IT Insight

#58 NOVEMBRO 2025

media NEXT
STAY AHEAD • STAY RELEVANT

REINVENÇÃO EXECUTIVA

DECIDIR, LIDERAR E COMPETIR EM TEMPOS DE IA

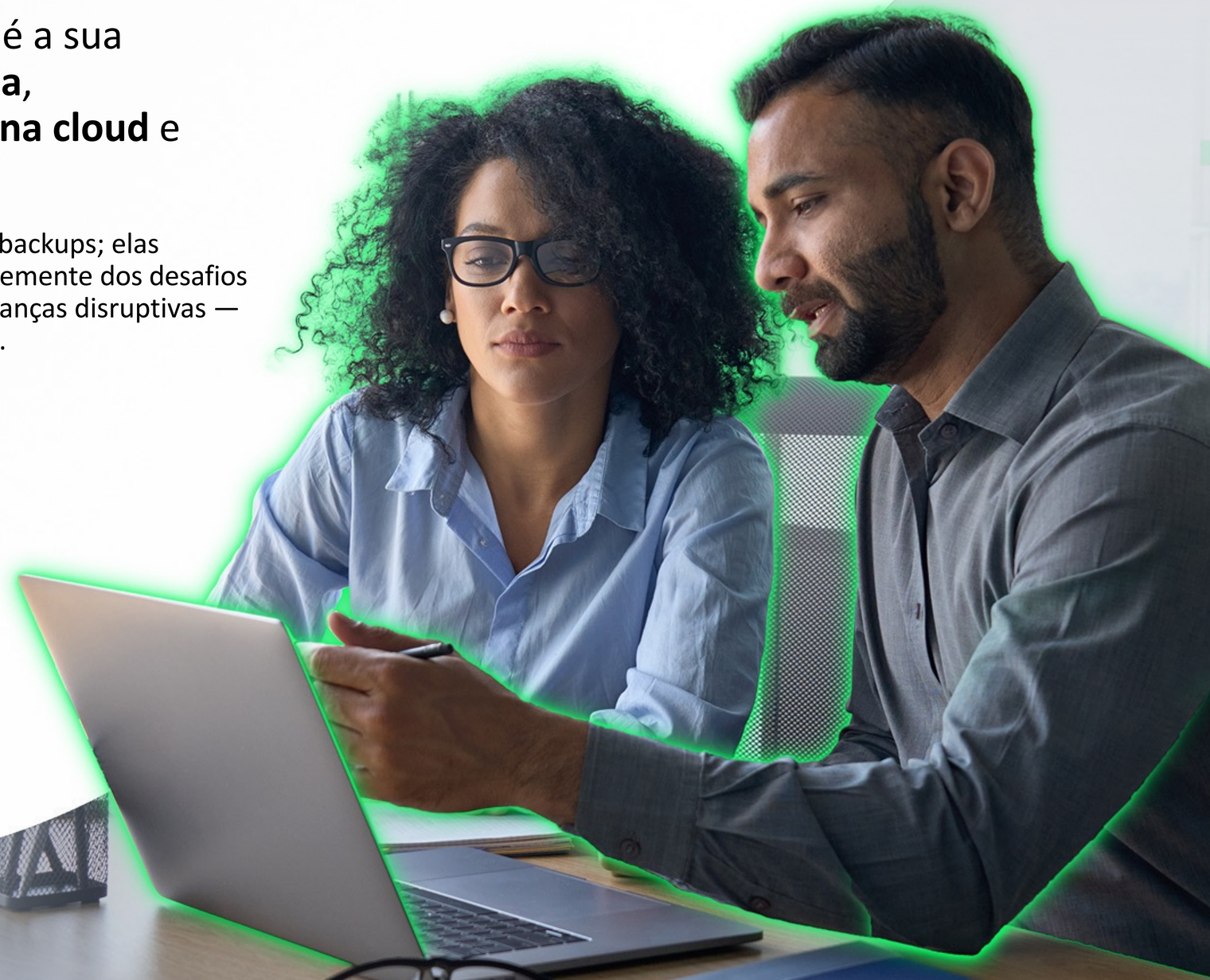
Veeam é Mais

Vai além do backup e da recuperação — é a sua vantagem estratégica em **ciber-resiliência**, **portabilidade de dados**, **storage seguro na cloud** e **operações em cloud híbrida.**

As corporações modernas procuram mais do que simples backups; elas requerem uma resiliência de dados genuína. Independentemente dos desafios enfrentados pelo seu negócio — seja ciberataques ou mudanças disruptivas — a Veeam assegura uma recuperação rápida das operações.

Veeam é Mais+
É **ciber-resiliência**
- É portabilidade de dados
- É storage na cloud seguro
- É a cloud híbrida

Saiba mais



IT·Insight

#58 NOVEMBRO **2025**

IN DEEP

d_AI_gest por Henrique Carreiro

COVERAGE
IT Security Conference: a visão dos CISO para o futuro da proteção digital

360º VIEW | ANDRÉ ASSUNÇÃO
“A inovação já não é sobre o que compramos, mas como integramos de forma segura”

TRANSFORM
Controlo financeiro e integração entre áreas: Brighten Consulting e Sage melhoram negócio da Flatlantic

IN DEEP | LEADERSHIP IN THE DIGITAL TRANSFORMATION ERA
Liderar na fronteira entre pessoas e tecnologia

IT INSIGHT TALKS | BUSINESS CONTINUITY
Continuidade de negócio: a redundância deixou de ser opcional

FACE 2 FACE | HUGO MARTINS
“A maior parte das pessoas dá como adquirido que os sistemas vão estar sempre a funcionar”

WISHLIST
Asus lança em Portugal um supercomputador pessoal de IA

IP Telecom

Housing
IPT Cloud

CloudSolutions
Housing
Hosting

Nato Secret

EU Secret

Rede Nacional CSIRT

AOS

gaia-x

LIGAMOS NEGÓCIOS

Telecomunicações | Data Center | Cloud Computing

VIRTUAL DATACENTERS

BACKUP AS A SERVICE

STORAGE AS A SERVICE

CYBER SECURITY

DDoS DEFENSE

CYBER DEFENSE

OPTICAL NETWORKS

VIRTUAL PRIVATE NETWORKS

NETWORK & SECURITY OPERATION CENTER

VIRTUAL DESKTOPS

DISASTER RECOVERY

CLOUD STORAGE

www.iptelecom.pt

comercial@iptelecom.pt

IT·Insight

#58 NOVEMBRO **2025**

IT INSIGHT TALKS
BUSINESS CONTINUITY

Commvault Porque são as cleanrooms essenciais para uma ciberrecuperação eficaz?

IP Telecom Soberania e Resiliência da Continuidade de Negócio

SECURNET ALWAYS ONLINE | ALWAYS SECURE ALWAYS RESILIENT - Vantagem competitiva ou sobrevivência?

veeam Pagamentos de ransomware estão a diminuir, mas organizações da EMEA continuam despreparadas para ataques

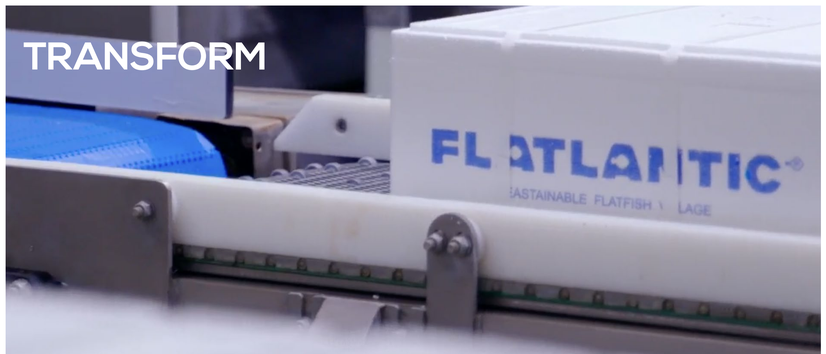
VisionWare since 2005 O que todos os líderes devem saber sobre continuidade de negócio

IN DEEP
LEADERSHIP IN THE DIGITAL TRANSFORMATION ERA

claranet Modernizar para Liderar: O novo mandato da Era Digital

...e ainda

LISPOLIS POLO TECNOLÓGICO DE LISBOA



LISPOLIS
DESDE 1991

HUB PARA EMPRESAS TECNOLÓGICAS E INOVADORAS EM LISBOA

LABORATÓRIOS INDUSTRIAIS, ESPAÇOS DE ESCRITÓRIO, EVENTOS DO ECOSSISTEMA E COMUNIDADE

+140 EMPRESAS

02 VENTURE BUILDERS

06 ASSOCIADOS FUNDADORES

04 ASSOCIADOS EFETIVOS

06 LOTES DISPONÍVEIS

COMUNIDADE

ESPAÇOS PARA EVENTOS

LISPOLIS IGNITE

Queres acelerar o teu negócio e não sabes por onde começar?
Junta-te ao nosso programa de aceleração.

HENRIQUE CARREIRO

O elo mais frágil da cadeia tecnológica global

A CADEIA DE ABASTECIMENTO de semicondutores é, provavelmente, o sistema industrial mais complexo e interdependente do mundo. Conecta milhares de empresas, de inúmeros setores, das minas de quartzo às fábricas que produzem chips com dimensão de nós inferiores a cinco nanómetros, numa rede global que nenhuma região consegue dominar isoladamente.

A Europa, através da neerlandesa ASML, fornece as máquinas de litografia ultravioleta extrema que tornam possível a gravação de circuitos à escala atómica. Taiwan, com a TSMC, concentra a produção dos chips mais avançados: na prática também outro monopólio, como o da ASML. Os Estados Unidos lideram no design, nomeadamente de circuitos cruciais para as aplicações de IA, e nas ferramentas EDA, enquanto matérias-primas críticas têm origem em todos os continentes: o paládio da Rússia e da África do Sul, o néon da Ucrânia, o gálio da China, o cobre do Chile. Cada *wafer* é o produto final de um ecossistema multinacional de uma precisão quase orgânica.

Mas essa interligação, fonte de eficiência e de inovação, é também uma vulnerabilidade estrutural. A pandemia, a guerra na Ucrânia e as tensões em torno da autonomia de Taiwan expuseram a fragilidade de um modelo que depende da fluidez global. As respostas — o CHIPS Act nos EUA, o European Chips Act e os programas asiáticos de soberania tecnológica — visam reduzir dependências externas, mas alimentam uma tendência de isolamento que ameaça o equilíbrio do sistema.

O isolacionismo tecnológico é uma reação expectável, mas perigosa. Nenhum país pode, realisticamente, replicar toda a cadeia de valor dos semicondutores. O desafio não é erguer barreiras, mas reforçar resiliência através da cooperação, da redundância e da partilha de conhecimento.

A fragmentação deste ecossistema global não trará autonomia; trará atraso. E num mundo cada vez mais digital, o tempo é o recurso mais escasso de todos. ■

SECURNET

ALWAYS ONLINE | ALWAYS SECURE

MAIS DO QUE UMA MARCA, UM PARCEIRO DE CONFIANÇA.

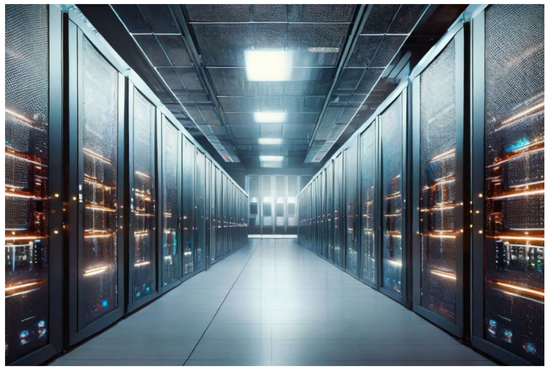
☆☆ **HPE 'FY24**	Parceiro do Ano - HPE GreenLake Parceiro do Ano - HPE Aruba Networking
☆ **Veeam Software**	The best COM partner of the year 2024, Portugal
☆☆ **IT Channel Award2025**	Parceiro Cybersecurity Parceiro do Ano

A TECNOLOGIA EVOLUI. E NÓS TAMBÉM.

PORTO +351 224 673 094
LISBOA +351 213 622 204

DATA CENTERS PORTUGUESES PODEM VALER 3,7 MIL MILHÕES DE EUROS ATÉ 2031

Estudo aponta que o setor português de data centers pode valer 3,7 mil milhões de euros até 2031.



De acordo com o estudo "*Market Outlook Data Centers Portugal 2025*", da Associação Portuguesa de Data Centers, o setor de data centers e infraestruturas digitais tem previsões que apontam para um impacto de 3,7 mil milhões de euros no PIB até 2031. O estudo aponta que o setor criou 2.800 empregos em 2024, e deverá criar mais de 9.400 cargos até 2031, o que contribui para um crescimento de 160 milhões para 3,7 mil milhões de euros.

De acordo com o estudo, a posição privilegiada de Portugal torna o país no grande ponto de interligação entre os vários continentes, apoiado por cabos submarinos internacionais, além dos novos pontos de intercâmbio de tráfego e da concentração de Transit Providers Tier 1. O estudo sublinha que o setor português de data centers opera com um cabaz energético renovável e que tem o compromisso de alcançar a neutralidade carbónica até 2045. ■

MAIORIA DA POPULAÇÃO PORTUGUESA AFIRMA QUE IA FACILITOU AS SUAS VIDAS

Estudo revela que 89% dos portugueses utiliza inteligência artificial.

Um estudo realizado com 800 portugueses revela que 89% utilizam Inteligência Artificial (IA) e consideram-na uma ferramenta que facilita a vida, apesar das preocupações éticas e sociais. Entre os principais benefícios estão a rapidez na obtenção de informação, a poupança de tempo com a automatização de tarefas e a tradução de idiomas. A IA é também valorizada no acesso a recursos educativos, com quase três em cada dez a utilizarem ferramentas de aprendizagem baseadas em IA.

Dois terços dos inquiridos acreditam que a IA pode melhorar os serviços de saúde, reduzindo tempos de espera e aumentando a eficiência. Metade sente-se confortável com a sua aplicação em diagnósticos e tratamentos, mas existem receios relacionados com erros nos diagnósticos, impactos nos tratamentos, violação de privacidade, riscos de segurança e perda de emprego. ■

Empurrar limites para moldar o futuro

Cloud & Infra

Workplace

Applications

Data & AI

Security

claranet.com/pt

claranet®

ANACOM ESCOLHIDA PARA REGULAR IA EM PORTUGAL

Bernardo Correia, Secretário de Estado para a Digitalização, anunciou a escolha, destacando a importância de desenvolver um "ambiente regulatório que celebre a inovação".

A Anacom será a autoridade responsável pela supervisão do Regulamento Europeu sobre Inteligência Artificial (IA) em Portugal, anunciou Bernardo Correia, Secretário de Estado para a Digitalização, sublinhando que a transformação digital é um "pilar" da reforma do Estado e o digital uma "alavanca transformadora da sociedade", assente em cinco eixos estratégicos: o primeiro redefine a visão do Estado sobre a tecnologia, com a criação do primeiro Chief Tecnology Officer da Administração Pública; o segundo reforça os serviços públicos digitais, promovendo o princípio do *once only*; o terceiro incide na economia e inovação digital, atraindo investimento internacional; o quarto promove a adoção de uma IA "ética, auditável e livre de enviesamentos"; enquanto o quinto aposta na literacia e nas competências digitais.

O governante defendeu a ideia de um ambiente regulatório "que garanta que a tecnologia tem um impacto positivo na comunidade". ■

FUTURO TECNOLÓGICO DESAFIA EMPRESAS EM PORTUGAL

Um estudo da Compuworks revela que as empresas portuguesas continuam vulneráveis a ciberataques e que a inteligência artificial e a cibersegurança vão continuar a marcar o IT.

A Compuworks apresentou o estudo "*IT Future Trends 2035*", realizado para o mercado português com o apoio do Ecossistema Inova. Segundo o CEO da Compuworks, Ricardo Teixeira, "as empresas estão ainda pouco preparadas para os desafios que vão surgir muito rápido nos próximos anos". De acordo com o estudo, 76% dos líderes acreditam que a sua organização sofrerá um ciberataque material até 2035, embora 58% admitam não estar prontos. Cerca de 55% das empresas já desenvolvem ou planeiam ter soluções de inteligência artificial. Ricardo Teixeira considera que "a Europa está a perder terreno tecnológico", com 92% da infraestrutura de cloud controlada por empresas norte-americanas. De acordo com estudo, o futuro do trabalho em Portugal será marcado pelo modelo híbrido, exigindo formação contínua e atualização do ensino. ■

20 anos

VisionWare

since 2005

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

+100
colaboradores

+200
clientes ativos

5000
projetos desenvolvidos

Os nossos serviços

- Cyber Defense Operations
- Privacy & Legal
- Cybersecurity
- Professional Services
- Ethics & Compliance
- Strategic Intelligence & Risk Analysis
- Forensic Investigations
- VisionWare Academy

Challenging an Unsafe World

Porto | Lisboa | Praia | Mindelo

geral@visionware.pt

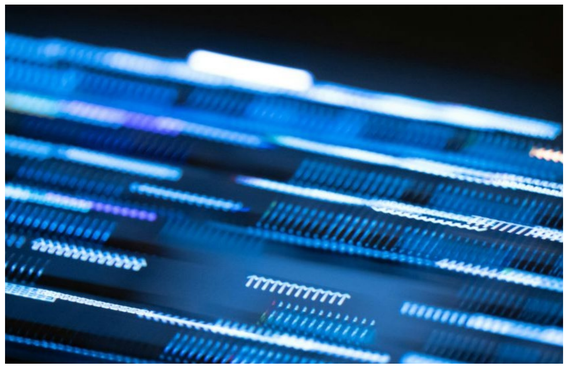
+351 225 323 740

SCAN ME

visionware.pt

MAIORIA DAS EMPRESAS VAI AUMENTAR INVESTIMENTO EM IA EM 5%

Estudo revela que a inteligência artificial está a assumir um papel cada vez mais essencial na redução de custos nas empresas.



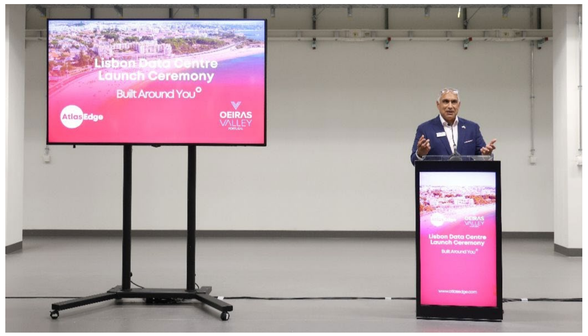
O novo estudo "*Scaling AI While Controlling Tech Costs*" da Bain & Company, sete em cada dez empresas revelaram que vão aumentar o investimento em Inteligência Artificial (IA) em mais de 5%. Segundo o estudo, que inquiriu 480 gestores tecnológicos, 31% das empresas prevê aumentar o investimento entre 5 e 10%, 25% prevê aumentar entre 10 e 20% e 13% entre 25 e 50%.

A análise destaca que a IA pode contribuir para a redução de custos ao detetar despesas ocultas, identificar software que já não é utilizado pelas equipas, melhorar a eficiência operacional e ajudar a otimizar a infraestrutura ao permitir uma visão mais nítida da utilização de recursos.

De acordo com o estudo, para além dos custos diretos, a IA aumenta a complexidade da gestão de uma empresa e do suporte ao ritmo cada vez maior de mudança da tecnologia. ■

ATLASEDGE INAUGURA NOVO DATA CENTER EM PORTUGAL

Carnaxide, na região de Lisboa, recebe o novo data center da AtlasEdge que conta, para já, com 5MW.



