

IA PARA REINVENTAR O NEGÓCIO

IT·Insight
talks

NIS 2: cumprir com eficácia



Empurrar limites para **moldar** o futuro



Cloud & Infra



Workplace



Applications



Data & AI



Security

claranet.com/pt

claranet®

IT Insight



#60 MARÇO 2026

IA PARA REINVENTAR
O NEGÓCIO



IN DEEP

d_Δl_gest por Henrique Carreiro

360° VIEW

“A Luís Simões passou a encarar a tecnologia como um acelerador de eficiência, escalabilidade e diferenciação”

TRANSFORM

EDP-DXC transforma IA em operação com fábrica de modelos

WISHLIST

Samsung Galaxy S26 reforça IA, desempenho e privacidade

IN DEEP | DATA STRATEGY & AI GOVERNANCE: TURNING DATA INTO BUSINESS VALUE

Estruturar dados para transformar o negócio com IA

IT INSIGHT TALKS | CIBERSEGURANÇA

Entre a exigência e a maturidade na era da NIS2

FACE 2 FACE | DAVID MARQUES

“Temos de aproveitar este paradigma da entrada em vigor da NIS2 e cada vez mais passar para modelos de gestão de risco”

BEST OF BREED | NEXT-GEN NETWORKING & ENTERPRISE CONNECTIVITY

Networking: a infraestrutura que o negócio não vê

IT INSIGHT TALKS



CIBERSEGURANÇA

FACE 2 FACE



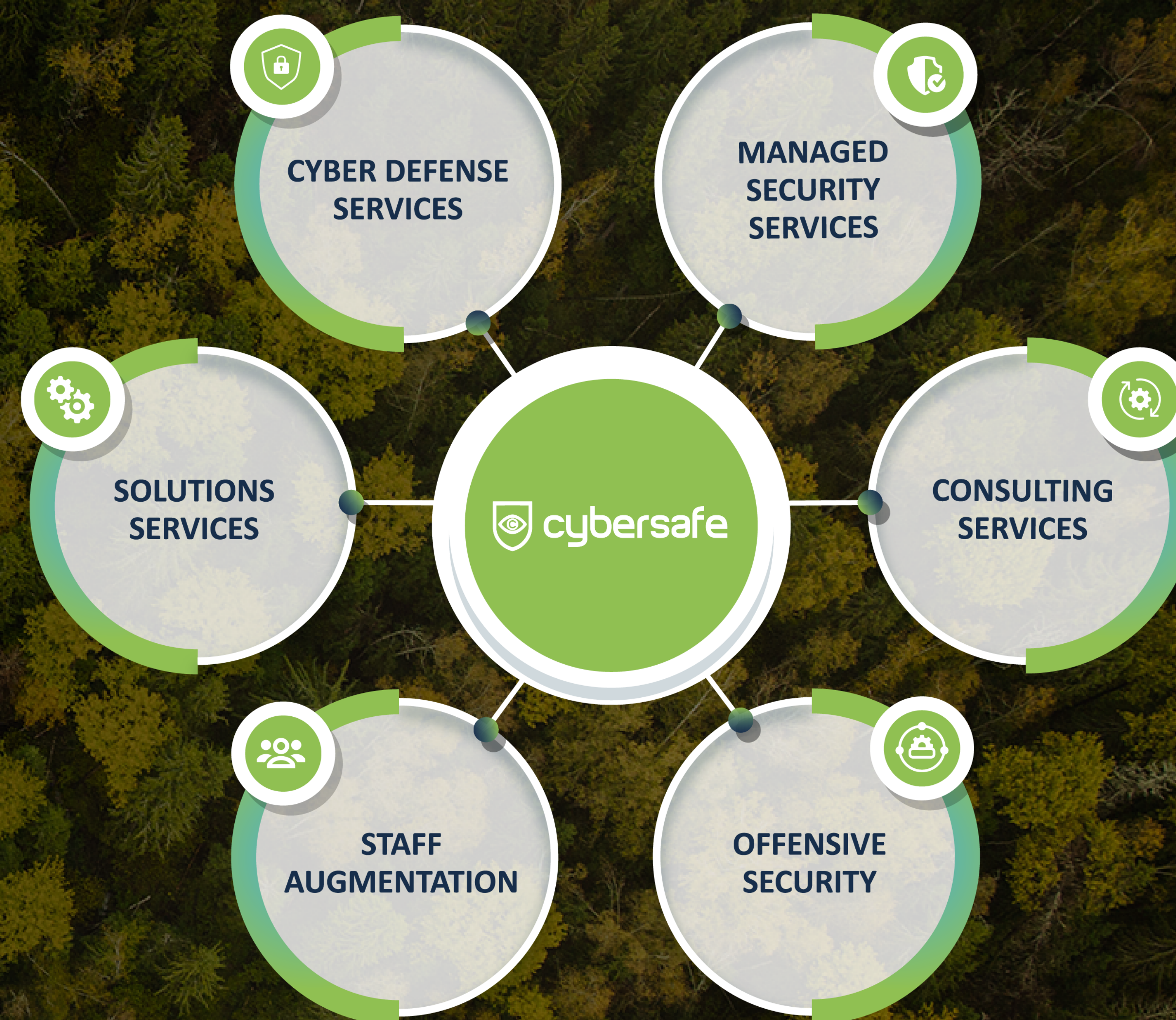
DAVID MARQUES,
GRUPO NABEIRO



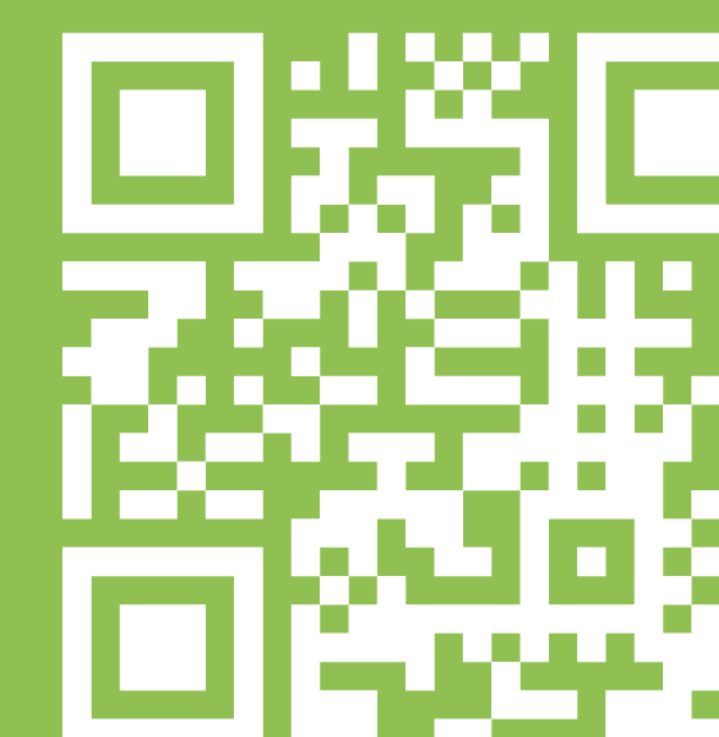
CYBERSECURITY EVERYWHERE

Empresa totalmente focada em soluções e serviços de cibersegurança, empenhada em tornar as organizações mais seguras e resilientes. Defendemos o conceito de “cybersecurity everywhere”: segurança contínua e integrada, desde a infraestrutura ao utilizador.

5 CONTINENTES +150 CLIENTES



SAIBA MAIS:



+351 210 360 276 contacto@cybersafe.pt www.cybersafe.pt

IT Insight



#60 MARÇO 2026

D_AI_DIGEST



IT INSIGHT TALKS | CIBERSEGURANÇA

 **cybersafe** Da conformidade à maturidade: os desafios da NIS 2 para as organizações portuguesas

ManageEngine  O direito à privacidade deve aplicar-se também à sua atividade online — sem exceções

 **LOGICALIS** Architects of Change Da ameaça à força: como resolver a escassez de competências em Cibersegurança

 **SECURNET** ALWAYS ONLINE | ALWAYS SECURE NIS2: No mínimo e para começar, um (bom) plano...

 **Symantec** ZTNA: A Alternativa às VPNs que Está a Redefinir a Segurança no Trabalho Híbrido

 **VisionWare** O que dizem os olhos da NIS2: conformidade em alta definição

IN DEEP

DATA STRATEGY & AI GOVERNANCE: TURNING DATA INTO BUSINESS VALUE

NOESIS Como alinhar estratégia de Dados e Governance de IA ao negócio

 **SECURNET** ALWAYS ONLINE | ALWAYS SECURE Adoção segura de IA: Transformar risco em vantagem competitiva

BRANDED CONTENT | BEST OF BREED

 **IP Telecom** Next-Gen Networking & Enterprise Connectivity

...e ainda

claranet

LiSPOLiS
POLO TECNOLÓGICO DE LISBOA



BEST OF BREED



360° VIEW

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

HENRIQUE CARREIRO



Agentes de IA e a nova superfície de ataque: do perímetro ao comportamento

A NIS2 nasceu num mundo em que a conversa pública sobre risco gira sobretudo em torno da indisponibilidade: ransomware, DDoS, falhas de fornecedores. A própria diretiva, porém, é mais ampla e agnóstica: exige gestão de risco, controlo de acessos e segurança da cadeia de abastecimento, entre outros aspetos. E eis que, no início de 2026, os agentes de IA começam a ser usados de forma alargada, ao princípio, pelo menos, em desenvolvimento de software, e mudam o eixo da conversa. Quando uma aplicação, tenha ela a forma que tiver, deixa de ser ferramenta e passa a ser um “colega” que decide, escreve código, abre *tickets*, transfere ficheiros, envia emails e negocia com API, a superfície de ataque deixa de ser perímetro e passa a ser comportamento.

Os agentes introduzem brechas novas e ainda mal enquadradas na prática regulatória e operacional: identidade delegada (*tokens* persistentes, chaves partilhadas, *service accounts* sem dono), permissões acumulativas (cada integração acrescenta um caminho de exfiltração de dados), *prompt injection* e envenenamento de dados (o atacante persuade em vez de explorar portas), cadeias de ferramentas e *plugins* com dependências opacas, e atualizações de modelo que alteram decisões em produção sem controlo de alteração. Há também um problema de prova: como demonstrar, num incidente, o que o agente “viu”, que contexto recebeu, que ferramentas acionou e por que executou uma ação concreta?

“

É AQUI QUE SE COMEÇA A DESENHAR UMA NIS3, OU EQUIVALENTE, QUE TORNE EXPLÍCITOS OS CUIDADOS A TER NESTE NOVO MUNDO. NÃO POR FALTA DE REGRAS, MAS POR FALTA DE ENCAIXE ENTRE GOVERNAÇÃO DA ENTIDADE E SEGURANÇA DO SISTEMA DE IA”

Isto já não é hipotético. Há organizações a dar a agentes privilégios de escrita em repositórios, sistemas de CRM e de faturação, bases de dados e fluxos de aprovação. Um erro ou manipulação passa a ter a escala e a velocidade de um utilizador super-privilegiado, mas sem o instinto humano de cautela. E quando o agente falha, a tentação é atribuir o evento à imprevisibilidade do modelo, como se isso fosse justificação plausível, ignorando que a responsabilidade emerge da cadeia inteira: modelo base, fornecedor, integrador e entidade que delega credenciais.

É aqui que se começa a desenhar uma NIS3, ou equivalente, que torne explícitos os cuidados a ter neste novo mundo. Não por falta de regras, mas por falta de encaixe entre governação da entidade e segurança do sistema de IA. Terá de tratar agentes como infra-estruturas operacionais autónomas: inventário obrigatório (o que existe, onde atua, com que creden-

ciais), limites de autonomia por classe de risco, segregação e rotação de credenciais, privilégio mínimo com elevação controlada, registos auditáveis que permitam reconstruir a sequência factual (*inputs*, contexto entregue, ferramentas invocadas e *outputs*), testes de segurança específicos para interação (*red teaming* de *prompts* e de cadeias de ferramentas), e deveres claros para fornecedores e integradores sobre actualizações, deriva de comportamento e vulnerabilidades conhecidas. E na notificação de incidentes, “foi o agente” não pode funcionar como biombo: tem de haver responsabilidade técnica e organizacional, distribuída com critério ao longo da cadeia.

No novo mundo dos agentes, um pedido, ainda que bem formulado, pode tornar-se a vulnerabilidade dominante. A regulação tem de acompanhar esta mudança antes que a autonomia se transforme em ataque por procuração. ■

Há uma coisa que nem uma
empresa de mil milhões de
dólares pode pagar:

uma violação de segurança

Proteja o seu negócio com a

ManageEngine



Gestão de Identidade e Acesso
Segurança da Informação e Gestão de Eventos
Segurança de endpoints | Segurança de rede | Segurança de dados

<https://www.manageengine.com/br/cybersecurity-solutions.html>

OTIMISMO DOS EXECUTIVOS PORTUGUESES PARA 2026 CONTRASTA COM BAIXO INVESTIMENTO EM IA

Nove em cada dez executivos de topo em Portugal encaram 2026 com confiança, mas o investimento em IA continua significativamente abaixo dos níveis globais.



O mais recente barómetro C-Suite da Forvis Mazars Group indica que 90% dos executivos de topo em Portugal estão otimistas quanto ao crescimento em 2026, num contexto em que sete em cada dez empresas reportaram um aumento dos lucros

ao longo de 2025. Apesar deste cenário positivo, a incerteza económica e o aumento da concorrência continuam a ser apontados como fatores que podem travar a expansão dos negócios.

De acordo com o relatório, realizado entre outubro e novembro de 2025 junto de 3.012 líderes C-Suite de organizações com fins lucrativos, com receitas anuais superiores a um milhão de dólares, em quarenta países, a inteligência artificial, o aumento da concorrência, as novas tecnologias, a agitação social e os novos modelos de trabalho surgem como as forças externas que mais pressionam as empresas portuguesas. ■

UE APELA AO CONTROLO EUROPEU DAS TECNOLOGIAS CRÍTICAS

Dependência de grandes fornecedores tecnológicos norte-americanos aumenta riscos económicos e de cibersegurança, alertam responsáveis europeus.



A União Europeia deve manter o controlo sobre as tecnologias-chave que sustentam a economia do bloco, numa altura em que cresce a preocupação com a dependência de gigantes tecnológicos sediados fora da Europa. O alerta foi deixado pela

Comissária Europeia dos Serviços Financeiros, Maria Luís Albuquerque, num contexto de tensões geopolíticas e de maior exposição a riscos digitais. “A Europa tem de reter o controlo sobre as tecnologias essenciais que sustentam e impulsionam as nossas economias”, afirmou a comissária durante uma conferência dedicada à regulação do setor fintech, em Bruxelas. A declaração surge num momento em que o conceito de soberania digital ganha peso na agenda europeia, o que reflete, por sua vez, o receio de que uma dependência excessiva de empresas tecnológicas dos Estados Unidos possa representar uma ameaça à segurança económica e estratégica da região. ■

- **Porque é que a escassez de competências em cibersegurança é um risco crítico para as organizações?**
- **Porque é tão difícil atrair e reter talento especializado?**
- **Porque motivo as competências certas em cibersegurança são decisivas para os CIOs?**

Para saber a resposta a estas questões,
faça o download gratuito do estudo:

pt.logicalis.com/estudos-idc-logicalis



PORTUGAL DESTACA-SE NA CORRIDA EUROPEIA À IA GENERATIVA

Um estudo da Bain revela que 62% dos portugueses utilizam estas ferramentas regularmente.



Portugal posiciona-se na linha da frente da adoção de Inteligência Artificial (IA) generativa na Europa, segundo o estudo “*European Consumer Gen AI Sentiment & Behaviour*”, da Bain & Company, que analisou os mercados de Portugal,

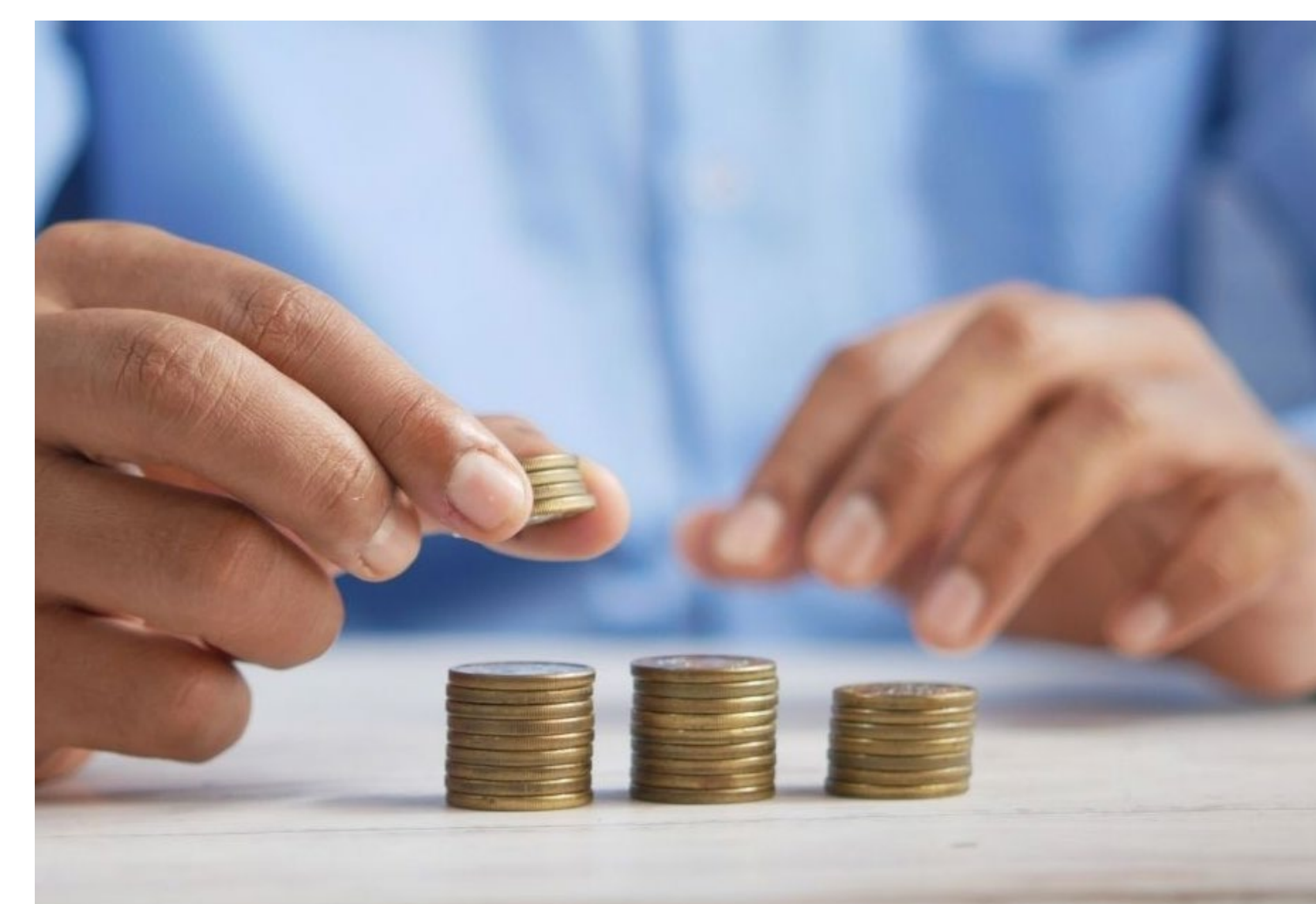
Espanha, Reino Unido, França e Alemanha, no último trimestre de 2025, num total de 7.298 respostas válidas (1.351 em Portugal).

De acordo com os dados, 62% dos portugueses inquiridos afirmam utilizar regularmente ferramentas de IA generativa, acima da média europeia de 52%. Nos últimos quatro anos, a taxa de utilização em Portugal entre os inquiridos passou de 6% para 62%, refletindo uma aceleração significativa na adoção destas tecnologias.

Embora 55% dos utilizadores portugueses indiquem que recorrem sobretudo a estas ferramentas para uso pessoal, o primeiro contacto com a IA generativa ocorreu maioritariamente em contexto académico ou profissional. ■

GASTOS GLOBAIS EM IT SOBEM 10,8% EM 2026 E CHEGAM A 6,15 BILIÕES

O investimento mundial em IT deverá atingir 6,15 biliões de dólares em 2026, impulsionado sobretudo pela corrida à inteligência artificial, com forte aceleração em servidores e centros de dados.



Os gastos mundiais em tecnologias de informação devem atingir os 6,15 biliões de dólares em 2026, um aumento de 10,8% face a 2025, impulsionados sobretudo pelo investimento contínuo em infraestruturas de Inteligência

Artificial (IA), de acordo com a mais recente previsão da Gartner. Segundo a consultora, o crescimento do investimento em infraestruturas de IA mantém-se robusto, apesar das preocupações em torno de uma eventual “bolha” tecnológica. A procura por parte dos grandes operadores de cloud continua a alimentar o investimento em servidores otimizados para cargas de trabalho de IA. Nesse contexto, a despesa com servidores deve vir a acelerar significativamente em 2026, com um crescimento anual de 36,9%. ■

NOESIS

Technology for real growth

A Noesis é uma **consultora tecnológica internacional** com **30 anos de experiência** focada em impulsionar a transformação digital e apoiar o crescimento das organizações.

Os nossos serviços de TI incluem Cloud & IT Operations, Cybersecurity, Custom and Low-code Software Development, Analytics, AI, Automation e Quality Assurance – todos desenhados e desenvolvidos para responder às necessidades dos nossos clientes.



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

www.noesis-corporation.com



IT Operations & Infrastructure

Cloud & Security

Enterprise Application Integration

Application Development

Data Analytics & AI

DevOps & Automation

Quality Management

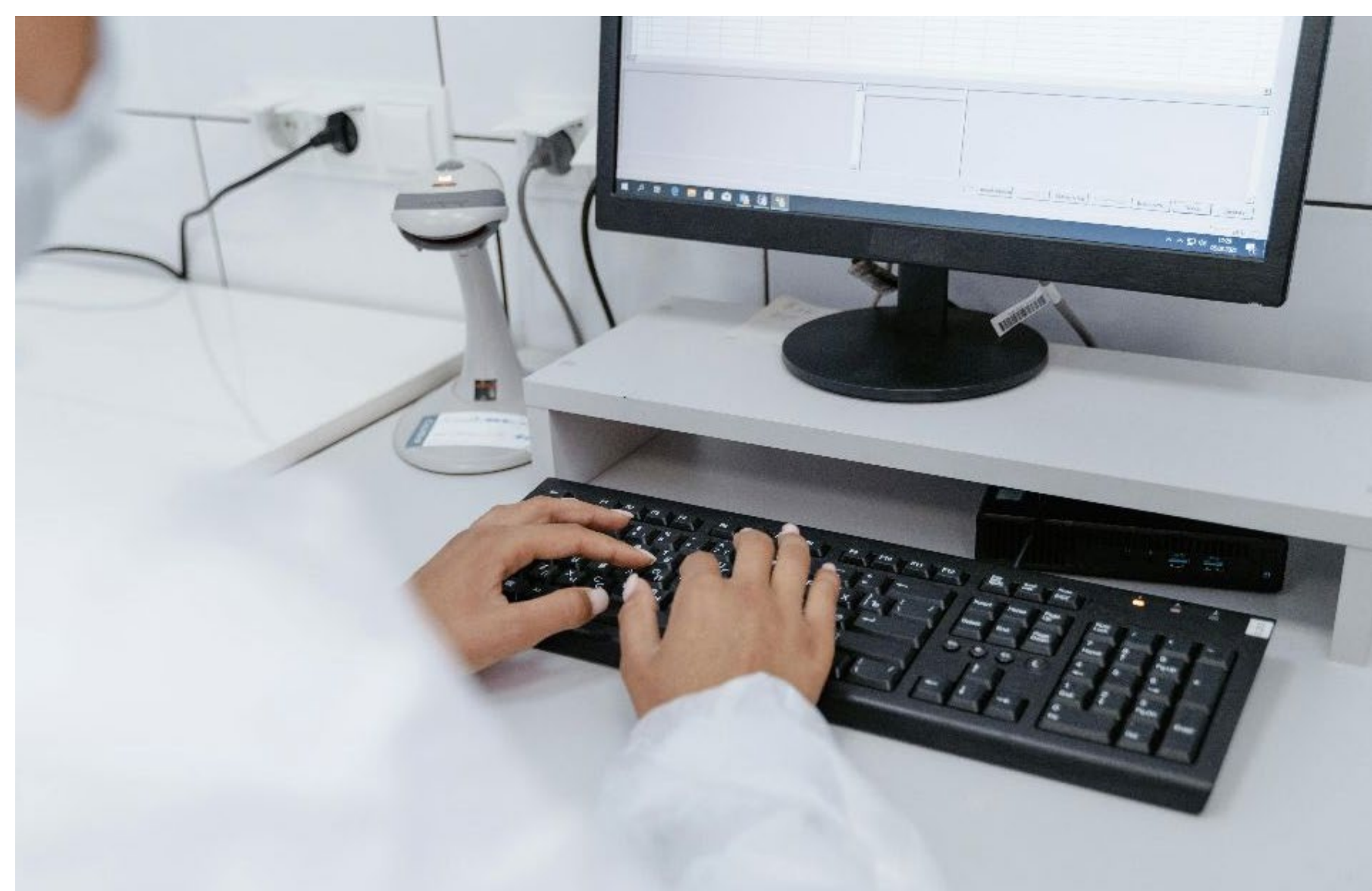
Professional Services



© Noesis. All rights reserved.

PORTUGAL PREPARA-SE PARA ESPAÇO EUROPEU DE DADOS DE SAÚDE

Investigadores portugueses preparam-se para o Espaço Europeu de Dados de Saúde. O regulamento europeu vai permitir acesso seguro a dados para investigação e políticas públicas.



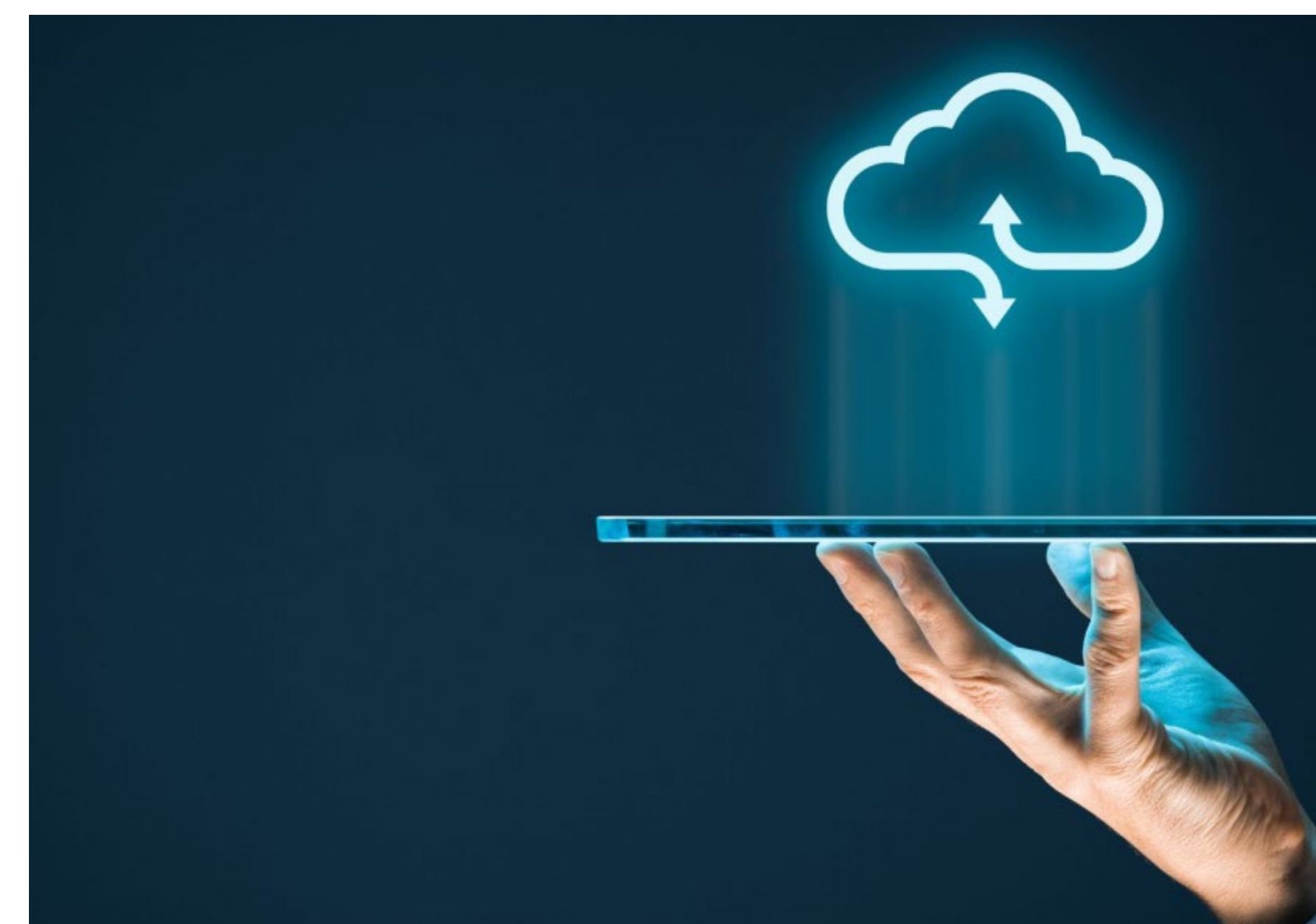
A comunidade científica e académica portuguesa prepara-se para a implementação do Espaço Europeu de Dados de Saúde (EEDS), o primeiro espaço comum europeu dedicado à partilha estruturada de dados de saúde. O novo enquadramento, esta-

belecido por regulamento da União Europeia, pretende garantir um acesso seguro, simplificado e interoperável a informação clínica em toda a Europa, com o objetivo de acelerar a investigação, apoiar a definição de políticas públicas e fomentar a inovação no setor da saúde.

