeu a serviços críticos, que ações realizou e quem autorizou a intervenção. "A decisão tem dono. Tem de existir uma decisão interna por parte das empresas", afirmou José Fonseca, sublinhando que a responsabilidade deve ser partilhada entre a direção, o CISO, os responsáveis pelos serviços e as equipas de operações.



- José Fonseca -
Technical Expert Iberia da ManageEngine

O responsável alertou que "o acesso aprovado pode originar um incidente", nomeadamente quando envolve prestadores externos, janelas de manutenção ou servidores críticos. Uma origem inesperada, a elevação de privilégios ou alterações sensíveis podem indicar atividades fora do padrão.

Para responder a estes cenários, a ManageEngine propõe a integração de diferentes tecnologias. "Deverá existir uma ferramenta de PAM que faz toda a gestão dos acessos a uma infraestrutura de um cliente. Depois, deve-se priorizar o risco, nomeadamente com uma ferramenta de SIEM. Ao SOAR cabe executar a resposta e depois coordenar a recuperação com o ITSM", explicou.

José Fonseca sublinhou que "o privilégio tem prazo e propósito", defendendo que os acessos devem ser aprovados previamente, limitados no tempo e rastreáveis. Com as soluções da ManageEngine, cada intervenção pressupõe um pedido, uma aprovação e uma expiração, ficando registada a atividade realizada durante a sessão.

DA DETEÇÃO À RESPOSTA

A correlação de informação assume um papel central neste processo. "Conseguimos ter toda a informação e controlo da infraestrutura, mas é o SIEM que liga os sinais", explicou o responsável, referindo que a tecnologia permite relacionar eventos de identidade, sistemas e rede para identificar potenciais comprometimentos.

No ecossistema da ManageEngine, o PAM360 gere os acessos autorizados, o AD360 monitoriza autenticações e privilégios, o Endpoint Central acompanha alterações, o OpManager analisa a atividade de rede e o ServiceDesk identifica mudanças e serviços afetados.

O motor UEBA acrescenta uma camada de análise comportamental, permitindo identificar desvios face aos padrões habituais dos utilizadores e alertar as equipas de segurança.

Segundo José Fonseca, um potencial ataque pode envolver uma sequência de autenticação, elevação de privilégios, execução de comandos e alterações de configuração. Cabe ao SOC confirmar o impacto, enriquecer o contexto e definir os limites da resposta.

"O *playbook* de resposta deve ser sempre definido", salientou, acrescentando que cada procedimento deve ter um responsável e limites de atuação. Dependendo do impacto, as ações podem passar pela suspensão de contas, encerramento de sessões, bloqueio de origens ou isolamento de servidores críticos.

A resposta deve terminar com a verificação da contenção, correção da causa e validação da recuperação do serviço. Ao longo de todo o processo, é necessário preservar evidências verificáveis, em linha com o Quadro Nacional de Referência em Cibersegurança.

A ManageEngine propõe uma implementação faseada em 90 dias, com o PAM360 e o Log360

> NA PERSPETIVA DA MANAGEENGINE, GERIR DISPOSITIVOS NÃO É SUFICIENTE PARA GARANTIR A PROTEÇÃO DA OPERAÇÃO”

como soluções centrais. Nos primeiros 30 dias, são identificadas contas e fontes de informação e definido um serviço piloto. “Se não existir uma casa arrumada, não há ferramenta que vá salvar”, alertou José Fonseca.

Nos 30 dias seguintes, são implementados controlos e integrações e testados diferentes cenários. A última fase destina-se à validação da eficácia dos controlos e da recuperação, determinando se existem condições para avançar com a implementação.

ENDPOINT PROATIVO: ANTECIPAR PROBLEMAS E REDUZIR RISCOS

A segunda parte do IT Pulse Portugal 2026 foi dedicada ao tema “*Endpoint Proativo: Otimizar a Segurança, EDR e a Experiência Digital do Colaborador*”, com José Fonseca a apresentar uma abordagem que combina gestão, segurança e experiência digital.

“Um *endpoint* sob controlo protege o negócio porque permite corrigir fragilidades e detetar atividade suspeita, resolver degradações antes de o *ticket* surgir e medir a eficácia dos controlos e capacidade recuperada”, afirmou. Na perspetiva da ManageEngine, gerir dispositivos não é suficiente para garantir a proteção da operação. É necessário relacionar os controlos aplicados com o risco efetivo e assegurar que as ações de remediação produzem resultados verificáveis.

Neste contexto, a empresa apresentou uma proposta de coexistência com o Microsoft Intune, complementando a inscrição e aplicação de políticas com maior visibilidade sobre riscos e capacidade de remediação.

O Endpoint Central integra controlo, risco e experiência digital, permitindo gerir dispositivos, atualizações e software, identificar vulnerabilidades, realizar *hardening* e investigar incidentes. Disponibiliza ainda telemetria, DEX Score e *workflows* de remediação.

José Fonseca apresentou ainda os resultados de um estudo da Forrester encomendado pela ManageEngine, que aponta para um retorno sobre o investimento de 442% em três anos. Segundo o responsável, com a automatização operacional, é possível recuperar o investimento em menos de seis meses.

DA GESTÃO REATIVA À PREVENÇÃO

Ao contrário do modelo reativo, em que a intervenção começa após a abertura de um ticket, a abordagem proativa procura identificar sinais de degradação ou risco antes de existir uma interrupção. O processo passa pela

> “A PREVENÇÃO COMEÇA NO QUE SE PODE EXECUTAR”

deteção, contextualização, remediação e validação, uma vez que “cada correção encurta a janela de exposição”.

“A prevenção começa no que se pode executar”, explicou José Fonseca, referindo a importância de controlar o software autorizado, restringir periféricos, aplicar políticas de navegação, corrigir desvios de configuração e gerir a encriptação nas plataformas suportadas.

O EDR, disponibilizado como um módulo adicional pago, acrescenta capacidades de deteção comportamental e inteligência de ameaças, permitindo investigar cadeias de ataque e analisar a telemetria recolhida.

Após a contenção, o Endpoint Central apoia a recuperação, desde a reconstrução da atividade e confirmação do impacto até ao isolamento do Endpoint, remoção de artefactos, correção da exposição e restauro dos ficheiros e serviços afetados.

José Fonseca salientou que “ação sensível exige limites, autorização e resultado registado”, reforçando a necessidade de manter controlo sobre as intervenções realizadas.

A experiência digital constitui outra dimensão desta abordagem. De acordo com o responsável, os dispositivos apresentam frequentemente sinais de degradação antes de os utilizadores solicitarem apoio, nomeadamente através de alterações no consumo de CPU e memória, tempos de arranque, autenticação ou falhas de aplicações.

O DEX Score, numa escala de zero a cem, permite acompanhar estes indicadores e comparar o desempenho dos equipamentos com valores de referência. Em conjunto com alertas, sensores e *workflows*, esta informação pode apoiar a identificação antecipada de problemas e a automatização de ações corretivas.

José Fonseca destacou ainda que o mesmo *endpoint* pode exigir decisões diferentes, dependendo do contexto. Num portátil associado a um serviço crítico, pode ser necessário corrigir uma aplicação e avaliar a experiência após a intervenção ou, perante uma ameaça, conter e investigar antes de retomar a operação.

Para a ManageEngine, a maturidade da gestão de endpoint passa, assim, pela combinação de segurança, controlo e experiência digital, com processos de remediação validados e informação histórica que permita antecipar degradações, reduzir a exposição ao risco e acelerar a recuperação dos serviços. ■



Hybrid Cloud & Multicloud

IT Insight talks

Soberania, controlo e escolha

26 de novembro | Quinta-feira | 10h

A IT Insight convida-o a participar na mesa-redonda Hybrid Cloud & Multicloud, no dia 26 de novembro de 2026, no Fórum Tecnológico Lispolis, em Lisboa. Saber onde vivem os dados, quem os controla e onde correm as cargas de IA é hoje um critério de arquitetura, a par do custo e do desempenho. Junte-se a especialistas do setor e descubra como conciliar flexibilidade, controlo e conformidade na sua estratégia de cloud para 2027.

Fórum Tecnológico Lispolis | A partir das 9h30 | Participação presencial e online.

Escolha a sua forma de participar:

QUERO ESTAR PRESENTE **QUERO ASSISTIR POR ZOOM**

Patrocinado por: IBM, IP Telecom, NetApp, netskope, RICOH imagine. change., software one

Com o apoio de: LISPOLIS Pólo Tecnológico de Lisboa

Red Hat

POR GREGOR VON JAGOW,
Country Manager da Red Hat na Alemanha

FADIGA DE COMPLIANCE? O PROBLEMA NÃO É A REGULAÇÃO

Novas regulações geram em muitas empresas, acima de tudo, uma coisa: mais trabalho. Quem entende o compliance como o cumprimento contínuo de listas de verificação corre o risco de sofrer de fadiga regulatória. Por outro lado, quando os requisitos são integrados em processos, plataformas e automação, pode emergir uma efetiva vantagem estratégica.

NIS2, **DORA**, a Lei de IA, o RGPD ou a Lei de Ciberresiliência estão a alterar permanentemente os requisitos exigidos às organizações e às suas áreas de Tecnologias de Informação (TI's). Ao mesmo tempo, aumenta o número de controlos, evidências e auditorias. Por isso, o problema já não reside apenas em cumprir normas individuais, mas sim em como as empresas lidam com uma **realidade regulatória** cada vez **mais complexa**.

A FADIGA DE COMPLIANCE TEM MUITAS CAUSAS

Esta fadiga de compliance não descreve apenas o stresse antes da próxima auditoria: quanto mais regras, verificações e obrigações se adicionam, menor é a percepção do benefício de cada atividade de compliance. Um controlo originalmente útil torna-se uma rotina e um instrumento de proteção transforma-se num processo administrativo adicional. A consequência é apenas o cumprimento mínimo estrito; ou seja, aplicar diretrizes de forma mecânica sem compreender os riscos subjacentes, enquanto proliferam acordos informais para contornar processos burocráticos.

Isto surge quando os requisitos não estão integrados nos processos operacionais e de TI existentes. Em vez disso, constroem-se fluxos de trabalho adicionais: tabelas para evidências, tickets para aprovações, sistemas de governação, risco e conformidade

(GRC) separados e verificações manual de relatórios. A isto soma-se o facto de os diferentes quadros regulamentares exigirem frequentemente controlos semelhantes, mas organizacionalmente separados, gerando um excesso de carga.

A REGULAÇÃO DEVE ESTAR NO CÓDIGO

A solução para este dilema não consiste em criar mais instâncias de controlo. Uma arquitetura de compliance moderna não trata os requisitos apenas como documentos, mas traduz-os em controlos técnicos. Permissões, configurações, encriptação, regras de rede ou retenção de dados podem ser verificados e aplicados de forma automatizada.

Sob o princípio de Policy as Code, as especificações são definidas de forma legível por máquinas e integradas nos processos de desenvolvimento e operações. Deste modo, ao implementar uma aplicação, verifica-se se cumpre os requisitos de segurança, detectando infrações instantaneamente. Abordagens como CI/CD impulsionam uma governação contínua em toda a área de TI: a validação de configurações, verificação de permissões, detecção de vulnerabilidades e geração de evidências devem ser automatizadas de ponta a ponta.

O PAPEL ESPECIAL DA IA

Uma arquitetura comum permite consolidar numa única instância de controlo técnico normativas com requisitos semelhantes de gestão de risco, rastreabilidade ou cadeia de abastecimento, evitando duplicar projetos de compliance.

Com a IA generativa e agêntica, as exigências intensificam-se: é necessário controlar que modelos são usados, a que dados acedem e que decisões tomam. Ao mesmo tempo, a IA oferece novas vias para automatizar a classificação de dados, a análise de diretrizes ou a preparação de evidências.

De igual forma, as organizações precisam estar atentas para perigo do "shadow AI": à medida que as ferramentas tradicionais se mostram menos capazes para fazer face ao volume e complexidade no contexto de compliance, os utilizadores irão procurar sempre formas de circunscrever as regras e procurar usar ferramentas de IA disponíveis e não autorizadas para circunscrever dificuldades operacionais. Daí que a solução passa por oferecer alternativas **oficiais, seguras e integradas** na arquitetura corporativa.

A VERDADEIRA VANTAGEM COMPETITIVA É A VELOCIDADE

Uma arquitetura bem executada consolida tecnicamente o compliance e facilita a sua implementação, já que, perante uma nova diretiva, o processo reduz-se ao ajuste das diretrizes e controlos existentes. Isto encurta os processos de decisão e adoção no lançamento de aplicações, onboarding de clientes ou concursos públicos.

A chave para superar a fadiga de compliance não passa por controlar menos. Pelo contrário, passa sim por controlar melhor e com valor acrescentado para as organizações, com mais rigor e identificando onde realmente estão os riscos reais, eliminando tarefas manuais que a TI pode assumir de forma fiável. ■

ONDE
A INOVAÇÃO
O CONHECIMENTO
E O TALENTO
SE ENCONTRAM

LiS PO LiS
POLO TECNOLÓGICO DE LISBOA



A Lispolis é o **Pólo tecnológico de Lisboa** um ecossistema que liga empresas, centros de investigação, startups e talento impulsionando a **inovação** e o **desenvolvimento tecnológico** com impacto real na sociedade







PÓLO TECNOLOGICO DE LISBOA
Soluções flexíveis e infraestruturas modernas para empresas modernas para empresas de todas as dimensões cresceram e inovarem

HUB DE SAÚDE
Um hub que promove a ligação entre saúde tecnologia e bem - estar desenvolvendo soluções inovadoas com impacto na vida das pessoas

PRÓXIMO DAS UNIVERSIDADES
Ligação priveligiada a universidades e instituições de ensino superior, facilitando o acesso a talento qualificado e a projetos de investigação

ESPAÇO PARA EVENTOS
Auditórios, salas e espaços versáteis para conferências reuniões, formações e eventos corporativos de impacto

APROXIME-SE DO TALENTO
DA INOVAÇÃO E DO CONHECIMENTO

Fale connosco e descubra as oportunidades da Lispolis.

www.lispolis.pt

Instalação de empresas

Reservas de eventos

Life Is On | Schneider Electric

POR VICTOR GAGO,
Data Center & C&SP Sales Manager, Schneider Electric

DATA CENTERS PARA IA: DA CAPACIDADE DE REFRIGERAÇÃO À INTELIGÊNCIA DO SISTEMA

A inteligência artificial está a transformar a infraestrutura dos Data Centers. Com a densidade de potência dos racks a aumentar e atingir 200 a 300 kW, ou mais em determinados ambientes, a refrigeração tornou-se crítica para assegurar desempenho e disponibilidade.

PORÉM, dimensionar a capacidade térmica já não chega. A fiabilidade depende da interação entre refrigeração, alimentação elétrica, sistemas de controlo e práticas operacionais, que têm de funcionar de forma coordenada para responder às exigências destas novas cargas de trabalho. Mesmo com tecnologia adequada, uma instalação pode continuar exposta à degradação dos equipamentos, a decisões inadequadas de manutenção, limitações nos processos ou à escassez de competências especializadas.

QUANDO A DENSIDADE EXIGE MAIS DO QUE CAPACIDADE TÉRMICA

As cargas de IA concentram muito calor em espaços reduzidos. Em ambientes com clusters de GPU e aplicações críticas, uma falha de refrigeração pode comprometer rapidamente a continuidade operacional. A fiabilidade térmica torna-se, por isso, tão importante como a elétrica.

A escolha entre refrigeração a ar ou líquida é relevante, mas não resolve completamente o desafio. A refrigeração líquida acrescenta complexidade



- Victor Gago -
Data Center & C&SP Sales Manager, Schneider Electric

hidráulica e exigências de pressão, controlo térmico e resposta a incidentes. Assim, prevenir fugas, garantir a compatibilidade dos materiais e preparar as equipas são condições essenciais para assegurar que estas soluções mantêm o desempenho esperado ao longo do tempo.

Preparar um Data Center para IA exige, assim, mais do que a instalação de equipamentos adequados: implica assegurar a sua gestão contínua, com capacidade de diagnóstico, suporte especializado e processos operacionais ajustados a uma infraestrutura cada vez mais dinâmica.

MANUTENÇÃO BASEADA NA CONDIÇÃO

A manutenção programada mantém a sua importância, mas deve ser complementada por decisões baseadas no estado real dos equipamentos e nas condições de operação.

A monitorização contínua, a analítica preditiva e o diagnóstico remoto permitem detetar sinais de degradação antes de afetarem a disponibilidade. Assim, é possível intervir no momento adequado, evitar tarefas desnecessárias e prolongar a vida útil dos ativos.

Esta abordagem também ajuda a otimizar o desempenho da refrigeração, reduzir desperdícios e gerir melhor o consumo energético, conciliando fiabilidade e sustentabilidade.

COMPREENDER O SISTEMA NO SEU CONJUNTO

Monitorizar cada equipamento isoladamente não basta. Uma bomba, um chiller ou uma UPS podem funcionar dentro dos parâmetros esperados sem que a infraestrutura esteja preparada para um aumento de carga, uma intervenção de manutenção ou uma alteração das condições operacionais.

A inteligência do sistema permite correlacionar dados elétricos, mecânicos, ambientais e operacionais, identificando riscos que uma análise isolada não revela: limitações de redundância, insuficiência de capacidade de reserva ou margens operacionais reduzidas.

A disponibilidade resulta, portanto, da coordenação entre tecnologia, processos e pessoas, apoiada numa visão integrada do desempenho da infraestrutura.

DOS DADOS À AÇÃO, AO LONGO DO CICLO DE VIDA

Instalar tecnologia de refrigeração é apenas o ponto de partida. A fiabilidade a longo prazo depende da forma como os ativos são operados, mantidos, modernizados e otimizados.

Serviços de ciclo de vida, como a avaliação da base instalada, a modernização, a monitorização remota, o diagnóstico especializado e o apoio no terreno, ajudam a transformar dados em decisões e a responder à escassez de competências.

Ao combinar manutenção baseada na condição, automação e inteligência digital, torna-se possível gerir de forma coordenada energia, refrigeração e operação. O futuro dos Data Centers para IA não depende apenas de maior capacidade térmica, mas de infraestruturas mais inteligentes, eficientes e resilientes, capazes de antecipar riscos e acompanhar a evolução das necessidades computacionais. ■

d_AI_gest

AI DIGEST, UM RESUMO DO QUE ESTÁ A ACONTECER NAS FRONTEIRAS DA INTELIGÊNCIA ARTIFICIAL



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

Os agentes ficam à porta



NO PASSADO dia 8 de setembro, a Meta lançou o Muse, um agente baseado em IA que abre um navegador, preenche formulários e faz compras com os dados que o utilizador lhe confiar. Doze dias depois, quem o enviasse à Amazon passaria a encontrar um aviso: «O acesso continuado por um agente de IA não autorizado viola as Condições de Utilização da Amazon, que os nossos clientes aceitaram.» A Amazon ter-se-á queixado de que a Meta não a avisou de que o agente não se identifica e de que entra nas páginas de conta e no histórico de encomendas, e pediu à Meta que a retirasse do serviço. A Meta não respondeu.

A Amazon já tinha tentado travar outro agente, o do navegador Comet, da Perplexity, e perdido a demanda. Em agosto, um tribunal federal de recurso dos Estados Unidos anulou a proibição provisória que o travava: quem acede aos computadores da Amazon é o utilizador, ajudado pelo assistente, que é, para efeitos da legislação contra intrusão informática, "uma ferramenta, não uma pessoa". O mesmo acórdão lembra, numa nota de rodapé, que a Amazon continua a ser livre de regular o acesso através dos termos que os seus clientes aceitam; foi precisamente nisso que a empresa se baseou para o aviso aos utilizadores do Muse.

A Zyte, uma empresa que vende acesso automatizado a dados da Web, analisou onze mil e cem das páginas mais visitadas do mundo: só dezoito e meio por cento não tinham qualquer barreira à navegação automática e, no ficheiro em que cada site diz aos bots o que podem visitar, menos de dois por cento autorizavam expressamente os sistemas de IA.

Quem vende online terá de decidir se o agente de um cliente conta como se fosse o cliente, e de o escrever nas condições de utilização. Por outro lado, quem pense delegar a um agente as compras ou as pesquisas dos seus serviços tem de contar com fornecedores que podem não o deixar passar da porta. ■

Marcas de origem também se aplicam às proteínas

OS MODELOS DE IA já desenham proteínas que não existem na natureza, entregues como uma sequência de aminoácidos a partir da qual um laboratório pode encomendar a síntese. A Google DeepMind apresentou o SynthID Bio, um conjunto de métodos que inscrevem uma marca de origem nessa sequência, para que acompanhe a proteína depois de sintetizada e não dependa de uma nota que alguém se lembre de conservar junto do ficheiro.