- Tesh Durvasula, CEO da AtlasEdge, durante a inauguração do LIS001 da AtlasEdge -

A AtlasEdge inaugurou no dia 28 de outubro o primeiro dos três data centers que vai abrir em Carnaxide, na zona de Lisboa. O primeiro edifício – LIS001 – conta com uma capacidade de IT de 5MW. Quando os outros dois edifícios estiverem construídos, o campus do AtlasEdge terá uma capacidade de IT de 30MW. Sem detalhar clientes, o campus de Carnaxide afirma que o LIS001 já tem a sua capacidade completamente contratada por "clientes *top-tier*". Espera-se que o data center fique a funcionar no final de 2025. Já o LIS002 deverá estar disponível em 2028.

A AtlasEdge também anunciou a aquisição de um terreno de dez mil metros quadrados contíguo ao LIS002, que irá acolher o terceiro data center do campus, o LIS003. Esta aquisição eleva, então, a capacidade total futura do campus para 30MW. A operadora também anunciou que assegurou um financiamento verde de 253 milhões de euros para apoiar o desenvolvimento do seu campus data center. ■

Hybrid cloud & Multicloud

IT Insight talks

Tendências e estratégias para 2026

11 de dezembro | Quinta-feira | 10h

A IT Insight convida-o a participar na mesa-redonda Hybrid cloud & Multicloud, no dia 11 de dezembro de 2025, no Fórum Tecnológico Lispolis, em Lisboa. Neste evento vamos explorar as últimas tendências, estratégias e melhores práticas num ambiente digital em constante evolução. Junte-se a especialistas do setor e compreenda como otimizar a eficiência e flexibilidade dos serviços em cloud para impulsionar os seus negócios, a nível global.

Fórum Tecnológico Lispolis | A partir das 9h30 | Participação **presencial** e **online**
Escolha a sua forma de participar:

QUERO ESTAR PRESENTE

QUERO ASSISTIR POR ZOOM

Com o apoio de: LISPOLIS Pólo Tecnológico de Lisboa · LOGICALIS Architects of Change · noesis an Altia Company · Red Hat

d_AI_gest

AI DIGEST, UM RESUMO DO QUE MAIS IMPORTANTE ESTÁ A ACONTECER NO CAMPO DA INTELIGÊNCIA ARTIFICIAL

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

Doze modelos, uma especificação, muitos desacordos

Imagem: Daniel by Freepik

A Anthropic e o Thinking Machines Lab publicaram um artigo que relata uma experiência em que 12 LLM foram colocados perante mais de 300 mil cenários onde valores colidem — equidade vs. eficiência, utilidade vs. segurança — para observar o que realmente prioritizam quando a especificação não resolve o conflito. O retrato é consistente: a família Claude privilegia responsabilidade ética e integridade intelectual; a linha OpenAI inclina-se para eficiência e otimização de recursos; Gemini 2.5 Pro e Grok dão mais peso à dimensão relacional.

O desacordo é estrutural, com variação substantiva em mais de 220 mil casos e rotura limpa em cerca de 70 mil — um modelo favorece um valor que outro rejeita. As recusas expõem filosofias de segurança distintas (Claude recusa mais e justifica, o3 opta pelo "não" lacónico), mas há uma linha vermelha comum nos pedidos com risco para menores. O dado incómodo é este: nos cenários de maior discordância, os incumprimentos da própria especificação multiplicam-se por 5–13, sintoma de tensões internas ("assumir boas intenções" a chocar com "prevenir danos") e de ambiguidade suficiente para pôr avaliadores a discordar.

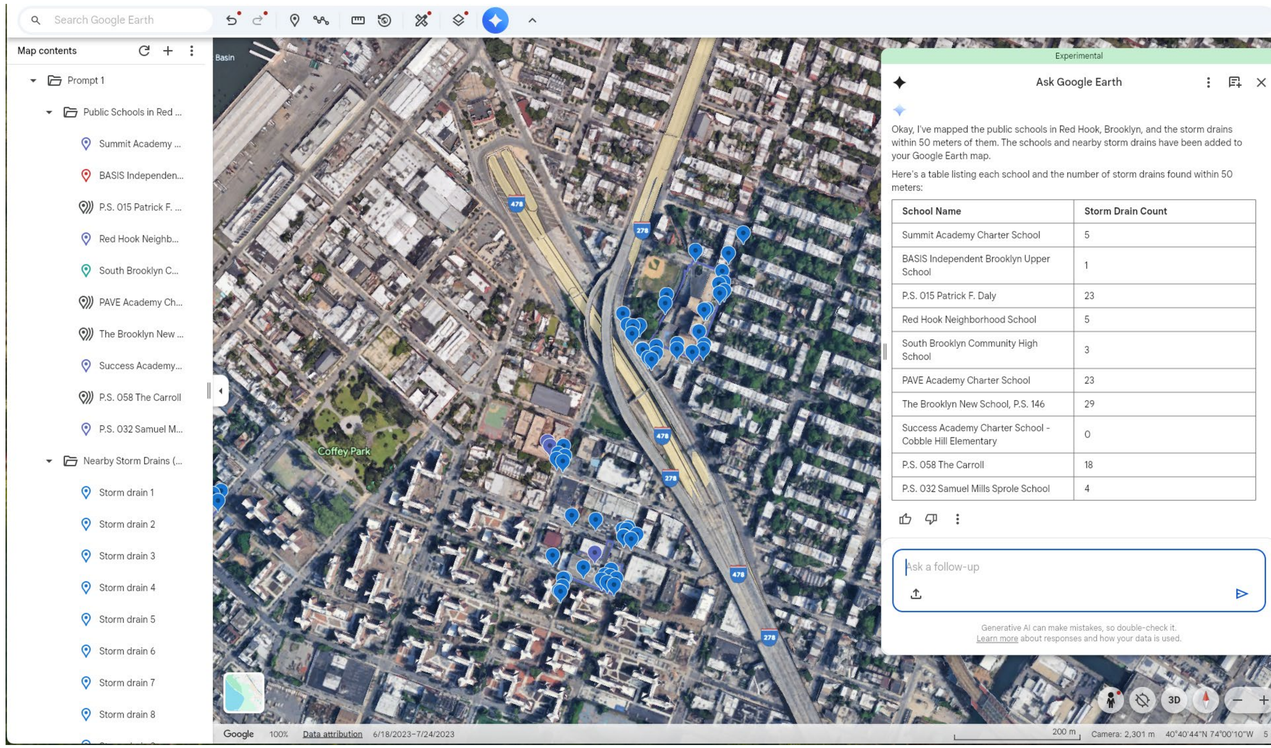
Os casos atípicos ajudam a mapear caráter — Grok 4 aceita pedidos que outros classificam como nocivos, Claude 3.5 Sonnet recusa pedidos inofensivos — e há falsos positivos de segurança, do plano geral de estudo em biologia a operações triviais em Rust marcadas como "ciber-risco". A norma é a mesma; o critério não. ■

Google Earth AI: mapas que respondem a perguntas

A Google está a transformar o Earth num instrumento de análise. A nova plataforma Earth AI combina décadas de modelação geoespacial com o raciocínio do Gemini, permitindo que empresas, cidades e organizações sem fins lucrativos passem de observar o planeta a interrogá-lo. A camada de *geospatial reasoning* liga previsões meteorológicas, mapas de população e imagens de satélite para responder a perguntas complexas — não apenas onde uma tempestade vai bater, mas que infraestruturas ficam em risco e que comunidades são mais vulneráveis.

No Google Earth, a integração com os modelos de Earth AI permite detetar padrões e objetos em imagem: identificar rios secos antes de provocarem tempestades de poeira, localizar florescimentos de algas que podem contaminar a água potável ou antecipar escassez hídrica em regiões críticas. O acesso arranca nos EUA, através das versões Professional e Advanced do Google Earth, e estende-se a *testers* no Google Cloud, com modelos de Imagem, População e Ambiente disponíveis para cruzar com dados próprios.

A OMS/África usa esta combinação para prever surtos de cólera na República Democrática do Congo; a Planet e a Airbus aplicam-na à deteção de desflorestação e à manutenção de redes elétricas; e a Bellwether, da X/Alphabet, explora-a para afinar previsões de furacões usadas por seguradoras. Menos mapa decorativo, mais inteligência operacional — e uma nova forma de perguntar ao planeta o que se prepara para acontecer. ■



Netflix aposta tudo na IA generativa — criatividade, promete o CEO, não se automatiza

Na sua carta trimestral aos acionistas, a Netflix descreve a IA generativa como uma "oportunidade significativa" em toda a plataforma: desde o sistema de recomendações ao negócio publicitário e à própria produção de séries e filmes. A empresa diz estar a disponibilizar ferramentas GenAI aos criadores para acelerar processos e explorar variações criativas.

O relatório cita exemplos recentes: Happy Gilmore 2 recorreu a técnicas de "*de-aging*" para rejuvenescimento de personagens; e a série Billionaires' Bunker usou modelos generativos para experimentar guarda-roupa e cenários em pré-produção.

Ted Sarandos, CEO da empresa, insistiu na distinção essencial: "A IA pode ajudar-nos, e aos nossos parceiros criativos, a contar histórias melhor, mais depressa e de formas novas —, mas não faz de ninguém um bom contador de histórias."

A posição da Netflix chega num contexto de desconfiança generalizada no setor. A ideia de atores ou argumentistas substituídos por modelos generativos ainda é tóxica em Hollywood — e foi precisamente essa tensão que, em 2023, levou à longa greve da SAG-AFTRA, o sindicato dos atores, resultando nas primeiras cláusulas contratuais que limitam o uso de IA em cinema e televisão. Mais recentemente, o estúdio Particle6 reacendeu o debate ao anunciar planos para criar e gerir "atores sintéticos" totalmente gerados por IA.

A Netflix tenta demarcar-se com novas orientações internas para o uso responsável de IA na produção. A promessa é pragmática: automatizar o que é infraestrutural — pesquisa, pré-visualização, marketing — e preservar o território da autoria. Se resultar, a IA será um assistente invisível; se não, um eco que ensurdece a voz criativa que ainda distingue o humano do algoritmo. ■

REINVENÇÃO EXECUTIVA

DECIDIR, LIDERAR E COMPETIR EM TEMPOS DE IA

LIDERAR EM TEMPOS DE INTELIGÊNCIA ARTIFICIAL

Nestes tempos, em que se fala de agentes e de robots como se falava antes de PC ou de Internet, com a certeza de uma inevitável presença futura, liderar já não é um ato de comando: é um exercício de tradução.

HENRIQUE CARREIRO

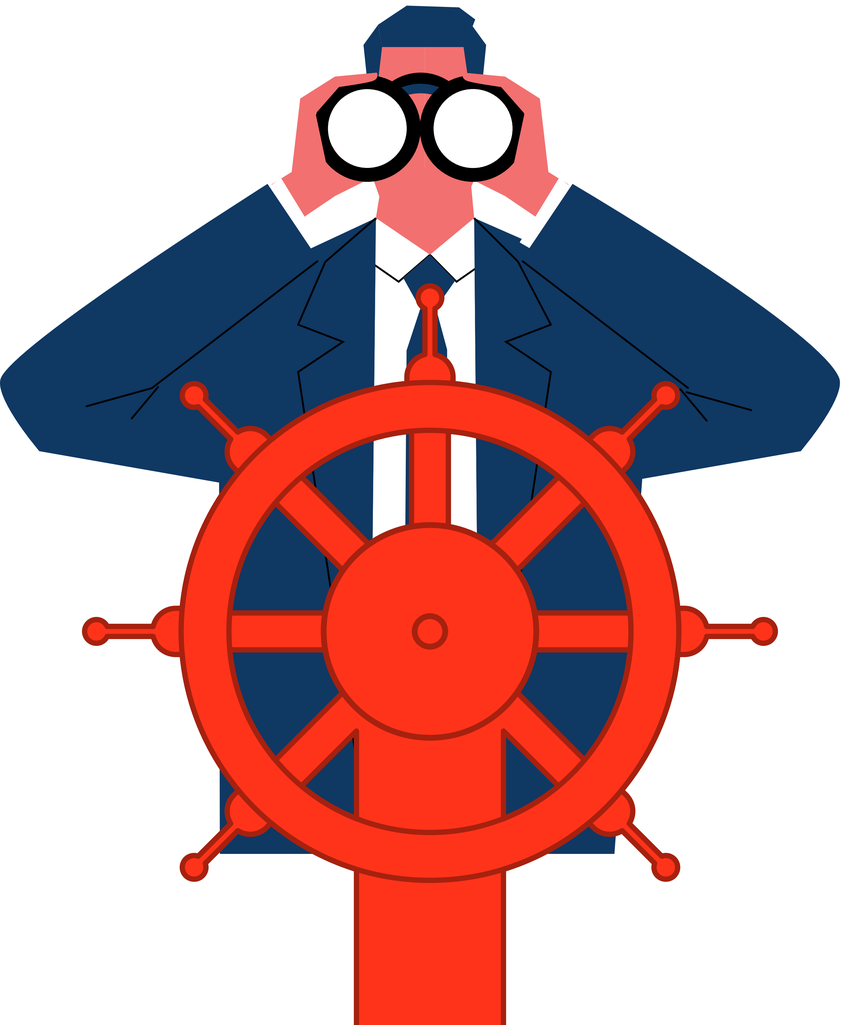
AS ORGANIZAÇÕES operam dentro de sistemas de decisão que aprendem, preveem e recomendam. A Inteligência Artificial (IA) deixou de ser uma ferramenta para se tornar um ambiente. E o líder é, antes de mais, alguém que procura manter a lucidez organizacional dentro desse ambiente.

Durante décadas, associámos liderança a intuição, a visão e a experiência acumulada. Nada disso desapareceu, mas perdeu exclusividade. A autoridade humana passou a partilhar o espaço de decisão com a inferência algorítmica. Quem gere organizações tem hoje de compreender o que significa decidir quando se multiplicam os prismas sobre os quais a realidade é interpretada.

Um erro recorrente é confundirmos automatização com progresso. A eficiência é uma virtude instrumental, não moral. A IA é exímia a replicar padrões, mas desastrosa fora das balizas de treino — daí as bem conhecidas alucinações. Liderar na era da IA é proteger o espaço da interpretação: o território onde os dados terminam e o sentido começa.

A questão é, no fundo, de poder. As organizações foram desenhadas como hierarquias humanas, não como ecossistemas híbridos homem-máquina. Quando uma entidade artificial se transmuta em colaborador, a autoridade muda de natureza. O dirigente deixa de ser a origem da decisão para

> “PORQUE A IA NÃO É NEUTRA. CADA MODELO TRANSPORTA OS ENVIESAMENTOS DOS DADOS E DAS INTENÇÕES QUE O MOLDARAM, REPRODUZINDO O PASSADO COM A APARÊNCIA DE OBJETIVIDADE”



se tornar o arquiteto de um diálogo entre inteligências — uma humana, outra computacional. E essa mediação exige uma qualidade que as teorias de gestão raramente contemplam: humildade cognitiva.

Porque a IA não é neutra. Cada modelo transporta os enviesamentos dos dados e das intenções que o moldaram, reproduzindo o passado com a aparência de objetividade. A liderança responsável é a que torna visível o que o sistema tende a naturalizar. É a que promove culturas onde a dúvida não é fraqueza, mas método. Porque as máquinas aprendem com o que foi; só os humanos conseguem contestá-lo.

Ao mesmo tempo, a delegação do raciocínio às máquinas revela o vazio de propósito. Se a organização sabe calcular, resta-lhe decidir porquê. É aqui que a função diretiva volta a ser humana — não pela emoção, mas pela capacidade de deliberar com consciência.

O novo líder é menos gestor de resultados e mais curador de sentido. A sua competência não está em dominar a tecnologia, mas em situá-la. Não em resistir à IA, mas em impedir que a IA se torne o critério do que é real.

Liderar em tempos de inteligência artificial é isto: sustentar o humano quando o pensamento deixa de ser exclusivo da humanidade. ■

LIDERAR NA FRONTEIRA ENTRE PESSOAS E TECNOLOGIA

Atualmente, ser líder já não é só gerir pessoas; é perceber máquinas sem esquecer a ética, inovar com objetivos e usar a transformação digital para mudar a cultura e o propósito. A inteligência artificial generativa e a automação vieram para alterar as regras do jogo empresarial, desde os processos às equipas. Numa era em que cada decisão é medida, a liderança passou a assumir responsabilidades num território onde a tecnologia e a Humanidade se cruzam de forma inevitável.

INÊS GARCIA MARTINS

O DIA-A-DIA de quem lidera entrou numa nova era, com a digitalização e a Inteligência Artificial (IA) generativa a tornarem as organizações mais rápidas e eficientes, mas também a exporem fragilidades no modelo de liderança tradicional. De acordo com a Gartner, apenas 48% das iniciativas digitais atingem os resultados esperados, sinal de que a tecnologia avança mais depressa do que a capacidade de liderança que a deve orientar.

Da gestão de pessoas à definição de estratégias, multiplicam-se as variáveis que exigem novas competências e uma força de trabalho capaz de colaborar com sistemas inteligentes. A transformação digital deixou de ser apenas um tema estratégico para se tornar também uma questão ética e jurídica.

Tudo isto converge num ponto inevitável – a liderança está a ser reprogramada. Emanuel Agostinho, Strategy & Consulting da Accenture, encara esta evolução como uma libertação, que "dá tempo para pensar estrategica-

- Emanuel Agostinho -
Strategy & Consulting da Accenture

> “UM BOM LÍDER É AQUELE QUE ESTÁ “MAIS PRÓXIMO DA TRANSFORMAÇÃO – NÃO APENAS A INCENTIVÁ-LA, MAS A VIVÊ-LA NO DIA-A-DIA”
>
> EMANUEL AGOSTINHO, STRATEGY & CONSULTING DA ACCENTURE

mente e definir as regras do jogo”. Rui Gonçalves, Partner e Head of Technology Consulting da KPMG Portugal, defende que está a ser reconfigurada “em três dimensões: mentalidade, competências e ferramentas”. Já Sérgio Viana, Managing Partner da Xpand IT, considera que a reprogramação é positiva, desde que o líder continue a garantir que as decisões assentam em informação correta e fiável.

TRANSFORMAÇÃO DIGITAL VS. ADOÇÃO DE FERRAMENTAS

Muitas empresas confundem transformação digital com adoção de ferramentas, e é aí que costumam falhar, defende Sérgio Viana. Aponta que “uma empresa pode adotar várias ferramentas e, na realidade, não estar a fazer qualquer transformação digital efetiva”, sendo que a mudança “implica uma alteração na forma como as empresas funcionam e utilizam tecnologia para servir melhor os seus objetivos e clientes”.

Essa visão é partilhada por Emanuel Agostinho, que sublinha o erro recorrente de tratar as ferramentas como um fim em si mesmas. O Strategy & Consulting da Accenture considera que as organizações mais avançadas na adoção de inteligência artificial são as que constroem primeiro um “núcleo digital robusto” – uma infraestrutura de dados, cloud, e plataformas interoperáveis – antes de dispersar iniciativas isoladas. Sem esse alicerce, diz, os projetos “ficam isolados e têm dificuldades para escalar”.

Nas palavras de Rui Gonçalves, a "transformação digital é uma reformulação estratégica" e, por sua vez, "uma jornada que requer adaptação contínua, compromisso da liderança e um *roadmap* claro" que envolve repensar modelos de negócio, operações e cultura.

O PAPEL DAS CHEFIAS NA NOVA ERA DE TRABALHO

Por se tratar de um processo longo e completo, a transformação digital exige clareza nos objetivos traçados. O desafio passa a ser estrutural e, aqui, o papel das chefias ganha destaque. Sérgio Viana considera que "a mudança tem de ser apoiada pela liderança das empresas".