O regulamento define um modelo assente em dois pilares. O primeiro diz respeito à utilização primária dos dados, centrada na prestação de cuidados de saúde, permitindo que cada cidadão aceda à sua informação clínica, a controle e a partilhe além-fronteiras. ■

GASTOS GLOBAIS EM CLOUD SOBERANA VÃO ATINGIR 80 MIL MILHÕES DE DÓLARES EM 2026

O investimento em serviços de cloud soberana continua a acelerar à medida que governos e setores regulados procuram maior controlo sobre dados e infraestruturas críticas.



Os gastos mundiais em infraestrutura de cloud soberana como serviço (IaaS) podem vir a atingir os 80 mil milhões de dólares em 2026, o que representa um crescimento de 35,6% face a 2025, de acordo com a mais recente previsão da Gartner.

De acordo com esta análise, o aumento das tensões geopolíticas está a levar organizações fora dos Estados Unidos e da China a investir de forma mais significativa em cloud soberana, com o objetivo de reforçar a independência digital e tecnológica.

Os governos vão manter-se como os principais impulsionadores deste mercado, seguidos por setores altamente regulados e organizações de infraestruturas críticas, como energia, *utilities* e telecomunicações. ■



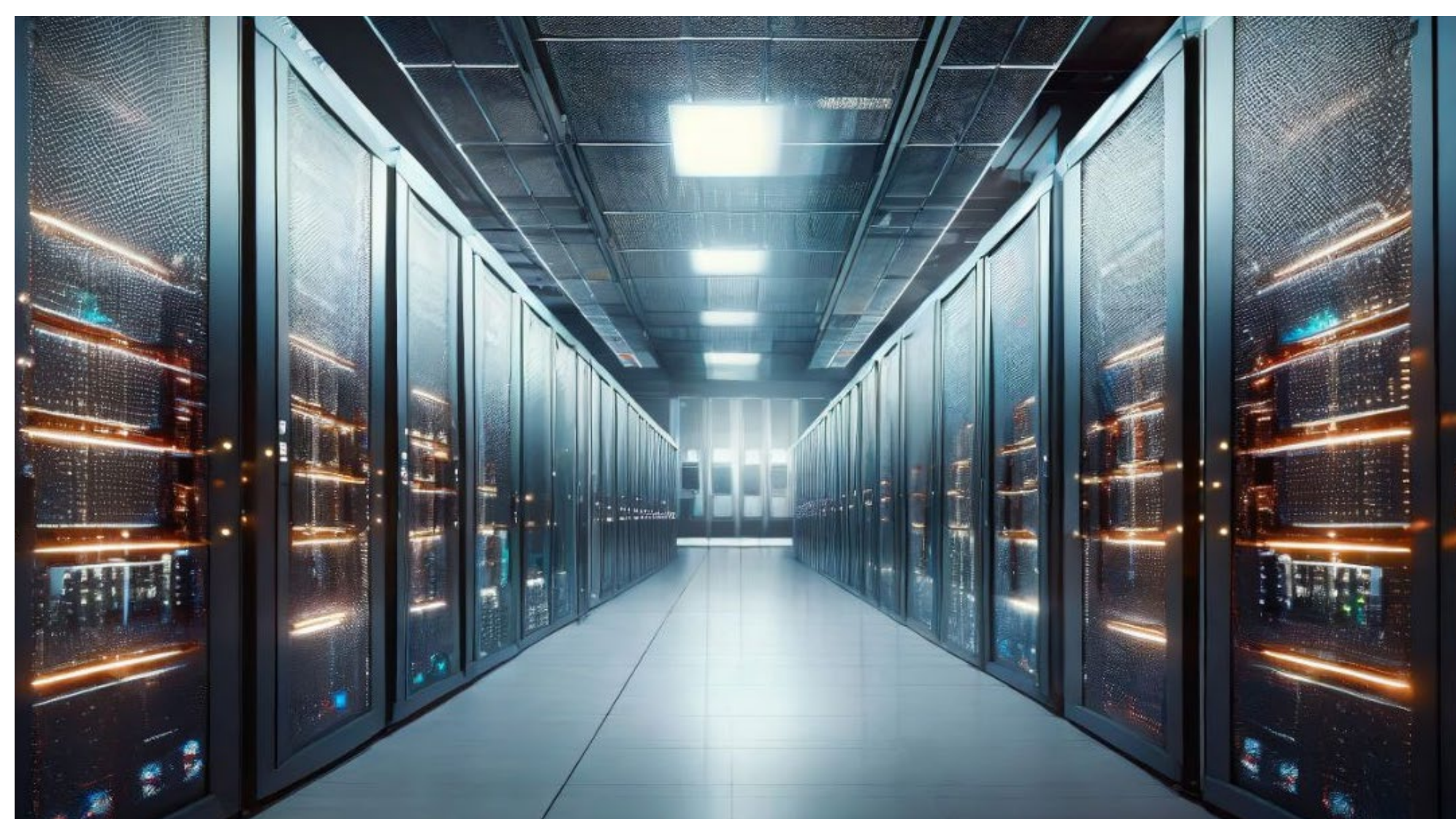
A GESTÃO DE RISCO COMEÇA NA ESCOLHA DOS PARCEIROS CERTOS!

☆ **SECURNET** | Parceiro do Ano HPE 2025



SETOR DE DATA CENTERS ACELERA NA EUROPA COM RÁPIDA EXPANSÃO EM PORTUGAL

O novo relatório “State of European Data Centres 2026” mostra um crescimento acelerado de data centers na Europa, impulsionado por IA, cloud e soberania digital.



O setor de data centers está a passar por uma fase de expansão sem precedentes, impulsionada pela rápida digitalização, pela adoção de inteligência artificial, pelo crescimento de *workloads* de cloud

e pela necessidade de infraestruturas digitais resilientes e soberanas.

As conclusões constam do relatório “*State of European Data Centres 2026*”, uma análise abrangente lançada pela European Data Centre Association (EUDCA) sobre a evolução, impacto económico e desafios do setor de data centers na Europa

O relatório destaca que os mercados do Sul da Europa, como Portugal, Espanha e Itália, estão a assistir a uma rápida expansão, assim como os países nórdicos, a Europa Central e de Leste e várias metrópoles de segunda linha. ■

COMÉRCIO GLOBAL ENTRA EM ESTAGNAÇÃO EM 2026 APÓS CRESCIMENTO DO ÚLTIMO ANO

Depois de crescer 3,5% em 2025, o comércio global entra em estagnação este ano, pressionado pela guerra comercial, novas tarifas e a incerteza política nos Estados Unidos.



Depois de um crescimento de 3,5% em 2025, o comércio global deverá registar um momento de estagnação em 2026, travado pela intensificação da guerra comercial, pela antecipação de compras no ano anterior e pela incerteza política

nos Estados Unidos. A recuperação só deverá chegar em 2027, com um avanço estimado de cerca de 2%, segundo um novo relatório da Crédito y Caución.

A seguradora explica que o desempenho de 2025 foi impulsionado, sobretudo, pelo aumento do investimento em inteligência artificial, em particular nos EUA. No entanto, a imposição de novas tarifas alfandegárias está agora a alterar o cenário, levando empresas a repercutirem custos adicionais nos preços finais, o que reduz a procura e condiciona o investimento. ■

CYBERATTACKS ARE INCREASING

HERE ARE THREE STEPS TO PROTECT YOUR CRITICAL DATA

1

REPLACE YOUR
VIRTUAL PRIVATE NETWORK (VPN)
WITH SYMANTEC ZTNA

2

COMBINE SYMANTEC ZTNA WITH
THREAT INTELLIGENCE AND
DATA LOSS PREVENTION (DLP)

3

IMPLEMENT ZTNA + DLP IN STEPS

Legends Never Die

VENDAS EM PORTUGAL PRIORIZAM IA EM 2026

Estudo da Salesforce aponta que equipas comerciais em Portugal colocam a inteligência artificial no topo das prioridades para 2026.



As equipas comerciais em Portugal estão a posicionar a Inteligência Artificial (IA) e os agentes de IA como prioridade estratégica para 2026. A conclusão resulta da mais recente edição do “*State of Sales Report*”, da Salesforce, baseada num

inquérito a 4.050 profissionais de vendas de mais de 20 países, incluindo Portugal, realizado entre agosto e setembro de 2025.

Segundo o estudo, que abrangeu líderes de vendas, representantes comerciais, profissionais de desenvolvimento de negócio e operações, representando mercados como Portugal, Espanha, Alemanha, Reino Unido, Estados Unidos e Japão, 89% das equipas e empresas de vendas inquiridas em Portugal já utilizam alguma forma de IA em tarefas como prospeção, previsão, pontuação de leads ou redação de emails. Entre os utilizadores, 89% afirmam que a tecnologia melhora a compreensão do cliente e 87% indicam que reduz o nível de stress associado ao trabalho comercial. ■

APENAS 6% DAS EMPRESAS TÊM COMPETÊNCIAS PARA PROJETOS CRÍTICOS

Estudo revela que a escassez de competências se está a agravar em 2026. A maioria das organizações planeia contratar para colmatar lacunas, num contexto de maior complexidade no recrutamento.



As empresas entram em 2026 confrontadas com lacunas de competências cada vez mais acentuadas e processos de contratação mais complexos. De acordo com um estudo da Robert Half, apenas 6% das organizações afirmam

dispor do talento necessário para concluir projetos considerados prioritários. O inquérito, realizado junto de mais de 2.000 gestores de contratação nos Estados Unidos, indica que 62% consideram que as lacunas de competências são hoje mais evidentes do que há um ano. A escassez afeta transversalmente várias áreas, com níveis particularmente baixos em funções como jurídico, marketing, finanças, recursos humanos, tecnologia e saúde.

No setor jurídico, apenas 1% dos gestores afirma ter o talento necessário para projetos críticos. Em marketing e áreas criativas, esse valor desce para 4%. ■



+5000 projetos desenvolvidos



+100 colaboradores



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



+200 clientes ativos



+10 geografias



Porto | Lisboa | Praia | Mindelo



geral@visionware.pt



+351 225 323 740



visionware.pt

GOVERNO REGULAMENTA DIREITO AO ESQUECIMENTO

O Conselho de Ministros aprovou a regulamentação da Lei do Direito ao Esquecimento. O diploma visa eliminar discriminação no acesso ao crédito e seguros.



O Conselho de Ministros aprovou a regulamentação da Lei do Direito ao Esquecimento, prevista na Lei n.º 75/2021, de 18 de novembro, assegurando a sua plena aplicação mais de quatro anos após a publicação do diploma original.

A medida visa eliminar práticas discriminatórias no acesso ao crédito à habitação, ao crédito ao consumo e aos seguros associados, relativamente a pessoas que tenham superado ou mitigado situações de risco agravado de saúde ou de deficiência.

A legislação já estabelecia limites temporais para a utilização de informação de saúde em contexto pré-contratual por parte de instituições de crédito e seguradoras, prevendo, no entanto, regulamentação posterior quanto a aspetos específicos, incluindo a definição de prazos mais favoráveis ao consumidor. Segundo o Governo, esses prazos regulamentares tinham sido ultrapassados, comprometendo a efetividade do regime. ■

PERMISSÕES EXCESSIVAS A AGENTES DE IA CRIAM VULNERABILIDADES NA CADEIA DE SOFTWARE

Estudo alerta para riscos de exposição de credenciais, ataques de prompt injection e introdução de código malicioso em projetos empresariais e open source.



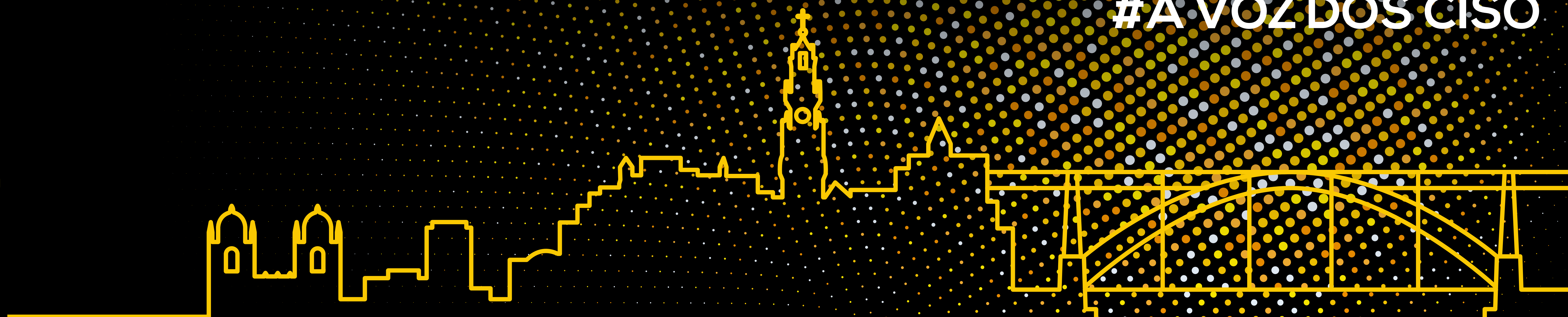
A utilização de ferramentas de *vibe coding* baseadas em Inteligência Artificial (IA) está a ganhar tração entre equipas de desenvolvimento, mas nem sempre com as salvaguardas necessárias. Uma análise

da UpGuard a mais de 18 mil ficheiros públicos de configuração de agentes de IA no GitHub conclui que cerca de 20% dos programadores concedem a estes agentes acesso irrestrito às suas estações de trabalho, permitindo ações de elevado risco sem qualquer validação humana.

Segundo o estudo, na tentativa de ganhar eficiência, muitos *developers* autorizam os agentes de IA a descarregar conteúdos da internet e a ler, escrever ou apagar ficheiros localmente de forma autónoma. Esta prática elimina controlos básicos de segurança e abre caminho a incidentes graves. ■



#A VOZ DOS CISO



14 ABRIL 2026 | GAIA

A VOZ DOS CISO

Depois do sucesso da primeira edição, a IT Security Summit regressa à região Norte no dia 14 de abril de 2026, no Tivoli Kopke Porto Gaia, em Vila Nova de Gaia, duplicando o espaço em plateia para acomodar um número ainda maior de leitores da revista IT Security e profissionais do setor.

Centrada nos temas da resiliência e compliance com ênfase nas necessidades práticas das empresas da região norte e dando voz aos seus protagonistas, a IT Security Summit será uma oportunidade para explorar as tecnologias mais inovadoras que impactam um grande número de indústrias, para além da partilha de conhecimentos entre CISO, CSO, diretores de segurança e diretores de IT com responsabilidade de cibersegurança, originando um ecossistema único de networking.

MARQUE A DATA NA SUA AGENDA.
ÚLTIMA OPORTUNIDADE PARA SE INSCREVER!

INSCREVA-SE AQUI!

PARCEIROS

DIAMOND



PLATINUM



GOLDEN



SILVER



SILVER EXHIBITION



VAD PARTNERS



INSTITUTIONAL PARTNER



“MAIS DO QUE CENTRALIZAR EQUIPAMENTOS, CENTRALIZAMOS NORMAS DE EXCELÊNCIA”

Portugal alcançou a pontuação mais elevada no indicador “Government as a platform” do “OECD Digital Government Index 2025”. Para a ARTE, este resultado assenta numa governação digital robusta e numa estratégia que coloca a resiliência no centro da transformação da Administração Pública.

INÊS GARCIA MARTINS



O mais recente relatório europeu sobre as ameaças digitais alerta para ataques mais sofisticados, exploração de vulnerabilidades conhecidas e riscos acrescidos na cadeia de fornecimento tecnológica. Num cenário em que as infraestruturas críticas e os serviços públicos estão entre os principais alvos,

a maturidade digital do Estado torna-se indissociável da sua capacidade de defesa.

Portugal destacou-se no indicador “Government as a platform” do “OECD Digital Government Index 2025”, ao alcançar a pontuação mais elevada entre os países analisados, superando a Dinamarca, a Coreia, a Austrália e a Irlanda. Em declarações à IT Insight, a Agência para a Reforma Tecnológica do Estado (ARTE) refere que este desempenho “reflete a robustez da governação digital, a conceção de serviços públicos centrados no cidadão, e o investimento em plataformas digitais tais como o portal e a aplicação gov. pt e a Interoperabilidade na Administração Pública”.

A Estratégia Digital Nacional contribuiu para o resultado alcançado, ao “estabelecer objetivos ambiciosos até 2030, com vista a fortalecer a prestação de serviços públicos centrados no cidadão”, enquadramento que assenta na ideia de que “todas as políticas implementadas, assentes em medidas coerentes, promovem a resiliência como um dos pilares da transformação digital do setor público”.

ARQUITETURA DIGITAL E DEFESA EM PROFUNDIDADE

Face aos riscos associados a modelos centralizados e à interdependência tecnológica, a centralização é acompanhada por uma arquitetura de segurança reforçada, já que “a ARTE gere o risco da centralização através de uma estratégia de defesa em profundidade” e “implementamos mecanismos de deteção e resposta que permitem isolar incidentes sem comprometer o todo”.

A uniformização de critérios é igualmente assumida, uma vez que “mais do que centralizar equipamentos, centralizamos normas de excelência” e “garantimos que qualquer serviço, seja em ambiente *on-premises* ou cloud, cumpre os mesmos critérios rigorosos de segurança e continuidade de negócio”.

GESTÃO DE VULNERABILIDADES E SOBERANIA DIGITAL

Quanto à exploração de vulnerabilidades conhecidas, identificada como vetor dominante, sublinha-se que “Portugal dispõe de um quadro robusto liderado pelo Centro Nacional de Cibersegurança e pelo cumprimento das diretivas NIS e a recente transposição da NIS2”.

Em termos operacionais, “na ARTE, a gestão de vulnerabilidades é um processo transversal e sistémico” e “operamos sob os mais elevados padrões

internacionais, utilizando a certificação ISO 27001 como base para os nossos processos críticos e estendendo essas melhores práticas de gestão de risco a toda a organização”.

Esse reforço inclui o Quadro Nacional de Referência para a Cibersegurança, que “permite uma monitorização em tempo real e uma capacidade de resposta imediata à exploração de vulnerabilidades conhecidas”.

Também a dependência de fornecedores internacionais, identificada como fator de risco acrescido para economias de menor dimensão, é enquadrada como um tema de soberania digital, já que “a dependência de tecnologia global é um desafio de soberania digital que Portugal aborda com critérios de segurança rigorosos nos processos de aquisição”.

Para dar resposta, a entidade integra “cláusulas de segurança alinhadas com as orientações europeias, que exigem transparência total sobre a cadeia de fornecimento”, sendo ainda priorizados “fornecedores que garantam conformidade estrita com o RGPD e que possuam certificações de segurança auditáveis”.

A prioridade é, segundo a ARTE, assegurar que “a inovação tecnológica internacional serve o cidadão português sem nunca comprometer a autonomia do Estado ou a integridade dos dados nacionais”. ■

LiSPOLiS

DESDE 1991

HUB PARA EMPRESAS TECNOLÓGICAS E INOVADORAS EM LISBOA

LABORATÓRIOS INDUSTRIAIS, ESPAÇOS DE ESCRITÓRIO, EVENTOS
DO ECOSISTEMA 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.**



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

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

Luxo com capa barata: quando a Gucci decide poupar onde não deve



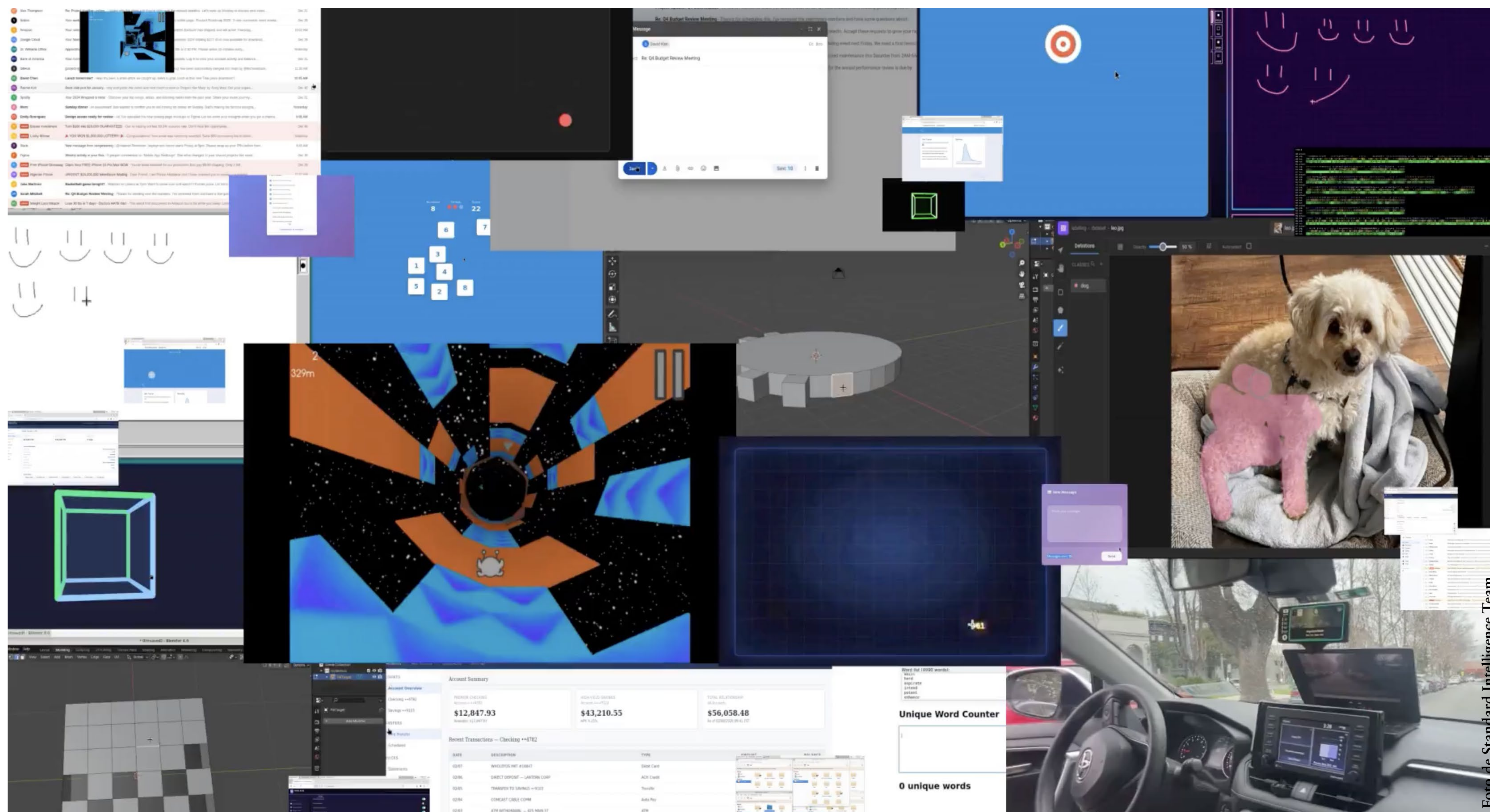
Foto de Gucci/Divulgação

A Gucci decidiu anunciar a estreia de diretor criativo Demna em Milão com imagens geradas por IA e, previsivelmente, a internet reagiu como quem vê uma costura a desfazer-se à distância: ameaças de boicote, acusações de que a marca estava a tornar-se promotora de pechisbeque, indignação com perfume de nostalgia. A Gucci até fez o gesto correto para 2026: identificou as imagens como sintéticas e misturou-as com fotografia tradicional. Só que, em luxo, a transparência não substitui a mão.

O problema não é usar IA. O problema é usar IA para produzir imagens que parecem personagens de um videojogo genérico e esperar que a aura resolva. Quando a falha é visível, a tecnologia deixa de ser ferramenta e torna-se mensagem. E a mensagem, para muita gente, foi desconfortavelmente simples: se isto serve para comunicar o topo da pirâmide, então o “artesanato” era mais cenário do que substância.

Há quem defenda que é coerente com a história recente da Gucci, sempre na linha da frente do digital. Além disso, dizem, o setor inteiro está a fazer testes parecidos. É certo. Mas o luxo vive de uma disciplina: o erro custa caro, precisamente porque o preço compra obsessão. Se a marca quer que a IA tenha lugar, tem de impor-lhe o mesmo padrão que impõe a um corte, a uma pele, a um detalhe que só se nota quando não está lá. Caso contrário, a IA não “democratiza” nada; apenas denuncia onde a marca acha que pode poupar sem ser apanhada — e foi. ■

Um “piloto automático” para interfaces: o que a Standard Intelligence está realmente a vender

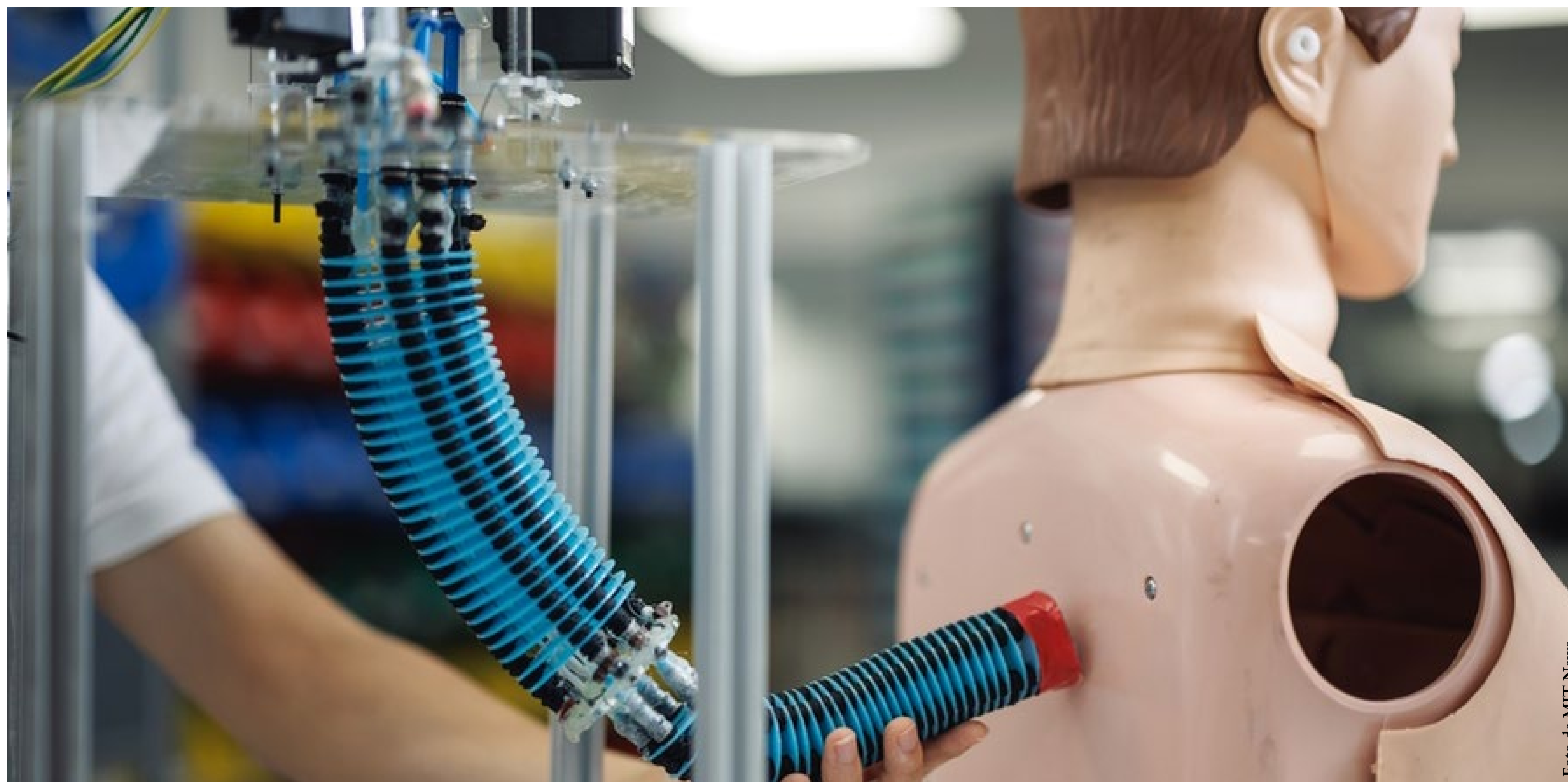


A Standard Intelligence, uma startup na área de IA, apresentou um projeto com uma ambição grande: o FDM-1 será um modelo “geral” para agir num computador. O que isto significa: não é um chatbot, nem um gestor de agentes. É um sistema que aprende a produzir *inputs* humanos — movimentos do rato, cliques, teclas — a partir do que vê no ecrã, instante a instante, como um piloto automático de interface.