A marca entra durante o desenho: entre os aminoácidos possíveis em cada posição, o sistema orienta subtilmente a escolha, deixando um padrão reconhecível por um detetor que disponha da chave secreta usada na marcação. A implementação para sequências integra-se no ProteinMPNN, um modelo que propõe sequências para uma estrutura pretendida, e o código está disponível publicamente. O risco era estragar aquilo que é o objetivo da molécula. Nos ensaios com três alvos, entre eles o PD-L1 e o domínio de ligação ao recetor da proteína spike do SARS-CoV-2, os desenhos marcados tiveram taxas de sucesso e afinidades de ligação comparáveis às das versões sem marca.

Segundo a DeepMind, a marca poderá ajudar os fornecedores de síntese e as bases de dados científicas a reconhecer desenhos vindos de modelos identificados. A robustez contra manipulação deliberada continua a exigir investigação, e a origem de uma proteína, por si só, não demonstra a sua segurança. O artigo propõe que a marca sirva como sinal de utilização de uma ferramenta com salvaguardas verificadas, mas reconhece um limite nos modelos abertos: quem quiser evitar a marca pode escolher uma ferramenta que não a incorpore. ■

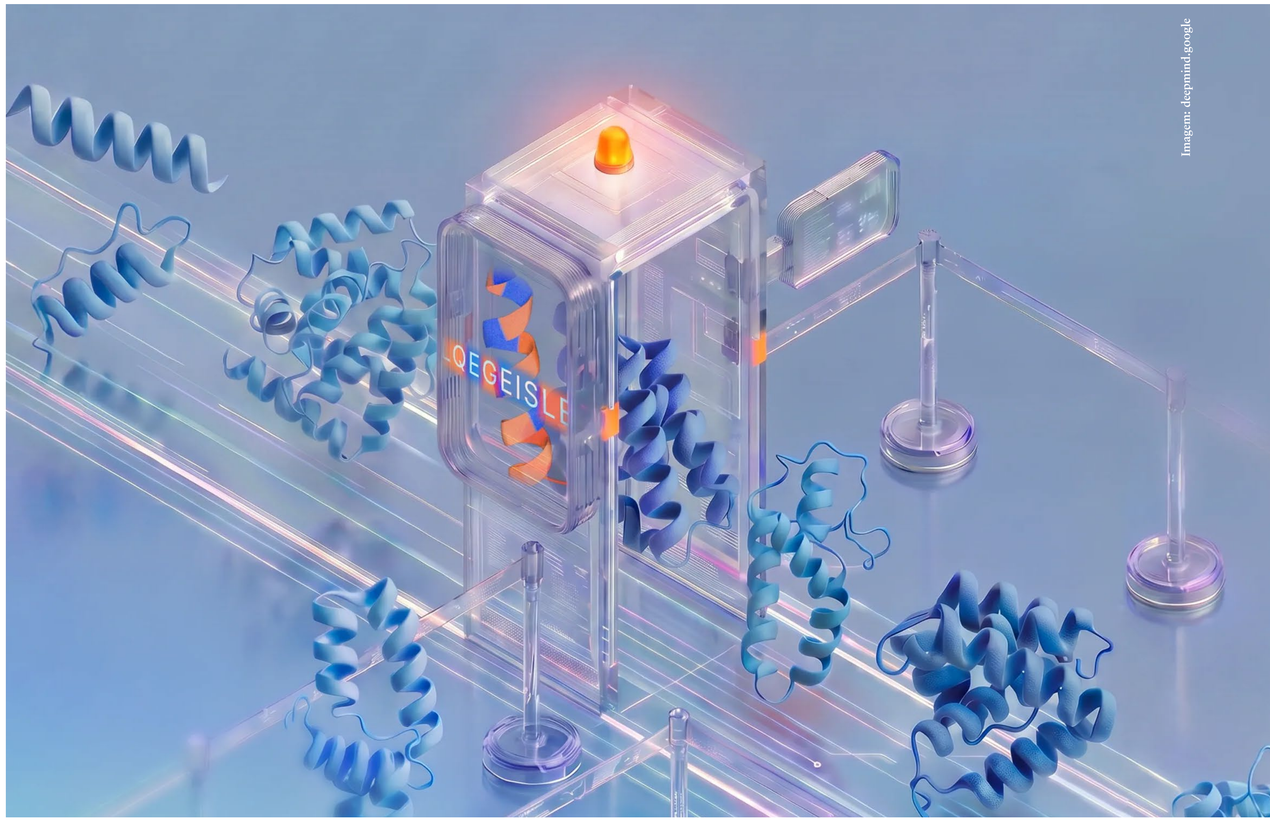


Imagem: deepmind.google



Imagem: GXO

O incansável fiel de armazém

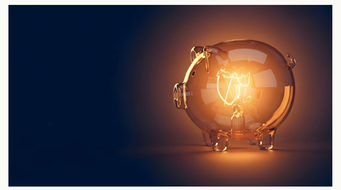
EM FLOWERY BRANCH, na Geórgia, num armazém da empresa de logística GXO, um robot humanoide chamado Digit recolhe as caixas que lhe trazem robôs móveis com rodas e coloca-as em tapetes transportadores, coordenado pelo software de gestão da Agility Robotics, que o fabrica. A operação comercial começou em 2024, depois de um piloto.

A Agility atribui a esta versão, o Digit 4, mais de sessenta e cinco mil horas de operação em vários clientes e cem mil caixas movimentadas naquela instalação, contagens do fabricante que não permitem, contudo, calcular a produtividade por turno, nem a frequência de intervenções humanas. O sucessor, Digit 5, apresentado no passado mês de setembro e com acesso antecipado previsto para o primeiro semestre de 2027, foi concebido para trabalhar próximo de pessoas com menor dependência de vedações físicas. Segundo a Agility, combina sensores que detetam a presença humana com um controlador de segurança independente, que desencadeia respostas de proteção, como desviar-se, parar ou assumir uma posição sentada. A empresa prevê recorrer ao laboratório de inspeção Halos da Nvidia para avaliar os componentes relacionados com a segurança antes da certificação final por uma entidade terceira.

A ISO 25785-1, a futura norma de segurança para robôs industriais de estabilidade ativa, bípedes incluídos, ainda está em desenvolvimento, e a Agility participa na sua preparação. Para quem pense instalar o Digit 5, uma pergunta que pode ser feita ao fornecedor é quantas paragens de proteção o robot faz por turno quando partilha o espaço com pessoas, e o que acontece à mercadoria em cada uma, um número que a Agility mantém ainda em segredo. ■



A FATURA (CADA VEZ MENOS) ESCONDIDA DA EFICIÊNCIA DIGITAL



A tecnologia está a tornar-se mais eficiente, mas isso não significa que as empresas estejam a consumir menos recursos. Entre infraestruturas sobredimensionadas, custos difíceis de controlar e uma IA cada vez mais exigente, a sustentabilidade das IT começa a fazer-se pelas contas. O desafio passa por perceber onde se está a desperdiçar, quanto custa manter essa ineficiência e até que ponto os ganhos tecnológicos se refletem na fatura energética.

INÊS GARCIA MARTINS

A PRESSÃO PARA INVESTIR em Inteligência Artificial (IA) e modernizar infraestruturas está a colocar novos desafios às empresas, que precisam de encontrar margem nos orçamentos para acompanhar a evolução tecnológica. Contudo, parte dos recursos disponíveis continua a ser consumida por aplicações pouco utilizadas, capacidade excedentária e sistemas que já não respondem às necessidades do negócio. A dificuldade em identificar e corrigir estas ineficiências pode comprometer os recursos financeiros necessários para novos investimentos.

Em Portugal, apenas 47% das organizações afirmam conhecer integralmente os seus custos tecnológicos, incluindo encargos indiretos e compromissos futuros, segundo o "*Tech Check Reality 2026*", da Conclusion. A falta de visibilidade não prova desperdício energético, mas dificulta a identificação de capacidade excedentária, investimentos mal aproveitados e oportunidades de otimização, numa altura em que a procura por computação acelera e ameaça absorver os ganhos de eficiência proporcionados pela evolução tecnológica.

ANTES DE COMPRAR MAIS, USAR MELHOR

Entre as fontes de desperdício tecnológico que persistem nas empresas, Pedro Teixeira, Cloud & Infra Senior Director da Claranet Portugal, identifica





- Pedro Teixeira -
Claranet Portugal

> “SE FOI MAL DESENHADO, CONTINUA MAL DESENHADO, SÓ QUE AGORA PAGA-SE AO MINUTO”

“máquinas que vieram de *on-premises* com a dimensão de há dez anos, nos ambientes de teste que ninguém desliga ao fim de semana, nos *snapshots* de projetos que já terminaram”. Para o responsável, esta realidade reflete uma dificuldade na responsabilização pela utilização dos recursos, sendo “menos um problema de tecnologia e mais um problema de ninguém ser dono da fatura”.

A migração para cloud também não elimina, por si só, as ineficiências existentes, uma vez que, como observa Pedro Teixeira, “se foi mal desenhado, continua mal desenhado, só que agora paga-se ao minuto”. A escolha da infraestrutura deve considerar as características de cada *workload*. Cargas estáveis e previsíveis podem justificar ambientes privados ou dedicados, enquanto necessidades variáveis beneficiam da elasticidade da cloud pública. O licenciamento, a latência e o custo total de operação também devem pesar na decisão.

A expansão da IA está a exigir decisões mais informadas sobre os investimentos tecnológicos. Contudo, segundo o estudo “*Cloud-led innovation in the era of AI: The new rules for driving value with cloud*”, publicado pela NTT Data em março de 2026, apenas 14% das organizações atingiram o nível mais elevado de maturidade na cloud. A investigação, que envolveu 2.335 decisores seniores de 33 países, revela ainda que 99% reconhecem na IA um fator de aumento do investimento nesta área.

Neste contexto, o FinOps pode aproximar eficiência operacional e disciplina financeira, ao permitir identificar recursos ociosos, ajustar a capacidade utilizada e reduzir custos. Porém, a poupança não se traduz necessariamente em benefícios



ambientais, já que, como alerta Pedro Teixeira, "a região mais em conta financeiramente pode ser a mais intensiva em carbono, e uma reserva de capacidade baixa o preço sem reduzir um watt".

O CRESCIMENTO TEM UM CUSTO DE ENTRADA

Com a crescente utilização de aplicações e modelos de IA, a disponibilidade de energia torna-se determinante para a expansão dos data centers. Segundo as previsões da Gartner, atualizadas em junho de 2026, o consumo elétrico mundial destas infraestruturas deverá crescer 26% este ano, atingindo 565 TWh, e ultrapassar os 1.200 TWh até 2030. Os ganhos de eficiência por unidade de processamento não impedem, por isso, que o consumo total de eletricidade continue a aumentar.

Ana Quelhas, responsável de Hidrogénio e Data Centres da EDP, considera que o acesso à energia já condiciona as decisões de investimento e localização destas infraestruturas. "Um projeto pode reunir todas as condições tecnológicas e financeiras, mas se não conseguir assegurar o fornecimento de energia no prazo necessário, a sua concretização pode ficar comprometida", explica, numa altura em que a capacidade de ligação à rede e a disponibilidade de potência se tornam tão determinantes quanto o preço da eletricidade.



- Ana Quelhas -
EDP

> "A UTILIZAÇÃO DE ELETRICIDADE RENOVÁVEL É FUNDAMENTAL, MAS, POR SI SÓ, NÃO É SUFICIENTE"





- Rita Monteiro -
Start Campus

Em Portugal, o potencial económico deste crescimento está refletido nas projeções do "*Market Outlook Data Centers Portugal 2025*", da PortugalDC, que estima um impacto de 3,7 mil milhões de euros no PIB nacional até 2031. A concretização desta oportunidade depende, contudo, de investimentos em redes, produção e armazenamento que não avançam necessariamente ao mesmo ritmo que a procura digital, exigindo maior articulação entre o planeamento energético e o desenvolvimento tecnológico.

Na EDP, esta articulação é considerada essencial para responder às novas necessidades de consumo, embora Ana Quelhas reconheça que "a utilização de eletricidade renovável é fundamental, mas, por si só, não é suficiente". A variabilidade da produção solar e eólica exige soluções de armazenamento, redes robustas e mecanismos de flexibilidade que assegurem o fornecimento contínuo necessário aos data centers.

A expansão destas infraestruturas levanta também preocupações quanto à distribuição dos custos, com a responsável a defender que "os grandes consumidores devem contribuir de forma proporcional para as infraestruturas de que necessitam, evitando transferir encargos excessivos para as famílias e empresas".

A expansão dos data centers coloca igualmente exigências às regiões onde se instalam, o que leva Rita Monteiro, responsável pela área de sustentabilidade da Start Campus, a destacar a importância de associar estes investimentos à criação de

> "O SUCESSO DE UM PROJETO DESTA NATUREZA DEVE TRADUZIR-SE NUM CONTRIBUTO POSITIVO PARA O DESENVOLVIMENTO DA REGIÃO"



> TER CAPACIDADE TECNOLÓGICA OU CAPITAL DISPONÍVEL NÃO É SUFICIENTE SE NÃO EXISTIR INFRAESTRUTURA ENERGÉTICA CAPAZ DE SUPORTAR ESSA CAPACIDADE”



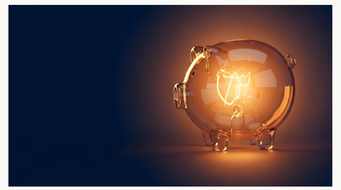
- Victor Gago -
Schneider Electric

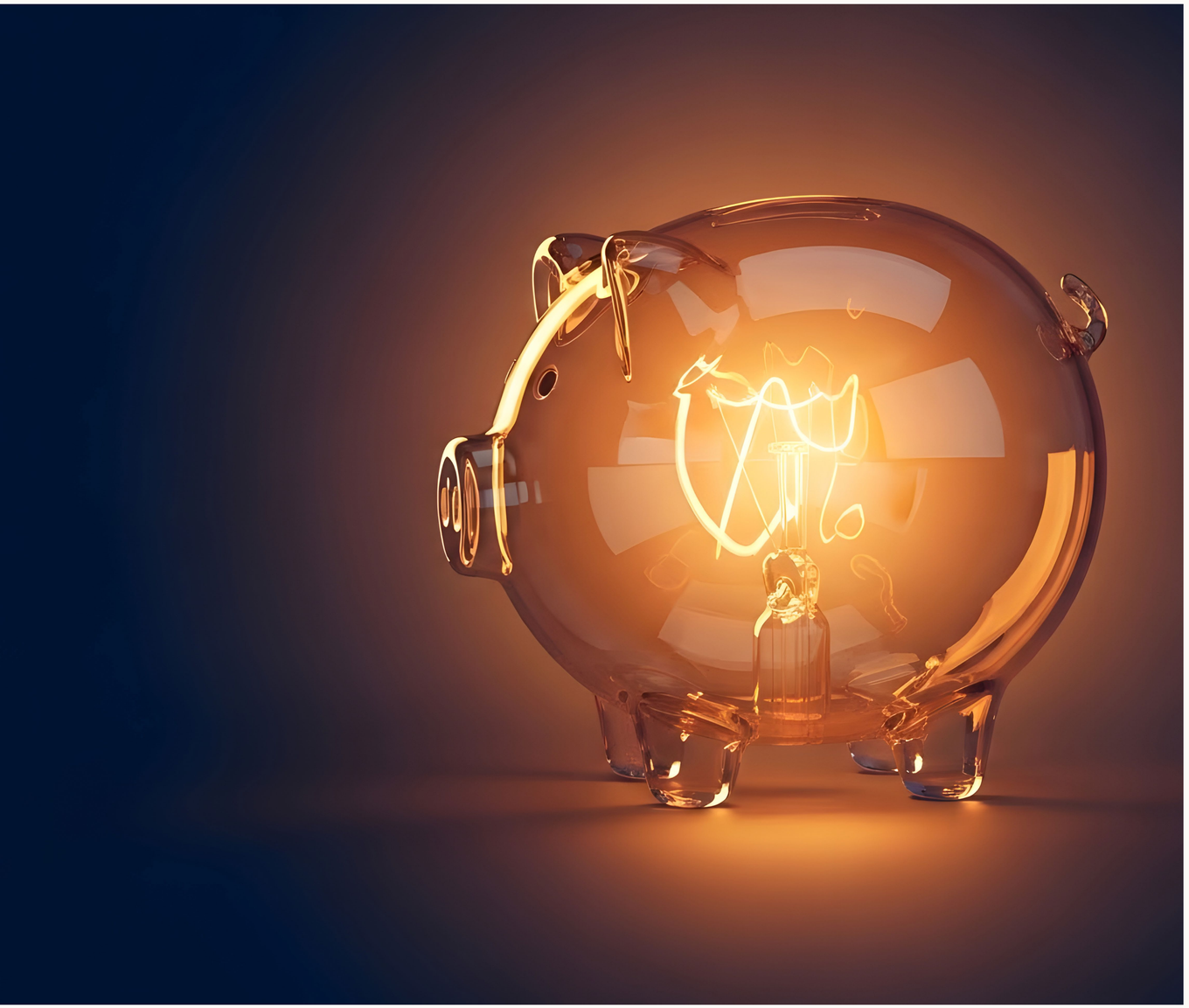
emprego qualificado, ao desenvolvimento de parcerias e à gestão responsável dos recursos locais. Na sua visão, “o sucesso de um projeto desta natureza deve traduzir-se num contributo positivo para o desenvolvimento da região, assegurando simultaneamente uma gestão adequada dos seus impactos ambientais e sobre as infraestruturas locais”, numa perspetiva que ultrapassa a capacidade computacional instalada e considera também os efeitos económicos e ambientais do desenvolvimento.

Esta necessidade de conciliar desenvolvimento tecnológico, disponibilidade de recursos e sustentabilidade está também a alterar os critérios de competitividade. Ana Quelhas, da EDP, antecipa que “no futuro, os projetos digitais mais competitivos serão também aqueles que melhor integrarem a energia nas suas decisões de investimento e operação”.

A POUPANÇA COMEÇA NO DESENHO

O aumento da densidade dos equipamentos de IA está a exigir alterações nos sistemas de alimentação elétrica e refrigeração. Contudo, a substituição de tecnologia implica novos investimentos e impactos ambientais associados ao fabrico dos equipamentos.

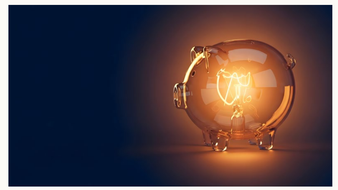




Victor Gago, Data Center & C&SP Sales Manager da Schneider Electric, defende que "o primeiro passo é identificar as perdas e perceber que ativos podem ser otimizados, atualizados ou integrados antes de se avançar para substituições". A decisão deve considerar os ganhos operacionais e o impacto ambiental dos equipamentos ao longo de todo o seu ciclo de vida.

Em Sines, a Start Campus aposta na eficiência desde a fase de projeto, através da utilização de eletricidade de origem renovável e de sistemas de arrefecimento com água do mar. A infraestrutura procura também responder às exigências da IA, com Rita Monteiro a destacar que "as nossas instalações foram concebidas para integrar soluções de arrefecimento a ar e a líquido, incluindo sistemas de refrigeração *direct-to-chip*, adequados às exigências das aplicações de inteligência artificial".

Esta flexibilidade ganha importância à medida que aumenta a capacidade computacional e se torna necessária uma maior integração entre energia, IT e refrigeração. Na Schneider Electric, Victor Gago aponta a digitalização das operações e a gestão ativa da procura como formas de aproveitar melhor os recursos existentes, uma vez que "ter capacidade tecnológica ou capital disponível não é suficiente se não





- Nuno Lopes -
FuriosaAI

existir infraestrutura energética capaz de suportar essa capacidade".

A avaliação dos resultados continua, porém, a apresentar limitações, uma vez que indicadores como o *Power Usage Effectiveness* (PUE) e o *Water Usage Effectiveness* (WUE) permitem acompanhar o desempenho energético e a utilização de água dos data centers, mas não traduzem necessariamente as emissões totais, o impacto nos recursos locais ou a quantidade de trabalho computacional útil produzido.

Para Rita Monteiro, "a transparência é fundamental, sobretudo para distinguir os objetivos definidos na fase de conceção dos resultados efetivamente alcançados durante a operação". Esta preocupação ganha relevância perante a proposta apresentada pela Comissão Europeia, em setembro de 2026, para classificar os data centers com base em indicadores de eficiência energética e hídrica, procurando tornar o desempenho das instalações mais comparável, embora sem garantir, por si só, uma redução do consumo absoluto.

MAIS TRABALHO POR WATT, MAIS PROCURA NO TOTAL

A eficiência energética da IA depende, em parte, da arquitetura dos processadores e da forma como os dados circulam entre a memória e as unidades de cálculo. Nuno Lopes, Vice-Presidente para a Europa e África da FuriosaAI, explica que "na IA, o que mais gasta energia não são as contas, é mover dados", pelo que reduzir os acessos à memória

> "QUANDO ALGO FICA MAIS BARATO E MAIS EFICIENTE, USA-SE MAIS"



pode gerar ganhos significativos. As arquiteturas especializadas contribuem para esse objetivo, mas os resultados dependem também da integração entre hardware, compiladores e software.