No entanto, segundo Rui Gonçalves, muitos líderes ainda não alinham estratégia e cultura com tecnologia, limitando-se a iniciativas táticas. Na sua perspetiva, é essencial "definir uma visão clara e comunicá-la continuamente", patrocinar a mudança cultural e criar métricas que reflitam a adoção digital. Com base no "*CEO Outlook 2025*" da KPMG, o responsável destaca que 26% dos CEO valorizam a agilidade e rapidez nas decisões, 24% sublinham a transparência na comunicação e 23% consideram essencial uma gestão ativa de riscos, nomeadamente em áreas como cibersegurança, ética da IA e ESG. O estudo mostra ainda que 71% dos líderes estão a investir fortemente em IA e talento, embora nem todos alinhem esses esforços com a transformação cultural necessária.

- Rui Gonçalves -
Partner e Head of Technology Consulting da KPMG Portugal

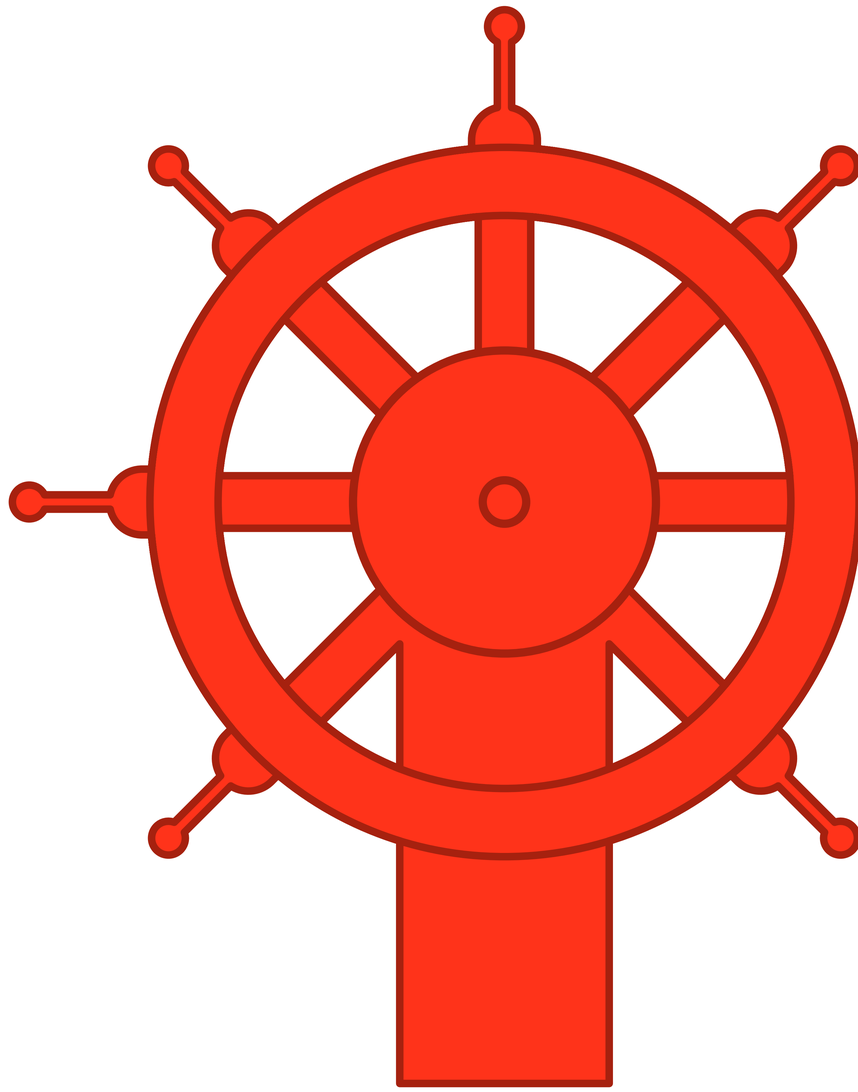
> "A TRANSFORMAÇÃO DIGITAL É UMA REFORMULAÇÃO ESTRATÉGICA" E, POR SUA VEZ, "UMA JORNADA QUE REQUER ADAPTAÇÃO CONTÍNUA, COMPROMISSO DA LIDERANÇA E UM ROADMAP CLARO"
>
> RUI GONÇALVES, PARTNER E HEAD OF TECHNOLOGY CONSULTING DA KPMG PORTUGAL

Um bom líder, na visão de Emanuel Agostinho, é aquele que está "mais próximo da transformação – não apenas a incentivá-la, mas a vivê-la no dia-a-dia". A experiência, afirma, mostra que as organizações mais bem-sucedidas são aquelas em que o C-suite participa ativamente no processo, e não apenas o supervisiona. Numa era em que a velocidade das decisões é crítica, o responsável acredita que a liderança deve ser capaz de equilibrar risco e rapidez, "sabendo quando confiar em modelos e quando exigir intervenção humana".

O IMPACTO DA INTELIGÊNCIA ARTIFICIAL

A esta altura, o impacto da IA nas equipas está a reconfigurar o conceito de liderança, com a IA generativa a "libertar tempo das equipas para tarefas de maior valor". De acordo com Emanuel Agostinho, "as pessoas continuam essenciais na definição do contexto, na tomada de decisão e na relação humana". O foco, diz, passa por gerir a colaboração entre humanos e máquinas e medir o impacto da tecnologia com base em resultados. O futuro, para Sérgio Viana, será de equipas aumentadas por tecnologia, onde os líderes têm de procurar compreender "como liderar estas equipas mistas, tirando partido do melhor que cada elemento tem para oferecer". Rui Gonçalves acrescenta que os gestores estão a transformar-se em "orquestradores", liderando ecossistemas híbridos de pessoas e IA. Esta nova realidade exige requalificação contínua, políticas claras de ética e privacidade e uma comunicação transparente sobre o papel humano.

Entre a automação e o humanismo, o equilíbrio é cada vez mais frágil e, na Xpand IT, acredita-se que "a automação, quando bem feita, liberta as pessoas de tarefas repetitivas e permite focar nas que dependem de competências humanas".



- Sérgio Viana -
Managing Partner da Xpand IT

> “A AUTOMAÇÃO, QUANDO BEM FEITA, LIBERTA AS PESSOAS DE TAREFAS REPETITIVAS E PERMITE FOCAR NAS QUE DEPENDEM DE COMPETÊNCIAS HUMANAS”
>
> SÉRGIO VIANA, MANAGING PARTNER DA XPAND IT

No entanto, Rui Gonçalves alerta para o risco contrário: a desumanização do trabalho, caso a automação não seja acompanhada por uma gestão cultural atenta. “A cultura deve ser uma prioridade estratégica”, afirma, defendendo políticas de governação ética e investimento em competências como empatia, colaboração e liderança.

Alexandra Andrade, Country Manager da Adecco Portugal, afirma que “já não é o futuro, é o presente”. Trabalhar lado a lado com agentes de IA representa uma nova forma de inteligência coletiva e, por isso, quem domina ferramentas *copilot*, entende *prompts* e supervisiona resultados “com espírito crítico, multiplica o seu impacto”. A literacia em IA, diz, “é o novo saber ler e escrever da era digital”; no entanto, a transformação será sempre humana, uma vez que “a inteligência artificial pode amplificar o potencial humano, mas é o ser humano que continuará a dar-lhe direção, ética e alma”.

RECURSOS HUMANOS E EVOLUÇÃO DAS COMPETÊNCIAS

A par da liderança, importa explorar de que modo a transformação digital está a reconfigurar o mercado de trabalho e a redefinir o conceito de talento. A Country Manager da Adecco Portugal descreve o momento como “uma revolução silenciosa – uma transformação que não é apenas tecnológica, é profundamente humana”. No centro dessa mudança, afirma continua a estar

"aquilo que nenhuma máquina poderá replicar: o nosso propósito, a nossa empatia e a nossa capacidade de criar sentido". Neste momento, as empresas procuram "construtores de impacto", profissionais que dominam IA generativa, *machine learning*, dados e automação inteligente, mas que saibam transformar tecnologia em valor, "para o negócio e para as pessoas".

Segundo a responsável, "o talento do futuro é híbrido: combina o raciocínio lógico de um engenheiro com a sensibilidade de um líder". São perfis que unem pensamento estratégico e empatia, capazes de compreender tanto métricas como emoções. Num mundo cada vez mais automatizado, "o diferencial humano é o que realmente faz a diferença", e competências como liderança, comunicação e capacidade de inspirar equipas tornaram-se simultaneamente as mais procuradas e as menos comuns.

- Alexandra Andrade -
Country Manager da Adecco Portugal

Enquanto, diz, "a inovação corre e a aprendizagem tropeça", é fundamental encurtar essa distância e reinventar a forma de aprender. As empresas mais avançadas estão a criar "academias internas de IA, com programas curtos, práticos e centrados em desafios reais", com o objetivo de "aprender 'fazendo' – e fazer 'aprendendo'". A ideia passa por colocar a aprendizagem "no centro da estratégia e da performance", porque "o futuro não será de quem sabe mais, mas de quem aprende mais depressa, e com propósito".

> "A INTELIGÊNCIA ARTIFICIAL PODE AMPLIFICAR O POTENCIAL HUMANO, MAS É O SER HUMANO QUE CONTINUARÁ A DAR-LHE DIREÇÃO, ÉTICA E ALMA"
>
> ALEXANDRA ANDRADE, COUNTRY MANAGER DA ADECCO PORTUGAL

IMPLICAÇÕES JURÍDICAS DA NOVA FORMA DE TRABALHO: DECISÕES COM IA OU PELA IA

A transformação digital trouxe novos dilemas jurídicos para as empresas, sobretudo com a incorporação de sistemas de IA nos processos de decisão. A questão da responsabilidade está no centro do debate: quando uma decisão automatizada dá errado, quem responde pela mesma? Para Daniel Reis, Sócio de IPT da DLA Piper, "a responsabilidade é da pessoa (singular ou empresa) que toma a decisão, utilizando um sistema de IA ou decisões automatizadas" e dá o exemplo de um banco que ao "recusar conceder um crédito com base numa decisão automatizada, a responsabilidade será do banco. Em condições normais, nem o gestor nem o programador serão responsáveis".

- Daniel Reis -
Sócio de IPT da DLA Piper

> "A RESPONSABILIDADE É DA PESSOA (SINGULAR OU EMPRESA) QUE TOMA A DECISÃO, UTILIZANDO UM SISTEMA DE IA OU DECISÕES AUTOMATIZADAS"
>
> DANIEL REIS, SÓCIO DE IPT DA DLA PIPER

Martim Bouza Serrano, Sócio da área de Tecnologias, Media e Telecomunicações da CCA Law Firm, dá conta da complexidade do tema, já que "a responsabilidade depende sempre do contexto e do grau de autonomia do sistema. Na prática, o problema raramente é da IA, mas sim de quem a concebe, implementa, supervisiona ou decide delegar-lhe a capacidade de decisão". O especialista alerta para a "difusão da responsabilidade" e lembra que "a cadeia de decisão torna-se opaca, e os tribunais vão ter de analisar e identificar quem responde".

A fronteira entre decisões tomada com IA e decisões tomadas pela IA é um ponto de divergência. Há quem desvalorize a distinção, como é o caso de Daniel Reis, que afirma que "do ponto de vista jurídico não é relevante uma decisão tomada pela IA, a decisão é sempre tomada por quem está a utilizar IA". Já Martim Bouza Serrano considera que a diferença é importante porque "uma decisão com IA significa que o humano continua no centro", isto é, "a IA apoia, mas não substitui o juízo humano". No entanto, aponta, "uma decisão pela IA implica delegação total ou quase total da decisão, o que levanta questões de responsabilidade, transparência e até de validade jurídica".

REGULAMENTAÇÃO COMO PILAR DA IA

A velocidade do progresso tecnológico revela-se um desafio para o enquadramento jurídico atual e Daniel Reis considera que "a tecnologia evolui sempre mais rápido do que a regulação" e isso "não é um fenómeno novo". Por isso, as empresas já estão habituadas a viver com incerteza e nada disto é "muito grave". O essencial, defende Martim Bouza Serrano, "é garantir princípios sólidos e mecanismos de adaptação". A regulação, aponta, deve gerar confiança "sem travar a inovação".

Este tópico traz algumas nuances porque "o legislador chega sempre depois, muito depois de a inovação ter já transformado práticas e modelos de negócio e, por norma, com regras para uma realidade que, entretanto, também já se alterou". Nas palavras do especialista, "a principal diferença é a escala e a velocidade com que a IA se está a entranhar em todos os setores, reduzindo drasticamente a margem de erro das empresas".

Os riscos legais começam muito antes de o algoritmo ser ativado e Daniel Reis nota que "o risco

“O PROBLEMA RARAMENTE É DA IA, MAS SIM DE QUEM A CONCEBE, IMPLEMENTA, SUPERVISIONA OU DECIDE DELEGAR-LHE A CAPACIDADE DE DECISÃO”

MARTIM BOUZA SERRANO, SÓCIO DA ÁREA DE TECNOLOGIAS, MEDIA E TELECOMUNICAÇÕES DA CCA LAW FIRM

- Martim Bouza Serrano -
Sócio da área de Tecnologias, Media e Telecomunicações da CCA Law Firm

está na utilização de IA”. Por isso, defende que “a aquisição ou desenvolvimento de soluções que utilizem IA deve ter presente as obrigações legais aplicáveis” e que compreender o impacto da sua utilização deve ser “encarado como um processo de negócio a introduzir em todas as empresas que pretendam beneficiar da IA”. Martim Bouza Serrano acrescenta que o perigo surge “na definição do propósito e na recolha dos dados”. É aí que “se decidem as bases do tratamento, a proporcionalidade, a transparência e o eventual viés”.

“O erro mais comum continua a ser a falta de antecipação e preparação das empresas para as constantes alterações legislativas”, indica Martim Bouza Serrano, que critica a tendência para encarar o regulamento “como mais um conjunto de requisitos burocráticos, que não apresenta qualquer vantagem para o dia-a-dia do negócio”. A par disso, Daniel Reis, vê “a aquisição de soluções sem se analisar ou sequer pensar nos riscos que podem daí resultar” como principal problema.

Com a entrada em vigor do AI Act e de outros regulamentos europeus, as empresas estão a ser obrigadas a reverem contratos, políticas de privacidade e cláusulas de propriedade intelectual. “Estamos a assistir a uma revisão profunda de contratos tecnológicos, sobretudo nas cláusulas de responsabilidade, confidencialidade, propriedade de dados e outputs gerados”, reforça Martim Bouza Serrano. ■

claranet®

POR ANTÓNIO MAIA,
Applications & Workplace Senior Director,
Claranet Portugal

MODERNIZAR PARA LIDERAR:
O NOVO MANDATO DA ERA DIGITAL

A era digital redefiniu o conceito de liderança. Hoje, o papel do líder vai muito além da função de gestor: um líder é um orquestrador da mudança – um impulsionador de inovação, capaz de alinhá-la com os objetivos de negócio, enquanto ajuda a organização a navegar num ambiente de constante mudança.

A TECNOLOGIA evoluiu de um elemento de suporte às operações para um fator determinante na forma como equipas interagem, colaboram e inovam. O ritmo da mudança tecnológica dita a competitividade, e os líderes precisam de traduzir essa transformação em valor percebido - é aqui que a *modernização aplicacional* assume um papel central na estratégia organizacional, como motor da inovação contínua.

Cloud computing, Inteligência Artificial e Big Data estão a impulsionar a transformação digital, redefinindo processos, cadeias de valor e modelos de operação. Neste contexto, as *aplicações de negócio* deixaram de ser ferramentas operacionais isoladas e tornaram-se o sistema nervoso central das organizações mais 'digitais', conectando equipas, dados e processos.

- António Maia -
Applications & Workplace Senior Director, Claranet Portugal

COMBINADAS, ESTAS ABORDAGENS [SOLUÇÕES **CLOUD-NATIVE** E PLATAFORMAS **LOW-CODE**] CRIAM UMA BASE TECNOLÓGICA SÓLIDA, CAPAZ DE SUSTENTAR DECISÕES MAIS RÁPIDAS, INFORMADAS E ESTRATÉGICAS, MELHORAR A EXPERIÊNCIA DO CLIENTE E REFORÇAR A FLEXIBILIDADE E ESCALABILIDADE DAS OPERAÇÕES. AO MESMO TEMPO, IMPULSIONAM UMA **CULTURA DE INOVAÇÃO** CONTÍNUA EM TODA A ORGANIZAÇÃO. UM LÍDER QUE COLOCA A **MODERNIZAÇÃO** NO CENTRO DA ESTRATÉGIA TORNA-SE, ASSIM, UM PROMOTOR DE AGILIDADE, PRODUTIVIDADE E INOVAÇÃO.

A adoção de *soluções cloud-native* tem permitido às organizações inovar rapidamente e responder de forma ágil às exigências do mercado – uma tendência reforçada pela IDC, que prevê que, em 2025, 90% das novas aplicações desenvolvidas sejam cloud-native. Paralelamente, plataformas low-code ajudam a reduzir custos de desenvolvimento e a acelerar a implementação de soluções personalizadas. Como a *Gartner* sintetiza, a via certa não é o big-bang, mas uma modernização contínua, iterativa e orientada a produto, que reduz risco, preserva valor do core e acelera a obtenção de resultados.

Combinadas, estas abordagens criam uma base tecnológica sólida, capaz de sustentar decisões mais rápidas, informadas e estratégicas, melhorar a experiência do cliente e reforçar a flexibilidade e escalabilidade das operações. Ao mesmo tempo, impulsionam uma cultura de inovação contínua em toda a organização. Um líder que coloca a modernização no centro da estratégia torna-se, assim, um promotor de agilidade, produtividade e inovação.

DOS DADOS À AÇÃO: A FORÇA DAS DECISÕES DATA-DRIVEN E DA INTELIGÊNCIA ESTRATÉGICA

A *modernização aplicacional* não é apenas operacional, é também estratégica, permitindo às lideranças atuar com maior precisão num ambiente complexo. A principal vantagem competitiva nasce da capacidade de transformar dados em decisões concretas e confiáveis. Decisões data-driven ajudam os líderes a prever tendências, mitigar riscos e identificar oportunidades antes da concorrência.

As aplicações inteligentes e as plataformas analíticas avançadas oferecem visibilidade em tempo real sobre o desempenho organizacional, o

A DECISÃO MAIS ESTRATÉGICA É ESCOLHER O PARCEIRO CERTO, QUE PRIVILEGIA QUEM PROVE CAPACIDADE END-TO-END – DO ASSESSMENT AO REFACTOR –, EXCELÊNCIA OPERACIONAL, DOMÍNIO MULTICLOUD E UM MODELO QUE ELEVA A MATURIDADE ORGANIZACIONAL..

comportamento dos clientes e a eficiência operacional, tornando a gestão mais informada, transparente e ágil. Mas este nível de visão exige também uma cultura de aprendizagem, colaboração e partilha, onde a tecnologia complementa a intuição e reforça a capacidade estratégica das equipas.

CULTURA DE INOVAÇÃO: PESSOAS NO CENTRO DA TRANSFORMAÇÃO

A tecnologia, por si só, não garante inovação. É a cultura organizacional que a transforma em resultados tangíveis. Criar um ambiente onde a inovação seja constante depende de líderes que incentivem a curiosidade, a colaboração interdisciplinar e a experimentação. A integração entre cultura e tecnologia é o fator que permite traduzir a inovação em impacto real nos resultados da organização.

As *aplicações modernas* libertam as equipas de tarefas repetitivas, permitindo-lhes concentrar-se em iniciativas mais criativas e estratégicas. Equilibrar a pressão por resultados imediatos com o investimento em inovação é a chave para distinguir organizações reativas de organizações verdadeiramente resilientes.

