

Mário Campolargo “Líderes têm o desafio de introduzir a IA de forma ética e responsável nas empresas”

A utilização das infraestruturas digitais por cidadãos e empresas precisa de aumentar no sentido de transformar a abordagem das empresas aos negócios, defende o antigo secretário de Estado da Digitalização e da Modernização Administrativa ■ P.3-9



19.09.2025

Diretor
André Macedo
Subdiretores
Lígia Simões
e Ricardo
Santos Ferreira

Special Report Cibersegurança

Caderno publicado como suplemento do Jornal Económico nº 2318. Não pode ser vendido separadamente.

Segurança digital também é uma questão cultural

■ Há consciência da necessidade de investir em cibersegurança e preocupação com os efeitos do desenvolvimento tecnológico, mas falta preparação e trabalho conjunto. Ideias a retirar da conferência promovida pelo JE. ■ P. 16-18



CRISTINA BERNARDO

Número e sofisticação das ameaças crescem e obrigam empresas a esforço de atualização

Mais incidentes e mais sofisticados, promovidos por atores com maior capacidade, marcaram o último ano no ciberespaço português. O desafio das empresas é conseguirem atualizar-se à mesma velocidade, para se defenderem. Não é fácil. ■ P.4-5

Jorge Silva Carvalho: Ambição regulatória ou miragem? ■ Ensaio P.2

Manual de preparação para a tempestade regulatória ■ P.14

“Desinformação é o maior cancro na internet” ■ António Gameiro Marques



Ensaio

■ **Jorge Silva Carvalho** consultor em Segurança e Estratégia



Ambição regulatória ou miragem de resiliência digital?

A transformação digital deixou de ser uma escolha para se tornar numa inevitabilidade. Bancos, seguradoras e gestoras de ativos são hoje inseparáveis das tecnologias de informação e comunicação.

É nesse contexto que surge o *Digital Operational Resilience Act* (Lei de Resiliência Operacional Digital, DORA no acrónimo em inglês), um novo regulamento europeu que procura reforçar a resiliência operacional digital do setor financeiro.

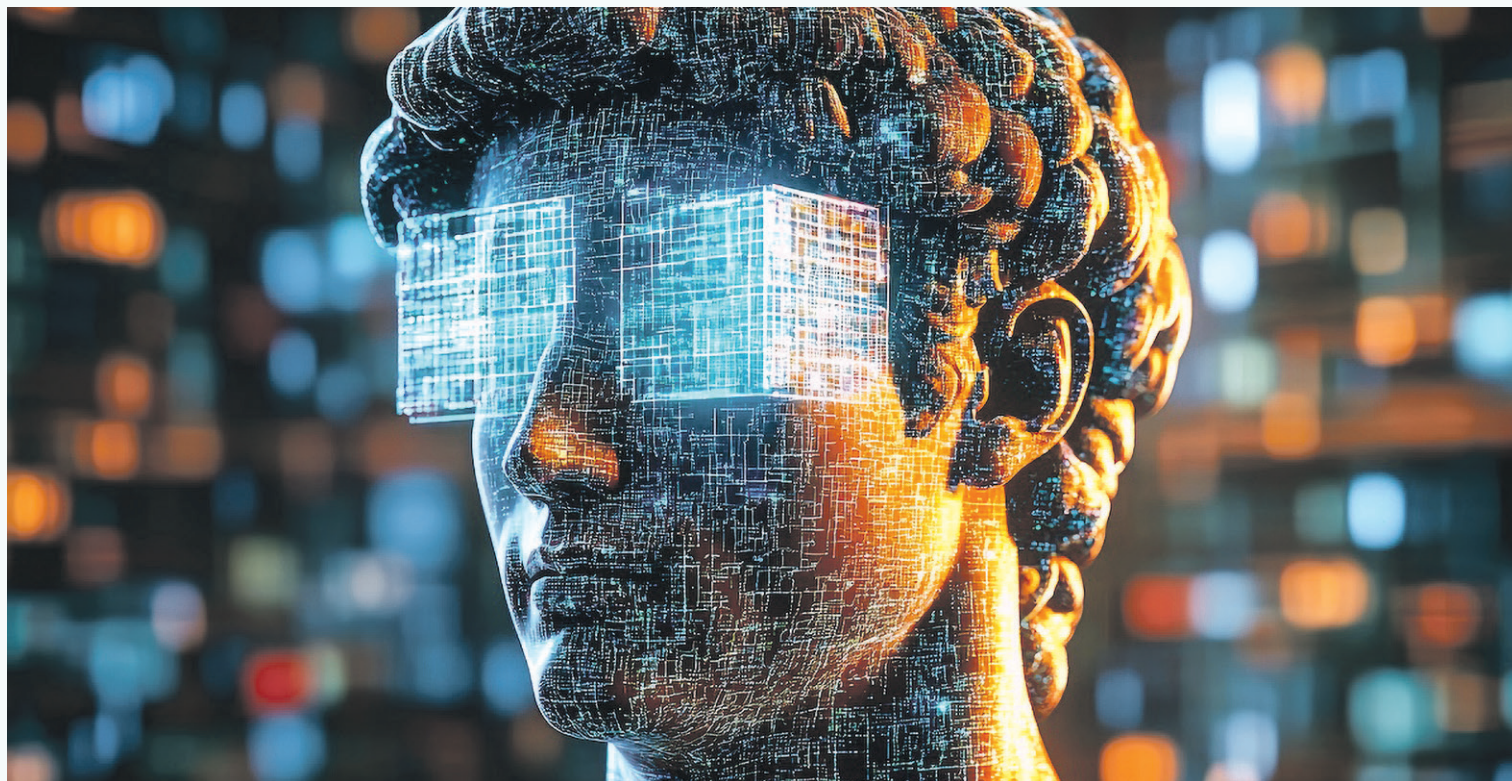
A ideia é simples: garantir que todas as instituições financeiras, bem como prestadores de serviços tecnológicos críticos, adotem padrões elevados de cibersegurança e estejam preparadas para resistir a crises digitais.

Mas, olhando de perto, percebe-se que a ambição do DORA esbarra num problema central: exige “resiliência”, mas sem definir com clareza quais medidas concretas devem ser implementadas.

Este vazio deixa demasiado espaço para interpretações diferentes entre instituições e Estados Membros. Em vez de aproximar a Europa em torno de um quadro comum, a norma pode acentuar desigualdades e criar várias Europas digitais a diferentes velocidades, moldadas pela capacidade financeira, maturidade tecnológica e ambiente político de cada país.

Há ainda o risco de este projeto se revelar mais político do que técnico.

Enquanto potências como Estados Unidos, China ou Israel seguem estratégias digitais claras e operacionais, a União Europeia pode ficar presa a normas abstratas, agradáveis no papel, mas com pouco efeito prático.



O DORA estabelece objetivos, mas carece de um manual de instruções: faltam-lhe orientações técnicas, testes definidos e mecanismos de auditoria que transformem intenções em prática.

Outro aspeto merece reflexão: será o setor financeiro o único que justifica esta prioridade? O impacto devastador de falhas em áreas como energia, saúde, comunicações ou infraestruturas do Estado mostra que a vulnerabilidade não se limita às finanças.

Talvez faça mais sentido uma visão transversal, integrando quadros como a NIS2 e normas técnicas já consolidadas, em vez de multiplicar regulamentos setoriais fragmentados.

As dificuldades práticas já se fazem sentir. O DORA apresenta um quadro complexo e exigente que obriga as instituições a recorrer a consultores e análises de conformidade sem oferecer um ‘roadmap’ realista.

Sem medidas técnicas sólidas, recursos dedicados e auditorias rigorosas, o DORA corre o risco de se tornar apenas mais uma norma de prateleira — elegante no papel, mas irrelevante na realidade

Implica monitorização contínua de riscos, testes regulares, revisões contratuais e novas obrigações de governação.

Mas mais do que sistemas, o grande desafio será cultural: mudar mentalidades, investir em conhecimento e criar uma verdadeira consciência organizacional de ciberresiliência.

Acresce a difícil questão da partilha de informação entre entidades e reguladores.

O regulamento incentiva essa cooperação, mas construir redes de confiança genuínas continua a ser um desafio pouco resolvido.

Sem confiança, a rede falha; e sem essa rede, não há resiliência coletiva.

O DORA é, ainda assim, uma oportunidade.

Obriga as instituições financeiras a olhar para os riscos digitais de forma mais estratégica. Mas não basta decretar resiliência: é preciso

transformar os enunciados políticos em processos claros, investimentos concretos e práticas efetivas.

Uma Europa digitalmente segura exige mais do que regulamentação — exige ação.

Se queremos que o continente se afirme como bloco competitivo e estável no mundo digital, não podemos continuar a confundir declarações de intenção com garantias de cibersegurança.

Sem medidas técnicas sólidas, recursos dedicados e auditorias rigorosas, o DORA corre o risco de se tornar apenas mais uma norma de prateleira — elegante no papel, mas irrelevante na realidade.

A ambição europeia é justa e necessária. Mas, se não for acompanhada da capacidade para transformar teoria em prática, o grande perigo será este: trocar a verdadeira resiliência por uma ilusão regulatória.



O seu negócio pode

**ter uma equipa que
nunca se deixa enganar**

Vodafone Security Awareness

Identifique comportamentos de risco e disponibilize formação online em tempo real aos seus colaboradores, para reforçar a cultura de cibersegurança na sua empresa.

Com Vodafone Security Awareness, o seu negócio pode tudo.

vodafone.pt/business



Together we can
vodafone
business

O risco de ficar para trás na guerra da cibersegurança

Ameaças ■ Mais incidentes e mais sofisticados, promovidos por atores com maior capacidade, marcaram o último ano no ciberespaço português. O desafio das organizações é conseguirem atualizar-se à mesma velocidade, para se defenderem. Não é fácil.

Ricardo Santos Ferreira
rsferreira@medianove.com

O número de incidentes de segurança aumentou fortemente no ano passado e a expectativa é de que a tendência se mantenha este ano. É natural que assim seja, porque somos uma sociedade cada vez mais digitalizada, interconectada. Depois, o quadro crispado geopolítico em que vivemos também incentiva a que isso aconteça. O mundo digital é um território disputado e o risco é ficarmos para trás na guerra da segurança, ultrapassados por quem funciona na ilegalidade.