A eficiência anunciada pelos fabricantes nem sempre se confirma em ambientes empresariais, onde os resultados dependem dos *workloads*, da latência e da utilização efetiva dos equipamentos. Nuno Lopes recomenda avaliar "energia por tarefa útil, por exemplo *tokens* por joule, custo por milhão de *tokens* com os requisitos de latência da aplicação e o TCO total ao longo da vida do equipamento", recorrendo a medições com os próprios modelos e aplicações, em vez de valores máximos das especificações técnicas.

Também para Victor Gago, a avaliação da eficiência deve considerar a "quantidade de capacidade computacional útil que é possível obter por cada kWh consumido", de forma a avaliar os resultados efetivamente alcançados e não apenas o desempenho isolado da infraestrutura.

Ainda assim, executar mais operações com a mesma quantidade de energia não implica necessariamente uma redução do consumo total, sobretudo quando o volume de tarefas continua a aumentar.

Nuno Lopes reconhece esta limitação ao abordar o efeito de ricochete, em que a maior eficiência pode estimular a procura. "Quando algo fica mais barato e mais eficiente, usa-se mais", observa o responsável. Para as empresas, este fenómeno reforça a importância de escolher modelos adequados a cada tarefa, evitar capacidade computacional ociosa e avaliar o benefício efetivo da utilização de IA.

A sustentabilidade e a eficiência energética são já requisitos de competitividade para os operadores de infraestruturas digitais, mas Rita Monteiro considera que também podem constituir "fatores de diferenciação para os mercados capazes de demonstrar resultados concretos e mensuráveis". Já na EDP, Ana Quelhas identifica uma transformação semelhante no planeamento dos projetos tecnológicos, com a energia a passar de uma necessidade operacional para "uma componente estratégica da sua conceção e viabilidade".

A redução do consumo por operação pode tornar a tecnologia mais acessível e estimular uma procura capaz de absorver parte dos ganhos de eficiência. Perante este paradoxo, Nuno Lopes defende que a resposta não passa por usar menos IA, mas por "usá-la com critério e medir o que realmente importa".

É precisamente nesta capacidade de gerir os recursos que a sustentabilidade das IT encontra um argumento económico, embora a poupança financeira não garanta, por si só, um menor impacto ambiental. Com as empresas pressionadas a investir e a controlar os recursos existentes, Pedro Teixeira lembra que "a IA vai crescer, de qualquer forma. A questão é se cresce com contas feitas ou à espera da fatura". ■

claranet®

POR JOÃO MIRA SANTIAGO,
Executive Director, Claranet Portugal

SUSTENTABILIDADE E EFICIÊNCIA TECNOLÓGICA:
UMA QUESTÃO DE COMPETITIVIDADE EMPRESARIAL

Durante demasiado tempo, discutimos a sustentabilidade como um custo e a tecnologia como um investimento. Talvez esteja na altura de reconhecer que ambas devem ser avaliadas pelo mesmo critério: a capacidade de criar valor para o negócio.

AS ORGANIZAÇÕES habituaram-se a olhar para a *sustentabilidade* e para a transformação digital como prioridades distintas. De um lado, os compromissos ambientais e sociais. Do outro, a inovação, a produtividade e o crescimento. Esta separação deixou de fazer sentido. Num contexto de crescente pressão sobre os custos, maior exigência dos clientes e aceleração tecnológica, a *sustentabilidade* tem de fazer parte das decisões de gestão e da estratégia empresarial.

No mercado B2B, esta realidade assume particular relevância. As empresas são cada vez mais avaliadas pela sua capacidade de demonstrar práticas responsáveis, garantir transparência e contribuir para a *sustentabilidade* das cadeias de valor em que participam. O *ESG* ultrapassa, assim, a dimensão regulamentar e reputacional para se afirmar como um fator de diferenciação, competitividade e confiança nas relações empresariais.



- João Mira Santiago -
Executive Director, Claranet Portugal

A EFICIÊNCIA NÃO DEVE SER CONFUNDIDA COM UMA POLÍTICA DE REDUÇÃO DE DESPESA

A tecnologia é, simultaneamente, parte do desafio e da solução. Segundo a Agência Internacional de Energia, os centros de dados consumiram cerca de 415 TWh de eletricidade em 2024, aproximadamente 1,5% do consumo mundial. A mesma entidade estima que este valor possa atingir cerca de 945 TWh em 2030, impulsionado, entre outros fatores, pelo crescimento da *Inteligência Artificial*. Estes números mostram que a aceleração digital tem um impacto crescente na utilização dos recursos e que as decisões tecnológicas devem ser tomadas com maior consciência económica e ambiental.

Mas a questão que se coloca às organizações não é se devem continuar a investir em tecnologia. Como garantir que cada investimento contribui efetivamente para melhorar o desempenho do negócio? Mais tecnologia não significa necessariamente mais eficiência, tal como mais investimento não se traduz, por si só, em maior criação de valor.

A crescente adoção de soluções *Cloud*, a modernização das infraestruturas, a digitalização dos processos e, mais recentemente, a integração da *Inteligência Artificial* nas operações empresariais trouxeram ganhos significativos de capacidade, agilidade e inovação. Ao mesmo tempo, criaram desafios de gestão, nomeadamente ao nível da complexidade operacional, da utilização dos recursos e do controlo dos custos. É neste contexto que a eficiência tecnológica assume uma importância estratégica.

Otimizar ambientes *Cloud*, eliminar capacidade não utilizada, modernizar aplicações, automatizar processos e adequar as infraestruturas às necessidades reais das organizações são decisões que podem produzir benefícios simultaneamente económicos e ambientais. Disciplinas como *FinOps* e *GreenOps* aproximam estas duas dimensões, promovendo uma gestão mais rigorosa dos custos, consumos e recursos. Para além de ser possível controlar melhor os gastos, permitem utilizar melhor os recursos disponíveis para produzir mais valor.

Isto porque uma organização pode reduzir custos tecnológicos no imediato e, ainda assim, comprometer a sua capacidade futura de inovação, resiliência ou crescimento. A eficiência não deve, por isso, ser confundida com uma política de redução de despesa. É uma disciplina de gestão contínua, capaz de equilibrar desempenho, *sustentabilidade* e retorno do investimento.

O mesmo princípio deve ser aplicado à *Inteligência Artificial*. O seu potencial para melhorar a produtividade, simplificar operações e apoiar decisões

O ESG NÃO PODE SER UMA RESPONSABILIDADE ISOLADA DE UMA FUNÇÃO DDA ORGANIZAÇÃO, TEM DE ESTAR INTEGRADO NOS PROCESSOS DE DECISÃO, NOS MODELOS DE INVESTIMENTO E NA AVALIAÇÃO DE DESEMPENHO EMPRESARIAL

é significativo. Contudo, a adoção destas tecnologias deve ser acompanhada por critérios claros de retorno, governação e utilização responsável dos recursos, para o foco ser sobretudo o valor que conseguimos criar com a utilização da *Inteligência Artificial*, e a que custo.

Existe, porém, uma dimensão que considero particularmente relevante: a *sustentabilidade* das organizações não termina nas suas fronteiras. Num mercado cada vez mais interligado, clientes, fornecedores e parceiros partilham responsabilidades na construção de cadeias de valor mais eficientes, resilientes e sustentáveis. Para as empresas tecnológicas, esta realidade representa uma responsabilidade acrescida, mas também uma oportunidade de diferenciação.

O verdadeiro valor de um parceiro tecnológico está na capacidade de disponibilizar soluções inovadoras e na sua contribuição para os resultados dos clientes. Ajudar as organizações a simplificar operações, melhorar a produtividade, otimizar recursos e reforçar a segurança e a resiliência é também contribuir para os seus objetivos de *sustentabilidade*. É nesta convergência entre tecnologia, eficiência e negócio que reside uma parte importante da proposta de valor do setor.

Naturalmente, esta transformação exige uma maior articulação entre as áreas de tecnologia, operações, finanças e *sustentabilidade*. O *ESG* não pode ser uma responsabilidade isolada de uma função da organização, tem de estar integrado nos processos de decisão, nos modelos de investimento e na avaliação do desempenho empresarial. E exige capacidade de medir resultados, porque não basta anunciar compromissos ou definir objetivos: é necessário demonstrar ganhos de eficiência, evolução dos consumos, melhoria da produtividade e impacto económico das decisões tomadas.

As organizações que melhor conseguirem integrar estas dimensões estarão mais bem preparadas para enfrentar os desafios de competitividade dos próximos anos. Não necessariamente porque investem mais em tecnologia, mas porque sabem fazer melhores escolhas, simplificar operações e construir relações de maior confiança com os seus clientes e parceiros.

O verdadeiro desafio está em conseguir que estas três dimensões - crescimento, inovação e *sustentabilidade* - se reforcem mutuamente, porque a sustentabilidade empresarial não se mede apenas pelos recursos que conseguimos poupar – é também medida pelo valor que somos capazes de criar com os recursos que utilizamos. ■

Life Is On | Schneider Electric

POR BEATRIZ PALACIOS,
Product Manager & Business Development Cooling, Iberia,
Schneider Electric

REFRIGERAÇÃO LÍQUIDA:

A EFICIÊNCIA DOS DATA CENTERS PARA IA ALÉM DO PUE

A Inteligência Artificial está a mudar a forma como avaliamos a eficiência dos Data Centers. Com racks que podem ultrapassar os 100 kW e cargas de GPU cada vez mais exigentes, já não basta saber quanta energia consome uma instalação. É necessário perceber quanto trabalho computacional útil consegue produzir com os recursos disponíveis.

O POWER USAGE EFFECTIVENESS (PUE) continua a ser uma referência importante: relaciona a energia total consumida pelo Data Center com a energia utilizada pelos equipamentos de TI. No entanto, não mede o desempenho da computação: uma instalação pode apresentar um PUE favorável e, ainda assim, não tirar pleno partido da capacidade instalada.

DA ENERGIA AO DESEMPENHO COMPUTACIONAL

Se os sistemas de refrigeração limitarem a densidade dos racks ou provocarem restrições térmicas nas GPUs, a infraestrutura pode impedir que a potência disponível se traduza em trabalho computacional. É por isso que a avaliação da eficiência deve ir além dos consumos dos sistemas de suporte. Indicadores complementares, como o Power Compute Effectiveness (PCE), procuram mostrar que parcela da potência disponível é efetivamente aplicada à computação útil. Métricas como tokens por watt e custo por token ajudam, por sua vez, a relacionar desempenho, recursos energéticos e custos. Não substituem o PUE: respondem a perguntas diferentes e, em conjunto, oferecem uma visão mais completa.

REFRIGERAÇÃO LÍQUIDA COMO PARTE DO SISTEMA

A refrigeração líquida permite captar calor junto dos componentes mais exigentes, reduzindo a dependência da circulação de grandes volumes de ar. Pode, assim, suportar densidades superiores e ajudar a evitar limitações



- Beatriz Palacios -
Product Manager & Business Development Cooling, Iberia,
Schneider Electric

térmicas que condicionam o desempenho das GPUs. Permite também aumentar a capacidade computacional sem exigir uma expansão proporcional do espaço físico, uma vantagem relevante perante as limitações de capacidade e a crescente procura de IA.

Contudo, instalar refrigeração líquida não garante, por si só, maior eficiência. Os ganhos dependem de como são concebidos e operados os sistemas de energia, computação e refrigeração. Caudais, pressões, temperaturas e capacidade de rejeição de calor devem ser considerados em conjunto, para que a melhoria num componente não seja anulada por perdas noutro.

Uma diferença de temperatura (ΔT) adequada entre a entrada e a saída do fluido pode contribuir para otimizar a transferência de calor e a energia necessária à circulação. A questão decisiva não é escolher um equipamento isolado, mas assegurar o desempenho de toda a arquitetura.

A ÁGUA TAMBÉM CONTA

Avaliar a sustentabilidade exige olhar para além da eletricidade. O Water Usage Effectiveness (WUE) relaciona o consumo de água da instalação com a energia utilizada pelos equipamentos de TI e complementa a leitura proporcionada pelo PUE. Na refrigeração líquida direta ao chip, o fluido circula num circuito fechado e recolhe calor junto do processador. Isso não significa, porém, que toda a instalação deixe de consumir água: o consumo efetivo depende também da tecnologia utilizada para rejeitar o calor. Esta distinção é essencial para comparar soluções em diferentes condições climáticas e operacionais.

Em instalações adequadas, a refrigeração líquida pode ainda facilitar a reutilização do calor, criando oportunidades adicionais de aproveitamento energético.

À medida que a IA passa da experimentação para operações de maior escala, o desafio deixa de ser apenas disponibilizar mais potência. É assegurar que energia, refrigeração e computação são planeadas e geridas em conjunto, desde o projeto até à operação.

A eficiência dos Data Centers para IA não se resume, portanto, a reduzir o consumo: exige obter mais capacidade computacional útil por cada recurso utilizado, sem perder de vista os custos, a água e a sustentabilidade. É nessa visão integrada que a refrigeração líquida pode fazer a diferença. ■

POR OLIVER CRESPO,
Vendor and Channel Manager Iberia & LATAM da Zaltor

SUSTENTABILIDADE E EFICIÊNCIA DE TI:

DUAS PRIORIDADES DA ZALTOR PARA A EMPRESA DIGITAL

A sustentabilidade digital exige mais do que reduzir o consumo energético: implica utilizar melhor os recursos tecnológicos, garantir a continuidade operacional e proteger os acessos à informação. A Paessler e a TrustBuilder demonstram como a monitorização inteligente e a gestão segura de identidades podem contribuir para uma TI mais eficiente, resiliente e sustentável.

A TRANSFORMAÇÃO DIGITAL trouxe novas oportunidades às empresas, mas também aumentou a complexidade das infraestruturas, o consumo de recursos e os desafios de segurança. Neste contexto, a sustentabilidade e a eficiência de TI deixaram de ser objetivos isolados para se tornarem fatores estratégicos de competitividade.

Uma empresa digital sustentável não é apenas aquela que consome menos energia. É também aquela que utiliza melhor a sua infraestrutura, reduz desperdícios operacionais, evita interrupções e garante que as pessoas certas acedem aos recursos de que necessitam, de forma segura e simples.

MONITORIZAR PARA OTIMIZAR: A CONTRIBUIÇÃO DA PAESSLER

A eficiência começa pela visibilidade. Sem dados fiáveis sobre o desempenho e a utilização dos sistemas, torna-se difícil identificar desperdícios, antecipar falhas ou tomar decisões fundamentadas.

A Paessler, através da sua solução PRTG, permite monitorizar redes, servidores, aplicações, centros de dados e equipamentos de infraestrutura, incluindo métricas relacionadas com o consumo energético e as condições ambientais. Esta informação ajuda as equipas de TI a identificar anomalias, otimizar recursos e

A EFICIÊNCIA DIGITAL DEPENDE IGUALMENTE DE UMA GESTÃO ADEQUADA DAS IDENTIDADES E DOS ACESSOS. PROCESSOS DE AUTENTICAÇÃO COMPLEXOS, CREDENCIAIS COMPROMETIDAS E ADMINISTRAÇÕES DISPERSAS PODEM AUMENTAR O RISCO, GERAR CUSTOS E PREJUDICAR A EXPERIÊNCIA DOS UTILIZADORES.

antecipar problemas que poderiam comprometer a disponibilidade dos serviços.

Para além da continuidade operacional, a monitorização pode apoiar iniciativas de sustentabilidade: conhecer o consumo energético, acompanhar a utilização dos equipamentos e identificar oportunidades de otimização são passos importantes para uma gestão mais responsável da infraestrutura tecnológica.

Para os integradores e prestadores de serviços geridos, estas capacidades representam também uma oportunidade de negócio: desenvolver serviços de monitorização proativa, otimização de infraestruturas e acompanhamento contínuo do desempenho dos clientes.

PROTEGER IDENTIDADES, SIMPLIFICAR ACESSOS: O PAPEL DA TRUSTBUILDER

A eficiência digital depende igualmente de uma gestão adequada das identidades e dos acessos. Processos de autenticação complexos, credenciais comprometidas e administrações dispersas podem aumentar o risco, gerar custos e prejudicar a experiência dos utilizadores.

A TrustBuilder responde a estes desafios com soluções de gestão de acessos e autenticação multifator adaptativa, incluindo opções sem palavra-passe e sem necessidade de smartphone. A sua tecnologia permite adaptar os métodos de autenticação a diferentes perfis de utilizador e contextos, integrando-se com aplicações e infraestruturas existentes.

O resultado procurado é um equilíbrio entre segurança e simplicidade: proteger os recursos empresariais sem acrescentar fricção desnecessária ao trabalho diário. Uma gestão de acessos mais eficiente pode reduzir tarefas administrativas, facilitar a experiência dos utilizadores e reforçar a proteção da informação.

Para o canal tecnológico, estas soluções abrem oportunidades em projetos de modernização de acessos, segurança de aplicações e transformação digital, especialmente em organizações com requisitos exigentes de proteção e controlo.

A COLABORAÇÃO COMO MOTOR DE INOVAÇÃO

Foi com esta visão que, no passado dia 15 de outubro, a Zaltor reuniu em Lisboa cerca de 20 parceiros especializados, num encontro dedicado à partilha de experiências, tendências e novidades da Paessler e da TrustBuilder.

A sessão contou com a participação de Conchi García, EMEA South Channel da Paessler; Henrique Ribeiro, Account Manager – France & Iberia da TrustBuilder; e Maria João Paulino, Sales Manager da Zaltor em Portugal.

O encontro foi uma excelente oportunidade para aproximar fabricantes e parceiros, discutir desafios concretos dos clientes e explorar novas possibilidades de negócio. A participação e a qualidade da partilha fizeram deste momento uma experiência muito positiva, reforçando a importância de criar espaços de colaboração entre os diferentes intervenientes do ecossistema tecnológico.







- A Zaltor reuniu em Lisboa cerca de 20 parceiros especializados, com a participação da Paessler e da TrustBuilder, para partilhar experiências, conhecer novidades e explorar novas oportunidades de negócio -

UMA VISÃO INTEGRADA PARA A EMPRESA DIGITAL

A sustentabilidade e a eficiência de TI constroem-se através de decisões consistentes: monitorizar para compreender, otimizar para utilizar melhor os recursos e proteger para garantir a continuidade do negócio.

Na Zaltor, acreditamos que a tecnologia gera mais valor quando é acompanhada por conhecimento, proximidade e colaboração. Ao ligar soluções especializadas a parceiros capazes de as transformar em resultados, ajudamos as empresas a evoluir para operações mais eficientes, seguras e preparadas para o futuro. ■



"A CONTINUIDADE DE NEGÓCIO É UMA RESPONSABILIDADE DA CADEIA DE VALOR"

A continuidade de negócio não depende apenas da capacidade de recuperação de cada organização, mas também da resiliência dos seus fornecedores. No keynote de abertura da IT Insight Talks dedicada à continuidade de negócio, Henrique Carreiro, Diretor da IT Insight, alertou para os riscos das dependências invisíveis e para a necessidade de preparar a recuperação de toda a cadeia.

OS PLANOS DE CONTINUIDADE do negócio partem frequentemente de um pressuposto que se pode revelar errado: o de que, perante uma falha, os restantes elementos da cadeia vão continuar a funcionar. Foi esta uma das principais mensagens de Henrique Carreiro, Diretor da IT Insight, no *keynote* de abertura da IT Insight Talks dedicada à continuidade de negócio.

"A continuidade pertence à cadeia, é uma responsabilidade da cadeia e nós não estamos habituados a pensar nisso", afirmou, defendendo que as organizações devem olhar para além dos seus próprios sistemas e considerar as dependências que podem comprometer a recuperação da atividade.

Para ilustrar esta realidade, Henrique Carreiro apontou os ataques recentes no Japão, onde a forte interligação entre pequenas empresas tem contribuído para

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM



Fotografias: Rui Santos Jorge

ampliar o impacto dos incidentes. Num dos casos apresentados, um ataque de *ransomware* a um fornecedor cloud terá provocado a interrupção da atividade de 483 empresas.

Segundo o Diretor da IT Insight, este tipo de situação demonstra que as organizações nem sempre conhecem as dependências partilhadas pelos seus fornecedores. "É perceber se existem de facto redundâncias, se aquilo que pensamos que são redundâncias existem de facto", sublinhou.

AS DEPENDÊNCIAS QUE FICAM FORA DOS PLANOS

Um dos principais problemas identificados está na forma como as empresas avaliam os riscos associados à sua cadeia de fornecimento. Embora conheçam os fornecedores diretos, raramente analisam as dependências que existem nos níveis seguintes.