Na modernização aplicacional, colocar o colaborador no centro não é "nice to have", é condição de sucesso: como evidencia o *The Enterprisers Project*, transformações estagnam sem employee experience e novos modelos de trabalho sólidos - e é precisamente o IT que deve orquestrar plataformas, práticas e métricas para produtividade híbrida, garantindo continuidade da mudança e retenção de talento.

A decisão mais estratégica é escolher o parceiro certo, que privilegia quem prove capacidade end-to-end – do assessment ao refactor –, excelência operacional, domínio multicloud e um modelo que eleva a maturidade organizacional.

Assim, modernizar para liderar é sinónimo de transformar tecnologia em valor, dados em visão e inovação em propósito. E os líderes que o fazem estão, sem dúvida, a colocar as suas organizações na linha da frente da transformação digital. Este é o caminho que distingue aqueles que moldam o futuro daqueles que apenas o acompanham. ■

"PODEMOS DIZER QUE FALHAR NÃO É OPÇÃO; MAS ÀS VEZES FALHAR É A INEVITABILIDADE"

Henrique Carreiro, Diretor da IT Insight, abriu mais uma edição da IT Insight Talks com uma apresentação dedicada à continuidade de negócio, com foco na importância da perceção das falhas e no uso do tempo e da comunicação a favor da recuperação.

MARTA QUARESMA FERREIRA

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

Fotografias: Luís Santos Ribeiro

"**QUANTO MAIOR FOR O TEMPO** para recuperar, maior é o custo". Este foi um dos motes da apresentação de Henrique Carreiro, Diretor da IT Insight, no âmbito de mais uma IT Insight Talks, que decorreu no Fórum Tecnológico Lispolis, em Lisboa.

Com o tema Business Continuity em discussão, Henrique Carreiro começou por esclarecer que a continuidade de negócio pressupõe um conjunto de circunstâncias a ter em consideração, como é o caso de desastres naturais, questões processuais e até mudanças relacionadas com fornecedores, num mundo cada vez mais conectado.

O Diretor da IT Insight sublinhou que os custos de um incidente tendem a aumentar com o tempo, nomeadamente quando há uma perceção tardia sobre os incidentes, logo, uma recuperação também ela tendencialmente mais lenta. "Nada disto é *paperwork*. Podemos pensar que temos isto no papel, mas nada vai funcionar se, na prática, não forem feitos outros processos".

PREVENÇÃO É DIFÍCIL, MAS PERCEÇÃO DAS FALHAS É CHAVE

Numa semana marcada pelo incidente da AWS, que afetou a região US-EAST-1 e que impactou os mais diversos serviços na internet, Henrique Carreiro relembrou alguns dos exemplos de interrupção de serviço que afetaram algumas empresas este ano, como foi o caso da Jaguar Land Rover, cujas linhas de produção foram atacadas; o ataque à Marks & Spencer, que colocou parte das lojas *offline* e obrigou a empresa de comércio britânico a regressar ao pagamento manual; e o caso do incêndio num data center sem *backup* na Coreia do Sul que culminou na perda de uma elevada quantidade de dados.

O Diretor da IT Insight sublinhou que a prevenção para os casos exemplificados "é difícil", não existindo uma "ciência exata". No entanto, apesar das mais diversas origens das interrupções, a pressão mantém-se e o tempo é o fator central na hora de recuperar.

USAR TEMPO E A COMUNICAÇÃO A FAVOR

Ao encarar um problema ou um incidente, o tempo adquire um peso relevante na balança. "Tem de haver uma forma de sermos alertados para o facto de a falha estar a acontecer", reiterou Henrique Carreiro, que aponta para um possível conjunto de sistemas que podem auxiliar na deteção. "Outro ponto importante é o tempo que conseguimos recuperar – não o serviço todo, mas um mínimo operacional", frisou.

Aliado a este tema, Henrique Carreiro destacou a importância de existirem planos de comunicação que entram para a equação da continuidade de negócio para garantir uma comunicação constante em caso de falha. "Há casos em Portugal em que levamos horas e dias e em que estamos completamente 'às escuras' em termos de comunicação. A nível de cultura nacional, ainda não chegámos a esse ponto".

FALHAR DE FORMA MAIS SEGURA

Em caso de falha, o especialista considera que deve existir "um mínimo de qualidade" perante a mesma, com a implementação de um plano B, que não passa necessariamente por garantir o total

funcionamento dos serviços, mas sim um serviço que, embora mais reduzido, forneça garantias de segurança. Outro dos pontos elencados para garantir a continuidade de negócio passa pelo improviso e pela preparação prévia, com decisões pré-aprovadas para os mais diversos cenários: "Podemos dizer que falhar não é opção; mas às vezes falhar é a inevitabilidade", relembra.

Na preparação dos planos de continuidade de negócio, Henrique Carreiro afirma que é igualmente necessário garantir uma rede de fornecedores e compreender junto dos mesmos "os ritmos de atualização e os planos B em caso de falha".

OS NÃO-NEGOCIÁVEIS NA RECUPERAÇÃO

O Diretor da IT Insight considera que é necessário olhar para "os mínimos" que têm de continuar a funcionar perante uma falha e perceber como é que vão operar. A visão passa por tirar os procedimentos do papel e realizar testes em tempo real de forma a compreender o seu real funcionamento.

O padrão de não-negociáveis em caso de recuperação deve incluir a nomeação de um responsável ao nível dos serviços críticos; um modo seguro que garante o mínimo necessário ao funcionamento e uma solução alternativa testada; um *bypass* com visibilidade para números, nomeadamente o ritmo de recuperação; e atualizações ritmadas aos clientes, mesmo que as notícias não sejam animadoras.

"Têm de existir processos pré-aprovados. Se tivermos esta ideia presente e se estiver determinado quem faz o quê quando acontecer o inevitável, o negócio não está necessariamente seguro, mas há uma calma maior que, ainda assim, não deve esconder a preocupação. Contudo, não devemos viver em circunstâncias de crise permanente", conclui Henrique Carreiro. ■

"TÊM DE EXISTIR PROCESSOS PRÉ-APROVADOS. SE TIVERMOS ESTA IDEIA PRESENTE E SE ESTIVER DETERMINADO QUEM FAZ O QUÊ QUANDO ACONTECER O INEVITÁVEL, O NEGÓCIO NÃO ESTÁ NECESSARIAMENTE SEGURO, MAS HÁ UMA CALMA MAIOR QUE, AINDA ASSIM, NÃO DEVE ESCONDER A PREOCUPAÇÃO. CONTUDO, NÃO DEVEMOS VIVER EM CIRCUNSTÂNCIAS DE CRISE PERMANENTE"

CONTINUIDADE DE NEGÓCIO:
A REDUNDÂNCIA DEIXOU DE SER OPCIONAL

Quando os sistemas críticos de uma organização média migraram para a cloud e as operações se tornaram progressivamente digitais por defeito, o custo de uma interrupção multiplicou-se exponencialmente. Na era em que a continuidade de negócio deixou de ser uma opção, Commvault, IP Telecom, Securnet, Veeam e VisionWare partilham a sua visão sobre o mercado de business continuity.

RUI DAMIÃO

O CUSTO MÉDIO de *downtime* em IT era, há vários anos, estimado em 5.600 dólares por minuto, mas em setores como banca ou e-commerce esse valor pode facilmente ultrapassar o milhão de dólares por hora. O problema é que muitas organizações ainda tratam a continuidade de negócio como um exercício de *compliance* e não como uma estratégia operacional.

Existe um plano, guardado numa pasta partilhada, que não é testado há anos. Há *backups* automáticos configurados, mas ninguém verificou se são efetivamente recuperáveis. Com a importância de manter os negócios *up-and-running* 24/7, Commvault, IP Telecom, Securnet, Veeam e VisionWare partilharam, num evento híbrido, a sua visão sobre o mercado de continuidade de negócio.

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

AOS DIAS DE HOJE, O QUE É QUE CONSIDERAM SER *BUSINESS CONTINUITY* E QUAIS OS ASPETOS QUE DEVEM SER ENGLOBADOS NESTA CATEGORIA? QUANDO HÁ UMA FALHA, QUEM É NORMALMENTE O CULPADO: A TECNOLOGIA OU AS DEPENDÊNCIAS QUE NINGUÉM DOCUMENTOU?

BRUNO CASTRO, FOUNDER & CEO, VISIONWARE: "A continuidade de negócio não são só *backups*. É a capacidade de repor a base do negócio depois de algum tipo de incidente. Estamos muitas vezes envolvidos em processos de recuperação de desastre e olhamos para isto 'à engenheiro': há muitas variáveis. Temos de gerir cada um dos pilares dessas variáveis, com base no orçamento e na importância para o negócio. Tem de ser o *top management* a definir essa importância e a sua implementação"

- Bruno Castro, VisionWare -

> "AGORA HÁ UMA EXPLOSÃO DE COISAS NA INTERNET EM QUE TUDO SALTOU PARA A INTERNET. SE HOUVE UMA GRANDE QUANTIDADE DE PESSOAS A IR PARA A INTERNET, TAMBÉM O CIBERCRIME EXPLODIU COM ATAQUES ESPECIALIZADOS PARA AS ORGANIZAÇÕES. O RANSOMWARE É SÓ A FASE MAIS VISÍVEL DO CIBERCRIME"
>
> BRUNO CASTRO, FOUNDER & CEO, VISIONWARE

LUÍS FEITOR, ADVANCE SPECIALIST ENGINEER, COMMVAULT: "Este é um tema complexo. Há muitas variáveis envolvidas. A continuidade de negócio tem de se manter em que circunstância? Não é apenas recuperação de desastre. A culpa só se vê no fim; uma grande generalidade das empresas que consegue sobreviver a um ciberataque, ao fim de um ano, fecha as portas. Este é um cenário que é preciso preparar; temos de olhar para o cenário real e procurar implementar as medidas necessárias para o prevenir"

- Emanuel Santos, SOC Manager, Securnet -

EMANUEL SANTOS, SOC MANAGER, SECURNET: "A continuidade de negócio parece um bicho-papão e parece algo muito complexo. Tem uma série de *checklists* que se deve seguir, mas a NIS2 vai ajudar muito nisto; a continuidade de negócio está muito presente na NIS2. Estes planos de continuidade de negócio têm de ser implementados a cada empresa porque as empresas não são iguais umas às outras. Isto não é só tecnologia, também são as pessoas, e é preciso documentar dependências – de fornecedores, obviamente, mas também das pessoas"

> "ANTES OS BACKUPS IMUTÁVEIS CHEGAVAM E ESTAVAM ÓTIMOS, MAS AGORA HÁ UMA CULTURA DE EXTORSÃO: FURTAM OS DADOS E AMEAÇAM A SUA PUBLICAÇÃO. AS ORGANIZAÇÕES PRECISAM DE UM PARCEIRO TECNOLÓGICO QUE OLHE PARA ISTO"
>
> EMANUEL SANTOS, SOC MANAGER, SECURNET

AS ORGANIZAÇÕES COMPRAM SOLUÇÕES DE *BUSINESS CONTINUITY*. QUAL É A PERCENTAGEM QUE EFETIVAMENTE AS IMPLEMENTA CORRETAMENTE VERSUS AQUELES QUE TÊM A TECNOLOGIA INSTALADA, MAS CONFIGURADA DE FORMA QUE NÃO FUNCIONARIA NUMA CRISE REAL?

FILIPE FRASQUILHO, DIRETOR DE SERVIÇOS TI, IP TELECOM: "As pessoas são um dos pontos mais críticos desta equação. A grande maioria das organizações não têm planos de continuidade de negócio; têm planos de *disaster recovery* porque falta, normalmente, o ponto das pessoas. Temos tido uma noção clara que as empresas têm planos de *disaster recovery*, e até funcionam, mas é muito para o *compliance*. No entanto, planos reais, onde também entram as pessoas e os processos, são muito poucas que têm"

- Filipe Frasquilho, IP Telecom -

> "O PLANO DE CONTINUIDADE DE NEGÓCIO TEM DE COMEÇAR NO BOARD E TEM DE TER A CONTRIBUIÇÃO DE TODAS AS PESSOAS DA EMPRESA. ESSE ENVOLVIMENTO É FUNDAMENTAL PARA QUE, DEPOIS, OS TESTES FUNCIONEM"
>
> FILIPE FRASQUILHO, DIRETOR DE SERVIÇOS TI, IP TELECOM

POR NORMA, O QUE FALHA NOS PROJETOS DE IMPLEMENTAÇÃO DE *BUSINESS CONTINUITY* QUANDO O CLIENTE DESCOBRE QUE O PLANO NÃO FUNCIONA: TECNOLOGIA, PROCESSO OU PESSOAS?

RICARDO OLIVEIRA, TERRITORY MANAGER, VEEAM: "Este triângulo e o ISO 27001 é muito importante. Não existe um ponto de falha único; podemos chegar a uma determinada organização que compra muita tecnologia e a que é certa, mas pode ter a 'casa desarrumada' ou não ter as pessoas suficientes. Outras podem ter as pessoas, mas não têm o orçamento disponível para o investimento necessário. Para além destes três pontos, há um que está ligado às pessoas e que vou chamar de cultura e às vezes os planos falham por uma questão de cultura"

FILIPE FRASQUILHO, IP TELECOM: "O plano de continuidade de negócio tem de começar no *board* e tem de ter a contribuição de todas as pessoas da empresa. Esse envolvimento é fundamental para que, depois, os testes funcionem. Dou um exemplo: tivemos, no início do ano, dois sismos relativamente pequenos; quem é que aplicou os planos para sismos? Praticamente ninguém, mas as crianças, por exemplo, fizeram porque são treinadas todos os anos para isso"

COM AMBIENTES HÍBRIDOS E MULTICLOUD, O *RECOVERY TIME OBJECTIVE* REAL AUMENTOU OU DIMINUIU? TEMOS MAIS FERRAMENTAS, MAS TAMBÉM MAIS PONTOS DE FALHA; COMO É QUE SE EQUILIBRA?

LUÍS FEITOR, COMMVAULT: "Estes ambientes multicloud trazem novos desafios, até porque os *cloud providers* são muito distintos e as funcionalidades também. Os clientes protegem o *workload* que está na cloud, mas nem sempre protegem a cloud em si. Temos de estar preparados para recuperar em qualquer local e fazer a portabilidade dos dados de um local para o outro, mas também a configuração desses ambientes. É preciso fazer, por vezes, um *trade off* entre aquilo que precisamos de continuidade de negócio e aquilo que podemos investir"

RICARDO OLIVEIRA, VEEAM: "Consideramos que existem desafios, de facto, mas o *governance* dos dados torna-se mais complicado com a dispersão dos dados. Se temos os nossos dados numa caixinha na nossa casa, o *governance* é completamente diferente de os ter numa multicloud. Não podendo fugir desta realidade – seja em maior ou menos escala –, também pode ser uma oportunidade, porque num cenário de *disaster recovery* em que as pessoas têm tudo on-premises, os dados que estão em cloud provavelmente vão ser mais difíceis de recuperar"

COMO É QUE O AUMENTO DE CIBERATAQUES, NOMEADAMENTE DE RANSOMWARE, MUDOU A ABORDAGEM DOS FORNECEDORES DE SERVIÇOS E DOS CLIENTES? OS *BACKUPS* IMUTÁVEIS SÃO SUFICIENTES OU É PRECISO MAIS?

EMANUEL SANTOS, SECURNET: "O ransomware profissionalizou-se. Para além de terem existido muitos ataques, o pânico instala-se nas organizações, mas para nós é só mais um dia. O que sentimos é que são os mesmos grupos a terem abordagens completamente diferentes. Vê-se uma aceleração muito rápida. Antes os *backups* imutáveis chegavam e estavam ótimos, mas agora há uma cultura de extorsão: furtam os dados e ameaçam a sua publicação. As organizações precisam de um parceiro tecnológico que olhe para isto e que as aconselhe da melhor maneira"

LUÍS FEITOR, COMMVAULT: "A abordagem tem vindo a mudar por necessidade. Podíamos enfrentar este cenário com uma terceira cópia num ambiente isolado, mas, por vezes, esses dados também já podem estar comprometidos. Embora tenhamos pessoas e tecnologia altamente especializada, os ataques continuam a ser bem-sucedidos. Quando a encriptação ocorre num determinado sistema, o comportamento desse próprio sistema muda e, assim, é preciso definir qual é o comportamento habitual desses sistemas"

- Luís Feitor, Commvault -

> "A IA DEVE SER APLICADA A CENÁRIOS EM QUE TRAZ BENEFÍCIOS CLAROS. NA CONTINUIDADE DE NEGÓCIOS E NA PROTEÇÃO DE DADOS PODE TER A AJUDA DA INTELIGÊNCIA ARTIFICIAL PARA ANALISAR LOGS"
>
> LUÍS FEITOR, ADVANCE SPECIALIST ENGINEER, COMMVAULT

FILIPE FRASQUILHO, IP TELECOM: "Não são os fornecedores que estão a fazer alteração na abordagem. Os clientes é que estão a mudar o paradigma. O que temos reparado é que os clientes já se preocupam – e ainda bem – em ter várias cópias, dados imutáveis, tudo coisas que há uns anos as organizações achavam que não era necessário. O paradigma mudou porque as empresas viram outras ao seu lado a serem atacadas e a terem problemas graves"

RICARDO OLIVEIRA, VEEAM: “Há uma mudança de paradigma e de escala dos ataques. A escala aumentou muito e o ransomware não é o único problema da cibersegurança; o ransomware é facilmente escalável para os atacantes. É preciso ter uma abordagem holística na componente da segurança. Também a forma como o ataque é feito é diferente hoje, porque existe uma preparação por parte do cibercriminoso”

BRUNO CASTRO, VISIONWARE: “Estou no mercado há vários anos e quando nos questionam o que é que mudou, principalmente foi um banho de humildade. Se nos perguntassem um dia,antes do ataque à Vodafone se aquilo era possível de acontecer, eu dizia que era impossível. Agora há uma explosão de coisas na Internet em que tudo saltou para a Internet. Se houve uma grande quantidade de pessoas a ir para a Internet, também o cibercrime explodiu com ataques especializados para as organizações. O ransomware é só a fase mais visível do cibercrime”

O *BUSINESS CONTINUITY* COMPETE POR ORÇAMENTO COM INOVAÇÃO E NOVOS PROJETOS. COMO É QUE SE PODE CONVENCER O RESPONSÁVEL FINANCEIRO A INVESTIR EM ALGO QUE, SE FUNCIONAR BEM, NÃO ACONTECE NADA? QUE MÉTRICAS OU ARGUMENTOS FUNCIONAM?

FILIPE FRASQUILHO, IP TELECOM: "Não é assim tão difícil. Estamos a falar de algo que tem a ver com o negócio e a sua continuidade; se querem que o negócio continue, têm de fazer o investimento necessário para que isso aconteça. Uma forma simples é perguntar para que é que querem os seguros? Ninguém os quer utilizar, mas todos têm. É certo que muito é por obrigação, mas a NIS2 também terá impacto nesse ponto que leva a esse caminho e que vai ajudar a quem decide. Isto faz parte do negócio"

RICARDO OLIVEIRA, VEEAM: "Se estamos a falar com o *board*, estes *stakeholders* têm objetivos, tal como nós. Temos de conseguir pôr um número em cima da mesa, colocar em cifrões quanto custa à nossa organização estar em baixo durante um determinado tempo que faça sentido. Se isso não for suficiente para convencer o negócio de que é preciso investir na continuidade de negócio, então provavelmente não temos os valores certos para apresentar"

- Ricardo Oliveira, Veeam -

> "A ESCALA AUMENTOU MUITO E O RANSOMWARE NÃO É O ÚNICO PROBLEMA DA CIBERSEGURANÇA; O RANSOMWARE É FACILMENTE ESCALÁVEL PARA OS ATACANTES. É PRECISO TER UMA ABORDAGEM HOLÍSTICA NA COMPONENTE DA SEGURANÇA"
>
> RICARDO OLIVEIRA, TERRITORY MANAGER, VEEAM

A INTELIGÊNCIA ARTIFICIAL (IA) GENERATIVA E A AUTOMAÇÃO PODEM ACELERAR A RECUPERAÇÃO OU CRIAR RISCOS? ESTÃO A VER OS CLIENTES A INCORPORAR ESTA TECNOLOGIA NOS PLANOS DE *BUSINESS CONTINUITY* OU AINDA É MUITO EXPERIMENTAL?