O Relatório Riscos e Conflitos 2025, publicado pelo Centro Nacional de Cibersegurança (CNCS) esta semana, mostra que foram registados 11.163 incidentes de cibersegurança pelo CERT.PT no ano passado, um número que multiplica por mais de cinco o de 2023. Reflete, sobretudo, a melhoria das ferramentas de deteção automática utilizadas, sobretudo na deteção da classe código malicioso. No entanto, mesmo se deixarmos de lado este sistema e contabilizarmos, apenas, os incidentes registados com base em notificações, internas ou externas, como aconteceu nos anos anteriores, enfrentamos um aumento de 36%, para 2.758 incidentes notificados.

Estes dados traduzem uma inversão face à relativa estabilização registada em 2023, com um forte aumento dos incidentes e numa intensificação das ameaças. Depois de um ano mar-

cado por ocorrências sobretudo locais, “a tendência dos incidentes com impacto nacional ressurgiu em 2024”, com episódios de indisponibilidade generalizada e falhas críticas de sistemas a atingirem operadores essenciais e entidades públicas, aponta o CNCS.

É um regresso à tendência de crescimento anual acelerado observada desde 2016, após a quase estagnação de 2023, com um aumento limitado de 0,1%. Quando comparado com 2019, em que se contabilizavam pouco mais de 750 incidentes, o crescimento é de quase quatro vezes.

“É preciso reconhecer o facto de que a cibersegurança é, atualmente, um tema de preocupa-

ção para todas as empresas, mas simultaneamente verifica-se que existe ainda um desconhecimento significativo sobre o que podem ser, concretamente, as vulnerabilidades dos sistemas informáticos usados no dia-a-dia pelas empresas e seus colaboradores”, diz o presidente da Associação Empresarial de Portugal, Luís Miguel Ribeiro, ao Jornal Económico (JE).

“A opinião que recolhemos junto dos nossos associados é semelhante ao das empresas em geral, que é a de que, por mais que façamos em prol da sua segurança, o risco nunca é nulo, pelo que, paradoxalmente, as empresas acabam por estar, cada vez mais, expostas aos riscos de cibersegurança, que estão no ranking dos principais riscos a nível global”, acrescenta.

O relatório do CNCS revela que as tipologias de ataque também se transformaram. O phishing (tentativa de obter ilegalmente informações) e smishing (tentativa de fraude, mas através de mensagens por telemóvel) mantiveram-se como incidentes mais frequentes, com a incidência a crescer 13%. A engenharia social, em particular fraudes como “CEO Fraud” ou esquemas de recrutamento falso, registou um aumento de 567 incidentes, para 772, tornando-se a segunda categoria mais reportada, representando 27,97% do total.

A distribuição de malware (código malicioso) duplicou, para 248 ocorrências, enquanto o comprometimento de contas não privilegiadas subiram 37%. Já os ataques de ransomware, embora em



Luís Miguel Ribeiro
Presidente
da Associação Empresarial
de Portugal



Jorge Libório
partner e Cybersecurity
Leader da EY



queda de 35% para 35 incidentes, mantiveram “um impacto substancial e muito amplo”.

A nível setorial, verificou-se um aumento expressivo no setor da energia (+140%) e na administração local (+26%) e regional (+74%). Em termos de vulnerabilidades exploradas, o CERT.PT associou 45 incidentes a falhas conhecidas, algumas datadas de 2019, revelando fragilidades persistentes na mitigação.

O relatório evidencia igualmente a crescente sofisticação dos agentes de ameaça. Os cibercriminosos continuam a ser os mais ativos. Os atores estatais intensificaram atividades de ciberespionagem, visando informação estratégica de Portugal e dos seus parceiros internacionais. Já os grupos hacktivistas (invasão de sistemas pela promoção de uma causa), maioritariamente pró-russos, recorreram a ataques DDoS (negação de serviço por sobrecarga) e técnicas de hack and leak (roubo de dados para divulgação pública), ampliando

os efeitos através de redes sociais e fóruns digitais. Como alerta o relatório, “observou-se uma crescente predisposição para o uso de técnicas combinadas de disrupção”, aponta o CNCS.

A Agência da União Europeia para a Cibersegurança (ENISA, no acrónimo em inglês) refere ao JE que, no seu relatório anual, entre as principais tendências identificadas em relação aos atores de ameaças, “foi notável a crescente semelhança entre atores

“O desafio está em equilibrar este jogo de gato e do rato, entre a velocidade da evolução dos ataques e o investimento das empresas em capacidades equivalentes de defesa”, afirma Jorge Libório



JOHN NAZCA/REUTERS

com ligações entre Estados e supostas atividades hacktivistas”.

Investimento e impreparação

O retrato de 2024 é, assim, o de um ciberespaço português sob pressão crescente, com números que se aproximam da realidade europeia e global. Como conclui o relatório, “92% dos profissionais de cibersegurança consideram que o risco de uma entidade sofrer um incidente aumentou em 2024, e 90% perspetivam que se agrave em 2025”.

O problema é saber se as organizações, as empresas, estão preparadas para o aumento e para a crescente sofisticação das ameaças. Está tudo a acontecer muito rapidamente e é difícil acompanhar.

“Já existe uma maior preocupação por parte das instituições no que diz respeito aos riscos a que estão expostos, não por exemplos recentes de incidentes de segurança, mas também da própria regulamentação que tem introduzido coimas elevadas”, diz

Jorge Libório, partner e Cybersecurity Leader da EY. “Esta maior preocupação tem-se traduzido num aumento dos investimentos em medidas de cibersegurança, o que consequentemente tem aumentado a preparação destas instituições, principalmente nas grandes empresas e organizações”, acrescenta.

Um relatório da IDC revela que o investimento em cibersegurança cresceu 35% em 2024 e estima que em 2025 crescerá em mais cerca de 40%.

No entanto, nem todos têm a mesma capacidade e as organizações mais pequenas ressentem-se. “Nem sempre é fácil às organizações adotar medidas de resposta à mesma velocidade da evolução das ameaças. Quando falamos em PME, por exemplo, estas continuam com recursos limitados, tanto financeiros como técnicos, e, de uma forma mais lata, existe falta de mão de obra qualificada para trabalhar nas áreas da cibersegurança”, aponta Jorge Libório.

A reter do relatório do CNCS

A administração pública local (32%), a administração pública central e institutos públicos (27%) e o ensino superior (27%) foram as áreas governativas que mais notificações geraram.



O setor bancário passou do terceiro com mais incidentes registados, em 2023, para a nona posição. Número de incidentes caiu 69%.



Mas as marcas da banca foram as mais simuladas em ataques de phishing/smishing. Observou-se um aumento de 33%.

A engenharia social foi a tipologia que registou o maior aumento no número de incidentes passando a ser a segunda mais frequentemente observada.



O número de notificações de violação de dados pessoais caiu 19%, o que representa uma quebra da tendência observada desde 2019.



A confidencialidade foi comprometida em 70% das notificações da CNPD, tendo sido o princípio da segurança da informação mais visa do, enquanto as origens mais frequentes de notificação foram a falha humana (30% do total), a exploração de vulnerabilidades (15%) e o phishing ou engenharia social (15%) (CNPD).



A burla informática foi o crime mais registado em 2024, em particular as relacionadas com plataformas de pagamentos online, representando 29% do total.



As denúncias com o fenómeno conhecido por “Olá, Pai...Olá, Mãe” triplicou.

A burla online foi a tipologia mais frequentemente observada nas denúncias ao Gabinete Cibercrime da PGR, nomeadamente as de compra e venda online, falsos processos de recrutamento ou burlas relacionadas com falsas cobranças de dívidas de eletricidade.



E agora a inteligência artificial

■ A tecnologia emergente mais frequentemente considerada desafiante, no ano passado, foi a inteligência artificial (IA), com 78% das respostas dadas no inquérito feito pelo CNCS, e o valor subiu 16 pontos percentuais, para 94%, quando se perguntou sobre a perspetiva para este ano. Reflete a realidade objetiva, em que as soluções de IA estão rapidamente a ser adotadas.

“Nos últimos anos, tem-se observado que a utilização extensiva da IA pode abrir novos caminhos para métodos de manipulação e ataque, além de criar novos desafios para a segurança e a privacidade. É utilizada tanto para promover atividades ofensivas como é alvo para exploração”, referem ao Jornal Económico os responsáveis da Agência da União Europeia para a Cibersegurança (ENISA, no acrónimo em inglês).

“A ampla disponibilidade e utilização de sistemas de IA permitiram a escalabilidade e a proficiência em atividades maliciosas por parte dos atacantes. Embora o foco das atividades de ameaça que envolvem a IA tenha sido a utilização de ferramentas de IA de nível de consumidor para melhorar as suas operações existentes, em vez de alcançar capacidades avançadas, os sistemas de IA maliciosos emergentes têm levantado preocupações”, explicam.

Jorge Libório, partner da EY, concorda. “[A IA] facilita a rápida evolução e sofisticação de ataques tornando-os mais difíceis de detetar”. Permite a personalização das ameaças. Mas, ao contrário, também traz benefícios na defesa e proteção. “Conseguem analisar maiores volumes de dados e identificar padrões anómalos, facilitando a resposta a incidentes. Automação de testes e gestão de vulnerabilidades contribuem para a redução de tempos de reação à adversidade”, aponta.

O que devem fazer as empresas? Investir em conhecimento

Risco ■ As ameaças cibernéticas vão continuar a aumentar e as empresas têm de se adaptar. Parcerias, identificação de ativos críticos são caminhos obrigatórios, mas, primeiro, têm de investir na literacia.

Ricardo Santos Ferreira
rsferreira@medianove.com

O principal investimento que as empresas têm de fazer para responder ao aumento significativo do risco cibernético é na literacia, para criarem uma cultura de segurança que ajude a minimizar oportunidades para incidentes. O conhecimento é a base em que assentam as soluções tecnológicas.

“A literacia é fundamental, pois o reconhecimento de que a cibersegurança é uma questão da maior importância para a atividade das empresas, e para a continuidade do negócio, terá de ser o primeiro passo para se consciencializarem das suas fragilidades e da necessidade de aumentar os níveis de cibersegurança”, diz ao Jornal Económico (JE) o presidente da Associação Empresarial de Portugal, Luís Miguel Ribeiro.