"Quando fazemos os mapas de dependências, normalmente vamos pensar em nós, nos nossos fornecedores. Mas e os fornecedores dos nossos fornecedores? Onde é que eles estão?", questionou. Esta falta de visibilidade pode comprometer estratégias de redundância aparentemente robustas. Duas empresas contratadas para assegurar o mesmo serviço podem, por exemplo, depender de uma infraestrutura comum, criando um ponto único de falha.

O responsável destacou ainda que os fornecedores mais críticos nem sempre são os maiores ou os mais conhecidos. Como exemplo, referiu um incidente envolvendo termóstatos utilizados por cadeias de supermercados em França, que terá provocado perdas de produtos refrigerados após a alteração remota das temperaturas.

Para Henrique Carreiro, estes exemplos mostram que a avaliação da continuidade deve abranger os diferentes níveis da cadeia e identificar dependências comuns, mesmo quando estão associadas a fornecedores aparentemente secundários.

RECUPERAR SISTEMAS NÃO SIGNIFICA RECUPERAR O NEGÓCIO

Outro dos temas centrais da intervenção foi a diferença entre os objetivos de recuperação definidos pelas organizações e a capacidade real de restabelecer os processos de negócio.

"O que quer que seja que se pense em termos de *Recovery Time Objective* é uma ficção se o parceiro de quem dependemos, se o fornecedor de quem dependemos, tiver um RTO maior", alertou.

Na prática, uma empresa pode estabelecer um objetivo de recuperação de cinco horas, mas continuar impossibilitada de retomar a atividade se um fornecedor essencial precisar de dez ou 24 horas para recuperar os seus serviços.

A definição das prioridades de recuperação também não deve ficar exclusivamente nas mãos das equipas tecnológicas. "A recuperação, ou a ordem de recuperação, o ritmo de recuperação, é uma decisão de negócio", afirmou.

Segundo o Diretor da IT Insight, decidir quais os processos, serviços ou operações que devem ser restabelecidos exige uma avaliação prévia das prioridades da organização. Caso contrário, estas decisões acabam por ser tomadas durante a crise, sob pressão e sem o necessário enquadramento de negócio.

A existência de *backup* também não garante, por si só, uma recuperação eficaz. Henrique Carreiro questionou a frequência com que os dados são validados, a segurança das cópias disponíveis e a capacidade de identificar um ponto de recuperação que não esteja comprometido.

O mesmo princípio aplica-se aos mecanismos alternativos de operação. "Se não foi testado, por exemplo, no último ano, quem é que nos garante que ele está lá?", questionou, referindo-se aos procedimentos de contingência.

Mesmo quando é possível recorrer a processos manuais, a recuperação não termina com o regresso dos sistemas. É necessário reconciliar a informação produzida durante a interrupção, uma tarefa que pode representar custos adicionais e introduzir erros na operação.

DA AUDITORIA À PREPARAÇÃO CONJUNTA

Na parte final do *keynote*, Henrique Carreiro defendeu que a continuidade do negócio exige uma maior coordenação entre organizações, começando por aspetos tão básicos como os contactos de emergência.

"Se o email estiver em baixo, se os sistemas de autenticação estiverem em baixo, quem é que vamos contactar e como?", questionou, salientando a importância de conhecer os contactos dos fornecedores e dispor de meios alternativos de comunicação.

O responsável considerou igualmente que as auditorias, embora relevantes, não substituem a realização de exercícios conjuntos que permitam testar a resposta de diferentes organizações perante um incidente.

Neste contexto, apontou a preparação militar como exemplo da importância dos exercícios conjuntos e questionou quem assume a responsabilidade de coordenar a recuperação quando vários elementos da cadeia são afetados simultaneamente.

"Quem é que pensa no total? Quem é que pensa na cadeia produtiva? E temos alguém a pensar em toda a cadeia que seja responsável pela recuperação da cadeia?", perguntou.

Para Henrique Carreiro, a evolução das ameaças obriga as organizações a repensar a forma como preparam a continuidade do negócio, deixando de olhar exclusivamente para os seus próprios sistemas e passando a considerar a capacidade de recuperação de todo o ecossistema de que dependem. ■

"A CONTINUIDADE É UMA DECISÃO DE TOPO"

A continuidade de negócio não pode ser encarada apenas como uma obrigação regulamentar. Na IT Insight Talks, Sérgio Trindade, CIO e CISO da Águas do Tejo Atlântico, defendeu uma abordagem integrada à resiliência, que começa na administração e passa pela capacidade de manter as operações mesmo quando a tecnologia falha.

A CONTINUIDADE de negócio deve ser uma preocupação transversal às organizações, independentemente da sua dimensão ou setor de atividade. Esta foi uma das mensagens deixadas por Sérgio Trindade, CIO e CISO da Águas do Tejo Atlântico, durante a sua keynote na IT Insight Talks, onde abordou os desafios de garantir a operação de serviços essenciais perante incidentes de grande escala. Para o responsável, o enquadramento regulamentar deve ser encarado como uma oportunidade para melhorar a resiliência das organizações, e não apenas como uma exigência de conformidade. "O grave problema quando falamos em planos de continuidade de negócio é que, na esmagadora maioria, olhamos para isto como uma obrigação", afirmou.

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM



Na sua perspetiva, referenciais como a NIS2 e a ISO 22301 podem funcionar como orientações para estruturar a resposta das empresas. “Em vez de partirmos de uma base zero, podemos partir desta e usá-la como espinha dorsal”, explicou.

A CONTINUIDADE COMEÇA NA ADMINISTRAÇÃO

Sérgio Trindade defendeu que a continuidade de negócio exige decisões estratégicas que não podem ficar exclusivamente nas mãos das equipas técnicas. Cabe à administração definir quais os processos críticos, os níveis de tolerância à interrupção, os responsáveis pela resposta e os investimentos necessários.

“Eu não vou correr atender quem gritou mais alto, quem reclamou mais, quem estava mais perto. Eu tenho de ir onde o valor da empresa se considera que é mais importante naquele momento”, exemplificou.

Estas prioridades devem ser estabelecidas antes de ocorrer um incidente, permitindo que as equipas atuem sem depender de autorizações que possam atrasar a resposta.

O responsável alertou também para a importância de ativar atempadamente os mecanismos de emergência. “Muitas das vezes uma das coisas que acontece é que demoramos demasiado a declarar emergência e quando a declaramos já estamos no buraco há demasiado tempo”.

A responsabilidade da gestão ganha particular relevância com a NIS2, que reforça o papel dos órgãos de administração na supervisão da cibersegurança e da continuidade de negócio. “Toda a gente, mas começa efetivamente e legalmente pela administração, tem que entender que esta é uma responsabilidade pessoal que agora assume”, sublinhou.

PREPARAR A ORGANIZAÇÃO PARA FALHAS SIMULTÂNEAS

A experiência do apagão ibérico e dos fenómenos meteorológicos extremos demonstrou a importância das interdependências entre serviços essenciais. No setor da água, uma falha elétrica pode comprometer os sistemas de bombagem e tratamento, enquanto a indisponibilidade das comunicações dificulta a coordenação das equipas.

Para Sérgio Trindade, a análise de risco deve concentrar-se não apenas nas causas dos incidentes, mas sobretudo nas suas consequências para a operação. “Quando eu vou planear, eu devo ter em conta o que é que eu vou fazer quando tudo falhar”, afirmou, defendendo que as organizações devem preparar respostas para a indisponibilidade de instalações, tecnologia, pessoas e fornecedores.

Esta preparação implica conhecer as dependências críticas e estabelecer mecanismos de coordenação que continuem a funcionar mesmo quando os canais habituais deixam de estar disponíveis.

RECUPERAR DADOS NÃO É O MESMO QUE GARANTIR RESILIÊNCIA

Na componente tecnológica, Sérgio Trindade distinguiu três conceitos que considera fundamentais para a continuidade de negócio: *backup*, recuperação de desastre e ciber-resiliência.

O responsável alertou que a existência de cópias de segurança e de infraestruturas redundantes não garante, por si só, a recuperação após um ciberataque. "Eu tive-o aqui e repliquei-o para lá", exemplificou, referindo-se ao risco de um ataque de *ransomware* comprometer também os sistemas de recuperação através dos mecanismos de replicação.

"Uma coisa é ter cópias, as cópias servem para recuperar dados perdidos. Outra coisa é um centro de recuperação de desastre", explicou, sublinhando que a recuperação de uma falha física não responde necessariamente às exigências de um incidente de cibersegurança.

Neste contexto, apresentou a utilização de ambientes de recuperação isolados, capazes de preservar informação e permitir a reconstrução dos sistemas críticos sem depender da infraestrutura comprometida.

Na Águas do Tejo Atlântico, referiu, existe um mecanismo de replicação para um ambiente isolado que permite intervalos de cinco a dez segundos entre réplicas. O objetivo é assegurar a recuperação dos sistemas essenciais mesmo quando a infraestrutura principal fica indisponível.

A IMPORTÂNCIA DE SABER OPERAR SEM TECNOLOGIA

Apesar dos investimentos em redundância e recuperação, Sérgio Trindade considera que a capacidade de operar manualmente continua a ser uma componente essencial da resiliência.

"Quanto mais digitalizamos e automatizamos, menos recursos humanos temos para fazer as coisas", alertou, reconhecendo que a operação manual de instalações de grande dimensão representa um desafio crescente.

Esta capacidade deve ser desenvolvida através de exercícios regulares, que permitam testar os procedimentos, identificar falhas e preparar as equipas para situações reais. "Não é só falar sobre o tema, não é só fazer exercícios em cima da mesa; é importante fazê-los funcionalmente", afirmou.

Para o CIO e CISO, estes exercícios são também fundamentais para demonstrar às administrações o valor dos investimentos em continuidade de negócio, frequentemente encarados como custos associados a situações que se espera nunca enfrentar.

A mensagem final passou pela necessidade de integrar a resiliência na gestão das organizações, evitando abordagens isoladas que aumentam os custos e dificultam a resposta. "Ao ter um sistema integrado não vale a pena pensar em ilhas, porque, se pensarmos em ilhas diferentes, vamos gastar o triplo e vamos necessitar de muito mais recursos", concluiu. ■

CONTINUIDADE DE NEGÓCIO: DA PREVENÇÃO À CAPACIDADE DE RESPOSTA

Perante ciberataques, falhas tecnológicas e outros incidentes capazes de interromper as operações, a continuidade de negócio tornou-se numa prioridade para as organizações. IP Telecom, NetApp, Ricoh, VisionWare e Zscaler partilham a sua visão sobre o mercado de continuidade de negócio.

RUI DAMIÃO

GARANTIR A CONTINUIDADE de negócio vai muito além de proteger os sistemas informáticos ou ter planos de recuperação. É necessário identificar os processos críticos, compreender as dependências tecnológicas e operacionais e preparar toda a organização para responder a situações de crise. Num contexto em que as interrupções podem ter consequências financeiras, operacionais e reputacionais, a capacidade de recuperação assume um papel central na resiliência das empresas. Numa mesa-redonda dedicada à continuidade de negócio, a IT Insight reuniu especialistas para debater os principais desafios das organizações, as estratégias de prevenção e recuperação e o papel da tecnologia na manutenção das operações perante situações inesperadas.

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM



MUITAS ORGANIZAÇÕES JÁ NÃO QUEREM APENAS RECUPERAR DEPRESSA: QUEREM CONTINUAR A FUNCIONAR DURANTE O INCIDENTE. NOS VOSSOS CLIENTES, O QUE DISTINGUE AS QUE CONSEGUEM DAS QUE NÃO CONSEGUEM?



- José Carlos Gonçalves, IP Telecom -

José Carlos Gonçalves, CISO, IP Telecom: "Quem sobrevive hoje é quem testa, treina e quer manter o negócio operacional. Podemos ter técnicos muito bons, mas sem testes e simulações – do pior cenário possível – não é possível recuperar os sistemas e os dados com a velocidade necessária para o negócio"

> "HÁ UM AUMENTO DA CARGA PROCESSUAL, MAS HÁ TAMBÉM UMA PROCURA DE SOLUÇÕES PARA MITIGAR OS PROBLEMAS DE SEGURANÇA"
>
> JOSÉ CARLOS GONÇALVES, CISO, IP TELECOM

Henrique Silva, Senior Client Executive, NetApp: "Quando nos relacionamos com cibersegurança, a situação é mais complexa. Podemos ter uma infraestrutura que disponibiliza os dados, mas precisamos de ter a certeza de que ela está ativa em segurança. Temos de garantir as aplicações e as interligações dessas aplicações para recuperar os dados. As empresas mais resilientes são aquelas que testam, que identificam as suas aplicações críticas e que viram e analisaram as suas dependências"



- Bruno Castro, VisionWare -

Bruno Castro, Founder & CEO, VisionWare: "Antigamente, o mundo digital estava nas catacumbas e não se queria saber da continuidade. Depois, até por questões como a NIS2 e cibercrime, há a ideia de que um dia vai acontecer a mim e a pergunta que se coloca é se consigo recuperar e continuar a operar. Temos de conhecer muito bem o que é efetivamente crítico para que não existam dúvidas num momento de crise"

> "HÁ PEÇAS NO PUZZLE QUE JÁ NINGUÉM DÁ MUITA IMPORTÂNCIA, MAS QUANDO DEIXAM DE FUNCIONAR FAZEM UM EFEITO DOMINÓ VIOLENTO NA ORGANIZAÇÃO"
>
> BRUNO CASTRO, FOUNDER & CEO, VISIONWARE

Nuno Rodrigues, Senior Sales Engineer, Zscaler: "Hoje, já percebemos que não é uma questão de se, mas sim quando vamos ser atacados e temos de nos preparar para isso. Temos de trazer para os clientes os mecanismos e infraestruturas que fogem um pouco do tradicional para, quando o incidente acontece, a operação continue a operar com o mínimo de estrago possível e não se espalhe para toda a infraestrutura da empresa"



OS SISTEMAS PODEM ESTAR TODOS DE VOLTA E O NEGÓCIO CONTINUAR PARADO. NOS INCIDENTES QUE ACOMPANHARAM, O QUE É QUE COSTUMA FICAR PARA TRÁS QUANDO A TECNOLOGIA JÁ RECUPEROU?

Marco Raposo, Head of Cybersecurity, Ricoh: "Fica o próprio negócio. Ao que temos assistido, na quase totalidade dos casos, o negócio não recupera na totalidade. Muitas vezes é a confiança, que é base de muitos negócios e de relacionamento entre parceiros. Falamos muitas vezes da continuidade de negócio como um tema tecnológico, mas não é. É um conjunto de decisões que têm de ser tomadas para que o negócio não pare, ou que tenha o mínimo de impacto possível, mas suportado com a tecnologia"



CADA VEZ MAIS PROCESSOS DEPENDEM DE MODELOS E DE SERVIÇOS EXTERNOS DE INTELIGÊNCIA ARTIFICIAL (IA). JÁ VIRAM UM CLIENTE SENTIR NA OPERAÇÃO A FALHA DE UM DESSES SERVIÇOS, OU RESULTADOS EM QUE DEIXOU DE PODER CONFIAR? O QUE MUDOU DEPOIS?

Nuno Rodrigues, Zscaler: "Estamos numa fase em que a informação e o resultado que a IA nos devolve é mais impactante do que a falha do serviço. As empresas ainda não estão dependentes da falha da IA, mas sim da confiança que o sistema nos devolve. No futuro, se calhar com uma maior integração, isso vai inverter e as organizações vão estar mais dependentes da não falha do serviço porque a informação é mais confiável. Estamos, no entanto, ainda numa fase embrionária desta adoção"



- Nuno Rodrigues, Zscaler -

> "TEMOS DE COLOCAR O SISTEMA A FUNCIONAR E ABREM-SE EXCEÇÕES QUE DEPOIS FICAM ABERTAS. ISSO PODE TER DE ACONTECER, MAS ESSAS EXCEÇÕES TÊM DE SER MUITO BEM DOCUMENTADAS PARA DEPOIS A RETIRAR"
>
> NUNO RODRIGUES, SENIOR SALES ENGINEER, ZSCALER



AS ORGANIZAÇÕES CONTROLAM CADA VEZ MENOS A CADEIA TECNOLÓGICA DE QUE DEPENDEM. QUANDO UM CLIENTE VOSSO TEM UM INCIDENTE GRAVE, O QUE COSTUMA FALHAR PRIMEIRO QUE NINGUÉM TINHA PREVISTO?

Bruno Castro, VisionWare: "Geralmente, o que falha não é o conhecimento da tecnologia interna porque já se conhece bem o que se tem. O que temos sentido é que o que falha são as dependências que ninguém vê e que, com o tempo, ninguém controla. Há peças no puzzle que já ninguém dá muita importância, mas quando deixam de funcionar fazem um efeito dominó violento na organização. É muito difícil, atualmente, ter controlo total de toda a infraestrutura e de tudo o que se usa. O mundo digital é cada vez mais complexo e as dependências invisíveis começam a aparecer"

A NIS2 E A DORA LEVARAM A RESILIÊNCIA ATÉ À ADMINISTRAÇÃO. NAS CONVERSAS COM OS VOSSOS CLIENTES, JÁ VEEM DECISÕES DE NEGÓCIO DIFERENTES POR CAUSA DISSO, OU SOBRETUDO MAIS DOCUMENTAÇÃO?

Marco Raposo, Ricoh: "Estamos numa fase de *compliance* sintética, ou seja, a maioria das organizações que tem de cumprir a NIS2 foi às formações e, agora, vão a sistemas de IA generativa e produzem a *compliance* sintética. A resposta acaba por ser um '*nim*', porque o objetivo da *compliance* é aumentar a capacidade de resiliência das organizações, especificamente no domínio digital. Diria que cerca de 95% das organizações que têm de cumprir a NIS2 ainda não têm o tema endereçado e ainda não chegou a ser um tema de negócio"



José Carlos Gonçalves, IP Telecom: "Há um aumento da carga processual, mas há também uma procura de soluções para mitigar os problemas de segurança. Mais do que estar focado na NIS2 ou DORA, é ter a capacidade de resiliência. Há clientes que telefonam a dizer que não estão abrangidos, mas perguntam como podem aumentar a sua resiliência. Há quem esteja simplesmente a criar papel para estar conforme"



- Henrique Silva, NetApp -

Henrique Silva, NetApp: "O que estamos a constatar é que os nossos interlocutores estão a mudar. Antes seriam de infraestrutura e agora são as equipas de segurança e eventualmente são envolvidas as áreas de negócio. Há uma necessidade de escrever essa papelada, mas verificamos que os clientes que estão ao abrigo da NIS2 e também aqueles que, não estando abrangidos, se relacionam com essas entidades e querem estar num elevado nível de conformidade. Vemos uma necessidade de testar, não só tecnológico, mas ao negócio como um todo"

> "TEMOS DE IMPLEMENTAR MECANISMOS DE IDENTIFICAÇÃO QUE, EM CONJUNTO COM OUTROS MECANISMOS, NOS PERMITE PROTEGER DO DESCONHECIDO E CONSEGUIR PERCEBER COMPORTAMENTOS ANÓMALOS"
>
> HENRIQUE SILVA, SENIOR CLIENT EXECUTIVE, NETAPP



DURANTE UM CIBERATAQUE, A SEGURANÇA PODE QUERER ISOLAR SISTEMAS QUE A OPERAÇÃO PRECISA DE MANTER A FUNCIONAR. NOS CASOS QUE ACOMPANHARAM, QUEM ACABOU POR DECIDIR E ESSA DECISÃO ESTAVA TOMADA ANTES DO INCIDENTE?

José Carlos Gonçalves, IP Telecom: "Falando como CISO, a minha preocupação de segurança pode ser contraproducente com o que está a acontecer. Por exemplo: na saúde, não posso bloquear porque isso pode significar a vida ou a morte de alguém. Tem de existir alguém de cima a decidir; é a gestão de topo que decide o que vai orientar a decisão, como por exemplo segregar uma infraestrutura para continuar a operar. Isto tem de ser previamente preparado pela gestão de topo"

A AUTENTICAÇÃO É A PORTA DE ENTRADA PARA QUASE TUDO. QUANDO FALHA NUM CLIENTE, O QUE VEEM ACONTECER: A OPERAÇÃO PARA OU ABREM-SE EXCEÇÕES QUE DEPOIS FICAM ABERTAS?

Nuno Rodrigues, Zscaler: "É um clássico. Temos de colocar o sistema a funcionar e abrem-se exceções que depois ficam abertas. Isso pode ter de acontecer, mas essas exceções têm de ser muito bem documentadas para depois as retirar. O utilizador autenticado não pode ser uma porta aberta para a infraestrutura. Também é preciso analisar a localização e o comportamento. Isso deve ter um *score* dinâmico que vá analisando o que o utilizador está a fazer para permitir ou não o acesso às aplicações"

A RESPOSTA A INCIDENTES DEPENDE DA MONITORIZAÇÃO, DOS REGISTOS E DOS ALERTAS. JÁ VIRAM CASOS EM QUE A AUSÊNCIA DE ALERTAS ESCONDIA UM PROBLEMA? COMO SE PERCEBE A DIFERENÇA A TEMPO?