A engenharia gira em torno de um problema complexo: quase ninguém tem horas de vídeo de ecrã com registo perfeito do que foi feito no teclado e no rato. A solução é treinar primeiro um modelo “ao contrário”, capaz de inferir que ação terá causado uma mudança no ecrã. Com esse modelo, rotulam automaticamente um arquivo gigantesco de vídeo. Depois, com o arquivo já “legendado”, treinam o modelo final para prever a próxima ação.

O argumento mais interessante não é a demo em Blender ou a história do “*fuzzing*”. É a aposta em contexto longo: a empresa afirma conseguir comprimir quase duas horas de vídeo num milhão de *tokens*, precisamente para evitar o comportamento típico dos agentes que só “lembram” alguns segundos e começam a inventar a partir daí. Se esta parte for sólida, muda o que se pode pedir a um modelo: em vez de ensinar tarefa a tarefa, tenta-se ensinar a mecânica de estar num computador por imitação.

A ironia é que o anúncio fala de generalidade e até acena a AGI, mas o avanço real — a confirmar-se — tem outra natureza: melhor capacidade de tratamento de dados e de processamento de “*workflows*”. Em IA, o que parece magia muitas vezes é o mais prosaico. ■



Robôs macios, cérebro estável: a lição de neurociência que a robótica precisava

A robótica dita “macia” tem uma promessa fácil de vender e difícil de cumprir: máquinas flexíveis, seguras, úteis perto do corpo humano. O problema é que, quando o corpo do robô é complacente, o controle tende a ser frágil. Uma carga inesperada, uma rajada de ar, um atuador com menor desempenho, e o movimento deixa de ser “delicado” e passa a ser “imprevisível”. O MIT e a equipa SMART/NUS propõem uma solução inspirada numa divisão clássica da neurociência: separar o que é estável do que é adaptativo. Em linguagem menos evocativa, o controlador tem uma parte treinada *offline*, que aprende um repertório base de movimentos e mantém competências consistentes, e outra parte que ajusta online para compensar pertur-

bações no mundo real. A promessa adicional é que há um mecanismo de estabilidade para impedir que a adaptação, por si só, deite tudo a perder. Nos resultados apresentados, a história é de robustez: melhor seguimento de trajetórias sob perturbações, manutenção de forma com variações de carga, tolerância a falhas, incluindo cenários em que uma fração relevante dos atuadores deixa de colaborar. A escolha do exemplo de aplicação é reveladora: um braço leve pensado para tarefas de cuidado pessoal, como ajudar alguém a lavar as costas, com a ambição implícita de aliviar cuidadores e aumentar autonomia.

A ser bem sucedido, o resultado do projeto pode ser um método de controle que aceita que o mundo muda, que o hardware falha, e que, ainda assim, o robô tem de continuar a comportar-se de forma previsível. Se este modelo de operação escalar, a robótica macia pode sair do catálogo de demonstrações e entrar num papel onde a tecnologia conta: a rotina, a assistência, a confiança. ■



IA PARA REINVENTAR O NEGÓCIO



GOVERNAÇÃO DE DADOS EM TEMPOS DE IA:

O QUE AINDA NÃO ESTÁ NA AGENDA

É hoje um facto incontestado que a maioria das organizações, qualquer que seja a respetiva dimensão, tem vindo a aumentar competências na criação de infraestruturas de dados.

HENRIQUE CARREIRO

A PARTE DIFÍCIL, contudo, tem, amiúde, ficado pelo caminho: ou retida em planos ou, pior, ausente deles. Hoje, **o obstáculo raramente é “ter dados”**. É, antes, conseguir que duas equipas diferentes usem o mesmo termo com o mesmo significado e com a mesma responsabilidade, mesmo quando o contexto muda. A empresa aprende a medir em escala, mas continua a discutir, em escala, o que está a medir.

Governança de dados começa num ponto prosaico: estabilizar significado. “Cliente ativo”, “churn”, “margem”, “receita”, “fraude” parecem substantivos; na prática, funcionam como regras de decisão. Uma alteração num evento da aplicação, uma migração de sistema ou uma campanha que mude comportamentos, e a definição deixa de apontar para a mesma realidade.

A organização, porém, mantém incentivos, metas e modelos como se nada tivesse acontecido. O desvio aparece tarde, com a forma enganadora de uma “tendência” ou de uma “mudança do mercado”, e só então alguém percebe que o problema não estava na análise — estava na semântica.

ESPAÇOS ORGANIZACIONAIS EM BRANCO

É por isso que os catálogos de dados, ainda que relevantes, por si mesmos não são a panaceia. **Um catálogo ajuda a encontrar; não ajuda a concordar. Concordância exige autoridade. Não no sentido burocrático, mas no sentido operacional: alguém tem de poder dizer “a definição é esta” e impor consequências quando a definição muda.** Sem essa autoridade, as definições



tornam-se moedas locais: válidas num produto, inválidas noutra, e inúteis quando se tenta uma consolidação.

O que muitas organizações ainda não puseram na agenda é que governação séria é, em grande parte, gestão de mudança semântica. Definições não são peças de museu: evoluem. A pergunta não é se vão mudar, mas o que acontece quando mudam. **Sem versionamento de métricas e sem um mecanismo que obrigue a declarar a quebra de comparabilidade, cada alteração técnica cria uma dívida invisível que só é cobrada meses depois, quando um executivo olha para um gráfico e tira conclusões “de negócio” a partir de um objeto que já não é o mesmo.** E, quando ninguém consegue apontar o momento em que o significado derivou, a organização substitui causalidade por narrativa.

Esta fragmentação torna-se um risco sistémico com a entrada em vigor do Regulamento Governação de Dados. Ao promover a criação de espaços comuns europeus de dados e ao exigir interoperabilidade, o Regulamento expõe uma realidade simples: quem não consegue estabilizar e versionar o significado de “cliente” dentro de portas fica, na prática, incapaz de parti-

cipar numa economia de partilha de dados sem transformar cada integração num exercício de risco e renegociação.

A seguir vem a fiabilidade, que persiste em ser tratada como um detalhe de infraestrutura. O problema é que fiabilidade não é um atributo moral; é uma propriedade mensurável, ligada ao uso. Um conjunto de dados “bom”, em abstrato, não existe. Existe adequação a uma decisão, com o risco correspondente. Algumas decisões morrem com latência; outras tornam-se perigosas com opacidade; outras exigem cuidado com a forma como o erro se distribui. A governação começa a sério quando estas exigências deixam de estar “na cabeça de alguém” e passam a existir como promessa explícita: com dono, limites e resposta quando falha.

Aqui, o ponto que continua fora da agenda é assumir que promessas exigem travões. Sem testes automáticos, as promessas são apenas intenção. A realidade é dinâmica: os *pipelines* quebram, as fontes de dados mudam, os campos passam a ser nulos, os valores duplicam, a distribuição desloca-se por razões legítimas ou por *bugs*, e um relatório continua a ser produzido com a mesma estética e a mesma confiança. **A governação que interessa cons-**



trói um sistema nervoso: deteta problemas cedo, atribui o alerta a alguém com poder para agir e, quando necessário, impede a propagação dos erros.

Em decisões críticas, a resposta correta a uma falha pode não passar por abrir mais um *ticket*; pode antes ser congelar um indicador, bloquear um consumo, retirar um modelo. Sem capacidade de travagem, “qualidade” é um adjetivo; com travagem, fiabilidade torna-se um contrato operacional. A linhagem de dados (*data lineage*) entra aqui como capacidade de reconstrução. Quando alguém pergunta por que uma métrica mudou, ou por que uma decisão foi tomada, a resposta precisa de ser reconstituível: de onde vieram os dados, que transformações sofreram, que versões existiam, que dependências foram ativadas, que modelos os consumiram. Sem noção de linhagem, a organização substitui causalidade por narrativa. E, quando o problema é grave, substitui aprendizagem por culpabilização, porque não consegue localizar o ponto de falha.

Mais uma vez, o que falta muitas vezes não é a palavra “linhagem” nos slides, mas o seu efeito prático: a capacidade de ligar uma alteração semântica a todos os consumidores relevantes, de forma verificável. Linhagem útil não serve apenas para auditoria; serve para operar mudança. Quando uma definição muda, a organização precisa de saber que relatórios deixam de ser



comparáveis, que alertas ficam cegos, que *features* mudam de significado, que modelos passam a aprender outra coisa. Sem esta cartografia viva, a empresa reage tarde e em modo artesanal, exatamente quando o custo do erro já é alto.

INTELIGÊNCIA ARTIFICIAL COMO ESPELHO CONVEXO

A IA acelera esta necessidade por um motivo simples: transforma instabilidade em escala. Um modelo aprende padrões que dependem de definições, de rotulagens e de processos que mudam sem aviso. Quando o mundo se desloca, o modelo não faz perguntas; continua a responder. E o que era pequeno torna-se sistêmico. Por isso, governação aplicada à IA exige rotinas próximas de engenharia e operação: registos e versionamento vinculativos, critérios de aprovação proporcionais ao risco, monitorização de desempenho e de deriva por segmentos relevantes, e resposta a incidentes com ações claras. “Modelo em produção” é apenas uma fotografia; o que interessa é o regime de responsabilidade enquanto ele decide.

O ponto cego, aqui, é continuar a governar “o modelo” como artefacto isolado e ignorar o produto socio-técnico que o rodeia: o que entra no

contexto, o que sai, quem valida, com que evidência, com que retenção, com que acesso. Nos modelos generativos, o perfil de risco torna-se mais traiçoeiro porque o erro pode vir com boa escrita. A alucinação plausível soa a competência, não a falha. Junta-se a isso a tentação de colocar informação sensível em instruções “só para testar” e a tendência humana para delegar validação a algo que produz texto com fluência, e o resultado é previsível: incidentes que não se resolvem com uma correção, porque nascem de limites mal definidos. Governação tem de ser explícita onde dói: que usos se permitem, o que fica sujeito a validação humana, o que nunca entra no contexto, e o que fica registado de forma reconstituível.

No fim, a maturidade das organizações revela-se na capacidade de responder sob pressão: conseguir dizer o que um dado significa, quando mudou, quão fiável é para uma decisão concreta, quem responde por ele, como se deteta degradação, e como se prova a origem e o uso quando alguém pergunta.

Quando essa capacidade existe, as ferramentas e os dashboards deixam de ser adereços e passam a ser alavancas: dados e IA entram no núcleo das decisões com confiança operacional. E é aí que a escala deixa de ser volume e passa a ser continuidade. ■



ESTRUTURAR DADOS PARA TRANSFORMAR O NEGÓCIO COM IA

A corrida à inteligência artificial expôs fragilidades em organizações que não consolidaram dados, arquitetura e governação. Sem essa base, a escala fica limitada a pilotos e iniciativas isoladas. O impacto e a maturidade tornam-se visíveis quando dados, tecnologia e responsabilidades estão integrados nos processos centrais do negócio.

INÊS GARCIA MARTINS

A ESTRATÉGIA DE DADOS é atualmente assumida como pilar central da transformação nas organizações que investem em dados e Inteligência Artificial (IA). A aceleração da IA, particularmente nas vertentes generativa e agentes autónomos, aumentou a pressão sobre as empresas para demonstrarem impacto mensurável e capacidade de execução.

A consolidação desta agenda resulta da necessidade de traduzir investimento em dados e IA em ganhos operacionais, financeiros e estratégicos.

João Anastácio, Associate Director de Data & AI da Accenture Portugal, refere que a estratégia deixa de ser conceptual quando “passa de um exercício de visão para um modelo operativo com responsabilidade clara e métricas de valor associadas”.

Hervé Silva, Partner da Deloitte, observa, no entanto, um desfasamento entre ambição e prontidão operacional, indicando que “a maioria das organizações está menos preparada do que afirma”. A maturidade percebida tende a ser

superior à maturidade real, sobretudo ao nível da infraestrutura de dados, qualidade, integração e governação.

Não está em causa apenas a tecnologia, mas a disciplina estratégica, a capacidade de execução, a governação e a transformação estrutural das organizações.

MATURIDADE DE DADOS

O discurso público sugere que a maioria das organizações já consolidou as suas fundações de



dados. No entanto, a realidade no terreno é mais heterogénea. Na visão de Rui Afeiteira, Chief Information Officer da BI4All, “raramente está tudo pronto”. Isto é, a informação existe, mas encontra-se fragmentada por sistemas, com definições inconsistentes, qualidade variável e pouca rastreabilidade.

Também na análise de João Pinto, CSO da PDMFC, “ainda existe um caminho significativo a percorrer no que diz respeito aos dados nas empresas portuguesas”, com problemas recorrentes de dispersão, inconsistência e ausência de governação clara.

A Accenture Portugal sustenta, por sua vez, que uma *data strategy* não se resolve com tecnologia nem com apresentações internas; exige responsabilidade clara, redefinição de funções e mudança real na forma como a organização trabalha.

A chegada da IA generativa e dos agentes autónomos veio expor ainda mais estas fragilidades. Como aliás destaca a Deloitte, grande parte dos



- João Anastácio -

Associate Director de Data & AI da Accenture Portugal

dados não estruturados, documentos, emails, imagens, ainda “está por trabalhar”, o que pode limitar a promessa de escala.

Já Pedro Ruivo, responsável de uma linha de vendas na SAP e professor convidado na NOVA IMS, reforça que “os projetos que não saem efetivamente do *Proof of Concept* (POC) na maioria é porque não têm dados de qualidade ou processos não integrados”. Por outro lado, o sucesso depende de ter um responsável dedicado fora do IT tradicional e de implementar casos de uso escaláveis.

“MAIS DO QUE MULTIPLICAR INICIATIVAS, O ESSENCIAL É COMBINAR FUNDAÇÕES SÓLIDAS COM EXECUÇÃO FOCADA, CRIANDO CREDIBILIDADE E CAPACIDADE DE ESCALAR DE FORMA SUSTENTÁVEL”

JOÃO ANASTÁCIO, ASSOCIATE DIRECTOR DE DATA & AI DA ACCENTURE PORTUGAL



- Hervé Silva -
Partner da Deloitte

O VERDADEIRO TESTE

A passagem de um piloto para produção constitui um indicador relevante de maturidade. De acordo com Hervé Silva, o momento decisivo ocorre quando os casos de uso são operados em produção, com uma adoção real pelas equipas e métricas claras de valor, como a produtividade, a

“

QUANDO UMA ORGANIZAÇÃO PARTE DE UM NÍVEL BAIXO DE MATURIDADE DE DADOS, O RISCO MAIOR NÃO É ‘INVESTIR POUCO’, É INVESTIR DEPRESSA DEMAIS, EM DEMASIADAS FRENTES E SEM FOCO, O QUE PODE GERAR PILOTOS DESCONEXOS, DÍVIDA TECNOLÓGICA E FRUSTRAÇÃO”

HERVÉ SILVA, PARTNER DA DELOITTE

eficiência, o crescimento ou a melhor experiência do cliente.

Nas maiores empresas a operar em Portugal, cerca de 50% dos projetos com IA regenerativa e IA embebida já estão a ser utilizados em processos de gestão, enquanto os agentes ainda representam cerca de 20%, aponta Pedro Ruivo. A evolução face ao ano anterior indica aceleração, mas também evidencia diferenças significativas de maturidade entre organizações.

A distinção mais evidente nas empresas que conseguem escalar está associada à existência de um responsável dedicado aos projetos de IA fora da função tradicional de IT e à adoção de uma metodologia de crescimento incremental aplicada a processos concretos, segundo Pedro Ruivo.

A maturidade de dados não é um ponto de chegada. Trata-se de um caminho que se inicia quando a organização deixa de falar em dados



como conceito e passa a agir através de resultados que se integram nos processos centrais das empresas.

ARQUITETURA, INTEGRAÇÃO E CAPACIDADE DE ESCALA

Escalar dados não depende de modelos sofisticados, mas da base que os sustenta. Na maioria dos casos, as organizações ficam bloqueadas neste processo, não pela criação de algoritmos, mas pela infraestrutura que precisa de funcionar todos os dias, de forma confiável e consistente.



- Rui Afeiteira -

Chief Information Officer da BI4All

“O MAIOR INVESTIMENTO TENDE A ESTAR NA FUNDAÇÃO E OPERAÇÃO DA DATA PLATFORM: INTEGRAÇÃO, QUALIDADE, SEGURANÇA, GOVERNAÇÃO, PIPELINES, OBSERVABILIDADE E DISPONIBILIDADE DOS DADOS”

RUI AFEITEIRA, CHIEF INFORMATION OFFICER DA BI4ALL

Rui Afeiteira verifica que, na maioria dos projetos, “o maior investimento tende a estar na fundação e operação da *data platform*: integração, qualidade, segurança, governação, *pipelines*, observabilidade e disponibilidade dos dados”. O desenvolvimento de modelos pode ser relativamente rápido, mas “o custo real surge quando se quer colocar em produção, escalar e manter com fiabilidade”, reforça.

Pedro Gomes Mota, Responsável de Data, Analytics & AI do Grupo Brisa, afirma que a tecnologia e a arquitetura foram assumidas como “um dos pilares fundacionais da estratégia, e não apenas como um meio para executar casos de uso isolados”. O grupo criou uma Plataforma de Dados e Inteligência desenhada para integrar Dados, *Analytics*, IA e *Governance* de forma consistente, de modo a evitar a fragmentação e soluções ad hoc. A organização sublinha que “encarar a tecnologia como plataforma e não como projeto” foi determinante para conseguir escalar.



- João Pinto -
CSO da PDMFC

“DESTAQUE PARA A “NECESSIDADE DE ENORME CAPACIDADE PROCESSAMENTO (HPC); UNIDADES DE PROCESSAMENTO GRÁFICO (GPU), BAIXA LATÊNCIA DOS AMBIENTES CLOUD, ARMAZENAMENTO, SEGURANÇA E EFICIÊNCIA ENERGÉTICA”

JOÃO PINTO, CSO DA PDMFC

Na mesma linha, a EDP refere que “a adoção prematura de tecnologias com pouca maturidade em casos com alta amplitude de impacto, pode comprometer a capacidade de a escalar mais tarde”. A consolidação de uma arquitetura de referência robusta, com padrões de integração definidos desde o início e um modelo operativo coerente, tornou-se fundamental. A criação de

Centros de Excelência e de um AI Office é prova disso ao passar a assegurar estabilização metodológica, curadoria de modelos e práticas de MLOp e *Responsible AI*.

A **dimensão infraestrutural é particularmente exigente em contexto de maior intensidade computacional**. No seguimento, João Pinto destaca a “necessidade de enorme capacidade processamento (HPC); Unidades de Processamento Gráfico (GPU), baixa latência dos ambientes cloud, armazenamento, segurança e eficiência energética”. Em determinados casos de uso estratégicos e especí-

ficos de indústria, segundo o CSO da PDMFC, a adoção de LLM dedicados implica investimento elevado, ainda que associado a um potencial retorno igualmente significativo.

No que se refere à dimensão da governação tecnológica, Rui Barata Ribeiro, Senior Data & AI Sales da IBM Portugal, acrescenta que a realidade das organizações é híbrida e multicloud, considerando que “um ‘modelo único’ é mais exceção do que regra”. A recomendação passa por **uniformizar a confiança e o governo dos modelos, independentemente da tecnologia subjacente, garan-**



tindo rastreabilidade, observabilidade e controlo contínuo.

Por esse motivo, a BI4All sintetiza aquele que é um dos princípios operacionais mais fundamentais que é tratar “desde início o que normalmente só aparece mais tarde: produção, operação e controlo”.

GOVERNAÇÃO DA IA

A aceleração da adoção de inteligência artificial trouxe a governação para o centro da agenda executiva. A questão deixou de estar confinada a compliance e passou a integrar a discussão sobre risco operacional, reputacional e estratégico. A governação deixou de ser um mecanismo de controlo posterior e passou a integrar o ciclo de vida dos modelos desde a conceção. A responsabilidade é partilhada entre negócio, tecnologia e funções de risco, com níveis de supervisão ajustados ao impacto potencial de cada caso de uso.

“

OS PROJETOS QUE NÃO SAEM EFETIVAMENTE DO POC, NA MAIORIA DAS VEZES, É PORQUE NÃO TÊM DADOS DE QUALIDADE OU PROCESSOS NÃO INTEGRADOS”

PEDRO RUIVO, RESPONSÁVEL NA SAP E PROFESSOR CONVIDADO NA NOVA IMS



- Pedro Ruivo -

Responsável na SAP e professor convidado na NOVA IMS

A governação da IA “ganhou prioridade com o aumento do escrutínio regulatório, especialmente com o AI Act na União Europeia”, aponta João Anastácio. As organizações estão a evoluir para modelos formais e transversais, onde a responsabilidade não é exclusivamente tecnológica. O negócio gere a utilização e os resultados, a tecnologia e os dados garantem robustez e monitori-



zação, e as áreas de risco e jurídico asseguram conformidade e enquadramento ético.

Hervé Silva identifica um desfasamento entre o ritmo da tecnologia e o ritmo do controlo organizacional, referindo que “a IA avança mais rápido do que os mecanismos de controlo”. A maturidade em *governance* continua desigual, sobretudo quando entram em jogo agentes autónomos e modelos mais avançados.

Na prática, começa a surgir um modelo federado. Segundo Hervé Silva, órgãos executivos definem as diretrizes e os limites de risco, equipas de governação de IA supervisionam os modelos, e equipas técnicas garantem a monitorização constante e a resolução de problemas. A governação deixa de ser um silo e passa a estar distribuída pelas equipas, devendo ser “*embedded across teams*”. Rita Calvão, sócia associada da McKinsey & Company em Portugal, reforça que organizações bem-sucedidas criam “uma *governance*

executiva e multidisciplinar, orientada a valor de negócio, com o risco, o *compliance* e a parte legal a desafiar o desenho e a operação antes e depois da entrada em produção”. O controlo deve ser proporcional ao risco, com critérios definidos à partida e intensidade de supervisão ajustada ao caso de uso.

A operacionalização desta *governance* é também descrita sob o ponto de vista tecnológico, com Rui Barata Ribeiro a destacar mecanismos de rastreabilidade granular, explicabilidade integrada e monitorização contínua que permitem acionar alertas ou bloquear automaticamente modelos quando violam limiares definidos. A plataforma permite capturar “*datasets* utilizados, versões de código, hiperparâmetros, *pipelines* de treino, responsáveis e alterações” ao longo do ciclo de vida do modelo.

Rui Afeiteira sublinha a importância de integrar governação e agilidade, onde o equilíbrio



se encontra quando a governação é desenhada “como acelerador e não como burocracia”. A prática passa por modelos de *guardrails* com *self-service*, catálogos vivos ligados a decisões reais, controlo de acessos baseado em políticas e auditoria integrada em práticas de MLOp e LLMOp. Do lado das empresas utilizadoras, como a Brisa, Pedro Gomes Mota descreve a *governance*, segurança e ética como princípios “não negociáveis” e definidos *by design*. A organização distingue ambientes de experimentação de ambientes produtivos, sendo que a escala só ocorre quando os *guardrails* estão plenamente assegurados.

Na EDP, a criação de políticas claras de *Responsible AI*, alinhadas com o enquadramento regulatório aplicável, permitiu avançar “com agilidade sem comprometer rigor”. A existência de mecanismos de controlo integrados na política de *Responsible AI* garante conformidade com os pacotes regulatórios nos diferentes países onde opera.



- Pedro Gomes Mota -

Responsável de Data, Analytics & AI do Grupo Brisa

CASOS DE VALOR

Eficiência, produtividade e redução de riscos começam a traduzir-se em números reais, e em muitos casos já impactam diretamente as contas. Tal como reflete Pedro Gomes Mota, “desde 2024, os dados passaram a ser encarados pelo Grupo Brisa como um ativo estratégico e um verdadeiro gerador de valor”. A organização liga cada iniciativa de dados e IA a métricas estratégicas como rentabilidade, eficiência operacional, experiência de cliente ou mitigação de risco.

“ OS DADOS PASSARAM A SER ENCARADOS COMO UM ATIVO ESTRATÉGICO E UM VERDADEIRO GERADOR DE VALOR ”

PEDRO GOMES MOTA, RESPONSÁVEL DE DATA, ANALYTICS & AI DO GRUPO BRISA



- Rui Barata Ribeiro -

Senior Data & AI Sales da IBM Portugal

Os ganhos mais expressivos têm surgido no domínio da eficiência operacional, com melhorias em processos críticos. Na experiência de cliente, o Parking Buddy – modelo de previsão de estacionamento integrado na aplicação Via Verde – contribui para uma utilização mais previsível e conveniente dos serviços. Na vertente de mitigação de risco, algoritmos de deteção de incidentes suportam o Centro de Coordenação Operacional, com impacto direto na segurança rodoviária.

“O RETORNO MAIS IMEDIATO SITUA-SE EM “AUTOMAÇÃO DE TAREFAS INTENSIVAS EM INFORMAÇÃO, AUMENTO DA PRODUTIVIDADE ATRAVÉS DE AGENTES NO DESENVOLVIMENTO E OPERAÇÕES, E MODERNIZAÇÃO DOS SERVIÇOS AO CLIENTE”

RUI BARATA RIBEIRO, SENIOR DATA & AI SALES DA IBM PORTUGAL

Paralelamente, a EDP revela que “**todos os projetos de dados e inteligência artificial avançam apenas quando existe um *business case* mensurável e validado**”. A organização destaca ganhos operacionais e de produtividade, mas também refere **desafios** associados à rápida evolução tecnológica e à escassez de talento especializado. crescimento dos custos de cloud levou ao reforço de práticas de FinOps e iniciativas estruturadas como CloudHealth e programas de *Data Efficiency*, que permitiram “reduções expressivas de TOTEX e

uma gestão muito mais rigorosa do consumo”. No terreno da automação e produtividade, a BI4All identifica ganhos rápidos em suporte e atendimento, *backoffice* e operações, manutenção e analítica assistida. O Chief Information Officer da empresa vê na redução do tempo médio de atendimento, no aumento da resolução à primeira e na melhoria na consistência do serviço, exemplos recorrentes disso. **A integração da IA no fluxo de trabalho é ainda apontada como condição para que os ganhos sejam sustentáveis.**



A IBM observa que os casos com retorno mais imediato situam-se em “automação de tarefas intensivas em informação (como sumarização, pesquisa semântica ou extração documental), aumento da produtividade através de agentes no desenvolvimento e operações, e modernização dos serviços ao cliente”. De acordo com Rui Barata Ribeiro, estes casos combinam elevado volume transacional com impacto direto em eficiência e tempo.

A leitura e classificação de documentos manuscritos atingiu “uma taxa de sucesso superior a 90%”, revela João Pinto. Existem ainda casos de uso em manutenção, investigação e fraude, transcrição e tradução de áudio e vídeo em tempo real, cibersegurança e observabilidade.

Do ponto de vista financeiro, a sócia associada da McKinsey & Company em Portugal refere que “cerca de 35-40% das organizações com que trabalhamos já reportam algum impacto em EBITDA”, embora a maioria ainda não tenha

conseguido capturar esse impacto à escala. O valor está concentrado em automatização de trabalho recorrente, redução de fricção operacional e melhoria da qualidade das decisões.

Pedro Ruivo acrescenta que, excluindo os custos de limpeza e harmonização de dados, “o retorno é rápido (inferior a um trimestre assim que tenha sido implementada)”, desde que o processo de gestão esteja digitalizado e já seja medido. A fragmentação de sistemas e semânticas de dados distintas tende a comprometer os resultados.

Apesar destes avanços, a Deloitte alerta para iniciativas com “acesso sem adoção real”, onde ferramentas são disponibilizadas, mas não integradas nos fluxos de trabalho. Casos como este, onde os projetos são genéricos, replicáveis e desligados dos dados próprios da organização, acabam por gerar frustração e pouco retorno.

O padrão observado mostra que os ganhos mais consistentes surgem onde existe volume, repetição e métricas claras de desempenho. A integração nos





“

ORGANIZAÇÕES BEM-SUCEDIDAS CRIAM “UMA GOVERNANCE EXECUTIVA E MULTIDISCIPLINAR, ORIENTADA A VALOR DE NEGÓCIO, COM O RISK, O COMPLIANCE E A PARTE LEGAL A DESAFIAR O DESENHO E A OPERAÇÃO ANTES E DEPOIS DA ENTRADA EM PRODUÇÃO”

RITA CALVÃO,
SÓCIA ASSOCIADA DA MCKINSEY & COMPANY EM PORTUGAL



- Rita Calvão -

Sócia associada da McKinsey & Company em Portugal

processos *core* e a medição sistemática de impacto continuam a ser determinantes para converter experimentação em valor financeiro sustentável.

ONDE OS PROJETOS FALHAM

Apesar dos ganhos já mensuráveis, persistem entraves estruturais que atrasam, encarecem ou

inviabilizam projetos, sendo as expectativas irreais um dos riscos mais recorrentes. Fonte oficial da EDP reconhece que, em alguns casos, a IA não entregou o esperado e refere que “na maioria das situações, a causa esteve menos na tecnologia e mais nas expectativas irreais criadas pelo ‘buzz’ em torno da IA”. Noutros casos, a rápida evolução tecnológica tornou inviável a continuidade de abordagens iniciais, o que criou “atrasos e necessidades de recomeçar”.

Na Brisa, a principal causa de insucesso não esteve na tecnologia, mas em “necessidades de negócio mal formuladas, dados insuficientes ou expectativas desalinhadas”, revela Pedro Gomes Mota. A organização adotou uma abordagem de experimentação rápida e de baixo custo, avaliando os casos de uso numa ótica de incubação antes da escala.