Isto é verdade para todo o tipo de empresas, independentemente do tamanho, maturidade, e disponibilidade para o risco, mas para as pequenas e médias empresas (PME) é essencial.

“A AEP tem vindo a aumentar a oferta de ações de formação nestas áreas para as empresas, ações essas que têm tido uma procura crescente por parte do tecido empresarial”, diz Luís Miguel Ribeiro. “Mesmo assim, temos a perceção de que ainda há muitas empresas que, apesar de considerarem a cibersegurança como uma preocupação, não estão cientes sobre o que devem fazer para se posicionarem de forma mais segura nas questões digitais”, acrescenta.

“Investir na formação das pessoas para antecipar ou evitar comportamentos de risco, planos de continuidade de negócio atualizados, backups regulares,



Investir na formação das pessoas para antecipar ou evitar comportamentos de risco é uma prioridade

autenticação forte, são bons pontos para começar” a dar resposta ao aumento do risco, aponta Jorge Libório, partner e Cybersecurity Leader da EY.

A necessidade de conhecimento não se esgota, no entanto, na sensibilização para o risco cibernético e na formação, tanto dos colaboradores como da gestão de topo. “As empresas deverão começar por mapear claramente os seus ativos críticos e inventariá-los. Dependendo da sua criticidade e prioridade, deverão ser adotadas medidas e controlos proporcionais ao risco identificado”, diz Jorge Libório.

Temas como a gestão da continuidade de negócio, implementação de princípios *zero trust*, o que significa nunca confiar em dados históricos ou contextos passados e verificar sempre a necessidade de novos acessos, a formação, assim como seguir boas práticas de cibersegurança, como a utilização de autenticação multifator e cor-

reção de vulnerabilidades, deverão ser prioridades.

Libório aponta que quadros como a ISO 27001 (norma internacional de referência para um sistema de gestão de segurança da informação), o NIST CSF (guia para gestão de cibersegurança para a indústria, entidades públicas e outras organizações), ou até mesmo o Quadro Nacional de Referência de Cibersegurança poderão ser utilizados como base para a identificação, não só dos requisitos, mas também dos controlos a implementar.

Processo em curso

O processo de adaptação tem de ser contínuo, não termina. “Precisamos de adaptar continuamente a nossa postura, ferramentas e estratégias”, referem ao JE os responsáveis da Agência da União Europeia para a Cibersegurança (ENISA, no acrónimo em inglês). E aqui entram as parcerias, o unir forças. Não

se trata unicamente da colaboração entre os Estados-membros da UE, as instituições europeias e os setores público e privado, que a ENISA identifica como “vital para enfrentar as ameaças emergentes no mundo interligado de hoje”, mas também na capacidade das empresas recorrerem ao mercado para colmatar limitações.

“Para atividades de monitorização e mesmo compliance, regimes de outsourcing, num modelo as a service, podem ser uma forma mais efetiva e eficiente de endereçar o risco”, refere Libório.

Rui Guedes Henriques, partner de Managed Services da EY reforça esta mesma ideia: “Num contexto em que as ameaças cibernéticas evoluem a um ritmo acelerado, é essencial que as empresas adotem proativamente uma postura preventiva e colaborativa”, diz. Ou seja, preparar para os desafios da cibersegurança não passa apenas por inves-

Tendências para as ameaças cibernéticas

O Centro Nacional de Cibersegurança identificou seis grandes tendências na evolução das ameaças cibernéticas relevantes para o ciberespaço de interesse nacional num futuro próximo:

■ **Aumento de ataques** contra infraestruturas *cloud* e fornecedores.

■ **Exploração de vulnerabilidades** fruto do aumento da superfície de ataque.

■ **Infostealers** e comércio de credenciais online.

■ Potenciar do cibercrime por via de um **maior uso de criptomoedas**.

■ Utilização de **IA generativa para ciberataques**.

■ Alterações nas políticas das plataformas digitais poderão potenciar a **desinformação**.

tir em tecnologia, mas também por adotar modelos operacionais que promovam a partilha de recursos técnicos, como infraestrutura, soluções de monitorização e resposta a incidentes, competências especializadas e intelligence como indicadores de ameaça e boas práticas.

“Neste contexto, o Cyber Managed Services assumem um papel estratégico na forma como as empresas enfrentam os riscos cibernéticos. Ao recorrer a parceiros com experiência comprovada, é possível garantir uma proteção robusta, escalável e adaptada à complexidade do ambiente digital atual”, afirma. “Esta abordagem permite às organizações focarem-se no seu negócio core, enquanto beneficiam de uma vigilância permanente, evitam investimentos excessivos, obtêm uma redução de custos operacionais, uma maior agilidade na gestão de incidentes e uma resposta mais eficaz e contínua às exigências da segurança digital”, acrescenta.



If It's Connected, It's Protected.

A Cisco é líder mundial em tecnologia
que liga e protege organizações
na era da Inteligência Artificial.



Entrevista ■ Mário Campolargo, antigo secretário de Estado da Digitalização e da Modernização Administrativa e atual professor na Universidade de Aveiro, fala da evolução das políticas digitais europeias, da posição da Europa na corrida tecnológica e do desafio da inclusão digital no Estado e nas empresas.

“Líderes têm o desafio de introduzir a IA de forma ética e responsável nas empresas”

António Sarmiento
asarmento@medianove.com

A utilização das infraestruturas digitais pelos cidadão e empresas precisa de aumentar no sentido de transformar a abordagem das empresas aos negócios. Nesse sentido, as organizações e a administração pública devem formar os quadros para tirar o máximo partido, garantindo benefícios económicos e sociais na utilização de tecnologias disruptivas. Entrevista a Mário Campolargo, numa altura em que a União Europeia está a trabalhar em vários domínios de intervenção para promover um futuro digital para a Europa.

De que maneira o contexto geopolítico recente tem influenciado a evolução das políticas digitais europeias?
Nos anos de 2024 e 2025 assistimos a uma evolução na elaboração das políticas digitais e nas prioridades da União Europeia. Esta mudança não representa seguramente uma negação da anterior agenda mas, pelo contrário, o seu amadurecimento

claramente impulsionada por este ambiente de tensões geopolíticas crescentes, incluindo a guerra na Ucrânia e pela intensa concorrência global menos alinhada como uma ordem internacional estável à qual estamos habituados. Assim, a abordagem europeia evolui para se focar mais em garantir soberania tecnológica, segurança e competitividade dando de alguma maneira prioridade à construção de uma base industrial soberana (alinhado com relatórios Draghi e Letta) em que o desafio não pode ser já estabelecer como o mercado digital deve operar, mas sim garantir que a UE possua as competências, a capacidade de inovação, a capacidade tecnológica, industrial e de segurança para construir um mercado interno que seja robusto, claro e aberto ao exterior. Um exemplo disso são os investimentos em IA *factory* e *Gigafactories* que dão corpo a uma dimensão tecnológica industrial que está muito alinhada e complementa o regulamento da IA.

Como é que a União Europeia

encara a regulação de tecnologias disruptivas em comparação com outros modelos globais, como os EUA e a China?

No contexto das tecnologias disruptivas, a regulação é frequentemente vista como obstáculo à inovação ou como um escudo necessário para defender os valores fundamentais da sociedade. Julgo que na UE o nosso compromisso com a regulamentação, à qual podemos chamar proativa, não pode ser visto como uma barreira à inovação mas sim como uma base para a confiança da sociedade e dos cidadãos relativamente às tecnologias disruptivas e aos possíveis impactos sociais negativos ou mesmo distópicos, dirão alguns. Na verdade, penso que o desafio reside em encontrar um equilíbrio não necessariamente entre regulação e inovação, mas entre aquilo que chamaria uma fé cega no mercado ou no Estado e o progresso social responsável. É por isso que a abordagem da UE contrasta com os modelos amplamente auto-regulados que se observa nos EUA, que são guia-



Temos que garantir a formação dos quadros das empresas na área da cibersegurança e alertar nos níveis mais precoces de educação para as boas práticas dentro do mundo digital

dos pelo lucro e que reforçam plataformas dominantes a nível global e também com a abordagem mais centralizada e impulsionada pelo Estado, na China, que pode sacrificar em muitos casos os direitos dos próprios cidadãos.

Que medidas permitem que a Inteligência Artificial promova uma economia inclusiva e sustentável?

Garantindo que a IA europeia não é apenas inteligente, mas também é justa. Ou seja, regulada com base em direitos, orientada para oportunidades sociais, comprometida com a sustentabilidade e que de alguma maneira garanta a primazia da



governança democrática das nossas sociedades. Daqui resultam três aspetos: apostar num quadro regulatório orientado por valores, garantido por exemplo que os sistemas de IA respeitam os direitos humanos, que não criem discriminações algorítmicas, que são auditáveis, transparentes e explicáveis e que adotemos sempre um princípio de responsabilidade e de supervisão humana principalmente quando há riscos para a sociedade. Também é preciso apostar na inclusão social (apoio a pessoas idosas, com deficiência) ou a populações marginalizadas e laboral (garantindo a formação e a requalificação digital dos trabalhadores) para podermos

assegurar que quando há risco de automação eles encontram novas oportunidades profissionais. Sobre os aspetos de sustentabilidade, é verdade que o estágio de desenvolvimento atual da IA necessita de recursos energéticos muito significativos e é por isso que temos de apostar em novos paradigmas tecnológicos. E, ao mesmo tempo, utilizar a IA para otimizar consumo energético, prever fenómenos climáticos extremos, fazer a gestão de uma rede de transporte mais verde e até de uma agricultura mais sustentável.

De acordo com a sua experiência como governante, como é que olha para a

sociedade portuguesa no desenvolvimento da digitalização?