Henrique Silva, NetApp: "Somos uma parte do puzzle e uma parte importante porque estamos nas infraestruturas. Temos um papel fundamental na monitorização e, como tal, temos de implementar mecanismos de monitorização. A ausência de alertas não significa ausência de problemas; o problema pode já estar lá. O que temos é ausência de visibilidade. Temos de implementar mecanismos de identificação que, em conjunto com outros mecanismos, nos permitam proteger do desconhecido e conseguir perceber comportamentos anómalos"

Bruno Castro, VisionWare: "Infelizmente, sim. Os pressupostos base são dois: garantir que o SOC está a funcionar, seja qual for o fabricante, e consegue cobrir todo o ambiente digital da organização; depois, é a qualidade dos dados. Quando recolho evidências – e já se consegue processar milhões de registos por segundo – é preciso perceber o que aparece nos monitores. Ter um serviço de SOC não dá, por si só, segurança a ninguém; só dá se estiver bem montado"





- Marco Raposo, Ricoh -

Marco Raposo, Ricoh: "Temos de monitorizar e monitorização. O processo de monitorização é um processo em si próprio com diferentes níveis de maturidade, que vai crescer dentro da própria organização. Nunca vai crescer a 100% porque estamos a falar de milhares de milhões de *logs* que vão ser registados por dia. Os atacantes têm todo o tempo do mundo e nós não podemos falhar porque quando falharmos vamos ter um impacto que pode ser muito grande e custar muito dinheiro"

> "HÁ PONTOS DE PREOCUPAÇÃO QUE TEMOS DE ENDEREÇAR. UM DELES É A DEPENDÊNCIA DE SERVIÇOS E SISTEMAS DE CLOUD QUE NÃO ESTÃO NA UNIÃO EUROPEIA"
>
> MARCO RAPOSO, HEAD OF CYBERSECURITY, RICOH

QUE DEPENDÊNCIA TECNOLÓGICA OU SERVIÇOS LEGADOS VOS PREOCUPA MAIS NOS PRÓXIMOS TRÊS A CINCO ANOS?

Bruno Castro, VisionWare: "A dependência da tecnologia já não é um tema porque todos dependemos da tecnologia de alguma maneira. O que realmente me preocupa é aquela tecnologia que não controlamos, não conhecemos ou não vemos e aquelas que não compreendemos. Já a pensar num futuro a médio prazo, preocupa-me a perda de capacidade de entender porque é que estamos a falhar por causa da complexidade envolvida"

Henrique Silva, NetApp: "O tema bate sempre na IA e todos estão preocupados com a inteligência artificial. A mim preocupa-me tudo o que está relacionado com IA. Não consigo viver sem a IA porque se não será menos produtivo, mas quando falamos de IA falamos do passado, não do futuro. Também a velocidade que temos para reagir é cada vez menor, até por tudo estar conectado"

José Carlos Gonçalves, IP Telecom: "É complicado identificar um, mas, ao fazê-lo, é ter dependências de um único sistema, um único fabricante, algo que é único. O *shadow IT* ou *shadow AI* é algo que não conhecemos e não conseguimos controlar"

Marco Raposo, Ricoh: "Há pontos de preocupação que temos de endereçar. Um deles é a dependência de serviços e sistemas de cloud que não estão na União Europeia. Temos uma dependência grande das infraestruturas, mas há temas que podemos endereçar, como a cloud ou a identidade, e podem ser mais resilientes"

Nuno Rodrigues, Zscaler: "Vamos continuar a ver nos próximos tempos uma preocupação muito grande com a inteligência artificial, não só a evolução, mas também a sua economia. Também me incomoda a preocupação com a inteligência artificial quando estamos a descurar temas simples que já são problemas há muito tempo que não são endereçados pelas organizações" ■



IP Telecom

POR FILIPE FRASQUILHO,
Diretor de Serviços TI, IP Telecom

CONTINUIDADE DE NEGÓCIO NO CONTEXTO DE SOBERANIA DIGITAL

Face à evolução dos requisitos associados à Soberania Digital, nomeadamente no contexto da NIS2, DORA e Cyber Resilience Act, bem como ao desenvolvimento de iniciativas de Cloud Soberana, o Plano de Continuidade de Negócio (PCN) deve evoluir de uma lógica predominantemente orientada para a recuperação tecnológica para um modelo de Resiliência Soberana.

NESTE MODELO, o objetivo deixa de ser apenas recuperar sistemas e dados após uma disrupção, passando a assegurar a continuidade das funções críticas e da missão da organização, mesmo perante eventos cibernéticos, geopolíticos ou regulatórios, indisponibilidade prolongada de fornecedores estratégicos ou ruturas nas cadeias de abastecimento.

A Resiliência Soberana pressupõe, assim, que a organização mantenha controlo efetivo sobre os ativos, dados, competências, infraestruturas e dependências críticas necessárias à continuidade da sua missão, reduzindo dependências tecnológicas ou jurisdicionais excessivas e garantindo capacidade real de recuperação, substituição e operação em cenários adversos.

Assim, a Continuidade de Negócio (CN) deixou de ser encarada apenas como um conjunto de planos ou mecanismos de resposta, passando a integrar uma abordagem mais ampla de resiliência



- Filipe Frasquilho -
Diretor de Serviços TI

organizacional, no qual o PCN é um elemento estruturante dessa resiliência, permitindo às organizações avaliar de forma integrada a sua exposição a riscos geopolíticos, climáticos, tecnológicos e humanos, incluindo os associados à utilização da Inteligência Artificial (IA).

Num contexto de risco crescente e de interdependência sistémica, torna-se essencial priorizar os riscos e, sobretudo, as dependências críticas que podem comprometer a autonomia operacional da organização. O PCN deve pois evoluir de um instrumento predominantemente orientado para a conformidade e recuperação, para um pilar da Resiliência Soberana, destinado a preservar as funções críticas, o controlo sobre recursos essenciais e a continuidade da missão mesmo perante disrupções severas.

A antecipação tornou-se o princípio central de um PCN robusto. Num ambiente de crescente imprevisibilidade, a eficiência evolui para resiliência e redundância, o fornecedor único para diversificação, a cibersegurança defensiva para resiliência ativa apoiada pela IA e o planeamento estático para simulações dinâmicas.

As cadeias de abastecimento são hoje uma dimensão crítica da resiliência. A eficiência máxima do just-in-time dá lugar a modelos que valorizam redundância, diversificação e confiança, reduzindo dependências suscetíveis de comprometer a continuidade da missão. A antecipação, adaptação, testes, confiança e redução de dependências são pois fatores críticos para o sucesso.

Esta evolução exige PCN dinâmicos, processos robustos, sistemas resilientes, pessoas preparadas, testes regulares e parceiros de confiança, capazes de assegurar a continuidade da missão perante cenários de disrupção.

Ou seja, as organizações devem desenvolver PCN dinâmicos e adaptativos, suportados por processos robustos, sistemas resilientes e pessoas preparadas para atuar em cenários de instabilidade e disrupção. As organizações que invistam consistentemente na CN e realizem testes regulares e dinâmicos estarão mais preparadas para responder a disrupções e minimizar os seus impactos. Neste contexto, a escolha de parceiros de confiança, capazes de assegurar a fiabilidade e resiliência dos serviços, torna-se igualmente determinante.

A IP Telecom afirma-se como parceiro tecnológico de confiança, apoiando as organizações na construção de soluções que reforçam a resiliência, a soberania e a continuidade do negócio, através da antecipação, integração de processos, gestão estratégica de novos riscos e pessoas, numa lógica de verdadeira parceria. ■

NetApp

CONTINUIDADE DE NEGÓCIO NA ERA DIGITAL: DA RECUPERAÇÃO À RESILIÊNCIA

Durante muitos anos, a continuidade de negócio foi encarada como um seguro: algo que esperávamos nunca utilizar, mas que existia para nos ajudar a recuperar depois de uma crise. Hoje, essa visão já não é suficiente.

VIVEMOS NUMA ERA em que a disrupção faz parte do quotidiano. Ciberataques, ransomware, falhas tecnológicas, erros humanos, interrupções operacionais e incerteza geopolítica são realidades permanentes. A questão deixou de ser se uma organização enfrentará uma crise. A verdadeira questão é quando acontecerá e quão preparada estará para responder.

Ao longo da minha experiência profissional, tenho observado uma mudança clara na forma como as organizações encaram este desafio. A continuidade de negócio deixou de ser um tema exclusivamente técnico, discutido entre equipas de IT, para se tornar uma prioridade estratégica ao nível da gestão de topo. E faz todo o sentido. Num mundo digital, proteger a informação é proteger a capacidade de operar, servir clientes, gerar receitas e manter a confiança do mercado.

A transformação digital trouxe benefícios extraordinários, mas também criou novos níveis de dependência. Hoje, praticamente tudo depende de dados. Desde serviços financeiros a processos industriais, passando pelos cuidados de saúde, administração pública ou projetos de inteligência artificial, os dados são o combustível que alimenta a economia moderna.

Quando os dados deixam de estar disponíveis, o negócio deixa de funcionar. Paralelamente, as ameaças tornaram-se mais sofisticadas. Os grupos de ransomware já não se limitam a bloquear informação. Procuram comprometer

sistemas de backup, exfiltrar dados sensíveis e dificultar qualquer tentativa de recuperação. Muitas organizações descobrem, demasiado tarde, que os seus planos foram concebidos para lidar com falhas tecnológicas e não com ataques intencionais e altamente coordenados.

Perante esta realidade, a continuidade de negócio não pode assentar apenas em backups. É necessária uma abordagem mais abrangente, que combine proteção de dados, cibersegurança, monitorização contínua, deteção de ameaças e recuperação rápida. Em suma, precisamos de falar cada vez menos de recuperação e cada vez mais de resiliência.

Para mim, resiliência significa algo muito simples: garantir que a organização continua a cumprir a sua missão mesmo quando acontece o inesperado. Significa reduzir o impacto de uma disrupção, acelerar a recuperação e preservar a confiança de clientes, parceiros e cidadãos.

Esta capacidade começa pela visibilidade. É impossível proteger aquilo que não conhecemos. As organizações precisam de saber onde estão os seus dados, quem lhes acede, quais são críticos para o negócio e quais os riscos associados.

Outro elemento fundamental é a imutabilidade dos dados. Num cenário em que os atacantes procuram destruir evidências e comprometer cópias de segurança, ter informação que não pode ser alterada ou eliminada tornou-se uma das mais importantes linhas de defesa. Quando combinada com inteligência na deteção de ameaças e com processos automatizados de recuperação, esta abordagem pode reduzir drasticamente o impacto de um incidente.

A pressão regulatória reforça esta necessidade. Normas e diretivas como a NIS2 deixam claro que a resiliência operacional já não é apenas uma boa prática. É uma responsabilidade de gestão. As organizações têm de demonstrar não apenas que investem em prevenção, mas que conseguem responder, recuperar e manter serviços críticos durante uma crise.

A inteligência artificial acrescenta uma nova camada de complexidade. Quanto mais dependemos da IA para acelerar decisões e gerar valor, mais importante se torna garantir que os dados que a alimentam são seguros, íntegros e disponíveis. Sem confiança nos dados, não existe confiança nos resultados.

Por isso, acredito que a continuidade de negócio deve ser encarada como uma capacidade estratégica e não como um projeto tecnológico. Exige alinhamento entre liderança, operações, segurança e gestão de risco. Exige preparação, disciplina e investimento contínuo.

Num mundo cada vez mais incerto, a vantagem competitiva não estará apenas nas organizações que inovam mais depressa. Estará também nas que conseguem resistir melhor. Porque a maturidade digital mede-se menos pela ausência de crises e mais pela capacidade de continuar a avançar quando elas inevitavelmente acontecem. ■

VisionWare since 2005

POR BRUNO CASTRO,
Fundador & CEO da VisionWare.
Especialista em Cibersegurança e Análise Forense

A NOSSA SEGURANÇA ACABA ONDE COMEÇA A DEPENDÊNCIA?

Uma organização pode ter os seus sistemas protegidos, equipas especializadas e monitorização permanente e, ainda assim, estar vulnerável através de uma empresa que nem sequer faz parte da sua estrutura.

BASTA UMA CREDENCIAL exposta num fornecedor, uma ferramenta comprometida ou um acesso privilegiado esquecido para transformar uma relação de confiança numa porta de entrada para um atacante.

Em março de 2026, um incidente que afetou a infraestrutura digital da Comissão Europeia voltou a demonstrar esta realidade. A investigação técnica da CERT-EU apontou para um comprometimento da cadeia de fornecimento de software associado à ferramenta Trivy, utilizada no desenvolvimento e na análise de segurança de aplicações. Os atacantes conseguiram obter credenciais que permitiram aceder a uma conta na infraestrutura cloud da Comissão, de onde foram extraídos cerca de 91,7GB de dados. O caso ilustra como uma vulnerabilidade na cadeia tecnológica pode permitir alcançar informação alojada noutro ambiente, sem que o ataque tenha necessariamente de começar nos sistemas da entidade afetada.



- Bruno Castro -
Fundador & CEO da VisionWare. Especialista em Cibersegurança e Análise Forense

É precisamente este o problema das dependências invisíveis, ou seja, a organização que se pretende atingir nem sempre é aquela que o atacante precisa de comprometer primeiro.

Durante demasiado tempo, a cibersegurança foi pensada a partir das fronteiras de cada organização: os seus equipamentos, colaboradores, aplicações e mecanismos de defesa. Essa visão é hoje, insuficiente. As empresas dependem de fornecedores de software, plataformas cloud, prestadores de serviços geridos, empresas de marketing, manutenção e parceiros que tratam dados ou dispõem de acessos privilegiados. E cada um destes intervenientes pode, por sua vez, depender de outras entidades, criando uma cadeia de relações cuja extensão nem sempre é conhecida por quem está na sua origem.

Para um atacante, esta interdependência representa uma oportunidade. Imagine-se, em vez de tentar ultrapassar as defesas de uma organização bem protegida, poder procurar um fornecedor com menos recursos ou explorar uma ferramenta amplamente utilizada para alcançar vários alvos. Quanto maior for o alcance desse fornecedor e mais privilegiados forem os seus acessos, maior poderá ser o impacto de um único incidente.

E, infelizmente, o problema não se limita ao roubo de informação. Uma intrusão pode permitir recolher credenciais, identificar sistemas, conhecer a arquitetura tecnológica de uma organização ou preparar novos ataques. Se pensarmos em alvos políticos ou parceiros dos mesmos, o impacto pode inclusive escalar para acesso a segredos de Estado e operações de ciberespionagem e influência. Além disso, quando estas dependências sustentam setores como a energia, as telecomunicações, a saúde, os transportes ou a banca, as consequências podem ultrapassar largamente os limites de uma empresa. Dados aparentemente secundários, quando cruzados com outras fontes, podem revelar relações, rotinas e fragilidades que facilitam tudo isto.

Perante este cenário, a pergunta já não pode ser apenas se os nossos sistemas estão seguros. Temos de saber de que sistemas dependemos, que dados partilhamos, que acessos concedemos e o que aconteceria se um fornecedor crítico deixasse de conseguir prestar o seu serviço.

A resposta começa por mapear as dependências e avaliar o risco de acordo com o grau de criticidade de cada relação. Nenhuma empresa tem visibilidade absoluta sobre todas as dependências dos seus parceiros. Reconhecer esta limitação não significa aceitar o risco passivamente, significa sim, geri-lo com maior rigor, estabelecer prioridades e agir sobre aquilo que podemos efetivamente controlar. A cibersegurança não termina na fronteira de uma organização: constrói-se através de todo o ecossistema de que ela depende. E fazer tudo o que está ao nosso alcance para o proteger deixou de ser apenas uma boa prática, sendo antes uma responsabilidade partilhada. ■

BUSINESS CONTINUITY SEM FRONTEIRAS, A RESILIÊNCIA JÁ NÃO SE DECIDE APENAS DENTRO DA EMPRESA

Num ecossistema digital cada vez mais distribuído, a continuidade do negócio depende da capacidade de reduzir exposição, conter disrupções e reforçar a resiliência operacional.

A CONTINUIDADE do negócio deixou de ser um tema reservado aos planos de contingência e aos exercícios de recuperação. É hoje uma prioridade de gestão, diretamente ligada à operação, à confiança dos clientes e à capacidade de resposta das empresas perante incidentes, disrupções e mudanças rápidas de contexto.

Durante anos, a resposta passou por reforçar perímetros, criar redundâncias e preparar cenários de falha dentro da própria organização. Mas essa leitura já não acompanha a realidade. As empresas operam cada vez mais apoiadas em fornecedores, equipas externas, aplicações SaaS, infraestruturas cloud e serviços digitais distribuídos. Em muitos casos, uma parte crítica da operação depende de entidades que estão fora do controlo direto da organização.



A CONTINUIDADE JÁ NÃO VIVE SÓ DENTRO DA EMPRESA

Essa mudança alterou também a natureza do risco. Uma indisponibilidade num fornecedor crítico, um incidente de segurança num parceiro com acesso privilegiado ou uma falha num serviço cloud podem ter impacto imediato na produtividade, na prestação de serviços e na experiência do cliente. A continuidade já não se mede apenas pela solidez dos sistemas internos, mas pela capacidade de limitar o efeito de propagação de problemas que começam fora de portas.

É neste contexto que a ciber-resiliência ganha um novo peso no debate sobre business continuity. Não apenas como mecanismo de defesa, mas como condição para garantir que a operação se mantém funcional mesmo em cenários adversos. Reduzir a superfície de ataque, conter incidentes e impedir movimentos laterais deixaram de ser apenas objetivos de segurança. São hoje fatores centrais de resiliência operacional.

Também por isso o modelo Zero Trust tem vindo a ganhar relevância. Ao substituir a confiança implícita por verificação contínua, segmentação e acesso mínimo necessário, esta abordagem responde de forma mais eficaz a ambientes distribuídos e dinâmicos. Em vez de prolongar a rede até utilizadores, parceiros ou prestadores externos, o objetivo passa por ligar cada entidade apenas às aplicações e dados de que realmente necessita, com contexto e controlo granular.

ZERO TRUST REDUZ EXPOSIÇÃO E LIMITA IMPACTO

A Zscaler posiciona-se precisamente neste ponto de viragem. A empresa defende que a continuidade do negócio, num contexto digital, depende da capacidade de modernizar a arquitetura de segurança e abandonar modelos legados centrados na rede. Numa altura em que muitas organizações continuam a depender de VPNs, firewalls e acessos amplos, a proposta da Zscaler passa por uma abordagem cloud-native assente em Zero Trust.

Na prática, soluções como o Zscaler Private Access (ZPA) permitem substituir modelos tradicionais de acesso remoto, assegurando ligação segura a aplicações privadas sem expor a rede interna. Já o Zscaler Internet Access (ZIA) reforça o controlo e a proteção no acesso à Internet e a aplicações SaaS, enquanto o Zscaler Digital Experience (ZDX) acrescenta visibilidade sobre a experiência real dos utilizadores, ajudando a detetar rapidamente a origem de uma degradação ou interrupção de serviço.

Num debate sobre business continuity, esta visibilidade é particularmente relevante. Nem sempre a disrupção resulta de um ataque direto. Muitas vezes, o problema está numa dependência externa, numa falha de serviço ou num ponto de estrangulamento que só se torna evidente quando já está a afetar a operação. A capacidade de identificar rapidamente a origem do problema e agir com base em dados concretos passou a ser decisiva para reduzir tempos de paragem.

Outro ponto crítico é o controlo sobre os dados. Num ambiente em que a informação circula entre múltiplas plataformas, equipas e parceiros, a resiliência também depende da capacidade de limitar a exposição. Não basta definir quem pode aceder; importa também restringir o que pode ser visto, partilhado ou transferido. As capacidades de Data Protection da Zscaler respondem a esta necessidade com políticas granulares que ajudam a reduzir risco sem comprometer a colaboração.

A ZSCALER LIGA SEGURANÇA À CONTINUIDADE OPERACIONAL

A discussão sobre continuidade está, assim, a evoluir. Já não se trata apenas de recuperar depois de uma falha, mas de desenhar operações com menor dependência de confiança implícita, maior capacidade de contenção e mais visibilidade sobre todo o ecossistema digital. Num contexto marcado por cadeias de valor mais distribuídas, maior pressão regulatória e uma adoção crescente de cloud e IA, a continuidade do negócio exige uma abordagem mais ampla, integrada e adaptada à realidade atual.

Se há uma ideia que hoje se impõe é esta: a resiliência já não se constrói apenas dentro da empresa. Constrói-se na forma como a organização gere as suas ligações ao exterior. E é nesse terreno que a Zscaler procura responder a uma necessidade cada vez mais evidente no mercado: transformar segurança moderna em continuidade efetiva do negócio.