“Dados, processos e pessoas”, são, para Pedro Ruivo, os três bloqueios recorrentes nos projetos



que não escalam. Com exceção de algumas empresas, os dados surgem como o primeiro obstáculo, frequentemente dispersos, redundantes ou inacessíveis. O segundo bloqueio está nos processos de gestão configurados com base em customizações antigas e tecnologias não compatíveis com sistemas de IA.

Segundo João Pinto, a qualidade dos dados exige frequentemente “um trabalho intensivo de limpeza e padronização antes de qualquer análise”. Integrações com sistemas *legacy* fechados, definição pobre do caso de uso e falta de alinhamento estratégico com os objetivos de negócio surgem igualmente como causas de atraso.

Rui Afeiteira acrescenta que projetos se tornam mais complexos quando “o valor e os objetivos são pouco claros” ou quando “a produção e risco são tratados tarde”. Requisitos de segurança, privacidade e integração operacional que surgem

apenas no final obrigam a retrabalho significativo, segundo o Chief Information Officer da BI4All. O partner da Deloitte identifica um padrão claro nas iniciativas que não geram retorno. O mais recorrente é “acesso sem adoção real”. As ferramentas existem, mas não entram nos fluxos de trabalho nem têm métricas que obriguem a medir utilização e impacto. Outro entrave recorrente é a falta de governação estruturada. Sem responsáveis claros, critérios de sucesso definidos ou um modelo operativo consistente, as iniciativas perdem tração e acabam por ficar aquém do retorno esperado.

Neste quadro, a IBM reconhece que “a grande maioria das dificuldades associadas a governação de IA não são tecnológicas”. Rui Barata Ribeiro aponta para os desafios na qualidade dos dados, na evolução regulatória e na governação de agentes autónomos como os mais evidentes. Acrescenta

ainda a importância do *vendor risk management* e da análise da transparência dos modelos fundacionais utilizados.

O PRÓXIMO PASSO

É certo que “a IA tem potencial para transformar o *core* das organizações, nomeadamente através das arquiteturas de agentes de IA – baseadas em agentes autónomos capazes de tomar decisões e orquestrar ações entre múltiplas funções e aplicações”, no entanto, segundo a Accenture Portugal, “na maioria dos casos, essa reinvenção não deverá ocorrer no curto prazo”. O ritmo e a profundidade dessa transformação, contudo, variam consoante a maturidade das fundações e a disciplina de execução. Há um padrão transversal que indica que a transformação estrutural não ocorre por substituição do *core* ou pela rutura total do mesmo.



Esta transformação passa pela integração progressiva da IA nos processos críticos, com reforço de governação, clarificação de responsabilidades e disciplina financeira. Como a velocidade de adoção é elevada, a capacidade de reorganização interna continua a ser o fator determinante para que essa adoção se traduza em vantagem competitiva sustentável.

Para organizações que estão a dar os primeiros passos e ainda não têm maturidade de dados, a prioridade no primeiro ano passa por “construir as fundações”. O Associate Director de Data & AI na Accenture Portugal, salienta que “mais do que multiplicar iniciativas, o essencial é combinar fundações sólidas com execução focada, criando credibilidade e capacidade de escalar de forma sustentável”. Em paralelo, recomenda definir uma estratégia clara, estabelecer um modelo de governação de dados e IA eficaz, garantir uma base tecnológica coerente e implementar um número

limitado de casos de uso com valor evidente e alinhados ao negócio para demonstrar impacto e criar tração interna.

Hélver Silva reforça que “quando uma organização parte de um nível baixo de maturidade de dados, o risco maior não é ‘investir pouco’, é investir depressa demais, em demasiadas frentes e sem foco, o que pode gerar pilotos desconexos, dívida tecnológica e frustração”. O primeiro ano, segundo o partner da Deloitte, “deve ser encarado como ano de fundações inteligentes, onde a meta não é ‘fazer tudo’, mas sim criar condições para escalar valor nos anos seguintes: foco, disciplina, governação e um *backbone* de dados/tecnologia que seja adaptativo, modular e preparado para IA”.

“Fechar o *gap* entre acesso e adoção, escolher dois ou três casos de uso com *business case* evidente; criar uma visão clara e um North Star para IA alinhado à estratégia; construir as fundações

mínimas de dados e tecnologia; implementar governança desde o dia zero; preparar pessoas e redesenhar trabalho; escolher entre incrementalismo disciplinado ou transformação radical”, prioriza o responsável.

Rita Calvão alerta para o risco de decisões estruturais irreversíveis e defende que “o mais eficaz é experimentar e provar valor rapidamente, em ambientes mais pequenos e controláveis, e construir as fundações à medida que se escala”. Para isso, sublinha, é essencial priorizar os casos de uso com maior retorno, garantir dados “*fit for purpose*”, capacidade de desenvolvimento, talento de *change management* e ferramentas de medição de impacto. Ao longo do percurso, acrescenta, é igualmente importante consolidar um modelo operacional leve, com equipas, processos e governação capazes de gerir o *backlog* com cadência, responsabilização e foco em resultados. ■

NOESIS

POR LUIS GONÇALVES,
Data Analytics & AI Director, Noesis

COMO ALINHAR ESTRATÉGIA DE DADOS E GOVERNANCE DE IA AO NEGÓCIO

Falamos muito de dados, Inteligência Artificial, investimento e inovação. No entanto, muitas organizações continuam a levantar a mesma questão: como usar os dados para tomar decisões que façam realmente a diferença no negócio?

RARAMENTE FALTA TECNOLOGIA. As empresas investem em plataformas modernas, soluções de analytics e modelos de IA cada vez mais sofisticados, sem que essa aposta se traduza numa vantagem competitiva clara. A razão é simples: os dados, por si só, não criam valor. É a informação que deles extraímos e as decisões que daí resultam que o fazem.

Os desafios surgem, muitas vezes, a montante da tecnologia. Surgem quando não existe clareza sobre que decisões precisam de ser melhoradas, sobre os processos internos a otimizar, sobre as métricas

verdadeiramente relevantes para o negócio, sobre as fontes de dados e como estes estão estruturados, ou sobre o impacto que se pretende alcançar. Sem essa estratégia base, os dados acumulam-se, mas não geram verdadeiro valor.

É aqui que a estratégia de dados deve adquirir outro significado. **Uma estratégia de Data Governance não pode ser apenas um plano tecnológico.** Deve estar ancorada na estratégia de negócio e responder, de forma clara, às suas prioridades. Se a organização pretende reforçar a experiência do cliente, os dados devem permitir compreender comporta-



- Luis Gonçalves -
Data Analytics & AI Director, Noesis

mentos, antecipar necessidades e medir impacto. Se o objetivo é aumentar a eficiência operacional, a estrutura de dados deve oferecer visibilidade, consistência e capacidade de otimização.

Quando esta ligação não existe, cada área define os seus próprios indicadores e interpreta a realidade a partir de perspetivas distintas. O resultado não é apenas falta de alinhamento, mas sim, “fricção” organizacional. As decisões tornam-se mais lentas, menos consistentes e, por vezes, contraditórias.

É precisamente aqui que a governance de dados deixa de ser um conceito abstrato e passa a ser um elemento estruturante. Durante anos foi vista como sinónimo de controlo excessivo ou de burocracia, mas, na prática, uma governance bem definida faz exatamente o contrário. Ao clarificar responsabilidades, definir regras comuns e estabelecer critérios de qualidade, reduz dúvidas e acelera a tomada de decisões.

Perceber como estruturá-la na prática é o passo seguinte.

A primeira mudança é estrutural. **A estratégia de governance de dados não pode ser delegada**

apenas à área tecnológica. Deve envolver as áreas de negócio na definição de ownership, métricas críticas e regras de qualidade.

Já a governance de IA introduz uma camada adicional de responsabilidade. A utilização de sistemas de IA exige supervisão ao mais alto nível da organização, envolvendo liderança executiva, áreas legais e de risco, e garantindo que o uso de algoritmos está alinhado com princípios éticos, regulatórios e de transparência.

O enquadramento europeu, reforçado pelo EU AI Act, deixa claro que a utilização de sistemas de IA exige responsabilidade ao mais alto nível. Isto implica classificar sistemas por nível de risco, garantir documentação técnica adequada, supervisão humana e mecanismos de auditoria contínua. Transparência, rastreabilidade, avaliação de risco e supervisão humana deixam de ser recomendações e passam a ser requisitos concretos.

Outra recomendação fundamental é integrar a Data Governance, de IA e dos modelos, no ciclo de vida dos projetos. Muitas organizações criam políticas robustas, mas aplicam-nas demasiado tarde. **Uma governance de dados eficaz começa**

na arquitetura da solução: estabelecendo critérios claros de qualidade de dados, incorporando mecanismos de validação contínua, garantindo documentação consistente e prevendo revisões periódicas. Quando incorporada desde o início, torna-se parte integrante e natural da execução. Há também uma dimensão cultural que não pode ser ignorada. Decidir com base em dados exige literacia analítica, e também organizacional. Não basta disponibilizar informação, é preciso garantir que as equipas compreendem o que estão a analisar, conhecem as limitações dos modelos e mantêm espírito crítico perante resultados automatizados.

No fundo, uma Data Governance eficaz pressupõe clareza estratégica, matrizes de responsabilidade definidas e controlo proporcional ao risco. Apenas quando estes elementos estão devidamente alinhados, é possível inovar com ambição e sem comprometer confiança.

Na era da IA, não se trata apenas de adotar tecnologia, é necessário garantir que os dados que sustentam cada decisão são fiáveis, éticos e sustentáveis. ■



ADOÇÃO SEGURA DE IA: TRANSFORMAR RISCO EM VANTAGEM COMPETITIVA

A inteligência artificial generativa (GenAI), um dos tipos de IA, está a transformar as operações, gestão e até inovação nas organizações. Da automatização de tarefas à elaboração de estudos complexos, incluindo a criação de conteúdos de texto, imagem e vídeo, o impacto na economia e na sociedade é irrefutável.

AS ORGANIZAÇÕES permitem a adoção de IA e de GenAI por ser central no sucesso, mesmo que criando mais ativos e superfícies de ataque (aplicações, modelos e agentes autónomos) que exigem segurança específica de IA que, por sua vez, evolui mais rapidamente do que qualquer equipa de cibersegurança consegue acompanhar. E a transformação não é opcional, é existencial.

PLATAFORMA ESTRATÉGICA INTEGRADA

A Check Point, líder mundial de cibersegurança preconiza nesta “Era da IA” uma nova e disruptiva abordagem sem mais ferramentas de segurança, nem complexidade na sua gestão e operação, no exato momento em que é exigida clareza, eficiência e redução mensurável de riscos.



A visão defendida, e acompanhada pela SECURNET, assenta em quatro pilares estratégicos:

- **Segurança da rede híbrida** - distribuída por centros de dados, nuvem híbrida, Internet, filiais e SASE, alimentada e com aplicação consistente de IA, com foco e prioridade na prevenção.
- **Segurança da área de trabalho** - composto por dispositivos, navegadores, correio eletrónico, aplicações SaaS e acessos remotos protegidos, onde humanos interagem cada vez mais com IA.
- **Gestão da exposição** - dando visibilidade total das superfícies, priorizando riscos reais com contexto e transformando a gestão reativa das vulnerabilidades em redução contínua de riscos baseada em inteligência.
- **Segurança de IA** - protegendo a stack completa de IA, alimentada por dados, infraestrutura e utilizada por colaboradores, aplicações empresariais, agentes autónomos e modelos.

A estratégia, onde pontuam produtos e tecnologias como o **Check Point GenAI Protect**, **ThreatCloud AI**, **Infinity AI Copilot** e **AI Cloud Protect**, entre

muitos outros em fase de entrada no portefólio, assenta numa plataforma de integração com um amplo ecossistema de tecnologias - “Open Garden” - que reflete a própria visão e operação das empresas mais modernizadas. A abordagem, que prioriza a prevenção e inova com IA, implementa um plano de controlo unificado, potencia a adoção segura de IA em escala e impulsiona a produtividade.

VISIBILIDADE E CONTROLO NUMA ERA CONVERSACIONAL

A “adoção invisível” de GenAI com a utilização de ferramentas sem qualquer tipo de supervisão, expõe perigosamente dados sensíveis. Enquanto cresce a utilização de GenAI impulsionando valor de forma exponencial, torna-se imperativa uma estratégia de **governança de GenAI**, materializada em soluções como a **Check Point GenAI Protect**, que, ao contrário das soluções tradicionais, combina **visibilidade contextual, classificação avançada de dados e prevenção de perda em tempo real**, compreendendo a lógica conversacional dos prompts generativos e proporcionando benefícios como:

- **descoberta de aplicações GenAI**, destrinchando as geridas e autorizadas;
- **avaliação de risco por aplicação e sessão**, com métricas que permitem priorizar políticas e investimentos com base no uso real;



- **prevenção de perda de dados em tempo real**, que analisa a informação impulsionada por IA, identificando conteúdo de baixo e alto risco e protegendo dados sensíveis;
- **conformidade regulatória e rastreabilidade**, com relatórios detalhados e alinhados com as principais normas e diretivas europeias que apoiam processos de auditoria e resposta a incidentes.

TRANSFORMAR A GOVERNAÇÃO DE IA EM ESTRATÉGIA CORPORATIVA

Este nível de governação transforma experimentação em vantagem estratégica para organizações que estejam a testar informalmente GenAI, assegurando adoção segura, acelerada e em larga escala, equilibrando inovação e produtividade com a previsibilidade e controlo.

O futuro da governação de GenAI está na seleção e adoção de soluções que compreendam não apenas “o que” as pessoas usam, mas “como e porquê” o fazem.

As organizações que expandem e generalizam o uso de GenAI, integrando segurança contextual, visibilidade e conformidade em todos os níveis, estarão a melhor se posicionar para colher os benefícios desta **revolução tecnológica**. Com **confiança e resiliência**.

A SECURNET é Elite Partner da Check Point - o mais elevado nível de parceria e reconhecimento no ecossistema, para além de um dos mais antigos parceiros em atividade em Portugal, propondo-se **ajudar a proteger, sem comprometer a revolução IA** impulsionando a **vantagem competitiva!**

Contate-nos em: info@securnet.pt ou comercial@securnet.pt ■



“A NIS2 NÃO SERÁ JULGADA COMO UM PROJETO DE COMPLIANCE, MAS SIM QUANDO SURGIR O PRIMEIRO INCIDENTE”

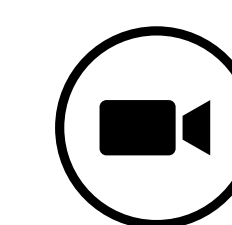
No keynote de abertura de mais uma edição da IT Insight TALKS, Henrique Carreiro, Diretor da IT Insight, alertou para o verdadeiro teste para as organizações com a entrada em vigor da NIS2 – a capacidade de decidir sob pressão, com informação incompleta e nas primeiras horas de um incidente.

MARTA QUARESMA FERREIRA

A POUCO MAIS DE UM MÊS da entrada em vigor da Diretiva NIS2 em Portugal, Henrique Carreiro considera que ainda “tendemos a ver a NIS2 em termos de métricas, *scorecards*, prazos e *compliance*”.

No âmbito da primeira edição de 2026 da IT Insight TALKS, dedicada a cibersegurança, o diretor da IT Insight começou por recorrer aos dados da ENISA, referentes aos gastos IT por Estado-Membro na União Europeia, para contextualizar a posição de Portugal, que regista um valor mediano de gastos na ordem dos 37 milhões de euros.

No entanto, o cenário muda quando o tema é segurança da informação, revelando uma assimetria preocupante face a outros Estados-Membros: o investimento das



PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM



“AS PRIMEIRAS DUAS HORAS [DE UM INCIDENTE] VÃO DETERMINAR TUDO O RESTO”

empresas portuguesas nesta área é, em média, de 1,9 milhões de euros, um valor que contrasta, por exemplo, com os 5,5 milhões de euros apresentados pela vizinha Espanha. “É evidente que o risco não escolhe o país; o risco vai escolher a parte mais fraca”, garantiu.

ARRUMAR A “CASA”, MESMO COM INFORMAÇÃO INCOMPLETA E CONTRARRELÓGIO

Na perspetiva do Diretor da IT Insight, a “NIS2 não será julgada como um projeto de compliance, mas sim quando surgir o primeiro incidente”, sendo este o verdadeiro teste à perceção e ação para limitar os danos. A deteção tardia, aliada a decisões lentas, pode culminar no prolongamento de uma crise no caso de um incidente aparentemente “normal”.

Outro dos pontos enaltecidos durante a apresentação prende-se com a necessidade que muitas organizações têm de ter a informação completa perante uma situação de incidente. Para o Diretor, é essencial “construir a capacidade antes de surgir [um incidente], para podermos decidir com a informação incompleta”.

A NIS2 vem, assim, eliminar o possível “terreno intermédio” disponibilizado às equipas, obrigando as mesmas a tomarem “uma decisão defensável”, num caminho que vai levar ao “redesenho de processos”. No fim, tudo se resume “às capacidades que as organizações têm para decidir sob pressão, com informação incompleta”, reitera Henrique Carreiro.

O tempo é outra das variáveis a acrescentar a esta equação. “As primeiras duas horas [de um incidente] vão determinar tudo o resto”, afirmou, defendendo a ideia de que o prazo da comunicação altera a forma como a resposta a incidentes deve ser concebida e não documentada. O plano de ação passa por uma classificação inicial rápida para garantir que a primeira parte de uma crise de segurança não assenta apenas num processo dependente de reuniões de consenso sobre como atuar, mas sim em ações concretas. No fundo, o plano não precisa de ser perfeito; necessita apenas de suficiente evidência para atuar de forma responsável, nomeadamente saber qual o serviço crítico que está em risco, saber o que está comprovado, quem pode classificar a gravidade e reportar e o que fazer para reduzir os danos.

CONSTRUIR BASES SÓLIDAS

No que diz respeito aos investimentos em segurança, os números reportados pela ENISA não deixam grande margem para dúvidas: “Portugal é o elo mais fraco e temos de pensar nessa perspetiva – se queremos ser o elo mais fraco nesta cadeia”, lembrou Henrique Carreiro. Neste caso, e com as operações em Portugal, ainda dependentes de fornecedores globais e partilhados, **é crucial repensar nas dependências que podem parar os serviços e nos planos de operação para estas eventualidades.**

“Parece que temos uma lista imensa de *to do's*, mas acho que se pode começar simples: vamos identificar um processo e torná-lo defensável”, aponta o Diretor da IT Insight.

A proposta não passa, por isso, por extensas listas de procedimentos, mas antes por um processo crítico, defensável, testado, treinado, a partir do qual seja possível escalar.

Perante a exigência do contexto regulatório, Henrique Carreiro recordou a Lei de Goodhart – em que uma medida que se torna num objetivo, deixa de ser uma boa medida – para chamar a atenção para o risco de se transformar a conformidade num fim em si mesmo.



“Os *scorecards* podem ser desenhados, cumpridos, as métricas podem estar todas lá, mas o resultado não é aquilo que se espera. Portanto, vamos fazer o contrário: **vamos procurar resultados e, a partir daí, ter um *scorecard* que mereça a pena, sem estar a desperdiçar esforços naquilo que não vale a pena**”, conclui. ■

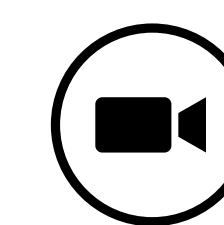
ABRIL TRAZ NIS 2 E A “URGÊNCIA DAS ORGANIZAÇÕES COMEÇAREM A PREPARAR-SE”

Faltam menos de dois meses para a entrada em vigor da NIS 2 e, no setor empresarial português, a cibersegurança entrou numa fase de pré-cumprimento em que a margem para adiar decisões se tornou residual. Na IT Insight TALKS dedicada à cibersegurança, Margarida Leitão Nogueira, Partner na DLA Piper, sublinhou que esta proximidade pode transforma o tema num problema de gestão.

INÊS GARCIA MARTINS

NO ANO em que a diretiva NIS 2 entra em vigor em Portugal, a discussão deixou de se centrar apenas na resiliência digital e passou a focar-se no cumprimento de obrigações concretas. O Decreto-Lei n.º 125/2025, que transpõe a diretiva para o ordenamento jurídico nacional, “foi publicado no dia 4 de dezembro de 2025 e entrará em vigor no dia 3 de abril de 2026”, recordou Margarida Leitão Nogueira, Partner na DLA Piper, na primeira edição de 2026 da IT Insight TALKS dedicada à cibersegurança.

A cronologia, contudo, inclui um elemento relevante, já que “**existe ainda um conjunto de normas regulamentares que deverão ser aprovadas pelo Centro Nacional de Cibersegurança**”. De seguida, inicia-se “um período de 24 meses



PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM



para que determinadas normas deste diploma produzam efeitos”. A partner sublinhou ainda que devido à aprovação destas normas materiais, “as organizações têm aqui um período de tempo para se prepararem”.

Apesar desse período, o enquadramento traz mudanças estruturais. A diretiva e o novo diploma “trazem algumas diferenças significativas quando comparado com o anterior regime”, desde logo “um alargamento significativo dos setores abrangidos e, conseqüentemente, das entidades abrangidas”, bem como “uma maior exigência ao nível das medidas de gestão de riscos e de notificação de incidentes”.

ÂMBITO E CLASSIFICAÇÃO

A primeira questão prática para as organizações é determinar se estão ou não abrangidas. “Este regime jurídico classifica as entidades como entidades essenciais, entidades importantes e entidades públicas relevantes”, explicou. Este enquadramento não se limita à dimensão das empresas, já que existem entidades que, “independentemente da sua dimensão, também são consideradas essenciais”. Além disso, “se uma organização se qualificar em mais do que uma deve escolher-se aquele que é mais exigente do ponto de vista das exigências”.

A regra geral é apenas o ponto de partida, até porque, como foi sublinhado, “existe um conjunto de exceções” e pode suceder que “a resposta a algumas

destas questões pode ser negativa e ainda assim, por via das exceções, a entidade estar abrangida”.

Isto é, mesmo quando uma organização conclui que não está abrangida, a análise pode não terminar aí. Caso preste serviços ou forneça produtos a uma entidade regulada, “pode ter de cumprir obrigações” ao nível da cadeia de abastecimento. As entidades abrangidas “devem avaliar as vulnerabilidades destes prestadores de serviços e destes fornecedores” e “devem avaliar a qualidade global dos produtos do ponto de vista da cibersegurança.”

MEDIDAS E NOTIFICAÇÕES DE INCIDENTES

No capítulo das medidas, o novo regime representa uma mudança de patamar. As medidas de gestão de riscos “são mais exigentes do que eram no passado” e devem assentar numa “abordagem sistémica”. Essas medidas, segundo a responsável, “devem incidir sobre um conjunto muito variado de áreas, nomeadamente o tratamento de incidentes, tratamento de vulnerabilidades, práticas de ciberhigiene”.

É neste sentido que o reporte de incidentes assume particular relevância no novo regime. Perante um incidente significativo, “a notificação inicial deve ser feita no prazo de 24 horas após determinação que o incidente é significativo”.

Um incidente significativo é descrito como “um incidente suscetível de causar graves danos operacionais à entidade e ou danos financeiros ou que seja



suscetível de causar ou de afetar terceiras entidades, causando-lhes danos materiais ou imateriais”.

Após a notificação inicial, há uma notificação de fim de impacto e um relatório final, podendo ainda ser exigido relatório intercalar caso o incidente se mantenha em curso.

Ao nível da supervisão, a diferença entre categorias de entidades é clara.

No caso das entidades essenciais, existe supervisão *ex ante* e *ex post*, o que significa sujeição a medidas “independentemente de existirem indícios, provas ou informações de incumprimento”. Já as entidades importantes estão sujeitas a supervisão *ex post*, exigindo que exista informação, provas ou indícios de incumprimento.

REGIME SANCIONATÓRIO

O impacto potencial das sanções coloca o tema no centro da gestão. O regime pode resultar na aplicação de “coimas avultadas” e, no caso de uma entidade essencial que pratique uma contraordenação muito grave, “as coimas podem ascender aos dez milhões de euros de euros ou a até ou 2% do volume de negócios anual global”.

O regime vai mais longe ao prever que os órgãos de direção, gestão e administração “podem ser responsabilizados pelas infrações e podem ser responsabilizados por ação ou por omissão”, o que desloca o tema da cibersegurança para o centro da governação.

A estes órgãos são atribuídos deveres concretos, nomeadamente que “devem aprovar as medidas de gestão de riscos, supervisionar a sua implementação” e que “devem ainda com uma periodicidade regular, realizar ações de formação em matéria de ciber cibersegurança”.

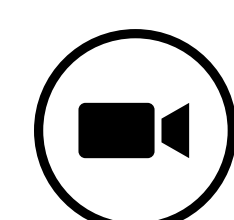
Margarida Leitão Nogueira sublinhou “a urgência das organizações começarem a preparar-se” e a necessidade de “começarem a olhar para aquilo que é o âmbito de aplicação do diploma para determinar se estão direta ou indiretamente abrangidas e assim poderem preparar-se para o cumprimento destas obrigações”. ■

ENTRE A EXIGÊNCIA E A MATURIDADE NA ERA DA NIS2

Na primeira edição de 2026 da IT Insight TALKS dedicada à cibersegurança, a CyberSafe, a Logicalis, a ManageEngine, a Securnet, a Symantec e a VisionWare subiram ao paco para discutir o impacto da NIS2 nas organizações. Custos, coimas, falta de talento, cloud, IA, cadeia de abastecimento e responsabilidade dos órgãos de gestão marcaram um debate sobre governação, risco e maturidade num novo ciclo de exigência regulatória.

INÊS GARCIA MARTINS

NA PRIMEIRA EDIÇÃO de 2026 da IT Insight TALKS dedicada à cibersegurança, a CyberSafe, a Logicalis, a ManageEngine, a Securnet, a Symantec e a VisionWare subiram ao paco para discutir o impacto da NIS 2 nas organizações. Custos, coimas, falta de talento, cloud, IA, cadeia de abastecimento e responsabilidade dos órgãos de gestão marcaram um debate sobre governação, risco e maturidade num novo ciclo de exigência regulatória.



PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM



A NIS2 TRAZ PENALIZAÇÕES SIGNIFICATIVAS, MAS IMPLEMENTAR CONFORMIDADE TEM CUSTOS. COMO EQUILIBRAM O ARGUMENTO 'ISTO É CARO' COM O RISCO REAL DE COIMAS, INCIDENTES E DANOS REPUTACIONAIS? QUE ABORDAGENS PRÁTICAS RECOMENDAM PARA COMEÇAR COM ORÇAMENTOS LIMITADOS?

Artur Martins, CISO & Cybersecurity Strategy Executive Advisor, Logicalis: “A *compliance* não deve ser encarada como o medo. O mais importante será a abordagem e o plano que nós temos para transformar o *compliance* não nesse medo, mas sim num catalisador do investimento necessário e da organização da casa. Passo número um, fazer o chamado *gap analysis* ou um *assessment*. Não encarar isto como binário de ‘sim ou não’. Há um ponto aceitável para cada exigência. Depois, gerir o investimento e empenho necessário em todo esse projeto”

“ A NOTIFICAÇÃO É MUITO IMPORTANTE, MAS, EM VEZ DE ESTARMOS TODOS EM PÂNICO A TENTAR COMUNICAR ALGUMA COISA, É FUNDAMENTAL DEFINIR PRIMEIRO O PLANO DE RESPOSTA A INCIDENTES E AS RESPONSABILIDADES INTERNAS ”

ARTUR MARTINS, CISO & CYBERSECURITY STRATEGY EXECUTIVE ADVISOR, LOGICALIS



- Artur Martins, Logicalis -

TODOS FALAM DA FALTA DE PROFISSIONAIS DE CIBERSEGURANÇA. MAS ATÉ QUE PONTO ISTO É UMA LIMITAÇÃO REAL À PREPARAÇÃO PARA NIS2 E ATÉ QUE PONTO É UM SINTOMA DE ESTRATÉGIAS ERRADAS, COMO FALTA DE AUTOMAÇÃO, PROCESSOS INEFICIENTES OU EXPECTATIVAS IRREALISTAS SOBRE PERFIS DE CONTRATAÇÃO?

Dinis Fernandes, Executive Manager, Cybersafe: “Há uma inércia que se colmata facilmente com a utilização de prestadores como nós, em que podemos ajudar num gap assessment inicial, na definição de um plano para colmatar as lacunas face aos requisitos do NIS2, na definição de um modelo de análise de risco e na seleção de tecnologia. **Existem formas de colmatar essa falta de recursos, mas também há organizações com equipas que têm falta de processo e de sistematização**, o que dificulta a resposta atempada a incidentes”

Bruno Castro, Founder & CEO, VisionWare: “**A NIS2 não vem obrigar que as empresas contratem um exército de especialistas. Vem obrigar, no fim do dia, a termos um modelo de governação sólido**, forte, estruturado, com processos simples e pragmáticos, capazes de responder adequadamente sempre que é necessário. O risco tem de estar na agenda do *top management*. Quem decide não é o técnico, não é o CISO; é o *top management*. No fim do dia, o *target* deverá ser construirmos um modelo de governação e um nível de maturidade adequado ao nosso setor”

José Fonseca, Technical Consultant Iberia, ManageEngine: “Não é preciso contratar um exército para implementar a NIS 2. O que é importante referenciar é que tudo passa pela parte do conhecimento e de preparar as pessoas e os negócios para estarem em conformidade com aquilo que são as *frameworks*. O que não existe na realidade não é a escassez de recursos, às vezes é as ferramentas mal configuradas e a preparação dos técnicos para criar *playbooks* e automação, para automatizar o máximo possível de tarefas e serem analistas e não tanto tarefeiros”

A CLOUD, O TRABALHO HÍBRIDO E A INTELIGÊNCIA ARTIFICIAL (IA) SÃO FATORES QUE ALARGAM A SUPERFÍCIE DE ATAQUE. QUAIS SÃO OS RISCOS CONCRETOS E SUBESTIMADOS NESTAS ÁREAS? COMO É QUE A NIS2 MUDA (OU NÃO) A RESPONSABILIDADE PARTILHADA ENTRE ORGANIZAÇÕES E FORNECEDORES DE CLOUD/SAAS?