Portugal é considerado um país líder em digitalização nos serviços públicos e sempre entendi que o nosso telemóvel é como uma loja de cidadão no bolso. Devia conter uma *app* que nos permitisse identificar e autenticarmo-nos com muita segurança para podermos dialogar com a administração, cumprir com as nossas obrigações, permitindo-nos ter a nossa carteira digital com os documentos oficiais (cartão do cidadão, carta de condução, documentos automóveis, etc) e ter o nosso registo digital sempre à mão e também assinar digitalmente docu-

mentos e contratos. Como em todos os países, temos de investir mais na literacia digital dos cidadãos e das empresas, e simplificar processos quer no contexto da iniciativa privada ou pública. O digital é uma oportunidade para criar serviços mais simples e intuitivos.

Como é que os governos e as empresas podem usar a IA e outras tecnologias digitais para melhorar processos, decisões e serviços aos cidadãos?

A utilização das infraestruturas digitais pelos cidadão e empresas precisa de aumentar no sentido de transformar a abordagem das empresas aos negócios cujos modelos são muito afetados pela lógica digital. Ou seja, além de ter acesso a boa conectividade, adoção de *cloud* ou IA, as preocupações ao nível da cibersegurança devem estar no horizonte das nossas empresas e assim complementamos boa infraestrutura com um conjunto de tecnologias que nos permitem radicalmente mudar os nossos negócios, modelos de produção, ser mais eficazes e exportar mais. A adoção da IA é por vezes invisível ao cidadão porque trabalha no *backoffice*. Ela otimiza, automatiza processos e é uma ajuda importante à tomada de decisão. E o governo de que fiz parte investiu em muitas áreas do *backoffice* como a Justiça, a Segurança Social ou as Finanças. Mas com a introdução de uma assistente virtual baseada em IA quisemos dar um sinal de modernidade a todos os cidadãos e da utilização de tecnologias disruptivas mas com propósito. De facto, utilizamo-la para ajudar na adoção da chave móvel digital, que precisa de ser mais adoptada porque é o paradigma da identidade digital de cada um de nós. Os líderes têm um grande desafio, que é introduzir a IA de forma ética e responsável nas suas empresas e administração pública, e formar os quadros para tirar o máximo partido, garantindo benefícios económicos e sociais.

Falando em segurança, no digital é muito importante chamar também a atenção para a cibersegurança e privacidade dos dados...

Temos de considerar múltiplos vetores. Ter uma estratégia nacional como Portugal tem, que con-

solida o papel de entidades como o centro nacional de cibersegurança, reforçar as organizações com os chamados centros de operações de segurança, ter equipas de resposta rápida e, acima de tudo, protocolos claros e *report* entre entidades a nível nacional. Um terceiro fator será fazer investimentos em atualização tecnológica, garantindo a gestão de acesso à informação e aos dados através de uma autenticação forte. Não posso deixar de dizer também o investimento na capacitação humana e garantir que há uma cultura em que os incidentes sejam reportados dentro da organização e do contexto nacional. Para isso, é muito importante uma cooperação público-privada e setorial. Ou seja, não basta só tecnologia. É preciso termos uma estratégia nacional e, dentro das empresas, uma cultura de cibersegurança e formação contínuas. Quanto maior é o investimento no digital mais importante é termos consciência de que a cibersegurança não pode ser percecionada como uma despesa adicional. Ela é verdadeiramente um fator distintivo, um investimento para dar confiança ao utilizador. É um fator de sucesso na sociedade em que vivemos.

Até que ponto a falta de talento em cibersegurança é hoje um risco para a competitividade das empresas portuguesas?

O talento é fundamental em qualquer área do digital. O ambiente geopolítico em que vivemos põe um foco muito importante nos aspetos de cibersegurança e, por isso, temos de investir ao nível das universidades em cursos de formação avançada. Mas isso não é suficiente. Temos que garantir a formação dos quadros das empresas na área da cibersegurança, alertar nos níveis mais precoces de educação para a importância da privacidade e boas práticas dentro do mundo digital. É também importante que os cidadãos tenham consciência dos aspetos importantes no domínio da ciber. Os ataques ocorrem muitas vezes pelo lado mais fraco, que é muitas vezes o elo humano. Sabemos quais são os tipos de ataque a que podemos estar sujeitos. Ler antes de clicar é absolutamente fundamental para prevenir a progressão de ataques aos cidadãos.

VisionWare: há 20 anos a marcar o futuro da Cibersegurança

Decorreu no passado dia 11 de setembro, no espaço SUD Terrazza, em Lisboa, o evento que assinalou o 20º aniversário da VisionWare, empresa 100% portuguesa especializada em cibersegurança e segurança da informação, e que contou com vários profissionais do setor e especialistas nacionais e internacionais para refletir sobre os principais desafios e oportunidades da cibersegurança na atualidade, e no futuro.

Ao longo de duas décadas, a VisionWare foi-se afirmando como uma referência incontornável no setor da cibersegurança em Portugal e além-fronteiras, acompanhando a transformação tecnológica e a rápida digitalização da sociedade. Este aniversário foi, por isso, mais do que um simples marco simbólico: representou uma oportunidade para olhar para trás, valorizar o caminho feito e, sobretudo, projetar o futuro num cenário global cada vez mais complexo.

O evento contou com a presença de várias personalidades, entre as quais se destacou Paulo Portas. Na sua intervenção, o antigo vice-primeiro-ministro defendeu que a NATO deve criar um “quarto ramo das Forças Armadas”, dedicado em exclusivo ao domínio digital e à ciberdefesa. Segundo Portas, este passo seria fundamental para enfrentar ameaças que já não são apenas hipotéticas, mas sim uma realidade diária que afeta diretamente Estados, empresas e cidadãos comuns.

Subordinada ao tema “Ameaças híbridas, Ciberespaço e o papel da Europa na nova era da Ciberdefesa”, a sua intervenção deixou claro que a ciberguerra é hoje tão ou mais relevante do que a guerra convencional. A diferença, como frisou, reside no facto de, ao contrário dos conflitos clássicos, em que o inimigo é imediatamente identificável, no ciberespaço



“A tecnologia não pode ser cúmplice da erosão democrática. Tem de servir a verdade, a participação e uma sociedade mais justa, informada e livre.”
António Gameiro Marques



podem passar meses até que se descubra a verdadeira origem de um ataque, bem como as suas motivações. Além disso, enquanto uma guerra tradicional tem sempre um perímetro de operações, delimitado no espaço físico, no ciberespaço tudo está em aberto, sem fronteiras claras, tornando-se particularmente difícil estabelecer linhas de defesa.

Paulo Portas alertou ainda para a vulnerabilidade das democracias, mais expostas à desinformação e a ataques híbridos, muitas vezes invisíveis a olho nu mas profundamente destabilizadores. Recordou que regimes autocrá-

ticos tendem a deter uma vantagem competitiva no controlo da informação e na utilização intensiva de tecnologias emergentes, como a inteligência artificial. Outro dos pontos sublinhados foi a velocidade da inovação digital, que ultrapassa largamente a capacidade de resposta dos reguladores. Para o ex-governante, apenas com investimento robusto em cibersegurança, maior cooperação entre setor público e privado e um reforço da capacidade de resposta das instituições internacionais será possível proteger valores fundamentais como a democracia, a liberdade e a eco-



“A NATO deve criar um quarto ramo das Forças Armadas, dedicado em exclusivo ao domínio digital e à ciberdefesa.”
Paulo Portas



nomia num cenário de ameaças globais cada vez mais sofisticadas.

Após este primeiro momento, a reflexão centrou-se nas perspetivas de especialistas europeus em cibersegurança. António Gameiro Marques, antigo diretor-geral do Gabinete Nacional de Cibersegurança (GNS) e do Centro Nacional de Cibersegurança (CNCS), trouxe à discussão a visão europeia sobre os desafios da área. Sublinhou que a Europa “não está a dormir” no combate à desinformação nem na resposta a grandes incidentes digitais. Ainda assim, deixou um alerta claro: é urgente reforçar a cooperação entre as áreas da defesa, dos serviços de inteligência e do setor privado. Além disso, destacou a necessidade de investimentos muito mais significativos em Inteligência Artificial e em soluções avançadas de cibersegurança.

Para Gameiro Marques, a soberania digital vai muito além de uma questão meramente tecnológica ou estratégica – é também uma questão ética e social. “A tecnologia não pode ser cúmplice da erosão democrática. Tem de servir a verdade, a participação e uma sociedade mais justa, informada e livre”, afirmou, sublinhando que a defesa do espaço digital tem de estar ancorada em princípios sólidos.

A intervenção foi complementada por Dan Cîmpean, diretor-geral do Gabinete Nacional de Cibersegurança da Roménia, que partilhou uma perspetiva muito concreta sobre o impacto da desinformação. Para Cîmpean, este fenómeno deve ser encarado como um problema de cibersegurança, já que compromete diretamente a integridade e a disponibilidade da informação, dois pilares fundamentais da segurança digital. Como exemplo, trouxe o caso das eleições presidenciais romenas de 2024, nas quais foram identificadas cerca de 80 mil máquinas a operar de forma coor-

“Criámos uma unidade de Strategic Intelligence para distinguir o que é verdadeiro do que é falso — uma frente crítica no combate às ameaças digitais.”
Bruno Castro,
CEO da VisionWare.

denada, manipulando massivamente redes sociais como o TikTok. O resultado foi tão impactante que “um candidato teve mais visualizações do que a Taylor Swift ou a Rihanna em apenas seis dias”, relatou. A gravidade do caso foi tal que o Tribunal Constitucional romeno acabou por anular o ato eleitoral – algo inédito na história do país.

O encerramento do evento ficou reservado para um momento especial: a intervenção de Bruno Castro, fundador e CEO da VisionWare, acompanhado pelos seus dois parceiros de negócio e cofundadores, Filipe Custódio e António

Veiga. Juntos recordaram os primeiros passos dados em 2005, “num mundo certamente menos digital”, no qual poucos prestavam verdadeira atenção à cibersegurança. Hoje, 20 anos depois, a empresa é uma tecnológica portuguesa credenciada pela NATO, com um olhar atento e global sobre o cenário das ciberameaças.

Bruno Castro sublinhou que fenómenos como ataques híbridos, campanhas de desinformação ou a proliferação de deepfakes deixaram há muito de ser exceções, tornando-se parte integrante do quotidiano digital. Perante este contexto, a VisionWare criou recentemente uma unidade de Strategic Intelligence, dedicada precisamente a distinguir o verdadeiro do falso, numa frente de combate que já se tornou crítica para a atividade da empresa.

