

**ANÁLISE**



**Sharp Inspire Expo 2026**

14

**EM FOCO**



**O negócio do Canal em 2026**

40

**TEM A PALAVRA**



**Pedro Vieira, HP Portugal**

16

**DELL** Technologies  
AUTHORIZED DISTRIBUTOR

DATABOX, o seu Distribuidor Autorizado DELL

## Qualidade Líder da Indústria

Modernize o local de trabalho e transforme o futuro do seu negócio com uma oferta unificada e um portefólio de equipamentos preparados para a era da IA.

**Databox**  
Informática, S.A.

🌐 Saiba mais em [www.databox.pt](http://www.databox.pt)

✉ [databox@databox.pt](mailto:databox@databox.pt)

☎ 214 308 400  
chamada para rede fixa nacional

A CPCDI recomenda Windows 11

# CPCDi

## Os PCs DI com AMD RYZEN vieram QUEBRAR TODAS AS REGRAS



# Windows 11



## VAMOS PROGREDIR EM CONJUNTO COM O WINDOWS 11 PRO

O suporte ao Windows 10 terminou dia 14 de outubro de 2025. Atualize para o Windows 11 Pro e garanta mais **segurança, flexibilidade e produtividade**

## O DESEMPENHO QUE O LEVA MAIS LONGE

- Ryzen 7 9800X3D
- ASUS TUF GAMING X870-PLUS WIFI
- ASUS TUF-RTX5070TI-O16G-GAMING
- SSD M.2 NVMe Serie 990 PRO 2TB c\ Dissipador
- 32GB 6000MT/s DDR5 CL30 FURY Beast RGB



[WWW.CPCDI.PT](http://WWW.CPCDI.PT)

Conheça a APP CPCDI

Disponível para sistema operativo Android e IOS.



Porto: R. Monte dos Pupos, 649 | 4460-059 Guifões | Tel 22 9570200 | Fax 22 955 26 58  
Lisboa: Largo da Lagoa 8-E | 2795-116 Linda-a-Velha | Tel 21 4148200 | Fax 21 419 29 93

Intel, the Intel logo, Intel Core, and Core Inside are trademarks of Intel Corporation in the U.S. and other countries.



## Novos Suportes de Secretária **Full-Motion Napofix**

Os novos suportes Full-Motion Napofix oferecem ajuste total do monitor, garantindo ergonomia e eficiência em ambientes profissionais. Compatíveis com monitores 13" a 32".

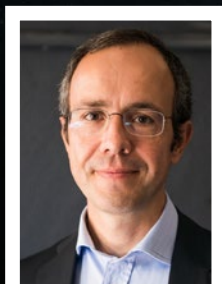
**Conheça os Novos Modelos Napofix**  
no seu Distribuidor Habitual

*Referências disponíveis na Webshop ALSO:*  
DM2110B | DM2110W | DM2130S | DM2130G

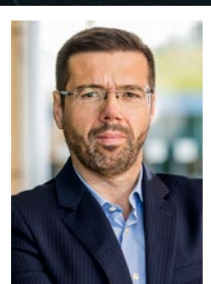


## CIBERSEGURANÇA

# Quem liderar a ciber**SEGURANÇA** domina o mercado



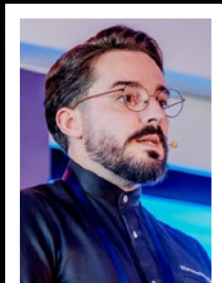
CYBERINSPECT



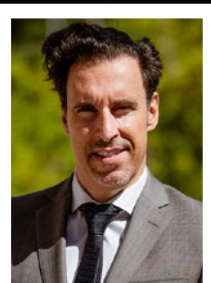
ESET



FORCEPOINT



MANAGEENGINE



VISIONWARE



V-VALLEY



WATCHGUARD



**12** ANÁLISE | RED HAT  
SIMPLIFICA PROGRAMA DE CANAL  
E REFORÇA COMPETÊNCIAS

**46** CASE STUDY | INCENTEA  
CAIADO CONSOLIDA SEGURANÇA  
E REFORÇA PARCERIAS

**47** PARCEIRO DO MÊS | XPLOR  
APOSTA EM ESPECIALIZAÇÃO PARA  
AJUDAR ORGANIZAÇÕES

## SÓNIA CASACA DEIXA HPE ARUBA



**Protagonistas** Sónia Casaca vai sair da HPE Networking, anteriormente conhecida como HPE Aruba. A Country Manager deixa a empresa ao fim de sete anos e indica que o futuro passa “pelo universo de cibersegurança”. Sónia Casaca entrou na HPE Aruba em 2019 como Sales & Channel Manager, tendo assumido a pasta de Country Sales Manager em maio de 2023. Antes, esteve em empresas como Arrow ECS, Exclusive Networks, Magirus Portugal e Tech Data.

## PABLO COLLANTES É O NOVO COUNTRY MANAGER DA WATCHGUARD EM PORTUGAL



**Protagonistas** A WatchGuard Technologies nomeou Pablo Collantes como novo Country Manager para Portugal e Espanha, atribuindo-lhe a responsabilidade de liderar a estratégia de crescimento da empresa na região ibérica. A nomeação surge num contexto de reforço da aposta da empresa em cibersegurança unificada para organizações e prestadores de serviços geridos (MSP). Collantes substitui Álvaro García Abarrio que deixou a fabricante em outubro de 2025.

## ATOS NOMEIA NOVO COUNTRY MANAGER PARA PORTUGAL

**Protagonistas** A Atos anunciou a nomeação de Daniel Luz como



novo Country Manager para Portugal. O responsável assume funções com o objetivo de dar continuidade à estratégia de crescimento, inovação e excelência operacional da organização no mercado nacional. Daniel Luz é licenciado em Organização e Gestão de Empresas e conta com mais de 15 anos de experiência na Atos Portugal.

## MÁRIO LOPES ASSUME LIDERANÇA DO GRUPO GIGAS EM PORTUGAL E DIREÇÃO COMERCIAL DA ONI



**Protagonistas** O Grupo Gigas anunciou a nomeação de Mário Lopes como novo Country Manager em Portugal, função que acumula com a Direção Comercial da ONI. A decisão insere-se na estratégia de crescimento do grupo no mercado português e no reforço da posição da ONI junto de clientes empresariais e Parceiros internacionais.

## ARROW E DARKTRACE ASSINAM ACORDO DE DISTRIBUIÇÃO NA EMEA

**Parcerias** A Arrow Electronics anunciou a assinatura de um acordo de distribuição com a Darktrace para a região EMEA, permitindo aos Parceiros de Canal da Arrow disponibilizar o portfólio completo de soluções da Darktrace. O acordo abrange proteção de cloud, rede, email, ambientes industriais OT e endpoint.

## ESPRINET REFORÇA PARCERIA COM A MICROSOFT

**Parcerias** A Esprinet anunciou o reforço da sua Parceria estratégica com a Microsoft. A empresa foi selecionada como novo Parceiro exclusivo de distribuição de software e acessórios Xbox em Portugal e Espanha. Esta decisão assenta na relação de longa data e bem-sucedida entre a Esprinet e a Microsoft em Itália. Com a extensão da Parceria à Península Ibérica, é criado um centro unificado de distribuição no Sul da Europa, permitindo aumentar a escala, a eficiência operacional e o impacto no mercado em toda a região.

## TD SYNnex ALARGA DISTRIBUIÇÃO DO BRICSCAD A TODA A EUROPA ATRAVÉS DA DATECH

**Parcerias** A TD Synnex revelou a ampliação da disponibilidade do BricCAD em todo o mercado europeu através da Datech, a sua unidade dedicada a software de design. A decisão dá continuidade à colaboração iniciada no início deste ano na região das Américas e reforça a presença da solução CAD junto dos Parceiros europeus.

## COMMVAULT REFORÇA PARCERIA COM GOOGLE CLOUD

**Parcerias** A Commvault anunciou a expansão da sua colaboração com a Google Cloud, com o objetivo de reforçar as capacidades de proteção de dados, segurança e ciber-resiliência para clientes empresariais. A Commvault introduziu novas capacidades integradas numa única plataforma, focadas em proteção imutável, recuperação acelerada de dados e aplicações cloud e suporte a requisitos de conformidade.

## MITEL REFORÇA PROGRAMA GLOBAL DE PARCEIROS

**Parcerias** A Mitel anunciou um Programa Global de Parceiros

reforçado, com o objetivo de alinhar de forma mais eficaz o ecossistema de Parceiros com a evolução do mercado das comunicações híbridas. O novo Programa assenta nas melhorias introduzidas em 2025 na experiência dos Parceiros e incorpora *feedback* recolhido a nível global, procurando criar maior consistência, previsibilidade e foco em crescimento sustentável.

## IBM ANUNCIA AQUISIÇÃO DA CONFLUENT

**Aquisições** A IBM chegou a acordo para adquirir a Confluent, uma empresa de infraestrutura de dados, nativa na cloud. O acordo, avaliado em 11 mil milhões de dólares, pretende ampliar a oferta da IBM na área de *cloud computing* de forma a responder à procura crescente, impulsionada pela IA. A Confluent oferece uma plataforma de *streaming* de dados corporativos *open source* que conecta, processa e governa dados reutilizáveis e confiáveis em tempo real, fundamentais para a implementação de IA

## SEALPATH CRESCE MAIS DE 55% EM 2025

**Resultados** A SealPath encerrou 2025 com um crescimento de vendas superior a 55%, consolidando a sua estratégia de internacionalização e o posicionamento da sua tecnologia no mercado global de cibersegurança. O crescimento foi particularmente expressivo em regiões onde a procura por soluções de soberania de dados tem vindo a intensificar-se. Na América Latina, a empresa registou um crescimento superior a 500%, impulsionado pela consolidação de novos enquadramentos regulatórios de proteção de dados e pelo aumento da exigência em torno do controlo da informação. No Médio Oriente e no sul da Europa, o crescimento superou os 100%. ■



## ASUS ExpertBook B3 B3405

# AI PC, configurado para si

O ASUS ExpertBook B3 AI PC oferece uma personalização extensiva para potenciar as suas necessidades empresariais do dia-a-dia. Equipado com o mais recente processador Intel® Core™ Ultra 7 com Intel vPro®, NPU Intel AI Boost e gráficos Intel® Arc, este AI PC oferece uma performance sólida para lidar com uma vasta gama de tarefas sem compromissos. Inclui ferramentas de IA como o ASUS AI ExpertMeet, o Microsoft Copilot e a tecnologia AI Noise Canceling, proporcionando uma experiência de produtividade inigualável. Com durabilidade de classe militar, uma gama completa de portas de I/O, Wi-Fi 6E ultrarrápido e funcionalidades de segurança avançadas, este AI PC leve garante flexibilidade e eficiência em movimento. Além disso, com uma bateria de longa duração, imagem e áudio excepcionais, e um design amigo do ambiente, o ASUS ExpertBook B3 suporta um fluxo de trabalho sustentável e simplificado - mantendo a produtividade em qualquer lugar.



Intel® Core™ Ultra 7 processor powering Intel vPro®, Built for Business

SAIBA MAIS EM: <https://www.asus.com/pt/laptops/for-work/expertbook/asus-expertbook-b3-b3405/>

## RIS 2048 ADQUIRIDA PELA BECHTLE

As marcas RIS e Evoware (antiga Evonic) vão continuar a operar, agora debaixo da alçada do Bechtle Group, que amplia assim o seu portfólio de consultoria e serviços de IT em Portugal

**A** Bechtle anunciou a aquisição da portuguesa RIS 2048. Em comunicado, a Bechtle refere que o integrador português, fundado em 2000 e com sede em Aveiro e escritório em Lisboa e no Porto, vai continuar a operar sob as marcas RIS e Evoware (antiga Evonic), agora inseridas no Bechtle Group.

Atualmente, a RIS e a Evoware empregam, em conjunto, 165 trabalhadores, com receitas superiores a 50 milhões de euros em 2025. A Bechtle amplia, assim, o portfólio de consultoria e serviços de IT em Portugal.

De acordo com a Bechtle, os cofundadores e ex-acionistas maioritários Luís Catalão, que

lidera a RIS 2048, e Nuno Silva, Diretor Geral da Evoware, vão continuar à frente dos respetivos negócios.

O acordo agora anunciado tem como objetivo acelerar o crescimento dentro de uma grande organização europeia, reforçando a estratégia de aquisições europeias da Bechtle.

John Malone, Vice-Presidente Executivo do Sul e Leste da Europa da Bechtle AG, destaca o “grande sucesso” que o grupo tem obtido em Portugal e Espanha nos últimos anos. Sobre esta mais recente aquisição, John Malone refere que o negócio agora anunciado “dá um impulso significativo e reforça a ambição de estar entre os cinco maiores fornecedores de serviços da Península Ibérica até 2030. As equipas da RIS



e da Evoware representam um avanço notável para o Grupo Bechtle”.

Em comunicado, Luís Catalão, cofundador, ex-acionista maioritário e Diretor Executivo da RIS, afirma que existem “oportunidades significativas de longo prazo para acelerar o nosso crescimento como parte de um grupo europeu de IT financeiramente forte e voltado para o futuro. Há equipas excelentes a unirem-se de ambos os lados, criando sinergias substanciais, fortalecendo-se mutuamente, o que nos permite conquistar uma fatia clara de mercado”. ■

## CISCO APRESENTA NOVO PROGRAMA GLOBAL DE PARCEIROS

A Cisco anunciou o Cisco 360 Partner Program, um novo modelo global criado com Parceiros para responder à era da IA, reforçar a rentabilidade e acelerar resultados para os clientes

**A** Cisco anunciou o lançamento do Cisco 360 Partner Program, um novo Programa global de Parceiros desenvolvido ao longo de 15 meses em co-criação com o seu ecossistema. A iniciativa visa reforçar a colaboração com Parceiros e simplificar a forma como estes ajudam os clientes a responder aos desafios da era da Inteligência Artificial (IA), em áreas como data centers preparados para IA, ambientes de trabalho preparados para o futuro e resiliência digital.

Concebido para diferentes modelos de negócio, como *developers*, consultores, *managed services providers*, *resellers* e distribuidores, o Cisco 360 Partner Program pretende oferecer maior clareza, previsibilidade de ganhos e diferen-



ciação baseada em valor e especialização. Em paralelo, a Cisco lançou uma nova ferramenta - o Cisco Partner Locator -, que permite aos clientes identificarem facilmente Parceiros qualificados em áreas como segurança,

*networking*, colaboração, serviços, Splunk e infraestrutura cloud e de IA.

Num artigo publicado no blog da Cisco, Tim Coogan revela que “a transformação do mercado tecnológico obrigou a repensar o modelo de Parceria”. O Senior Vice President sublinha que cerca de 90% das receitas da Cisco passam pelo ecossistema de Parceiros, o que torna a sua rentabilidade e sucesso um indicador central do desempenho da própria empresa.

O Cisco 360 Partner Program evolui o modelo anterior para alinhar melhor as prioridades da Cisco, dos Parceiros e dos clientes. Um dos pilares é o Cisco Partner Incentive (CPI), já em vigor, que consolida Programas anteriores e oferece um modelo de incentivos mais simples e previsível, alinhado com o *roadmap* da Cisco. A empresa introduziu ainda bónus temporários associados a especializações estratégicas, como Secure Networking e Secure AI Infrastructure, válidos até julho de 2026. ■

# GCC SERIES

A solução tudo-em-um que redefine UC & Networking, substitui múltiplos equipamentos e converge toda a infraestrutura de IT numa única plataforma

 Firewall

 VPN

 IP PBX

 Router

 Switch



## Gestão centralizada

Gestão de funcionalidades UC, rede e segurança totalmente centralizada.

Gestão de todas as funcionalidades da plataforma GCC através de um único ponto de administração.



## Plataforma completa

Gestão em nuvem ou local para todos os dispositivos Grandstream.

Automatize atualizações, manutenção e aprovisionamento de forma remota e segura.



## Segurança máxima

Segurança avançada integrada na infraestrutura de rede.

Proteção de comunicações, acessos e dados críticos com Firewall NGFW, VPNs, IDS/IPS, DPI e encriptação.

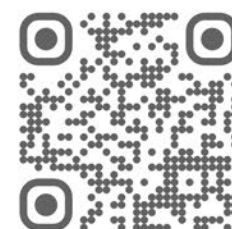
Distribuidor exclusivo em Portugal

 **VOXSYS**

 [www.voxsys.pt](http://www.voxsys.pt)

 [info@voxsys.pt](mailto:info@voxsys.pt)

 300 40 40 40



Em alternativa, poderá usar o número (+351) 21 919 7220. Custo da chamada para rede fixa nacional.

## CANAL DEVERÁ GERAR MAIS DE QUATRO BILHÕES DE DÓLARES EM VENDAS EM 2026

Previsões da Omdia apontam para um crescimento anual de 6,7%, num mercado de IT que deverá ultrapassar os seis bilhões de dólares

**A**s vendas realizadas através do Canal deverão gerar mais de quatro bilhões de dólares em valor a nível global em 2026, impulsionadas por um crescimento anual de 6,7%. A previsão é avançada pela Omdia, que estima que o mercado global de IT cresça mais de 10% este ano, ultrapassando os seis bilhões de dólares em investimento total.

De acordo com a empresa, cerca de dois terços do investimento global em IT continuará a ser mediado pelo Canal, apesar de uma ligeira redução face a 2025, quando os Parceiros representavam pouco mais de 70%



do mercado endereçável. Esta alteração reflete o peso crescente dos investimentos diretos dos *hyperscalers* em infraestruturas de inteligência artificial.

O forte aumento do investimento em cloud — incluindo novos modelos como GPU-as-a-Service e neoclouds — está a impulsionar um crescimento anual de 18% no investimento direto dos fabricantes e fornecedores. Ainda assim, a Omdia sublinha que os Parceiros continuam a ser decisivos nas decisões de compra, sobretudo em áreas como integração, serviços geridos, consultoria e transformação digital.