- José Antunes, Symantec -

José Antunes, Arrow Pre Sales Specialist, Symantec: “Em termos objetivos de cloud e do SaaS, a utilização de *storage* na cloud vai expandir o perímetro de defesa. As coisas já não estão só no meu data center, controladas por mim, vão estar fora. Depois temos o *shadow IT*, numa zona cinzenta que obviamente aumenta o risco. Em termos da inteligência artificial, quando uso um Gemini, um Copilot, estou a passar informação para dentro dessa infraestrutura. A grande explosão em termos de risco vem daí”

“HAVER UMA CHECKLIST PODE TER UM EFEITO PERNICIOSO. O BOARD NÃO QUER SÓ QUE LHE DIGAM ‘ESTÁ VERDE’ NO DASHBOARD. VAI QUERER PERCEBER SE EFETIVAMENTE ESTÁ VERDE (...) E CARREGAR PARA VER O QUE SE PASSA”

JOSÉ ANTUNES, ARROW PRE SALES SPECIALIST, SYMANTEC

Bruno Castro, VisionWare: “Ainda há aquele *mindset* que é: se colocar isto na cloud, fica seguro. É um chavão e não é. Colocar na cloud não resolve o problema de NIS 2 porque não consigo transferir para lá o risco na totalidade. A falsa sensação de segurança é um erro gravíssimo. O que vemos é muito permissivo do lado dos *providers*. O que é que nos obriga a NIS 2? Controlarmos isso. Temos de fiscalizar o *provider* onde decidimos colocar a informação”

“ A NIS 2 NÃO É SÓ COIMAS, É UM TESTE DE MATURIDADE. NO FIM DO DIA, É UMA QUESTÃO DE ECOSSISTEMA E DE GARANTIR QUE O MEU RISCO NÃO IMPLICA O RISCO DO OUTRO ”

BRUNO CASTRO, FOUNDER & CEO, VISIONWARE



- Bruno Castro, VisionWare -

A DIRETIVA DÁ ÊNFASE À SEGURANÇA DA CADEIA DE ABASTECIMENTO. NA PRÁTICA, COMO AUDITAM E GARANTEM A CONFORMIDADE DE FORNECEDORES TERCEIROS? ISTO É EXEQUÍVEL PARA PME, OU VAI CONSOLIDAR AINDA MAIS O MERCADO EM TORNO DE GRANDES PLAYERS?

Miguel Barreiros, Executive Manager, Securnet: “Há uma questão fundamental que é a proporcionalidade, ou seja, aquilo que é exigível a um grande fornecedor terá de ser muito diferente daquilo que é exigido a um pequeno fornecedor. Nós não podemos chegar a tudo, portanto, temos de começar por classificar a cadeia de abastecimento por grau de importância. Vai ou não parar o meu negócio? Se sim, é um fornecedor crítico. Se não, o risco é menor. Não faz sentido tratar da mesma forma um fornecedor de serviço eletrónico e um de café verde. Uma pequena empresa que apresenta uma certificação vai diferenciar-se da sua concorrência”

Dinis Fernandes, CyberSafe: “Há uma abordagem baseada no risco e também baseada na criticidade. Um fornecedor muito importante para o negócio pode não significar grande risco do ponto de vista de IT. No entanto, o tema nunca é assim tão simples. Já tivemos um caso em que um fornecedor de matérias-primas teve um ataque ransomware e ficou impedido de operar, o que teve um impacto muito grande no negócio, embora do ponto de vista de IT não tivesse tido impacto nenhum. Se pensarmos só no risco do ponto de vista de IT, pode não ser suficiente para a nossa resiliência do ponto de vista de organização e do negócio”

A NIS2 IMPÕE PRAZOS APERTADOS PARA NOTIFICAÇÃO DE INCIDENTES. QUANTAS ORGANIZAÇÕES TÊM REALMENTE PLAYBOOKS TESTADOS, EQUIPAS TREINADAS E CANAIS ESTABELECIDOS PARA RESPONDER DENTRO DESTES TIMINGS? O QUE FALHA MAIS FREQUENTEMENTE NOS TESTES QUE FAZEM?

Bruno Castro, VisionWare: “Percebemos quando uma empresa já testou antes esse modelo de resposta a incidente ou a desastre, ou quando está meramente em modo de reação. Não quer dizer que testar vezes sem conta faça com que funcione 100%, mas garantidamente vai funcionar melhor. O que temos visto como dificuldades é a falha na capacidade de detecção em tempo útil e o saber o que fazer no momento do incêndio. No fim do dia, o que mais sentimos é: saber comunicar. Quem comunica, de que forma, para quem e com que *timing*”

Artur Martins, Logicalis: “Um bom plano de resposta a incidentes deve ter já pré-definido as categorias de incidentes que é possível termos e quem são os responsáveis internos para cada fase. Há responsáveis pela detecção, *reporting*, avaliação de impacto, investigação, mitigação e identificação da *root cause*. Em todas estas fases é muito importante ter um procedimento operacional. A notificação é muito importante, mas, em vez de estarmos todos em pânico a tentar comunicar alguma coisa, é fundamental definir primeiro o plano de resposta a incidentes e as responsabilidades internas”

Dinis Fernandes, CyberSafe: “Ao pensarmos que o número de organizações abrangidas pela NIS 2 passou de cerca de 300 para três mil, diria que a maior parte das organizações está num processo muito embrionário. Não têm *playbooks* nem processos de resposta a incidentes bem definidos, quanto mais testá-los. Muito dificilmente organizações com dimensão reduzida vão conseguir fazer uma monitorização 24 horas por dia ou dar uma resposta atempada aos incidentes. Nessas situações não há outra solução senão recorrer a um prestador de serviços SOC-as-a-Service ou MDR”

“HÁ QUICK WINS QUE SE PODEM FAZER. O MAIS IMPORTANTE É MOSTRAR DILIGÊNCIA, TER MÉTRICAS DE RISCO E UM PLANO DE AÇÃO PARA ENDEREÇAR AS LACUNAS”

DINIS FERNANDES, EXECUTIVE MANAGER, CYBERSAFE



- Dinis Fernandes, Cybersafe -

A NIS2 FALA MUITO DE RESILIÊNCIA. TER OS SISTEMAS SEGUROS NÃO É O MESMO QUE TER SISTEMAS RESILIENTES A ATAQUES. COMO DESENHAM ARQUITETURAS QUE ASSUMEM QUE A VIOLAÇÃO É INEVITÁVEL E GARANTEM CONTINUIDADE, MESMO SOB ATAQUE?

José Antunes, Symantec: “Temos de assumir que vai acontecer algo. Temos de nos preparar para isso. Não é só ter um *playbook*. Vamos aqui todos falar e perceber como é que vamos resolver isto. Temos de ter em conta que, literalmente, tudo pode acontecer. Os nossos adversários só fazem aquilo 24 horas por dia. Tem de ser esse o racional: vai acontecer. Depois criar cenários, fazer os *fire drills*. E há uma dualidade: eu quero repor as coisas e pôr aquilo a funcionar, mas isso pode fazer desaparecer as provas e depois não vou saber como endereçar o problema”



Artur Martins, Logicalis: “No tema da resiliência, não vale a pena reinventar a roda. Existe uma boa ISO 22301. Falamos de identificação de processos críticos e das suas dependências. **Nós focamo-nos sempre na tecnologia e esquecemo-nos das pessoas. Existem sempre os ‘super-homens’ que sabem tudo e menos documentam. Se essa pessoa não estiver, vamos estar todos em modo caótico.** A resiliência passa por identificar processos críticos e dependências, não só tecnológicas, mas também operacionais, e criar uma cultura de *security by design*”

Bruno Castro, VisionWare: “A memória fica tatuada depois de um super-ataque, da *layer* mais operacional à componente executiva. Levámos uma valente dose de humildade e repensámos o modelo. Hoje a abordagem é diferente: prevenção, deteção e recuperação. É assumir que um dia vai-me acontecer e tenho de ser capaz de responder e recuperar de forma eficaz, rápida e permanente. A NIS 2 não é só coimas, é um teste de maturidade. No fim do dia, é uma questão de ecossistema e de garantir que o meu risco não implica o risco do outro”



A NIS2 COLOCA RESPONSABILIDADE DIRETA NOS ÓRGÃOS DE GESTÃO. ISTO VAI MUDAR REALMENTE O NÍVEL DE ATENÇÃO DO C-LEVEL À CIBERSEGURANÇA, OU SERÁ MAIS UM REQUISITO DE COMPLIANCE BUROCRÁTICO? QUE CONVERSAS É QUE OS RESPONSÁVEIS DE CIBERSEGURANÇA DEVEM ESTAR A TER NESTE MOMENTO COM OS CONSELHOS DE ADMINISTRAÇÃO DAS SUAS ORGANIZAÇÕES?

José Fonseca, ManageEngine: “Isto acaba por ser um equilíbrio entre o risco financeiro e a responsabilidade do Conselho Executivo. O CISO tem de ser o elo entre quem operacionaliza e quem paga. Se não existir liderança por parte do Conselho Diretivo, a responsabilidade recai sempre sobre o CISO, e isso não deve existir. A NIS 2 vem complementar nesse sentido de não ser só *one man show*. Devem ser gerados relatórios com métricas consistentes: exposição, impacto, risco reputacional e continuidade, suportados por KPI executivos”

“ DESDE QUE EXISTA UM ROTEIRO, UM PLANEAMENTO, UMA ANÁLISE, UMA AUTOMAÇÃO HUMANA OU MESMO A NÍVEL DE SISTEMAS, DESDE QUE EXISTA UM PROCESSO, TUDO ISTO ACABA POR SE DESENROLAR DE FORMA EFICIENTE ”

JOSÉ FONSECA, TECHNICAL CONSULTANT IBERIA, MANAGEENGINE



- José Fonseca, ManageEngine -

Miguel Barreiros, Securnet: “Tem-se falado muito de tecnologia e de ausência de recursos. Eu acho que há é falta de *coaching* para as gerências. A cibersegurança faz parte do dia a dia. A NIS 2 é só a digitalização daquilo que já acontece no nosso mundo empresarial. Cibersegurança é cultura, mas a cultura sem tecnologia é muito mais vulnerável. Não tem a ver com a quantidade, tem a ver com a qualidade. O gestor não tem de ser técnico, tem de ser decisor. Tem de tomar decisões informadas com base naquilo que os técnicos e especialistas lhe dizem”

José Antunes, Symantec: “A atenção do *board* é um recurso escasso e a NIS 2 veio trazer uma ferramenta, se quiserem, à cibersegurança para ter um bocadinho de atenção. O que que a NIS 2 nos traz é essa capacidade de ‘não percebes o que eu estou a dizer, mas, de qualquer modo, no fim do dia há responsabilização’. Vamos tentar encontrar aqui o *middle ground* e falar a mesma linguagem”

HÁ O RISCO DE AS ORGANIZAÇÕES TRATAREM NIS2 COMO CHECKLIST BUROCRÁTICO, FAZENDO O MÍNIMO PARA PASSAR AUDITORIAS. COMO TRANSFORMA A PRESSÃO REGULATÓRIA NUMA OPORTUNIDADE REAL PARA MELHORAR A POSTURA DE SEGURANÇA, EM VEZ DE GERAR APENAS DOCUMENTAÇÃO E TEATRO DE SEGURANÇA?



- Miguel Barreiros, Securnet -

Miguel Barreiros, Securnet: “É não encarar como uma *checklist*, é encarar como uma oportunidade de transformação. Se o objetivo é estar verde, vai ficar verde. A questão é perceber se é só um teatrinho ou se é, de facto, uma cultura. Se é algo que se conseguiu introduzir como conceito na empresa. Acho que este é o ponto-chave: cultura, cultura, cultura. A resposta é: é para cumprir a *checklist* ou é para ter cultura? Já que se vai gastar o dinheiro, ao menos que se tenha cultura, porque cumprir a *checklist* consegue-se”

“HÁ COISAS FÁCEIS DE FAZER EM MENOS DE DOIS MESES. O MFA PRECISA DE UMA CONSULTORA? NÃO. QUALQUER RESPONSÁVEL DE IT DEVE CONSEGUIR CONFIGURAR ISSO. TESTAR OS BACKUPS? NÃO. JÁ DEVIA ESTAR FEITO”



José Antunes, Symantec: “Se é para estar verde, vai estar verde. Mas é preciso perceber que vai haver consequências, e consequências a dois níveis para o *board*. Estar verde não é desculpa para os impactos em termos de imagem e financeiros. O haver uma *checklist* pode ter um efeito pernicioso. O *board* não quer só que lhe digam ‘está verde’ no *dashboard*. Vai querer perceber se efetivamente está verde ou se é a melancia, e carregar com o dedo para ver o que se passa”

José Fonseca, ManageEngine: “Além da *checklist*, é ter uma real melhoria relativamente ao serviço. É ter métricas reais e uma governação operacional de tudo aquilo que são os sistemas. Não é só dizer ‘está verde’. É ter capacidade de apresentar ao conselho que, relativamente ao incidente, está tudo sob controlo. Não só na parte da *compliance* NIS 2, mas com ferramentas que tenham mais potência e sensibilidade, na componente de observabilidade, *workflow*, deteção e automação, para ajudar parceiros e clientes relativamente aos incidentes”

COM BASE NA VOSSA EXPERIÊNCIA NO TERRENO, QUAIS SÃO OS TRÊS ERROS MAIS COMUNS QUE AS ORGANIZAÇÕES COMETEM AO SE PREPARAREM PARA A NIS2? QUE PASSOS CONCRETOS PODEM DAR PARA NÃO OS REPETIR?

Artur Martins, Logicalis: “Um terrível erro é não ter a casa arrumada. Está na altura de termos departamentos de *compliance* e de risco com uma base de dados centralizada de controlos de segurança, para responder rapidamente e saber o que falta cobrir. Tecnologia não é a solução para o problema. Grande parte da solução é planeamento, documentação, maturidade e testes. A conformidade com a NIS 2 não é tudo ou nada. É perceber com o *board* qual é o risco que estão dispostos a aceitar, porque não há *budget* para estar a 100% em tudo”

FALTAM MENOS DE DOIS MESES PARA A ENTRADA EM VIGOR DA NIS2. IMAGINEM UMA EMPRESA QUE AINDA NÃO COMEÇOU A TRATAR DO TEMA. SE FOSSEM CONSULTORES DESSA EMPRESA, QUAL SERIA O VOSSO PLANO ATÉ 3 DE ABRIL? QUE AÇÕES PRIORITÁRIAS RECOMENDARIAM E PORQUÊ?

Dinis Fernandes, CyberSafe: “O comboio já seguiu. O dia 3 de abril é uma meta para demonstrar diligência, não é para ter tudo conforme aos requisitos do NIS 2. Há mínimos que têm de ser feitos, como um *gap assessment*. Mesmo aguardando *guidelines*, há temas que já se sabe que são necessários, como o *multifactor authentication* e o processo de notificação de incidentes. Há *quick wins* que se podem fazer. O mais importante é mostrar diligência, ter métricas de risco e um plano de ação para endereçar as lacunas”

José Fonseca, ManageEngine: “O roteiro é o segredo. Desde que exista um roteiro, exista um planeamento, exista uma análise, que exista uma automação humana ou mesmo a nível de sistemas, desde que exista um processo, tudo isto acaba por se desenrolar de forma eficiente. Que, no final do dia, é aquilo que toda a gente acaba por querer: eficiência no processo de transposição para a NIS 2”

Miguel Barreiros, Securnet: “Há coisas fáceis de fazer em menos de dois meses. O MFA precisa de uma consultora? Não. Qualquer responsável de IT deve conseguir configurar isso. Testar os *backups*? Não. Já devia estar feito. A questão do roteiro é fundamental. Se uma empresa nesta altura não tem um rumo quanto a esta matéria, já é preocupante. Servindo a NIS 2 como motor ou alavancagem, em dois meses consegue traçar um rumo, que é o mais importante. Se ainda não têm um rumo e têm um parceiro, troquem de parceiro” ■





POR STHEFANIE DAL MAGRO,
Consulting Services Manager, CyberSafe

DA CONFORMIDADE À MATURIDADE: OS DESAFIOS DA NIS 2 PARA AS ORGANIZAÇÕES PORTUGUESAS

A transposição da Diretiva 2022/2555 (NIS 2) para Portugal, por meio do Decreto-Lei 125/2025, impôs diversos desafios que impactam as organizações classificadas como críticas e essenciais.

O QUE ANTES se restringia a uma abordagem focada na notificação de incidentes, no envio de relatórios anuais e na designação de responsáveis de cibersegurança e pontos de contacto, agora exige uma perspectiva mais abrangente, profunda e estratégica da cibersegurança, com a implementação de medidas técnicas e organizativas relacionadas com a abordagem aos riscos organizacionais.

Um dos principais desafios está na necessidade de formalização dos processos. Apesar de muitas organizações já adotarem práticas de cibersegurança, essas

ocorrem, frequentemente, de forma dispersa ou pouco documentada. No entanto, a NIS 2 passa a exigir coerência, rastreabilidade e evidências, de modo que políticas, procedimentos, avaliações de risco e mecanismos de controlo deixem de existir apenas de modo informal e passem a ser definidos, testados e alinhados. Outro desafio significativo é integrar a cultura de cibersegurança na estratégia organizacional. A cibersegurança deve deixar de ser um tema tratado apenas pela equipa de IT e passa a exigir o envolvimento da gestão de topo. A responsabilização dos órgãos



- Sthefanie Dal Magro -
Consulting Services Manager, CyberSafe

GARANTIR QUE OS FORNECEDORES MANTÊM NÍVEIS ADEQUADOS DE SEGURANÇA E QUE ESSES RISCOS SÃO AVALIADOS DE FORMA CONTÍNUA PODE REPRESENTAR UM ESFORÇO ACRESCIDO PARA MUITAS ORGANIZAÇÕES, EM ESPECIAL PARA AQUELAS QUE POSSUEM MENOS MATURIDADE OU RECURSOS LIMITADOS

de administração implica o acompanhamento regular, definição de prioridades e alocação adequada de recursos. Esta mudança pode ser complexa, especialmente em estruturas onde a cibersegurança é vista como um tema puramente operacional.

A dimensão técnica também se torna mais exigente. Para além da aquisição de tecnologia, é necessário integrá-la num modelo consistente, com processos e responsabilidades bem definidos, de modo a garantir que a implementação das medidas relacionadas com a proteção de redes e sistemas, a utilização de mecanismos de dupla autenticação, a cifragem, a continuidade das operações e a resposta a incidentes, seja planeada e coordenada.

A supervisão da cadeia de abastecimento é outro ponto crítico. A dependência crescente de fornecedores tecnológicos, plataformas cloud e serviços externos amplia a exposição ao risco. Garantir que os fornecedores mantêm níveis adequados de segurança e que esses riscos são avaliados de forma contínua pode representar um esforço acrescido para muitas organizações, em especial para aquelas que possuem menos maturidade ou recursos limitados.

Neste contexto, todos estes elementos demonstram que os desafios são simultaneamente regulatórios, técnicos e culturais. A legislação portuguesa que concretiza a NIS 2 estabelece um quadro mais rigoroso, mas também oferece uma oportunidade: reforçar a maturidade, reduzir a exposição ao risco e integrar a cibersegurança como pilar estratégico do negócio.

É precisamente neste âmbito que o papel de parceiros especializados, como a CyberSafe, ganha relevância. Mais do que apoiar na interpretação do Decreto-Lei 125/2025, o valor acrescentado está na capacidade de transformar requisitos legais em planos de ação ajustados à realidade de cada organização. Desde a realização de avaliações de maturidade e análises de gap, até à definição de roadmaps faseados, implementação de controlos técnicos, revisão de processos e sensibilização das equipas e da gestão, o acompanhamento especializado permite reduzir a incerteza e priorizar investimentos de forma racional. Num contexto em que os desafios são simultaneamente técnicos, organizacionais e estratégicos, contar com um parceiro experiente pode fazer a diferença entre uma abordagem meramente documental e uma transformação efetiva da postura de cibersegurança. ■

O DIREITO À PRIVACIDADE DEVE APLICAR-SE TAMBÉM À SUA ATIVIDADE ONLINE – SEM EXCEÇÕES

A maioria de nós já sabe que está a ser monitorizada sempre que navega na internet — cookies para aqui, permissões para ali.

TEM HAVIDO BASTANTE CONTESTAÇÃO face ao que muitos consideram, e bem, salvaguardas de privacidade insuficientes — tanto por parte dos governos como do público.

Mas, apesar de todos os progressos alcançados, ainda estamos longe do objetivo. A verdadeira privacidade online continua distante. E, com a tecnologia a evoluir a um ritmo acelerado, as leis e as proteções de privacidade precisam de acompanhar esta evolução ou correm o risco de ficar para trás — como aconteceu até há bem pouco tempo.

O OLHO QUE TUDO VÊ (O BIG BROTHER ESTÁ A OBSERVAR)

Como se sentiria se todas as conversas que tem, cada chamada telefónica que faz, cada carta que envia, fossem constantemente monitorizadas? Até que ponto o rastreamento da atividade online está assim tão distante de uma vigilância tão invasiva?

Claro que, quando existe fundamento legal, o governo e as autoridades policiais podem obter autorização especial para monitorizar uma pessoa sob investigação. Mas a expressão-chave aqui é autorização especial. A vigi-



- Eric Roshaan -
Senior Content Specialist, ManageEngine

lância deve ser a exceção, não a regra. E também não deve ser o padrão no ambiente online.

O direito à privacidade é um direito humano fundamental. Desde que não esteja a infringir a lei, a sua privacidade merece ser respeitada — independentemente de quem seja. A privacidade não é um privilégio. É um direito. E deve ser a expectativa padrão, tanto online como offline.

O VERDADEIRO CUSTO DA CONVENIÊNCIA

Apesar dos avanços, continuamos a ser “forçados” a abdicar da privacidade, especialmente quando utilizamos serviços gratuitos.

Talvez já tenha ouvido falar do *escândalo da Cambridge Analytica*, no qual uma entidade terceira conseguiu recolher dados de mais de 50 milhões de contas do Facebook para criar anúncios políticos direcionados antes das eleições presidenciais dos Estados Unidos. Embora as partes envolvidas tenham inicialmente negado qualquer irregularidade, a *Meta acabou por concordar em pagar 725 milhões de dólares* num acordo cole-

tivo para resolver alegações relacionadas com o tratamento indevido de dados de utilizadores por terceiros como a Cambridge Analytica.

Várias plataformas de redes sociais também partilham informações dos utilizadores com entidades terceiras. Por norma, estes dados são utilizados para criar experiências personalizadas, e as plataformas tendem a referir esta prática nas suas políticas de privacidade. Mas sejamos sinceros — quantos de nós leem estes documentos extensos, cheios de linguagem jurídica, criados mais para cumprir requisitos legais do que para serem facilmente compreendidos? Eu sei que não leio.

A nossa privacidade não é negociável, e a partilha de dados com terceiros deveria tornar-se coisa do passado se as empresas e os reguladores estiverem realmente empenhados em defender os direitos à privacidade na era digital.

MANTENHAM OS VOSSOS OLHOS CURIOSOS LONGE DOS MEUS DADOS

Fico satisfeito por ver a proteção de dados no centro do debate tecnológico. A aprovação de

regulamentos como o RGPD representa um passo significativo rumo à soberania individual sobre os dados. É encorajador que grandes economias em todo o mundo tenham seguido o exemplo, inspirando-se na União Europeia em direção a uma verdadeira proteção da privacidade.

Isto já está a produzir resultados, com governos e até gigantes tecnológicos a restringirem a maioria das formas de rastreamento online. Por exemplo, o Safari da Apple e o Firefox da Mozilla bloqueiam agora cookies de terceiros por defeito, e o Chrome da Google optou por uma abordagem baseada na escolha do utilizador.

A questão da privacidade online só poderá ser resolvida através de legislação mais robusta, e é reconfortante ver os governos a lançar luz sobre as práticas invasivas das grandes tecnológicas. Se esta tendência continuar, o futuro da privacidade poderá não ser tão sombrio como já pareceu — uma notícia refrescante numa era dominada por manchetes cada vez mais distópicas. ■

DA AMEAÇA À FORÇA: COMO RESOLVER A ESCASSEZ DE COMPETÊNCIAS EM CIBERSEGURANÇA

A escassez de competências em cibersegurança é atualmente um dos principais desafios para as organizações.

NUM CENÁRIO em que as ameaças evoluem a um ritmo acelerado e recorrem cada vez mais à Inteligência Artificial, a escassez de talento especializado expõe as empresas a riscos acrescidos, compromete a transformação digital e amplifica o impacto financeiro dos incidentes de segurança. De acordo com a investigação mais recente da IDC e da Logicalis, 73% dos incidentes de ransomware resultam de erro humano e 67% conduzem a breaches bem-sucedidas por parte dos cibercriminosos. As consequências são significativas:

21% das organizações que optaram por pagar um resgate, pagaram entre 100.000 e 1 milhão de dólares para recuperar o acesso aos seus sistemas ou dados, enquanto 81% enfrentaram interrupções do negócio durante vários dias ou mesmo semanas.

A dificuldade em atrair e reter profissionais qualificados vem agravar este cenário. A procura de talento em cibersegurança continua a superar largamente a oferta, os orçamentos são limitados e a crescente complexidade tecnológica exige



- Artur Martins -

CISO & Cybersecurity Strategy Executive Advisor, Logicalis Portugal

PARA CIOs E LÍDERES DE SEGURANÇA, OS DESAFIOS SÃO EVIDENTES: AMEAÇAS POTENCIADAS POR IA QUE EVOLUEM MAIS RAPIDAMENTE DO QUE AS DEFESAS, ATACANTES CADA VEZ MAIS SOFISTICADOS E UMA ESCASSEZ PERSISTENTE DE COMPETÊNCIAS CRÍTICAS

competências em permanente atualização. Como resultado, 42% das organizações demoram mais tempo a preencher vagas, 35% registam atrasos nos seus projetos de transformação digital e 40% enfrentam dificuldades na retenção de talento altamente qualificado.

Para CIOs e líderes de segurança, os desafios são evidentes: ameaças potenciadas por IA que evoluem mais rapidamente do que as defesas, atacantes cada vez mais sofisticados e uma escassez persistente de competências críticas. Apesar dos avanços na automação, a necessidade de equipas especializadas, disponíveis 24x7 e com experiência nas ferramentas mais recentes, continua a representar um obstáculo significativo.

Neste contexto, depender exclusivamente de equipas internas já não é suficiente. A adoção acelerada da cloud e da Inteligência Artificial introduz novos riscos relacionados com privacidade de dados, governação e configurações inadequadas, muitas vezes associados à falta de especialização interna.

Para colmatar este problema, muitas organizações estão a recorrer a Managed Security Services – e, segundo a IDC, 48% reconhecem claramente os benefícios desta abordagem.

“Os Managed Security Services da Logicalis garantem proteção de nível enterprise, com uma abordagem integrada, escalável e 24x7, combi-

nando especialização e automação para reduzir a exposição a ameaças e reforçar a resiliência do negócio.”

– Artur Martins, CISO & Cybersecurity Strategy Executive
Advisor, Logicalis Portugal

Ao complementar as suas capacidades internas com Managed Security Services, as organizações reforçam a sua resiliência, reduzem o tempo de resposta a incidentes e ganham confiança para crescer de forma sustentada num ambiente digital cada vez mais complexo.

Para saber mais sobre este estudo, faça o download gratuito do infográfico da IDC em www.pt.logicalis.com/estudos-idc-logicalis ■



POR MIGUEL BARREIROS,
Sales & Marketing Director
da SECURNET

NIS2: NO MÍNIMO E PARA COMEÇAR, UM (BOM) PLANO...

Ainda estamos a tempo de usar a NIS2 como catalisador para algo de que há muito precisamos, investindo em práticas estruturadas e transformando-a em resiliência operacional. Ganhando vantagem competitiva! Outrossim será uma oportunidade perdida.

MUITO SE TEM DEBATIDO sobre as implicações da NIS2 mas, numa visão mais descomplexada, quase sempre a partir dos interlocutores errados. Têm sido as áreas tecnológicas a alertar e pressionar a gestão de topo para a preparação necessária. Pergunta-se, não deveria ser precisamente esta a questionar as suas áreas tecnológicas e operacionais sobre o estado de maturidade e prontidão?

SENSIBILIZAÇÃO OU OTIMISMO?

Há muito que ninguém ousa questionar que qualquer organização e setor de atividade

dependem das tecnologias de informação para sobreviver. Ora, os infelizes acontecimentos no nosso País, de há um ano a esta parte, do apagão energético às tempestades, trouxeram à evidência que a ausência de um plano de resposta a incidentes, de quaisquer tipos de incidentes, poderá trazer consequências irreversíveis.