Olhando para o futuro, o responsável garantiu que a mesma ousadia que marcou o nascimento da VisionWare continua a ser o motor da equipa. Hoje, essa ousadia traduz-se numa “área de inovação ultra agressiva”, que rejeita zonas de conforto e procura constantemente novas soluções. “Estamos continuamente à procura de respostas abrangentes, inovadoras, e atentos ao que está a acontecer – ou ainda vai acontecer – no ciberespaço”, afirmou. Para Castro, é essa inquietação permanente, quase uma insatisfação criativa, que permite à VisionWare manter-se na linha da frente num ambiente digital cada vez mais complexo, acelerado e desafiante.

Em suma, o evento de celebração dos 20 anos da VisionWare foi mais do que um encontro institucional. Foi um palco de debate sobre o presente e o futuro da cibersegurança, sobre as ameaças reais que pairam sobre o mundo digital e sobre a responsabilidade coletiva – de governos, empresas, instituições e cidadãos – em construir um espaço digital mais seguro, resiliente e transparente. Ao mesmo tempo, foi um testemunho da trajetória de uma empresa portuguesa que, com visão, resiliência e inovação, conquistou um lugar de destaque num setor em constante transformação.



O tsunami da União Europeia para segurar o mundo digital

Regulação ■ O edifício regulatório europeu para o mundo digital está em construção acelerada, tendo a cibersegurança como elemento central. Já é perceptível que as empresas serão obrigadas a adaptar-se e que o tempo para o fazerem está a esgotar-se.

Ricardo Santos Ferreira
rsferreira@medianove.com

NIS2, DORA, CRA, CER, AI Act, Data Governance Act. São estes os acrónimos e siglas que constituem o edifício regulamentar com que a União Europeia (UE) está a transformar o mundo digital. Os avanços tecnológicos das últimas décadas motivaram uma resposta legislativa harmonizada europeia. Mais recentemente, a massificação de produtos e serviços que integram inteligência artificial pressionou a tentativa de regulação desta tecnologia. Tudo isto, constitui um desafio de adaptação para as empresas.

“A Europa está a criar um ecossistema mais seguro, resiliente e inovador, e as organizações precisam de se adaptar rapidamente a esta nova realidade”, diz Inês Antas de Barros, Sócia da área de Comunicações, Proteção de Dados & Tecnologia da sociedade de advogados VdA. Trata-se de uma “estratégia digital ambiciosa para capacitar pessoas e empresas face a uma nova geração de tecnologias, com o objetivo de tornar esta década a ‘década digital’ da Europa”, acrescenta.

O objetivo é promover a inovação tecnológica, num quadro em que a Europa está atrasada, corre mais devagar do que os blocos constituídos pelos Estados Unidos da América e pela China, mas também definir mecanismos para minimizar riscos associados.

“Neste contexto, surgem vários diplomas que impactam diretamente a cibersegurança, com objetivos claros: garantir a segurança e resiliência das empresas, em particular aquelas que atuam em setores críticos, e fomentar o desenvolvimento de produtos digitais mais seguros, o que reforça a confiança dos consumidores”, aponta Inês Antas de Barros. “Compreender a natureza interconectada dos diferentes diplomas é fundamental não



Objetivo da UE é promover a inovação tecnológica, mas também definir mecanismos para minimizar riscos

só para garantir o cumprimento legal e a eficiência operacional, mas também para permitir que as organizações desenvolvessem estratégias avançadas de monetização dos dados que possuem, criando produtos e serviços inovadores e ajustados às reais necessidades dos consumidores”, acrescenta.

O processo está em curso e longe de estar terminado. Ricardo Henriques, sócio e coordenador da área de prática de Propriedade Intelectual e Tecnologias de Informação da Abreu Advogados, aponta que os prestadores de sistemas de inteligência artificial têm já de cumprir determinadas obrigações previstas no Regulamento de IA, seguindo-se a aplicação faseada das restantes normas até ao ano de 2027.

Destaca-se, a seguir a diretiva NIS 2. “O novo regime jurídico da cibersegurança que será instituído pela transposição desta diretiva afetará a resiliência e



Inês Antas de Barros
Sócia
da VdA



Ricardo Henriques
Sócio
da Abreu Advogados

cibersegurança de entidades públicas e privadas que operam em setores críticos da sociedade, como a energia, saúde, transportes, finanças, infraestruturas digitais e alimentação, complementando a regulamentação já existente sobre resiliência das entidades críticas”, diz Ricardo Henriques.

O Cyber Resilience Act complementará, a partir de 2026, este enquadramento legislativo, para os fabricantes de produtos com elementos digitais, responsabilizando-os durante todo o ciclo de vida do produto.

“Este mosaico normativo gera um ambiente regulatório significativamente mais exigente, acompanhado de uma moldura contraordenacional substancialmente mais pesada para o infrator e com possibilidade de responsabilização direta da gestão”, avisa. “Nos próximos anos, será de esperar uma fase de execução destes normativos. Como tal, é tempo

das entidades privadas, e públicas, avaliarem a sua sujeição a estes regimes jurídicos e mapearem a sua trajetória para a conformidade, mapearem e prevenirem os seus riscos e testar a sua resiliência”, acrescenta.

A cibersegurança é central a todas as peças de legislação. É “colocar a cibersegurança como uma das prioridades das organizações”, refere Inês Antas de Barros. “Isso implica a adoção de uma cultura efetiva de segurança *by design*, que inclua a avaliação contínua de riscos e ameaças, a monitorização rigorosa da cadeia de abastecimento, o reporte eficaz de incidentes e vulnerabilidades, assim como a capacitação constante dos colaboradores através de formação adequada”.

Isto vai impactar as grandes empresas, com maiores recursos, mas também micro, pequenas e médias empresas, que terão maior dificuldade de resposta.

“A regulamentação europeia tem procurado acompanhar a evolução das tecnologias, mas a sua complexidade crescente torna difícil criar um quadro regulamentar que seja eficaz para os utilizadores, criador de uma atmosfera de segurança efetiva”, diz ao JE Luís Miguel Ribeiro, presidente da Associação Empresarial de Portugal. É uma queixa recorrente dos empresários: o quadro regulamentar é pesado.

“Uma das maiores fragilidades na implementação destes regulamentos tem a ver com a intervenção das entidades que gerem estas matérias em cada país, que detêm o poder de fiscalização e que têm por missão garantir a conformidade com as melhores práticas”. É outra queixa: nem sempre a regulação é uma ajuda, a começar pela tendência para o gold plating (que aprofunda a legislação europeia quando é transposta, tornando-se masi exigente).

xpand it



**The future isn't artificial.
It's intelligently built.**



www.xpand-it.com

Como as empresas devem enfrentar a tempestade regulatória

Legislação ■ Vai ser um desafio, que para muitas empresas será gigantesco, mas terá de ter resposta. O processo de adaptação também pode ser uma oportunidade para repensar o negócio e acelerar.

Ricardo Santos Ferreira
rsferreira@medianove.com

A tempestade regulatória europeia sobre o mundo digital é inescapável, portanto, as empresas têm de perceber a direção em que sopram estes eventos e reagir em conformidade. Não há outra forma.

“A principal preocupação das empresas, sejam grandes ou pequenas e médias empresas, deve ser, desde logo, compreender quais são as novas obrigações legais que lhes aplicam”, diz Inês Antas de Barros, Sócia da área de Comunicações, Proteção de Dados & Tecnologia da sociedade de advogados VdA. “Estamos a falar de vários diplomas complexos, com âmbitos distintos, mas que estão interligados. Por isso, é fundamental navegar neste verdadeiro puzzle legislativo do setor digital para identificar lacunas e traçar um plano claro de implementação”, acrescenta.

O foco legislativo de Bruxelas é a cibersegurança, criando-se mecanismos para minimizar o risco que o desenvolvimento e a adoção acelerados de novas tecnologias, com a inteligência artificial à cabeça, geram.

Neste campo, da cibersegurança, “as empresas devem focar-se no cumprimento rigoroso dos requisitos específicos de cada diploma,

sob pena de poderem ficar sujeitas desde logo à aplicação de coimas e à responsabilidade dos órgãos de administração”, avisa Inês Antas de Barros, acrescentando que deve ser dada especial atenção à gestão da cadeia de abastecimento, incluindo a revisão dos processos de contratação e dos contratos, à gestão eficaz de incidentes e vulnerabilidades, à implementação do security by design, à formação contínua dos colaboradores e à criação de uma cultura sólida de segurança.

A questão das cadeias de abastecimento é importante, porque mesmo empresas de menor dimensão quando têm como clientes grandes empresas acabam por ver ser-lhes exigidos processos, conformidades regulamentares e informação.

“Quando falamos em empresas, temos de ter a noção de que estamos a lidar com realidades muito diversas. Se as grandes empresas, na sua maioria, conseguem operar com níveis aceitáveis de segurança nas áreas digitais, uma parte significativa de PME não terá capacidade, nem tampouco o conhecimento, para conseguir dar resposta, de forma eficaz, às questões da cibersegurança”, avisa o presidente da Associação Empresarial de Portugal, Luís Miguel Ribeiro.

O risco acrescido, neste caso,



As empresas vão ter de se adaptar à nova legislação rapidamente

é tomarem consciência da situação quando já é difícil reagir em tempo útil, arriscando a desconformidade, por um lado, ou a perda de mercado, por outro.

Inês Antas de Barros alerta que

“Independentemente do ponto de partida, é fundamental que todas as empresas procurem tirar o máximo proveito deste processo”, defende Luís Miguel Ribeiro

o plano de adaptação a esta realidade não deve resumir-se ao cumprimento da lei, mas “deve também adotar uma visão estratégica”.

“Estes diplomas trazem oportunidades valiosas, como a agilização do acesso e partilha de dados, que podem e devem ser exploradas para potenciar o negócio. As empresas que conseguirem transformar estes desafios em vantagens competitivas, garantindo segurança e resiliência, estarão muito melhor preparadas para o futuro”, defende.

Luís Miguel Ribeiro reforça esta ideia: “As empresas estão em diferentes níveis de maturidade. Há empresas que estão a dar os primeiros passos e outras, desde logo aquelas que atuam em setores já objeto de regulação no passado

relativamente a estes temas, partem de um patamar mais avançado”.