EMANUEL SANTOS, SECURNET: "As equipas com alguma maturidade já se começam a ver, mas ainda é muito experimental porque há muitos riscos. Fala-se de inteligência artificial, mas ainda é um assunto desconhecido. Aquilo que é controlado é respeitado e não vejo nenhuma organização a controlar internamente a inteligência artificial. A tecnologia é, sem dúvida, muito boa, mas tem muitos riscos e é apenas um tema experimental quando falamos da continuidade de negócios. A inteligência artificial é muito boa se treinarem o modelo, mas as pessoas não o treinam; colocam apenas informações para lá"

BRUNO CASTRO, VISIONWARE: "A inteligência artificial passou a ser o tema mais *trendy* a seguir à cibersegurança. A utilização de IA é inevitável e é provavelmente uma das maiores inovações a seguir à Internet. Se a adoção de tecnologia já é um risco para a sociedade, algo com IA tem um potencial muito maior; nas organizações é muito maior. Temos de colocar barreiras e controlos para impor limites, mas também para perceber os desafios que vão existindo. As organizações querem utilizar IA porque acham que vão acabar se não o fizerem, e não é assim; temos de impor o mesmo *framework* de segurança que qualquer outra solução"

LUÍS FEITOR, COMMVAULT: "A IA deve ser aplicada a cenários em que traz benefícios claros. Na continuidade de negócios e na proteção de dados pode ter a ajuda da inteligência artificial para analisar *logs*. Neste caso concreto, a inteligência artificial ajuda muito na automação, quando temos de criar um *workflow* e caminhar, validar e testar. Temos de garantir a veracidade daquilo que a inteligência artificial nos está a dizer"

SE TIVESSEM DE DAR APENAS UMA RECOMENDAÇÃO ACIONÁVEL QUE UMA EMPRESA POSSA IMPLEMENTAR ATÉ AO FINAL DO ANO PARA MELHORAR A SUA CONTINUIDADE DE NEGÓCIO, SEM GRANDE INVESTIMENTO, QUAL SERIA?

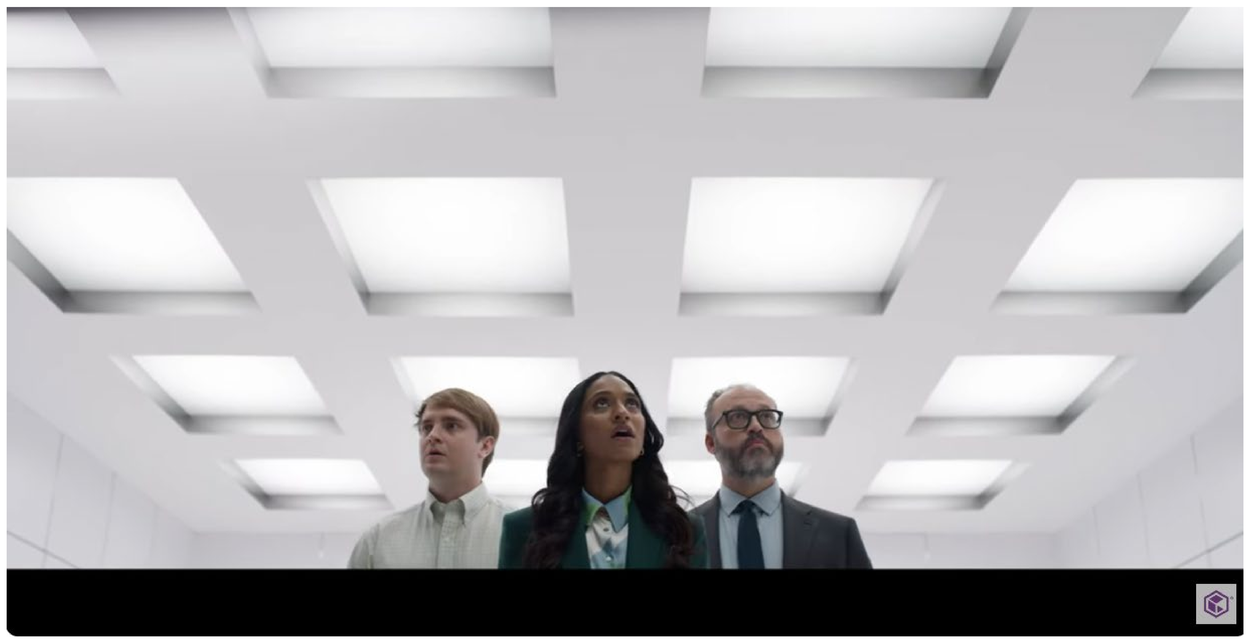
BRUNO CASTRO, VISIONWARE: "Primeiro, devem fazer as soluções à medida das organizações e não ir atrás daquilo que o mercado está a tentar vender. Depois, é importante ser feito com alguém que já o fez e não que diz que já o fez. Por fim, testar, de forma aberta e sem constrangimentos, o modelo de continuidade de negócio porque, quando precisarem, ele tem mesmo de funcionar"

EMANUEL SANTOS, SECURNET: "É preciso que as pessoas, por vezes, troquem de funções para, quando o momento surgir, haver mais do que uma pessoa que saiba fazer o que é necessário porque as pessoas também falham, também podem não estar disponíveis. Quando o momento chegar, é sempre melhor haver duas ou mais pessoas que sabem do tema do que só uma que, naquele momento, pode falhar" ■

Commvault®

PORQUE SÃO AS CLEANROOMS ESSENCIAIS PARA UMA CIBERRECUPERAÇÃO EFICAZ?

As salas limpas ou cleanrooms, também conhecidas como ambientes de recuperação isolados (Isolated Recovery Environments, IRE) — são tecnologias seguras, concebidas para evitar a contaminação de dados e o acesso não autorizado ou a introdução de código malicioso.



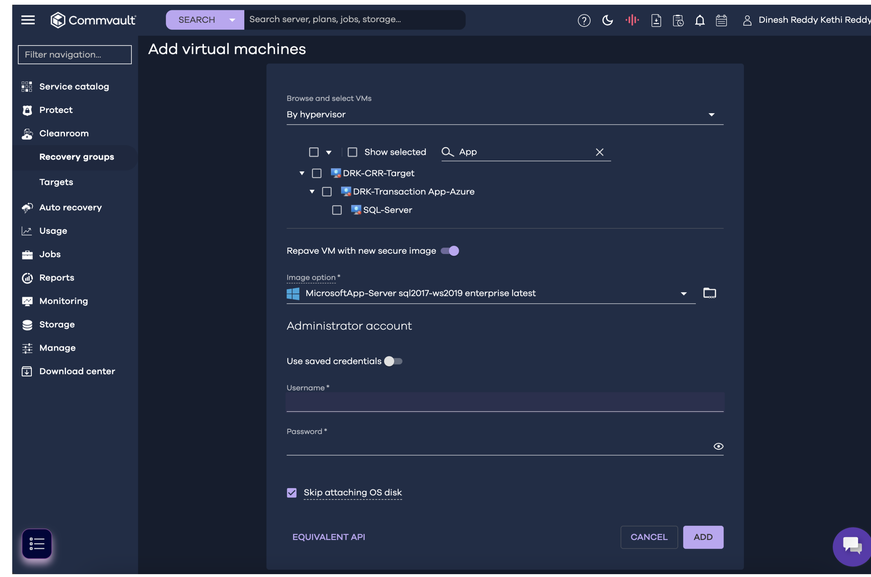
ESTES ESPAÇOS SEGUROS, independentes e isolados de software ou hardware infetado estão a tornar-se um elemento essencial para prevenir danos nos dispositivos de armazenamento e preservar a integridade dos dados recuperados após uma violação de segurança. São amplamente utilizadas por organizações que exigem um controlo rigoroso dos seus processos de proteção e recuperação de dados. Entre estas contam-se entidades governamentais e de defesa, empresas de cibersegurança e os sectores financeiro, aeroespacial e da saúde, entre outros, onde o impacto de um ciberataque pode ser especialmente prejudicial.

Na prática, as cleanrooms desempenham um papel crucial na garantia da segurança, manutenção da integridade dos dados, proteção da

PARA AS ORGANIZAÇÕES QUE ENFRENTAM RISCOS DE CIBERSEGURANÇA E DE PROTEÇÃO DE DADOS CADA VEZ MAIS COMPLEXOS E PERIGOSOS, AS CLEANROOMS CONTINUARÃO A DESEMPENHAR UM PAPEL VITAL NO PROCESSO DE RECUPERAÇÃO

propriedade intelectual e cumprimento das normas regulamentares do sector. No entanto, o conceito de cleanroom vai muito além de um espaço físico seguro: trata-se de uma abordagem abrangente à cibersegurança e à recuperação, que envolve um ambiente seguro, independente e controlado. Estes ambientes funcionam de forma autónoma em relação às redes de produção e dependem igualmente de um planeamento rigoroso, processos definidos, boas práticas e testes regulares.

O verdadeiro valor da tecnologia de cleanrooms reside na capacidade de reunir, de forma coesa e eficiente, várias funcionalidades essenciais. Para compreender plenamente o papel de uma sala limpa, é importante entender primeiro os riscos que ajuda a mitigar. Os ciberataques aumentaram drasticamente nos últimos anos e representam uma ameaça séria para organizações de todos os sectores, frequentemente com consequências devastadoras — desde perdas financeiras significativas até danos duradouros na reputação. Neste contexto, as cleanrooms são aplicadas à ciberrecuperação, especialmente em situações em que ataques maliciosos exigem processos mais complexos para identificar, isolar e erradicar ameaças.



CASOS DE UTILIZAÇÃO DIVERSOS

A recuperação em cleanroom é normalmente aplicada em cenários em que os métodos-padrão de recuperação de dados são insuficientes. Por exemplo, se um colaborador apagar acidentalmente um ficheiro ou ocorrer uma falha de sistema — como o incidente da CrowdStrike — uma sala limpa permite uma recuperação operacional, proporcionando acesso à cópia mais recente e intacta dos dados e acelerando o tempo de restauro.

Num cenário de recuperação de desastre em que os dispositivos de armazenamento sofrem danos físicos causados por água, fogo, impacto ou defeitos de fabrico, um ambiente de cleanroom

controlado garante que o processo de recuperação decorre sem risco de danos adicionais no hardware ou nos dados. De forma semelhante, quando os dispositivos são expostos a contaminantes como pó, sujidade ou partículas microscópicas — por exemplo, em ambientes industriais ou laboratoriais — pode ser necessário recorrer à recuperação em sala limpa para evitar a perda de dados e restaurar a plena funcionalidade dos sistemas.

Em situações em que os métodos convencionais de recuperação de dados não são adequados — como ataques de ransomware, fugas massivas de informação ou infeções generalizadas de malware — a recuperação em cleanroom oferece uma abordagem especializada, capaz de isolar os sistemas comprometidos, garantir a integridade dos dados recuperados e proporcionar um ambiente seguro para o restauro da produção. Além disso, permite realizar testes antes de um ataque e análises forenses seguras após o mesmo.

Estas capacidades são especialmente relevantes para sectores industriais altamente sensíveis ou regulados, nos quais a recuperação eficaz de dados é não só uma função crítica, como também uma exigência de conformidade. Ao assegurar que a informação crítica pode ser recuperada de forma segura, as salas limpas ajudam as organizações a cumprir as suas obrigações em matéria de privacidade, segurança e integridade dos dados. Em contextos em que fugas de informação e perdas de dados sensíveis podem ter consequências legais e financeiras graves, torna-se essencial implementar controlos e protocolos rigorosos para proteger a confidencialidade e integridade dos dados recuperados.

Isto significa que a recuperação em cleanroom também contribui para o cumprimento de diretivas de cibersegurança, como a NIS2, e de regulamentações específicas de cada sector, como a HIPAA (saúde), a PCI DSS (cartões de pagamento) ou a DORA (serviços financeiros). Estas normas exigem que as organizações implementem medidas adequadas para proteger dados sensíveis, incluindo processos de recuperação seguros.

COMO FUNCIONA A RECUPERAÇÃO EM CLEANROOM?

Perante estes desafios, as organizações recorrem à implementação de salas limpas para se protegerem contra riscos de violação e maximizar a sua capacidade de recuperação em caso de ataque. O uso de tecnologias de cleanroom para recuperação deve assentar num processo sistemático e rigoroso, num ambiente seguro e controlado.

O processo inicia-se com a identificação da natureza e da extensão da violação de dados e com o isolamento dos sistemas ou dispositivos afetados da rede de produção, evitando assim a propagação do incidente. Uma vez isolados, os dados são transferidos para o ambiente cleanroom através de canais cifrados, preservando a confidencialidade e a integridade. Dentro de uma cleanroom, os dados comprometidos são analisados detalhadamente para determinar o alcance da violação, identificar os sistemas afetados e avaliar vulnerabilidades que possam ter contribuído para o ataque. Seguidamente, são restauradas cópias de segurança limpas ou

O VERDADEIRO VALOR DA TECNOLOGIA DE CLEANROOMS RESIDE NA CAPACIDADE DE REUNIR, DE FORMA COESA E EFICIENTE, VÁRIAS FUNCIONALIDADES ESSENCIAIS

cópias não afetadas dos dados, garantindo que a informação recuperada está livre de malware ou código malicioso.

Os dados restaurados são sujeitos a verificações rigorosas de integridade e validação, assegurando a sua exatidão e fiabilidade. Isto inclui confirmar a coerência, executar verificações de checksums e comparar com cópias conhecidas como boas, de modo a confirmar a autenticidade. Para proteger o ambiente, aplicam-se ainda medidas adicionais de segurança, como a correção de vulnerabilidades e o reforço dos controlos de acesso. Após a recuperação são testadas a funcionalidade, o desempenho e a fiabilidade dos sistemas e dados restaurados. Quando o ambiente da sala limpa é considerado seguro e os dados validados, procede-se à transição controlada para o ambiente de produção, minimizando o risco de interrupções nas operações em curso.

Processos de recuperação eficazes dependem igualmente de controlos e protocolos rigorosos que garantam a integridade e segurança dos dados restaurados. Isto implica a adoção das melhores práticas do sector, o uso de tecnologias de segurança avançadas e a realização de auditorias e avaliações periódicas para assegurar a conformidade com as normas de proteção de dados.

OLHAR PARA O FUTURO

As soluções de cleanroom continuarão a evoluir à medida que a inteligência artificial (IA), o machine learning (ML) e as tecnologias de cloud alarguem o seu alcance e tragam novas capacidades ao mercado. Por exemplo, a IA está já a ser utilizada para analisar padrões, identificar potenciais problemas e automatizar determinados aspetos do processo de recuperação, aumentando a eficiência e a precisão.

A capacidade de recuperar dados diretamente a partir de ambientes cloud ajudará as organizações a reduzir o tempo de inatividade e a agilizar os processos de recuperação. Além disso, contribui para a otimização de custos, uma vez que as salas limpas podem ser ativadas apenas quando necessário e desativadas após a conclusão da recuperação ou dos testes, permitindo às empresas pagar apenas pelo que utilizam.

Para as organizações que enfrentam riscos de cibersegurança e de proteção de dados cada vez mais complexos e perigosos, as cleanrooms continuarão a desempenhar um papel vital no processo de recuperação. Para além de fornecerem capacidades eficazes de proteção e restauro, acrescentam uma camada adicional de confiança, garantindo que os dados mais valiosos podem ser protegidos de forma segura — mesmo que as defesas de perímetro sejam violadas. ■

IP Telecom

POR FILIPE FRASQUILHO,
Diretor de Serviços TI,
IP Telecom

SOBERANIA E RESILIÊNCIA DA CONTINUIDADE DE NEGÓCIO

A Continuidade de Negócio é um dos principais pilares para que as organizações enfrentem riscos cada vez mais extensos e complexos, como falhas de hardware, bugs de software, ataques cibernéticos, entre outros.

RECENTEMENTE, OS CONFLITOS GEOPOLÍTICOS vieram acrescentar uma variável de grande relevância: a Soberania. Este fator reforça a necessidade das organizações não só recuperarem rapidamente de interrupções, mas também manterem o controlo e a autonomia sobre os seus processos e dados, garantindo uma continuidade operacional segura e sustentável.

Um Plano de Continuidade de Negócio (PCN) robusto exige a integração eficiente de Processos, Pessoas e Tecnologia, bem como da Soberania operacional. A resiliência das áreas operacionais é fundamental para minimizar impactos e permitir uma recuperação rápida e eficaz, assegurando que a organização mantém o controlo sobre os seus processos críticos em qualquer circunstância.

As organizações, de acordo com a sua maturidade, capacidade financeira e requisitos de Compliance, devem definir, implementar e testar as estratégias de continuidade de negócio, considerando:

1. GESTÃO E ANÁLISE DE RISCOS:

• Identificação de ativos críticos (sistemas, dados, infraestrutura e recursos humanos).

- Filipe Frasquilho -
Diretor de Serviços TI, IP Telecom

• Identificação de ameaças relevantes à organização, sejam cibernéticas ou de outra natureza.
• Avaliação de vulnerabilidades internas e externas dos sistemas e processos, incluindo as cadeias de abastecimento e as dependências de terceiros.
• Avaliação do impacto de cada ameaça, considerando probabilidade e consequências para o negócio.

2. OBJETIVOS DE RECUPERAÇÃO:

• Definição dos objetivos de recuperação para cada ativo crítico, como o tempo máximo de inatividade tolerável (RTO) e o ponto de recuperação (RPO).
• Priorização dos ativos, de acordo com sua importância para o negócio.

3. PROCEDIMENTOS DE RECUPERAÇÃO:

• Planos de resposta a incidentes detalhados para a deteção, resposta e contenção de incidentes.
• Procedimentos específicos de recuperação de ativos críticos, incluindo a restauração de dados, a reconfiguração de sistemas e a reativação de serviços.
• Testes e exercícios regulares para garantir a eficácia e identificar melhorias.

4. COMUNICAÇÃO E COOPERAÇÃO COM AUTORIDADES:

• Gestão de crises, definir uma equipa de resposta a incidentes e estabelecer canais de comunicação claros e eficientes.
• Planos de comunicação para informar os stakeholders internos e externos sobre os incidentes de segurança e o estado da recuperação.
• Procedimentos para notificação às autoridades competentes, em caso de incidentes de segurança, conforme exigido pela legislação.

Sem o apoio e envolvimento ativo da Gestão de Topo na implementação, manutenção e testes do PCN, bem como na promoção de planos de formação e consciencialização dos colaboradores, incluindo treinos regulares e o reforço do papel fundamental de todos na prevenção e resposta a incidentes, existe uma elevada probabilidade de insucesso dos planos. O compromisso da liderança é determinante para garantir que o PCN seja eficaz e sustentável.