Muito provavelmente e também por isso, a NIS2 é hoje mais bem compreendida pelos gestores nacionais, o que terá levado 63% dos inquiridos a afirmar acreditar no prazo de 12 meses para

a cumprir, segundo um estudo muito recente da IDC e Microsoft.

Mas será sensibilização ou otimismo? Será que já houve uma “inversão na mesa” e a pergunta já passou de “quanto custa fazer?” para “quanto pode custar não fazer?” Será que as lideranças já estão conscientes de que a cibersegurança deixou de ser uma questão técnica e passou a um risco empresarial?

A NIS2 e a sua preparação devem ser um processo partilhado. Também compete aos gestores das áreas tecnológicas adaptarem o discurso e linguagem

no diálogo com o topo das organizações, levando impacto financeiro e exposição por serviço crítico, dependência de terceiros e consequências, capacidade real de recuperação ou outro tipo de métricas de negócio em detrimento de tecnologia. E a mudança só acontece com métricas e perguntas certas.

Não se exigem discussões tecnológicas na gestão de topo, nem tão pouco ferramentas ou orçamentos, exigem-se decisões informadas.

- Quais os serviços (de negócio) cuja paragem é inaceitável?
- Quanto tempo conseguimos operar degradados?
- Qual é o nosso apetite ao risco?
- Quem decide sob pressão num incidente grave e quem coordena o quê?

A maturidade não começa com ferramentas, começa com clareza. Sobre o que é crítico, quem decide e como se recupera. No fundo muito daquilo que já antes da NIS2 devia estar assegurado. Se a diretiva servir para criar essa clareza, já terá cumprido um papel transformador.

As organizações (ainda) estão a tempo de usar

a NIS2 como ponto de partida em vez de objetivo final e usar o seu verdadeiro valor como catalisador para algo que há muito precisavam de fazer. De cumprir a pressão regulatória investindo em práticas estruturadas, transformando-a em resiliência operacional e competitividade ou, de outra forma, serão recursos e oportunidades desperdiçadas.

OS RECURSOS HUMANOS E NÃO SÓ

Sempre que se abordam questões de TI e em especial cibersegurança (numa visão de engenharia) surge o tema da ausência de recursos humanos em número bastante e suficientemente qualificados. Mas não estarão as organizações a pedir respostas aos interlocutores errados? Serão áreas de engenharia as mais habilitadas e a quem são exigíveis respostas como as necessárias no contexto da NIS2?

Na SECURNET, acreditamos que “sem cultura a compliance resume-se a uma checklist e sem tecnologia a cultura é vulnerável”. É precisamente por isso que é a unidade de consultoria que autonomamente endereça as temáticas de governação, do risco e de compliance, como a NIS2, em para-

lelo com as áreas de engenharia. Acreditamos que conseguir, no final, entregar o melhor serviço e soluções quando se juntam estes dois mundos.

A IMPORTÂNCIA DE TER PLANOS

O problema não é cumprir a NIS2, não começa por aí, mas sim nas bases estratégicas da gestão de riscos. E ter planos! De implementação da diretiva, de resolução de problemas identificados, de continuidade de negócio e de resposta a incidentes. Começamos pelos planos de implementação e de resolução de problemas identificados, dividindo-o em três fases: visibilidade, redução de risco imediato e governação. Uma vez cumprido, e o processo não é necessariamente longo, já estarão dados importantes passos rumo aos objetivos iniciais.

Na primeira fase - visibilidade, um inventário de ativos e serviços com identificação clara de serviços críticos para a organização, identificação dos fornecedores críticos e nomeação do responsável. Na fase seguinte - redução de risco imediato, com implementação de multifator de autenticação (MFA), revisão de privilégios reduzindo-os aos

mínimos necessários, backups imutáveis (realmente testados) e desenho de guia de resposta a incidentes (um pouco mais demorado). Não será exagerado afirmar que se neste momento a organização não usa multifator de autenticação nos acessos e um bom e eficaz sistema de backups tinha já um problema de gestão, ainda que tecnológico, por resolver muito antes da NIS2.

Por fim, a última fase desta etapa - governação, com o envolvimento da gestão de topo da organização (administração ou gerência), a formalização de um roadmap realista, faseado e dotado dos meios necessários para ser concretizado (recursos humanos e financeiros) e o estabelecimento de métricas básicas para avaliação.

É bom lembrar que o mais importante (nesta fase) é demonstrar (com verdade) diligência e um plano estruturado.

A IMPORTÂNCIA DE TESTAR

A diretiva NIS2 estabelece prazos curtos para a notificação de incidentes, mas não serão neces-

sários prazos ainda mais curtos de reação a bem da sobrevivência das organizações? Aqui há claramente um caminho a percorrer face ao reduzido número de entidades com guias de resposta preparados e fundamentalmente testados, com equipas treinadas (do IT mas não só), canais de comunicação e cadeia de decisão definidos.

Será necessário estudar e preparar respostas num caminho que começa muito antes e a montante para que, no “dia D”, haja o sucesso possível a jusante. Testar, falhar, rever, melhorar, treinar e voltar a testar são passos de um ciclo contínuo fundamental. No tal “dia D” não bastará ter políticas não testadas, planos nunca treinados, backups nunca restaurados, nem inquéritos a fornecedores sem qualquer validação. Será necessário ter passado por exercícios regulares, testes de recuperação, revisão e ajuste de privilégios e métricas bem definidas sobre resiliência.

Quando se invoca o azar, fala-se que o diabo está atrás da porta. E já agora, nos pormenores ...

CONCLUSÃO

Para além daquilo que é o mais importante, o próprio negócio e as próprias organizações, e é assim que deve ser encarado este desafio como foi até agora explanado, a NIS2 é também muito acerca de gestão do risco e de evidências.

Se na gestão de risco exige-se que seja adequada ao contexto, sem complexidade desnecessária, quanto às evidências nem tudo se audita, nem tudo tem de ser auditado, antes de acordo e proporcionalmente à sempre presente gestão do risco.

Em dois meses não se atinge maturidade, mas consegue-se assegurar o controlo da situação.

Lembre-se, “o essencial é demonstrar governação, consciência de risco e plano estruturado” e para isso pode contar com a SECURNET como seu parceiro de redução de risco, que o ajude na definição de parâmetros de governação, um integrador pragmático focado em resiliência, não apenas em tecnologia!

Mais informações através de info@securnet.pt ou comercial@securnet.pt ■



Carbon Black.
by Broadcom



POR STEPHEN HEARTY,
Head of Symantec Product Marketing EMEA
e POR STANISLAV ELENKRICH
Director of Product Management, ESG, Broadcom

ZTNA: A ALTERNATIVA ÀS VPNS QUE ESTÁ A REDEFINIR A SEGURANÇA NO TRABALHO HÍBRIDO

Não é preciso procurar muito para perceber porque o Zero Trust Network Access (ZTNA) é uma boa ideia, nota-se nos números.

AS VIOLAÇÕES DE TERCEIROS aumentaram para 35,5% em todos os incidentes de segurança em 2024. Estes números evidenciam a necessidade de uma autenticação forte, não só nos endpoints, mas em toda a organização. É isso que a ZTNA oferece.

Muitas equipas de TI continuam a agarrar-se às suas VPNs, convencidos de que são suficientemente fiáveis para o trabalho híbrido atual. Mas, na realidade, a sua VPN funciona com um modelo desatualizado que coloca a sua organização em risco. É por isso que a Gartner previu que o ZTNA representará pelo menos 70% das

novas implementações de acesso remoto até ao final de 2025, em vez dos serviços VPN. O ZTNA é uma forma comprovada de maximizar a segurança de acesso mantendo qualquer interrupção ao mínimo. Seguem 5 razões para adotar esta abordagem à segurança:

1. AS VPNS ESTÃO OBSOLETAS

Os seus colaboradores precisam de acesso a aplicações específicas, não a toda a sua rede. Infelizmente, as VPNs não funcionam assim. Proporcionam acesso amplo à rede após uma única autenticação. Uma vez lá dentro, os cibercriminosos podem

mover-se para qualquer parte da rede e é exatamente isto que acontece em ataques de ransomware que exploram vulnerabilidades de VPN.

As VPNs tradicionais não têm acesso privilegiado no momento certo, o que dá acesso total a recursos desnecessários e dificulta o acompanhamento das atividades de um local para outro na rede. A ZTNA muda as regras do jogo ao fornecer conectividade ao nível da aplicação entre utilizadores autenticados e apenas a aplicações específicas, eliminando a exposição em toda a rede. Os recursos permanecem ocultos e invisíveis para utilizadores não autorizados.

2. O ZTNA MELHORA A EXPERIÊNCIA DO UTILIZADOR

Ninguém gosta de VPNs, especialmente os seus utilizadores. Encaminhar todo o tráfego através de núcleos de dados centralizados cria o temido efeito de hairpinning, onde o tráfego dos utilizadores segue o caminho mais longo.

Alguém no Reino Unido que queira ligar-se a um servidor em Londres não deveria ter de passar por um centro de dados em Munique para lá chegar. Isto causa latência, tornando as aplicações na cloud lentas.

Os contratantes externos têm ainda pior dificuldade quando os seus dispositivos encontram clientes VPN pouco práticos, que os impedem de realizar até tarefas básicas.

É aqui que os clientes existentes da Symantec Cloud SWG obtêm os maiores benefícios. A ZTNA integra-se perfeitamente com a sua infraestrutura, criando uma plataforma unificada de Security Service Edge (SSE). O Symantec SSE oferece cloud SWG, CASB, DLP, Web Isolation, ZTNA e muito mais. Isto consolida a segurança enquanto propor-



- Stephen Hearty -
Head of Symantec Product Marketing EMEA

ciona acesso, independente da localização. Isto significa menos fornecedores, gestão mais fácil, melhor integração e custos reduzidos.

3. A ZTNA MELHORA A PROTEÇÃO DE DADOS E PROPORCIONA DEFESA EM PROFUNDIDADE

As VPNs dão-lhe acesso à rede, mas zero visibilidade sobre o que os utilizadores estão a fazer com as suas aplicações e dados. Os registos estão frequentemente dispersos por vários servidores e locais, tornando difíceis as auditorias de conformidade.



- Stanislav Elenkrich -
Director of Product Management, ESG, Broadcom

Além disso, o Web Isolation mantém conteúdos sensíveis em contentores seguros, impedindo que o malware chegue ao dispositivo do utilizador. Isto dá-lhe uma melhor prevenção de ameaças diretamente na plataforma.

O ZTNA com DLP incorporado muda tudo. O detetor de cloud inspeciona os dados em movimento enquanto mantém o controlo de políticas local, garantindo que as suas regras DLP seguem os utilizadores onde quer que se conectem.

Pode usar DLP para identificar dados sensíveis em risco e depois aplicar políticas de proteção detalhadas. O Symantec ZTNA está até integrado

com o serviço de inteligência de ameaças confiável da Symantec para inspecionar todo o tráfego à procura de ameaças maliciosas, podendo bloquear cargas de malware provenientes de dispositivos infectados.

4. O ZTNA OFERECE MELHOR ESCALABILIDADE E DESEMPENHO DO QUE AS VPNS

As VPNs tradicionais foram criadas numa altura em que as aplicações trabalhavam em centros de dados e o trabalho remoto era uma raridade. Hoje, as aplicações estão dispersas por várias clouds. Tanto os seus colaboradores, como os seus parceiros externos, esperam acesso fluido e imediato em qualquer lugar.

As VPNs requerem configurações dispendiosas de DMZ e firewall que complicam a capacidade de crescimento. Em contraste, o Symantec ZTNA funciona na espinha dorsal do Google Cloud, oferecendo desempenho robusto e escalabilidade para organizações de todos os tamanhos.

O modelo SaaS da Symantec significa que não há hardware para gerir, nem dores de cabeça

no planeamento da capacidade, com atualizações automáticas que o mantem protegido. E pode fazer a implementação em minutos, não em meses. Quando a sua equipa de Minneapolis precisar de aceder a uma aplicação de Londres, a ligação será direta, sem desvios por centros de dados distantes.

5. A IMPLEMENTAÇÃO FASEADA FACILITA O INÍCIO.

Nada é mais inconveniente para uma equipa de TI do que dismantelar uma infraestrutura que ainda funciona tecnicamente. A implementação faseada do ZTNA permite-lhe manter a VPN ativa durante a transição. Focar primeiro no acesso de terceiros, contratados e trabalhadores remotos permite-lhe começar por mitigar os maiores riscos, uma vantagem que reduz imediatamente a superfície de ataque.

Ao adicionar informação de inspeção de ameaças em todo o tráfego e DLP para identificar e proteger dados sensíveis em risco, irá reforçar a sua segurança, trabalhando primeiro no conjunto de dados antes de implementar gradualmente o ZTNA em

toda a organização. A implementação pode ser feita por departamentos, por localização ou por grupos de utilizadores.

A prova está nos números. Verificámos que aproximadamente 80% dos clientes que realizam um projeto de demonstração do conceito ZTNA acabam por fazer a compra. Isto porque, começar pequeno permite demonstrar valor sem correr riscos. Pode até ser proposto como um “lançamento faseado” para clientes que ainda confiam nas suas VPNs ou que ainda não viram o valor que a ZTNA oferece.

MUDE PARA SEGURANÇA À PROVA DE FUTURO.

Atualizar uma infraestrutura VPN para ZTNA consiste em resolver falhas de segurança maiores antes que se tornem problemas graves. Vivemos num novo ambiente de trabalho remoto e híbrido e parcerias baseadas no acesso digital. Está na altura de repensar a forma como gerimos o acesso aos nossos dados e recursos computacionais, adotando a segurança ao nível da aplicação com verificação contínua. ■



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

O QUE DIZEM OS OLHOS DA NIS2: CONFORMIDADE EM ALTA DEFINIÇÃO

A NIS2 já não é só teoria, nem apenas tema de powerpoint de conferência. Está em vigor, foi transposta, tem obrigações e multas.

A NIS2 É MUITO MAIS que uma checklist, é um teste de maturidade e se está cansado de ler informação pouco direta sobre o que isto implica, este artigo é para si.

Começamos pelo ponto mais desconfortável: a NIS2 tira a cibersegurança da cave e leva-a para a sala do top management, já que a responsabilidade é da gestão de topo e não do “rapaz do IT”, nem do fornecedor externo, nem do consultor. É de quem decide.

A adaptação começa, portanto, por governação: definir quem manda, quem decide, quem reporta e quem assume o risco. Criar (ou formalizar) um modelo de gestão de risco cibernético alinhado com o risco empresarial e integrar a segurança no mapa estratégico da organização. Se o risco digital não está lado a lado com o risco financeiro ou reputacional, então a casa ainda não está arrumada.



- Bruno Castro -

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

Depois vem o exercício que separa as organizações maduras de organizações otimistas: a análise de lacunas, isto é, o famoso gap analysis. E aqui é preciso honestidade brutal. Existem políticas formais? São aplicadas ou apenas assinadas? Há inventário atualizado de ativos? Sabemos exatamente que sistemas suportam processos críticos? Conseguimos identificar dependências externas? Temos registros de testes a backups ou apenas assumimos que funcionam?

A NIS2 obriga a olhar para dentro, mas também para fora, com um novo foco na cadeia de fornecimento. Fornecedores de software, prestadores de serviços cloud, empresas de manutenção remota, serviços de marketing externos, etc, todos fazem parte do perímetro real. Adaptar-se implica rever contratos, exigir garantias, introduzir cláusulas de segurança e, em muitos casos, auditar terceiros. A pergunta passa a ser: “se o meu fornecedor “cair”, eu “caio” com ele?”

Em termos técnicos, não há magia, há disciplina. Autenticação multifator generalizada, segmentação de rede, gestão contínua de vulnerabilidades, patching atempado, encriptação adequada, backups offline testados, entre outros. No fundo, o que muda não é o nome das medidas, mas sim a profundidade da sua implementação.

A capacidade de deteção e resposta é outro divisor de águas. Não basta prevenir, é preciso assumir que, mais cedo ou mais tarde, algo vai falhar. Ter monitorização contínua e capacidade de resposta a incidentes (por exemplo,

através de um SOC), definir procedimentos claros de escalonamento, nomear responsáveis de crise, preparar comunicações internas e externas, e acima de tudo, treinar. A diferença entre o caos e o controlo raramente está na tecnologia – está na preparação.

Há também um elemento cultural que não pode ser ignorado. A maior parte dos incidentes graves começa com um erro humano, seja um clique, uma password fraca, uma partilha indevida. Adaptar-se à NIS2 implica investir em formação real, e preparar os colaboradores para que percebam que segurança não é um obstáculo; é sim, um mecanismo de proteção coletiva. E depois há a parte menos glamorosa: a documentação. A NIS2 exige evidências, políticas aprovadas, atas de reuniões, relatórios de auditoria, registros de formação, provas de testes. Em caso de incidente, a pergunta não será apenas “o que aconteceu?”, mas também “o que fizeram para evitar?”. Conseguir demonstrar diligência pode ser a diferença entre um incidente grave e um desastre jurídico.

A NIS2 é um desafio, mas pode ser igualmente uma oportunidade rara de limpar a casa a fundo, eliminar sistemas obsoletos, consolidar plataformas e repensar processos. Pode ser o pretexto certo para modernizar, para justificar investimento, para reforçar a confiança e a credibilidade junto de clientes e parceiros. Num mercado cada vez mais sensível à resiliência digital, demonstrar maturidade em cibersegurança é um argumento comercial poderoso. ■

DAVID MARQUES, HEAD OF CYBERSECURITY DO GRUPO NABEIRO

A portrait of David Marques, a man with short dark hair and a slight smile, wearing a grey blazer over a blue patterned shirt. He has his arms crossed and is standing in front of a blurred background of what appears to be a modern office or building.

**“TEMOS DE APROVEITAR
ESTE PARADIGMA DA
ENTRADA EM VIGOR DA NIS2
E CADA VEZ MAIS PASSAR
PARA MODELOS DE GESTÃO
DE RISCO”**

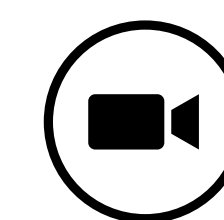
David Marques, Head of Cybersecurity do Grupo Nabeiro, subiu ao palco da primeira edição do ano da IT Insight Talks para uma entrevista onde abordou os temas da NIS2, a evolução do papel do CISO e a importância de evitar o burnout dos profissionais de cibersegurança.

RUI DAMIÃO

A NIS2 ESTÁ A CHEGAR E ENTRA EM VIGOR AINDA NA PRIMEIRA METADE DESTE ANO. COMO OLHA PARA ESTA REGULAMENTAÇÃO? O QUE SENTE QUE AS ORGANIZAÇÕES, COMO UM TODO, VÃO TER MAIS DIFICULDADE?

Há aqui alguns aspetos muito positivos. Por um lado, a NIS2 traz alguma harmonização a nível da União Europeia daquilo que são as medidas de cibersegurança de um conjunto de entidades. **Independentemente de cada país fazer uma transposição nacional, a verdade é que haverá alguma harmonização mínima daquilo que são os padrões.** Acho que isso acaba por ser muito positivo, especialmente para nós em particular em Portugal, porque tipicamente não somos propriamente dos países que têm mais maturidade deste ponto de vista.

Por outro lado, também traz um foco diferente ao tema da cibersegurança dentro das organizações. Há aqui alguns requisitos que efetivamente podem ser



PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM



transformadores. O facto de haver uma responsabilização maior dos órgãos de gestão de topo pode ser transformador; traz a cibersegurança para um patamar onde em algumas organizações ainda não chegava. Por exemplo, o facto de existir a nomeação de um responsável de cibersegurança, até pode não ser alguém que esteja a desempenhar esse papel a tempo inteiro e com foco exclusivo, mas o facto de existir uma responsabilização já é também um desenvolvimento muito positivo.

Por último, é o facto da gestão de risco de terceiros que acaba por ter um impacto positivo no ciberespaço nacional. Mesmo entidades que não estão diretamente abrangidas pela NIS2 vão acabar por ser impactadas porque aqueles que estão abrangidos vão começar a ser um bocadinho mais exigentes na sua cadeia de valor.

Os desafios são completamente diferentes tendo em conta as entidades. É bom lembrar que já existia uma NIS1. As entidades que já estavam abran-

gidas pela NIS1, entidades tipicamente em setores essenciais e críticos para o ciberespaço nacional, as alterações para essas não são assim tremendamente diferentes; creio que vão ter muita facilidade em adaptar-se a um conjunto de requisitos novos, muitos dos quais na prática já cumpriam e já vêm de trás.

Depois temos uma segunda camada, que são se calhar as empresas já com alguma dimensão, que têm equipas de cibersegurança próprias, autónomas, e aí creio que com alguma relativa facilidade vão conseguir atingir, quer do ponto de vista de *compliance*, quer do ponto de vista mais operacional, esses requisitos porque há equipas focadas para lá chegar.

Onde me parece claramente que haverá uma dificuldade muito maior será nas organizações que não estavam abrangidas pela NIS1 e não têm equipas de cibersegurança dedicadas, têm apenas equipas de IT que têm de chegar a muitos lados

“

MUITAS VEZES, NÃO É FÁCIL PARA NÓS, COMO RESPONSÁVEIS DE CIBERSEGURANÇA, LIGAR TODOS OS RISCOS COM TEMAS FINANCEIROS, MAS CREIO QUE A GESTÃO DE RISCO TAMBÉM É UM TEMA QUE A GESTÃO DE TOPO ESTÁ PERFEITAMENTE HABITUADA A LIDAR”

diferentes. Acredito que aí sim, haverá uma dificuldade muito maior, por um lado, em entender os requisitos e, depois, conseguir implementar operacionalmente esses requisitos do ponto de vista de cibersegurança. Essas entidades provavelmente vão precisar de ajuda de terceiros para conseguir lá chegar, mas haverá níveis de maturidade completamente diferentes.

A SEGURANÇA DA CADEIA DE VALOR É OBRIGATÓRIA E UM DOS PONTOS CENTRAIS DA NIS2. COMO É QUE AS ORGANIZAÇÕES CONSEGUEM REALIZAR UMA AVALIAÇÃO ADEQUADA DE DIFERENTES TIPOS DE FORNECEDORES?

Parece-me que sim, que esse é um dos pontos fundamentais de melhoria da NIS2, até porque nós sabemos, por notícias recentes, que esse é um dos maiores riscos que existe.

Como é que isto é possível implementar na prática: acho que a pergunta que ajuda a perceber a resposta; diferentes tipos de fornecedores. Os fornecedores têm diferentes tipos de importância do ponto de vista de cibersegurança para uma organização e isso até pode ser completamente diferente da importância que têm para o negócio.

Dou um exemplo no nosso caso em particular. Nós temos, por exemplo, fornecedores de café verde espalhados pelo mundo que têm uma relevância



muito grande para o negócio, mas na prática do ponto de vista de cibersegurança tem uma relevância muito baixa, porque há apenas uma troca de emails com esses fornecedores. Estabelecemos *tiers* para os nossos fornecedores; temos quatro *tiers* para os fornecedores, com critérios definidos, consoante a relevância que têm do ponto de vista de cibersegurança, e depois, em cada um destes *tiers*, fazemos um *assessment*, avaliamos esse *assessment*, pedimos evidências para algumas circunstâncias que dá origem a um determinado resultado. Com base nesse resultado há aqui algumas decisões, ou simplesmente aceitamos, está dentro do nosso nível de apetite de risco, ou



sugerimos um plano de tratamento, que na prática significa que devem implementar um conjunto de medidas do ponto de vista de cibersegurança, ou eventualmente se não cumprem um patamar mínimo, então na prática entra dentro do nosso processo de gestão de risco, ou seja, abrimos riscos em que terá de ser o negócio depois a decidir aceitar ou não trabalhar com aquele fornecedor que representa um risco do ponto de vista de cibersegurança.

Penso que esta é uma forma de gerir o tema, mas passa precisamente por diferenciar estas tipologias de fornecedores e depois ter uma abordagem para cada um deles consoante a importância que têm do ponto de vista de cibersegurança para a organização.

UM PONTO IMPORTANTE PARA O TRABALHO DE UM CISO É A MANEIRA COMO INTERAGE COM A ADMINISTRAÇÃO. CADA EMPRESA É UMA EMPRESA, NATURALMENTE, MAS DENTRO DAQUILO QUE CONHECE, OS CONSELHOS DE ADMINISTRAÇÃO REAGEM MELHOR A MÉTRICAS DE DINHEIRO OU DE VULNERABILIDADES?

Logicamente dinheiro; esse é o papel deles. Evidentemente, cada empresa é uma empresa; até mesmo dentro da gestão de topo há perfis completamente diferentes.

Diria que **falar de vulnerabilidades até pode assustar um bocadinho porque podem não entender o contexto**. Se vamos falar com uma gestão de topo e dizer que temos centenas de milhares de vulnerabilidades, pode-se criar um pânico. Não é esse o objetivo.

“

COSTUMO DIZER QUE, TODOS OS ANOS, TENHO UMA PRIORIDADE CLARA, INDEPENDENTEMENTE DE PASSARMOS MUITO TEMPO A FAZER 'N' ATIVIDADES DENTRO DA ORGANIZAÇÃO: A PRIORIDADE É NÃO TER UM INCIDENTE SIGNIFICATIVO PARA AS OPERAÇÕES DO GRUPO; ESTA É A PRIORIDADE”

Creio que há aqui duas linguagens que efetivamente a gestão de topo fala. E aí, independentemente do seu *background*, se tem um *background* mais tecnológico ou menos tecnológico, que é os temas financeiros. Muitas vezes, não é fácil para nós, como responsáveis de cibersegurança, ligar todos os riscos com temas financeiros, mas creio que a gestão de risco também é um tema que a gestão de topo está perfeitamente habituada a lidar. Eles próprios têm de gerir risco; assim como nós gerimos cibersegurança, eles gerem risco diariamente. Esse sim, creio que é o melhor caminho para conseguir chegar à gestão de topo e para transformar os riscos mais tecnológicos numa linguagem menos tecnológica, numa linguagem mais de impacto para a organização, para que consigam entender esse impacto e penso que isto, sim, pode ser transformador, porque entendendo a linguagem do risco, tipicamente é muito mais fácil potenciar decisões vindas da gestão de topo.

COMO SENTE QUE TEM EVOLUÍDO O PAPEL DO CISO OU DO RESPONSÁVEL DE CIBERSEGURANÇA DENTRO DAS ORGANIZAÇÕES? NOS ÚLTIMOS DOIS OU TRÊS ANOS, COM UM NÚMERO CRESCENTE DE CIBERAMEAÇAS, QUAL É A IMPORTÂNCIA DO CISO NA ORGANIZAÇÃO?

Creio que tem tido uma evolução muito positiva. O responsável de cibersegurança, CISO ou outro qualquer, era alguém que estava muito focado no tema tecnologia, tipicamente vendia tecnologia dentro da organização e, associada a isso, só vendia custo. Hoje é muito diferente. Hoje, o responsável de cibersegurança, o CISO, na prática, tem de entender o negócio, como é que a organização funciona e tem de suportar o negócio.

Isso tem acontecido cada vez mais e creio, das conversas que tenho, que aquilo que se sente é que cada vez mais a organização e até a gestão de



topo acaba por consultar o CISO para a tomada de decisão e esse é precisamente o objetivo.

Logicamente que o papel também difere muito consoante aquilo que é a organização, até a dimensão. Há uns dias falava com alguém, não era o CISO, mas era alguém que tinha responsabilidade numa multinacional europeia que tem uma equipa de cibersegurança de 300 pessoas. Evidentemente, o papel de um CISO de uma organização que tem 300 pessoas na área de cibersegurança é um bocadinho diferente do papel de um CISO que está

numa empresa que tem cinco ou seis pessoas numa área de cibersegurança. Os papéis são diferentes. O objetivo final é semelhante, mas os papéis logicamente podem mudar muito.

A CIBERSEGURANÇA É CADA VEZ MAIS COMPLEXA PARA UMA ORGANIZAÇÃO E UM GRANDE NÚMERO DE PROFISSIONAIS DE CIBERSEGURANÇA ACABA POR SOFRER DE *BURNOUT*. COMO É QUE SE PODE GERIR ESTA COMPLEXIDADE COM A NECESSIDADE DE TER AS OPERAÇÕES SEMPRE A FUNCIONAR?

Esse efetivamente é um problema. Não só o número, mas a complexidade das ameaças é cada vez maior; o número de tecnologias é cada vez maior, o número de alarmística é cada vez maior. Isso gera ansiedade e pode levar a *burnout*. Mesmo o papel do CISO que falávamos: há muitos CISO – cá em Portugal e fora – que, na prática, fazem omelete sem ovos o que leva a esse tipo de situações.