“Independentemente do ponto de partida, é fundamental que todas as empresas procurem tirar o máximo proveito deste processo, adotando uma postura proativa e estratégica. Só assim poderão transformar as exigências legais em oportunidades reais de crescimento, inovação e reforço da sua segurança e resiliência”, afirma.

O que é vital é que, independentemente da dimensão da empresa, que o processo de adaptação se inicie quanto antes, “com uma visão global dos diplomas aplicáveis, para tirar o máximo partido das oportunidades que surgem neste novo contexto digital”, remata Antas de Barros.

Utilizador é o elo mais frágil na segurança digital

Hospitais e organismos públicos são hoje terreno fértil para ataques digitais que podem bloquear sistemas, usurpar dados e explorar a falta de preparação dos utilizadores. Os cibercriminosos recorrem cada vez mais a esquemas de fraude digital e a programas que paralisam serviços até ser pago um resgate, colocando em causa informação sensível e a continuidade de funções críticas do Estado.

Em entrevista ao Jornal Económico, João Couras, Executive Director da Claranet Portugal, analisa os riscos e oportunidades que moldam este novo cenário, destacando o papel da Inteligência Artificial, dos centros de operações de segurança – equipas especializadas que monitorizam e reagem a ataques em tempo real – e a necessidade urgente de investir em formação contínua, já que o comportamento dos próprios utilizadores continua a ser o elo mais frágil de toda a cadeia de segurança digital.

Os setores da saúde e da administração pública são alvos prioritários de ciberataques pela sensibilidade dos dados que gerem. Quais são hoje as principais ameaças e que impactos reais podem ter na confiança e na vida dos cidadãos?

As principais ameaças de segurança de que as organizações da saúde e a administração pública são alvo não diferem muito de outros setores de atividade. Destacaria as ameaças de Ransomware e Phishing, na medida em que a importância e sensibilidade dos dados nestes setores torna a sua segurança absolutamente fundamental. No entanto, como sempre, as maiores vulnerabilidades estão centradas em falhas e ações dos utilizadores, pelo que a vertente de formação e sensibilização contínua são cruciais.

Como transformar a cibersegurança de custo inevitável em investimento estratégico e qual o papel da Claranet Portugal no apoio a entidades com falta de recursos e elevada complexidade tecnológica?

A Cibersegurança é já, atualmente, uma das principais rúbricas do orçamento de IT das organizações. O papel da Claranet Portugal é precisamente colmatar a falta de capacidade e recursos especializados das entidades, e em simultâneo apoiar e reforçar a resiliência das organizações com serviços como SOC (Security Operations Center) - um nível de resposta que a maioria dos organismos nunca conseguirá assegurar de forma autónoma, pelos elevados investimentos envolvidos.

A nova diretiva sobre cibersegurança NIS2 vem impor regras mais exigentes.



João Couras, Executive Director da Claranet Portugal.

De que forma pode ser vista não apenas como obrigação, mas também como oportunidade para elevar padrões de proteção e confiança digital?

Acima de tudo, a Diretiva NIS2 coloca a Cibersegurança no topo das prioridades das organizações, legitimando a necessidade de investimentos em meios (pessoas, processos e sistemas) com um referencial, ao mesmo tempo que classifica com clareza os serviços e organismos de acordo com a sua criticidade na sociedade.

Destacaria o serviço 360 Security & Compliance da Claranet Portugal, que permite às organizações obter, em tempo real, uma imagem clara da sua realidade, identificar riscos e vulnerabilidades e obter recomendações para melhorar a postura de segurança, cobrindo a área tecnológica, processos, políticas e obrigações legais e regulatórias (NIS2, DORA, DL/65, RGPD, etc.).

A Inteligência Artificial pode reforçar a cibersegurança, mas também cria riscos. Como equilibrar estas duas dimensões e garantir que a sua utilização não compromete a integridade dos dados dos cidadãos?

De facto, a Inteligência Artificial (IA) está a colocar a Cibersegurança num

novo patamar. Por um lado, os sistemas e as ferramentas atingem melhor performance e permitem enfrentar as chamadas ameaças “zero day” – vulnerabilidades desconhecidas e ainda não corrigidas ou endereçadas em softwares e sistemas operacionais. Por outro lado, surgem ameaças mais elaboradas e que recorrem também a IA para aumentar o nível de sofisticação e êxito dos ataques.

A forma de equilibrar estas duas realidades é recorrer a serviços e sistemas de última geração, garantindo assim as versões mais recentes e o conhecimento mais atualizado. Esta é uma das grandes vantagens dos serviços SOC, que tratam uma grande quantidade e variedade de ameaças.

Quais as grandes tendências que vão marcar a próxima década na interseção entre IA e cibersegurança? E que papel a Claranet Portugal ambiciona desempenhar como parceiro estratégico da modernização digital da saúde e da administração pública?

Aos dias de hoje, já não se consegue pensar a Cibersegurança sem a utilização de IA - desde o tratamento automático de tickets à sua categorização, tipificação e encaminhamento, bem como

à correlação de eventos e comportamentos. A IA está hoje presente em equipamentos, software e ferramentas de forma completamente integrada e indissociável.

Por outro lado, a questão da soberania dos dados é uma preocupação real, não só para garantir a segurança dos mesmos como também para permitir e acelerar a inovação com IA, particularmente em setores altamente regulados. A procura por soluções de Cloud soberanas e seguras é uma tendência que já estamos a acompanhar.

Perante estas tendências, a Claranet Portugal ambiciona ser um parceiro incontornável das organizações da saúde e administração pública, contribuindo decisivamente para aumentar a resiliência e a capacidade de recuperação, sem prescindir da inovação e modernização. Desde os serviços de consultoria, para ajudar no desenho e adequação dos processos, à implementação dos sistemas, à operação e análise de incidentes, passando pela formação e sensibilização dos utilizadores - a Claranet Portugal tem hoje uma oferta global e integrada com todas as áreas de IT, investindo continuamente para garantir a capacitação das equipas, o acesso a tecnologia de ponta e a adequação da oferta aos reais desafios dos Clientes.

Cibersegurança ainda é opaca, mas não é só investimento

Tecnologia ■ A segurança em ambiente digital também é uma questão cultural em Portugal. Falta preparação e trabalho em conjunto, destacam especialistas em evento do JE e da Cisco.

José Carlos Lourinho
jlourinho@medianove.com

A cibersegurança ainda sofre de alguma opacidade e é necessária alguma simplificação. Por outro lado, é importante perceber que a cibersegurança não se baseia apenas no investimento e a forma como as empresas a encaram reflete a cultura dos empresários em Portugal. Estas foram algumas das ideias deixadas no painel que debateu a IA e a Cibersegurança e como é que a tecnologia impacta na competitividade das empresas. Miguel Almeida, responsável máximo da Cisco em Portugal, destacou que “a quantidade de produtos ou plataformas que podemos ter na nossa empresa, em segurança, é brutal e isso leva a uma complexidade adicional.

“É difícil avançar numa simplificação, tendo em conta essa quantidade”, afirmou o responsável que apontou cinco áreas onde as empresas devem preparar-se para investir em soluções de Inteligência Artificial e cibersegurança (ver caixa ao lado)”, diz.

Alexandre Fonseca, presidente do Conselho Estratégico de Economia Digital da CIP, a cibersegurança está muito longe de ser apenas uma questão referente ao investimento uma vez que, no que concerne às empresas, há um aspeto cultural que deve ser assegurado e que é tão ou mais importante. Mas estarão as empresas conscientes dos riscos digitais que podem enfrentar?

Sim e não, conclui o antigo responsável da Altice Portugal: “Há uma consciência para estas temáticas mas não há um grau de preparação em Portugal, num tecido constituído sobretudo por PME. Estudos recentes mostram que em Portugal existe essa consciência, no top management e nas camadas intermédias de gestão. Há uma pressão exterior relativamente a esta temática, com impactos evidentes mas também uma consciência dos colaboradores que estão cada vez mais preocupados com a sua identidade e pegada digital”.

“Nas PME há essa preocupação mas não deixamos de ser latinos porque uma coisa é a consciência e outra é a preparação. Está relacionado com investimento mas também com uma questão cultural que obriga as empresas a agir só perante a casa roubada, digamos em sentido figurado. É preciso estratégia e uma cultura de segurança. O fator humano é relevante mas a empresa deve ter essa cultura de segurança e que essa cultura seja fomentada pela liderança”, destacou.

Alexandre Fonseca realça que a CIP “não fica tranquila” com aquilo que possa acontecer e confessa: “Há muito trabalho a fazer”. Se a tecnologia é “muito importante”, a verdade é que



Assista ao programa no seu smartphone através deste QR Code ou em www.jornaleconomico.pt

Cinco desafios da Cisco

■ **Foco no trabalhador** Primeiro foco deve estar no trabalhador e na forma como este tem que ter cuidado com a sua própria proteção e no mail que envia a uma pessoa, que por sua vez o envia a outra pessoa: “A identidade é um pilar importantíssimo”.

■ **Redobrar cuidados** Os dispositivos que usamos e a quantidade de equipamentos de que dispomos devem ser acautelados: “A proliferação de dispositivos obriga-nos a redobrar os cuidados, até porque muitas das nossas máquinas podem não ter o nível de proteção que deveriam ter.

■ **Resiliência das redes** A Cisco coloca ainda a tónica na resiliência das redes, um aspeto que a Cisco tem especial preocupação, e dá o exemplo da inspeção dos pacotes de criptação, que hoje é um aspeto crítico.

■ **Atenção à ‘cloud’** A tecnológica coloca ainda a tónica na resiliência das redes, um aspeto que a Cisco tem especial preocupação, e dá o exemplo da inspeção dos pacotes de criptação, que hoje é um aspeto crítico.

■ **Fortificação** A Cisco dá especial ênfase à importância da fortificação das plataformas de Inteligência Artificial e a forma como protegemos os dados que são usados nesse tipo de tecnologia.



No debate, Miguel Almeida (primeiro, à esquerda) defendeu que as empresas têm

“existe uma vertente comportamental que é extremamente importante e deve ser levada até à gestão, que muitas vezes acha que não precisa dessa formação”.