“Os serviços de IT deverão crescer ao ritmo mais rápido dos últimos anos, embora o hardware e o software continuem a crescer a um ritmo superior”, refere Jay McBain, Chief Analyst da Omdia, numa antevisão do estudo. Apesar do cenário de crescimento, o relatório destaca os desafios que o ecossistema do Canal enfrenta. A aceleração da Inteligência Artificial (IA), a mudança nos modelos de consumo tecnológico e as novas expectativas de fabricantes e clientes estão a redefinir o papel tradicional dos Parceiros, privilegiando serviços, especialização e resultados de negócio em detrimento da simples revenda. ■

## MERCADO EUROPEU DE MANAGED SERVICES MOSTRA SINAIS DE RECUPERAÇÃO

A procura por serviços tecnológicos na Europa registou um novo máximo no final de 2025, impulsionada pelo crescimento da inteligência artificial, da cloud e pela recuperação dos serviços geridos, segundo o mais recente ISG Index

**A** procura por serviços tecnológicos na Europa atingiu um novo máximo no quarto trimestre de 2025, registando o melhor desempenho trimestral do ano, impulsionada pelo crescimento acelerado da cloud, da Inteligência Artificial (IA) e pela recuperação dos serviços geridos, segundo o mais recente relatório setorial da Information Services Group (ISG).

De acordo com o EMEA ISG Index, que acompanha contratos de *outsourcing* comercial com um valor anual igual ou superior a cinco milhões de dólares, o valor anual contratado (ACV) combinado, que inclui serviços geridos

e soluções cloud as-a-Service, cresceu 27% no quarto trimestre, alcançando um recorde de 10,9 mil milhões de dólares. Este foi o oitavo trimestre consecutivo de crescimento do mercado combinado na região, com uma média de expansão de 16% nesse período.

“A Europa guardou o melhor para o fim do ano, com uma procura acelerada por serviços cloud impulsionados por IA, combinada com um novo dinamismo nos serviços geridos, o que resultou no trimestre mais forte de 2025”, afirmou Anthony Drake, presidente da ISG EMEA. O responsável destaca ainda o aumento da procura por serviços de engenharia associados à IA e o crescimento do valor médio



dos contratos, sinalizando maior confiança à entrada em 2026.

O ACV dos serviços geridos aumentou 19% em termos homólogos no quarto trimestre, para 4,6 mil milhões de dólares, e cresceu 21% face ao trimestre anterior. Foram atribuídos 298 contratos neste segmento, o que representa o melhor resultado trimestral do ano, incluindo três “mega negócios” (contratos com valor anual superior a 100 milhões de dólares), mais do que no mesmo período do ano anterior. ■



# 28 MAIO, 2026 | LISBOA

Lisbon Secret Spot, Montes Claros

**channel**   
itchannel conference

  
CHANNEL  
AWARDS  
2026  
itchannel

**CONFERENCE | WORKSHOPS | NETWORKING**

**O principal evento independente para integradores e MSPs**

**Tendências. Desafios. Networking. E o reconhecimento da indústria aos melhores Parceiros.**

Tudo o que interessa e acontece no Canal, converge no **Channel ON**. Marque na sua agenda: dia 28 de maio, em Montes Claros.

Pensado de parceiros para parceiros, o **Channel ON** é o ponto de encontro essencial para debate, partilha de conhecimento e networking qualificado, onde se analisam as principais tendências do setor, os temas críticos do presente, os desafios que irão moldar o futuro do canal e se **reconhecem os melhores Parceiros de 2026, na Cerimónia de entrega de Prémios Channel Awards, que encerra a edição de 2026.**

Com conteúdo independente e imparcial, o **Channel ON** oferece informação estratégica e formação relevante nas áreas mais sensíveis para **Integradores de Sistemas, MSPs e VARs**, apoiando a tomada de decisões num mercado em constante transformação.

O **Channel ON** reúne as principais empresas parceiras de canal do mercado português – responsáveis por uma parte significativa da integração e revenda de tecnologia de informação – com especial enfoque nos Parceiros que atuam no mercado empresarial e setor público.

Venha fazer parte de um ambiente único e exclusivo de **networking profissional**, promover relações estratégicas e novas oportunidades de negócio.

**inscreva-se já**

**Conf.itchannel.pt**

Revista IT CHANNEL | [www.itchannel.pt](http://www.itchannel.pt)

# Red Hat simplifica Programa de Canal e reforça foco em competências

A Red Hat introduziu alterações no seu Programa de Parceiros com o objetivo de simplificar a estrutura e aumentar a previsibilidade para o Canal, com foco num mercado orientado para serviços, cloud híbrida e automação

por Marta Quaresma Ferreira



está alinhado com a prioridade de escalar no segmento *Commercial* – aquele com maior potencial na região em termos de volume de empresas –, permitindo que os Parceiros locais sejam o motor de inovação na digitalização do tecido empresarial português, apoiando-se na robustez, flexibilidade e capacidade de inovação da Red Hat”, justifica Javier García Fiaño.

Com uma estratégia global centrada na “democratização da inovação tecnológica através do código aberto”, a Red Hat pretende oferecer às organizações a possibilidade de construir, implementarem e gerirem qualquer aplicação a partir de qualquer ambiente, desconstruindo a complexidade associada à infraestrutura.

“Pretendíamos eliminar silos e simplificar a forma como os Parceiros colaboram connosco, concentrando-nos na forma como prestam serviços de elevado valor acrescentado sobre a nossa oferta e maximizam o valor das nossas tecnologias no contexto específico de cada cliente”, reitera o Manager.

**M**ais simplificação e uma maior transparência. A Red Hat anunciou um conjunto de melhorias no seu Programa de Canal, que pretende posicionar-se como um pilar central na estratégia *go-to-market* da organização.

Numa altura em que o mercado exige agilidade, flexibilidade e capacidade de adaptação, Javier García Fiaño, Iberia Ecosystem Manager da Red Hat, explica ao IT Channel que os clientes “já não procuram apenas produtos, mas soluções integradas que abrangem desde o data center até ao edge e à cloud”.

Este contexto tem contribuído para acelerar a evolução do Canal para modelos mais orientados à entrega de serviços e projetos. Javier García Fiaño não tem dúvidas de que o ecossistema de Parceiros evoluiu de um modelo de “revenda” para assumir o papel de cocriador de valor. Esta mudança, aliada à crescente complexidade associada à gestão de ambientes de cloud híbrida e à integração de tecnologias como a

Inteligência Artificial (IA) generativa, culminou numa revisão à estrutura do Programa de Parceiros da Red Hat, que passa a apostar numa abordagem mais flexível e baseada em competências por domínio.

## AS MAIS-VALIAS PARA O ECOSISTEMA PORTUGUÊS

Desenhado para apoiar os Parceiros na criação, venda e entrega de soluções baseadas em *open source*, com foco em cloud, *hybrid cloud*, automação e plataformas de aplicações, a estratégia por detrás das mudanças do Programa passa por reduzir a complexidade associada à infraestrutura e clarificar a forma como os Parceiros se posicionam ao longo do ciclo de vida dos projetos. As competências e especializações ganham novo fôlego e a estratégia está agora mais alinhada com o Canal de Parceiros português, mais orientado para serviços e projetos.

“Portugal dispõe de uma rede de Parceiros com uma capacidade técnica muito elevada e um forte foco em serviços. O Programa



Javier García Fiaño, Iberia Ecosystem Manager da Red Hat

## O PARCEIRO NO CENTRO DO PROJETO

As alterações anunciadas refletem uma maior valorização do papel do Parceiro ao longo do ciclo de vida do projeto, através de incentivos para especialização técnica e prestação de serviços com, segundo a Red Hat, impacto direto na rentabilidade.

Para o Manager, “a grande diferença está na simplificação e na transparência”, uma vez que a empresa passou de ter “vários Programas fragmentados para uma estrutura unificada que reconhece diferentes modelos de negócio, desde integradores até fornecedores de serviços de cloud”.

Em paralelo, a nova plataforma digital de Parceiros foi desenhada para facilitar o acesso a ferramentas de capacitação e melhorar a visibilidade sobre incentivos, requisitos e evolução da relação com a Red Hat.

### ACELERAR O DESEMPENHO DO ECOSISTEMA

A aposta tecnológica da Red Hat para acelerar o desempenho do Canal continua assente na plataforma e no *open source* como base para cloud híbrida, automação e inteligência artificial.

Entre as soluções estratégicas, Javier García Fiaño destaca o Red Hat OpenShift, agora complementado com o Red Hat OpenShift AI, que permite aos Parceiros apoiarem os clientes na implementação e gestão de modelos de IA em ambientes híbridos.

Em Portugal, a automação tem ganho relevância na melhoria da eficiência operacional das infraestruturas, com o especialista a elencar o interesse crescente em projetos transversais de automação e AIOps.

### APERFEIÇOAR PARA CRESCER

No plano do negócio, a Red Hat identifica o aumento da previsibilidade como um dos principais benefícios das alterações introduzidas ao Programa. Os incentivos passam a ser mais claros, sobretudo para Parceiros com foco no segmento *Commercial*, permitindo um

planeamento mais consistente e seguro do crescimento.

“Para além disso, oferecemos um acesso mais direto a certificações e a recursos de engenharia. A oportunidade passa por deixar de ser um “fornecedor de tecnologia” para se tornar um Parceiro estratégico que apoia as empresas portuguesas na adoção de IA, da cloud híbrida e da automação, onde as margens associadas aos serviços são significativamente mais elevadas”, reitera. ■

### RESUMO

- A Red Hat anunciou melhorias ao seu Programa de Canal;
- Programa passa a ser mais modular, assente em competências, e com maior grau de previsibilidade;
- A cloud híbrida, a automação e a inteligência artificial são as áreas prioritárias para acelerar os projetos através do Canal.

# NOVA ERA DA DIGITALIZAÇÃO: SIMPLES E SEGURA

 imageFORMULA

DIGITALIZAÇÃO SEM SOFTWARE/DRIVERS

SEGURANÇA POR UTILIZADOR/FUNCIONALIDADES

GESTÃO REMOTA E CENTRALIZADA





**Canon DR-S250N**

Velocidade: 100 ipm (50ppm)  
Rede LAN + USB



**Canon ScanFront 400**

Velocidade: 90 ipm (45ppm)  
Rede LAN



**Canon DR-S350NW**

Velocidade: 100 ipm (50ppm)  
Rede LAN + Wi-Fi + USB

# Sharp reforça investimento no Canal para alavancar negócio europeu com foco em serviços

Durante a Inspire Expo 2026, em Lisboa, Joe Tomota, presidente da Sharp Europa, traçou o próximo capítulo da empresa na Europa, com foco numa abordagem mais integrada, orientada a serviços e ao ecossistema de Parceiros

por Marta Quaresma Ferreira

**A** Sharp Inspire Expo 2026 chegou a Lisboa para apresentar uma visão unificada e focada no futuro e no próximo capítulo da marca japonesa.

Num dia dedicado à imprensa, Joe Tomota, Presidente da Sharp Europa, começou por explicar que a Sharp está atualmente a iniciar um novo capítulo, mantendo o foco no acompanhamento do cliente, na compreensão das suas necessidades e na personalização das soluções. Sozinha, a Europa é responsável por 30% do negócio global B2B da Sharp. “É uma performance estável, que está crescer através da inovação, com a gestão dos documentos e serviços de *display*, agora combinados com a *expertise* de IT”, reforçou o presidente.

Em entrevista ao IT Channel, Joe Tomota considera que o mercado europeu de IT está a evoluir para um modelo mais orientado a serviços, com uma forte integração entre infraestrutura IT, aplicações e dados. O responsável reconhece, no entanto, que estas diferentes camadas ainda não estão totalmente integradas de forma homogénea em todo o continente europeu. “Estas três áreas ainda não estão completamente interligadas, e essa consolidação vai levar tempo”, admite, acrescentando que a abordagem terá sempre de ser ajustada às necessidades concretas de cada cliente.

## MERCADO EUROPEU FRAGMENTADO

Joe Tomota reconhece que competir no mercado de serviços de IT é cada vez mais complexo, não só porque a competição “é difícil”, mas também porque “os clientes enfrentam problemas muito semelhantes”.



Joe Tomota, Presidente da Sharp Europa

Ainda assim, a abordagem consultiva continua a ser um fator distintivo porque, perante uma solução desenhada especificamente para o cliente, a competição fica de lado. “Se a solução é tecnicamente complexa, mas simples para o cliente, a concorrência deixa de ser uma preocupação central”, afirma.

## TRABALHAR EM CONJUNTO COM OS PARCEIROS

Os Parceiros ocupam um lugar central na estratégia europeia da Sharp. O futuro é reforçado por uma ideia de força conjunta, onde a partilha de experiência e casos práticos é vista como essencial, sobretudo num contexto em que áreas tradicionais, como a impressão, enfrentam desafios. “O negócio de MFP já não tem, por si só, um futuro brilhante”, reco-

nhece o executivo, defendendo a necessidade de diversificação.

No âmbito do Canal, a Inspire Expo 2026 serviu de mote para apresentar as mais recentes novidades do fabricante, com destaque para o SharpOne.

Pensado para Parceiros, o novo portal é agora um *hub* para recursos de marketing, conteúdos de apoio ao serviço, notícias, eventos e ferramentas de capacitação que pretende facilitar a interação, a venda e o crescimento do Canal, em conjunto com a Sharp. Algumas das principais funcionalidades incluem painéis personalizados, com possibilidade de configuração de acordo com a função do utilizador; ferramenta de pesquisa global, concebida para facilitar a rápida localização da informação; e ferramentas de *co-branding*.

“Temos experiências e casos concretos que podemos partilhar com os Parceiros para os ajudar nessa transição e, juntos, sermos mais fortes”, reforça.

O executivo assume que a Sharp transformou o seu negócio, de forma deliberada, ao longo dos últimos anos, com a expansão de capacidades em serviços de IT, a integração total de audiovisual e a unificação das unidades de negócio. Hoje, sob o lema do SharpOne, a fabricante japonesa procura “servir as empresas de uma forma mais holística”. “Queremos proporcionar experiências digitais significativas que ajudem as empresas a tornarem-se mais orientadas pelo fator humano e potenciadas por IA”, explica.

## CONFIANÇA: A BASE PARA O FUTURO

Para Joe Tomota, ter visibilidade sob as tecnologias disponíveis no mercado – incluindo a inteligência artificial que já é parte integrante das soluções Sharp –, permite tomar decisões mais informadas.

Com as iniciativas de transformação digital em curso no ecossistema, o executivo considera que “tudo é possível” para os líderes de IT. No entanto, esta confiança está sobretudo assente na “experiência” e no “conhecimento”. ■

# SERVIDORES DELL POWEREDGE

Descubra a mais recente tecnologia PowerEdge

A última geração de servidores PowerEdge representa o portefólio de servidores mais amplo, automatizado e seguro de sempre da Dell Technologies. Com atualizações constantes de plataforma e inovações tecnológicas, o PowerEdge proporciona melhorias na qualidade dos negócios e serviços, tornando-se um investimento inteligente para sua empresa.

AI



DATABOX, o seu Distribuidor Autorizado DELL

TEM A PALAVRA

PEDRO VIEIRA, CHANNEL SALES MANAGER DA HP PORTUGAL

“PRECISAMOS DOS PARCEIROS COMO NINGUÉM: PRECISAMOS DAS SUAS CAPACIDADES, DA SUA COBERTURA E DE INOVAR CADA VEZ MAIS”



**E**ste mês o IT Channel dá a palavra a Pedro Vieira, o novo Channel Sales Manager da HP Portugal. Depois de mais de 20 anos à frente do retalho, e com experiência e visão acumulada do mercado ibérico, Pedro Vieira conduz agora os destinos do presente e do futuro do Canal de Parceiros a nível nacional, num contexto marcado pelo *shortage* e pela escassez de talento especializado em IT.

**Qual a análise que faz do atual ecossistema de Parceiros em Portugal, em particular do ecossistema de Parceiros da HP?**

Sobre o ecossistema de Parceiros, a HP é uma empresa de Canal. Cresci a aprender que o que mais valorizamos é o Canal e que temos um dos Canais mais amplos do mercado. Pretendemos continuar a desenvolvê-lo nesse sentido.

**O Pedro assumiu muito recentemente o cargo de Channel Sales Manager da HP Portugal. Quais são as primeiras prioridades que tem reservadas para o Canal?**

Comecei na HP há 24 anos, levo 22 anos de *retail* e hoje tenho três meses de experiência de Canal. As minhas primeiras prioridades são, naturalmente, conhecer os Parceiros. Funciono muito com proximidade e, portanto, nesta primeira fase quero conhecê-los a todos, compreender as suas preocupações, o que é que têm em vista para o futuro e quais são realmente aqueles pontos onde nós, como Parceiros, devemos atuar. Esse vai ser o meu grande foco nestas primeiras conversas.

**Qual é a estratégia que a HP tem preparada, pensada para este ano de 2026? Quais são as áreas de maior crescimento onde os Parceiros poderão investir?**

Um dos grandes temas da atualidade é, sem dúvida, a Inteligência Artificial [IA], que está neste momento a acontecer a uma grande velocidade. Acredito que este vai ser o caminho que todos nós vamos ter de fazer, apoiando, da melhor forma, as empresas e todo o ecossistema. Esse vai ser um dos focos da HP durante todo este ano, e o próximo, porque a inteligência artificial veio para ficar e estará cada vez mais presente nas nossas vidas.

**No início da entrevista, o Pedro referiu que a HP é uma empresa de Canal. Pensando nesta perspetiva, qual o peso do Canal no crescimento do negócio B2B em Portugal?**

Para nós o Canal é essencial e representa mais de 90% do nosso negócio. Nós só sabemos trabalhar com o Canal; muitos poderão dizê-lo, mas não o fazer, mas para nós é claramente o destino. Precisamos dos Parceiros como ninguém; precisamos das suas capacidades, da sua cobertura e de inovar cada vez mais na forma de ir ao negócio.

**A HP tem alguma novidade preparada para este ano, em termos de Programa de Canal, para apresentar aos Parceiros?**

O nosso Programa está em constante evolução. Temos um Programa de Canal há vários anos que antes se focava mais em KPI de negócio. Hoje agrega muito mais soluções de capaci-



tação, de serviço, etc. Portanto, hoje premiamos os Parceiros que evoluem nessa direção, o que nos permite ter mais valor acrescentado, assim como os nossos clientes.