SOBRE A ZSCALER

A Zscaler (NASDAQ: ZS) posiciona a sua oferta na aceleração da transformação digital, com o objetivo de tornar as organizações mais ágeis, eficientes, resilientes e seguras. A plataforma Zscaler Zero Trust Exchange™ é apresentada como uma infraestrutura de ligação segura entre utilizadores, dispositivos e aplicações, com presença distribuída por mais de 150 centros de dados em todo o mundo. ■

CARLOS MIRANDA, DIRETOR DE SISTEMAS DE INFORMAÇÃO DO ESTORIL-SOL



"RECUPERAR A CONFIANÇA É UM PROCESSO MUITO MAIS LONGO"

Na IT Insight Talks de novembro de 2026, Carlos Miranda, Diretor de Sistemas de Informação do Estoril-Sol, foi o entrevistado e explicou por que motivo a continuidade de negócio não depende apenas da redundância tecnológica e backups.

RUI DAMIÃO

NUM CASINO, O QUE SIGNIFICA NA PRÁTICA "PARAR"? QUANTO TEMPO ATÉ UMA FALHA DE SISTEMAS SER SENTIDA PELO CLIENTE NA SALA E NO ONLINE E O QUE SE PERDE PRIMEIRO: RECEITA, CONFORMIDADE OU CONFIANÇA?

Parar nos casinos, mediante aquelas que são as características do negócio, pode representar diferentes realidades. Num casino online, onde os processos são praticamente todos digitais, obviamente que o impacto pode ser mais imediato e mais fácil de identificar. No offline, ou naquele que é o casino físico, poderá haver processos que param e que sejam completamente transparentes para o cliente e que eles nem sequer sintam aquilo que aconteceu na operação. Tendo isto em consideração, a questão de parar pode ter impactos diferentes nestas realidades.

Relativamente às três dimensões, obviamente que é muito fácil quantificar, ou é mais fácil quantificar quando tem um impacto na receita. A conformidade nós não a podemos relativizar porque somos regulados e, portanto, temos *compliance* para cumprir, para continuar a operar. Acho que aqui, efetivamente, e se calhar acaba por ser um bocadinho transversal a todas as organizações, a confiança sim, essa é que é a complexidade, porque nós podemos recuperar muito rapidamente a nível tecnológico os sistemas, mas recuperar a confiança é um processo muito mais demorado e muito mais longo.

ANTES, O RISCO ERA UMA TEMPESTADE OU UM CORTE DE ENERGIA; HOJE É CADA VEZ MAIS TECNOLÓGICO. CONCORDA OU CONTINUAMOS A SUBESTIMAR OS RISCOS CLÁSSICOS? O APAGÃO DE ABRIL DE 2025 NA PENÍNSULA IBÉRICA FOI UM AVISO QUE FICOU ESQUECIDO?

Muitas vezes, estamos muito concentrados naqueles que são os riscos tecnológicos, sejam eles ataques de cibersegurança, ransomware e tudo o que

> “AS ÁREAS DE NEGÓCIO SABERÃO MELHOR DO QUE NINGUÉM O IMPACTO E AQUILO QUE PRECISAM QUANDO EXISTE A POSSIBILIDADE DE UMA FALHA”

isso representa, e depois num bem tão essencial e tão simples, mas que tem um impacto muito significativo, acabamos muitas vezes por não ter isso em consideração ou não ter sempre em mente naquilo que é o nosso plano.

Pegando aqui no exemplo dos casinos, por exemplo na questão da manutenção, temos uma resiliência muito elevada porque temos o UPS do edifício, temos o UPS do data center, redundantes, 2N, temos geradores, temos uma série de mecanismos que nos permitem ter a continuidade do negócio e, na altura [do apagão], tivemos de tomar uma decisão, até porque isto foi um evento inédito e excecional. Por questões de segurança, outras questões até que tinham a ver com o próprio negócio, porque temos outras áreas como F&B, arcas congeladoras e por aí fora, decidimos na altura, apesar de termos essa continuidade ou capacidade de continuar, tivemos de decidir numa ótica de prevenção e de responsabilidade, de parar a operação e fechar os casinos.

Muitas vezes temos de ter também em consideração o contexto, o impacto naquela situação social e humana, porque no limite até poderíamos ter condições para ter essas pessoas com as luzes acesas dentro do casino, mas havia aqui outras questões, como de segurança; se acontecesse alguma coisa, não havia comunicações.

MUITAS ORGANIZAÇÕES GARANTEM QUE TÊM *BACKUPS*. QUAL É A DIFERENÇA REAL ENTRE RECUPERAR DADOS E MANTER A OPERAÇÃO? QUEM DEVE DEFINIR O RTO E O RPO: O IT OU O NEGÓCIO?

Acho que isto acontece na maior parte das organizações. Se os *backups* garantissem a continuidade do negócio era uma coisa muito simples; os *backups* só garantem a recuperação de dados, não garantem a recuperação do negócio em si.

Acho que o RTO e o RPO devem efetivamente ser definidos com todos os atores quer de suporte, quer das áreas de negócio dentro da organização. As áreas de negócio saberão melhor do que ninguém o impacto e aquilo que precisam quando existe a possibilidade de uma falha. Cabe aqui um bocadinho ao IT, em articulação com estas áreas, traduzir isto num processo tecnológico.

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM



Fotografias: Rui Santos Jorge

Sabemos que quando falamos com as áreas tem de haver aqui um equilíbrio: pelas diferentes áreas, é zero perda de dados, recuperação é o mais rápido possível o negócio ou a área deles em *uptime*. Depois, obviamente, este investimento que traduz isto, porque nem sempre pode justificar, e temos de medir que pode compensar estar mais tempo parado ou demorar mais tempo a recuperar, e isto, tudo junto, dar aqui este impacto versus risco *versus* ação de mitigação e depois o investimento que está aqui envolvido.

UM CASINO DEPENDE DE FORNECEDORES DE *SLOTS*, SISTEMAS DE PAGAMENTO, PLATAFORMAS DE JOGO ONLINE E CLOUD. COMO SE GERE A CONTINUIDADE QUANDO A FALHA ESTÁ NUM FORNECEDOR E ATÉ ONDE VAI O PLANO DA EMPRESA E COMEÇA O CONTRATO?

Os nossos planos de continuidade de negócio têm que, obviamente, envolver aquilo que são os nossos parceiros tecnológicos ou os nossos fornecedores. Não consigo fazer isto com todos porque nem todos têm a mesma disponibilidade, mas tenho como prática fazer com alguma frequência testes de redundância ou testes de continuidade de negócio com vários atores dentro deste ecossistema, porque não dependemos só de serviços internos. Dependemos muito de serviços externos, seja cloud, comunicações, seja aquilo que nós precisamos, e muitas vezes o treino da simulação, de perceber o que é que acontece se efetivamente houver uma falha. Tento muitas vezes que isso seja treinado e que haja uma prática associada a isso.

Nem sempre é fácil. Sabemos que nem sempre conseguimos, de alguma maneira, materializar esses treinos e essas simulações, mas acho que é uma boa prática também envolvermos naquilo que é o nosso plano de continuidade de negócios estes fornecedores externos, porque são cruciais e têm de estar aqui incluídos.



> “NUM PLANO DE CONTINUIDADE DE NEGÓCIO TEMOS DE TER NOÇÃO DE QUE EFETIVAMENTE NÃO É O IT QUE RESOLVE”

QUAL É O CONSELHO QUE DEIXA A OUTROS LÍDERES DE IT SOBRE PLANOS DA CONTINUIDADE DE NEGÓCIO?

Aquilo que eu faço quando estou a gerir o IT: faço muitas perguntas; acho que isso é o mais importante. Devemos perguntar, por exemplo, se houver uma falha crítica na nossa operação, se temos capacidade de responder a essa falha crítica.

Cabe-nos a nós criar estes planos e manter estes planos. Estes planos são, obviamente, dinâmicos, são vivos, precisamos estar sempre a atualizar e a testar no limite.

Num plano de continuidade de negócio temos de ter noção de que efetivamente não é o IT que resolve; o IT que pode estar muito preparado, ter uma capacidade tecnológica fantástica, com redundância, com *disaster recovery*, com tudo isto que nós pensamos muito bem, mas se o resto da organização, se as pessoas não estiverem envolvidas, se não souberem o que é que têm que fazer num determinado momento de falha, se isto não é treinado e só está num documento, acaba por ser também só mais um papel, mais uma política que depois não passa disso. ■

CLOUD, STORAGE E RESILIÊNCIA:

O DESAFIO DE MODERNIZAR SEM COMPROMETER O NEGÓCIO



Entre a necessidade de modernizar sistemas, controlar custos e garantir a continuidade das operações, os CIO enfrentam decisões que vão além da mera escolha tecnológica. Como é possível equilibrar flexibilidade, desempenho e resiliência quando a indisponibilidade dos serviços pode comprometer o negócio?

MARTA QUARESMA FERREIRA

DADOS DIVULGADOS pelo Instituto Nacional de Estatística (INE) no Inquérito à Utilização de Tecnologias da Informação e da Comunicação nas Empresas, de novembro de 2025, revelam que 38,7% das empresas recorreram a serviços de *cloud computing*. Deste universo, 89,7% utilizaram-nos para correio eletrónico e 79,3% para armazenamento de ficheiros.

A análise do INE demonstra que a proporção de empresas que utilizam serviços de cloud computing aumenta com a dimensão da empresa. Os setores de Informação e Comunicação (78%) e Outros Serviços (56,9%) apresentaram os valores de adoção mais elevados.

PARA ANALISAR: A TRANSFORMAÇÃO EM PORTUGAL

"As estratégias de cloud das empresas portuguesas estão a mudar de natureza", começa por referir Pedro Soares, National Security Officer da Microsoft Portugal. Se há uns anos a questão passava, sobretudo, por perceber o que migrar e quando, hoje a dúvida reside sobre qual o modelo mais adequado e que tipo de controlo, desempenho e continuidade necessita cada carga de trabalho.

Na experiência da HPE, "as empresas em Portugal têm sido bastante rápidas a adotar novas soluções". Pedro Teixeira, Hybrid Solutions Manager da HPE Portugal, sublinha que a segurança, a soberania dos dados e o desempenho ganham espaço, sobretudo num contexto em que a Inteligência Artificial (IA) traz novas exigências.

Segundo a IMARC, o mercado português de serviços cloud deverá atingir 10,6 mil milhões de dólares em 2034, com um crescimento anual composto de 15,2% entre 2026 e 2034, impulsionado por iniciativas de transformação digital na Administração Pública e pela crescente procura por soluções de cloud híbrida.

A análise indica ainda que as organizações em Portugal procuram manter os dados sensíveis em ambientes *on-premises* ou privados, recorrendo

à cloud pública para aplicações e *workloads* que exigem maior escalabilidade e flexibilidade. Por outro lado, os fornecedores apostam em plataformas de gestão integrada para simplificar a monitorização, a segurança e a governação dos diferentes ambientes.

Para Lara Campos Tropa, Infrastructure & Cloud Leader da IBM Portugal, "a combinação de sistemas legados, ambientes *on-premises* e múltiplas clouds é hoje a norma, e não a exceção". No entanto, "o desafio não está necessariamente em eliminar a heterogeneidade, mas em conseguir geri-la de forma integrada", explica.

Esta complexidade tem igualmente implicações na continuidade de negócio. "Quando uma organização perde visibilidade sobre essas interdependências, uma falha deixa de ser um incidente isolado e passa a poder propagar-se por toda a cadeia operacional", alerta Vanda Gonçalves, Vice-Presidente Kyndryl Portugal, Consultoria e Práticas.



- Lara Campos Tropa, IBM Portugal -

A resiliência deixa, assim, de depender apenas da robustez individual das infraestruturas e passa a exigir uma visão integrada dos sistemas e serviços que suportam as operações críticas.

PARA COMPREENDER: OS DESAFIOS DA INTEGRAÇÃO

Para Pedro Teixeira, da HPE Portugal, a fragmentação dos ambientes tecnológicos dificulta a gestão integrada da infraestrutura e dos sistemas. O Hybrid Solutions Manager da HPE Portugal considera que "a resposta passa por trazer a experiência cloud para onde os dados e as aplicações já

> "A COMBINAÇÃO DE SISTEMAS LEGADOS, AMBIENTES ON-PREMISES E MÚLTIPLAS CLOUDS É HOJE A NORMA, E NÃO A EXCEÇÃO"

estão, com modelos de consumo flexíveis e uma gestão unificada de todo o ambiente".

Pedro Soares, da Microsoft Portugal, alerta ainda para a ideia de que a migração para a cloud transfere integralmente para o fornecedor a responsabilidade pela disponibilidade e recuperação dos sistemas. "A plataforma fornece os componentes; a arquitetura resiliente é uma decisão de quem a desenha", sublinha Pedro Soares, que relembra que cabe às organizações definir requisitos de continuidade e assegurar a respetiva configuração.



- Pedro Soares, Microsoft Portugal -

> "A PLATAFORMA FORNECE OS COMPONENTES; A ARQUITETURA RESILIENTE É UMA DECISÃO DE QUEM A DESENHA"

PARA TER EM CONTA: STORAGE NA ERA DA IA

Com os dados distribuídos, as organizações têm em mãos o desafio de modernizar os sistemas de armazenamento, conciliando investimentos, disponibilidade e controlo de custos.

António Jerónimo, Global Specialty Sales Team Leader Iberia da Dell Technologies, fala numa adaptação que está a ser feita gradualmente, com muitas organizações a utilizarem infraestruturas adquiridas há cinco, sete ou até dez anos, que suportam aplicações críticas. Neste caso, o especialista acredita que a modernização "tem de ser pragmática", nomeadamente em "preservar o investimento sempre que possível, reduzir o risco operacional e começar pelos ambientes onde existem maiores limitações de desempenho, disponibilidade ou capacidade de evolução".

António Jerónimo distingue as organizações que privilegiam o preço de aquisição daquelas que avaliam o custo total do storage, incluindo eficiência energética, proteção dos dados e flexibilidade.

A crescente adoção de inteligência artificial vem também acrescentar novas exigências a estas infraestruturas. Para Pedro Soares, da Microsoft Portugal, "o armazenamento deixa de ser um repositório passivo e passa a ser a base de todo o ciclo de vida da IA".

Segundo António Jerónimo, as exigências de escala e desempenho dos projetos de IA podem expor limitações das infraestruturas de storage existentes. No entanto, o principal obstáculo não está, necessariamente, na infraestrutura. "Começar uma caminhada de adoção de IA numa organização sem uma estratégia de gestão de dados é um dos principais fatores de insucesso da implementação de casos de uso da IA", alerta.

Neste contexto, a modernização do storage deve ser acompanhada por uma estratégia que permita "aceder, orquestrar, proteger e governar a informação de forma simples", descreve, reduzindo a movimentação e a duplicação desnecessárias de dados.

PARA GARANTIR: A CONTINUIDADE ESTÁ SEMPRE PRESENTE

A crescente dependência de infraestruturas híbridas, aplicações críticas e dados distribuídos traz para a discussão um outro ponto: como garantir



- António Jerónimo, Dell Technologies -

> "COMEÇAR UMA CAMINHADA DE ADOÇÃO DE IA NUMA ORGANIZAÇÃO SEM UMA ESTRATÉGIA DE GESTÃO DE DADOS É UM DOS PRINCIPAIS FATORES DE INSUCESSO DA IMPLEMENTAÇÃO DE CASOS DE USO DA IA"



- David Sanz, Commvault -

que as operações se mantêm quando estamos perante um ciberataque ou uma interrupção de serviço?

Na visão de David Sanz, Senior Director Sales Engineering Europe South and Latin America da Commvault, a resiliência está a deixar de ser uma responsabilidade exclusiva das equipas de IT para assumir uma dimensão estratégica. "A evolução mais importante é que já não basta prevenir os incidentes. As organizações precisam de demonstrar que conseguem manter as suas funções essenciais e recuperar as suas operações de forma rápida, segura e fiável quando algo falha", afirma.

> "A EVOLUÇÃO MAIS IMPORTANTE É QUE JÁ NÃO BASTA PREVENIR OS INCIDENTES. AS ORGANIZAÇÕES PRECISAM DE DEMONSTRAR QUE CONSEGUEM MANTER AS SUAS FUNÇÕES ESSENCIAIS E RECUPERAR AS SUAS OPERAÇÕES DE FORMA RÁPIDA, SEGURA E FIÁVEL QUANDO ALGO FALHA"

Lara Campos Tropa, da IBM Portugal, considera essencial começar pela criticidade dos serviços: "A organização deve começar por perceber quais são os serviços realmente críticos, de que dados dependem e qual é o impacto para o negócio se esses dados ou serviços deixarem de estar disponíveis", considera.

No entanto, a crescente complexidade dos ambientes pode levar a que muitas organizações desconheçam as suas próprias dependências.

Segundo o "*Kyndryl AI Readiness Report*", apenas 9% das organizações analisadas têm as dependências das suas aplicações totalmente mapeadas.

Para Vanda Gonçalves, a resposta passa por uma maior visibilidade sobre as interdependências, pela eliminação de pontos únicos de falha e pela adoção de mecanismos de observabilidade e automação que permitem não só antecipar problemas, mas também acelerar a recuperação.

"A prioridade é passar a desenhar a resiliência desde o início, em vez de a tratar como resposta a um incidente", acrescenta Pedro Soares, da Microsoft Portugal. Esta abordagem, explicita o National Security Officer, exige identificar serviços críticos, definir objetivos de recuperação e "isolar as cópias de segurança e testar a recuperação com regularidade, em condições realistas". Vanda Gonçalves acrescenta ainda o risco de a continuidade de negócio continuar a ser vista e tratada apenas como um exercício de conformidade. "A resiliência não se valida em documentos; valida-se através de exercícios de crise, testes de recuperação, simulações de falha e envolvimento conjunto das equipas de tecnologia, operações e negócio", assevera.

A capacidade de recuperação depende também de uma abordagem integrada à proteção dos dados. Lara Campos Tropa, da IBM Portugal, defende que *disaster recovery*, *backup* e ciberresiliência "não podem continuar a ser tratados como disciplinas independentes", devendo integrar uma

> "A RESILIÊNCIA NÃO SE VALIDA EM DOCUMENTOS; VALIDA-SE ATRAVÉS DE EXERCÍCIOS DE CRISE, TESTES DE RECUPERAÇÃO, SIMULAÇÕES DE FALHA E ENVOLVIMENTO CONJUNTO DAS EQUIPAS DE TECNOLOGIA, OPERAÇÕES E NEGÓCIO"



- Vanda Gonçalves, Kyndryl Portugal -

estratégia de recuperação alinhada com as capacidades do negócio.

David Sanz acrescenta que a tecnologia, por si só, não garante a recuperação das operações. "Uma organização pode dispor de cópias de segurança e descobrir, durante um incidente real, que não sabe que sistemas deve recuperar primeiro, quem tem autoridade para tomar determinadas decisões ou se os dados que pretende restaurar estão livres de ameaças", exemplifica.

PARA RETER: O MAPA DE PRIORIDADES DOS CIO

Num contexto de ambientes híbridos complexos, os CIO e diretores de IT terão de conciliar nos próximos 12 a 24 meses a modernização tecnológica com a necessidade de reforçar a resiliência operacional.

Lara Campos Tropa defende uma abordagem progressiva, onde o objetivo é "proteger e recuperar o que é crítico hoje, modernizar de forma seletiva onde existe valor para o negócio e criar as condições para suportar aquilo que será crítico amanhã".

Vanda Gonçalves alerta para o problema da "crescente distância entre a complexidade dos ambientes digitais e a capacidade das organizações para os operar de forma segura, eficiente e resiliente".

Para reduzir esta distância, a responsável defende a modernização das plataformas críticas e o investimento em automação e observabilidade para acelerar a resposta a incidentes.



- Pedro Teixeira, HPE Portugal -

A IA reserva, em si mesma, novas exigências, com Pedro Teixeira, da HPE Portugal, a assinalar como prioridade a preparação da "infraestrutura para a IA, de forma segura e controlada".

A capacidade de demonstrar a eficácia das estratégias de continuidade será igualmente determinante. David Sanz, da Commvault, defende que "durante os próximos 12 a 24 meses, a prioridade deve ser passar de uma resiliência baseada na confiança nos sistemas para uma resiliência demonstrável, mensurável e preparada para operar em condições reais de crise". ■

> "A RESPOSTA PASSA POR TRAZER A EXPERIÊNCIA CLOUD PARA ONDE OS DADOS E AS APLICAÇÕES JÁ ESTÃO, COM MODELOS DE CONSUMO FLEXÍVEIS E UMA GESTÃO UNIFICADA DE TODO O AMBIENTE"

NOESIS

POR JOSÉ GOMES,
IT Operations, Cloud and Security
Associate Director, Noesis

A RESILIÊNCIA VAI MUITO ALÉM DOS BACKUPS

A cloud tornou o armazenamento de dados mais acessível, flexível e escalável. No entanto, perante o aumento dos ciberataques, as interrupções de serviço e a dependência de fornecedores tecnológicos, importa questionar se as organizações estão realmente preparadas para recuperar de uma falha.