Um PCN eficaz e robusto contribui para minimizar os impactos financeiros e operacionais de qualquer interrupção. Com a rápida evolução da tecnologia, as organizações devem estar atentas às novas oportunidades para fortalecer o seu PCN, sem comprometer a soberania das suas operações e dados. É fundamental que a adoção de soluções inovadoras seja acompanhada de uma avaliação criteriosa dos riscos, garantindo que o controlo e a autonomia sobre os processos críticos permanecem salvaguardados.

Em resumo, o desafio consiste em garantir que a organização não só sobreviva a uma interrupção de serviço (parcial ou total), mas que o faça protegendo os seus ativos críticos e salvaguardando a sua autonomia decisional e operacional. A IP Telecom tem vindo a desenvolver um conjunto de atividades fundamentais que ajudam as organizações a fortalecer a sua capacidade de resposta e resiliência perante situações de disrupção, assegurando a soberania das suas operações. ■

SECURNET
ALWAYS ONLINE | ALWAYS SECURE

POR MIGUEL BARREIROS,
Sales & Marketing Director
da SECURNET

ALWAYS RESILIENT - VANTAGEM COMPETITIVA OU SOBREVIVÊNCIA?

Sempre que leio ou ouço alguém propor continuidade de negócio como vantagem competitiva, interrogo-me: não será mais uma questão de sobrevivência? E, num mundo cada vez mais global, conectado e interdependente não apenas da nossa sobrevivência, mas de todos os que de alguma forma, direta ou indireta, dependem de nós.

DEIXANDO ESTAS IDEIAS em aberto, pergunto: não será a continuidade de negócio também uma questão de cultura e sensibilidade para o tema, à semelhança da cibersegurança, ainda que longe da mesma notoriedade? Há uns anos, um cliente adjudicou-nos a **coordenação de resposta a incidentes disruptivos** com uma premissa curiosa: "se acontecer algo de errado e grave, para além de estarem preparados, dentro do gabinete de crise serão os mais tranquilos e os menos envolvidos emocionalmente no caos". Um belo exemplo de humildade e sabedoria, mas ao mesmo tempo mais uns créditos sobre a tese de que preparação e treino entregam serenidade quando mais é precisa.

Foto de Kenny Van Roosbroeck no Unsplash

> LEMBRE-SE QUE A ATENÇÃO DE GESTORES SE CAPTA COM NOMENCLATURA DE NEGÓCIO. E ATENÇÃO: SE TUDO FOR CRÍTICO, NADA É PRIORITÁRIO!”

Este exemplo reforça uma convicção: continuidade de negócio (da organização e não das TI) também é serenidade e discernimento. Falhas de todos os tipos acontecem, tornando no mais importante a recuperação rápida, com previsibilidade e boa comunicação. E isso só acontece com planeamento, preparação e treino, mesmo muito treino e se possível em cenário real. Como dizia um ilustre treinador “treina como jogas”.

Não caberia aqui um compêndio sobre continuidade de negócio. Ficam, por isso, algumas ideias práticas para quem quer ser, de facto, “Always Resilient”.

Patrocínio da gestão de topo - Envolva a gestão de topo na primeira oportunidade. Para além de garantir os meios materiais e humanos necessários, ou de pelo menos ficar mais próximo, esse patrocínio dar-lhe-á o empoderamento que fará falta mais cedo ou mais tarde. Pergunte a cada membro da gestão o que pensa sobre tomar uma decisão que comprometa definitivamente o futuro e a existência da empresa. No final, relembre que uma não decisão, por inação, é exatamente o mesmo.

Grupo de resposta a incidentes - Nas crises é fundamental organização: um grupo de trabalho, um líder inequívoco e uma cadeia de comando com substitutos mapeados para cada função. Decisões rápidas e informadas farão toda a diferença.

Problemas e indisponibilidades com “preços e nomes” - Quanto perdemos de receitas (em euros) com o sistema A ou B indisponível? A organização sobrevive a essa perda? O que se consegue, ou não, fazer sem determinados meios e informações? Faça um **Business Impact Analysis** (**BIA**) realista e traduza risco em euros. De pouco valerão dashboards, relatórios ou pedidos de investimento com pormenores técnicos que para a gestão de topo pouco ou nada valem. Lembre-se que a atenção de gestores se capta com nomenclatura de negócio. E atenção: se tudo for crítico, nada é prioritário!

Arquiteturas prontas a falhar - Continuar não significa “nunca cair”, mas sim “cair em pé”, rapidamente levantar e seguir o caminho. Prepare sistemas redundantes, locais de trabalho alternativos, fornecedores e canais de contin-

> “NUM MUNDO CADA VEZ MAIS GLOBAL, CONECTADO E INTERDEPENDENTE DE SERVIÇOS DISPONIBILIZADOS POR UMA MIRÍADE DE FORNECEDORES, SE UM FALHAR, TODOS FALHAMOS”

gência. Crie guias de operação simples (fáceis de encontrar, interpretar e executar por diversos perfis). As arquiteturas verdadeiramente resilientes são tolerantes a falhas, mas principalmente estão preparadas para recuperar facilmente ou integrarem alguns dos seus componentes noutros sistemas base.

Treinar, treinar, treinar - Quanto mais treinar, com propósito e em cenário real, melhor preparado estará para a crise que um dia chegará. Experimente exercícios de mesa (tabletops), simulacros e até cartões de bolso com passos essenciais. Não espere que alguém cumpra o seu papel se receber um “guia” apenas no dia do incidente.

Olhe à volta com saudável desconfiança - Num mundo cada vez mais global, conectado e interdependente de serviços disponibilizados por uma miríade de fornecedores, se um falhar, todos falhamos. Analise os SLAs, os horários de cobertura e os preçários; em caso de dúvida, confirme e faça testes. Garanta que tem os contatos certos para cada situação e momento.

Planeie toda a comunicação - Grande tensão e responsabilidade exigem comunicação objetiva e transparente. Defina, em momento de calma, quem comunica, o que comunica e como comunica. Estabeleça planos de comunicação interna e externa, selecione canais e treine mensagens-tipo. Lembre-se que em fase de crise importa reduzir o ruído e manter a confiança.

Pragmatismo antes do perfeccionismo - Resiliência também é pragmatismo e quase sempre vale a pena começar pequeno, porque o ótimo é inimigo do bom. Saber parar, sintetizar e simplificar é uma competência e… uma vantagem. Mais vale um plano simples, testado e conhecido por todos do que um extenso dossier que ninguém lê ou sequer abre às 3 da manhã.

A SECURNET apoia organizações em preparação, treino e resposta a incidentes, com uma equipa experiente, treinada e especializada - SECURNET, Always Resilient! Contacte-nos em *info@securnet.pt* ou pelos telefones +351 224 673 094 / +351 213 622 204.

PAGAMENTOS DE RANSOMWARE ESTÃO A DIMINUIR, MAS ORGANIZAÇÕES DA EMEA CONTINUAM DESPREPARADAS PARA ATAQUES

A Veeam analisou dados regionais dos seus relatórios de tendências de ransomware de 2024 e 2025, que refletem as conclusões do ano anterior e exploram as tendências a longo prazo de ransomware e de resiliência de dados na EMEA.

OS DADOS MOSTRAM que o número de organizações a pagar resgates diminuiu quase um quarto (22%) em relação ao ano anterior. No entanto, isto não significa que as organizações estejam a sofrer menos ataques, mas sim que estão a melhorar as suas capacidades de resiliência e que existe uma mudança de atitude quanto à negociação com cibercriminosos.

PAGAR RESGATES JÁ NÃO GARANTE A RECUPERAÇÃO DOS DADOS

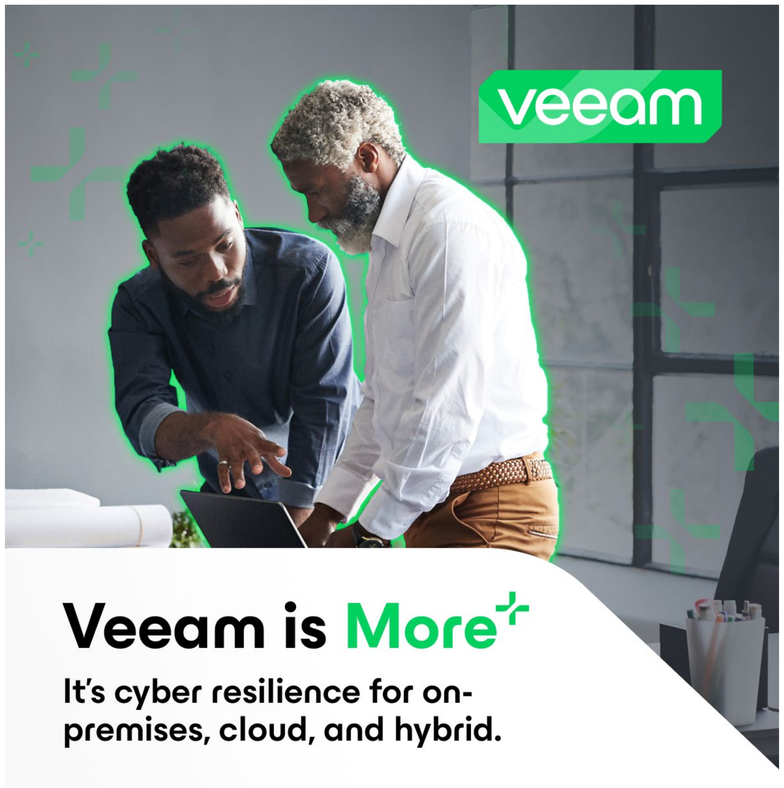
A análise dos dados revela que as organizações recuperam cada vez mais dados sem ter de pagar resgates; em 2023, 14% conseguiram recuperar dados sem pagar, enquanto em 2024 esse número subiu para 30%. Ao mesmo tempo, cresce a consciência de que pagar resgates não garante a recuperação dos dados; em 2023, mais de metade (54%) das organizações que pagaram conseguiram recuperar a informação, mas em 2024 esse valor caiu para apenas 32%.

"Os atacantes continuam a ser um método pouco fiável para recuperar dados e as organizações estão a melhorar as suas capacidades de recuperação, por isso não é surpreendente vermos uma queda nos pagamentos de resgates. Mas isto não significa que a ameaça do ransomware terminou," afirma Tim Pfaelzer, Vice-Presidente Sénior e Diretor-Geral da EMEA na Veeam. "Os

atacantes adaptam-se constantemente. Alguns já nem usam encriptação de ransomware, optando por roubar dados e extorquir dinheiro diretamente ou vendê-los no mercado negro. Para alguns, o objetivo nem é o lucro financeiro, mas sim causar disrupção. Os pagamentos podem diminuir, mas os ataques continuam. E os dados mostram que ainda existem lacunas significativas na resiliência de dados, deixando as organizações vulneráveis."

FALTAM MEDIDAS ESSENCIAIS DE RESILIÊNCIA DE DADOS

Com a introdução de várias regulamentações europeias para reforçar a resiliência digital, como o NIS2 e o DORA para os serviços financeiros, as organizações estão a preparar-se melhor para ataques de ransomware. Contudo, em 2024, apenas 37% das organizações da EMEA tinham planos para infraestruturas alternativas, o que significa que 63% continuam sem essas soluções. Sem infraestrutura alternativa, uma organização não consegue recuperar até que o local



principal seja considerado seguro, podendo demorar semanas. A paralisação total das operações durante semanas pode ser desastrosa, tanto para a reputação como para a parte financeira, sendo que estudos recentes indicam que uma interrupção pode custar mais de £1 milhão por hora, dependendo do tamanho da empresa.

"É claro que a recuperação passou a estar no centro da estratégia de resiliência de dados das organizações, em vez de depender de pagamentos de resgates, o que representa um avanço. Mas ainda há trabalho a fazer," acrescenta Tim Pfaelzer. "A regulamentação pode ter elevado os níveis de resiliência, mas as organizações devem ir mais longe. Devem melhorar a resiliência básica dos dados através de infraestrutura alternativa e backups robustos, eliminando a necessidade de pagar resgates. Assim, conseguem melhorias reais e duradouras na sua resiliência."

Os padrões de resiliência de dados estão a evoluir positivamente. Ao mesmo tempo, operações policiais como o desmantelamento do grupo Lockbit estão a dificultar a atividade dos atacantes. No entanto, ainda há muito por fazer. As organizações devem priorizar medidas como infraestruturas alternativas e backups seguros para alcançar verdadeira resiliência. Caso contrário, no próximo ataque, pode não haver pagamento, mas também não haverá forma de recuperar rapidamente a operação. ■

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

O QUE TODOS OS LÍDERES DEVEM SABER SOBRE CONTINUIDADE DE NEGÓCIO

O mais recente Microsoft Digital Defense Report (2025) identifica alguns pontos-chave que todos os líderes devem conhecer para proteger os seus ativos, operações e reputação, e que se revelam fundamentais para a resiliência organizacional e continuidade de negócio.

ESTE RELATÓRIO traça um retrato claro: proteger identidades, dados e infraestruturas, é hoje, o fator decisivo para garantir operações resilientes num cenário de ameaças cada vez mais sofisticadas.

A autenticação multifatorial (MFA) continua a ser a medida mais eficaz contra acessos indevidos, ao bloquear mais de 99% das tentativas de intrusão. Mas o relatório é também explícito ao afirmar que já não basta ter MFA, é essencial adotar soluções resistentes a ataques de engenharia social, como o phishing, capazes de evoluir a proteção ao elo mais fraco na cadeia de segurança, o fator humano.

Os cibercriminosos estão também cada vez mais focados em roubo e usurpação de identidades, através do roubo de credenciais que lhes dão acesso direto a dados valiosos que permitem desenvolver ataques mais elaborados e com maior impacto. Setores como o Governo, Administração Pública, Educação, Saúde e Tecnologia, estão entre os mais visados, em

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

grande parte porque armazenam quantidades massivas de informação de enorme valor para o cibercrime, como dados pessoais ou confidenciais. Quando uma identidade é comprometida, o impacto vai muito além do roubo de dados, já que compromete a confiança, a reputação e, em última instância, a capacidade de continuar a operar, podendo mesmo levar a impacto financeiro irreversível.

Curiosamente, apesar da constante evolução tecnológica, os vetores de ataque continuam a ser os mesmos velhos conhecidos de sempre (phishing, exploração de vulnerabilidades não corrigidas, e ataques de ransomware robotizados); a diferença, é que hoje os cibercriminosos exploram vetores de ataques, assentes em vulnerabilidades conhecidas, mais depressa do que nunca.

O mesmo relatório revela ainda que a maioria dos ciberataques continuam a ser motivados por razões financeiras. Ora, a cibercriminalidade tem vindo a consolidar-se como um modelo de negócio altamente lucrativo, e os dados exfiltrados são frequentemente usados para chantagem ou revenda num mercado "underground" que permite níveis de retorno económico difíceis de acreditar.

Por outro lado, e na perspetiva do pós-ciberataque, cada vez mais os planos de continuidade e recuperação são fundamentais para manter "vivo" o negócio da vítima. Recomendações como incluir cópias de segurança isoladas e imutáveis, mecanismos de deteção precoce a ações suspeitas ou maliciosas, ou procedimentos de resposta e recuperação devidamente testados, são fundamentais para conseguir recuperar a um ciberdesastre. A capacidade de restaurar operações rapidamente, pode fazer toda a diferença entre uma interrupção controlada e uma crise prolongada, que no extremo, pode condicionar a recuperação do negócio e da empresa para o futuro.

A Inteligência Artificial (IA) surge igualmente como um dos grandes temas deste ano. Se, por um lado, potencia a ciberdefesa através do incremento substancial de capacidades de deteção e resposta automatizadas (através de "inteligência"), por outro, também está a ser utilizada pelo cibercrime como multiplicador ao facilitar o desenvolvimento de modelos inovadores de ataques a pessoas através campanhas de phishing altamente convincentes, pela criação de deepfakes e incorporação de contexto personalizado para a vítima.

Por fim, a computação quântica, que embora traga promessas de inovação e progresso, representa também um risco potencial para os sistemas de encriptação que hoje sustentam a segurança digital. A transição para criptografia resistente a quântica, tem de ser planeada agora, como parte da visão de longo prazo para a continuidade e resiliência das organizações. A mensagem é inequívoca: a continuidade de negócio dependerá diretamente da capacidade de se conseguir antecipar, resistir e recuperar perante ciberataques. ■

HUGO MARTINS, IT DIRECTOR DA HORIZON VIEW

“A MAIOR PARTE DAS PESSOAS DÁ COMO ADQUIRIDO QUE OS SISTEMAS VÃO ESTAR SEMPRE A FUNCIONAR”

Fotografias: Luís Santos Ribeiro

Hugo Martins, IT Director da Horizon View, marcou presença na mais recente IT Insight Talks e ao vivo, perante uma plateia de leitores da IT Insight, abordou o tema da continuidade de negócio e de recuperação de desastre.

RUI DAMIÃO

O NOME HORIZON VIEW NÃO É O MAIS CONHECIDO NO MERCADO, MAS A EMPRESA JÁ ESTÁ PRESENTE HÁ VÁRIOS ANOS. O QUE É A HORIZON VIEW E QUE SERVIÇO É QUE O HUGO TEM SOB A SUA ALÇADA?

A Horizon View é uma marca recente, mas na verdade é uma empresa que já é viva desde 1886, tem quase 140 anos, está na família d'Orey já desde essa altura e é uma empresa nacional. O nome mais conhecido é realmente Orey e Horizon View é um *rebranding* da marca a partir de 2009 porque houve alguma separação de negócios.

É uma empresa cujo seu *core business* é parte de logística e transportes. É uma referência do mercado; na realidade, a Orey Shipping é uma das maiores empresas nesta área. Temos cinco grandes grupos de negócio, que é a parte de trânsitos marítimos e aéreos, agenciamento de navios, linhas regulares, logística e despachos aduaneiros. Temos outros negócios e outras áreas, mas

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

“QUANDO VEIO A PANDEMIA ATIVÁMOS O PLANO DE CONTINUIDADE DE NEGÓCIO QUE JÁ ESTAVA PREVISTO E COLOCÁMOS TODA A GENTE A TRABALHAR A PARTIR DE CASA RAPIDAMENTE. NO QUE TOCA AO PLANO DE CONTINUIDADE DE NEGÓCIO, A PANDEMIA NÃO NOS AFETOU POR AÍ ALÉM”

dentro destes grupos principais, temos implementado um plano de *business continuity* desde 2011, porque na altura tínhamos uma empresa financeira e as empresas financeiras são obrigadas a muitas regras e temos um plano desde essa altura. Temos continuado sempre a trabalhar no mesmo, já alterámos o plano várias vezes fruto de vários softwares, alterações estruturais de organização, temos feito essas alterações.

Temos, à data de hoje, um plano específico para cada área, porque por exemplo a logística, que não tem ligação com despachos aduaneiros, tem o seu próprio plano, mas também temos um plano global para tudo. Ou seja, temos um plano global que prevê o cenário mais catastrófico – a destruição completa do nosso data center, o ransomware que apague tudo. O nosso cenário é sempre o mais dantesco e é aí que estamos, essencialmente, mas temos um plano segregado para cada uma das áreas de negócio.

SABEMOS QUE MUITA COISA MUDOU COM A PANDEMIA. NESTES SEIS ANOS, O QUE É QUE MUDOU NOS RISCOS DE CONTINUIDADE DA HORIZON VIEW?

Não mudou necessariamente. O nosso plano de 2011 começa com o plano de *tape shipping* com um parceiro nosso onde entregávamos a *tape* com os *backups*, eles levantavam os sistemas e tinham uma salinha para nós, com cinco lugares onde colocávamos cinco utilizadores para trabalharem. Como na realidade nós precisávamos de mais do que cinco utilizadores, adotámos o nosso sistema para iniciar um acesso remoto a estes sistemas e começámos a trabalhar dessa forma.