**Que tipo de ferramentas e de especialização/formação é que a HP está a oferecer aos seus Parceiros para que estes possam oferecer ao cliente final um melhor produto?**

O nosso Programa de Canal tem vindo a adicionar essas especializações, premiando-as. Atualmente, o que fazemos cada vez mais é ter um plano de formação e capacitação dos nossos Parceiros. Em simultâneo, vamos ajudando-os a desenvolver as suas pessoas e a agregar também mais pessoas às suas equipas. Esta é, sem dúvida, a melhor forma de chegar ao mercado, de responder aos negócios que são apresentados pelos seus clientes [dos Parceiros] e pelos nossos clientes. Este é um trabalho que

tem vindo a ser feito de forma ativa, sem parar, porque é um Programa evolutivo e que está sempre em busca de soluções para satisfazer da melhor forma os clientes.

**A HP tem várias soluções, desde o portátil até às impressoras, e a própria agregação da Poly com outro tipo de produto. Quais são as áreas e as soluções do portfólio da HP que poderão posicionar-se como as mais relevantes para os Parceiros no atual contexto que vivemos?**

A Poly é realmente uma solução diferenciadora. Aliás, advém daí também a aquisição. A HP considera que quanto maior for o nosso portfólio, mais facilmente iremos satisfazer as necessidades dos clientes e das nossas empresas. Não só as soluções de serviços de software WXP, que são neste momento algo inovador que também estamos a desenvolver com o mercado, mas

também as soluções de conferência de Poly que, aos dias de hoje, e com o trabalho híbrido e a necessidade de existirem diferentes localizações de trabalho e de reuniões, são cada vez mais importantes para a comunicação à distância. Diria que estes são os principais fatores para optar por soluções de HP.

**Nas últimas semanas têm-se intensificado as notícias que dão conta de constrangimentos no mercado a nível da cadeia de abastecimento. Quais os efeitos concretos que este *shortage* tem atualmente na HP em Portugal e que tipo de ajustes são necessários para fazer face a estes constrangimentos?**

A resposta não é fácil. Estamos a começar a viver esta situação neste momento, apesar de haver algum ruído que já vem de trás. Existe realmente uma exponenciação da área de servidores e de IA que está, neste momento, a consumir mais componentes do que o habitual.

***“VAMOS CONTINUAR A ACOMPANHAR [O SHORTAGE] DE PERTO PARA DAR AS MELHORES SOLUÇÕES AOS NOSSOS PARCEIROS, UMA VEZ QUE É COM ELES QUE TRABALHAMOS TODOS OS DIAS PARA CHEGAR AOS NOSSOS CLIENTES”***

Desde a pandemia que nunca se tinha verificado tanto consumo de *devices* como até agora, portanto todas as cadeias de fornecimento estão neste momento a tentar adaptar-se e nós, como fabricante à escala mundial, iremos também

fazer todos os esforços para garantir ao máximo o maior número de componentes. Temos, neste momento, a capacidade para corresponder às necessidades do país. Vamos continuar a acompanhar esta situação de perto para dar as melhores soluções aos nossos Parceiros, uma vez que é com eles que trabalhamos todos os dias para chegar aos nossos clientes.

### **Que outros desafios considera que se podem colocar no caminho dos Parceiros neste atual contexto?**

Os desafios presentes e a curto prazo do Canal – e nossos também – passam pela dificuldade em encontrar mão de obra especializada. Vemos cada vez mais dificuldade nesse capítulo e aqui entra também a HP na ajuda a formar e a capacitar pessoas que sejam necessárias. Obviamente que também há um tema que está na atualidade que tem a ver com a concentração no Canal. Já aconteceu e já a vivi de perto em *retail*. Houve há já bastantes anos uma grande consolidação; neste momento também já vimos a acontecer a consolidação

▶ Para ver o vídeo clique sobre a imagem



Pedro Vieira, Channel Sales Manager da HP Portugal

**“QUEREMOS,  
ACIMA DE TUDO,  
PROTEGER TAMBÉM  
AS RENTABILIDADES  
PORQUE OS TEMPOS  
ESTÃO DIFÍCEIS PARA  
TODOS. ESSE VAI SER O  
NOSSO FOCO, É A NOSSA  
VONTADE”**

entre Parceiros noutros países, na procura de capacidades, muitos deles a procurarem ganhar tração e dimensão, portanto creio que serão dois dos maiores desafios que vamos ver no curto espaço de tempo.

### **Como é que é possível mitigar a escassez de talento no Canal, garantindo um futuro sustentável?**

Temos de criar condições e dar oportunidades e, acima de tudo, formá-los e capacitá-los da melhor forma, dar-lhes condições para que realmente se sintam bem. Este é um dos fatores que as empresas têm de cuidar: levar a que as pessoas se sintam melhor no seu ambiente de trabalho.

Este é um dos fatores em que a HP acredita para, de facto, reter talento: quanto mais as pessoas estiverem satisfeitas no seu ambiente de trabalho, e quanto mais se identificarem com os espaços em si, com os ambientes onde trabalham, com os seus *devices*, mais rapidamente se tornará a chave no futuro também para reter talento.

### **Qual a mensagem que quer transmitir aos Parceiros portugueses neste início de ano e de novo ciclo de liderança?**

Como dizia, eu sou uma pessoa de proximidade, ainda não tive contacto com todos os Parceiros, mas quero ter contacto com o maior número possível de Parceiros para os conhecer a todos.

A mensagem que a HP quer passar é de proximidade. 2026 vai ser um ano desafiante, por isso aquilo que podemos oferecer vai ser proximidade, confiança e negócio. Queremos, acima de tudo, proteger também as rentabilidades porque os tempos estão difíceis para todos. Esse vai ser o nosso foco, é a nossa vontade, e vamos fazer todos os possíveis para estar mais com os nossos Parceiros. ■

Jorge Bento e Marta Quaresma Ferreira



# SERVIÇOS ESPECIALIZADOS E O FUTURO DA CIBERSEGURANÇA NO CANAL DE PARCEIROS

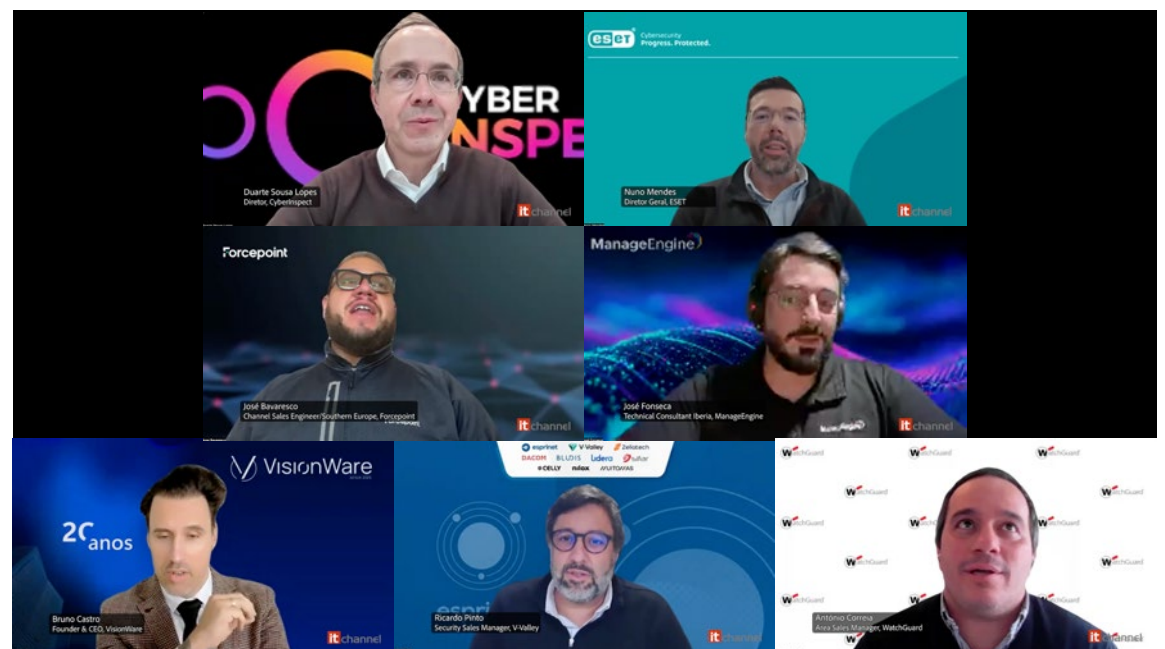
*Com o apoio de:*

CyberInspect | Eset | Forcepoint | ManageEngine | V-Valley | VisionWare | WatchGuard

**O pano de fundo para o primeiro live event de 2026 do IT Channel construiu-se a partir das promessas que ficaram de 2025, com a expectativa de que este ano comecem a ganhar execução. Esta sessão dedicada à cibersegurança mostrou que tecnologia isolada não resolve problemas. Entre dados, cloud, SOC-as-a-Service e NIS2, CyberInspect, Eset, Forcepoint, ManageEngine, V-Valley, VisionWare, e WatchGuard analisaram tendências, lacunas e, sobretudo, o papel do Canal de Parceiros na entrega de serviços geridos e especializados**

por Inês Garcia Martins

▶ Para ver o vídeo clique sobre a imagem



*Perante um público atento, o IT Channel promoveu uma mesa-redonda em formato live event, reunindo especialistas de referência para discutirem as tendências e desafios no mercado de Cibersegurança*

### QUAIS SÃO AS TENDÊNCIAS DE CIBERSEGURANÇA PARA 2026 QUE JÁ ESTÃO A TER IMPACTO REAL NOS INVESTIMENTOS E NAS ORGANIZAÇÕES EM PORTUGAL?

**José Bavaresco, Channel Sales Engineer | Southern Europe, Forcepoint:** “Uma tendência clara para 2026, é a mudança estrutural na forma como a segurança é pensada. A cibersegurança está numa transição, até 2030, em que deixa de estar centrada no perímetro ou na infraestrutura. O foco passa a ser os dados: onde estão, quem lhes acede e em que contexto são utilizados. As organizações estão a acelerar fortemente a adoção de cloud pública, soluções SaaS e também novas capacidades de Inteligência Artificial [IA], sobretudo generativa. Isso está a direcionar o investimento para plataformas que consigam descobrir e classificar continuamente dados críticos, tanto na cloud como em ambientes on-prem.”

### O QUE ESTÁ A MUDAR NA FORMA COMO OS CIBERATAQUES SÃO PREPARADOS E EXECUTADOS?



Bruno Castro, VisionWare

**Bruno Castro, Founder & CEO, VisionWare:** “A IA veio dar um impulso ao cibercrime, ao permitir ataques escaláveis, personalizados e com taxas de sucesso elevadas. São operações mais rápidas, sofisticadas e difíceis de detetar. Os atacantes conseguem fazer um *profiling* detalhado da vítima e direcionar os ataques ao elo mais fraco, que continua a ser o fator humano. O cibercrime está cada vez mais profissionalizado. Funciona como um verdadeiro modelo de negócio, altamente rentável, com grupos verticais e ultraspecializados, focados em setores específicos e com ataques padronizados para cada indústria.”

**Nuno Mendes, Diretor Geral, Eset:** “Temos observado um foco cada vez maior na cadeia de fornecimento como vetor de ataque, algo que já acontece há vários anos, mas que continua a ser particularmente preocupante e que, felizmente, também é endereçado pela NIS 2. Finalmente, há também um aumento do que chamamos EDR killers. Apesar de a indústria já dispor de várias tecnologias de defesa, os atacantes estão a desenvolver técnicas específicas para desativar ou contornar sistemas como EDR, tentando neutralizar as ferramentas de proteção antes de lançar o ataque.”

**Duarte Sousa Lopes, Diretor, CyberInspect:** “A industrialização e automatização do cibercrime, aliada à IA, mudou o perfil das organizações atacadas. Permite explorar de forma rentável empresas de menor dimensão. Atualmente, 90% dos ataques atingem PME, e mais de 80% das vítimas de ransomware são pequenas e médias empresas. Estatísticas internacionais indicam que, quando uma PME sofre um ataque bem-sucedido, cerca de 60% acabam por falir. Isto acontece porque não têm a mesma resiliência financeira que empresas maiores e, além disso, perdem a confiança de clientes e fornecedores. Este fenómeno não é exclusivo de 2026, mas é recente e tende a acelerar com a industrialização do cibercrime.”

### A CONVERGÊNCIA ENTRE SEGURANÇA DE ENDPOINT, REDE E CLOUD ESTÁ A ACONTECER NA PRÁTICA OU AINDA CONTINUA FRAGMENTADA?

**Ricardo Pinto, Security Sales Manager, V-Valley:** “Ferramentas como o e-mail, presentes em dispositivos móveis, portáteis e na cloud, tornam urgente pensar a segurança de forma integrada. O novo perímetro não é só a rede interna da empresa, mas também os dispositivos e as cloud com os quais interagimos. É essencial adotar um modelo que permita visão e gestão centralizada da segurança, garantindo maior controlo sobre toda a infraestrutura. Nesse sentido, muitos fabricantes têm vindo a desenvolver soluções que se complementam e oferecem uma visão mais integral da segurança entre *endpoint*, rede e cloud.”

**José Bavaresco, Forcepoint:** “Temos muitos agentes e elementos de segurança bastante fortes, mas cada um trabalha focado na sua área. Olhando para o panorama completo – servidores, serviços, infraestrutura em geral, não apenas on-prem – a segurança continua fragmentada. Cada elemento tem visibilidade apenas da sua própria parcela, o que gera desafios significativos em termos de *compliance* e de visão global do ambiente. A visibilidade integrada é, portanto, absolutamente crucial.”



Ricardo Pinto, V-Valley

---

## DE QUE LADO É QUE A INTELIGÊNCIA ARTIFICIAL ESTÁ A SER MAIS RELEVANTE: DO LADO DA DEFESA OU DO LADO DOS CIBERCRIMINOSOS?

**Nuno Mendes, Eset:** “Do lado da defesa, temos uma vantagem que é o facto de podermos usar a mesma tecnologia para proteger os clientes. A IA permite processar dados em massa, de forma automática e a velocidades impossíveis há dez ou quinze anos, recolher e analisar telemetria e antecipar ataques. Também permite criar ferramentas como *AI Advisors*, que ajudam os utilizadores a interpretar dados, eventos e incidentes em linguagem mais acessível, aliviando a escassez de recursos humanos e facilitando a identificação e correlação de ameaças.”



Nuno Mendes, Eset

**Bruno Castro, VisionWare:** “Do lado mau da força. Temos de perceber rapidamente que nos dá rapidez, dá-nos capacidade de escalar ataques, padronizá-los, moldá-los à vítima, deu até *boost* em termos de *skills* para grupos criminosos que eram *wannabe* e passaram agora a ser uma ameaça. Continuo a achar que a IA se tornou um esteroide muito grande para o cibercrime. Conseguimos estudar o *supply chain* com IA muito facilmente e conseguimos padronizar logo ecossistemas em redor da vítima, e depois o ataque é direccionado de forma global à vítima, não só às personas, não só à organização, não só à tecnologia, mas também ao seu ecossistema.”

## QUE DIFICULDADES PRÁTICAS CONSIDERAM QUE ESTÃO A SURGIR NA IMPLEMENTAÇÃO DOS REQUISITOS DA NIS 2 E QUAL O SEU IMPACTO PARA OS PARCEIROS?

**Duarte Sousa Lopes, CyberInspect:** “A NIS 2 representa um salto de escala e de exigência grande. Além de gerar pressão, permite aos Parceiros deixarem de ser apenas implementadores de ferramentas e passarem a ser implementadores de confiança, transmitindo aos clientes finais a confiança necessária para estruturar, reduzir a complexidade do que é exigido e previsto pela NIS 2, e ter alguma automatização e controlo sobre as respostas. Quem fizer esta transição acaba por ser beneficiado, porque consegue compreender a complexidade da NIS 2 e, ao mesmo tempo, implementar de forma natural e certa aquilo que é o objetivo.”

## O ECOSISTEMA ATUAL ESTÁ PREPARADO PARA RESPONDER, POR UM LADO, À COMPLEXIDADE CRESCENTE DAS AMEAÇAS E, POR OUTRO, À NECESSIDADE DE CUMPRIR COM AS REGULAÇÕES?



António Correia, WatchGuard

**António Correia, Area Sales Manager, WatchGuard:** “O principal desafio, invariavelmente, tem a ver com duas coisas muito simples: recursos técnicos especializados e a escassez dos mesmos. Por outro lado, a capacidade de investimento e a necessidade, acima de tudo, de priorizar o mesmo, porque naturalmente os recursos são e serão sempre escassos. As empresas têm cada vez mais que ter consciência de que têm, de facto, de caminhar, umas mais depressa, outras mais devagar, mas têm de fazer esse caminho, têm de fazer esse plano.”

**José Bavaresco, Forcepoint:** “Muitas ferramentas falham em proporcionar visibilidade básica, devido à fragmentação do ecossistema de segurança. Isto aplica-se tanto à infraestrutura como aos serviços, onde essa fragmentação é significativa. Na prática, falta-nos acesso ou visibilidade sobre os dados e repositórios sensíveis: quais são acessíveis e quais não são, que tipos de acessos existem a esses dados, quem acede aos mesmos, que aplicações utilizam as pessoas e se há exposição desses dados dentro ou fora da organização.”

## QUE MÉTRICAS FAZEM SENTIDO PARA DEMONSTRAR VALOR EM PROJETOS DE CIBERSEGURANÇA?

**José Fonseca, ManageEngine:** “Se a métrica não conversa com risco, dinheiro ou continuidade do negócio, então não tem qualquer valor, não aporta qualquer valor para as empresas. A partir do momento em que temos uma percentagem real de sistemas, identidades e acessos a serem monitorizados – não é termos só *logs*, mas também a percentagem da superfície de ataque que realmente está visível – podemos ter tudo visível e bem monitorizado. O ROI em cibersegurança mede-se muitas vezes pelo silêncio, quando nada aconteceu porque alguém estava a ver e foi proativo na sua resolução.”

**Nuno Mendes, Eset:** “A utilização de métricas é algo extremamente importante para valorizar o valor. Há um passo antes, que é a avaliação técnica, a escolha das tecnologias e dos serviços corretos e apropriados para a dimensão das empresas. Isso realmente traz aqui algum desafio na deteção das métricas. Temos métricas de redução de risco e exposição ao risco. É preciso fundamentar ao cliente qual é a superfície de risco a que ele está sujeito, portanto, é preciso fazer uma interação dos *assets*, fazer as perguntas certas para depois poder quantificar e medir esses riscos.”

### QUE TIPO DE SERVIÇOS GERIDOS SÃO HOJE MAIS PROCURADOS PELOS CLIENTES? COMO É QUE É POSSÍVEL GARANTIR A QUALIDADE E CONFIANÇA NUM MODELO DE SERVIÇOS CONTÍNUOS?