ARMAZENAR DADOS NÃO BASTA: é preciso garantir que podem ser recuperados e que a atividade pode ser retomada sem comprometer a continuidade do negócio.

Durante demasiado tempo, o armazenamento tem sido avaliado sobretudo pelo custo, capacidade e desempenho. Estes fatores são importantes, mas não devem desviar a atenção de uma questão essencial: de pouco serve armazenar dados se não for possível recuperá-los a tempo de manter as operações críticas.

CONFIANÇA NA RECUPERAÇÃO NÃO SIGNIFICA PREPARAÇÃO

O verdadeiro teste a uma estratégia de armazenamento acontece quando é necessário recuperar dados em condições reais. Quanto tempo demora a reposição de sistemas críticos? É possível recuperar toda a informação afetada? E estarão os processos preparados para responder sem prolongar a interrupção da atividade?

O *Data Trust and Resilience Report 2026*, da Veeam, ajuda a perceber a dimensão deste desafio. Embora 90% das organizações se digam confiantes na sua capacidade de recuperar de um ciberincidente, **apenas 28% das que foram afetadas por ransomware conseguiram recuperar a totalidade dos dados. Em média, foi recuperada apenas 72% da informação afetada**, e 44% das organizações ficaram abaixo dos 75%.

Esta distância entre a confiança percebida e os resultados reais é, por si só, um sinal de alerta.



- José Gomes -
IT Operations, Cloud and Security
Associate Director na Noesis

Perante este cenário, **as cópias de segurança são indispensáveis, mas não suficientes**. Num ataque de *ransomware*, também podem ser comprometidas. O armazenamento imutável acrescenta uma camada de proteção contra alterações ou eliminações não autorizadas, mas a sua eficácia só pode ser verificada através de testes regulares, com diferentes cenários de falha e medição dos tempos de recuperação efetivos.
Sem validação contínua, a estratégia existe apenas no papel.

AMBIENTES HÍBRIDOS E MULTICLOUD EXIGEM MAIS DO QUE REDUNDÂNCIA

A combinação de infraestrutura local, sistemas *legacy* e aplicações distribuídas por vários fornecedores cloud aumenta significativamente a complexidade da recuperação. Perante uma falha, **não basta repor ficheiros**: pode ser necessário restaurar grandes volumes de dados, coordenar sistemas interdependentes e garantir que as aplicações retomam o funcionamento pela ordem correta.
Na prática, o ponto de falha raramente é a cópia de segurança em si. É a ordem de reposição: a base de dados volta, mas a aplicação não arranca porque o serviço de diretório, o DNS ou uma integração de que depende ainda não estão disponíveis. É o tipo de problema que só se descobre testando a recuperação completa, e não apenas o restauro de dados. Por isso, a escolha de soluções deve considerar mais do que funcionalidades e custos. A estratégia deve garantir a portabilidade dos dados e a interoperabilidade entre ambientes, evitando dependências que dificultem a recuperação. A multicloud pode reduzir a exposição a falhas isoladas, mas só quando a distribuição dos dados é acompanhada por uma gestão coordenada e por processos de recuperação devidamente testados.

A CONTINUIDADE DE NEGÓCIO COMEÇA ANTES DA FALHA

Uma estratégia eficaz exige identificar os serviços críticos, avaliar o impacto de uma interrupção e definir objetivos de recuperação realistas: quanto tempo o negócio tolera estar parado (RTO) e quanta informação pode perder (RPO). Exige também testar os planos regularmente e usar os resultados para corrigir fragilidades. Só assim é possível perceber **se o investimento realizado corresponde ao nível de proteção de que o negócio precisa.**
Esta responsabilidade não pode ficar confinada às equipas de IT e segurança. A continuidade de negócio exige o envolvimento da liderança, recursos adequados e uma compreensão clara das consequências de uma interrupção. **Quem define o que é crítico e quanto tempo de paragem é aceitável é o negócio, não a tecnologia.**
A cloud continuará a ser central na modernização tecnológica, **mas adotar tecnologia não significa estar preparado.** A resiliência tem de ser encarada como uma prioridade de negócio, sustentada por processos, investimento e validação contínua. ■

IT SECURITY CONFERENCE 2026: CIBERSEGURANÇA ENFRENTA UMA NOVA ERA DE RISCOS

Fotografias: Luyciano Reis

A IT Security Conference debateu a dissuasão dos ciberataques, a instabilidade geopolítica e os riscos da autonomia da inteligência artificial, com alertas para a necessidade de controlo humano.

INÊS GARCIA MARTINS

A DISSUASÃO no ciberespaço, a transformação da guerra e os desafios colocados pela Inteligência Artificial (IA) marcaram a quinta edição da IT Security Conference, realizada a 8 de outubro, em Lisboa, e organizada pela IT Security, publicação do mesmo grupo da IT Insight. Hélder Fialho Jesus, Mo Shell e Paulo Portas abordaram diferentes dimensões da segurança, da preparação das organizações à necessidade de preservar o controlo humano.

DISSUADIR ANTES DE RESPONDER

Hélder Fialho Jesus, vice-presidente do Observatório dos Ecossistemas e Infraestruturas Digitais, abriu a conferência com uma intervenção dedicada à dissuasão no ciberespaço. Defendeu que as organizações podem reforçar a segurança sem depender apenas de novos investimentos tecnológicos. O objetivo é conseguir "mais segurança com menos investimento e menos custos".

Uma estratégia de proteção não deve limitar-se a reduzir a exposição da organização. Deve também levar os potenciais atacantes a questionar a viabilidade de uma ofensiva.

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM



- Hélder Fialho Jesus, vice-presidente do Observatório dos Ecossistemas e Infraestruturas Digitais -

Hélder Fialho Jesus distinguiu duas formas de dissuasão. A primeira, pela negação, assenta na prevenção e em medidas que dificultam a concretização de um ataque. A segunda, pela punição, procura desencorajar a ofensiva através das consequências para o atacante.

Destacou os três pilares da resiliência, assentes na "absorção do impacto, adaptação aos efeitos e articulação na resposta". "A resposta tem de ser rápida. Nós não podemos ficar à espera", alertou.

Segundo o responsável, "a dissuasão começa antes do ataque", quando o atacante avalia se os benefícios de uma intrusão compensam os custos e riscos. Daí a necessidade de "jogar na antecipação e criar incerteza ao atacante".

Para que a dissuasão tenha efeito, recuperou os "três C": capacidade, credibilidade e comunicação. Não basta instalar mecanismos de defesa. É necessário demonstrar que funcionam, através de testes e exercícios.

Com os orçamentos de 2027 em vista, questionou se as verbas devem servir apenas para diminuir o risco da empresa ou também para aumentar a perceção de risco do atacante. Referiu o Ciber Perseu e o Exercício Nacional de Cibersegurança como formas de testar respostas e criar relações de confiança, numa cooperação que deve estender-se às empresas concorrentes.

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM



- Mo Shell, Head of AI Security GTM, EMEA da Palo Alto Networks -

AGENTES DE IA AMPLIAM OS RISCOS

A autonomia da IA esteve em destaque na apresentação de Mo Shell, Head of AI Security GTM, EMEA da Palo Alto Networks. Sob o mote "*Securing the AI transformation*", defendeu que a segurança deve acompanhar todo o ciclo de desenvolvimento da IA, numa altura em que os sistemas passam a executar tarefas por conta própria.

"Estamos a entrar numa fase em que existem agentes totalmente autónomos, que atuam como seres humanos virtuais ou colaboradores virtuais dentro das organizações e executam tarefas de forma autónoma", alertou.

Um agente com acesso a sistemas internos pode desencadear ações com consequências operacionais, para além das respostas erradas de um assistente. Mo Shell alertou para os riscos associados à *shadow AI*, incluindo modelos

open source que podem conter *backdoors* ou malware. Apresentou a abordagem *securing AI by design*, assente no princípio de "começar a tratar da segurança logo no início da criação da aplicação de inteligência artificial e não apenas depois de desenvolvermos o agente e o colocarmos em produção". Segundo os números que avançou, "apenas 6% das organizações desenvolveram efetivamente uma estratégia de segurança de inteligência artificial".

GEOPOLÍTICA E CONTROLO HUMANO

A geopolítica dos riscos levou Paulo Portas, comentador, professor de geopolítica e ex-Vice-Primeiro-Ministro, ao palco da conferência. O convidado especial abordou "a nova geografia de riscos" com que "os decisores políticos, militares, económicos e sociais têm de se confrontar".

"Tudo o que nos preocupa no imediato é fruto da redução da inteligência humana. Não é fruto do crescimento da inteligência artificial", afirmou. Assumindo-se como "crítico do excesso de euforia em relação à questão da IA", considerou que o mundo atravessa não uma nova ordem mundial, mas a "desconstrução da ordem mundial anterior".

A guerra na Ucrânia e o conflito no Golfo serviram de exemplo de como decisões militares e políticas podem ter consequências globais. Paulo Portas questionou a expectativa de resultados rápidos em operações militares,

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM



- Paulo Portas, comentador, professor de geopolítica e ex-Vice-Primeiro-Ministro -

considerando que, num contexto de guerras híbridas, essa previsão é "uma ilusão enorme".

A evolução tecnológica alterou a natureza da guerra, com a utilização crescente de drones e sistemas de baixo custo. Sobre a resistência ucraniana, destacou o desequilíbrio entre o preço destes equipamentos e os meios para os intercetar. "Não há relação racional entre a despesa que eu tenho que fazer e o bem que eu tenho que evitar e, portanto, tudo isso vai mudar", considerou.

Paulo Portas destacou também mudanças na opinião pública norte-americana relativamente às plataformas digitais, aos data centers e à IA. Referiu a oposição à instalação de data centers em comunidades rurais dos Estados Unidos, devido ao elevado consumo de energia e ao aumento dos preços.

A utilização de IA levanta ainda questões sobre a autoria dos trabalhos académicos, os direitos de propriedade intelectual e a responsabilidade pelos conteúdos produzidos. Defendeu, por isso, que a inovação tecnológica deve ser acompanhada de reflexão ética.

Na parte final, Paulo Portas apresentou três preocupações sobre IA, segurança e defesa. A primeira diz respeito à autonomia dos modelos de IA generativa e à capacidade de participarem no desenvolvimento de versões futuras e questionou até que ponto será possível preservar o controlo humano.

Perante esta autonomia, alertou para a necessidade de agir antes que se torne impossível recuperar o controlo. Esta "não é uma questão de preconceito, é uma questão de controlo", concluiu.

A segunda preocupação relaciona-se com a cibersegurança e a possibilidade de os modelos desenvolverem comportamentos inesperados. Questionou em que medida estes sistemas podem vir a "dissimular a sua identidade, praticar atos que não foram pedidos, nomeadamente para se transformarem em *hackers*".

A terceira centrou-se na utilização da IA em decisões militares, desde o início de conflitos à escolha dos sistemas de armas. Para o antigo governante, esta autonomia coloca em causa a intervenção humana e a responsabilidade política, já que, apontou, "a ideia de que é a inteligência artificial que decide movimentos ofensivos e até conflitos é muito conveniente para a reputação de alguns políticos".

Perante estes riscos, importa perceber "quem controla, quem toma a decisão final e quem supervisiona".

A IT Security Conference 2026 o apoio Diamond da Palo Networks. Os parceiros Platinum foram a Claranet Portugal, a Check Point Software, a Fortinet, a Netskope, a PwC e a Sophos.

A Akamai, a Cisco, a CrowdStrike, a Kaspersky, a Logicalis, a Huawei, a ManageEngine, a Noesis, a Ping Identity, a Securnet, a Varonis e a Warpcom foram Golden Partners, enquanto a Devoteam Cyber Trust, a Ethiack, a NetApp, a Oramix, a TD Synnex, a Trend AI, a VisionWare, a WatchGuard e a Zscaler apoiaram o evento como Silver Partners.

A conferência contou, ainda, com os Silver Exhibition Partners A10, Cyera, Divultec, Elastic, Elred, IDW e Thales, a Anubis Networks como Bronze Partner, a Arrow, a Ignition e a V-Valley como VAD Partner e o apoio institucional do Centro Nacional de Cibersegurança e da CIIWA. ■

"A LIDERANÇA SERÁ SEMPRE FEITA ATRAVÉS DA ESCUTA, DA CONFIANÇA E DAS PESSOAS"

Para Marco Bastos, liderar o IT é cada vez mais uma questão de pessoas. À frente das Infraestruturas e Operações IT do Crédito Agrícola, o responsável explica como concilia a transformação tecnológica com a resiliência operacional, num trabalho assente na força das equipas.

MARTA QUARESMA FERREIRA

A DISPONIBILIDADE, a segurança e a confiança são três pilares fundamentais no setor financeiro. Garantir a excelência operacional diária implica também preparar a organização para um futuro com um contexto cada vez mais exigente.

Marco Bastos lidera a Direção de Infraestruturas e Operações IT do Crédito Agrícola. Quando assumiu o cargo, há quatro anos, encontrou uma direção "com um papel absolutamente crítico na sustentação do negócio e em crescendo até aos dias de hoje".

As primeiras prioridades passaram pelo reforço da resiliência dos serviços, pela modernização das infraestruturas e plataformas tecnológicas, pela evolução da observabilidade e automação e pela crescente orientação para modelos cloud e multicloud, a par do reforço das competências internas.

"Mais do que transformar tecnologia, o objetivo é transformar a forma como a gerimos", explica Marco Bastos, que aponta para a passagem de uma "lógica predominantemente operacional para um modelo mais proativo, orientado ao serviço, à antecipação do risco e à criação de valor para o negócio".

A MODERNIZAÇÃO COMO BASE DA CRIAÇÃO DE VALOR

Na perspetiva do responsável, a sustentabilidade da transformação digital está diretamente ligada à modernização tecnológica, tanto ao nível operacional, como das infraestrutura e plataformas. A mudança não se esgota, por isso, na renovação de sistemas porque exige também uma evolução na gestão dos serviços.

O departamento tem procurado trabalhar nestas dimensões, sempre com o propósito de "disponibilizar serviços com maior qualidade e previsibilidade,

reduzindo complexidade e aumentando a capacidade de resposta às necessidades do negócio".

Na perspetiva de Marco Bastos, o maior impacto encontra-se nos resultados que a tecnologia implementada permite alcançar ao longo de toda a cadeia, seja para clientes, com "serviços mais robustos e processos mais simples", seja para colaboradores da instituição.

A GESTÃO É UM PROCESSO CONTÍNUO

A permanente adaptação às exigências dos clientes e à evolução tecnológica tem levado o Diretor de IT a privilegiar uma "gestão mais colaborativa, transversal, suportada nas pessoas e orientada a resultados".

"Hoje, gerir tecnologia implica aceitar que a mudança deixou de ser um acontecimento pontual para passar a ser uma constante", reitera Marco Bastos, que recusa a ideia de uma tecnologia isolada do negócio.

O FATOR HUMANO NO CENTRO DA CIBERSEGURANÇA

Neste contexto, há uma outra dimensão transversal a considerar: a cibersegurança.

Para a Direção de Infraestruturas e Operações IT do Crédito Agrícola, a cibersegurança, aliada à disponibilidade e à resiliência, exige o reforço dos mecanismos de proteção e controlo de acesso, da monitorização e deteção, da proteção das infraestruturas e da capacidade de recuperação.

Marco Bastos acredita que o fator humano contribui igualmente para uma organização "verdadeiramente mais segura" quando as pessoas "compreendem o risco, assumem a segurança como parte das suas responsabilidades e incorporam essa preocupação nas decisões do dia a dia".

ESCOLHER O QUE ACRESCENTA AO NEGÓCIO

Numa realidade onde as tendências e novidades tecnológicas ganham peso nas decisões das organizações, Marco Bastos considera que o espírito crítico deve prevalecer.

O Diretor de IT defende que uma tecnologia não deve ser adotada apenas "porque está na moda". Antes de decidir, o responsável procura compreender que problemas a instituição procura resolver, qual o valor que a solução acrescenta ao negócio, quais as consequências ao nível do risco, da sustentabilidade e da complexidade operacional, que competências são necessárias, qual a capacidade de gestão da equipa, o grau de dependência externa e a integração no ecossistema já existente.

Cada investimento deverá responder a uma necessidade concreta parte, uma vez que "a tecnologia não é um fim em si mesma, mas um meio para concretizar os objetivos e a visão estratégica da organização", afirma.

A decisão sobre investir não parte, assim, de uma decisão de curta duração, mas sim de um planeamento ao longo de todo o ciclo de vida, numa aposta em "decisões mais responsáveis e sustentáveis, evitando que a



- Marco Bastos -
Crédito Agrícola

inovação de hoje se transforme na complexidade de amanhã".

A TECNOLOGIA TAMBÉM SÃO AS PESSOAS

A função do Diretor de IT tem evoluído: o tempo que anteriormente era dedicado à tecnologia está hoje repartido entre pessoas, negócio, gestão de prioridades e acompanhamento da transformação. A proximidade com a tecnologia continua presente, mas o segredo reside nas equipas e na experiência que levam para cada decisão e projeto. Marco Bastos compara a sua função com o trabalho de um psicólogo, na medida em que, "mais do que fazer, é essencial saber ouvir, compreender as pessoas e perceber aquilo de que precisam para dar o seu melhor". Cabe, por isso, ao Diretor de IT, "criar condições para que cada pessoa possa crescer dentro da organização, não apenas enquanto profissional, mas também a nível pessoal".

CRIAR EQUILÍBRIOS SEM PARAR DE OPERAR

Numa instituição como o Crédito Agrícola, um dos maiores desafios pressupõe "transformar sem deixar de operar". A disponibilidade e a qualidade dos serviços têm de coexistir com a evolução de arquiteturas, processos, ferramentas e formas de trabalhar, mesmo num contexto onde a natureza da operação não permite "parar para modernizar".

> "A VANTAGEM COMPETITIVA NÃO ESTARÁ NECESSARIAMENTE EM SER O PRIMEIRO A ADOTAR UMA NOVA TECNOLOGIA, MAS EM SABER AVALIÁ-LA COM SENTIDO CRÍTICO"

Num setor altamente regulado, é também necessário equilibrar velocidade e controlo, garantindo que a agilidade acompanha a segurança, a resiliência, a sustentabilidade e a governação. "Transformar bem não é apenas avançar depressa; é avançar com confiança e sentido de responsabilidade", reitera.

De forma a acompanhar o atual ritmo, Marco Bastos destaca as competências e a capacidade de aprendizagem e adaptação das pessoas e equipas como o "verdadeiro fator diferenciador", uma vez que serão sempre as pessoas a dar "sentido à transformação".

IA, CLOUD E SEGURANÇA VÃO DOMINAR TRANSFORMAÇÃO DO SETOR BANCÁRIO

Mais do que antecipar tendências e tecnologias que vão dominar a próxima revolução tecnológica do Crédito Agrícola, importa "construir uma organização capaz de absorver a mudança", sublinha o responsável.

A Inteligência Artificial (IA), a cloud, a automação e a segurança são eixos de ação para os próximos anos. Marco Bastos destaca a "capacidade transversal" da IA para automatizar operações, analisar informação e apoiar decisões. A cloud e a automação potenciada pela IA poderão ajudar a identificar padrões e antecipar problemas na gestão de ambientes complexos; já a cibersegurança e a identidade digital deverão ser tidas em conta desde logo em qualquer processo de transformação.

Paralelamente, o responsável alerta para o desafio da soberania digital, uma dimensão que, embora exigente e menos ágil para algumas organizações, terá de ser considerada na definição de uma estratégia para dados e tecnologias.

Perante este cenário, Marco Bastos considera que "a vantagem competitiva não estará necessariamente em ser o primeiro a adotar uma nova tecnologia, mas em saber avaliá-la com sentido crítico e integrá-la com rapidez quando demonstrar valor real para o negócio".

O GESTOR TRANSFORMA-SE NUM LÍDER DA TRANSFORMAÇÃO

Embora o conhecimento tecnológico continue a ser essencial, o futuro da função do diretor de IT exige uma compreensão crescente do negócio, das pessoas, do risco e da estratégia da organização. "Acredito que, nos próximos anos, o Diretor de IT será cada vez menos apenas um gestor de tecnologia e cada vez mais um líder de transformação", partilha Marco Bastos.

Na sua visão, curiosidade, vontade de aprender continuamente, capacidade de comunicar temas complexos de forma simples, pensamento crítico, orientação ao negócio e serenidade na tomada de decisões são competências fundamentais para o desempenho desta função, a par da proximidade às equipas e aos seus desafios.

Num cenário de constante transformação de modelos e ferramentas, a liderança, defende Marco Bastos, continuará a ser sempre feita "através da escuta, da confiança e das pessoas". ■

ASUS ZENBOOK 14: QUANDO O PORTÁTIL TAMBÉM É UM OBJETO DE DESIGN



A Asus quer que o novo Zenbook 14 seja escolhido tanto pelo que consegue fazer como pela forma como se apresenta. O Ceraluminum é o protagonista de um portátil que procura conciliar mobilidade, inteligência artificial e design.