Quando veio a pandemia ativámos o plano de continuidade de negócio que já estava previsto e colocámos toda a gente a trabalhar a partir de casa rapidamente. No que toca ao plano de continuidade de negócio, a pandemia não nos afetou por aí além.

Afetou-nos a parte da segurança; a segurança foi a grande alteração que tivemos com a pandemia, que foi, em vez de tomar conta de dez ou 20 escritórios, passei a tomar conta de 120. Cada pessoa passou a ter o seu próprio escritório em casa e o espectro de segurança e de controlo aumentou exponencialmente.

QUANTOS FORNECEDORES EXTERNOS SÃO CRÍTICOS PARA A OPERAÇÃO DA EMPRESA? O QUE É QUE ACONTECE AO NEGÓCIO QUANDO UM DESTES FORNECEDORES DEIXA, SIMPLESMENTE, DE FUNCIONAR?

Temos muitos fornecedores externos. Somos uma empresa de serviços; basta pensar que trabalhamos com todos os portos nacionais, internacionais, armadores, alfândega, autoridade tributária. Acho que faço uma divisão aqui entre os fornecedores: os fornecedores que nós, entre aspas, controlamos e os que não controlamos.

Se eu tiver um incidente com o ERP, tenho um contrato com o nosso fornecedor e, portanto, consigo chegar à fala com eles e dizer que precisamos de ajuda urgente. O nosso email está no Office 365, está na Microsoft. Se eu tiver um problema com o email, não tenho o número da Microsoft para ligar e dizer 'desenrasquem-me agora'. Se eu tiver um incidente com o Porto de Lisboa, é difícil dizer 'tenho um navio para entrar e não consigo aceder o vosso portal para dar entrada do navio'.

É difícil nós termos aqui uma gestão desta parte de fornecedores. Há uns que nós conseguimos, volto a dizer, entre aspas, controlar, outros não. A parte dos fornecimentos externos é hoje uma das grandes dificuldades que nós temos ao montar os planos de continuidade de negócio.

> “SE MONTAR EM JANEIRO UM PLANO DE CONTINUIDADE DE NEGÓCIO COM OS PROCESSOS DAS MINHAS ÁREAS, DE CERTEZA QUE QUANDO CHEGAR A JULHO ESSES PROCESSOS MUDARAM E HÁ UMA GRANDE DIFICULDADE DAS ÁREAS EM ATUALIZAREM ESSES DADOS”

ONDE É QUE AINDA ENCONTRA MAIOR RESISTÊNCIA NOS PROCESSOS DE CONTINUIDADE? AO MESMO TEMPO, COMO É QUE ‘VENDEM’ INVESTIMENTO EM *BUSINESS CONTINUITY* À ADMINISTRAÇÃO QUANDO EXISTEM OUTROS INVESTIMENTOS IGUALMENTE NA ‘LISTA DE COMPRAS’?

Respondendo à primeira parte da pergunta, o grande problema que temos hoje é manter a documentação atualizada. Ninguém gosta de documentar nada; esse é o grande problema destes processos.

Se montar em janeiro um plano de continuidade de negócio com os processos das minhas áreas, de certeza que quando chegar a julho esses processos mudaram e há uma grande dificuldade das áreas em atualizarem esses dados. Não sei como é nas outras organizações, mas, na minha, recai sempre sobre os ombros da informática atualizar. A informática tem de ir ter com o negócio e perguntar o que é que mudaram e o que é que não mudaram. Muitas vezes, só conseguimos apanhar quando começamos o processo de testes.

Temos uma semana em que fazemos testes em real, em que seguimos o *script*, e deparamo-nos com o *key user* que vem fazer o teste dizer ‘o procedimento já não é esse, isso está tudo alterado’, ou seja, se na realidade tivéssemos de atuar naquele momento num caso real, o *script* ou o teste já não estaria relacionado

Existe essa dificuldade de documentação porque a maior parte das pessoas dá como adquirido que os sistemas vão estar sempre a funcionar. Não é normal acordar de manhã e não ter email. É difícil até convencer as pessoas de que têm de preparar os sistemas, ou têm de documentar o que há para fazer em caso de desastre. Essa é a principal dificuldade que enfrentamos quando estamos a fazer os testes de *disaster recovery* ou a preparar estes planos.

A segunda parte, como é que vendemos isto às administrações: isso, para mim, é uma não questão, na realidade. Porque não é a informática que tem de vender nada; quem tem de vender é o negócio. O negócio é que pode dizer quanto tempo é que pode estar parado. É uma questão de gestão de risco. Se o meu negócio me disser que pode estar um mês parado, não tenho problema nenhum com isso. Agora, se o meu negócio disser não posso estar parado mais do que uma hora…

Fazendo aqui a relação diretamente com a Horizon View. Se tiver, por exemplo, um navio que está em porto e tiver o sistema em baixo e não

consigo dar saída do navio, o navio em porto se calhar custa-me dez mil euros por dia. Ao fim de cinco dias são 50 mil euros.

Essa análise é a administração, ou a gestão de risco quando existe, que tem de fazer. A informática, na verdade, só tem de dizer 'se queres o sistema reposto em uma hora, custa '*x*', se queres em um dia, custa '*y*'". Acho que há um *misconception* que é a informática que tem de ir. Eu não concordo; acho que a informática tem de atuar conforme o negócio indica.

JÁ 'LEVANTOU O VÉU' SOBRE ESTE TEMA, MAS COM QUE FREQUÊNCIA TESTAM OS PLANOS DE CONTINUIDADE? QUAL FOI O ÚLTIMO TESTE QUE FALHOU E O QUE É QUE APRENDERAM COM O MESMO?

Estamos com as pessoas uma vez por ano e nós, IT, todos os meses testamos levantar os sistemas – os nossos planos de *business continuity* e *disaster recovery* funcionam com base em data center principal e secundário – e costumamos fazer sempre um teste mensal, levantar os sistemas e testar nós diretamente, não envolvemos o resto das pessoas.

Fazemos um teste anual onde envolvemos as pessoas e o que notamos, ou as falhas que encontramos, têm sempre a ver com isto que já levantei antes: a documentação não está correta. Depois temos uma outra situação também

que é há um *key user* que prepara o *script* de teste para aquela área, mas depois na altura do teste o *key user* não tem tempo, não aparece, manda um colega, o colega chega e diz 'não tenho permissões, nunca fiz isto na minha vida, mandaram-me para aqui'. Este é o problema que temos que é se não praticamos, se não treinamos, quando chegar à altura do desastre é um problema.

Tenho uma história engraçada pessoal, uma história familiar sobre treino. Nós falamos muito do treino, mas na realidade ninguém treina. Já se passou há uns anos, a minha sobrinha estava a dormir em minha casa com os meus pais e teve um problema de saúde. Acordei de madrugada com os meus pais aflitos a discutirem, à frente do telefone, a perguntarem um ao outro qual era o número do 112. Isto é ridículo, mas a realidade é que o pânico faz com que nós deixemos de pensar. Se não treinarmos, se não praticarmos os riscos que temos, como é que levantamos os sistemas, onde é que estão os contatos, toda essa informação, é difícil atuarmos ou sabermos o que fazer em caso de desastre.

Nós tivemos recentemente um exemplo, que foi o apagão. Não sei como é que as outras pessoas fizeram, mas na minha empresa, literalmente, agarraram em livros que tinham lá na biblioteca e começaram a ler porque não tinham nada para fazer durante o dia. Ninguém sabia o que fazer. Foi uma situação que nunca tínhamos antecipado. A nossa ideia foi, se houver um desastre, agarramos o telefone enviamos um SMS massivo às pessoas a dizer, dirijam-se a '*x*', contactem '*y*'. Nesta situação não conseguimos contactar ninguém. São cenários que acho que temos de ir treinando. O treino é fundamental para mim nestes planos.

QUE CONSELHO DARIA A UM EXECUTIVO DE UMA EMPRESA QUE ESTEJA, POR ESTA ALTURA, A CONSIDERAR UM NOVO INVESTIMENTO EM CONTINUIDADE DE NEGÓCIO PARA A SUA EMPRESA?

Isto é um mundo. Temos de começar com uma coisinha e terminar numa coisa bastante complexa. *Keep it simple*; comecem com exercícios simples. Nós fazemos este exercício, nós às vezes chamamos as pessoas para uma *conference call* e dizemos 'se ficasses sem ERP daqui a cinco minutos o que é que fazias? Como é que emitias faturas? Tens algum método alternativo de emitir faturas? Tens algum método alternativo de enviar documentação?'

Acho que deveria partir por aí, ou seja, fazer exercícios com as organizações, perguntar o que é que precisam, o que é que não precisam, como é que testam, que falhas é que têm, porque acabamos por às vezes olhar um bocadinho só para o principal: o ERP está a funcionar, está tudo ok. Nós temos casos em que para dar saída do navio é preciso um ficheiro Excel que tem a contramarca do navio e esse ficheiro Excel está na rede. Se não tiver acesso à rede, não consigo dar saída do navio. Há pequenos casos que às vezes nós, IT, não notamos e também, muitas vezes, não são apanhados nos testes e só são apanhados em casos reais. Acho que às vezes estas pequenas conversas com os colegas a perguntar o que é que fazem e o que é que não fazem, é um bom ponto de partida. ■

IT SECURITY CONFERENCE: A VISÃO DOS CISO PARA O FUTURO DA PROTEÇÃO DIGITAL

Fotografias: Rui Santos Jorge

A IT Security Conference voltou a Lisboa. A conferência organizada pela IT Security – que pertence ao mesmo grupo da IT Insight – é uma das maiores conferências dedicadas a cibersegurança no país e este ano recebeu perto de 600 visitantes presenciais e contou com mais de 500 pessoas a acompanhar remotamente.

INÊS GARCIA MARTINS E FLÁVIA GOMES

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

- Lino Santos, Coordenador do CNCS -

O CENTRO NACIONAL DE CIBERSEGURANÇA (CNCS) anunciou, durante a IT Security Conference 2025, a criação de um novo esquema de certificação de serviços de cibersegurança.

Lino Santos, Coordenador do CNCS, partilhou que, há dois anos, a ENISA contactou o CNCS para pedir o nome de quatro empresas portuguesas a incluir num concurso europeu para serviços de cibersegurança. "Como é óbvio, eu fiquei com o problema nas mãos. Não vou nomear empresas, nem vou escolher a empresa A em detrimento da empresa B", relatou. Para contornar a situação, o CNCS recorreu à lista do Instituto dos Registos e Notariado.

Durante o processo, Lino Santos apercebeu-se de uma fragilidade estrutural no setor da cibersegurança em Portugal. "Há 140 empresas que, no seu objeto social, dizem trabalhar em segurança da informação ou cibersegu-

rança", referiu. A ausência de critérios técnicos que validem a competência das empresas surge como um problema estrutural para a área.

Perante esta necessidade, Lino Santos defende a criação de um mecanismo que permita distinguir quem tem, de facto, capacidade técnica na área. O novo esquema, de adesão voluntária, aplica-se a todas as organizações que prestam serviços de cibersegurança, independentemente da tipologia e dimensão, e define um conjunto de tipologias de serviço claramente delimitadas. "Arrancamos com os primeiros quatro serviços de cibersegurança, pretendemos alargar o portfólio durante o ano de 2026", indicou o coordenador, que detalhou os serviços iniciais: "monitorização e resposta a incidentes, gestão de vulnerabilidades, *cyber threat intelligence* e testes de intrusão".

"TUDO É COMPLEXO E NADA É PERFEITAMENTE SEGURO"

O Dr. Ron Ross viajou até Lisboa para participar na edição de 2025 da IT Security Conference. Na sua intervenção sobre "*Building Trustworthy Secure Systems: An Imperative for National and Economic Security*", destacou os "enormes progressos" e as "grandes parcerias de indústria e tecnologia avançada", mas não deixou de sublinhar que, mesmo assim, "continuamos a ter brechas e ataques que colocam países inteiros em risco".

O especialista descreveu o presente como um "campo de batalha invisível", onde a tecnologia passou a controlar tudo o que é vital – da energia à defesa, da mobilidade ao sistema financeiro.

Segundo Ron Ross, o verdadeiro objetivo da cibersegurança não é criar sistemas invulneráveis, mas garantir que, quando o impacto acontece, as operações não param. "Falamos de sistemas ciber-resilientes, capazes de aguentar o embate e manter as funções críticas ativas", explicou, acrescentando que "não existe zero confiabilidade – tudo é complexo e nada é perfeitamente seguro", apenas tecnologia em que é possível confiar em maior ou menor grau.

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

- Dr. Ron Ross, ex-NIST -

"TODAS AS EQUIPAS CONTRIBUEM PARA A SEGURANÇA DA INFORMAÇÃO"

Jorge Vicente desafiou a forma como as organizações olham para os dados em cibersegurança. O Diretor de Segurança da Informação do Lidl Portugal alertou para o risco de confundir recolha de métricas com inteligência real, e lembrou que as equipas estão atualmente "inundadas de métricas", mas essa informação nem sempre se traduz em decisões.

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

- Jorge Vicente , Diretor de Segurança da Informação do Lidl Portugal -

Entre números, alertas e processos, Vicente deu um retrato vivo da rotina de uma equipa de segurança da informação numa multinacional, com todos os desafios e complexidades que isso implica. Referiu que, internamente, o Lidl opera com 172 controlos automáticos – mecanismos que verificam bases de dados, acessos e volumes de informação – e com inúmeros controlos manuais, executados por equipas que monitorizam rotinas de *backup* e testes de recuperação. "A minha equipa está constantemente a pedir às outras equipas para executarem verificações e darem evidências", admitiu, enquanto garante que este esforço coletivo é o que garante que "todas as equipas contribuem para a segurança da informação".

"HÁ COISAS QUE ESTÃO LÁ AOS MILHARES E JÁ SABEMOS QUE NEM SEQUER VAMOS CORRIGIR"

David Marques, Head of Cybersecurity do Grupo Nabeiro, subiu a palco com o keynote "*Vulnerability Management - Patch Panic or Risk Reduction*", para falar de uma problemática com "que todos lidamos".

O Head of Cybersecurity destacou que o tema das vulnerabilidades já é falado há anos, e que ainda se continua a falar do tema por ser algo difícil de gerir por inúmeras razões, como é o caso de o número de vulnerabilidades subir a cada ano: "Todos os anos são milhares e milhares de vulnerabilidades novas, e estamos a falar apenas daqueles que têm um CVE atribuído, porque há mais além destas, mas todos os anos este número está a crescer".

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

- David Marques, Head of Cybersecurity do Grupo Nabeiro -

No entanto, as empresas demonstram um problema recorrente: as organizações apenas conseguem corrigir 10% das novas vulnerabilidades que aparecem no mercado. "É fácil de perceber qual é o problema: estamos a acumular mês após mês um *backlog* de 90% de vulnerabilidades que não conseguimos efetivamente corrigir". O orador acredita que as empresas são lentas a corrigir estes problemas e isso está relacionado com "as dificuldades impostas pelo negócio, com regras muito específicas. Há coisas que estão lá aos milhares e já sabemos que nem sequer vamos corrigir".

"MUITAS DAS VEZES, AQUILO QUE VAMOS ATRÁS É APENAS DE CUMPRIR A LEI"

"Gestão de Incidentes: preparar, responder e recuperar" foi o tema que Sérgio Trindade trouxe ao palco principal da IT Security Conference 2025. O CIO e CISO das Águas do Tejo Atlântico - Águas de Portugal fez uma reflexão sobre o estado real da cibersegurança operacional onde revela que, de forma geral, as organizações não sabem o que existe dentro do seu próprio perímetro tecnológico.

O responsável das Águas do Tejo Atlântico sublinha que a obsolescência de muitos dos equipamentos "torna-se crítica para conseguirmos o que temos de fazer", apontando-a como "uma das principais ameaças nos sistemas industriais e de abastecimento".

Segundo Sérgio Trindade, verifica-se que, apesar da evolução tecnológica, a gestão de risco ainda assenta sobretudo no cumprimento normativo. "Há aqui todo um caminho para melhoria, olhando para aquilo que são modelos de maturidade que estão muito desvinculados numa série de normas. Agora falamos muito da NIS2, e com toda a razão, e ainda bem

que ela veio" porque assim, afirma, "podemos basear-nos para saber o que é que temos que fazer e como". No entanto, defende que estes modelos devem ser utilizados para orientar práticas consistentes e não apenas para satisfazer exigências legais.

"Muitas das vezes, aquilo que vamos atrás é apenas de cumprir a lei", afirma, lembrando que essa abordagem "é completamente distorcida em relação àquilo que as empresas e os cidadãos necessitam".

O responsável defende que a gestão de risco deve assentar no que é mais adequado para o negócio e para a atividade da empresa, mas também na proteção dos cidadãos.

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM

- Sérgio Trindade, CIO e CISO das Águas do Tejo Atlântico - Águas de Portugal -

A IT Security Conference 2025 teve o apoio Diamond da Palo Alto Networks e Inspiring Solutions; o apoio Platinium da ACS, da Check Point, da Claranet Portugal, da ElRed, da Fortinet, da HPE, da PWC e da Sophos; o apoio Golden da Fujifilm, da HP, da Logicalis, da ManageEngine, da Rapid7, da Redshift, da Tenable, da Securnet e da Varonis; o apoio Silver da Art Resilia, da Balwurk, da Cisco, da Devoteam Cyber Trust, da Divultec, da IDW, da Kaspersky, da Oramix, da TD Synnex, da VisionWare e da WatchGuard; o apoio Bronze da Anubis Networks, da A10, da Cloudflare, da Crossjoin, da CyberArk, da Eset, da Factis, da Opentext, da Ping Identity e da Trellix. O evento, organizado pela IT Security, teve a Arrow, a Ignition e a V-Valley como VAD Partners, e ainda o apoio institucional do Centro Nacional de Cibereguranca e da CIIWA. ■

"A INOVAÇÃO JÁ NÃO É SOBRE O QUE COMPRAMOS, MAS COMO INTEGRAMOS DE FORMA SEGURA"

Com uma arquitetura baseada em cloud híbrida e automação, a Câmara de Gaia coloca a cibersegurança no centro da modernização digital, em conformidade com a Diretiva NIS2.

MARTA QUARESMA FERREIRA

OS 25 ANOS que leva de Câmara Municipal de Vila Nova de Gaia têm permitido a André Assunção, Especialista de Sistemas e Tecnologias da Informação, testemunhar uma "profunda evolução" no departamento e na própria liderança técnica.

No decurso destes anos, e do ponto de vista tecnológico, a mudança mais radical testemunhada por André Assunção passou pelo "abandono progressivo do 'ferro' – a tradicional infraestrutura física, *on-premises* – e o abraçar de serviços e arquiteturas baseadas na cloud".

Hoje, o especialista foca o seu trabalho numa camada cada vez mais fundamental nas organizações – a cibersegurança –, que levou a uma "maior alteração estratégica". "Passámos de um modelo de 'castelo e fosso', onde tentávamos 'fechar tudo a sete chaves', com acessos restritos, para um modelo de defesa em profundidade, baseado em camadas e identidade", contextualiza.

A CIBERSEGURANÇA PASSOU A TER UMA PALAVRA A DIZER

Para André Assunção, a mudança de paradigma da tecnologia – através da cloud –, e da estratégia – através da segurança em camadas –, leva a uma mudança de paradigma: "A inovação já não é sobre o que compramos, mas como integramos de forma segura. A cibersegurança deixou de ser um *add-on* para ser a fundação de qualquer novo projeto", defende o especialista.

"Na Câmara Municipal de Vila Nova de Gaia, a transformação digital é, hoje, inseparável da estratégia de cibersegurança. O nosso foco principal é garantir que a modernização dos serviços assenta numa postura de segurança robusta e numa base de confiança", esclarece, apontando para uma gestão da tecnologia com base na própria gestão do risco. "Quando surge uma inovação, a minha primeira pergunta não é 'quanto custa?', mas sim 'qual é o impacto na nossa superfície de ataque?'. Em vez de dizermos 'não' a um novo serviço cloud, dizemos 'sim, mas' e desenhamos a arquitetura com controlos compensatórios, como a autenticação multifator, para garantir que a inovação e a continuidade operacional podem e devem coexistir", frisa.

A certificação ISO/IEC 27001 e a preparação para a total conformidade com a Diretiva NIS2 são os dois pontos centrais na atual iniciativa estratégica do departamento. "Não se trata apenas de um exercício de *compliance*; é uma mudança cultural profunda", garante. No entanto, as limitações e a justificação para o investimento não deixam de ser uma realidade a ter em conta quando os atores são entidades do setor público.

- André Assunção -
Especialista de Sistemas e Tecnologias da Informação

A IA GENERATIVA AO SERVIÇO DA TOMADA DE DECISÃO

Na perspetiva do município, tecnologias como a Inteligência Artificial (IA) generativa, a automação, a cloud híbrida e a análise de dados são "ferramentas poderosas" que, no entanto, "exigem uma governação muito cuidada". Se a cloud híbrida já é uma realidade, a automação surgiu para ajudar na eficiência interna.

No que toca à IA generativa, a abordagem na Câmara de Gaia passa por um "uso controlado", com a exploração do seu potencial em processos internos, sem perder de vista, no entanto, "uma governação rigorosa sobre a soberania e a privacidade dos dados, garantindo o cumprimento total do RGPD antes de qualquer implementação em larga escala".

A análise de dados tem sido a grande beneficiada desta transformação, com a evolução "de uma gestão reativa para uma gestão proativa, baseada em factos". "A criação de métricas e *dashboards* específicos – seja para monitorizar a performance da infraestrutura, os tempos de resposta a incidentes ou os alertas de segurança em tempo real – permite que a tomada de decisão, tanto a nível

técnico como ao nível do Executivo Municipal, seja cada vez mais rápida e fundamentada em dados concretos", justifica André Assunção.

CIDADÃOS E COLABORADORES: OS MAIORES BENEFICIÁRIOS DA TRANSFORMAÇÃO

Na jornada positiva de transformação tecnológica, cidadãos e colaboradores são os que tiram maior partido desta mudança: se por um lado a automação de processos e a integração destas tecnologias nos sistemas existentes tem permitido aos colaboradores técnicos dedicarem-se a tarefas de maior inovação e valor, por outro, os resultados permitem uma abordagem aos serviços digitais "mais estável e segura para o cidadão".

A mudança cultural e a consequente capacitação de equipas é um dos principais desafios e prioridades da Divisão de Equipamentos e Sistemas de Informação. "Numa organização do setor público como a nossa, com uma superfície humana tão vasta e com perfis de utilizadores tão diversos – que vão desde auxiliares operacionais ao Executivo Municipal –, o desafio de nivelar os conhecimentos tecnológicos e de segurança é imenso".

A abordagem faz-se em várias frentes, através da formação específica, campanhas de *awareness*, sensibilização, colaboração, identificação e capacitação de "pontos focais", presentes em todos os serviços. "Estes 'guardiões' não são técnicos, mas permitem que todos os trabalhadores recebam formação adicional de segurança. Tornam-se elos de ligação ao nosso serviço, ajudando a 'traduzir' as nossas políticas de segurança para a realidade do seu trabalho e, em sentido inverso, trazem-nos os desafios específicos deles", reitera o especialista.

UM CLICHÉ COM MUITOS ROSTOS

"Podemos desenhar e implementar a arquitetura tecnológica mais avançada, mas a transformação digital começa e acaba na cultura da organização. No meu papel, muito focado em cibersegurança,

vejo diariamente que o ser humano é, por natureza, o vetor de ataque mais explorado e, por isso mesmo, o mais suscetível", considera o especialista, que aponta para as pessoas como fator-chave para o sucesso do processo de transformação digital de uma organização.

Neste ponto, André Assunção defende que "o sucesso de qualquer novo sistema digital está diretamente dependente da nossa capacidade de garantir a integridade do nosso sistema", o que, por si só, só é possível alcançar graças a uma "cultura ciber" que abarca desde o utilizador final à gestão de topo: "A transformação digital mais eficaz não começa nos sistemas ou nos servidores; começa nas pessoas".

DESAFIOS A ULTRAPASSAR

Internamente, um dos desafios, sublinha André Assunção, passa por "convencer, de forma contínua, a gestão de topo sobre a necessidade de investimento e, crucialmente, da necessidade de criar e formalizar novos papéis no setor público".

Externamente, a dificuldade passa por estabelecer uma "postura de defesa intermunicipal que seja permanente". "A cibersegurança exige arquiteturas e estratégias de longo prazo que, por definição, transcendem os ciclos de governação local. Frequentemente, as prioridades conjunturais, a natureza de cada mandato e a estratégia de cada Executivo Municipal terão de se adaptar à criação de alianças estratégicas de defesa que são fundamentais ao abrigo da própria Diretiva NIS2", observa o especialista.

O CAMINHO A SEGUIR

A prioridade da Divisão de Equipamentos e Sistemas de Informação passa por garantir "a conformidade total com a Diretiva NIS2", uma jornada que conta já com uma base sólida. "Existe já uma grande maturidade e foco na liderança técnica da nossa Divisão, como na nossa Direção Municipal, que sempre entenderam a importância da segurança como um pilar estratégico", partilha. A próxima fase irá exigir o alinhamento do esforço e dos processos implementados com as novas exigências.

Para o futuro, o papel do Diretor de IT será, na visão de André, "obrigatoriamente híbrido", mas sem que seja, necessariamente, "uma desculpa para a iliteracia tecnológica". "No setor público, a principal função de um líder de IT moderno é a gestão de risco. É impossível analisar o risco de negócio de uma vulnerabilidade, ou decidir sobre a implementação de uma arquitetura, sem ter um conhecimento técnico profundo. O líder de IT do futuro tem de ser um estratega que entende o "negócio", mas que só o consegue proteger e inovar porque fala fluentemente a linguagem tecnológica", conclui. ■

ASUS LANÇA EM PORTUGAL UM SUPERCOMPUTADOR PESSOAL DE IA

O Ascent GX10 da Asus conta com um chip Nvidia GB10 Grace Blackwell que oferece computação de inteligência artificial em escala petaflop.

A Asus anunciou a chegada a Portugal do novo Ascent GX10. Este é um supercomputador de Inteligência Artificial (IA) de secretária e, diz a fabricante, foi concebido para tornar o desenvolvimento avançado de IA mais acessível a programadores, investigadores e *data scientists*.

CAPACITAR A INOVAÇÃO

O Asus Ascent GX10 foi concebido para responder às exigências do desenvolvimento da IA. Acelerado pelo superchip NVIDIA GB10, que inclui uma CPU Nvidia Grace de 20 núcleos e uma GPU Nvidia Blackwell, o Ascent GX10 oferece até 1 petaflop de desempenho de IA para inferência e ajuste fino de modelos.

O Ascent GX10 Também integra 128 GB de memória unificada, possibilitando o trabalho em modelos com até 200 mil milhões de parâmetros diretamente num ambiente de trabalho. Com dimensões compactas de 150 x 150 x 51 mm, o Ascent GX10 é indicado para qualquer espaço de trabalho, aliando uma pegada mínima com um desempenho superior.

Apesar do seu tamanho reduzido, o Ascent GX10 é uma verdadeira solução de IA *full-stack* acelerada pelo abrangente *stack* de software de inteligência artificial da Nvidia. Esta plataforma integrada fornece todas as ferramentas necessárias para tarefas como prototipagem, ajuste fino e inferência para o desenvolvimento de aplicações em robótica, visão computacional e modelos de linguagem visual (VLM).

FLUXOS DE TRABALHO EM GRANDE ESCALA

A arquitetura escalável permite uma flexibilidade sem paralelo. Os utilizadores podem ligar duas unidades Ascent GX10 através das interfaces

de rede ConnectX-7 de alta velocidade para duplicar instantaneamente o desempenho de IA para 2 petaflops, com até 256 GB de memória unificada e 8 TB de armazenamento. O Ascent GX10 permite um poderoso treino de IA local a custos reduzidos, garantindo ao mesmo tempo segurança de nível empresarial e a manutenção dos dados confidenciais em ambiente local.

O Ascent GX10 disponibiliza opções de armazenamento flexíveis, adaptadas a todas as necessidades de desenvolvimento de IA. A opção de SSD M.2 2242 NVMe PCIe 4.0 x4 de 1 TB é adequada para iniciantes em IA que trabalham com conjuntos de dados menores e projetos experimentais. O modelo equipado com SSD M.2 2242 NVMe PCIe 4.0 x4 de 2 TB é ideal para suportar conjuntos de dados maiores, vários modelos e experiências em execução simultânea.

Para aqueles que lidam com fluxos de trabalho extensos e em grande escala, o futuro Ascent GX10 com SSD M.2 2242 NVMe PCIe 5.0 x4 de 4 TB é adequado para utilizadores que gerem vários conjuntos de dados ou projetos simultaneamente, garantindo que todos os dados estejam à mão.

DESIGN TÉRMICO

O Ascent GX10 foi meticulosamente projetado, diz a própria Asus, e apresenta um design térmico otimizado para lidar com cargas de trabalho exigentes e garantir um alto desempenho sustentado.

O avançado sistema térmico possui controlo de ventilador de 7 níveis, aletas ultra-largas, cinco tubos de calor e ventiladores duplos de 140 x 80 mm para puxar o ar através de aberturas discretas na parte inferior, garantindo um fluxo de ar potente e eficiente.

O supercomputador pessoal com IA Asus Ascent GX10 está disponível em Portugal. ■

CONTROLO FINANCEIRO E INTEGRAÇÃO ENTRE ÁREAS: BRIGHTEN CONSULTING E SAGE MELHORAM NEGÓCIO DA FLATLANTIC

Liderar um setor implica mais do que produzir em escala: exige também processos de gestão à altura. Foi com esta visão como ponto de partida que a Flatlantic identificou na modernização tecnológica um passo essencial para sustentar o seu crescimento e reforçar a competitividade.

MARTA QUARESMA FERREIRA

OS NÚMEROS não mentem: com uma produção anual de 3,5 milhões de pregados e 1,5 milhões de linguados, a Flatlantic posiciona-se como o maior produtor ibérico de pregado e o segundo maior da Europa.

Estes valores de produção necessitavam, no entanto, de uma gestão que fosse ao encontro do negócio, como explica Douglas Maroeli, CFO da Flatlantic: "precisávamos de substituir um ERP que já não respondia às exigências da nossa operação, quer pela falta de integração entre áreas, quer pela dificuldade em obter dados fiáveis em tempo real. A gestão de uma operação deste tamanho exige visibilidade, controlo e escalabilidade, e sentíamos que era o momento certo para dar esse salto".

TRANSFORMAR PARA CHEGAR MAIS LONGE

Identificada a necessidade de mudar o ERP, e analisados um conjunto de requisitos, João Caracol, Service Line Lead, da Brighten Consulting, sublinha que o Sage X3 demonstrou ser "a solução com melhor *fit* face à complexidade e ambição do negócio", destacando-se pela sua "flexibilidade, pela cobertura funcional e pela capacidade de acompanhar o nosso crescimento, nacional e internacional", acrescenta Douglas Maroeli.

Neste projeto, e de forma a atender à operação altamente especializada, o parceiro teve a missão de "garantir uma transição segura e simplificada para o novo ERP, minimizando o impacto na operação e assegurando que os objetivos estratégicos da Flatlantic fossem cumpridos". "Desde a análise inicial até à formação das equipas, a Brighten assumiu um papel consultivo e de implementação, com foco na eficiência e adaptação à realidade da empresa", sublinha João Caracol.

Do lado da Sage, e para enfrentar "os desafios comuns a empresas com operações em crescimento e forte vocação exportadora", a escolha desta solução "permitiu responder a estas necessidades com uma solução robusta,

flexível e adaptável a contextos multiempresa, multigeografia e com elevado volume de dados".

MELHOR PLANEAMENTO = MELHOR TOMADA DE DECISÃO

A decisão alinhada e validada pelo cliente culminou num projeto que decorreu "de forma muito positiva, com envolvimento direto da equipa de gestão da Flatlantic e uma calendarização faseada que permitiu mitigar riscos", recorda João Caracol.

A migração foi realizada com sucesso, sem impacto na operação, com a garantia da formação e capacitação das equipas para uma adoção "fluída e rápida". "Quando temos pessoas a trabalhar há muito tempo com um sistema há um pouco de resistência em mudar. [A nova solução] serviu para quebrar um paradigma", defende o CFO da Flatantic.

O projeto e *feedback* sobre a implementação "tem sido muito positivo", com o Service Line Lead da Brighten Consulting a destacar a forma como o parceiro conseguiu "simplificar um processo complexo, garantindo estabilidade e resultados desde o primeiro dia". No fim, "o cliente valorizou a nossa abordagem próxima, o conhecimento funcional e a capacidade de adaptação às especificidades da sua operação".

Da perspetiva de Douglas Maroeli, "a solução trouxe ganhos claros ao nível do controlo financeiro e da integração entre áreas como compras, vendas, logística e contabilidade", com um "acesso a informação fiável e em tempo útil, o que permite melhorar o planeamento e a tomada de decisão". Com uma outra empresa localizada em Espanha, uma das missões para o futuro passa por integrar os sistemas com a organização em Portugal. "Vai trazer-nos muitos benefícios e vantagens no nosso dia-a-dia", acredita. ■

A ERA DA ALGORITMOCRACIA

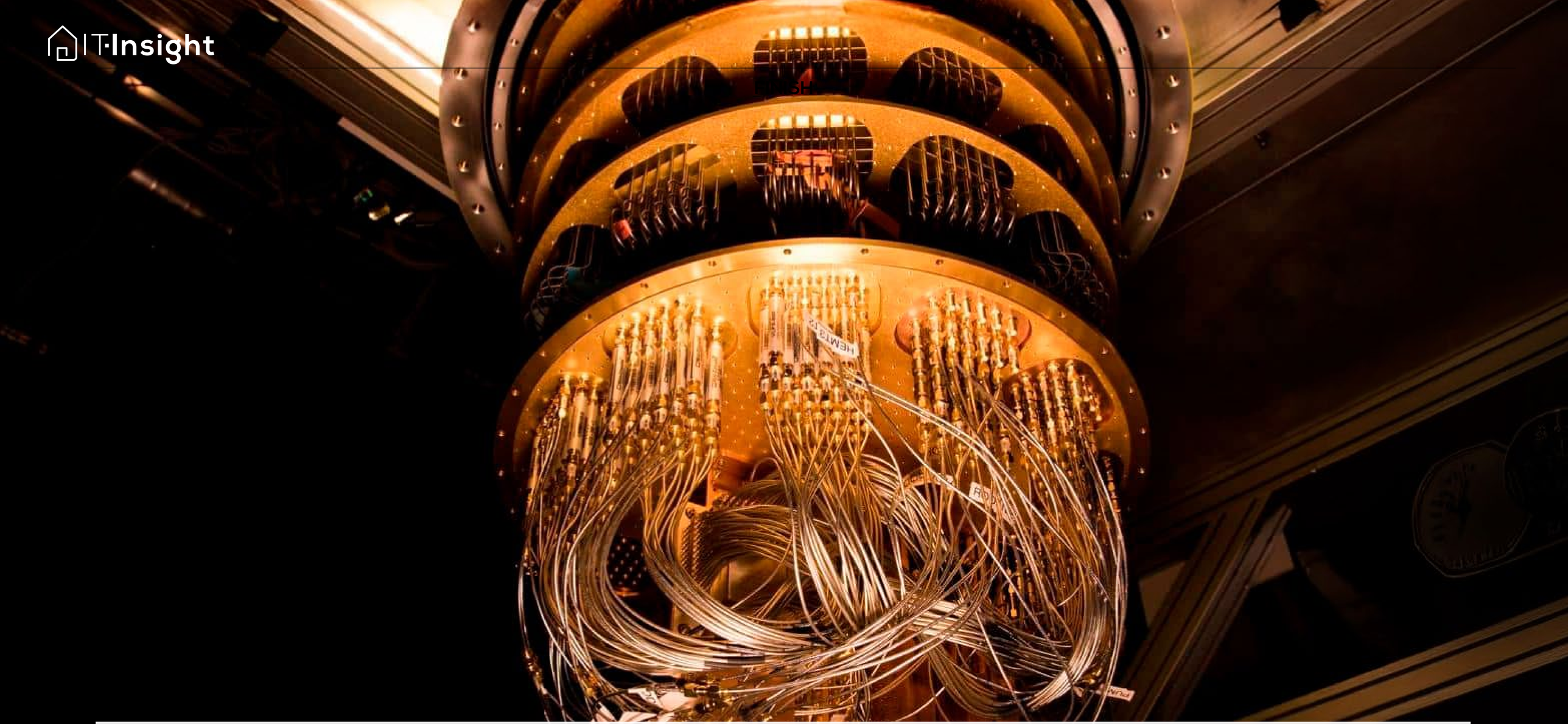
"Algoritmocracia", de Adolfo Mesquita Nunes, é uma leitura que parte de uma pergunta simples, mas inquietante: o que acontece à política quando começamos a confiar mais em algoritmos do que em pessoas? O autor mergulha no modo como a inteligência artificial está a reconfigurar o debate público, a influência das plataformas e o próprio exercício do poder. Uma reflexão sobre o equilíbrio frágil entre eficiência e liberdade, e sobre o lugar que ainda cabe ao julgamento humano num tempo em que os dados parecem saber mais do que nós. ■

SILVES CELEBRA A ARTE CONTEMPORÂNEA

Marco da criatividade e da expressão artística, a Art Expo Algarve transforma Silves num ponto de encontro para a arte contemporânea. O evento regressa de 14 a 16 de novembro, onde mais de 60 artistas dão vida a pinturas, esculturas, fotografias e instalações. Entre música ao vivo, performances e uma parede de graffiti em constante evolução, o evento convida o público a explorar e a descobrir a arte de forma próxima e informal, reafirmando o Algarve como território cultural nacional. ■

ALENTEJO REINVENTADO

Símbolo do trabalho e do tempo, o "Moagem – Industrial Lodge" nasceu de uma antiga moagem de cereais para se transformar num espaço de descanso e descoberta no coração de Viana do Alentejo. Entre paredes que guardam a memória industrial, o hotel combina o design contemporâneo e a hospitalidade alentejana. O exterior convida à pausa, com uma piscina e spa que se unem com a paisagem de oliveiras. A sustentabilidade marca o projeto, da recuperação do edifício à eficiência energética e ao apoio a produtores locais. No restaurante, o fogo assume o protagonismo numa cozinha aberta que reinterpreta a região com criatividade. ■



Google alcança avanço quântico 14 mil vezes mais rápido

A Google apresentou o primeiro algoritmo quântico com potencial de aplicação prática, executado no processador Sycamore 2. O sistema híbrido quântico-clássico revelou-se teoricamente 14 mil vezes mais rápido do que os supercomputadores convencionais em tarefas de otimização e simulação de materiais. O avanço resulta de progressos na correção de erros e na estabilidade dos qubits, aproximando a computação quântica da sua utilização comercial e inaugurando uma nova fase de aplicações reais.

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:

Beatriz Salzedas – beatriz.salzedas@medianext.pt - (351)910 788 082

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: Luís Santos Ribeiro, 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