E como podem as PME preparar-se quando o investimento pode ser avultado? “A segurança digital é uma tema estratégico e por isso tem que ser um desígnio da organização e não apenas uma preocupação da equipa de IT. Qualquer investimento que seja feito tem que estar assente numa estratégia definida a partir do topo, com métricas e satisfação dessas métricas”.

O responsável máximo da Cisco em Portugal defendeu que a elasticidade económica que as empresas têm para investir em Inteligência Artificial não vai permitir que o façam em outras áreas, como por exemplo a vertente humana.

“A rotatividade que temos hoje em Portugal é incrível, porque há poucas pessoas. Temos muitos portugueses que estão no país, mas não trabalham para o mercado português”, sublinhou.

Miguel Almeida revelou ainda que 86% das empresas estão cientes das ameaças da IA e a sua perceção, assumindo que vão sofrer ataques baseados em Inteligência Artificial, mas que não estão preparadas para responder aos mesmos.

IA: aprender da pior forma

Os desafios e riscos da Inteligência Artificial ganharam maior preponderância para as empresas depois da pandemia e no caso de alguns CEO, esse impacto foi sentido pela negativa. O alerta foi dado por Bruno Castro, CEO da Visionware, no Special Report – IA e Cibersegurança, organizado pelo JE e pela Cisco.



Em cinco desafios a responder, começando pelo foco no trabalhador

“No pós-Covid os gestores começaram a perceber, alguns da pior maneira, o papel da Inteligência Artificial nas suas empresas”, afirmou, salientando que hoje em dia já não conseguimos ver o que é o risco sem pensar no ciberespaço.

Como tal, o CEO defende que este é o ponto para o qual devemos partir para montar um modelo de governação para proteger as empresas desses riscos. “A Inteligência Artificial veio transformar-se num catalisador para o cibercrime”, referiu.

Bruno Castro alertou para o facto, de que hoje qualquer grupo criminoso consegue ter armas e ferramentas através da IA, estando disponível de uma forma global e sem fronteiras.

“No lado do cibercrime consegue-se hoje tornar um ataque que antes era custoso e demorado, criando um e-mail de phishing através da IA, que o

torna mais duradouro e menos dispendioso”, sublinhou.

Trabalhar em conjunto

“Não temos que resolver os problemas todos sozinhos”: essa foi uma das mensagens-chave que o dirigente da CIP deixou neste evento do JE. “As PME têm que trabalhar em conjunto nos vários sectores, a capacidade de trabalhar em rede e de gerar cyber intelligence e partilhar recursos. O outsourcing é fundamental nisto porque há entidades que só se ocupam destes temas. A maior parte das PME em Portugal não têm capacidade para ter um Chief Information Security Officer.

Também é importante olhar para a gestão de risco para que as PME possam impactar este tema da cibersegurança. É importante também que se promova a proximidade às pessoas e às empresas”.

“Desinformação é o maior cancro que podemos ter na internet”

■ António Gameiro Marques, ex-líder do Centro Nacional de Cibersegurança, alerta que vivemos tempos em que o meio digital deixou de ser apenas uma ferramenta e tornou-se um território.

Rodolfo Alexandre Reis
rreis@medianove.com

Areas ferramentas digitais estão a tornar-se um território que se não for conhecido vai trazer riscos para as empresas, democracias e sociedades. O alerta foi deixado por António Gameiro Marques, ex-Diretor-Geral do Gabinete Nacional de Segurança e do Centro Nacional de Cibersegurança, no Special Report – IA e Cibersegurança, organizado pelo Jornal Económico, que decorreu no Hotel Intercontinental Lisboa, na passada quarta-feira.

“Vivemos tempos em que o digital deixou de ser apenas uma ferramenta, tornou-se um território. A desinformação é o maior cancro que podemos ter na internet”, afirmou, realçando que a Inteligência Artificial e cibersegurança podem fazer algo positivo, mas é necessário analisar os impactos que podem trazer ao modelo de sociedade em que vivemos.

Como tal, destacou que como em qualquer território que é novo, é preciso conhecê-lo, até porque há riscos caso isso não aconteça, mas também oportunidades.

“O digital pode redefinir o que é uma empresa, uma democracia e uma sociedade. Olhar para o digital apenas como uma tecnologia, não é olhar pela perspetiva certa”, sublinhou, acrescentando que os desafios da IA não são apenas de natureza técnica, mas sim de natureza política e ética.

O relatório do Centro Nacional de Cibersegurança divulgado na segunda-feira aponta entre outras preocupações para mais ataques a infraestruturas na cloud e um uso ofensivo de ferramen-

tas de Inteligência Artificial degenerativa, dando conta que entre 2019 e 2020, o número de ataques informáticos duplicou e tem vindo a escalar desde então.

Face a estes dados, António Gameiro avisa que é preciso olhar para a IA como uma aliada nas ameaças digitais. “Não olhem para ela como uma adversidade. Bem usada é uma ajuda enorme e eficaz como usamos o nosso tempo. O maior risco não é a IA em si, mas sim a nossa passividade”, referiu.

A finalizar o ex-diretor do Centro Nacional de Cibersegurança salientou ainda a importância da liderança ética, que não pode ser apenas voluntária tem de ser obrigatória e por isso é preciso investir neste campo.

“O digital pode redefinir o que é uma empresa, uma democracia e uma sociedade. Olhar para o digital apenas como uma tecnologia, não é olhar pela perspetiva certa”, afirmou Gameiro Marques

Formação, dinâmica de alianças e beneficiar da Inteligência Artificial

■ António Gameiro Marques, x-Diretor-Geral do Gabinete Nacional de Segurança e do Centro Nacional de Cibersegurança, deixou três conselhos que, no seu entender, devem ser seguidos pelas empresas para saberem lidar com os desafios que se colocam no ecossistema digital. O primeiro conselho passa pelo investimento na formação em literacia digital e deu o exemplo de vários cursos online que podem ser encontrados na página do Centro Nacional de Cibersegurança. Depois, o keynote speaker deste evento do JE e da Cisco realçou a importância de que as empresas se inspirem no Tech Accord e que promovam alianças entre si, lamentando que as alianças para a cibersegurança, promovidas pelo Centro Nacional de Segurança, podiam funcionar melhor. No entanto, deixou uma mensagem de esperança: “as alianças devem ter a dinâmica dos seus próprios membros”. O terceiro e último conselho passa por encarar a Inteligência Artificial como um aliado na deteção de ameaças digitais e no apoio à decisão em casos de crise: “Não olhem para a IA como uma adversidade porque se for bem usada, é ajuda enorme à eficácia e à eficiência com que usamos o nosso tempo. Façam as perguntas certas e garantam a consulta a várias fontes de informação”. A finalizar, António Gameiro Marques deixou uma convicção: “O maior risco não é a IA mas sim a nossa passividade perante essa tecnologia, sobretudo perante os seus efeitos nocivos”. Este responsável deixou o cargo de diretor-geral do Gabinete Nacional de Segurança (e da Autoridade Nacional de Segurança) no final de maio deste ano, ao final de quase nove anos.



Miguel Almeida, diretor-geral da Cisco Portugal



Alexandre Fonseca, do Conselho de Economia Digital da CIP



José Carlos Lourenço, administrador da M9 à conversa com António Gameiro Marques e Ricardo Henriques da Abreu Advogados



Sala cheia no Intercontinental de Lisboa



Ricardo Santos Ferreira e José Carlos Lourenço



O painel do pequeno-almoço de trabalho sobre IA e Cibersegurança



Diogo Madeira da Silva, diretor da Huawei Portugal

Cibersegurança: topo da gestão deve estar envolvida

■ Com a cibersegurança associada à competitividade, estes especialistas deixaram conselhos para que as empresas sejam bem-sucedidas.

José Carlos Lourinho
jlourinho@medianove.com

O envolvimento do topo da gestão nos temas de cibersegurança deve ser um aspeto a ser acautelado pelas empresas para lidar eficazmente com os riscos que o digital acarreta ao funcionamento de organização que está num mercado regulado. Esta foi uma das ideias deixadas no painel do Special Report que contou com especialistas de várias áreas e que assim, conferiram uma visão abrangente desta problemática.

Alexandre Fonseca, presidente do Conselho Estratégico de Economia Digital da CIP, realçou a importância de que as empresas não se limitem a diagnosticar mas também que se foquem na execução e sobretudo que não se escudem sempre nas questões jurídico-regulatórias que são fundamentais mas que não podem bloquear a verdadeira mudança: “É importante definir um plano, perceber onde é que estamos e para onde



Bruno Castro diz que a IA “transformou-se num catalisador para o cibercrime”

é que queremos ir. As empresas têm que se ser geridas de forma diferente, sejam as pequenas ou as grandes”.

Defendeu é importante que, também nas questões da cibersegurança, não se trabalhe sozinho e que se procure trabalhar em rede. Por outro lado, este responsável da CIP falhou na importância de falhar como parte do processo de aprendizagem: “Atitude positiva e execução é fun-

damental”, realçou. Bruno Castro, CEO da Visionware, socorreu-se dos 25 anos de experiência no mercado para dar um conselho rápido na gestão da cibersegurança: “Implementem o modelo de governação de segurança à vossa medida. O envolvimento obrigatório do top management é obrigatório e criem níveis de maturidade de compliance”, destacou. Alertou ainda para a necessidade de comprar

segurança à medida daquilo que a empresa precisa: “Por favor, não comprem banha da cobra e ‘vacinas’ que se dizem milagrosas. Não têm que comprar o melhor, têm que comprar aquilo que se adequa à vossa medida”. Miguel Almeida, diretor-geral da Cisco, aconselhou as empresas portuguesas a definirem os seus modelos de governação olhando para o mercado global.

A formação e a literacia devem ser pedras de toque na resposta da sociedade como um todo, e das empresas em particular, relativamente aos grandes desafios que se colocam face à digitalização. Esta reflexão foi deixada por Ricardo Henriques, Sócio e Coordenador da Área de Prática de Propriedade Intelectual e Tecnologias de Informação da Abreu Advogados. Questionado sobre a grande pressão que se coloca às cadeias de valor, em torno do tema das certificações, este advogado da Abreu Advogados realçou que, face à realidade da digitalização que se vive na economia e na sociedade, “todo o enquadramento regulatório da UE é uma resposta a essa mudança que temos assistido, tanto no AI Act como na Cloud Act”.

“Temos muita legislação nova de que as empresas têm que ter consciência, não só os colaboradores como a própria gestão, ou seja, uma maior responsabilização dos gestores. A formação e a literacia devem ser prioridades, assim como a definição de estratégias e perfil de risco.

Cinco pilares da CIP

■ **Infraestruturas** Apesar de Portugal ser um dos melhores países do mundo nas infraestruturas das redes de comunicação, está na fase de arranque a cobertura de zonas brancas com fibra ótica.

■ **Competências** É importante investir mais tempo nas competências digitais dos adultos em idade ativa e criar a consciencialização em todas as idades de que a Inteligência Artificial vive connosco.

■ **Inovação** A inovação tem que ser uma prioridade e em Portugal deve-se trabalhar na inovação concreta e de curto prazo, criando uma maior proximidade entre o mundo académico e o empresarial.

■ **Valorização** As empresas têm que ter um papel ativo nas questões da economia digital e devem ser promovidas aquelas que entregam resultados à economia.

■ **Estado mais digital** Se o Estado pede à economia que seja mais digital, tem que se tornar ele próprio mais digital. O Estado tem que se modernizar tecnologicamente.

Cibersegurança deve antecipar o futuro para combater ataques e desinformação

Os avanços da tecnologia da informação permitem criar conteúdos falsos que, rapidamente, chegam a milhões de pessoas e podem abalar a credibilidade de instituições, governos e partidos. A boa notícia é que existem soluções que podem identificar padrões de risco, reforçar a monitorização e antecipar cenários

É cada vez mais difícil manter o controlo sobre os conteúdos que circulam nos órgãos de informação, sobretudo nas redes sociais. Por vezes, as revelações mais improváveis sobre pessoas, empresas e governos podem parecer a mais absoluta verdade. O fenómeno chega a atingir a própria diplomacia e bases da democracia e por suas vezes criar conflitos preocupantes. “A guerra moderna já não se combate apenas com tanques, mísseis e soldados no terreno. Inevitavelmente, as batalhas também se desenrolam nos ecrãs, nos algoritmos e nas narrativas”, escreveu Bruno Castro, especialista em cibersegurança e análise forense e também fundador e CEO da tecnológica VisionWare, num recente artigo de opinião.

A credibilidade em risco

Em Portugal, as próximas eleições autárquicas não surgem, felizmente, em contexto de guerra, mas a desinformação ocorre igualmente e pode constituir uma séria ameaça à democracia. Os deepfakes, facilmente produzidos através da inteligência artificial, e os bots que interagem com humanos e não deixam desconfiar que algo pode estar a ser manipulado, revelam que cidadãos e, sobretudo, partidos devem saber como se defender. E vale lembrar que somos, sabidamente, um país em que o pouco interesse dos eleitores se reflete em índices de abstenção elevados, pelo que a questão da credibilidade se impõe e a urgência das soluções se torna evidente.

As soluções existem

A boa notícia é que as soluções existem e a VisionWare tem 20 anos de experiência em segurança da informação. A área de Strategic Intelligence, por exemplo, ao recolher, analisar e interpretar informação, permite antecipar cenários de ameaça e identificar padrões de risco geopolíticos muitas vezes decorrentes de campanhas de desinformação. Desta forma é possível analisar o risco e prevenir ao criar repostas antes que uma crise aconteça. “A forma como as histórias são contadas, percebidas e manipuladas são agora tão relevantes como a ca-



pacidade de realizar um ciberataque. Neste novo cenário, o storytelling e as novas tecnologias emergentes estão a redefinir a estratégia militar e política no espaço digital”, alerta o CEO da VisionWare. A empresa sugere ainda a implementação de um Security Operations Center, SOC, que consiste numa unidade especializada, dedicada à monitorização, deteção, análise, mitigação, resposta a incidentes de segurança e sua respetiva recuperação. Através de avançadas ferramentas de análise e inteligência em coordenação com equipas de operadores/analistas experientes, é possível estabelecer um serviço contínuo de monitorização e alarmística que permita detetar e reagir em tempo útil a eventuais ações erróneas, suspeitas ou maliciosas.

As medidas complementam-se

Para a VisionWare, em quase todos os casos, a proteção cibernética requer não apenas uma, mas um conjunto de medidas que se complementem e tornem realmente seguro o ecossistema virtual. Estas devem ser selecionadas em função daquilo que se pretende proteger, sejam pessoas ou organizações. Nesse sentido, a empresa disponi-

biliza uma gama de serviços altamente especializados que abrangem áreas desde a cibersegurança à ética, privacidade, e investigação forense. Além disso, e uma vez que as pessoas continuam a ser as grandes responsáveis pela consumação das ameaças à segurança da informação organizacional, a VisionWare detém ainda a sua área de formação, VisionWare Academy, que visa sensibilizar e formar os recursos humanos de forma a torná-los agentes de defesa conscientes e proativos.

Cibersegurança estratégica e continuidade operacional

Sendo uma empresa pioneira e altamente especializada em segurança de informação, a VisionWare tem como missão preparar as empresas para enfrentar os riscos diários e atuais da cibersegurança. Com parte do seu compromisso com cada cliente, garante sigilo absoluto e um apurado sentido de responsabilidade. A informação é o bem mais preciso de uma empresa e o foco da VisionWare passa exatamente por zelar por este ativo, orientar as melhores práticas e mitigar riscos em prol de um ambiente de negócio mais fiável e resiliente.

20 anos a conquistar confiança

VisionWare é uma empresa tecnológica 100% portuguesa, fundada em 2005 e que conta já com 20 anos de experiência em Segurança de Informação. É atualmente detentora de uma ampla gama de serviços especializados que incluem: Cibersegurança, TI, Cyber Defense Operations, Investigação Forense, Compliance, Privacidade, Formação e Intelligence. Credenciada pela NATO, a VisionWare é reconhecida pelo seu elevado know-how e capacidade técnica, por instituições portuguesas e internacionais, tendo estado envolvida em mais de 5.000 diversos projetos apoiados pela União Europeia. Com operações comerciais em mais de 12 geografias distintas, a VisionWare possui mais de 200 clientes ativos, e escritórios em Portugal (Sede – Porto, e Filial – Lisboa), bem como em Cabo Verde, no TechPark da Praia e no recém-inaugurado TechPark do Mindelo. A perspetiva futura é de crescimento, contribuindo sempre para o sucesso dos seus clientes, num mundo que é marcado pelas constantes inovações tecnológicas.

Liderar o risco é liderar o futuro: a cibersegurança na agenda da gestão de topo

A cibersegurança deixou de ser uma questão técnica para se afirmar como um risco estratégico de negócio. No setor financeiro, onde a confiança é o ativo mais valioso, garantir resiliência digital é hoje um imperativo para a liderança.

Num mundo cada vez mais interligado, os riscos que afetam as instituições financeiras vão muito além do crédito ou da volatilidade económica. A cibersegurança assumiu-se como uma das principais preocupações, não apenas pela complexidade das ameaças, mas pelo impacto direto que pode ter na confiança dos clientes e na continuidade do negócio. Durante demasiado tempo, este tema foi encarado como responsabilidade exclusiva das equipas de IT. Hoje, sabemos que não é apenas uma questão técnica: é um risco organizacional, que deve ser avaliado ao mais alto nível de gestão. Um incidente cibernético pode comprometer a reputação, a liquidez e, no limite, a própria sobrevivência de uma empresa.

A confiança dos clientes depende, em larga medida, da capacidade de proteger a informação e garantir a continuidade dos serviços.

O setor financeiro está na linha da frente desta realidade. A sensibilidade dos dados que gere, o volume de transações em tempo real e a atratividade

para cibercriminosos tornam-no um alvo preferencial. Segundo o relatório ENISA Threat Landscape – Finance Sector 2024, só no último ano foram registados 432 ataques cibernéticos contra instituições financeiras europeias. O número impressiona, mas mais relevante é o que está em causa: a confiança.

Na Cofidis, tratamos a cibersegurança como risco estratégico, avaliado regularmente pelo Comité de Direção e pelo Conselho de Administração. Não é um ponto secundário na agenda: é central. Este compromisso traduz-se em formações contínuas para todos os colaboradores, testes de resiliência e planos de crise e continuidade bem definidos. Além disso, práticas de desenvolvimento seguro são aplicadas a cada novo projeto, garantindo que a segurança está integrada desde a origem. O novo paradigma da liderança de risco exige mais do que prevenir: é preciso antecipar e preparar respostas. A resiliência constrói-se com políticas claras, processos robustos e equipas treinadas para agir de forma rápida e transparente. Só assim é possível reduzir o impacto de um incidente e preservar a confiança. E é precisamente a confiança



Cláudio Pimentel, Diretor de Sistemas de Informação da Cofidis Portugal

A governação do risco cibernético é uma responsabilidade partilhada que começa no topo.

o ativo mais crítico do setor financeiro. A proteção rigorosa dos dados e a capacidade de responder com transparência em caso de incidente são determinantes para manter a credibilidade junto dos clientes e do mercado. Mais do que proteger ativos, uma instituição que investe em cibersegurança fortalece a sua marca e a sua posição competitiva. Mas não basta tecnologia e governação. A literacia digital e de segurança das equipas é hoje essencial. Quanto mais preparados estiverem os colaboradores para identificar riscos e comportamentos fraudulentos, maior será a resiliência da organização. Por isso, a formação contínua e a cultura de segurança devem ser encaradas

como investimento estratégico, não como custo.

Para os gestores de topo, a mensagem é clara: integrar a cibersegurança no mapa global de riscos, envolver todas as áreas da organização e avaliar regularmente a capacidade de resposta. Liderar o risco é liderar a confiança. E sem confiança não há sustentabilidade possível. No setor financeiro, a cibersegurança já não é uma escolha – é um imperativo estratégico. Só as organizações que combinam visão integrada, cultura de resiliência e governação de risco robusta estarão preparadas para prosperar. Em última análise, liderar o risco é liderar o futuro.

Não basta prevenir — é crucial antecipar, preparar respostas e construir verdadeira resiliência cibernética