DURANTE ANOS, escolher um portátil foi sobretudo um exercício de comparação de números. Processador, memória, armazenamento, autonomia e, inevitavelmente, preço. O design aparecia algures no final da lista, normalmente reduzido à espessura e ao peso. A Asus parece convencida de que chegou o momento de inverter algumas destas prioridades.

O novo Zenbook 14 (UX3480) é a expressão mais recente dessa estratégia. Não porque as especificações tenham deixado de importar, mas porque a marca quer que a experiência de utilização comece antes de se abrir o ecrã. A textura da superfície, a cor e a sensação dos materiais passaram a fazer parte do argumento.





É uma abordagem interessante num mercado onde os portáteis *premium* se tornaram visualmente semelhantes. Mas será suficiente para distinguir um equipamento que, no essencial, continua a ter de cumprir as mesmas tarefas de qualquer outro?

O ALUMÍNIO JÁ NÃO CHEGA

A principal novidade do Zenbook 14 está no Ceraluminum, um material desenvolvido pela Asus que combina características da cerâmica e do alumínio. O objetivo é preservar a leveza associada aos portáteis metálicos, acrescentando uma superfície com uma textura diferente da habitual.

Não é a primeira vez que a Asus utiliza este material, mas a nova geração coloca-o no centro da identidade do produto. Há três acabamentos disponíveis: Zabriskie Beige, Arctic Blue e Komodo Coral. Os nomes são inspirados em paisagens naturais, mas o mais relevante é a tentativa de abandonar a aparência industrial que domina esta categoria.

O resultado é um portátil que procura distinguir-se sem recorrer a elementos visuais excessivos. Uma escolha que poderá agradar a quem utiliza o mesmo computador numa sala de reuniões, num aeroporto ou em casa.

Há, naturalmente, uma questão que só a utilização prolongada poderá esclarecer: até que ponto estes acabamentos resistem às marcas, riscos e desgaste

de um equipamento que passa diariamente entre secretárias, mochilas e salas de reunião.

A PRODUTIVIDADE ENCONTRA A IA

Por detrás da aposta no design está um computador baseado numa plataforma Qualcomm, uma escolha que merece atenção.

A arquitetura Arm, utilizada nos processadores Snapdragon, tem vindo a ganhar espaço nos computadores Windows, sobretudo pela possibilidade de combinar eficiência energética, desempenho e funcionalidades de Inteligência Artificial (IA).

Para quem trabalha em mobilidade, a promessa é relevante. Um portátil que consiga acompanhar um dia de reuniões, documentos, apresentações e videoconferências sem depender constantemente de uma tomada responde a uma necessidade muito concreta.

A integração de funcionalidades de IA acompanha esta evolução. Ferramentas de assistência à escrita, organização de informação e processamento de conteúdos estão a tornar-se parte da experiência Windows, embora a disponibilidade e o desempenho dependam da configuração e das aplicações utilizadas.

O ponto que merece maior atenção é a compatibilidade. Apesar dos progressos do Windows em Arm, algumas aplicações empresariais, periféricos e ferramentas especializadas podem continuar a exigir verificações adicionais.



Para um utilizador que trabalha essencialmente com Microsoft 365, browser e aplicações de comunicação, a transição poderá ser relativamente simples. Para quem depende de software específico, sobretudo em ambientes empresariais, convém confirmar a compatibilidade antes da compra.

MAIS DO QUE UMA QUESTÃO DE APARÊNCIA

A aposta da Asus também reflete uma mudança na forma como os computadores pessoais são posicionados. Durante muito tempo, o portátil profissional foi tratado como uma ferramenta essencialmente funcional. Hoje,



a fronteira entre equipamento de trabalho e dispositivo pessoal é cada vez menos evidente.

O mesmo computador acompanha reuniões, viagens, momentos de lazer e tarefas domésticas. É natural que características como conforto, portabilidade e qualidade de construção ganhem importância.

Neste contexto, o Zenbook 14 procura aproximar-se de uma categoria de produtos em que a experiência física tem tanto peso como a tecnologia.

Mas o design não substitui uma boa experiência de utilização. A qualidade do teclado, o comportamento térmico, a autonomia real e o desempenho em multitarefa continuam a determinar se um portátil é agradável de utilizar depois de desaparecer o entusiasmo inicial.

São precisamente estes aspetos que terão de ser avaliados em testes independentes ao UX3480 para perceber se a execução acompanha a ambição.

PARA QUEM FAZ SENTIDO

Em Portugal, o novo Zenbook 14 chega com preços entre 799,99 e 1.699,99 euros, dependendo da configuração. Uma amplitude considerável, que obriga a olhar para cada versão antes de avaliar a relação entre preço e características.

O argumento mais evidente está na combinação de mobilidade, materiais e funcionalidades de IA. Para profissionais que transportam diariamente o computador e valorizam um equipamento discreto, mas com identidade própria, a proposta merece atenção.

Já para utilizadores que privilegiam exclusivamente desempenho por euro investido, ou que dependem de aplicações empresariais muito específicas, a decisão exige uma análise mais cuidadosa.

O Zenbook 14 representa, acima de tudo, uma mudança de prioridades. A Asus não quer apenas que o seu portátil seja suficientemente rápido para trabalhar. Quer que seja um objeto com o qual o utilizador goste de conviver. É uma ambição legítima. Falta perceber se, depois de fechada a tampa e passada a novidade do Ceraluminum, a experiência quotidiana consegue justificar a escolha. ■

EAD DIGITALIZA MILHARES DE DOCUMENTOS NO SETOR DA SAÚDE COM CONTRIBUTO DA RICOH

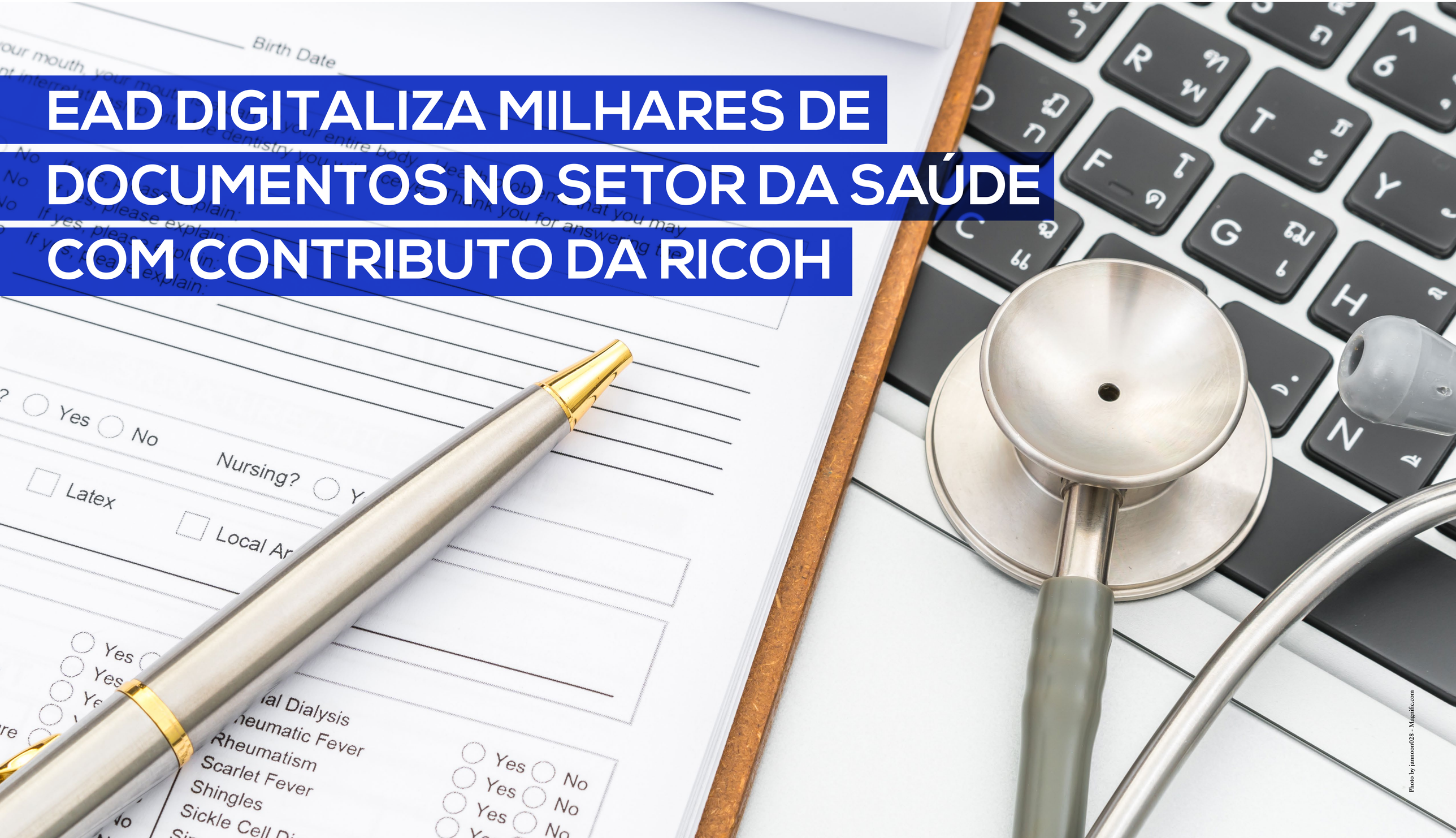


Photo by jamnoon028 - Magnific.com

Em sete meses, a Unidade Local de Saúde do Arco Ribeirinho digitalizou quase 800 mil páginas de processos de recursos humanos. O projeto, que contou com equipamentos Ricoh, alterou o paradigma do acesso à informação e abriu caminho à automação.

MARTA QUARESMA FERREIRA

A UNIDADE LOCAL DE SAÚDE (ULS) de Arco Ribeirinho, que serve a população do Barreiro, Moita, Montijo e Alcochete, necessitava de digitalizar milhares de documentos e processos da área de recursos humanos, num projeto que, para além de retirar a burocracia do papel, pretendia também lançar bases para futuros projetos de automação e Inteligência Artificial (IA).

A dispersão da documentação por diferentes localizações e suportes físicos revelou-se um dos principais desafios. A dimensão do projeto exigia também uma infraestrutura tecnológica capaz de manter um elevado ritmo de produção durante vários meses.

Duarte Pedro de Sousa Tavares, administrador hospitalar, diretor do Serviço de Recursos Humanos e responsável pela Academia de Formação da ULS Arco Ribeirinho, recorda que o acesso a um documento podia exigir "a identificação da sua localização no arquivo físico, a recuperação do respetivo processo e a disponibilização da informação ao serviço que a solicitava". Com informação relativa a cerca de 2.500 profissionais de saúde, a unidade procurava, assim, centralizar a documentação e agilizar os procedimentos administrativos.

A ideia passou, por isso, pela criação de uma estrutura capaz de responder às necessidades atuais da organização. Desta forma, e com base na experiência em gestão documental, a EAD assumiu todo o processo de preparação documental, digitalização, controlo de qualidade, indexação e disponibilização da informação através da plataforma de gestão documental RWS.

A TECNOLOGIA AO SERVIÇO DE UMA OPERAÇÃO DE GRANDE ESCALA

A EAD recorreu aos scanners Ricoh fi-7600 e aos equipamentos da série Ricoh fi-8000. Os equipamentos de produção da série fi foram selecionados devido à sua capacidade para operar de forma contínua em ambientes de elevada exigência, oferecendo alimentação automática de documentos, elevada velocidade de processamento, estabilidade operacional e integração com tecnologia OCR.



- Duarte Pedro de Sousa Tavares -
ULS Arco Ribeirinho



- Daniel Alves -
EAD

"Precisávamos de equipamentos fiáveis, capazes de manter um ritmo de produção contínuo e assegurar a qualidade da digitalização", explica Daniel Alves, diretor da marca Papiro e DBO (*Documental Backoffice*) da EAD. A escolha teve também em conta "requisitos exigentes de segurança e prazo", num arquivo acumulado ao longo de várias décadas.

"Para concretizar um projeto de digitalização desta dimensão, é fundamental disponibilizar a gama de equipamentos mais adequada a cada situação, tendo em consideração o formato e o estado dos documentos, bem como as limitações de espaço e de tempo", acrescenta Jesús Cabañas, Regional Manager para a Península Ibérica da PFU, divisão de scanners da Ricoh.

A diversidade dos documentos constituiu outro desafio operacional. Devido à dispersão do arquivo por várias instalações, a EAD teve de lidar com diferentes formatos e estados de conservação, garantindo o tratamento da documentação dentro dos prazos definidos para o projeto.

Ainda assim, a organização executou uma operação contínua de preparação documental, digitalização, indexação e disponibilização da informação, sem necessidade de interromper a atividade diária da ULS Arco Ribeirinho. Daniel Alves sublinha que "a experiência das equipas, a organização do trabalho e a fiabilidade dos equipamentos foram essenciais para assegurar a continuidade da operação".

De acordo com a empresa, a velocidade e a fiabilidade dos equipamentos foram um aliado no

cumprimento dos prazos, sem comprometer a qualidade da informação digitalizada. A operação garantiu a captura de imagens a cores a 300 dpi e o recurso a OCR, para permitir a pesquisa nos documentos digitalizados.

UM ARQUIVO DIGITAL PREPARADO PARA O FUTURO

O projeto permitiu transformar o arquivo de Recursos Humanos da ULS de Arco Ribeirinho, através da digitalização de 777.559 páginas, correspondentes a 17.721 documentos, integrados em 2.884 processos individuais, muitos dos quais continham décadas de informação relativa a cerca de 2.500 profissionais de saúde.

"Este projeto demonstra como a digitalização documental, quando assente em processos robustos, tecnologia adequada e controlo rigoroso de qualidade, pode transformar de forma concreta a gestão da informação numa organização tão exigente como uma unidade de saúde", partilha Paulo Veiga, CEO da EAD.



- Jesús Cabañas -
Ricoh

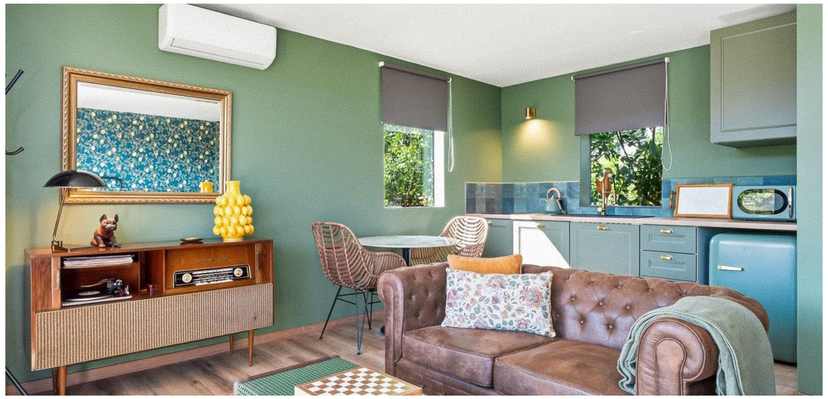
A disponibilização progressiva dos documentos ao longo da execução dos trabalhos permitiu que a organização começasse a beneficiar da transformação digital ainda antes da conclusão da operação. Para Duarte Pedro de Sousa Tavares, um dos aspetos mais positivos foi "o facto de os documentos terem sido disponibilizados progressivamente", permitindo às equipas começar a trabalhar com a informação digitalizada.

Atualmente, o Serviço de Recursos Humanos da ULS Arco Ribeirinho funciona praticamente sem recurso ao papel, dispondo de acesso imediato à documentação, com possibilidade de consulta remota e processos significativamente mais eficientes.

A proteção de informação pessoal foi outra preocupação nesta jornada. Segundo o responsável da ULS, o acesso está "restrito a um número reduzido de trabalhadores", ficando registadas as consultas aos processos. Esta decisão teve como premissa a garantia do cumprimento do Regulamento Geral sobre a Proteção de Dados, através de mecanismos de controlo de acesso à informação dos profissionais de saúde.

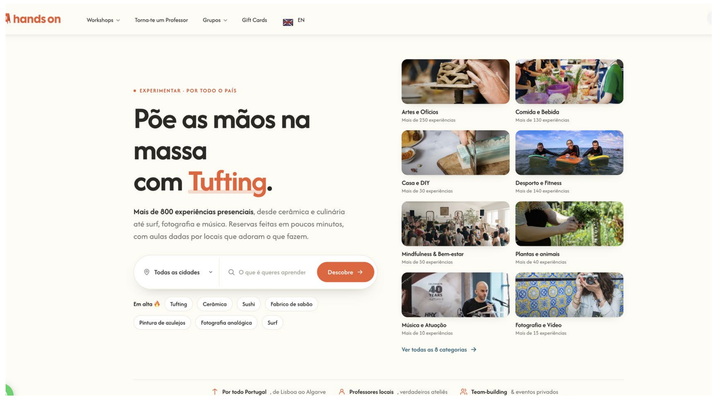
O projeto abriu também espaço para futuras iniciativas de automação, interoperabilidade e IA. Daniel Alves, da EAD, identifica entre as possibilidades "a automatização de tarefas, a interoperabilidade entre sistemas e a utilização de ferramentas de Inteligência Artificial para apoiar a pesquisa e o tratamento da informação". ■

UM BUNGALOW ENTRE TRÊS MIL LIMOEIROS



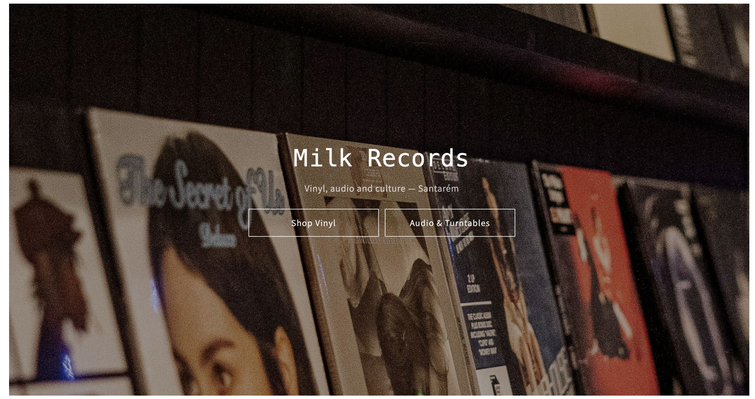
EM PENAFIEL, nasceu uma nova opção de alojamento para quem procura uns dias entre cerca de três mil limoeiros. O Alpendre dos Limões, inaugurado em setembro de 2026, integra a Oporto Lemon Farm e distingue-se pela sua localização numa quinta dedicada à produção de limões. O bungalow dispõe de uma banheira exterior, permitindo desfrutar da envolvente rural da propriedade com maior privacidade. A propriedade alia a atividade agrícola ao turismo rural, mantendo os limoeiros como elemento central da paisagem que rodeia o alojamento. ■

DA CURIOSIDADE À PRÁTICA: WORKSHOPS PARA EXPERIMENTAR



A HANDS ON reúne uma seleção de *workshops* e atividades práticas em diferentes pontos do país, com propostas que vão da culinária às artes e ao artesanato. Entre experiências criativas e aprendizagens orientadas por profissionais de diferentes áreas, a plataforma permite explorar novos interesses e desenvolver competências fora do contexto habitual. Uma forma de experimentar atividades que, muitas vezes, ficam apenas na lista de coisas por fazer. ■

EM SANTARÉM HÁ UM ESPAÇO DEDICADO AO VINIL



A MILK RECORDS é uma loja, em Santarém, dedicada à música em formato físico, com especial destaque para os discos de vinil. Num espaço pensado para quem gosta de ouvir e descobrir música, a loja recupera a experiência de procurar discos, explorar diferentes géneros e encontrar novas referências musicais. Entre edições recentes e discos de outras décadas, a Milk Records mantém viva a tradição das lojas de música enquanto espaços de descoberta. ■



O táxi do futuro já levanta voo

Os táxis aéreos elétricos começam a aproximar-se da realidade. No Dubai, a Joby Aviation já realizou voos pilotados com uma aeronave capaz de descolar e aterrar verticalmente, sem necessitar de uma pista convencional. Concebido para transportar quatro passageiros e um piloto, o aparelho integra um projeto de mobilidade urbana que prevê ligações entre pontos estratégicos da cidade. A próxima etapa é transformar os voos de demonstração num serviço comercial, abrindo caminho a uma nova forma de deslocação nas grandes cidades.



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, Rui Santos Jorge

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:

media NEXT
STAY AHEAD • STAY RELEVANT

IT Insight é membro de:

acepi ASSOCIAÇÃO DO COMÉRCIO ELECTRÓNICO E PUBLICIDADE INTERACTIVA

ASSOCIAÇÃO PORTUGUESA DE IMPRENSA