Não sendo especialista nessa matéria, acho que a única forma de gerir este tema e evitar chegar a esse ponto é sermos muito realistas e termos uma definição de prioridades muito clara. Realismo em que sentido: na prática, nunca conseguimos fazer tudo e temos de assumir claramente que não vamos conseguir atingir tudo aquilo que queremos fazer. Realismo também no

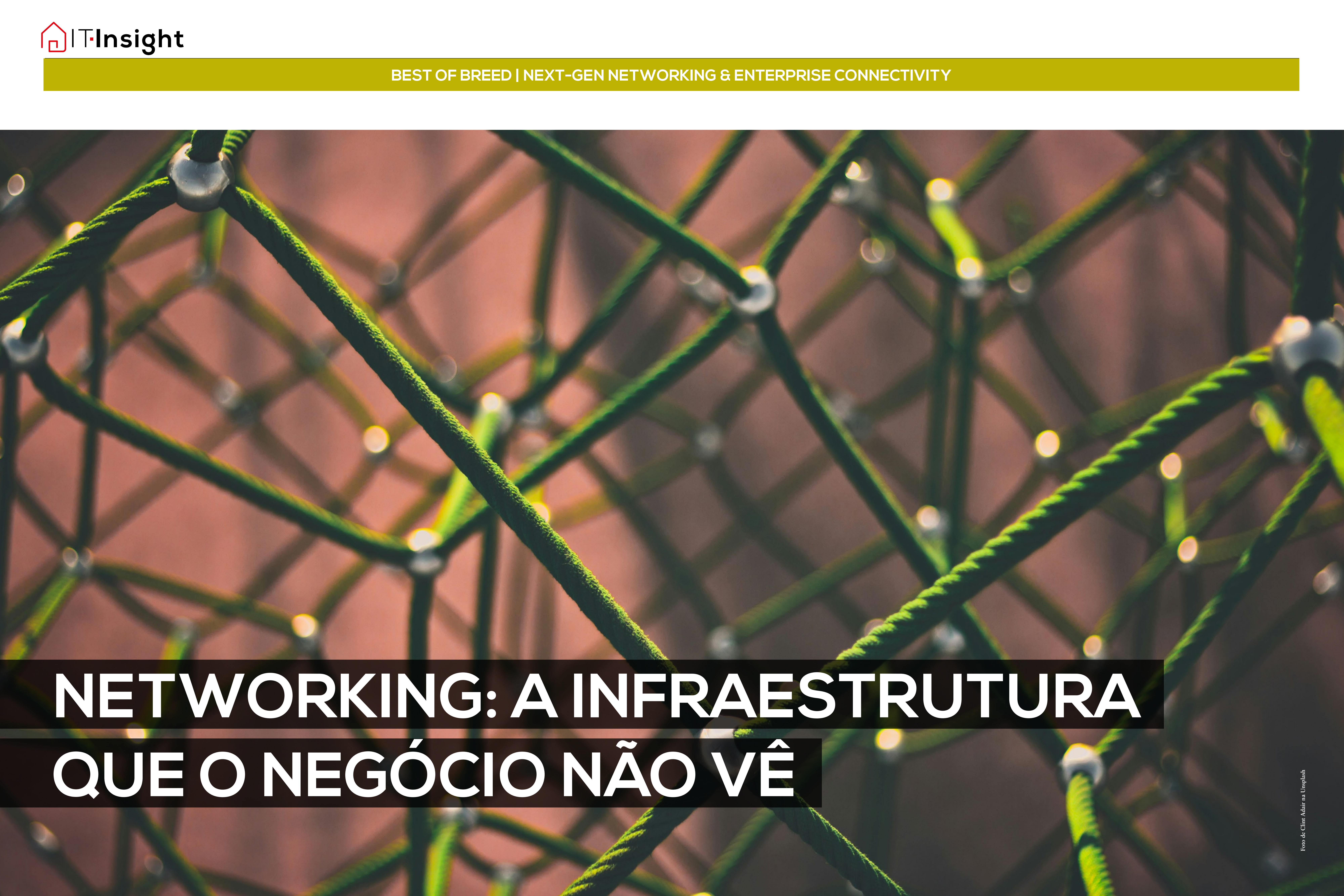
sentido que temos de assumir que os atacantes vão estar sempre à nossa frente. Acho que temos de assumir isso claramente. Nós vamos estar atrás. Temos de gerir muito bem as prioridades. Costumo dizer que, todos os anos, tenho uma prioridade clara, independentemente de passarmos muito tempo a fazer ‘*n*’ atividades dentro da organização: a prioridade é não ter um incidente significativo para as operações do grupo; esta é a prioridade. Acho que se nós definirmos muito bem aquilo que são as prioridades e não andarmos o tempo todo a correr atrás de coisas urgentes, eventualmente conseguimos gerir este tema um bocadinho melhor. Organizações em que na prática não gerem prioridades e gerem urgências, também acredito que é muito mais difícil chegar a esse ponto.

QUAIS SÃO OS CONSELHOS QUE OS CISO DEVEM TER EM CONTA NOS PRÓXIMOS ANOS?

Primeiro, penso que temos que mudar um bocadinho o paradigma da proteção e estar tão focados na proteção para um paradigma mais de resiliência operacional. A questão não é tanto se vamos sofrer um ataque, a questão não é tanto se vão conseguir, hão de conseguir mais cedo ou mais tarde; a questão é quão bem preparado estou eu para, quando isso acontecer, conseguir manter ou recuperar rapidamente a minha resiliência. É um bocadinho o conceito de *zero trust*, assumir que isto vai acontecer e como é que nós vamos conseguir lidar com isso, mantendo a operação a funcionar.

Em segundo lugar, a priorização. Falávamos há bocadinho que não conseguimos andar a correr atrás de tudo, não paramos o vento com as mãos. A única hipótese é priorizar, é conseguirmos definir, dentro daquilo que são os nossos programas de cibersegurança, aquilo que é efetivamente prioritário, aquilo que vai levar à tal resiliência operacional e tentarmos focar os recursos que temos naquilo que é prioritário, e que os nossos *roadmaps*, no fundo, acabem por refletir isso. Percebo que é muito bonito mostrar *roadmaps* para as gestões de topo, é espetacular ver não sei quantas iniciativas, mas é muito fácil depois chegar ao *burnout*, ou então ter que depois dizer que metade daquilo nós não conseguimos fazer.

Em terceiro, acho que há que aproveitar este paradigma da entrada em vigor da NIS2 e cada vez mais passar para modelos de gestão de risco. Basear aquilo que são as nossas decisões, não tanto naquilo que são os paradigmas tecnológicos, não tanto se calhar naquilo que é o *push* do mercado, mas efetivamente conseguir gerir risco adequadamente, conseguir comunicar risco adequadamente, porque creio que é isso que vai fazer com que haja visibilidade do ponto de vista de cibersegurança na gestão de topo e não uma visibilidade negativa, que estes tipos são chatos porque estão sempre a pedir dinheiro para investir aqui e ali, mas uma visibilidade do ponto de vista de risco para a organização e, ao mesmo tempo, se gerirmos risco, também eventualmente vamos conseguir priorizar melhor e evitar o *burnout* que creio que é realmente importante. ■



NETWORKING: A INFRAESTRUTURA QUE O NEGÓCIO NÃO VÊ

A rede empresarial nem sempre aparece nas conversas da administração, até ao dia em que falha. Conectividade, SD-WAN, Wi-Fi 7 e convergência com segurança são temas que vivem nos relatórios técnicos, mas cujas consequências chegam à margem operacional, à experiência do cliente e à velocidade de execução do negócio.

RUI DAMIÃO

A REDE não é apenas uma infraestrutura, mas sim uma estratégia das organizações. Para os CIO e CTO que gerem organizações em plena transformação digital, as decisões sobre conectividade empresarial têm hoje implicações que vão muito além da largura de banda ou do alcance do sinal Wi-Fi. **Segurança, resiliência operacional, suporte a modelos de trabalho híbridos e preparação para Inteligência Artificial (IA) passa tudo pela rede.**

Em 2025, o mercado global de SD-WAN valia cerca de 8,9 mil milhões e deverá mais do que duplicar até 2030, com uma taxa de crescimento anual composta superior a 12%, segundo a Data Intelligence. O Wi-Fi 7, a mais recente norma de

conectividade sem fios, representava já 31% das receitas do segmento *enterprise* de *access points* no terceiro trimestre e 2025, face a apenas 11% no início do mesmo ano, de acordo com a IDC.

CONVERGIR NÃO É OPCIONAL

O tema central desta geração de soluções de *networking* empresarial é, antes de mais, convergência. Convergência entre rede e segurança, entre gestão central e execução distribuída e entre conectividade com fios e *wireless*. A adoção de uma visão fragmentada (em que a rede, a segurança e a gestão vivem em silos separados) é cada vez mais identificada como um fator de risco operacional e financeiro.

A Gartner estima que, até 2026, 60% das novas aquisições de SD-WAN vão fazer parte de uma oferta *Secure Access Service Edge* (SASE) de fornecedor único, comparado com apenas 15% em 2022. **O mercado está a apontar para ter menos consolas de gestão, menos zonas cinzentas entre produtos de diferentes fabricantes e mais responsabilidade consolidada.**

Para a Fortinet, esta convergência é a espinha dorsal da proposta de valor. Hugo Azevedo, Business Development Manager e LAN Edge Specialist da Fortinet Portugal, resume a abordagem da empresa: “no centro desta estratégia está o conceito de Site Controller, suportado por um equipamento FortiGate, que funciona como

plano de gestão unificado para todo o *site*. Isto permite consolidar num único dispositivo como Secure SD-WAN, *routing*, *firewall* de próxima geração, controlo de *switching* e *wireless*, bem como capacidades de controlo de acessos”.

A simplificação que este modelo promete tem consequências diretas na operação, uma vez que leva a menos intervenções manuais, visibilidade *end-to-end* e uma superfície de ataque mais controlável. No entanto, também implica uma aposta num ecossistema fechado, com os *trade-offs* a que isso obriga.

A Cisco apresenta uma lógica semelhante, ainda que o portfólio seja mais extenso. Ricardo Silva, CTO & Leader, Sales and Solutions Engineering da Cisco Portugal, defende que a diferenciação está na profundidade da integração. “Somos a única empresa com uma arquitetura verdadeiramente convergente que une SD-WAN, Wi-Fi, *switching*, *routing* e segurança nativa, sem compromissos de



- Hugo Azevedo, Fortinet Portugal -

funcionalidade ou capacidade”, explica Ricardo Silva, acrescentando que “a cada solução Cisco que o cliente adiciona, tem o benefício específico da própria, assim como o efeito composto que acrescenta vantagens adicionais”.

WI-FI 7 ESTÁ A CHEGAR AO MERCADO

A norma Wi-Fi 7 (IEEE 802.11be) obteve certificação oficial em janeiro de 2024. Desde então, a curva de adoção em ambiente *enterprise* tem

“

É POSSÍVEL
CONSOLIDAR UM ÚNICO
DISPOSITIVO COMO
SECURE
SD-WAN, ROUTING,
FIREWALL DE PRÓXIMA
GERAÇÃO, CONTROLO
DE SWITCHING E
WIRELESS, BEM
COMO CAPACIDADES
DE CONTROLO DE
ACESSOS”

sido mais rápida do que a geração anterior: a IDC apontava para que o Wi-Fi 7 representasse 17% das receitas *enterprise* de *access points* até ao final de 2025, mas os números reais acabaram por superar essa projeção, chegando aos 31% no terceiro trimestre de 2025.

Em Portugal, o cenário tem especificidades próprias, até porque o Wi-Fi 6E nunca chegou a ter uma adoção expressiva. A maioria das organizações ainda opera em Wi-Fi 6, mas a procura pelo Wi-Fi 7 começou a acelerar de forma clara no segundo semestre de 2025.

Marilyne Michel, Head of D-Link Iberia and France, confirma que “a procura pelo Wi-Fi 7 está a acelerar desde o segundo semestre de 2025, impulsionada pela explosão dos usos da nuvem e da IA, bem como pelos preços cada vez mais competitivos. Esta procura provém principalmente de setores pioneiros como o turismo e as universidades”.

Há, no entanto, um constrangimento técnico que os decisores precisam de incorporar nos seus

planos de investimento: a infraestrutura de *switching* existente. A maioria dos *switches* de edge instalados nas organizações portuguesas e europeias, de uma forma geral, opera a 1 Gigabit. O Wi-Fi 7 pode atingir velocidades até 7.200 Mbps, mas esse potencial pode ficar estrangulado se os *access points* estiverem ligados a portas gigabits. A recomendação dos fabricantes é portas de, pelo menos, 2,5G, idealmente 10G.

“90% dos switches de extremidade são gigabit, o que representa um estrangulamento para o Wi-Fi 7”, alerta Marilyne Michel. Esta realidade transforma o que parecia ser uma simples troca de *access points* num projeto de modernização mais abrangente, e com o correspondente impacto no TCO.

Hugo Azevedo identifica um padrão de substituições diretas, sem revisão da arquitetura. “Existe uma tendência para substituições *like-for-like* que geram sobreprovisionamento. A adoção de uma estratégia *Wi-Fi first* implica reduzir infraestrutura fixa e redimensionar corretamente o *switching*,

evitando substituições diretas desnecessárias”, aconselha.

SD-WAN: DA RACIONALIZAÇÃO DE CUSTOS À PLATAFORMA DE IA

O argumento original do SD-WAN era, sobretudo, económico: substituir ou complementar circuitos MPLS dispendiosos por ligações de Internet com gestão inteligente de tráfego. Esse argumento mantém-se, mas ficou para segundo plano face a uma agenda mais ampla.

No mercado português, a Fortinet observa que o SD-WAN continua a ser impulsionado pela migração para serviços cloud, mas que a procura mais forte é, atualmente, pelo Wi-Fi *enterprise* seguro, que Hugo Azevedo designa como o movimento *Secure Wi-Fi First*. “O *wireless* tornou-se na principal tecnologia de acesso em escritórios modernos, suportando forças de trabalho móveis, aplicações colaborativas em tempo real e elevada densidade de dispositivos. Muitas organizações estão a otimizar infraestrut-



- Ricardo Silva, Cisco Portugal -

tura, reduzindo *switching* fixo e direcionando investimento para Wi-Fi de alto desempenho”, explica.

A Cisco aponta para a inteligência artificial como o vetor que redefine o valor do SD-WAN. As capacidades de IA que lançou no início de 2025 (que incluem o AgenticOps e a integração com ThousandEyes) são apresentadas como operacionais e não como promessas futuras. “Antecipa e evita degradação de aplicações, deteta anomalias

e acelera a sua resolução, até de forma autónoma, reduzindo o MTTR de horas para minutos”, descreve Ricardo Silva. “Não é uma *buzzword* – são funcionalidades operacionais que os nossos clientes já usam diariamente para ter redes mais resilientes, com menos intervenção manual e melhor experiência das aplicações e dos utilizadores”.

A Fortinet tem uma abordagem equivalente com o FortiAIOps, uma componente que a empresa considera verdadeiramente diferenciador para 2026: análise proativa baseada em inteligência artificial e machine learning, com identificação de causas raiz antes de qualquer disrupção chegar aos utilizadores finais.

“O OBJETIVO É ELIMINAR UM DOS MAIORES PROBLEMAS: AS ZONAS CINZENTAS ENTRE UMA SOLUÇÃO DE SEGURANÇA E OUTRA”

POSICIONAMENTOS DISTINTOS, NECESSIDADES DISTINTAS

Um dos aspetos mais relevantes para os decisores portugueses é perceber que os três fabricantes aqui presentes não competem exatamente no mesmo espaço e que essa distinção tem implicações práticas.

A Cisco domina o mercado de Wi-Fi *enterprise* com uma quota de 37,4% das receitas globais no terceiro trimestre de 2025 (segundo a IDC) e é reconhecida como líder no Magic Quadrant da Gartner para SD-WAN. A proposta para o mercado português assenta em dois vetores principais: a plataforma Meraki, vocacionada para organizações que preferem gestão SaaS e máxima

simplicidade operacional, e o ambiente Catalyst, para quem quer controlo total *on-premises* e elevada capacidade de configuração. Ricardo Silva explica que “é muito simples e resolvido numa pergunta”: se é pretendido uma gestão SaaS, ou se se quer uma plataforma de gestão *on-premises* e totalmente controlada pelo cliente.

A Fortinet, também reconhecida como líder no Magic Quadrant para SASE, para SSE, para SD-WAN e Enterprise Wired and Wireless LAN Infrastructure da Gartner, apela a organizações que valorizam a convergência nativa de rede e segurança acima de tudo. O cliente típico português, de acordo com Hugo Azevedo, é “uma organização em processo de digitalização que procura consolidar *networking* e segurança num modelo mais eficiente e resiliente, evitando soluções baseadas em múltiplos produtos isolados e estruturas fragmentadas”. Setores como indústria, retalho e serviços financeiros são referidos como casos de uso privilegiados.

AD-Link ocupa um espaço diferente. Presente junto das PME, ganha cada vez mais quota junto das grandes empresas e no setor industrial. Marilyne Michel rejeita a etiqueta de ‘marca de baixo custo’ e reivindica o que chama de “pragmático premium”, ou seja, a D-Link oferece “o mesmo poder tecnológica que os fabricantes premium, mas sem a carga orçamental frequentemente associada às empresas globais. Se ser ‘Value’ significa permitir que um hotel na Madeira ou uma fábrica em Braga se equipem com um Wi-Fi 7 ultrarrápido sem sacrificar a sua margem operacional, então somos esse ator e reivindicamo-lo com orgulho”.

Em Portugal, onde a larga maioria das empresas são PME, este argumento tem alcance real. A D-Link identifica hotéis, alojamentos locais, escolas e administração pública como clientes prioritários, setores onde a conectividade é crítica para a experiência do cliente ou para operações, mas onde os recursos internos de IT são tipicamente limitados.

O QUE OS PROJETOS ENSINAM

Para além dos posicionamentos de mercado, interessa perceber o que acontece quando estas soluções são implementadas. Portugal tem sido historicamente um *early adopter* em SD-WAN e SDN; Ricardo Silva refere explicitamente que “Portugal sempre foi reconhecido internacionalmente como um *early adopter* de sucesso nas tecnologias de SD-WAN, DAS e ACI”, o que significa que há experiência acumulada no mercado.

Um aspeto que os três fabricantes sublinharam é a importância do planeamento prévio. As falhas nas implementações raramente se devem a limitações tecnológicas, mas sim a planeamento insuficiente, ao mau dimensionamento do ambiente RG, à subestimação da complexidade de integração com sistemas legados ou à falta de envolvimento executivo para remover bloqueios operacionais.

A D-Link apresenta um caso concreto: uma empresa parceira que gere redes de hotéis em

“

A PROCURA PELO
WI-FI 7 ESTÁ A
ACCELERAR DESDE
O SEGUNDO
SEMESTRE DE 2025,
IMPULSIONADA PELA
EXPLOSÃO DOS USOS
DA NUVEM E DA IA,
BEM COMO PELOS
PREÇOS CADA VEZ
MAIS COMPETITIVOS”



- Marilyne Michel, D-Link Iberia and France -

Portugal e Cabo Verde implementou uma solução 100% *wireless* com Wi-Fi 7 e ligações 10G PoE num edifício de escritórios: dez *access points* DAP-E9560 e três *switches* DXS-1210-10MP, geridos pelo controlador Nuclias Connect. “A solução é praticamente *plug and play*, não houve nenhuma dificuldade na implementação e o cliente continua extremamente satisfeito após todos estes meses sem nenhuma paragem”, refere Marilyne Michel.

Nos projetos de maior escala, a abordagem da Fortinet passa por uma arquitetura modular baseada em *templates* dimensionados por tipologia de site, de XS a XXXL, com pilotos validados antes do *rollout* total. A componente de governação executiva é explicitamente identificada como fator crítico: sem envolvimento da liderança para remover bloqueios, os projetos alinham.

Por sua vez, a Cisco salienta os ganhos de automação que distinguem os seus projetos: “o tempo de projeto é muito menor *versus* a nossa concorrência pela nossa capacidade de criação de perfis e automação completa da rede, logo desde a sua implementação. Sendo ainda mais notório em projetos de grandes dimensões”.

SEGURANÇA, O FIO QUE LIGA TUDO

Não existe hoje uma conversa sobre *next-gen networking* que não passe, inevitavelmente, pela segurança. A adoção massiva de cloud e SaaS, o modelo híbrido de trabalho, a proliferação

de dispositivos IoT e OT nas instalações, tudo isto aumentou a superfície de ataque de forma significativa.

A Cisco aponta para o seu investimento em segurança nativa como elemento diferenciador, começando no desenho dos próprios *chips*, com uma visão zero-trust universal e políticas centralizadas aplicáveis a componentes de segurança de diferentes fabricantes. “O objetivo é eliminar um dos maiores problemas: as zonas cinzentas entre uma solução de segurança e outra”, explica Ricardo Silva.

Na Fortinet, a segurança não é um módulo adicional, mas é o princípio organizador de toda a plataforma. O protocolo FortiLink estende a Security Fabric até aos *access points*, com microsegmentação e controlo de acesso à rede desde o momento da ligação. Para ambientes com dispositivos IoT industriais, esta capacidade é particularmente relevante, uma vez que permite segmentar tráfego OT sem depender de soluções externas.

A questão do *lock-in* é, neste contexto, incontornável.

Ricardo Silva defende que a Cisco tem uma filosofia aberta, com participação nos *standards* e interoperabilidade multivendor onde necessário, e que a fidelização resulta do valor gerado, não de restrições artificiais. Hugo Azevedo reconhece os *trade-offs* da abordagem Fortinet: existe um equilíbrio entre custo e resiliência e a transição para um modelo *security-driven* implica decisões sobre depreciação de ativos existentes e planeamento faseado.

O QUE OS DECISORES DEVEM RETER

As três perspetivas recolhidas convergem em alguns pontos essenciais para os decisores portugueses.

A infraestrutura de *switching* é o gargalo real da adoção de Wi-Fi 7. Antes de decidir sobre *access points*, é necessário avaliar o estado dos *switches* de extremidade. Migrar para portas MultiGigabit não é opcional se se quiser extrair valor real do Wi-Fi 7 e esse custo tem de entrar nos cálculos de TCO desde o início.

A convergência rede-segurança deixou de ser uma tendência para se tornar num requisito operacional. Gerir redes e segurança como entidades separadas aumenta complexidade, custo e risco. A questão não é se convergir, mas a que ritmo e com que modelo de transição.

O planeamento continua a ser o fator que separa implementações bem-sucedidas de projetos que falham as expectativas. Dimensionamento RF, envolvimento executivo, gestão da depreciação de ativos legados e pilotos validados antes do *rollout* total são praticamente que aparecem, de forma consistente, nas histórias de sucesso.

E, por fim, a escolha do fabricante deve ser conduzida por adequação às necessidades reais da organização, não por posicionamento de mercado. Uma PME portuguesa do setor da hotelaria tem requisitos muito diferentes de uma organização industrial com ambientes OT complexos ou de uma empresa financeira com dezenas de filiais. O mercado oferece, hoje, opções sólidas para cada um desses perfis. ■



POR FILIPE FRASQUILHO,
Diretor de Serviços TI da IP Telecom

NEXT-GEN NETWORKING & ENTERPRISE CONNECTIVITY

O tema Next-Gen Networking e Enterprise Connectivity centra-se na modernização das infraestruturas de TI que suportam a transformação digital, o trabalho híbrido e a explosão de dispositivos IoT.

HOJE, O MAIOR ERRO das organizações é ver a rede apenas como um custo. As empresas que a tratam como um **ativo estratégico** conseguem lançar produtos digitais de forma significativamente mais rápida que a concorrência.

O objetivo passa por abandonar o modelo tradicional baseado em hardware simples e gestão manual, evoluindo para redes inteligentes, automatizadas e altamente seguras.

As redes deixaram de ser ligações passivas para a troca de informação e tornam-se num ativo fundamental, capaz de adaptar às necessidades de conectividade das empresas, dos utilizadores e dos dispositivos.

Tecnologias como **Network as Code** - onde a infraestrutura de rede é tratada como software, permitindo implementar redes completas em minutos, com configurações padronizadas e replicáveis em qualquer localização, **Edge Networking & AI** - que tira partido de modelos de IA nos equipamentos de Edge para processar dados junto dos utilizadores, reduzindo drasticamente a latência, **Redes Sustentáveis** - que recorrem a otimização inteligente de rotas e gestão energética de portas e equipamentos para reduzir a pegada de carbono dos Datacenters e **Quantum-Safe Networking** – com a aplicação de protocolos criptográficos que permitem uma segurança adicional



- Filipe Frasilho -
Diretor de Serviços TI da IP Telecom

através da computação quântica para proteger dados transmitidos, são algumas das tendências atuais das redes empresariais.

Contudo, a implementação destas tendências enfrenta desafios relevantes. A automação não elimina a complexidade — e as redes cresceram em funcionalidades, aumentando também a sua dificuldade de gestão.

Alguns desses desafios são a **Escassez de Talentos**, na medida em que existe um gap significativo entre o perfil tradicional do analista de redes (focado em CLI/hardware) e as exigências modernas que incluem competências de programação (Python, APIs e modelos Cloud), a **Complexidade de ambientes Multi-Cloud e On-Prem** onde a integração políticas de segurança consistentes entre diferentes plataformas é um enorme desafio operacional, a **Interoperabilidade entre Fabricantes**, em que muitos fornecedores mantêm ecossistemas fechados, dificultando a criação de redes realmente unificadas e finalmente a **Segurança e Visibilidade**, onde cada dispositivo, seja IoT ou outro, e cada utilizador remoto, representam um

potencial ponto de entrada numa rede descentralizada, exigindo controlo contínuo.

As oportunidades, porém, são vastas. A telemetria avançada da rede permite entender os comportamentos dos utilizadores/consumidores passando para modelos de gestão como serviço, transformando CAPEX em OPEX.

Estas redes possibilitam ainda que robôs e AGVs (veículos autónomos) se movam livremente com ligações muito estáveis e seguras, garantindo **Resiliência Cibernética** adicional ao tirar partido da IA para isolar ataques automaticamente, criando uma vantagem competitiva e evitando paragens de produção onerosas com impacto no negócio. Estas funcionalidades permitem que a rede identifique falhas de forma automática e as corrija sem intervenção humana (**Self-Healing**) assim como a configuração de novos dispositivos ser automatizada ao serem ligados à rede (**Provisionamento Zero-Touch**), tornando a operação mais eficiente e segura. Para que estas funcionalidades possam ser uma realidade é necessário garantir a Visibilidade e Observabilidade com IA (**AIOps**) de modo a

entender o que acontece em cada milissegundo e ter uma **Análise Preditiva** e uma **Root Cause Analysis** efetiva de diagnóstico instantâneo de problemas complexos nas ligações complexas que devem ser isoladas em cada segmento de modo a garantir que as ameaças não sejam espalhadas pela totalidade da rede (**Microsegmentação**).

A transição para estas tecnologias é motivada principalmente pela necessidade de acesso ultrarrápido a aplicações SaaS e pela urgência de garantir segurança num contexto onde o perímetro da empresa é global.

A **IP Telecom** destaca-se por combinar a competitividade no mercado das redes para Datacenters Empresariais e Edge Computing com a garantia de **soberania dos dados**, tirando partido do posicionamento estratégico de Portugal nas comunicações internacionais. Esta vantagem geográfica e infraestrutural potencia a **interligação global**, assegurando que estas tecnologias e funcionalidades avançadas de gestão de redes se tornam um verdadeiro fator **diferenciador** para as organizações. ■

“A LUÍS SIMÕES PASSOU A ENCARAR A TECNOLOGIA COMO UM ACELERADOR DE EFICIÊNCIA, ESCALABILIDADE E DIFERENCIAÇÃO”

Com uma renovação dos sistemas core e maior maturidade em integração e cibersegurança, o CIO da empresa de logística e transportes revela como a tecnologia passou a ser um vetor central de eficiência e escalabilidade no negócio logístico.

MARTA QUARESMA FERREIRA



ANDRÉ SANTOS é o nome por detrás da evolução tecnológica e digital da Luís Simões.

A desempenhar o cargo desde 2023, o CIO destaca a jornada de consolidação da “visão do IT como área estratégica”, que integra tanto a criação de valor para o negócio, como a transformação do modelo operacional da empresa portuguesa de logística e transporte, fundada na década de 1940, que é já uma referência em toda a Península Ibérica.

Os tempos são agora outros e o ímpeto do desenvolvimento tecnológico, tal como revelam os dados do estudo “Desafios de Talento em Logística”, do

ManpowerGroup, em parceria com a Associação Portuguesa de Logística, destacam a transformação digital como a principal prioridade estratégica do setor.

Em entrevista à IT Insight, André Santos afirma que tem existido uma “renovação significativa dos sistemas *core*”, em áreas como a logística e transportes, com a **transformação a refletir-se num “reforço claro da camada de integração entre aplicações e uma maior maturidade em temas como cibersegurança e governação tecnológica”**.

Neste ponto, o CIO explica que “a Luís Simões passou a encarar a tecnologia, não apenas como suporte à operação, mas como um verdadeiro acelerador da eficiência, da escalabilidade e da diferenciação num setor altamente competitivo”.

O VALOR NA GESTÃO DA TECNOLOGIA E DA INOVAÇÃO

A estratégia de transformação digital da organização, explica André Santos, está hoje assente na eficiência operacional, na visibilidade *end-to-end*

da cadeia logística e na melhoria da experiência de colaboradores e clientes.

Com o objetivo de tornar os processos mais integrados e suportados, a empresa portuguesa tem apostado na implementação de novos sistemas de gestão de transportes e de armazéns, na harmonização de processos entre geografias e na melhoria da experiência digital interna.

“A inovação tecnológica deixou de ser pontual e passou a fazer parte do dia a dia, com maior proximidade às áreas operacionais, maior foco na adoção das soluções e também numa governação que privilegia decisões informadas, rapidez de execução e simplicidade”, revela.