**Bruno Castro, VisionWare:** “A adoção de serviços tem sido uma tendência no mercado. A razão é óbvia: falta de recursos. O custo para implementar uma boa plataforma de segurança é elevado. A necessidade de ter uma especialização muito acentuada face à complexidade e evolução do cibercrime também obriga. Portanto, já não dá para montar a solução mais ou menos em casa. Qual é aqui o grande desafio? No meu entender, é escolher bem o Parceiro. Escolher um Parceiro que saiba o que está a fazer, que tenha experiência na área, não apenas alguém que vende barato ou que apareceu agora porque “é *trendy*” vender segurança. O Parceiro tem de saber responder eficazmente.”

**Ricardo Pinto, V-Valley:** “A forma correta de endereçar isto é efetivamente a construção de um SOC, que permita “mastigar” toda a informação que nos chega e tomar medidas preventivas e reativas, se for o caso, ao nível de segurança. Mas o custo de implementação de um SOC é gigante. E se olharmos para o tecido empresarial em Portugal, maioritariamente empresas pequenas e médias, é completamente inviável qualquer empresa implementar uma solução sozinha. A forma de darmos resposta a isto e a oportunidade de negócio para os nossos Parceiros é efetivamente o SOC-as-a-Service.”

### O QUE É NECESSÁRIO PARA QUE UM PARCEIRO CONSIGA ESCALAR SERVIÇOS DE SEGURANÇA DE FORMA SUSTENTÁVEL?



José Fonseca, ManageEngine

**José Fonseca, ManageEngine:** “Escalar serviços de segurança não é contratar pessoas, é reduzir a dependência das pessoas. Isto requer que existam plataformas cada vez mais automatizadas e dinâmicas. Para isso, temos de ter alguma resposta relativamente a isso. O maior erro dos Parceiros, muitas das vezes, é tentar escalar apenas com talento humano e isto às vezes não escala, só encarece cada vez mais a fatura. Para crescer de forma sustentável, é obrigatório ter uma plataforma integrada e não um conjunto de ferramentas soltas.”

**António Correia, WatchGuard:** “Acho que é essencial que o cliente escolha o Parceiro certo. A mesma coisa se aplica ao Parceiro na seleção da tecnologia em que apoia o seu serviço. É essencial, sem dúvida absolutamente nenhuma, que seja um serviço antes de mais. Não é só uma questão de atirar tecnologia de uma cor ou de outra para cima do problema. Tem muitíssimo a ver com a necessidade de, baseado em determinada tecnologia, ser capaz de prestar um bom serviço ao cliente.”

**Duarte Sousa Lopes, CyberInspect:** “O tema do modelo operativo é absolutamente crítico para conseguir servir clientes em escala de uma maneira eficiente e que liberte margem. Isto é o primeiro ponto. Não é só um tema de adquirir tecnologia, é um tema também para a nossa organização. Nós sabemos qual é o modelo operativo que faz sentido e o modelo operativo que conseguimos implementar. É muito difícil, se não impossível, vender alguém a um serviço de SOC ou algo que se compara a um serviço de SOC se o cliente nem sequer percebe o risco a que está exposto.”

### COMO É QUE FABRICANTES E DISTRIBUIDORES PODEM APOIAR MELHOR OS PARCEIROS NA ESPECIALIZAÇÃO?

**Ricardo Pinto, V-Valley:** “Não é só chegar com o catálogo e perguntar quantos quilos de firewall e quantas gramas de *endpoints* é que quer. Cada vez mais a exigência técnica vai obrigar a fazer aqui uma separação entre o trigo e o joio. Temos de ter um Parceiro ao nosso lado que aporte confiança para que depois o mesmo também possa aportar a confiança ao seu cliente. No fundo, aquilo que nós queremos ser é o acelerador da especialização para os nossos Parceiros, para que consigam ter um crescimento sustentável.”

---

**António Correia, WatchGuard:** “Não devemos atirar tecnologia para os problemas. Tanto os fabricantes como os distribuidores, têm um papel essencial e começa logo na génese. Tudo aquilo que desenvolvemos, mais do que estar pensado para o cliente, está pensado para servir o Canal e o Parceiro. Tem a ver com a capacidade de gerir todos os clientes, sejam eles pequenos ou de grande dimensão, numa única consola. Todos os fabricantes caminham neste sentido e estamos muito orientados para lhes entregar algo que seja capaz de escalar. Isso facilita muito a especialização.”

## QUAL É A MENSAGEM FINAL PARA OS PARCEIROS SOBRE AS OPORTUNIDADES NA ÁREA DA CIBERSEGURANÇA EM 2026?

**Nuno Mendes, Eset:** “Falem com os seus Parceiros. Façam algum trabalho de *procurement*. Não olhem sempre para as mesmas soluções e procurem diversificar tecnologias, procurem ter algo que também é uma necessidade crescente, que é procurar alguma soberania europeia. É algo importante para os clientes finais que, cada vez mais, apreciam e valorizam.”



José Bavaresco, Forcepoint

**José Bavaresco, Forcepoint:** “As organizações portuguesas enfrentam desafios como a adoção da NIS 2, as migrações massivas para a cloud e a pressão para utilizar a inteligência artificial de forma segura. Estes desafios representam oportunidades para oferecer visibilidade, soluções de controlo e automatização dos dados, tanto na cloud como em sistemas *on-premises*. Esta é uma oportunidade para, em conjunto com os Parceiros, criar soluções diferenciadoras e de valor.”

**José Fonseca, ManageEngine:** “Deixamos de vender apenas um produto ou uma licença e passamos a entregar um serviço contínuo, gerido e governado. Existem várias oportunidades, não só em projetos de identidade e perímetro, mas também na automação, resposta, *compliance* e nos *checks* recorrentes, bem como nas métricas de maturidade. Os Parceiros beneficiam disto porque passam a falar a linguagem do risco, mostram valor com métricas e constroem relações de longo prazo com os clientes.”

**Ricardo Pinto, V-Valley:** “Este é mais um ano de oportunidades para os nossos Parceiros. A mensagem é de confiança. Não tenham receio de abordar os clientes. Quem conseguir ser especialista, ter uma visão holística da segurança e simplificar os processos para o cliente terá uma vantagem. O essencial é que os Parceiros sintam que podem contar connosco, que conheçam a nossa abordagem à cloud e à segurança, e que juntos possamos fazer a diferença em 2026 e nos anos seguintes.”

**António Correia, WatchGuard:** “Existem oportunidades enormes a nível de cibersegurança, mas os Parceiros devem focar-se nos serviços que podem entregar. Procurem ser uma mais-valia e posicionem-se no mercado para estar presente a longo prazo, não apenas vender hoje e deixar para depois. É essencial concentrar-se no problema do cliente, resolvê-lo e ser capaz de prestar um serviço de cibersegurança que escale e garanta a subsistência e o sucesso do negócio, assim como a sua rentabilidade.”

**Duarte Sousa Lopes, CyberInspect:** “Há aqui um caminho enorme a percorrer em termos de capacidade de explicação, enquanto Canal, fabricantes ou Parceiros, para transmitir isto de forma clara. Senão o que vai acontecer é que as pessoas vão deixar isso para a última da hora e, se isso acontecer, na prática, o ecossistema não consegue tirar partido desta oportunidade.”

**Bruno Castro, VisonWare:** “O objetivo é proporcionar maturidade, permitindo ao cliente reduzir rapidamente o seu ciber-risco e, cada vez mais, ser uma referência em segurança dentro do seu ecossistema e junto dos Parceiros. Preparar as nossas equipas para responder a todas as exigências normativas e certificações do cliente é essencial para garantir que não existe risco nas interações do seu ecossistema.” ■



Duarte Sousa Lopes, CyberInspect

# A identificação de risco como motor de negócio para os Parceiros

Num mercado em que o risco digital cresce mais depressa do que a capacidade das pequenas e médias empresas (PME) o gerir, os MSP têm uma oportunidade clara: transformar a cibersegurança num serviço recorrente. A CyberInspect permite às empresas de serviços IT colocar a identificação de risco no centro da relação com o cliente, tornando visível o risco real a que estão expostos e abrindo caminho à venda de serviços de cibersegurança e serviços conexos resultantes da remediação

## SEM RISCO VISÍVEL, NÃO HÁ DECISÃO DE INVESTIMENTO

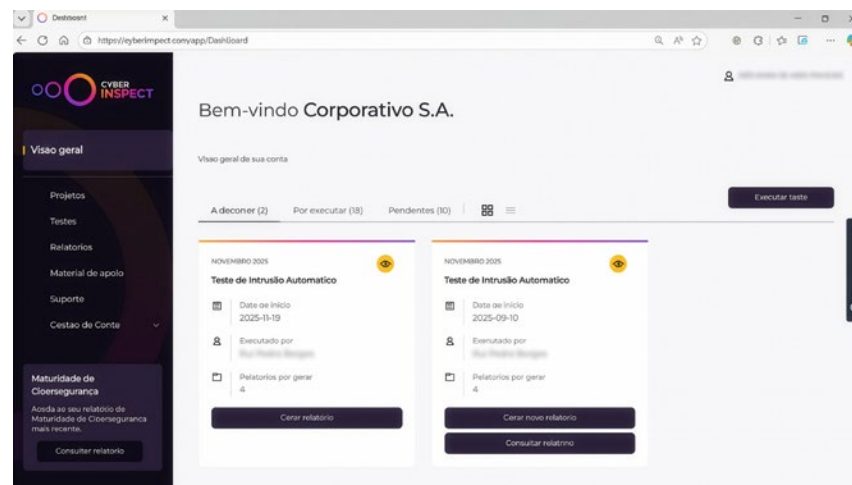
A cibersegurança deixou de ser um tema exclusivamente técnico para se afirmar como um assunto estratégico do negócio. A automatização dos ataques e o uso intensivo de inteligência artificial alteraram profundamente a escala e a rentabilidade do cibercrime. Hoje, as PME são os principais alvos, não por serem menos relevantes, mas por serem mais fáceis de explorar e serem em muito maior número (mais de 90% do total de empresas). Ainda assim, persistem lacunas significativas na perceção do risco, o que bloqueia decisões de investimento e atrasa a adoção de medidas eficazes.

Para o canal, esta realidade representa simultaneamente um desafio e uma oportunidade. Sem visibilidade, a conversação com o cliente fica presa ao preço, à urgência do incidente ou ao cumprimento mínimo de requisitos. Com visibilidade, a discussão passa a centrar-se em impacto, prioridades e continuidade do negócio.

## O PRIMEIRO PASSO PARA UM MODELO DE NEGÓCIO SUSTENTÁVEL

Construir um modelo de negócio sustentável em cibersegurança exige a capacidade de avaliar e explicar a exposição digital dos clientes de forma clara e consistente. Quantificar e contextualizar essa exposição permite estruturar ofertas, justificar investimento e criar uma relação contínua com o cliente. Quando este processo é manual ou pontual, deixa de escalar, sobretudo no universo das PME.

A CyberInspect foi desenvolvida para responder precisamente a este desafio. A plataforma permite às empresas de serviços IT realizar diagnósticos de cibersegurança de forma automatizada, consistente e escalável, integrando a avaliação de exposição no portefólio de serviços sem aumentar a complexidade operacional. A partir de um único ponto de acesso, é possível analisar a exposição digital, executar testes de forma automática e identificar vulnerabilidades – verdadeiras portas de entrada para ciberataques – e acompanhar a evolução do risco ao longo do tempo. Outro bloqueio recorrente à venda de serviços de cibersegurança é a dificuldade em comunicar resultados técnicos a decisores de negócio. A CyberInspect responde a este desafio com relatórios desenvolvidos internamente, suportados por inteligência artificial, que agregam os



resultados técnicos e os traduzem para uma linguagem clara de cliente final, orientada a impacto e prioridade. Para o parceiro, isto significa menos tempo gasto na interpretação de dados e mais capacidade para vender, priorizar e aprofundar a relação com o cliente.

## NIS2 E A CADEIA DE ABASTECIMENTO: QUANDO A ESCALA SE TORNA DECISIVA

Num contexto em que a NIS2 e os requisitos associados à cadeia de fornecimento vão gerar um aumento significativo da procura, a escala do desafio torna-se evidente. As cerca de 4.000 entidades diretamente abrangidas pela diretiva representam mais de 40.000 empresas impactadas ao longo da respetiva *supply chain*. Perante esta pressão, a capacidade de escalar de forma qualificada é crítica.

A CyberInspect funciona como um facilitador de modelo operativo, permitindo aos MSPs empacotar capacidades técnicas em serviços próprios, criar receitas recorrentes e reforçar a sua posição como parceiros estratégicos dos clientes. Num mercado onde o risco é inevitável, torná-lo visível é o primeiro passo para o transformar em negócio. ■

### CYBERINSPECT | VANTAGENS PARA OS PARCEIROS

- ✓ Desenvolvimento de oferta numa área em forte expansão
- ✓ Permite criar serviços recorrentes a partir da avaliação de risco
- ✓ Cria oportunidades comerciais assentes em serviços de remediação
- ✓ Ganho de capacidade de escala por via da simplicidade e automação
- ✓ Reforça a relação de confiança ao falar a linguagem do decisor

**Conheça a CyberInspect e transforme a identificação de risco em valor para os seus clientes e em oportunidades para o seu negócio.**

**INFO**  
[cyberinspect.com](https://cyberinspect.com)



# O PRIMEIRO PASSO COMEÇA NA IDENTIFICAÇÃO DO RISCO.

Muitas empresas não conseguem dar esse passo sozinhas. Cada diagnóstico de risco é uma oportunidade de negócio.

Saiba mais

# A importância dos parceiros no novo paradigma de cibersegurança

Durante muito tempo, falar de cibersegurança era falar de prevenção



Nuno Mendes, Diretor Geral na ESET Portugal

**F**irewalls, antivírus, políticas de acesso e a expectativa — muitas vezes irrealista — de que seria possível impedir todos os ataques. Hoje, esse discurso já não acompanha a realidade. O cenário de ameaças evoluiu, os atacantes profissionalizaram-se e a questão deixou de ser se uma organização vai ser alvo de um incidente, passando a ser quando — e com que impacto.

O ESET Threat Report H2 confirma esta tendência. Observa-se uma consolidação de campanhas de ransomware mais direcionadas, com grupos a operarem quase como empresas, combinando malware sofisticado, exploração de vulnerabilidades conhecidas e técnicas de engenharia social altamente eficazes. Notamos, por exemplo, um aumento preocupante no uso de ferramentas legítimas para fins maliciosos (Living off the Land), o que torna a detecção

mais complexa e reduz drasticamente a eficácia de abordagens exclusivamente reativas.

É neste contexto que o conceito de resiliência ganha centralidade. Prevenir continua a ser fundamental, mas já não é suficiente. A resiliência em cibersegurança assenta na capacidade de detetar rapidamente um incidente, limitar a sua propagação, garantir a continuidade do negócio e recuperar de forma controlada. Como a ESET tem vindo a sublinhar no portal WeLiveSecurity, assumir que uma falha pode acontecer não é sinal de fraqueza — é sinal de maturidade organizacional.

A evolução tecnológica tem sido um aliado importante neste caminho. A combinação de inteligência artificial, análise comportamental e threat intelligence global permite identificar padrões anómalos e ameaças emergentes que escapam aos mecanismos tradicionais baseados

em assinaturas. No entanto, a tecnologia não resolve tudo. Sem processos claros, equipas preparadas e planos de resposta testados regularmente, mesmo as melhores soluções ficam aquém do seu potencial.

O fator humano continua a ser um dos principais desafios. O relatório da ESET volta a destacar o peso do phishing e da engenharia social como vetores iniciais de ataque, agora potenciados pelo uso de IA generativa para criar mensagens mais credíveis. A resiliência passa, inevitavelmente, por investir na sensibilização e formação dos colaboradores, reduzindo o risco de erro humano e aumentando a cultura de segurança no dia a dia.

Para o ecossistema de parceiros de IT, esta mudança de paradigma traz novas responsabilidades — e oportunidades. As organizações procuram cada vez mais apoio especializado para avaliar o seu nível de maturidade, implementar soluções integradas e garantir monitorização contínua. Serviços geridos, modelos de deteção e resposta (EDR e MDR) e uma abordagem consultiva tornam-se elementos-chave num mercado que já não procura apenas proteção, mas continuidade e confiança.

O futuro da cibersegurança não passa pela promessa de ambientes impenetráveis, mas sim pela capacidade de adaptação, resposta e recuperação. A transição da prevenção para a resiliência é uma evolução natural e necessária num mundo digital onde a única constante é a mutação das ameaças. Para os parceiros de IT, o desafio é agora: transformar esta visão em soluções práticas que garantam a robustez dos seus clientes, posicionando-se não apenas como fornecedores, mas como pilares estratégicos de confiança. ■

**INFO**  
[eset.com/pt/](https://eset.com/pt/)



# European Excellence in Cybersecurity, Driving Partner Success



# Identidades Não Humanas: Um Novo Desafio para a Segurança Empresarial

A gestão e proteção de identidades não humanas tornou-se um desafio crítico para as organizações que procuram mitigar riscos, manter controlo e garantir segurança em ambientes cada vez mais automatizados



**A**s organizações estão a interagir cada vez mais com identidades que não estão associadas a utilizadores humanos. Ao mesmo tempo, a crescente adoção de inteligência artificial está a acelerar o aumento exponencial de identidades não humanas nos ambientes empresariais.

Atualmente é comum encontrar identidades de máquinas criadas sem supervisão adequada, tokens sem data de expiração, serviços com permissões excessivas e uma falta de rastreabilidade que dificulta a identificação da causa raiz de falhas. Nestes cenários, uma API comprometida pode representar um risco de segurança maior do que uma conta humana com privilégios elevados.

Ao longo deste ano, prevê-se que o número de identidades não humanas ultrapasse largamente o número de utilizadores humanos, com uma estimativa de 92 para um. Apesar deste crescimento, muitas organizações não têm

visibilidade sobre quantas destas identidades existem, para que são utilizadas ou quem é responsável por elas. Sem uma governação adequada, o chamado “shadow IAM” deixa de ser impulsionado pelos colaboradores e passa a ser gerado pelos próprios processos automatizados da organização.

## CADA IDENTIDADE É UM ATIVO CRÍTICO

Enfrentar este desafio exige um inventário proativo de identidades (ISPM), a implementação de uma governação de identidade eficaz (IGA) e a definição de políticas que gerem todas as identidades — humanas e não humanas — com o mesmo nível de rigor, controlo e rastreabilidade (IAM + PAM). O princípio base é tratar cada identidade, independentemente da sua natureza, como um ativo crítico, suportado por rotação regular de credenciais, aplicação rigorosa de privilégios mínimos, automação bem governada e supervisão centralizada que vá além dos métodos manuais de controlo.

## AUTENTICAÇÃO E PROTEÇÃO DE IDENTIDADE

À medida que os ataques baseados em identidade continuam a aumentar e as técnicas de movimento lateral se tornam mais sofisticadas, as organizações devem adotar uma plataforma de autenticação unificada combinada com chaves de segurança baseadas em hardware. Este modelo de defesa em múltiplas camadas permite proteger ambientes que tradicionalmente não suportam autenticação multifator. Neste contexto, uma plataforma de autenticação que permita estender a autenticação física multifator a todos os sistemas e recursos — incluindo ambientes on premises, cloud e sistemas legados — sem necessidade de instalar agentes, implementar proxies ou modificar aplicações existentes. Esta abordagem possibilita a aplicação consistente de políticas de acesso e princípios Zero Trust em toda a organização. Para além disto, existem também as chaves de segurança baseadas em hardware, que oferecem um nível elevado de proteção contra phishing através de normas como FIDO2 e WebAuthn. Quando integradas numa camada de autenticação centralizada, esta proteção pode ser estendida a ambientes críticos como Active Directory, servidores de terminal, bases de dados, infraestruturas de tecnologia operacional (OT) e sistemas industriais onde o MFA tradicional não pode ser implementada. A adoção combinada destas tecnologias constitui um avanço significativo no sentido de assegurar uma identidade contínua e devidamente verificada em todos os pontos de acesso, estabelecendo a segurança como um pilar fundamental da infraestrutura empresarial moderna — um contexto em que a confiança deixa de ser presumida e passa a ser constantemente validada. ■

**INFO**  
[ignition-technology.pt](https://www.ignition-technology.pt)

# IGNITION

An Exclusive Networks Company



Em cibersegurança,  
estamos um passo  
à frente



VAD especialista em cibersegurança e ciberinteligência

[www.ignition-technology.pt](http://www.ignition-technology.pt)

# Guia sobre engenharia social: tudo o que precisa de saber

O elo mais frágil de qualquer sistema de segurança é o ser humano



**P**or sermos imprevisíveis e suscetíveis à manipulação, ataques de engenharia social exploram erros humanos para induzir vítimas a partilhar informações pessoais, bancárias ou corporativas. Esses golpes podem ocorrer por e-mail, telefone, redes sociais ou até presencialmente.

A engenharia social utiliza técnicas psicológicas para influenciar comportamentos. Criminosos fazem passar-se por pessoas confiáveis ou figuras de autoridade para conquistar a confiança da vítima e, em seguida, extrair dados confidenciais.

Entre as principais técnicas de persuasão estão:

**Simpatia:** o golpista age de forma amigável para ganhar confiança, como golpes de falsos presentes de aniversário que cobram taxas falsas de entrega.

**Urgência:** cria-se pressão emocional com mensagens como “a sua conta será bloqueada em 24 horas”, levando a decisões impulsivas.

**Compromisso e coerência:** a vítima sente-se obrigada a cumprir acordos, como golpes de falso pedido de dinheiro de conhecidos.

**Prova social:** o criminoso afirma que outras pessoas já colaboraram, incentivando a vítima a fazer o mesmo.

**Autoridade:** o golpista faz-se passar por chefe, bancos ou órgãos oficiais para exigir informações.

**Reciprocidade:** oferece algo em troca, como reembolsos falsos, para obter dados pessoais.

Os ataques mais comuns incluem:

**Phishing:** e-mails ou mensagens falsas que imitam empresas conhecidas para roubar dados.

**Spear phishing:** versões mais direcionadas a empresas ou departamentos específicos.

**Pretexting:** criação de histórias falsas para extrair informações.

**Quid pro quo:** troca de “ajuda técnica” por acesso ou dados.

**Tailgating:** invasão física de áreas restritas aproveitando a gentileza de colaboradores.

Normalmente, estes ataques seguem quatro etapas: recolha de informações, criação de um enredo convincente, execução do golpe e remoção de vestígios.

No Brasil, estes crimes são enquadrados como estelionato ou furto mediante fraude, com penas que podem chegar a oito anos de prisão em casos graves.

Os alvos mais comuns incluem idosos e pessoas com problemas legais ou financeiros, por serem mais vulneráveis à pressão psicológica.

No futuro, espera-se o aumento de golpes com deepfakes, perfis falsos de influenciadores e sites clonados que imitam páginas legítimas para roubo de credenciais.

Para se proteger, é fundamental:

- Desconfiar de mensagens urgentes e pedidos de dados
- Usar autenticação multifator
- Limitar acessos a informações sensíveis
- Evitar partilhar excessos nas redes sociais

A conscientização continua sendo a principal defesa contra ataques de engenharia social. ■

**INFO**  
manageengine.com

**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>

# V-Valley Advanced Solutions: um distribuidor de valor acrescentado para a segurança empresarial do presente e do futuro

Num cenário em que a cibersegurança assume um papel central na resiliência e competitividade das organizações, o ecossistema tecnológico enfrenta desafios cada vez mais complexos

**A** sofisticação das ameaças, a expansão das superfícies de ataque e a crescente dependência de ambientes digitais, exigem abordagens integradas, sustentáveis e orientadas para a resolução cabal dos desafios identificados. É neste contexto que a V-Valley Advanced Solutions se afirma como um **distribuidor de valor acrescentado de referência na área da segurança empresarial**.

Mais do que um fornecedor de tecnologia, a V-Valley posiciona-se como um parceiro estratégico do canal, com uma visão clara, **ajudar os parceiros a disponibilizar soluções completas de proteção**, ajustadas às necessidades reais dos seus clientes, independentemente da sua dimensão ou maturidade tecnológica.

O portfólio de segurança da V-Valley é cuidadosamente selecionado para cobrir, de forma integrada, os principais domínios da segurança moderna. Inclui soluções para proteção de **endpoint, rede, cloud e email**, bem como componentes críticas, como gestão de identidades, **MFA, SASE, WAF** e proteção contra ataques **DDoS**. A esta base juntam-se soluções avançadas para **ambientes mais complexos e críticos**, nomeadamente, **OT e IoT, Data Loss Prevention (DLP), Dynamic Application Security Testing (DAST), observabilidade, gestão de vulnerabilidades e patch management**. Dessa forma permite-se responder a cenários empresariais altamente exigentes e regulados. Esta abrangência não é meramente tecnológica. A V-Valley privilegia soluções que se integram entre si, com modelos de gestão centralizada, elevada visibilidade e capacidade de resposta



Ricardo Pinto, V-Valley Portugal Security Sales Manager

coordenada, reduzindo a fragmentação e a complexidade operacional –fatores que hoje representam um dos maiores riscos para a eficácia da segurança.

O verdadeiro diferencial da V-Valley reside no seu envolvimento ativo ao longo de todo o ciclo de vida dos projetos. A empresa aposta fortemente no **apoio em pré-venda, no desenho de arquiteturas, na realização de provas de conceito e no suporte à implementação**, sempre que os parceiros o solicitem. É uma abordagem consultiva que possibilita acelerar processos de decisão, mitigar riscos técnicos e aumentar a taxa de

sucesso dos projetos. Tudo isto, com o intuito de reforçar a confiança entre parceiros e clientes finais.

Como complemento a esta estratégia, a V-Valley disponibiliza a sua plataforma própria **Lidera Cloud**, que materializa uma abordagem moderna de segurança como serviço. Através da Lidera Cloud, os parceiros podem aceder a soluções de diferentes fabricantes num modelo **Pay as you go**, com custos previsíveis, escaláveis e alinhados com o consumo real.

Adicionalmente, a plataforma permite a contratação de **serviços de gestão continuada** das soluções comercializadas, que apoiam os parceiros na operação diária e, dessa forma, colmatam a escassez de recursos especializados. A evolução da Lidera Cloud integrará, ainda, **serviços de XDR e SOC as a Service**, oferecendo capacidades avançadas de deteção, correlação e resposta a incidentes, como complemento à oferta dos parceiros.

Esta abordagem contribui para uma melhor experiência do cliente final, ao promover relações de longo prazo, maior fidelização e um modelo de segurança contínuo, proativo e orientado a resultados.

Com uma visão estratégica, um portfólio sólido e uma forte aposta em serviços, a V-Valley Advanced Solutions consolida-se como um **facilitador do crescimento sustentável do canal**. Dessa forma, espera ajudar os parceiros a evoluir de um modelo centrado na venda de produtos para uma proposta de valor baseada em soluções integradas e serviços geridos de segurança empresarial. ■

**INFO**  
v-valley.com/pt/



## A CIBERSEGURANÇA É UM FATOR CRÍTICO PARA A CONTINUIDADE DO NEGÓCIO.

A V-Valley, enquanto distribuidor de valor acrescentado, disponibiliza um portefólio robusto de soluções de cibersegurança, serviços avançados e acompanhamento especializado ao longo de toda a jornada – da prevenção à deteção, da resposta à recuperação.

**Mais do que soluções, entregamos confiança e parceria.**

V-Valley. Quando a segurança é crítica,  
o parceiro faz a diferença.

[www.v-valley.com](http://www.v-valley.com)



# O futuro é SOC, [só que] resiliente

O mercado global de serviços de Managed Detection & Response (MDR) atingiu 9,6 mil milhões de dólares em 2025 e deverá crescer para 46,9 mil milhões até 2035, com uma taxa média anual de crescimento de 17,2%.

**E**ste crescimento é impulsionado quer pelo aumento das ameaças digitais, quer pela sofisticação e rapidez com que são executados, mas também pela escassez de profissionais especializados em cibersegurança que possam responder às necessidades emergentes do contexto cibernético da atualidade.

Segundo o Inquérito SANS SOC 2025, 69% dos centros de operações de segurança (SOC) ainda recorrem a processos manuais para reportar métricas e apenas 42% utilizam ferramentas inteligentes baseadas em IA com algum grau de sofisticação que permita escalar a capacidade de deteção e resposta. Esta realidade tem impacto direto na eficácia da resposta a incidentes onde cerca de 61% das organizações, com serviço de SOC ativo, admitem já ter “ignorado” alertas críticos por falta de capacidade de processamento ou assertividade, que acabaram por resultar em falhas de segurança graves.

Este tipo de situações é grave, não só porque tem sido recorrente no mercado, mas sobretudo, pela falsa sensação de segurança que se estabelece no mindset das organizações quando se adquire um serviço de SOC sem garantir que este realmente contempla a capacidade de resposta e as necessidades específicas de cada organização. Adicionalmente, e no decorrer de uma escolha acertada assente na relação custo-benefício, atualmente, qualquer serviço de SOC terá de, no mínimo, apresentar a funcionalidade de deteção e resposta modernas, e principalmente, assentar em mecanismos de escalabilidade e inteligência. Essa terá de ser a responsabilidade de cada organização ao selecionar no mercado um serviço de SOC adequado a si própria.

No entanto, num contexto marcado por tantas falsas promessas em torno da IA, uma das áreas onde o valor é efetivamente real e mensurável, é na forma como a IA está a transformar a deteção e a resposta a incidentes. Não para



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

substituir o “emprego” dos analistas de segurança, mas antes para simplificar processos, eliminar tarefas repetitivas e libertar tempo para decisões de maior valor, sobretudo para as equipas que trabalham com inúmeras plataformas de segurança num ambiente cada vez mais complexo, e que obriga a decisões rápidas e assertivas sem grande margem de dúvida ou latência. Assim, a grande vantagem da integração de IA em plataformas de cibersegurança é principalmente em infraestruturas de SOC, onde a IA vem acrescentar valor na capacidade de tornar estas soluções e serviços mais automatizados e orientados, ao combinar automatização avançada com supervisão humana, permitindo maior eficiência operacional e capacidade de resposta.

Em Portugal, o apagão nacional verificado em abril de 2025 funcionou como um stress test

real à resiliência digital a nível nacional. Nesse contexto de desastre energético generalizado, e pelo facto de termos redundância na infraestrutura, mas também nas equipas operacionais por duas geografias distintas, permitiu que o SOC da VisionWare tenha sido, provavelmente, dos poucos a manter-se operacional a nível nacional e internacional, sem registo de qualquer quebra ou latência de serviço aos seus clientes, assegurando uma monitorização contínua e uma capacidade de resposta eficaz num momento tão crítico para o país. Obviamente que, para além de redundância de infraestrutura e equipas, também importa referir que, o SOC da VisionWare integra componentes de IA nos seus processos de deteção, análise e resposta e detém já uma plataforma desenvolvida 100% in-house que centraliza e processa de forma rápida, assertiva e inteligente toda a informação angariada dos nossos clientes, para que assim, as nossas equipas de analistas possam responder em tempo útil.

Esta situação de desastre e surpresa do apagão veio reforçar ainda mais a importância de se investir em arquiteturas resilientes, tecnologia inteligente e equipas especializadas capazes de garantir a continuidade operacional, a rapidez de decisão e a capacidade de adaptação em cenários de elevada pressão.

O verdadeiro valor estratégico da IA reside na sua capacidade de potenciar a capacidade, decisão e atenção humana, reduzir trabalho repetitivo e melhorar a consistência operacional, e não, “substituir as pessoas”; a IA deve funcionar de forma transparente e com mecanismos claros de escalabilidade, garantindo que as organizações mantêm controlo e acumulam conhecimento e eficácia operacional ao longo do tempo.

Os líderes que compreenderem esta diferenciação e alinhem a adoção da IA com o grau de maturidade compatível à sua organização, análise de risco e capacidade de governação conseguem posicionar as suas operações de segurança para escalar de forma sustentável, responder com maior taxa de precisão e manter a resiliência num cenário de ameaças cada vez mais complexo e exigente. ■

**INFO**  
[visionware.pt/](http://visionware.pt/)

20 anos



VisionWare  
since 2005

Porto | Lisboa | Praia | Mindelo

geral@visionware.pt

+351 225 323 740



SCAN ME

visionware.pt

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



**+100**

colaboradores



**+200**

clientes ativos



**5000**

projetos desenvolvidos

## Os nossos serviços



Cyber Defense  
Operations



Cybersecurity



Ethics & Compliance



Forensic  
Investigations



Privacy & Legal



Professional Services



Risk Intelligence



VisionWare Academy

Challenging an Unsafe World



# Zero Trust da WatchGuard: Transformar complexidade em valor para MSPs

Num cenário de ameaças cada vez mais sofisticadas e clientes mais exigentes, os MSPs precisam de ir além das ferramentas isoladas. A abordagem Zero Trust da WatchGuard transforma segurança avançada numa oferta simples, escalável e verdadeiramente vendável

**O**s Managed Service Providers vivem hoje um paradoxo desafiante: os clientes exigem níveis de segurança cada vez mais elevados, mas continuam a esperar simplicidade, previsibilidade de custos e impacto mínimo na operação diária. Ao mesmo tempo, o cenário de ameaças tornou-se mais sofisticado, mais automatizado e mais agressivo — e já não distingue grandes empresas de pequenas e médias organizações.

É neste contexto que o Zero Trust deixa de ser apenas uma tendência conceptual e passa a ser um modelo prático de prestação de serviços de segurança. Para os MSPs, a questão já não é se devem adotar Zero Trust, mas como o podem fazer de forma escalável, rentável e fácil de gerir. É precisamente aqui que a abordagem da WatchGuard Technologies se diferencia.

## ZERO TRUST COMO SERVIÇO — NÃO COMO PROJETO COMPLEXO

Historicamente, o Zero Trust foi visto como um projeto pesado, reservado a grandes empresas

com equipas dedicadas, múltiplas ferramentas e longos ciclos de implementação. Para MSPs, este modelo é simplesmente impraticável.

A WatchGuard adota uma visão diferente: Zero Trust como serviço gerível, integrado e vendável, desenhado desde a raiz para ambientes distribuídos, equipas reduzidas e múltiplos clientes. O WatchGuard Zero Trust Bundle não é um conjunto solto de tecnologias — é uma arquitetura coerente que permite aos MSPs entregar segurança moderna sem aumentar drasticamente a complexidade operacional.

O princípio é claro: verificar sempre, conceder apenas o acesso mínimo necessário e reavaliar continuamente o risco, com tudo orquestrado a partir de um único plano de controlo.

## PORQUE É QUE OS MSPS PRECISAM DE ZERO TRUST AGORA

Os dados são claros: as pequenas e médias empresas são hoje dos alvos preferenciais dos atacantes, mas continuam a estar entre as menos preparadas. Para os MSPs, isto

representa simultaneamente um risco e uma oportunidade.

Risco, porque um incidente grave num cliente pode comprometer a relação, a reputação e até a responsabilidade contratual do prestador de serviços.

Oportunidade, porque muitos clientes reconhecem finalmente que os modelos tradicionais — VPNs estáticas, passwords isoladas, firewalls sem contexto — já não são suficientes.

O Zero Trust permite aos MSPs reposicionar a conversa: deixar de vender ferramentas isoladas e passar a vender resultados de segurança, baseados em políticas, contexto e controlo contínuo.

## O ZERO TRUST BUNDLE COMO MOTOR DE EFICIÊNCIA

A grande vantagem da abordagem da WatchGuard para MSPs está na integração nativa dos seus componentes e na forma como estes se traduzem em serviços facilmente empacotáveis:

### • Identidade como novo perímetro

Com o WatchGuard AuthPoint, os MSPs podem implementar MFA, SSO e controlo de acesso baseado em identidade, reduzindo drasticamente o risco associado a credenciais comprometidas — hoje um dos principais vetores de ataque. A deteção de passwords

expostas na dark web acrescenta valor imediato e mensurável ao serviço.

#### • **Endpoint como ponto de decisão**

O EPDR da WatchGuard garante que apenas dispositivos confiáveis e verificados acedem aos recursos. Para o MSP, isto significa menos incidentes, menos tickets reativos e mais controlo preventivo, tudo gerido de forma centralizada.

#### • **Acesso moderno sem VPNs tradicionais**

Com o FireCloud Total Access, os MSPs podem substituir VPNs complexas e difíceis de manter por acesso baseado em aplicação, sessão e contexto. O resultado é menos fricção para o utilizador final e menos problemas de suporte para o prestador.

#### • **Gestão unificada na WatchGuard Cloud**

Talvez o ponto mais crítico para MSPs: todas as políticas, alertas e decisões de acesso são geridas a partir de uma única consola multi-tenant. Isto traduz-se em eficiência operacional, redução de custos e escalabilidade real.

### **MENOS FERRAMENTAS, MAIS MARGEM**

Um dos maiores desafios dos MSPs é o chamado tool sprawl: múltiplas soluções, múltiplas consolas, múltiplos contratos — e margens cada vez mais pressionadas.

A estratégia da WatchGuard aposta na consolidação inteligente: menos fornecedores, melhor integração e maior previsibilidade. Ao combinar identidade, endpoint e acesso seguro numa única oferta, os MSPs conseguem:

- Reduzir custos operacionais
- Simplificar formação das equipas
- Criar ofertas de segurança mais claras e fáceis de explicar aos clientes
- Aumentar a margem por cliente através de serviços recorrentes



O Zero Trust deixa assim de ser um custo adicional e passa a ser um fator de diferenciação comercial.

### **DO DISCURSO TÉCNICO À PROPOSTA DE VALOR**

Para muitos clientes finais, “Zero Trust” pode soar abstrato. Para os MSPs, a WatchGuard ajuda a traduzir o conceito em mensagens simples e vendáveis:

menos risco, menos interrupções, mais controlo e melhor experiência de utilizador.

Ao adoptar o Zero Trust Bundle, os MSPs não estão apenas a reforçar a segurança dos seus clientes — estão a evoluir o seu próprio modelo de negócio, passando de suporte reativo para prestação de serviços de segurança proactiva e contínua.

### **UMA PARCERIA PENSADA PARA CRESCER**

Para os MSPs, o sucesso não depende apenas da robustez da tecnologia, mas da capacidade de a transformar num serviço sustentável, escalável e alinhado com a evolução do mercado. A WatchGuard compreende esta realidade e estrutura a sua abordagem Zero Trust como uma parceria de crescimento, pensada para apoiar o canal a longo prazo.

Isso reflete-se numa plataforma concebida para ambientes multi-cliente, num modelo de licenciamento flexível que acompanha a maturidade dos clientes finais e numa clara aposta

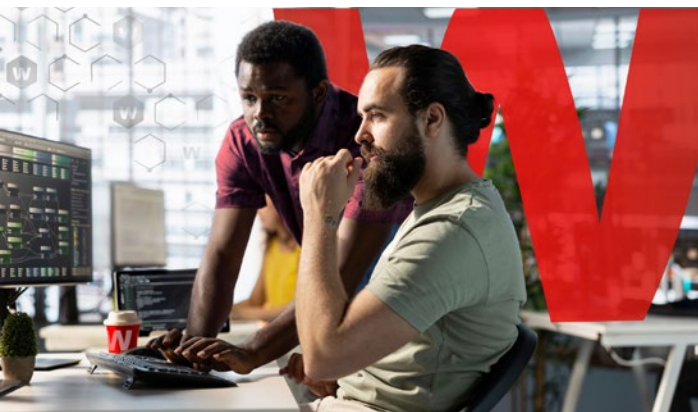
em receitas recorrentes. Em vez de soluções rígidas ou projetos pontuais, os MSPs ganham a possibilidade de construir ofertas adaptáveis, fáceis de gerir e simples de expandir.

A dimensão da capacitação é igualmente central. A WatchGuard investe em formação, certificação e apoio ao go-to-market, ajudando os parceiros a traduzir Zero Trust em propostas de valor claras, compreensíveis e relevantes para o negócio dos seus clientes. Este apoio reduz a fricção comercial e reforça o papel do MSP como consultor estratégico.

Num mercado onde a diferenciação é cada vez mais difícil, a WatchGuard posiciona-se como um aliado que simplifica a complexidade, reduz barreiras à adoção e cria bases sólidas para crescimento sustentado. Para os MSPs, isso significa menos esforço operacional e mais foco em gerar valor — hoje e no futuro. ■

**Com a WatchGuard, o Zero Trust deixa de ser um obstáculo técnico e passa a ser uma oportunidade estratégica — para proteger melhor os clientes finais e para construir serviços mais sólidos, previsíveis e rentáveis.**

**INFO**  
[watchguard.com](https://watchguard.com)



# O negócio do Canal em 2026: crescer com margem já não é opcional

O Canal português entra em 2026 num novo ciclo. O crescimento mantém-se, mas o contexto muda com o fim do PRR, maior pressão sobre custos e risco operacional acrescido. O desafio deixa de ser apenas crescer e passa a ser crescer com margem e capacidade

por *Jorge Bento*

## PONTOS-CHAVE

- *Crescimento acima da média, margem mais exposta;*
- *Fim do PRR muda o ciclo de investimento;*
- *Hardware com maior imprevisibilidade;*
- *IA e NIS2 aceleram mercado e risco;*
- *Serviços geridos sustentam margem;*
- *Execução passa a ser fator crítico.*

## CRESCER DEIXOU DE SER O PRINCIPAL DESAFIO DO CANAL

Nos últimos anos, o Canal habituou-se a falar de crescimento. Crescimento de faturação, de carteira de clientes, de projetos e de especialização. Esse crescimento aconteceu e trouxe sinais claros de maturidade. Há mais foco no segmento empresarial e no setor público, mais serviços, mais integração e menor dependência da transação pura.

À entrada de 2026, o debate muda de lugar. O crescimento continua, mas já não é o único indicador de saúde. Em muitos casos, é precisamente o crescimento que expõe fragilidades. Margens pressionadas, equipas curtas, projetos mais complexos, prazos mais rígidos e clientes com menor tolerância ao erro.

O Canal não entra num ciclo negativo. Entra num ciclo mais exigente, onde vender mais sem controlo pode sair caro.

## O CONTEXTO PORTUGUÊS E A MATURIDADE QUE AGORA É TESTADA

O Canal português tem razões para confiança. Há sinais de desempenho sólido e uma evolução que não surgiu por acaso. O mercado nacional aprendeu a operar em contexto de complexidade, desde a diversidade do tecido empresarial até ao peso do setor público e dos grandes programas estruturais.

Essa evolução puxou o Canal para competências de execução, integração e serviço. Em 2026, essa maturidade será colocada à prova. Os clientes vão exigir provas de valor, previsibilidade e capacidade de entrega.

Aqui surge uma linha clara de diferenciação. Quem souber operar e não apenas vender parte em vantagem. Quem depender sobretudo de desconto e volume vai sentir maior fricção.

## O FIM DO PRR E A TRANSIÇÃO PARA UM NOVO CICLO DE INVESTIMENTO

É impossível analisar o crescimento recente do setor sem reconhecer o impacto do Plano de Recuperação e Resiliência (PRR). Mesmo quando não foi o motor direto de um projeto, o PRR acelerou decisões de investimento em IT e digitalização que, noutro contexto, teriam sido adiadas ou diluídas no tempo.

Portugal tem uma dotação global de 22,2 mil milhões de euros, com cerca de 21% associada à transição digital. Na prática, isso colocou dinheiro e urgência em modernização de infraestruturas, cibersegurança, digitalização de serviços públicos e capacitação tecnológica.

O PRR tem, no entanto, um calendário definido. Os Estados-membros têm de cumprir marcos e metas até 31 de agosto de 2026, com pagamentos finais previstos até 31 de dezembro



---

do mesmo ano. O ponto central não é o fim do PRR. É a mudança de lógica.

Sem essa almofada, o investimento passa a ser cada vez mais suportado diretamente pelos clientes. Haverá mais escrutínio, maior exigência de retorno e menor tolerância ao erro. Para o Canal, isto não elimina oportunidades. Filtra-as. Obriga a propostas mais sólidas, a uma conversa mais exigente sobre valor e a um modelo comercial menos impulsivo.

### **HARDWARE MENOS PREVISÍVEL E IMPACTO DIRETO NA EXECUÇÃO**

O hardware voltou a ser um tema estratégico, não por inovação, mas por disponibilidade, prazos e custo. A escassez de componentes já não é apenas um eco do passado recente. Está a ser reforçada por uma transformação estrutural, com a indústria a canalizar capacidade para infraestruturas de IA e a apertar o resto do mercado.

A memória é um dos sinais mais claros. Fabricantes e analistas apontam para procura acima da oferta em 2026, com tensão prolongada para 2027 e preços sob pressão. Há segmentos com capacidade já comprometida, o que levou os próprios fabricantes a reforçar controlos sobre encomendas e alocação.

Para Parceiros mais transacionais, isto traduz-se em margens ainda mais vulneráveis. Para Parceiros de projeto, significa risco operacional acrescido. Prazos que derrapam, custos que mudam e alternativas que têm de ser validadas sob pressão. Em 2026, gerir hardware é gerir expectativas, planeamento e contratos alinhados com a realidade do *supply*.

### **SERVIÇOS, RECORRÊNCIA E OPERAÇÃO COMO BASE DO CRESCIMENTO SAUDÁVEL**

É precisamente num contexto mais volátil que os serviços ganham centralidade. *Managed Services*, operação contínua, suporte especiali-

zado, observabilidade, continuidade de negócio e segurança gerida passam a ser a base do crescimento sustentável.

A recorrência é mais do que previsibilidade financeira. É o mecanismo que permite absorver a volatilidade do hardware, a pressão sobre custos e o maior escrutínio do investimento. Também cria proximidade real com o cliente, ao transformar o Parceiro numa parte ativa da operação.

Em 2026, a margem constrói-se mais na operação do que na venda pontual. Isso favorece quem tem processos, disciplina e capacidade de execução consistente.

### **IA, CIBERSEGURANÇA E NIS2 EM 2026**

A Inteligência Artificial (IA) é um dos principais motores de crescimento do setor a médio prazo. Não existe isoladamente nem pode ser tratada como uma camada adicional. Exige dados, redes, armazenamento e computação. Como efeito colateral, aumenta a pressão sobre componentes críticos e contribui para um mercado mais tenso.

Ao mesmo tempo, reforça a centralidade da cibersegurança. A entrada em vigor da NIS2, já em abril, transforma a segurança de opção técnica em obrigação operacional. Mais dados críticos, mais automação e mais integrações aumentam a superfície de ataque e o risco, também para os Parceiros que integram, operam e garantem continuidade.

A mensagem é simples. IA sem cibersegurança e sem conformidade não é inovação. É exposição. Existe aqui uma oportunidade clara para o Canal, desde que haja capacidade para entregar com responsabilidade, da governação de dados à proteção de ambientes híbridos e à monitorização contínua.

### **PESSOAS, EXECUÇÃO E MARGEM COMO LIMITE REAL DO CRESCIMENTO**

O verdadeiro limite do crescimento em 2026 não está no mercado. Está dentro das organi-

zações. Talento escasso, pressão salarial, maior complexidade e exigência de serviço contínuo criam um bloqueio real.

A tentação de aceitar tudo para crescer pode ser a forma mais rápida de destruir margem e reputação. A disciplina passa por escolher clientes, escolher projetos, empacotar serviços, automatizar onde for possível e investir apenas onde a margem se defende. Crescer com controlo torna-se uma competência tão valiosa como vender.

### **2026 COMO ANO DE ESCOLHAS CONSCIENTES**

2026 não é um ano de rutura. É um ano de escolhas. O fim do PRR altera a lógica do investimento, o hardware tornou-se menos previsível e a pressão sobre prazos, custos e capacidade de entrega é real. Ao mesmo tempo, IA, cibersegurança e NIS2 continuam a puxar o mercado, mas exigem mais planeamento, mais responsabilidade e mais capacidade operacional.

Neste contexto, crescer deixa de ser uma decisão automática. Passa a ser uma escolha estratégica. Escolher onde investir, que clientes priorizar, que projetos aceitar e que modelos de serviço escalar. O mercado vai continuar a oferecer oportunidades, mas já não recompensa quem cresce por volume ou por impulso.

O Canal que sai reforçado em 2026 é o que conhece os seus limites, controla a execução e protege a margem. É o que estrutura serviços, clarifica propostas de valor e alinha contratos com a realidade operacional. É também o que investe em pessoas e processos com critério, sabendo que capacidade e qualidade são hoje fatores tão críticos como tecnologia.

Há espaço para o Canal português continuar a crescer, porque o mercado valoriza execução, serviço e confiança. Em 2026, não vencerá quem cresce mais depressa, mas quem cresce de forma sustentável, com margem, estrutura e controlo. ■

# O Canal na Era da IA: Como Transformar a Inovação em Rentabilidade Sustentável

Com a Inteligência Artificial a migrar da cloud para o dispositivo e para a periferia (edge), os parceiros enfrentam o desafio de evoluir da revenda tradicional para a entrega de soluções inteligentes. Na Lenovo, acreditamos que este salto tecnológico é a maior oportunidade de crescimento da década, mas o sucesso dependerá da capacidade de aliar um portfólio abrangente a uma estratégia de serviços sólida



O panorama do setor tecnológico está a mudar a uma velocidade sem precedentes. Dados recentes da Canalys indicam que, em 2026, mais de 53% dos computadores expedidos a nível global já são “AI-capable”. Este não é apenas um ciclo de renovação de hardware; é uma mudança de paradigma que redefine a produtividade empresarial. Para o canal em Portugal, esta tendência representa uma janela de oportunidade crítica: quem souber posicionar o valor da IA Híbrida não estará apenas a vender equipamento, estará a preparar o futuro dos seus clientes.

## UM PORTEFÓLIO SEM SILOS: O TRUNFO DA LENOVO

Atualmente, o mercado exige mais do que o equipamento como uma commodity. A tendência dominante é a IA Híbrida, um modelo onde a inferência de dados acontece localmente, assegurando a privacidade, a

baixa latência e a eficiência de custos para as organizações. As previsões mais recentes apontam para que o investimento em serviços de TI cresça de forma mais acelerada do que a venda direta de hardware (cerca de 9,6%), o que obriga o canal a procurar margens na integração de soluções. É precisamente neste ponto que a Lenovo diferencia a sua proposta de valor, permitindo que o parceiro aproveite um portfólio que não conhece silos. Ao integrar as unidades de negócio de dispositivos, infraestrutura e serviços, oferecemos uma base sólida para que o canal possa vender soluções “end-to-end”, uma infraestrutura capaz de correr modelos de linguagem locais (LLM) com segurança, apoiada por soluções que escalem à medida das necessidades do negócio.

## LENOVO 360: EQUIPAR O CANAL PARA VENCER

Sabemos que a tecnologia, por si só, não garante o sucesso do negócio. No centro desta estra-

tégia de crescimento está a visão de “Smarter AI for All”. Para os parceiros, isto traduz-se no acesso a ferramentas que lhes permitem endereçar áreas de volume, mas também de maior rentabilidade, como as workstations ou sistemas desenhados para salas de colaboração. No entanto, o crescimento sustentável em 2026 exige olhar para além do posto de trabalho. Áreas como o Edge Computing e os servidores preparados para a IA generativa são onde a verdadeira diferenciação acontece. Além disso, a adoção de modelos de consumo flexíveis, como o TruScale (as-a-service), permite que os parceiros gerem receita recorrente e previsível, um fator vital para a saúde financeira do canal num mercado que valoriza cada vez mais a previsibilidade financeira que o DaaS ou IaaS proporcionam.

Mas vamos mais longe. Para aumentar a rentabilidade dos nossos parceiros, colocamos à disposição o nosso portal de parceiros que permite autonomia e rapidez no acesso às cotações; especialistas dedicados nas diferentes áreas, que ajudam a desenhar arquiteturas personalizadas para cada cliente; um programa de incentivos que valoriza não apenas o volume de vendas, mas também a especialização em áreas estratégicas;

## CONCLUSÃO: O MOMENTO DE AGIR É AGORA

O crescimento para os parceiros em 2026 será fruto da especialização. Os parceiros que abraçarem a transição para a IA, apoiados por um fabricante que oferece inovação, que seja competitivo, estável, e que esteja presente para os apoiar serão os líderes do mercado. A Lenovo continua empenhada em ser esse parceiro, em conjunto com os seus distribuidores, fornecendo os meios — tecnológicos e financeiros — para que cada projeto se traduza em valor real para o cliente e rentabilidade para o parceiro. O futuro é inteligente, é híbrido e, acima de tudo, é construído em parceria. ■

## INFO

[lenovo.com/pt/pt/](https://lenovo.com/pt/pt/)

## Lenovo Workstation Solutions

# ThinkStation PGX

## Personal AI Developer Workstation

- Powerful Small Form Factor AI Device
- Personal and/or Remote (Headless/Node) Usage
- NVIDIA DGX OS (Linux) + AI Software Stack
- NVIDIA ConnexxtX7 Smart-NIC
- Optional Multi-PGX Cluster Support
- Aprox. 400B Parameter LLM Support



2025 ©Lenovo. All rights reserved.

Lenovo is not responsible for photographic or typographic errors. Lenovo makes no representation or warranty regarding third-party products or services.

LENOVO, ThinkStation, and ThinkPad are trademarks of Lenovo. NVIDIA, NVIDIA RTX PRO, NVIDIA DGX, and NVIDIA ConnectX are trademarks and/or registered trademark of NVIDIA Corporation in the U.S. and other countries. Intel, Intel vPro, Core, Xeon, and Thunderbolt are trademarks of Intel Corporation or its subsidiaries. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Microsoft and Windows are registered trademarks of Microsoft Corporation. Other company, product, and service names may be trademarks or service marks of others.

## Brother aposta em impressão A3 inteligente para pequenas empresas

**A** Brother anunciou o lançamento da nova gama Business Smart de equipamentos de tinta A3, desenvolvida para responder às necessidades de escritórios em casa (SOHO), pequenas empresas e pequenas e médias empresas (PME). A oferta inclui os modelos MFC-J6760DW e MFC-J6960DW, bem como o MFC-J6975DW X Series.

A nova gama integra o chip de impressão MAXIDRIVE, que permite velocidades mais elevadas e maior precisão. A combinação entre manutenção automática, componentes duradouros e tintas pigmentadas assegura impressões consistentes, com cores vivas e texto nítido, mesmo em ambientes de utilização intensiva. Os modelos Business Smart A3 oferecem funções completas de impressão, digitalização, cópia e fax a cores até ao formato A3, com conectividade via PC, dispositivos móveis ou USB. Através da aplicação Brother Mobile

Connect, os utilizadores podem configurar os equipamentos, imprimir e digitalizar remotamente, acompanhar os níveis de tinta e personalizar atalhos, facilitando a gestão do dia a dia.

O modelo MFC-J6975DW X Series, destinado a PME, acrescenta capacidades avançadas de gestão e compatibilidade com soluções de terceiros. Inclui um novo sistema de tinteiros concebidos para remanufatura, com redução do desperdício de tinta e rendimentos até 12 mil páginas a preto e dez mil páginas a cores, permitindo volumes elevados de impressão a custos controlados. Este modelo destaca-se ainda pela aposta na sustentabilidade, integrando materiais reciclados, embalagens sem EPS, uma redução de 4% nas emissões de CO2 face à geração anterior e certificação ambiental Blue Angel.

Ao nível da gestão, o X Series é compatível com soluções da Brother como Secure Print+,



Custom UI e impressão de códigos de barras, bem como com plataformas de terceiros como Tungsten e Ysoft. Os administradores de IT beneficiam de funcionalidades de gestão remota do parque de impressão, reduzindo tempos de inatividade e simplificando a manutenção. ■

## NOVA SÉRIE DA D-LINK APOSTA EM DESEMPENHO PARA AMBIENTES EMPRESARIAIS

**A** D-Link apresentou a nova série DGS-1530 de switches Smart Managed Pro, concebida para responder às necessidades de comutação na camada de agregação ou na extremidade da rede em ambientes empresariais. A gama disponibiliza modelos com dez a 52 portas Gigabit, opções com portas de fibra ótica, *uplinks* 10 Gigabit SFP+ e empilhamento físico de até nove unidades.

Segundo o fabricante, a série DGS-1530 distingue-se pela flexibilidade de configuração e pelas capacidades avançadas de gestão, integrando funcionalidades como VLAN avançadas, *static routing* L3, agregação de ligações e mecanismos de redundância como ERPS e Multiple Spanning Tree. Estas características permitem a sua utilização tanto em redes de



campus como em infraestruturas empresariais de média dimensão.

A gama inclui modelos com suporte para Power over Ethernet, permitindo alimentar dispositivos como pontos de acesso Wi-Fi, câmaras IP, telefones IP ou sistemas de vídeo e áudio IP através do mesmo cabo de rede. O orça-

mento PoE pode atingir 370 W e chegar aos 740 W com recurso a uma fonte de alimentação redundante opcional.

Entre os destaques técnicos encontram-se as portas 10G SFP+ para *uplinks* ou empilhamento, proteção contra sobretensões até 6 kV em todas as portas Ethernet e a disponibilidade de um modelo exclusivamente com portas de fibra ótica. A gestão pode ser realizada através de interface Web ou linha de comandos, com suporte para SNMP e OAM.

A D-Link sublinha ainda a adequação da série DGS-1530 a cenários de AV sobre IP e tráfego multicast. Funcionalidades como IGMP/MLD Snooping e ISM VLAN permitem otimizar a distribuição de fluxos multicast, reduzindo tráfego redundante e melhorando o desempenho em aplicações como IPTV, *streaming* de vídeo e ambientes audiovisuais profissionais.

A nova gama DGS-1530 já se encontra disponível através da rede de distribuidores e Parceiros certificados da D-Link, com preços de venda ao público recomendados a partir de 554 euros. ■



## ASUS REFORÇA APOSTA EM COMPUTAÇÃO COM IA E APRESENTA NOVOS PC COPILOT+

**A** Asus apresentou no CES 2026 a sua nova família de PC Copilot+ com Inteligência Artificial (IA), reforçando a aposta em desempenho, criatividade e produtividade para criadores, profissionais e consumidores. A nova geração integra as mais recentes plataformas de processamento da AMD, Intel e Qualcomm, aliadas a aplicações Asus AI exclusivas.

Entre os principais destaques está o ProArt GoPro Edition (PX13), desenvolvido em

Parceria com a GoPro e vencedor de um CES Innovation Award 2026. Este portátil conversível de 13 polegadas integra acesso direto à GoPro Cloud e à aplicação StoryCube com IA, permitindo organizar, editar e categorizar conteúdos, incluindo vídeo 360°, diretamente no dispositivo. O modelo combina um processador AMD Ryzen AI Max+ 395, até 128 GB de memória unificada e um ecrã tátil OLED 3K.

A gama ProArt inclui ainda o ProArt PX13, orientado para criação de conteúdos avançada com suporte para modelos de IA de grande dimensão, e o ProArt PZ14, um tablet destacável ultraleve de 14 polegadas, equipado com Snapdragon X2 Elite, direcionado a criadores em mobilidade.

No segmento de consumo premium, o Zenbook DUO 2026 destaca-se pelo novo design em Ceraluminum e pelos dois ecrãs

OLED 3K de 14 polegadas, combinados com um processador Intel Core Ultra X9 Série 3. O modelo aposta na produtividade em dois ecrãs, com melhorias ao nível da dobradiça, autonomia e desempenho térmico, sendo também distinguido com um prémio de inovação na CES 2026.

A Asus apresentou ainda os novos Zenbook A16 e A14, equipados com processadores Snapdragon X2 Elite e X2 Elite Extreme, focados em portabilidade, autonomia prolongada e desempenho de IA, bem como a renovada série Zenbook S e a gama Vivobook S.

O ecossistema de IA é complementado por novos *desktops* e PC *all-in-one*. Entre eles, destaca-se o Asus VM441QA AiO, o primeiro *all-in-one* do mundo equipado com processador Snapdragon, e os *desktops* da série V, que integram capacidades Copilot+ para uso doméstico e profissional. ■

## Epson apresenta novo projetor 4K real de curta distância

**A** Epson anunciou o lançamento do Lifestudio Grand EH-LS970, o novo topo de gama da marca em projetores de curta distância para home cinema. Com resolução 4K real, elevada luminosidade e integração de Google TV, o novo modelo foi concebido para proporcionar uma experiência cinematográfica de alta qualidade, aliando desempenho tecnológico a um design premium.

Sucessor do modelo EH-LS800, o EH-LS970 baseia-se no sucesso da série Lifestudio Grand EH-LS670 e oferece 8,3 milhões de píxeis reais em resolução 4K UHD (3840 × 2160). Graças à tecnologia laser 3LCD, o projetor garante imagens luminosas, sem efeito arco-íris, com uma luminosidade de quatro mil lúmenes e uma relação de contraste dinâmico de 5.000.000:1. O formato de distância ultracurta permite projetar imagens até 150 polegadas a apenas

alguns centímetros da parede, tornando-o adequado para salas de estar modernas sem necessidade de instalações complexas. O equipamento integra ainda um motor de otimização de imagem com tecnologia de inteligência artificial, concebido para ajustar automaticamente a qualidade visual de acordo com o conteúdo.

Ao nível do áudio, o projetor inclui um sistema de som Bose com suporte Dolby Audio. A plataforma Google TV integrada dá acesso direto a aplicações de *streaming*, incluindo a Netflix, enquanto o modo de jogo ALLM assegura baixa latência, inferior a 20 ms, para uma experiência fluida em videojogos.

O funcionamento silencioso, com apenas 29 dB (ou 18 dB em modo silencioso), a fonte de luz laser com durabilidade até 20 mil horas e a aplicação Epson Setting Assistant, que permite uma configuração guiada através do smart-



phone, reforçam a facilidade de utilização do equipamento.

A Epson sublinha também o compromisso com a sustentabilidade, através de modos de baixo consumo energético, utilização de uma fonte de luz de longa duração, embalagens recicláveis e uma garantia de cinco anos.

O Epson Lifestudio Grand EH-LS970 estará disponível no mercado a partir de abril de 2026. ■

# Caiado consolida segurança e reforça Parcerias com a ajuda da WatchGuard e da inCentea

A Caiado reforçou a sua estratégia de cibersegurança com soluções WatchGuard, num projeto desenvolvido com a inCentea que permitiu consolidar a gestão, aumentar a visibilidade e reduzir riscos operacionais

por Marta Quaresma Ferreira



**A** Caiado conta com mais de 50 anos de experiência na área da iluminação e do material elétrico, num percurso marcado pela evolução, que procura aliar a tradição à inovação.

Com uma aposta na proximidade aos clientes, a segurança da informação tornou-se uma prioridade para a organização que procura, há vários anos, soluções que garantam a proteção integral das operações, desde os dispositivos, até às redes, passando pelos utilizadores.

“Antes da WatchGuard tínhamos várias soluções isoladas. Eram difíceis de gerir e não tínhamos a visibilidade centralizada. Com o crescimento da infraestrutura, tornou-se essencial garantir a monitorização em tempo real, o controlo de acessos remotos, a gestão de atualizações e respostas a vulnerabilidades”, começa por explicar Alexandre Costa, Responsável de Sistemas de Informação da Caiado.

## PROJETO BASEADO NUM PARCEIRO DE CONFIANÇA

A resposta passou por um portfólio modular e escalável, ajustado às necessidades reais da

organização, e com a implementação a cargo da inCentea, Parceiro tecnológico de longa data da Caiado.

A escolha do cliente recaiu na Plataforma de Segurança Unificada da WatchGuard, que garantia, desde logo, uma “gestão cloud acessível em qualquer lado”, tal como explica Alexandre Costa, que destaca ainda a flexibilidade e o licenciamento e expansão como fatores decisivos para a escolha da solução. O projeto garantiu a implementação de um conjunto de soluções integradas e geridas, desde firewalls, autenticação multifator, passando por segurança de *endpoints* e Wi-Fi seguro.

Na perspetiva de Lúcio Crespo, Project & Service Manager da inCentea, “a implementação desta solução permitiu à Caiado transformar a sua abordagem à cibersegurança, adotando uma solução integrada, automatizada e escalável”.

A visibilidade em tempo real, combinada com a capacidade de resposta automatizada, contribuiu para “posicionar a empresa num patamar superior de maturidade de segurança, substituindo eficazmente as soluções *legacy* por uma arquitetura de segurança moderna e integrada”.

## MAIS-VALIAS DO PROJETO

Soluções como a WatchGuard Firebox, AuthPoint, EPDR e Patch Management permitiram à empresa de material elétrico “unificar num só painel, agir de forma preventiva e reduzir riscos de segurança”, reforça o responsável de IT da Caiado.

Um dos exemplos das vantagens da implementação, recorda Alexandre Costa, aconteceu durante a pandemia de COVID-19: “Já tínhamos o MFA implementado, o que nos deu uma enorme vantagem. Conseguimos migrar os postos para casa com toda a segurança e tranquilidade”.

Fábio Ribeiro, Sales Engineer da WatchGuard considera que “a inCentea tem tido um papel fundamental em ajudar o cliente, não só porque o conhece muito bem, mas também porque tem um grande domínio técnico sobre as nossas soluções, implementando-as e gerindo-as da forma mais correta”. Na sua visão, “a proximidade com o cliente permite continuar a evoluir o modelo de segurança”.

O fabricante tem caminhado em conjunto com a Caiado na resolução de diversas preocupações, principalmente no que toca a ameaças mais avançadas. Fábio Ribeiro recorda que, perante um cliente que conta com diversas soluções WatchGuard, o fabricante tem a “capacidade de entregar XDR, o que permite responder às ameaças até numa fase muito embrionária”.

A cibersegurança assume, assim, um papel central na estratégia de negócio da Caiado, que aposta em continuidade, confiança e Parceria. ■

## RESUMO

- A Caiado apostou numa plataforma unificada da WatchGuard para garantir uma gestão centralizada de segurança;
- A implementação esteve a cargo da inCentea, Parceiro tecnológico de longa data;
- Firewalls, MFA, segurança de endpoint e XDR permitiram aumentar a maturidade de segurança.

# Xplor aposta em especialização para ajudar a transformar organizações através da tecnologia

Com foco no ecossistema Sage, a Xplor afirma-se como integrador tecnológico, com presença em vários mercados. O Parceiro combina especialização em gestão empresarial com uma estratégia de expansão internacional

por Marta Quaresma Ferreira

“**A** tecnologia só cria valor quando está verdadeiramente alinhada com o negócio das empresas”. Este foi o ponto de partida para a criação da Xplor, em 2012.

O Parceiro português, que começou no ecossistema Sage, apresenta-se como um integrador de tecnologia, cuja proposta de valor assenta em três pilares: *Business Applications*, *Infra & Cybersecurity* e ESG.

Em Portugal, a Xplor posiciona-se como um Parceiro tecnológico para empresas do segmento médio-alto e é reconhecido pela especialização em soluções de gestão empresarial e pela capacidade de integrar a tecnologia de forma estratégica.

O negócio expande-se além-fronteiras, com presença no Reino Unido, Polónia e Brasil, onde o Parceiro é Master Reseller do Sage X3 para a América Latina e responsável pelo desenvolvimento e manutenção da localização brasileira da solução.

“Olhamos para o mercado como sendo global, muito focados nas necessidades de organizações com operações internacionais e níveis elevados de complexidade”, explica Tiago Baptista, CEO da Xplor, que recorda o propósito que esteve na base da criação da empresa: “ajudar as organizações a crescer, inovar e transformar-se através de tecnologia com impacto real no negócio”.

## CRESCIMENTO SEMPRE PRÓXIMO DO CLIENTE

Setores como a indústria transformadora, a distribuição, os serviços profissionais, a tecnologia e as operações multinacionais têm contribuído para o crescimento da Xplor, que aponta também para um “crescimento consistente” em áreas como o retalho e a logística.



Tiago Baptista, CEO da Xplor

“O principal objetivo da Xplor é criar valor real e sustentável para os seus clientes através da tecnologia. Trabalhamos para tornar as organizações mais eficientes, mais seguras e mais preparadas para um contexto de negócio cada vez mais exigente”, afirma o CEO.

Com uma aposta em equipas altamente qualificadas, investimento contínuo em conhecimento, certificações e novas áreas de competência, o foco a médio e longo prazo passa por, como explica Tiago Baptista, “liderar nos mercados onde já operamos, reforçando áreas estratégicas, e crescer de forma estruturada a nível internacional, mantendo sempre a proximidade com os clientes e a qualidade do serviço como prioridades”.

## PRINCIPAIS PARCEIROS E SOLUÇÕES

O Parceiro conta atualmente com cerca de cem colaboradores, entre eles consultores certificados em soluções Sage *mid-market*. A Xplor tem também procurado reforçar as equipas nas áreas de cloud, cibersegurança, ESG e inteligência artificial para garantir uma “abordagem multidisciplinar”.

Para além da “relação estratégica de longa data” com a Sage – que já valeu o estatuto de Platinum Partner –, o Parceiro procura complementar o trabalho com outras parcerias com a C-More, com a Ethiack e a Fortinet.

Entre as soluções que garantem eficiência, controlo e escalabilidade, Tiago Baptista destaca o ERP da Sage, o X3, e o XRT, uma solução de *cash management* e comunicação bancária. O CEO identifica também um “crescimento muito significativo” na área de *Infra & Cybersecurity*, em especial soluções cloud.

## CONSOLIDAR E ACELERAR: VERBOS PARA PROJETAR O FUTURO

Ainda que o ambiente de negócios português apresente “desafios estruturais”, o CEO não tem dúvidas de que “existem oportunidades claras associadas à transformação digital, à cibersegurança e à sustentabilidade”.

O Parceiro tem como estratégia “consolidar a liderança em Portugal e acelerar o crescimento internacional”, depois dos dados do último exercício darem conta de um crescimento de 15%. Para 2026, o plano passa por atingir um volume de negócios próximo dos dez milhões de euros, resultantes de um crescimento orgânico, combinado com “a avaliação seletiva de oportunidades de crescimento inorgânico”, justifica Tiago Baptista.

Se no mercado nacional o futuro passa por investir na especialização e no reforço das áreas *core*, a nível internacional o objetivo é “crescer nos mercados onde já temos presença relevante” e expandir e reforçar o investimento em Espanha. “Em qualquer mercado, o nosso objetivo é claro: criar valor real para os clientes e afirmar a Xplor como Parceiro tecnológico de referência.” ■

## RESUMO

- A Xplor iniciou a sua atividade focado no ecossistema Sage;
- *Business Applications*, *Infra & Cybersecurity* e ESG são as três áreas estratégicas;
- No último exercício, a empresa cresceu cerca de 15%.

# Da manutenção reativa à governação inteligente: AMS como pilar estratégico



por **Luís Filipe Freitas**,  
Vice-President Consulting Delivery, CGI



e da automação reforça essa tendência, mas a verdadeira transformação depende sobretudo da forma como olhamos para esta área e do papel que lhe atribuímos.

A Manutenção e Suporte de Aplicações deve ser entendida como uma camada de governação inteligente, capaz de assegurar que cada aplicação – seja nova, antiga ou em transição – continua a gerar valor, permanece segura e evolui ao ritmo das expectativas dos utilizadores. Quando mais de metade dos orçamentos de IT continuam a ser direcionados para operação e manutenção, e quando grande parte das interrupções resulta de mudanças mal compreendidas ou requisitos incompletos, a forma como gerimos pedidos, requisitos e melhorias torna-se tão determinante quanto a própria tecnologia. A complexidade em torno das aplicações empresariais é um reflexo direto do que os estudos mais recentes têm vindo a mostrar: as organizações aumentaram substancialmente o número de aplicações que suportam, o que elevou não só o volume de manutenção, mas também o risco de incompatibilidades e falhas de integração.

O mais recente estudo CGI Voice of Our Clients confirma esta pressão crescente. Apesar de se observar uma melhoria no retorno das iniciativas de digitalização, quase metade dos executivos inquiridos identifica os seus sistemas antigos ou obsoletos como uma das principais barreiras à obtenção de sucesso digital. Esta realidade reforça a importância estratégica da Manutenção e Suporte de Aplicações. Num cenário em que os sistemas limitam a modernização e dificultam a obtenção do valor pleno das iniciativas digitais, a forma como se gere a manutenção, a evolução e a integração das aplicações torna-se decisiva.

Ao mesmo tempo, a emergência de tecnologias de Inteligência Artificial, Machine Learning e Processamento de Linguagem Natural está a

transformar profundamente este domínio. Hoje, a IA já permite detetar ambiguidades, inconsistências e impactos entre requisitos, algo que antes exigia longas revisões manuais. Sistemas inteligentes adaptam formulários, questionários e pedidos ao contexto específico de cada organização, reduzindo erros e melhorando a qualidade da informação recolhida. A automação acelera tarefas repetitivas, classifica pedidos de forma inteligente e até antecipa incidentes. E, graças aos avanços em linguagem natural, a comunicação informal dos utilizadores pode ser convertida em requisitos claros e estruturados, reduzindo perdas de contexto e aproximando o negócio da tecnologia.

Este movimento não resulta apenas em eficiência. Representa um novo modelo operativo, mais rápido, mais inteligente e mais alinhado com as necessidades reais das organizações. Organizações que continuarem a encarar a manutenção como uma função reativa arriscam consolidar um défice tecnológico difícil de recuperar, perder agilidade e comprometer a experiência dos utilizadores. Pelo contrário, aqueles que encaram a área de AMS como uma plataforma de governação inteligente, suportada por processos modernos e reforçada por capacidades de IA, estarão mais bem preparados para crescer, inovar e modernizar com segurança.

Num contexto marcado pela escassez de talento, pela pressão por eficiência e pela aceleração digital, repensar o papel da área de AMS é uma das decisões mais impactantes que as lideranças podem tomar. Talvez a questão já não seja “como manter as aplicações”, mas antes “como garantir que continuam a gerar valor”. E essa resposta passa, inevitavelmente, por uma nova visão da Manutenção e Suporte de Aplicações: estratégica, integrada e essencial para a transformação digital sustentável. ■

O contexto empresarial atual demonstra claramente que a tecnologia deixou de ser apenas um suporte operacional para assumir o papel de motor da transformação. Contudo, à medida que as organizações acumulam sistemas, camadas tecnológicas, integrações e aplicações críticas, cresce também a dificuldade de os manter, modernizar e alinhar com objetivos que mudam cada vez mais depressa. É precisamente aqui que a Manutenção e Suporte de Aplicações (AMS) ganha uma relevância estratégica que nem sempre é reconhecida.

Durante muito tempo, a AMS foi vista como uma função essencialmente reativa, dedicada a corrigir incidentes, resolver problemas e garantir a continuidade dos sistemas. Hoje, por imperativos estratégicos, está no centro da eficiência operacional, da estabilidade das operações e da capacidade de adaptação das empresas. A evolução da inteligência artificial

in



## Entre a escala e a independência

por **Jorge Bento**

**N**os últimos dois anos, o Canal português de serviços IT entrou num novo ciclo. A aquisição de Parceiros nacionais por empresas internacionais e fundos de investimento acelerou de forma clara, com mais de uma dezena de operações conhecidas num mercado que, pela sua dimensão, raramente assistia a movimentos desta escala. Não se trata de episódios isolados, mas de uma tendência estrutural.

Este movimento era antecipável desde 2020, quando a elevada liquidez dos fundos começou a procurar ativos com retorno previsível. A consolidação iniciou-se nos principais mercados europeus e só mais tarde chegou a Portugal, muitas vezes de forma indireta, através de grupos espanhóis já adquiridos. Em paralelo, alguns fabricantes, pressionados por mercados estagnados, optaram por reforçar a área de serviços através da compra de empresas já em operação, por ser a via mais rápida para ganhar escala e capacidade de execução.

A lógica de gestão destes novos acionistas difere da tradição do Canal português. O foco está na margem no curto prazo e na eficiência financeira. Fatores como cultura, identidade local ou relação histórica com clientes tendem a perder peso. Isso ajuda a explicar os choques culturais

após as aquisições e a saída frequente dos fundadores, seja por acordo prévio ou por desgaste. Num mercado onde algumas empresas têm segundas linhas frágeis, o risco de perda de continuidade é real.

Para os fabricantes, a escala é, em regra, benéfica. Menos Parceiros, mas maiores e mais estruturados, facilitam a gestão do ecossistema e a previsibilidade da execução. Para os Parceiros independentes, o cenário é mais exigente. Num mercado mais concentrado, a ausência de relações fortes com fabricantes e distribuidores pode traduzir-se em perda de relevância.

Ainda assim, a independência continua a ser uma oportunidade. Os Parceiros que permanecem fora da consolidação não estão condicionados por KPI externos nem por ciclos financeiros impostos. Isso permite maior agilidade, maior proximidade ao cliente e liberdade para ajustar propostas e modelos de serviço. O desafio está em transformar essa liberdade numa vantagem competitiva clara.

A consolidação não é boa nem má por definição. É um sinal de maturidade do mercado. O impacto dependerá das escolhas feitas por investidores, fabricantes e Parceiros. Entre a escala e a independência, esse equilíbrio será determinante para o futuro do Canal português. ■

ANCHOR



## O caminho em construção para o data center fotónico

por **Henrique Carreiro**

**A** fotónica já faz parte do data center há anos: sempre que um *link* é feito por fibra, a informação viaja em forma de luz. O que está a mudar é o ponto onde a luz entra na arquitetura. Em vez de ficar limitada ao “transporte”, começa a aproximar-se dos locais onde hoje se perdem watts e nanossegundos: a interligação dentro do *rack*, entre *racks* e, em alguns casos, partes do próprio processamento.

Há duas frentes distintas nesta transformação. A primeira é rede/*interconnect*. Aqui, o objetivo é aumentar largura de banda e reduzir o custo energético do I/O, sobretudo em clusters de IA, onde a comunicação entre aceleradores e *switches* cresce mais depressa do que a capacidade de manter tudo em cobre ou em módulos óticos tradicionais. É nesta linha que surgem abordagens como *co-packaged optics* (ótica colocada junto do ASIC do *switch*, em vez de módulos *pluggable* na face do equipamento) e *silicon photonics* (integração das funções óticas em circuitos integrados), para encurtar o percurso elétrico de alta velocidade e reduzir o custo energético por bit.

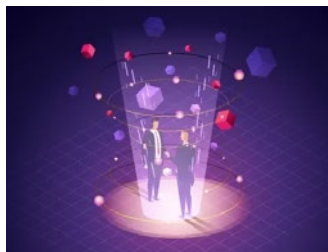
A segunda frente é computação fotónica, com circuitos integrados fotónicos a executar operações específicas (muito centradas, atual-

mente, em processamento matricial). Em vez de substituir CPU, estas abordagens aparecem como aceleradores para tarefas bem definidas, incluindo componentes para redes neuronais fotónicas. Um dos obstáculos históricos deste caminho tem sido a necessidade de converter repetidamente sinais entre os domínios ótico e elétrico, o que introduz latência e consumo. Nesse contexto, trabalhos recentes em *latches* fotónicos (unidades de memória volátil no domínio ótico) são relevantes por endereçarem precisamente o problema do armazenamento temporário sem sair do domínio da luz.

O ponto importante, para uma leitura operacional, é maturidade e integração. Não existe hoje um “data center fotónico” completo, pronto a ser replicado como modelo de referência. O que existe é um conjunto de tecnologias com trajetórias diferentes de adoção: primeiro nas interligações e na rede (onde a fotónica já é familiar), e mais tarde em aceleração computacional especializada. Para equipas de infraestrutura, isto traduz-se numa pergunta concreta: que partes da arquitetura estão a ser limitadas por conectividade, densidade de I/O e energia por bit — e quais dessas partes podem beneficiar de integração ótica mais profunda sem alterar todo o *stack*. ■

## 01

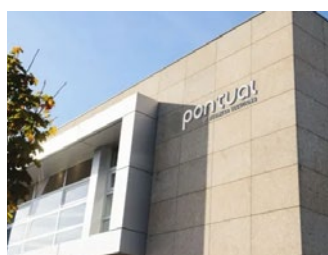
## HP LEVA VISÃO PARA O FUTURO DO TRABALHO ATÉ AO CES 2026



A HP apresentou, no CES 2026, um conjunto de novos produtos, soluções e iniciativas estratégicas centradas no futuro do trabalho, com o objetivo de responder aos desafios enfrentados por profissionais do conhecimento e organizações num contexto de mudança acelerada. A empresa defende que a tecnologia pode desempenhar um papel decisivo na melhoria da realização profissional e, consequentemente, no crescimento dos negócios. A empresa sublinha que o acesso a ferramentas adequadas e o investimento das organizações nos seus colaboradores têm impacto direto na produtividade.

## 02

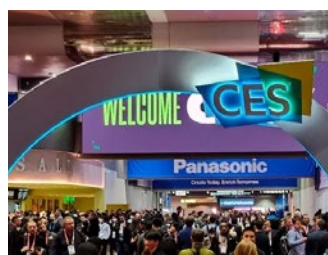
## FUNDO DE PRIVATE EQUITY ADQUIRE POSIÇÃO MAIORITÁRIA NO GRUPO PONTUAL



A Atena Equity Partners adquiriu uma participação maioritária no Grupo Pontual, reforçando a sua presença no setor dos serviços de tecnologias de informação. A operação foi realizada através do fundo Atena III e tem como objetivo apoiar a expansão do grupo em Portugal e Espanha. Com a entrada da Atena, a atual equipa de gestão mantém-se na liderança e na estrutura acionista do grupo, ficando responsável por conduzir o plano de crescimento. A estratégia passa pela combinação de crescimento orgânico com aquisições, incluindo a integração de empresas, equipas especializadas e carteiras de clientes.

## 03

## O EPICENTRO DA INOVAÇÃO TECNOLÓGICA COM A IA COMO PROTAGONISTA



A primeira semana do ano é sinónimo de Consumer Electronics Show (CES). A maior feira de tecnologia do mundo arranca esta terça-feira e decorre até ao próximo dia 9 de janeiro, em Las Vegas, nos EUA. A edição deste ano contou com mais de quatro mil expositores, sendo esperados mais de 150 mil visitantes. O evento, que agrega as principais empresas mundiais dos mais diversos segmentos, serve de palco para lançar e divulgar as mais recentes novidades tecnológicas reservadas para 2026, apesar de muitas empresas terem já antecipado pré-divulgações e lançamentos durante o mês de dezembro.

## 04

## MICROSOFT APRESENTA NOVO ACELERADOR DE IA FOCADO EM INFERÊNCIA



A Microsoft anunciou o Maia 200, o seu mais recente acelerador de IA para inferência, concebido para responder às exigências crescentes de execução eficiente de modelos avançados de IA. Produzido com tecnologia de três nanómetros, integra mais de 140 mil milhões de transístores e foi otimizado para operações de baixa precisão, essenciais nos modelos modernos. O novo acelerador suporta nativamente cálculos em FP8 e FP4, alcançando mais de 10 petaFLOPS em FP4 e mais de 5 petaFLOPS em FP8. Segundo a Microsoft, o Maia 200 oferece cerca de 30% mais desempenho por dólar face à geração mais recente de hardware.

## 05

## PROOFPOINT CONCLUI AQUISIÇÃO DA HORNETSECURITY



A Proofpoint anunciou que concluiu a aquisição do Hornetsecurity Group pelo valor de 1,8 mil milhões de dólares. O acordo impulsiona as capacidades da Proofpoint junto das PME e, em particular, dos MSP. A conclusão do negócio, revela a empresa em comunicado, representa “um marco significativo na estratégia da Proofpoint de estender a sua plataforma de segurança *human-centric* para organizações das mais variadas dimensões, através de uma abordagem construída essencialmente para o Canal de MSP”. A Hornetsecurity vai operar como uma unidade de negócios dedicada focada em atender MSP e PME a nível global. ■

fevereiro 2026 | n. 124

itchannel.pt



Diretor: Jorge Bento

Diretor Editorial: Rui Damião  
rui.damiao@medianext.pt

Coordenadora Editorial: Marta Quaresma Ferreira

Senior Contributor: Henrique Carreiro

Jornalistas: Inês Garcia Martins, Flávia Gomes

Design e Paginação: Teresa Rodrigues

Fotografia: Luciano Reis

Ilustrações e fotografias em banco de imagens:

Adobe Stock | IStockPhoto

Business Development:

Catarina de Brito

(+351) 910 121 200 | catarina.brito@medianext.pt

João Calvão

(+351) 910 788 413 | joao.calvao@medianext.pt

Marketing &amp; Events Director: Rosa Bento

rosa.bento@medianext.pt

Marketing Communications: Rita Rodrigues

(+351) 912 971 161 | rita.rodrigues@medianext.pt

Colaboraram nesta edição: Luís Filipe Freitas

**media  
NEXT**

STAY AHEAD • STAY RELEVANT

Editado por:

MediaNext Professional Information Lda.

Gerente: Pedro Botelho

Publisher: Jorge Bento

Sede e Redação: Largo da Lagoa, 7c,

2795-116, Oeiras, Portugal

Tel: (+351) 214 147 300 Fax: (+351) 214 147 301

E-mail: info@medianext.pt

Propriedades e direitos:

IT CHANNEL é marca registada de MediaNext Professional Information Lda., NIPC 510 551 866, empresa jornalística registada na ERC nº224011. Proprietários com mais de 5% do Capital Social: Margarida Bento e Pedro Lemos. Todos os direitos reservados. A reprodução do conteúdo (total ou parcial) é proibida. O editor não poderá ser responsabilizado por gralhas ou erros gráficos surgidos. As opiniões expressas em artigos assinados são da inteira responsabilidade dos seus autores. Consulte estatutos editoriais em [www.itchannel.pt/pages/estatuto-editorial](http://www.itchannel.pt/pages/estatuto-editorial)

Depósito Legal nº: 368072/13

Impressão e acabamento: Grafisol, Edições e Papelarias, Lda. - Sintra

Expedição: Porenvel, Alfragide

Distribuído por: CTT Correios de Portugal S.A.

Serviço de assinantes: assinantes@medianext.pt

Preço de assinatura: (10 números)

Portugal 50€, Estrangeiro 100€

Se é um profissional do Canal de TIC pode solicitar assinatura gratuita pelo registo no site [itchannel.pt](http://itchannel.pt)

O IT Channel utiliza as melhores práticas de privacidade sobre dados em acordo com o RGPD. Consulte: [www.itchannel.pt/pages/privacidade](http://www.itchannel.pt/pages/privacidade)

Tiragem: 2 013 exp. (média 2024) - AUDITADO  
Assinantes digitais: 6 072 exp. (média 2024) - AUDITADO

Periodicidade: mensal (10 edições ano)

Registo na ERC: O IT Channel está registado na Entidade Reguladora para a Comunicação Social com o nº 127294

Membro da ACEPI  
Associação da Economia DigitalMembro da APCT - Associação  
Portuguesa de controlo de Tiragem  
e CirculaçãoMembro da API - Associação  
Portuguesa de Imprensa

# CALENDÁRIO DE EVENTOS 2026

Os nossos leitores são a nossa comunidade e é com essa comunidade que celebramos encontros presenciais onde se vive de perto o setor mais dinâmico, mas também um dos mais exigentes, pela necessidade constante de atualização de conhecimento e competências.

Venha viver o jornalismo ao vivo, atualizar o seu conhecimento, trocar experiências e criar oportunidades de networking.

QUA  
FEV 25

**IT INSIGHT TALKS #1 – CYBERSECURITY**  
FORUM TECNOLÓGICO DE LISBOA – LISPÓLIS | PRESENCIAL + LIVE STREAM  
TÓPICOS: AMEAÇAS EMERGENTES, REGULAMENTAÇÕES E DEFESA EM CYBERSECURITY  
PÚBLICO: CISOS, CTOS, SECURITY MANAGERS

IT·Insight  
talks

TER  
ABR 14

**IT SECURITY SUMMIT PORTO**  
TIVOLI KOPKE PORTO GAIA | PRESENCIAL  
TÓPICOS: DATA PROTECTION, AMEAÇAS EMERGENTES, REGULAMENTAÇÃO  
PÚBLICO: CISOS, CTOS, SECURITY MANAGERS



QUI  
MAI 28

**CHANNEL ON**  
LISBOA – MONTES CLAROS SECRET SPOT | PRESENCIAL + LIVE STREAM  
TÓPICOS: ESTRATÉGIAS DE CANAL, OPORTUNIDADES  
PÚBLICO: CHANNEL PARTNERS, INTEGRADORES

channel on  
channel conference

QUI  
JUN 18

**IT INSIGHT TALKS #2 – AI & DATA**  
FORUM TECNOLÓGICO DE LISBOA – LISPÓLIS | PRESENCIAL + LIVE STREAM  
TÓPICOS: AI, ANÁLISE DE DADOS  
PÚBLICO: CIOS, DATA MANAGERS

IT·Insight  
talks

QUI  
OUT 08

**IT SECURITY CONFERENCE**  
LISBOA – O CLUB + ESTUFA DE MONSANTO | DOIS PALCOS + LIVE STREAM  
TÓPICOS: ESTRATÉGIAS DE DEFESA, AI IN CYBERSECURITY  
PÚBLICO: CISOS, CIOS, CTOS, DPOS



QUA  
OUT 28

**IT INSIGHT TALKS #3 – BUSINESS CONTINUITY**  
FORUM TECNOLÓGICO DE LISBOA – LISPÓLIS | PRESENCIAL + LIVE STREAM  
TÓPICOS: CONTINUIDADE DE NEGÓCIO, RESILIÊNCIA  
PÚBLICO: CIOS, RISK MANAGERS

IT·Insight  
talks

QUI  
NOV 26

**IT INSIGHT TALKS #4 – HYBRID CLOUD & MULTICLOUD**  
FORUM TECNOLÓGICO DE LISBOA – LISPÓLIS | PRESENCIAL + LIVE STREAM  
TÓPICOS: ESTRATÉGIAS HYBRID E MULTICLOUD  
PÚBLICO: CLOUD ARCHITECTS, IT DIRECTORS

IT·Insight  
talks

Lenovo™

ThinkPad

# ThinkPad X9-14 Glacier White

O poder de um top performance num design que quebra convenções  
A inédita cor **Glacier White** eleva o estilo ThinkPad a um novo patamar

## Design inovador

Inovação cromática que marca tendência

## Desempenho sem compromissos

Intel® Core™ Ultra, LPDDR5x e SSD PCIe Gen4.

## Visual impressionante

Ecrã OLED. Alta definição e ampla gama de cores.

## Conectividade e segurança

Com Wi-Fi 7, Thunderbolt 4 e tecnologias de segurança como reconhecimento facial

## Autonomia e eficiência

Bateria com autonomia duradoura e estrutura ultraleve

## Design responsável

Chassis construído com materiais reciclados e embalagens sustentáveis



 **esprinet**®  
enabling your tech experience

Distribuidor oficial Lenovo em Portugal

Compre já!