O PAPEL DAS TECNOLOGIAS EMERGENTES NA TRANSFORMAÇÃO DOS PROCESSOS

O negócio tem-se adaptado à inevitável evolução tecnológica, numa integração que tem decorrido de “forma pragmática” e orientada “a casos de uso concretos”.



- André Santos -
CIO, Grupo Luís Simões

Entre as tecnologias emergentes, André Santos identifica **a cloud híbrida como um garante de flexibilidade, escalabilidade e resiliência, permitindo “manter o controlo sobre os sistemas críticos”**; outro dos destaques vai para a automação inteligente, onde os maiores beneficiários



são os processos operacionais e administrativos. A equação fica completa com a inteligência artificial generativa, explorada “de forma ética e responsável” e, sobretudo, “como ferramenta de apoio à produtividade e à análise de informação” na operação.

Numa era de dados, a área de transporte e logística também não é exceção, pelo contrário: a importância estratégica do tema levou a Luís Simões criar uma Direção de Dados em janeiro de 2025 de forma a acompanhar a tendência, garantindo

uma maior previsibilidade e uma gestão mais informada.

A disponibilização de dados consistentes contribui igualmente para suportar decisões rápidas e informadas ao longo da cadeia de valor. O acesso a dados fiáveis tem permitido às equipas operacionais tomarem “decisões com maior confiança”, num setor “onde o tempo e a eficiência são críticos”.

MEDIR O PULSO À TRANSFORMAÇÃO

A tríade que alinha estratégia, tecnologia e pessoas é, na visão de André Santos, **o fator-chave para o sucesso de uma organização no processo de transformação digital, que só pode ser bem-sucedida “quando existe uma visão clara do que se pretende alcançar, uma liderança comprometida e uma forte aposta na adoção e na mudança cultural”**, e acrescenta: “a tecnologia é um meio, não um fim”.

Para o CIO, um dos principais desafios que se impõe nesta jornada prende-se com “o equilíbrio

entre a continuidade operacional de um negócio crítico e a implementação de mudanças estruturais profundas”. Por outro lado, é igualmente necessário “assegurar o alinhamento” entre as diferentes áreas e geografias para garantir “consistência sem perder agilidade”.

A cibersegurança é uma das prioridades para a próxima fase, a par da “consolidação dos sistemas core implementados” e do “reforço da arquitetura de integração”, assim como a utilização de dados como suporte à decisão operacional e estratégica.

Ao projetar o futuro, André Santos considera o diretor de IT vai assumir um papel “cada vez mais híbrido”, numa equação que inclui “um sólido domínio tecnológico”, acompanhado por “uma profunda compreensão do negócio, capacidade de liderança e visão estratégica”. **“O CIO assume-se, cada vez mais, como um agente de transformação, focado na criação de valor, na gestão da mudança e no impacto real da tecnologia nos resultados da organização.** É isto que tento, no meu dia a dia, assumir desde já”, conclui. ■

SAMSUNG

Galaxy S26 Ultra
Galaxy AI ✨

SAMSUNG GALAXY S26 REFORÇA IA,
DESEMPENHO E PRIVACIDADE

Samsung apresenta a série Galaxy S26 com IA mais autónoma, melhorias significativas de performance, novo ecrã com Privacy Display integrado e foco reforçado na segurança.

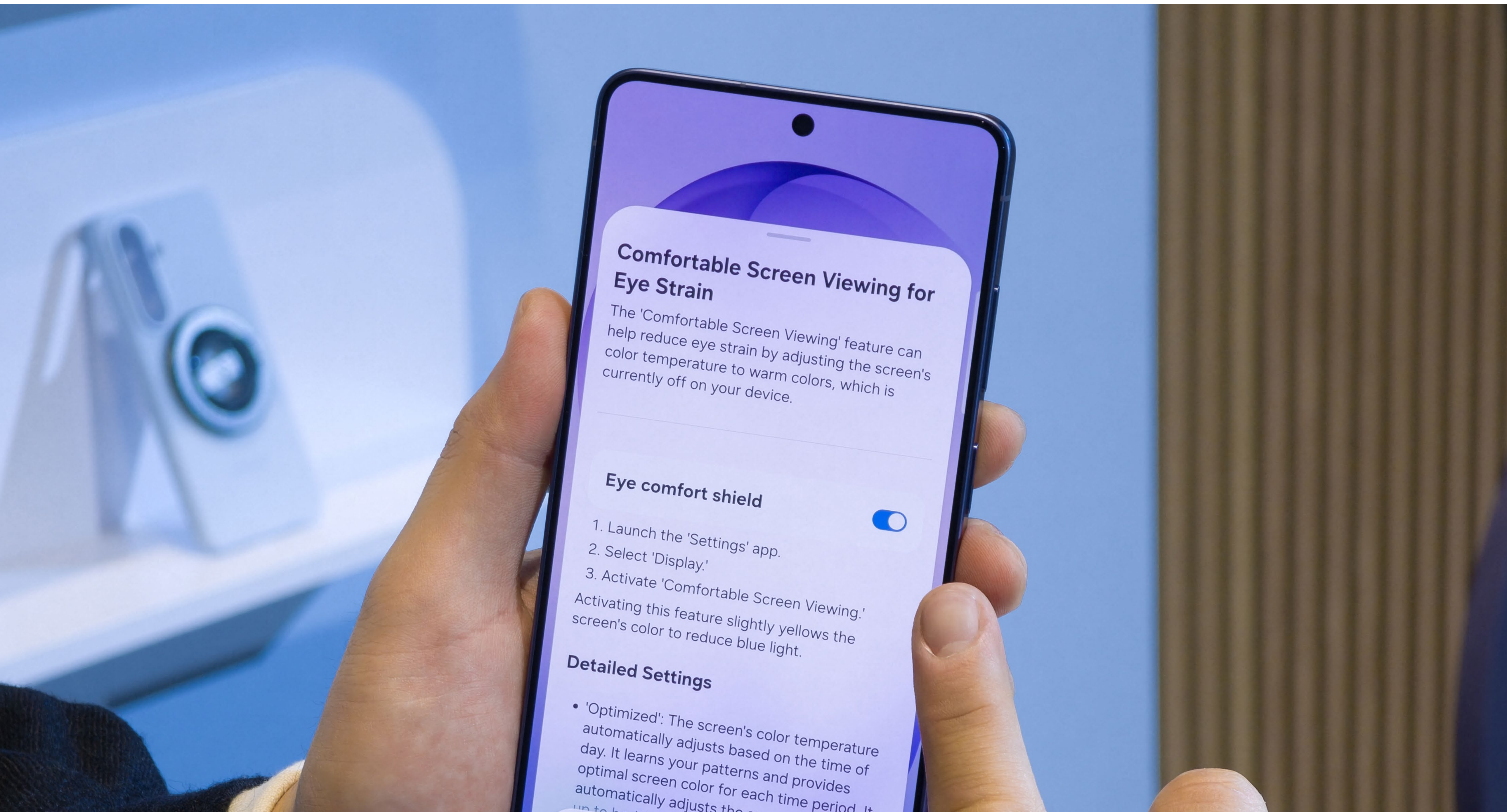
A SAMSUNG ELECTRONICS anunciou a nova série Galaxy S26, composta pelos modelos Galaxy S26, S26+ e S26 Ultra, posicionando-a como a geração mais avançada de smartphones Galaxy com Inteligência Artificial (IA). A nova linha aposta numa experiência mais fluida e proativa, combinando hardware de elevado desempenho, sistema de câmara aprimorado e camadas adicionais de proteção de dados.

Segundo a marca, o objetivo é tornar a IA praticamente invisível, operando em segundo plano para reduzir o esforço e o número de passos necessários nas tarefas do quotidiano.

IA MAIS PROATIVA E ADAPTATIVA NO DIA A DIA

A série Galaxy S26 integra a evolução do Galaxy AI, concebido para antecipar necessidades e simplificar interações. A tecnologia passa a atuar de forma





contextual, sugerindo ações relevantes e automatizando tarefas.

Funcionalidades como Now Nudge apresentam sugestões em tempo real, por exemplo, recomendando automaticamente fotografias recentes quando um contacto solicita imagens de uma

viagem. Já o Now Brief surge mais personalizado, propondo *playlists* de exercício ou alertas com base no contexto individual.

O Circle to Search com Google foi melhorado com reconhecimento multiobjeto, permitindo identificar diferentes elementos numa única imagem,

desde peças de vestuário a acessórios, numa única pesquisa.

A série oferece ainda integração com múltiplos assistentes (Bixby, Gemini e Perplexity) possibilitando a execução de tarefas complexas através de comandos de voz ou um simples toque. A realização de ações em múltiplas etapas, como reservar um táxi, pode ser feita de forma quase automática.

DESEMPENHO DE TOPO COM FOCO EM EFICIÊNCIA

No centro do Galaxy S26 Ultra está o novo processador Snapdragon 8 Elite Gen 5 Mobile Platform for Galaxy, otimizado para IA, eficiência energética e estabilidade térmica.

A Samsung anuncia melhorias até 19% no desempenho do CPU, 39% no NPU e 24% no GPU. Ao mesmo tempo, o modelo Ultra integra ainda uma Vapor Chamber redesenhada, com novo sistema

de dissipação térmica que distribui melhor o calor, garantindo desempenho consistente mesmo em gaming, multitarefa intensiva ou gravação de vídeo.

Em termos de autonomia, o Super-Fast Charging 3.0 permite carregar até 75% da bateria em cerca de 30 minutos, segundo a própria empresa.

A experiência visual é reforçada com tecnologias proprietárias como o ProScaler, que melhora a nitidez de texto e detalhe, e o mDNiE, que aumenta a precisão de cor face à geração anterior.

SISTEMA DE CÂMARA MAIS INTELIGENTE E VERSÁTIL

A nova geração aposta num sistema de captação e edição totalmente integrado, facilitando a criatividade sem necessidade de conhecimentos técnicos avançados.



O Galaxy S26 Ultra apresenta aberturas de lente mais amplas para melhor desempenho em baixa luminosidade, Nightography Video melhorado, estabilização Super Steady com bloqueio horizontal e processamento AI ISP também otimizado para selfies.

O equipamento estreia o suporte ao APV (*Advanced Professional Video*), um novo *standard* de compressão profissional que permite vídeo de elevada qualidade com compressão eficiente.

Na edição, o Photo Assist permite alterações através de linguagem natural, como transformar uma cena diurna em noturna ou restaurar partes de uma imagem. O Creative Studio centraliza ferramentas de criação para gerar conteúdos como convites, autocolantes ou *wallpapers* personalizados.

Ferramentas como o Document Scanner com IA removem automaticamente distorções e organizam múltiplas imagens num único PDF.

PRIVACIDADE REFORÇADA A NÍVEL DE HARDWARE

Um dos principais destaques é o novo Privacy Display integrado no Galaxy S26 Ultra, descrito como o primeiro do setor com proteção de privacidade embutida no próprio ecrã.

A tecnologia controla a dispersão da luz ao nível dos pixéis, limitando a visibilidade lateral quando ativada, sem comprometer a qualidade para o utilizador. O modo pode ser configurado para ativação automática em situações como introdução de PIN ou utilização de aplicações específicas.

A série inclui ainda encriptação pós-quântica (PQC) para processos críticos, atualizações ao Knox Matrix, AI-powered Call Screening, alertas de privacidade com deteção de acessos sensíveis, álbuns privados integrados na Galeria e sete anos de atualizações de segurança.

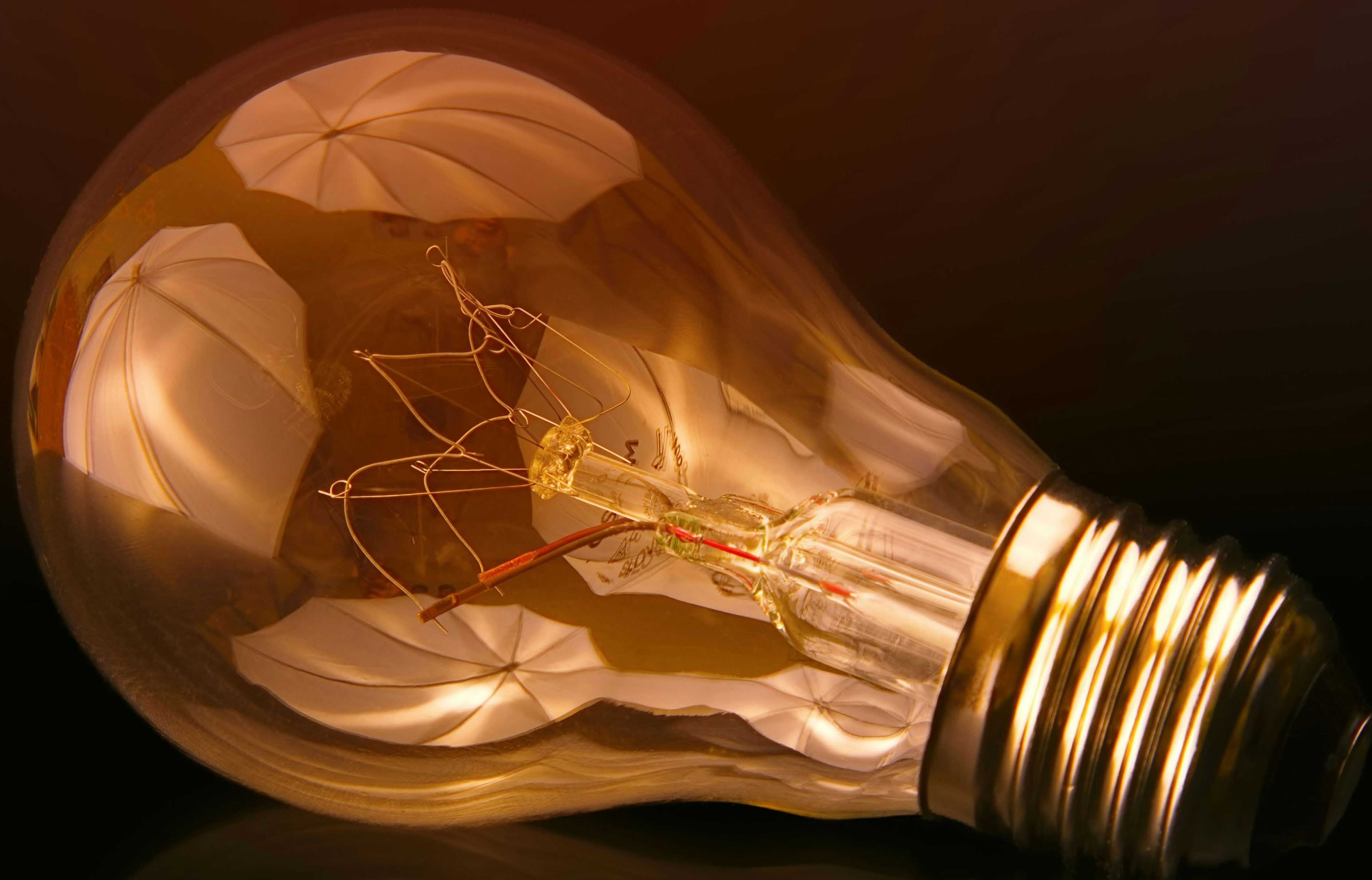
A proteção é suportada pela plataforma Samsung Knox, combinando segurança ao nível do hardware e software.



DISPONIBILIDADE

A série Galaxy S26 da Samsung fica disponível em Portugal a partir de 11 de março, nas cores Cobalt Violet, White, Black e Sky Blue, além de opções exclusivas online como Pink Gold e Silver Shadow.

Com esta nova geração, a Samsung reforça a sua aposta numa experiência móvel centrada em IA autónoma, alto desempenho e proteção avançada de dados, posicionando o Galaxy S26 como um dos lançamentos mais ambiciosos da empresa. ■



EDP-DXC TRANSFORMA IA EM OPERAÇÃO COM FÁBRICA DE MODELOS

A EDP enfrentava um problema comum em empresas maduras em dados, com muitos modelos de IA difíceis de operar. Para resolver, lançou, em parceria com a DXC, uma framework de MLOps que transforma protótipos em soluções que funcionam no dia a dia.

INÊS GARCIA MARTINS

A EDP está a dar um passo decisivo na forma como leva a Inteligência Artificial (IA) do laboratório para a operação. Num contexto em que o número de modelos de machine learning cresce rapidamente em diferentes áreas do grupo, desde a previsão de consumo à manutenção preditiva, a empresa avançou para a criação de uma *framework* organizacional de Machine Learning Operations (MLOp), em parceria com a DXC Technology e com suporte tecnológico da Microsoft.

O objetivo passa por **acelerar a passagem de protótipos para produção, reduzir esforço manual e garantir governança e rastreabilidade num ciclo de vida cada vez mais complexo.**

Mais do que um projeto tecnológico, trata-se de uma mudança estrutural na forma como a organização transforma dados em decisões e automação, com impacto direto na eficiência e na escalabilidade da IA.

O DESAFIO DA EDP

A EDP já vinha a reforçar a utilização de inteligência artificial em múltiplas frentes, mas o crescimento orgânico de projetos e equipas começou a expor um problema típico de organizações maduras em dados que passa pela falta de consistência e de processos comuns entre iniciativas.

Como explica a própria empresa, “**à medida que o número de modelos e casos de uso cresceu em diferentes áreas do Grupo, tornou-se imperativo estabelecer uma *framework* corporativa que assegurasse consistência, rastreabilidade e qualidade em todo o ciclo de vida dos modelos de IA**”.

Este desafio não era apenas técnico, mas principalmente organizacional, uma vez que os projetos desenvolvidos em momentos diferentes, com ferramentas distintas e maturidades desiguais, dificultavam a reutilização, a escalabilidade e a manutenção sustentável.

A DXC enquadra este tipo de problema como recorrente em grandes organizações europeias, onde os modelos acabam frequentemente por ficar presos entre provas de conceito e produção. Um dos sintomas mais críticos era o tempo necessário para colocar modelos em produção, agravado por integrações complexas com *pipelines* de dados e sistemas existentes, já que “apenas uma em cada dez organizações consegue colocar em produção mais de 75% dos seus protótipos de IA”, segundo o responsável da DXC que citou um estudo da Gartner.

O resultado era um cenário comum em empresas que já provaram o valor da IA, mas ainda não a industrializaram, com modelos relevantes, mas difíceis de operacionalizar de forma rápida, repetível e auditável.

DA EXPERIMENTAÇÃO A UMA “FÁBRICA DE MODELOS”

A resposta da EDP foi assumir o MLOp como uma etapa estratégica de maturidade, com o objetivo



- Nuno Moura Pinheiro -
Head of Data & AI na DXC, Portugal



de “*padronizar e industrializar os processos de desenvolvimento, implementação e manutenção de modelos de machine learning*”.

Nuno Moura Pinheiro, Head of Data & AI na DXC em Portugal reforça esta ideia ao definir MLOp como “a prática que se dedica à integração dos modelos de machine learning nos processos de negócio e aplicações”, suportada por uma *framework* de software, automatismos e boas práticas para acelerar desenvolvimento e operação.



APENAS UMA EM CADA DEZ ORGANIZAÇÕES
CONSEGUE COLOCAR EM PRODUÇÃO MAIS DE 75%
DOS PROTÓTIPOS DE IA”

O projeto decorreu em três fases bem estruturada que refletem, por sua vez, uma abordagem típica de transformação, incluindo aconselhamento, implementação e operacionalização.

Na fase inicial, foram realizados os *workshops* “As Is”, “To Be” e “Roadmap”, para mapear maturidade, alinhar *stakeholders* e definir arquitetura e modelo operacional. Esta metodologia permitiu garantir que a tecnologia respondia a necessidades reais e que a mudança era aceite por diferentes áreas.

A EDP descreve esta etapa como um processo transversal, liderado pelo Centro de Excelência de Data & AI, mas envolvendo também áreas críticas como Arquitetura Global, Cibersegurança e Gestão de Risco em IA.

A SOLUÇÃO TECNOLÓGICA

Na fase de implementação, a DXC aplicou um princípio que se tornou quase uma assinatura dos seus projetos de modernização bem-sucedidos, assente na lógica de “Pensar em Grande”, “Começar Pequeno” e “Escalar Rapidamente”.

O núcleo da solução foi construído com base na abordagem DXC Quickstart for MLOp, de modo a tirar partido de ativos reutilizáveis e aceleradores já desenvolvidos pelo Centro de Excelência Europeu da empresa. Estes aceleradores, segundo a DXC, funcionam como serviços nativos em plataformas

como Azure, Databricks ou AWS, sendo altamente configuráveis e adaptáveis ao caso de uso.

A relevância desta componente tornou-se evidente, já que permite reduzir o tempo de implementação e diminuir custos de engenharia repetitiva, proporcionando “a evolução de uma abordagem artesanal, assente na criatividade dos artesões, para uma abordagem industrial”.

Do ponto de vista técnico, a implementação não deixou margem para experimentalismos. Assentou em práticas hoje incontornáveis quando se fala de IA à escala empresarial, com *pipelines* de integração e entrega contínua, uma abordagem GitOps para gerir a movimentação de ativos entre ambientes, versionamento rigoroso de dados e modelos, mecanismos de linhagem que garantem rastreabilidade e reprodutibilidade e módulos preparados para monitorização permanente e deteção de *drift*.

A deteção de *drift*, ou seja, identificar quando um modelo começa a perder precisão devido a mudanças nos dados reais, é particularmente crítica em empresas como a EDP, onde o comportamento do consumo, redes ou ativos pode mudar com a sazonalidade, o clima, as alterações regulatórias ou novas dinâmicas de mobilidade elétrica.

Ao mesmo tempo, a EDP sublinha que esta *framework* reforça a *governance* “através de práticas de versionamento, auditoria, gestão de risco e deteção

de *drift*”, o que garante, por sua vez, transparência e confiança na evolução dos modelos.

ESCALA EM AÇÃO

Depois de construída a base técnica, a fase de operacionalização foi decisiva para aplicar a *framework* em casos reais, garantindo que o MLOp não ficava apenas como *blueprint*.

A EDP não ficou pela teoria e escolheu três frentes onde a IA teria impacto mensurável. O Electric Dots antecipa os melhores locais para instalar postos de carregamento de veículos elétricos, cruzando dados para reduzir risco e acelerar decisões. A previsão de chamadas no Contact Center permite estimar procura e ajustar recursos com maior precisão, num contexto em que eficiência operacional pesa diretamente nos custos. Já a detecção automática de portas por computer vision apoia equipas no terreno com identificação rápida e fiável, aproximando o algoritmo da operação diária. Estes três casos distintos, unidos têm como objetivo comum transformar dados em decisões com efeito prático.

Os modelos vão muito além do *analytics* organizacional e têm impacto direto na infraestrutura, nas operações, no planeamento de recursos e na produtividade das equipas técnicas, domínios onde o retorno se mede em

eficiência, tempo e custos. É neste contexto que o MLOp ganha relevância, ao oferecer uma *framework* capaz de sustentar, no mesmo ecossistema, modelos preditivos para o contact center, soluções geoespaciais aplicadas à mobilidade elétrica e algoritmos de visão computacional que apoiam operações no terreno.

IMPACTOS MEDIDOS

Os resultados apresentados pela DXC apontam para ganhos claros de industrialização, com destaque para a aceleração do *deployment*. Um dos indicadores mais relevantes foi a redução do tempo de colocação em produção “de meses para semanas”, resultado direto da automatização e normalização dos processos.

A inovação da DXC **transforma a operação empresarial através de processos mais eficientes e automatizados aumentam a produtividade, enquanto a escalabilidade permite integrar IA em ambientes complexos**. Os custos caem à medida que se reduz a intervenção manual e se automatiza a manutenção, e a tomada de decisão torna-se mais sólida graças a governance rigorosa e monitorização constante. Quatro impactos estratégicos que provam que a tecnologia só é relevante quando altera a forma como a organização funciona.

Na EDP, a evolução ganha forma na previsibilidade e na sustentabilidade, com rastreabilidade completa, reprodutibilidade assegurada, governance reforçada e menor esforço manual em tarefas repetitivas. A experiência demonstra que a criação de modelos é apenas o ponto de partida e que o verdadeiro valor da IA está na sua gestão consistente e sustentada no tempo.

A DIMENSÃO HUMANA E ORGANIZACIONAL

Para lá do peso tecnológico, o projeto evidencia um ponto que muitos programas de IA desvalorizam, a necessidade de reorganização cultural. A EDP descreve o processo como um exercício de colaboração transversal, com envolvimento ativo de equipes de negócio e áreas críticas como cibersegurança e gestão de risco em IA.

Nuno Moura Pinheiro destaca a urgência de quebrar silos e aponta como um dos problemas centrais a “falta de colaboração entre equipes”, com desenvolvimento e produção a trabalhar de forma isolada.

A transformação concretizou-se não na simples criação de *pipelines* automatizados, mas na construção de um modelo operacional comum, capaz de fazer com que diferentes áreas falem a mesma linguagem desde a concepção do modelo até à sua validação, implementação e monitorização.

MLOP COMO BASE PARA IA

Enquanto o mercado debate IA generativa, copilotos e automação inteligente, o case EDP-DXC prova que a IA não cresce sozinha. Sem uma base operacional sólida, modelos sofisticados permanecem no papel e nunca chegam à escala.

A DXC distingue entre uma abordagem tática e outra estratégica, cada uma com objetivos e impactos próprios dentro da transformação empresarial. A tática entrega resultados rápidos, mas tende a criar uma “cultura artesanal de modelos”, dispendiosa e difícil de sustentar. Já a abordagem estratégica exige uma prática estruturada de MLOp, criando um ambiente de “fábrica” que estabiliza e acelera todo o ciclo de vida.

A EDP, por sua vez, enquadra este projeto como parte direta da sua estratégia de transformação digital e de IA, onde fundações comuns e práticas transversais são vistas como essenciais para criar valor sustentável.

À medida que mais organizações adotam IA, a diferença competitiva vai deixar de estar em “ter modelos” e passa a estar em “operar modelos” com confiança, ética, governança e eficiência, integrando a inteligência artificial de forma consistente nas operações e decisões do negócio. ■

O REFÚGIO GOURMET NO CORAÇÃO DA TRADIÇÃO PORTUGUESA



A MERCEARIA TÓME afirma-se como um espaço para quem valoriza produtos gastronómicos com história e autenticidade. É onde se encontram iguarias tradicionais, ingredientes selecionados e sugestões que celebram a cultura alimentar portuguesa. Entre compotas artesanais, queijos curados e propostas sazonais de menu, o espaço articula mercearia e cozinha, valorizando a matéria-prima e uma abordagem contemporânea à tradição. ■

BRANCO PREMIADO QUE ELEVA A BEIRA INTERIOR



A REGIÃO da Beira Interior continua a ganhar destaque no mapa vinícola português. Desta vez, o destaque vai para o Quinta da Biaia, o vinho branco que já tem lugar entre os melhores. Este vinho, feito com a casta da região, Síria, combina frescura aromática com a elegância e a intensidade, que traduzem o seu carácter singular. Com uma estrutura e um perfil único, é uma descoberta obrigatória para quem valoriza a autenticidade. ■

PESTANA DUNAS PORTO SANTO INAUGURA EM ABRIL



PORTO SANTO, na Madeira, conquista pela pausa. Entre as dunas e o silêncio, descobre-se o novo Pestana Dunas Porto Santo, que abre portas em abril para trazer uma proposta que privilegia a proximidade à natureza e o conforto. Neste destino atlântico, a experiência constrói-se ao ritmo da ilha, através da areia dourada, dos horizontes abertos e dos dias que se prolongam sem pressa, num cenário onde o que realmente importa ganha espaço. ■



Do satélite diretamente ao seu smartphone

A 26 de fevereiro, a Virgin Media O2 lançou no Reino Unido o O2 Satellite, o primeiro serviço europeu a ligar smartphones directamente a satélites LEO com tecnologia Starlink Direct-to-Cell. Para já, permite mensagens e dados quando não existe cobertura móvel terrestre. O próximo passo poderá chegar pela Vodafone, em parceria com a AST SpaceMobile, que prepara 4G e 5G com as todas as funcionalidades habituais directamente via satélite ainda em 2026.

OBRIGADO POR TER LIDO A IT Insight

Para continuar a receber regularmente a sua IT Insight, por favor atualize os seus dados profissionais [aqui](#)

Conheça a política de privacidade da IT Insight [aqui](#)

IT Insight

PUBLISHER: Jorge Bento 

DIRETOR: Henrique Carreiro

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

COORDENADORA EDITORIAL: Marta Quaresma Ferreira

REDAÇÃO: Inês Garcia Martins e Flávia Gomes

GESTÃO DE PARCEIROS:

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

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

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

MARKETING & COMMUNICATIONS: Rita Rodrigues

ARTE E PAGINAÇÃO: Teresa Rodrigues

FOTOGRAFIA: Rui Santos Jorge

ILUSTRAÇÕES E IMAGENS: Adobe Stock e DALL-E

DESENVOLVIMENTO WEB: Global Pixel

A REVISTA DIGITAL INTERATIVA IT INSIGHT É EDITADA POR:
MediaNext Professional Information Lda.

GERENTE: Pedro Botelho

SEDE E REDAÇÃO: Largo da Lagoa, 7c, 2795-116
Linda-a-Velha, Portugal

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

PERIODICIDADE: Bimestral

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

Consulte [aqui](#) o Estatuto Editorial

PROPRIEDADES E DIREITOS

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

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

Editado por:

IT Insight é membro de:

