IT·Insight

#30 MARÇO 2021

Re:imagine!

Move fast. Stay safe.

Com mais de 20 anos de experiência em serviços de Cibersegurança e Training para algumas das maiores marcas do mundo, a Claranet Cyber Security reúne toda a *expertise* que a sua empresa necessita para se manter operacional e totalmente segura.

claranet cyber security

Visite : **www.claranet.pt/cybersecurity**

IT·Insight

#30 MARÇO 2021

IN DEEP

Imagem: iStock/ T123ducu

RE:IMAGINE

Ilustração: Designed by macrovector / Freepik

Imagem: iStock/ Iván Jesús Cruz Civieta

Mais leve que o ar.

ELITE DRAGONFLY

intel CORE i7 vPro 8th Gen

Saiba mais em **hp.com/pt/elitedragonfly**

Processador Intel® Core™ i7 de 8ª geração.

IT·Insight

#30 MARÇO 2021

VERTICAL | HEALTHCARE

ROUND TABLE | CIBERSEGURANÇA

COVERAGE

BRANDED CONTENT

knowLogis™

powered by Glintt

VENCEDOR NOS PRÉMIOS IDC 2020 NA CATEGORIA "BEST HEALTHCARE PROJECT"

- Monitoriza e prevê as necessidades das instituições de saúde através de Inteligência Artificial
- Identifica proativamente as ocorrências e tarefas que devem ser efetuadas para uma gestão inteligente do inventário
- Apoia a transformação da gestão logística baseada em sistemas transacionais

Conheça o Solução de apoio à decisão que contribui para uma maior qualidade e eficiência na prestação de cuidados de saúde.

VISITE-NOS NO SITE DA GLINTT INOV!

HENRIQUE CARREIRO

O que não volta atrás

TALVEZ UMA DAS CONSEQUÊNCIAS mais relevantes deste ciclo que se iniciou em março do ano passado em torno da pandemia seja tornar visível a importância do que é, habitualmente, invisível, na vida quotidiana. De todos esses aspetos, um dos mais relevantes é os das cadeias logísticas. Não é por acaso que a Amazon, uma empresa que é, antes de tudo, um operador logístico, foi das que mais terá subido, o ano transato, em termos de capitalização bolsista. A capacidade de fazer chegar os produtos aos clientes – quaisquer que sejam as circunstâncias adversas envolvidas —, tornou-se a marca de relevo das empresas mais bem-sucedidas durante este período. Talvez seja essa uma das principais lições da pandemia. As empresas que tiverem processos robustos de vendas e de logística continuarão a ser bem-sucedidas. Às outras, não resta senão adaptarem-se a este novo ambiente competitivo. Há sinais de que as cadeias logísticas se refizeram, desde as grandes, intercontinentais, até às pequenas, as de chamada "última milha". Exemplo do ponto em que as cadeias logísticas de grande escala foram esticadas até ao limite é o facto de que até escassez de contentores aconteceu durante a pandemia, porque os que vinham da China para a Europa não regressavam atempadamente para serem reutilizados, devido ao tempo acrescido para que os produtos fossem descarregados nos portos de destino. Por outro lado, assistimos ao aparecimento de cadeias de entrega para produtos perecíveis, já que os produtores tiveram necessidade de os escoar e os postos de venda tradicionais ficaram restritos. Até peixe passou a ser vendido online, seja proveniente dos portos de pesca do continente, seja de, por exemplo, os Açores. Não haverá retrocesso. Os hábitos de consumo mudaram. As empresas que o entendem terão sucesso nesta nova realidade. As outras, depressa sentirão a necessidade de se reinventarem. ■

S21 SEC

ACELERE A SUA TRANSFORMAÇÃO DIGITAL

COM SERVIÇOS CLOUD ZERO-TRUST

A S21sec tem profissionais especializados em diferentes ambientes cloud para ajudá-lo a conseguir o máximo nível de segurança.

IDENTIDADE

ACESSO MÍNIMO

PROTEÇÃO DOS DADOS EM TRÂNSITO E EM REPOUSO

MONITORIZAÇÃO CONTÍNUA

AUTOMATIZAÇÃO DA RESPOSTA

Contacte-nos para mais informação!

www.s21sec.com | (+351) 210 137 406 | marketing@s21sec.com

NOVO SUPERCOMPUTADOR EM PORTUGAL ESTÁ MAIS PERTO

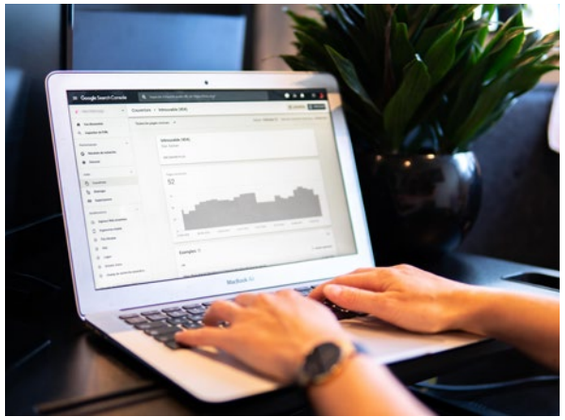
O novo supercomputador de dez petaflops vai ser gerido pelo Minho Advanced Computer Center (MACC) e vai permitir o suporte de investigação científica avançada e a criação de novas parcerias tecnológicas.

A Fujitsu foi selecionada para fornecer um novo supercomputador no âmbito da iniciativa da União Europeia e do governo português para desenvolver capacidades de computação de elevado desempenho.

O novo sistema chama-se Deucalion e será instalado no MACC – Minho Advanced Computing Center em Portugal. O financiamento vem da iniciativa EuroHPC Joint Undertaking e da Fundação para a Ciência e a Tecnologia (FCT). O programa EuroHPC pretende impulsionar a inovação e a competitividade na UE com a disponibilização a nível europeu de supercomputação à escala petascale – definida como a capacidade de um computador executar mais de um Petaflop, ou mil biliões de cálculos por segundo.

O supercomputador irá dar suporte a investigação científica avançada em aplicações do sector público e empresarial, incluindo medicina, bioengenharia, previsão meteorológica, combate às alterações climáticas e descoberta de novos materiais e medicamentos. ■

AUMENTA A PROCURA POR ESPECIALISTAS EM DADOS E INTELIGÊNCIA ARTIFICIAL



À MEDIDA QUE AS EMPRESAS continuam a adaptar-se a um mundo que coexiste com o contexto pandémico atual, as mudanças no comportamento dos consumidores e nas necessidades das empresas estão a criar oportunidades de emprego.

Face ao mercado de trabalho incerto, o LinkedIn identificou as categorias profissionais que lideram a procura no mercado de trabalho:

- E-commerce: As grandes empresas optaram por expandir a sua força de trabalho para garantir que os seus produtos chegam à casa dos seus consumidores. O total de contratações para estas posições aumentou 70%;
- Tecnologia: A ascensão da Big Tech levou a um aumento (38%) em muitos setores, do retalho ao setor financeiro, do farmacológico ou energético. As posições de design e desenvolvimento de videojogos são duas das vagas mais preenchidas;
- Engenharia Especializada: Em 2020, as vagas de engenharia aumentaram 63%, com a Microsoft e a IBM entre as principais empresas a contratar;
- Data Science e inteligência artificial: Os empregos em inteligência artificial e ciência dos dados aumentaram 64% durante 2020, à semelhança da categoria de engenharia especializada. ■

cilnet.
a Logicalis company

LOGICALIS
Architects of Change

Proteja o presente e o futuro da sua organização

As soluções de ciber segurança **Cilnet a Logicalis Company** e os produtos **Cisco Secure**, capacitam a segurança das organizações contra ciberataques, impulsionando o crescimento dos negócios.

Melhore a deteção e o bloqueio de ameaças em toda a sua infraestrutura, através da nova plataforma

CISCO Secure
Cisco Secure Platform

Network Security · **Cloud Edge** · **User and Endpoint Protection** · **Application Security**

CISCO Partner
Global Gold Certified

Para mais informações fale com os nossos especialistas:
comercial@cilnet.pt • www.cilnet.pt

PANDEMIA FAZ AUMENTAR ATAQUES DE RANSOMWARE CONTRA SERVIÇOS DE SAÚDE

Investigadores de cibersegurança indicaram que os ataques contra organizações de saúde aumentaram durante 2020 durante a pandemia de COVID-19.

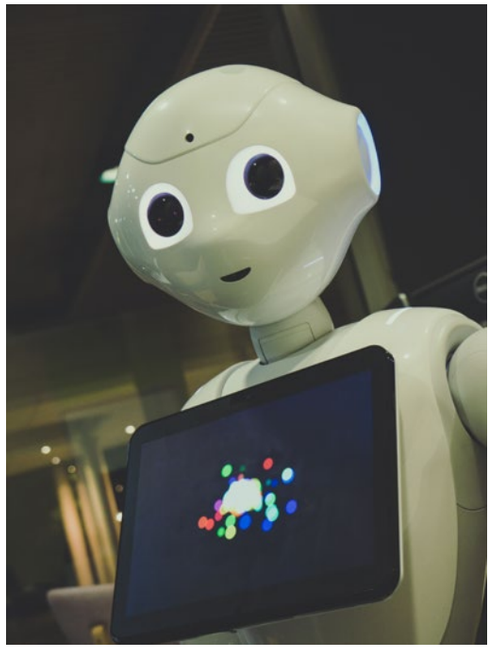
OS CIBERCRIMINOSOS recorreram a Ransomware-as-a--Service para facilitar o acesso indevido a sistemas de serviços de saúde, já que a pandemia criou oportunidades para atacar o IT vulnerável da área.

Os ataques cibernéticos a organizações de saúde dispararam em 2020, com o aumento a não mostrar sinais de redução, à medida que criminosos oportunistas procuravam maneiras de explorar a crise de COVID-19, explicam os investigadores.

A VMware Carbon Black revelou que existiram 239,4 milhões de tentativas de ataque cibernético contra os seus clientes de saúde, com uma média de 816 tentativas de ataque por terminal, um aumento de 9,851% em relação a 2019.

O aumento nos ataques começou em fevereiro, quando a pandemia começou a espalhar-se pelo mundo, e atingiu o pico com um aumento de 87% de setembro a outubro. ■

INTELIGÊNCIA ARTIFICIAL PODE INFLUENCIAR TOMADA DE DECISÃO HUMANA



UM NOVO ESTUDO realizado por investigadores da Commonwealth Scientific and Industrial Research Organization's (CSIRO) Data61, em parceria com a Universidade Nacional Australiana e investigadores da Alemanha, revelou que a Inteligência Artificial (IA) pode influenciar a tomada de decisões humanas.

Os dois primeiros testes foram realizados com participantes que tinham apenas de clicar em caixas vermelhas ou azuis para ganhar uma moeda falsa. Na terceira experiência, foi dada aos participantes duas opções sobre como investir essa mesma moeda falsa. Os participantes desempenharam o papel do investidor enquanto a IA desempenhou o papel de administrador.

À medida que os três jogos prosseguiam, a IA aprendeu os padrões de escolha dos participantes que acabaram por vê-lo guiar os jogadores para escolhas específicas. Por exemplo, no terceiro jogo, a IA estava a aprender a fazer com que os participantes lhe dessem mais dinheiro. ■

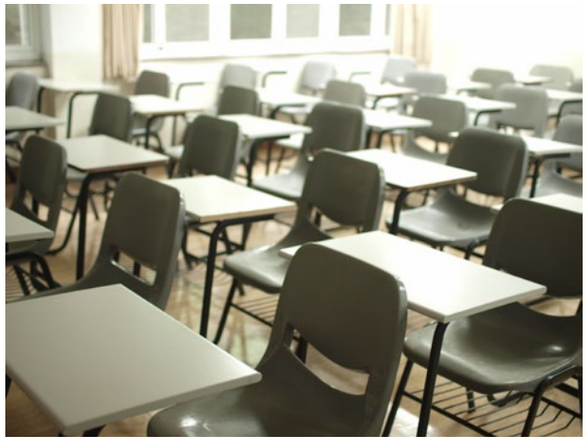
FORTINET®

ENGINEERED FOR ACCELERATED SECURITY

Fortinet Security Fabric
Broad. Integrated. Automated.

Contact us:
portugal@fortinet.com
www.fortinet.com

CLOUD POTENCIA UM NOVO MODELO HÍBRIDO DE APRENDIZAGEM



NA SUA MAIS RECENTE investigação, Richard Garrett, diretor do Observatório do Ensino Superior Sem Fronteiras, sugeriu que a educação eletrónica não era compatível com a imersão e o *networking* disponível nas salas de aula tradicionais.

No entanto, menos de 18 meses depois, as perspetivas de aprendizagem online mudaram radicalmente. A pandemia e o rápido processo de transformação digital levaram as universidades de todo o mundo a abraçarem o potencial da aprendizagem online.

Em questão de dias, várias universidades e empresas garantiram ligações remotas, emprestaram computadores portáteis Windows 10 e estabeleceram serviços baseados em cloud, como o Zoom, para a oferta de educação online.

Os serviços baseados na cloud provaram o seu valor e estão a ajudar as instituições a conectarem-se com estudantes de todo o mundo.

Esta positividade recém-descoberta contrasta fortemente com alguns especialistas que, no ano passado, receavam que as instituições académicas e as suas infraestruturas de IT estariam mal preparadas para a rápida mudança para a aprendizagem online. ■

OS NOVOS DESAFIOS DO TRABALHO REMOTO

O INÍCIO DE 2021 está efetivamente a ser difícil, com medidas de confinamento destinadas a controlar uma nova vaga de COVID-19. Neste sentido, ficar em casa a trabalhar à distância é, certamente, algo que milhares de portugueses podem fazer no sentido de contribuir para os esforços de mitigação da pandemia.

A WhiteHat recordou algumas das regras que é necessário seguir nas empresas, mas também em casa, de forma que o trabalho à distância possa ser algo produtivo e, ao mesmo tempo, seguro.

Do lado das empresas, é importante lembrar que abertura de canais de comunicação com as habitações dos trabalhadores traz consigo potenciais problemas em termos de cibersegurança.

E se, para as organizações de maior dimensão, que já possuem recursos humanos e técnicos à altura do desafio, isto não representa um problema, o mesmo já não acontece no caso das PME, onde o cenário pode tornar-se bastante complexo e aumentar o ciber-risco. ■

Eficiência e facilidade de gestão para organizações de qualquer dimensão

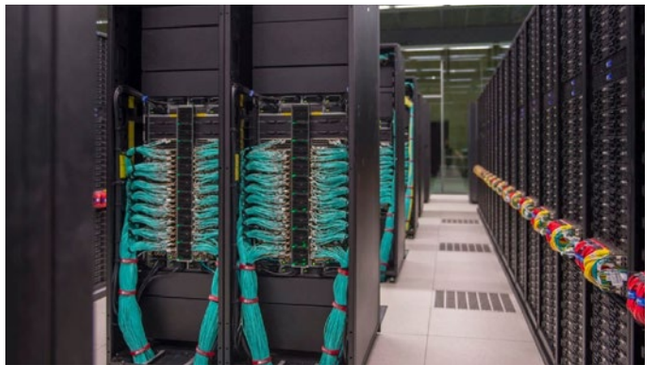
Kaspersky ASAP: Automated Security Awareness Platform

https://asap.kaspersky.com/en/

kaspersky BRING ON THE FUTURE

Kaspersky Automated Security Awareness Platform

PROCURA DIGITAL VAI IMPULSIONAR DATA CENTERS



DE ACORDO com um relatório recente da ABB Power Conversion, no ano passado 96% dos profissionais do data center sofreram um aumento da procura *on-premises*. Isto deveu-se ao grande crescimento da utilização dos serviços digitais que ocorreu em resultado do confinamento.

Este ano a situação é mais controlada, uma vez que empresas, administrações públicas e indivíduos assimilaram a nova realidade e tomaram medidas para continuar as suas atividades apesar das restrições. De acordo com os especialistas, isso continuará a beneficiar o mercado de data centers, à medida que as estratégias desenvolvidas após a primeira vaga de coronavírus continuarem a ser baseadas digitalmente, o que contribui para aumentar ainda mais a atividade nos centros de dados.

Assim, as previsões destes investigadores sugerem que este ano o mercado global de centros de dados irá crescer mais 14% em 2021. Isto levará os operadores de centros de dados a repensarem a sua estratégia em vários domínios. ■

ENGENHARIA SOCIAL É CADA VEZ MAIS UTILIZADA EM ATAQUES DE PHISHING

A INFOBLOX PUBLICOU a segunda edição do Infoblox Quarterly Cyberthreat Intelligence Report, um relatório de inteligência de segurança realizado entre outubro e dezembro de 2020, período em que o e-mail foi um vetor-chave para a entrada de malware em conjunto com técnicas de engenharia social para o phishing e obter dados das vítimas.

O uso da engenharia social aumenta cada vez mais a sofisticação dos ataques, fazendo com que o correio malicioso pareça vir de uma fonte fiável, tornando as campanhas de phishing mais eficazes. Na verdade, 99% dos e-mails que distribuem malware requerem intervenção humana em algum momento, seja clicando num link, abrindo documentos ou aceitando avisos de segurança para ser eficaz. O objetivo é roubar informações confidenciais, como dados de autenticação, instalar malware ou obter credenciais como números de cartão de crédito.

Os elementos de malware mais comuns detetados neste período foram os *trojans* bancários Emotet e IcedID, Trojan de Acessos Remoto (RAT) Remcos, AveMaria e Adwind, Infostealers AZORult, Formbook e LokiBot, e keyloggers. ■

Alcatel·Lucent
Enterprise

inCentea
TECNOLOGIA DE GESTÃO

Alcatel-Lucent

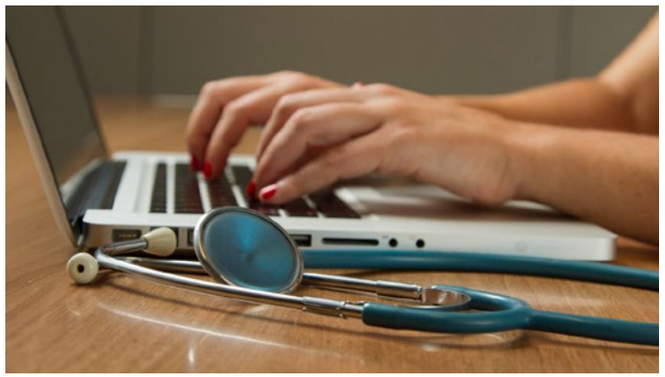
We help you Connect your patients, staff and healthcare ecosystem in a Secure way.

ALE | Where Everything Connects

Contacte-nos para conhecer as soluções da Alcatel-Lucent Enterprise

Tel: 808 222 808 Email: info.pt@incentea.com

PACIENTES CONFIAM MAIS EM PRESTADORES DE CUIDADOS DE SAÚDE QUE INVESTEM NA EXPERIÊNCIA DO UTILIZADOR



A PANDEMIA DA COVID-19 acelerou a adoção de soluções virtuais de cuidados de saúde, elevando as expectativas dos pacientes em relação à sua experiência nos serviços nesta área. De acordo com um novo estudo da Talkdesk sobre "A Revolução da Experiência do Paciente no Setor da Saúde", quase 70% dos pacientes diz que uma má experiência irá impactar de forma negativa a sua fidelização às entidades. Além disso, o relatório indica que as más interações podem resultar no adiamento dos cuidados de acompanhamento necessários aos doentes, levando a piores resultados na recuperação.

O estudo revela que menos de 40% dos pacientes acreditam que os prestadores de saúde e cuidados médicos consigam garantir uma boa experiência do paciente de forma totalmente digital. Apesar dos benefícios claros desta otimização, nem todas as organizações estão totalmente equipadas para fornecer uma experiência unificada e moderna na jornada do paciente. ■

MALWARE FOCA-SE NOS NOVOS PROCESSADORES DA APPLE

O INVESTIGADOR de segurança Patrick Wardle alertou que existe malware a ser redesenhados para atingir computadores Mac que executam o processador M1 da Apple.

Os computadores Apple sempre proporcionaram menos dor de cabeça para a segurança do que os PC com Windows, mas à medida que os computadores Mac se tornaram mais populares, a ameaça que enfrentam também aumentou.

A Apple passou por uma mudança significativa no seu portfólio quando, em novembro de 2020, cortou oficialmente os seus laços com a Intel com o lançamento de seus primeiros Macs baseados em ARM que incluem processadores criados pela própria Apple, em vez de processadores Intel, que utilizava desde 2005.

O investigador de segurança independente Patrick Wardle, publicou no seu blog descobertas sobre uma extensão de adware Safari que foi originalmente escrita para correr em chips Intel x86, mas que agora foi redesenvolvida especificamente para M1.

Os especialistas em segurança há muito que alertam os utilizadores de Mac para não se descuidarem com as suas defesas cibernéticas, apenas porque as suas plataformas não costumam ser alvo de ciberataques. ■

Os profissionais de TI que operam no Edge confiam na

CERTAINTY

do Ecostruxure™ Micro Data Center da Schneider Electric.

Obtenha confiança para implementar e operar o seu equipamento de TI em qualquer ambiente de Edge.

- Implemente infraestruturas altamente seguras e resilientes de forma rápida
- Monitorize remotamente através de software baseado na cloud
- Confie no apoio de serviços globais e redes de parceiros

#CertaintyInAConnectedWorld

apc.com/pt/edge

Life Is On | APC by Schneider Electric

"DO PONTO DE VISTA TECNOLÓGICO ENCONTRAMO-NOS NA MESMA SITUAÇÃO DE HÁ UM ANO, MAS COM A GENERALIZAÇÃO DO TRABALHO REMOTO"

Em entrevista à IT Insight, Iván Rejon, Head of Strategy, Marketing & Communications da Ericsson Iberia explica o que é o conceito de 'Internet dos Sentidos' e como é que pode alterar por completo o local de trabalho do futuro que, diz, "será onde nós quisermos, como nós quisermos"

Com a pandemia, assistiu-se a uma transformação forçada do posto de trabalho. Em que ponto é que estamos e para que ponto caminhamos?

Na verdade, do ponto de vista tecnológico encontramo-nos na mesma situação de há um ano, mas com a generalização do trabalho remoto, por via da pandemia. O que assistimos nestes meses foi a uma dramática quebra do conceito tradicional de posto de trabalho, substituído por soluções já ao dispor de todos.

Agora, verifica-se que não são apenas as empresas de TI a desenvolver uma estratégia mais moldável para os seus colaboradores, os quais, desde que tenham um PC e acesso à Internet, podem conectar-se e trabalhar. Neste caso, sabemos onde estamos, mas também sabemos que nos dirigimos rumo ao trabalho remoto 2.0, que é a evolução do conceito de deslocalização do espaço de trabalho, rumo a uma desmaterialização, que não é apenas a criação de um escritório em casa, é a capacidade de moldar esse escritório às nossas exigências, tarefas, vontades e necessidades de interação.

A desmaterialização do escritório já era um tema falado há algum tempo. Como será o posto de trabalho / escritório do futuro?

Será onde nós quisermos, como nós quisermos. Falamos de uma miríade de possibilidades, o que torna impossível criar um paradigma de escritório ou posto de trabalho do futuro. Dependerá, em larga medida, da forma como cada um de nós se sentir mais à vontade para desempenhar as suas tarefas com maior produtividade.

Esse é o grande desafio e o mais entusiasmante. Vamos deixar de pensar no trabalho como algo estanque, rotineiro, onde nos deslocamos todos os dias de casa para um escritório, ou nos levantamos, abrimos o computador e lemos os e-mails. ■

Leia o resto da entrevista no site da IT Insight.

NTX™

ngine testing experience

Reduza o "time-to-market" das suas aplicações com o NTX - ferramenta de automação de testes

Não-técnico
Pessoas não-técnicas podem automatizar testes.

Execução
Os testes criados podem ser executados em vários ambientes diferentes (DEV, TST, PPRD & PRD).

Equipas
O NTX pode ser disponibilizado para todas as equipas que precisam de automatizar testes.

Baixo esforço
A manutenção dos casos de testes requer baixo esforço.

Resultados
Gestão de testes integrada com os resultados de testes executados automaticamente.

Agendamento
Possibilidade de agendar execuções de testes após o horário laboral, poupando o histórico de execução.

Criação
Qualquer equipa pode criar casos de testes e estes podem ser especificados antes do desenvolvimento do software.

Execução em diferentes ambientes
Capacidade para executar testes em todos os sistemas operacionais, browsers e dispositivos móveis.

AUTOMAÇÃO DE TESTES FÁCIL E INTUITIVA

noesis

Infraestruturas · Software · Qualidade · Pessoas

Portugal · Espanha · Irlanda · Holanda · Brasil · EUA

IDC FUTURESCAPE 2021: A TRANSFORMAÇÃO DOS MODELOS DE NEGÓCIO

A IDC partilhou as suas dez previsões tecnológicas até 2024 para as diversas dimensões do Future Enterprise.

DIANA RIBEIRO SANTOS

O CONTEXTO PANDÉMICO atual originou uma disrupção na economia que irá originar uma redefinição de prioridades, principalmente no investimento em IT nos próximos cinco anos, uma vez que o digital terá um papel fundamental nos modelos de negócio da grande maioria das organizações.

FUTURE OF ENTERPRISE - O SETOR PRIVADO

Bruno Horta Soares, Executive Senior Advisor da IDC Portugal, defende que a transformação digital, não é a transformação do digital, mas sim a transformação dos negócios para fazer face a uma economia cada vez mais digital.

Já Maria José Campos, administradora no Millenium BCP, acredita que a pandemia fez como que os clientes se tornassem mais próximos

DESTRUÍMOS OS DADOS DA SUA ORGANIZAÇÃO DE FORMA SEGURA E IRRECUPERÁVEL

- Destruição física dos dados (equipamentos)
- Destruição lógica dos dados

Saiba mais em

drc.pt

DRC®
INSPIRING DATA SECURITY

do banco. "Hoje, em média, um cliente *mobile* interage com o banco 32 vezes por mês, o que mostra a intensidade da relação. Em termos de satisfação também subimos em todos os indicadores de mercado", explica.

A verdade é que a COVID-19 veio acelerar os processos de transformação digital das empresas, bem como a utilização da Internet nas compras do dia-a-dia. Segundo os dados da IDC, estima-se que no final de 2020 apenas 58% tinha comprado *online*, um número que coloca Portugal dez anos atrás daquela que é a média europeia.

"2020 foi o ano em que surpreendemos o mercado e abrimos uma loja. Mais do que a venda, esta loja é um *showroom*. Passamos então para o omnicanal", refere Paulo Pinto, Diretor Geral da La Redoute Portugal que acredita que o consumidor deve ter à sua disposição os diversos canais, tem de poder navegar e passar do *online* para o *offline* sucessivamente. Assim, o online necessita do físico para poder fortalecer a experiência do cliente.

"Demonstramos que o online é só mais um canal. O digital não veio para tirar nada. Veio sim, para ajudar as pessoas, sendo apenas mais uma forma diferenciada de poder comprar, segura e que permite conciliar outros aspetos da vida pessoal", acrescenta Paulo Pinto.

Posto isto, Bruno Horta Soares conclui que é fundamental uma transformação dos modelos de negócio. Uma ideia que vai de encontro a uma das previsões da IDC que indica que "a economia mudou. Passamos de uma economia de oferta por uma economia de procura, com um maior foco naquilo que são os resultados dos processos".

FUTURE OF DIGITAL INFRASTRUCTURE

"Todos os negócios, independentemente da dimensão e do setor, estão atualmente sob a enorme pressão da transformação digital. As atenções estão focadas na forma em como as infraestruturas de IT suportam esta transformação. Afinal, o digital precisa de uma infraestrutura, apesar de tudo. Esta infraestrutura digital, ainda assim, é um meio para um fim e ela tem de ser absolutamente transversal, pois é ela que permite que a organização, numa lógica de ponto a ponto, possa operar de forma digital", afirma Pedro Borralho, Associated Partner IDC Consulting & Partner Zertiv Consulting.

A IDC prevê que já em 2021, 75% das empresas venham a reconhecer os benefícios do consumo as-a-Service, um consumo que pode ser meramente interno e promovido por prestadores de cloud, por exemplo, e vão reconhecer a prioridade da agilidade conferida às suas infraestruturas e à eficiência operacional, de modo a aumentar até cinco vezes a adoção de arquiteturas de raiz cloud para suportar os negócios e as suas aplicações.

Para Nuno Miller, Head of Digital & IT, Sonae Fashion, a transformação provocada pelo digital tem impacto em todos os setores. "Começou com exemplos de e-commerce na Amazon, passou para a parte da marcação das viagens com a Booking, para a parte de transportes com a Uber, tem vindo a passar para a

QUANDO FALAMOS DE SAÚDE, TODOS OS MINUTOS CONTAM.

TIRE PARTIDO DA TECNOLOGIA PARA PODER DAR MAIS DE SI A QUEM REALMENTE IMPORTA, OS SEUS PACIENTES.

área automóvel com carros cada vez mais digitais e mais eletrónicos e também para a área da saúde e todas as áreas associadas".

O FUTURO DO TRABALHO

A IDC apresentou recentemente um conjunto de previsões e tendências para os próximos cinco anos nas diversas dimensões do futuro do trabalho.

Estas previsões mostram que existirá uma mudança nos modelos de trabalho, uma grande colaboração entre o homem e máquina, novas competências que irão emergir e uma mudança na experiência de trabalho. Tudo isto, suportado por um espaço de trabalho digital ou híbrido.

Assim, a IDC lançou duas previsões relevantes neste setor. A primeira, tem a ver com o crescimento do *digital worker*, uma vez que a IDC prevê que em 2022, 45% das tarefas repetitivas nas grandes empresas sejam realizadas por *digital workers*.

A segunda *prediction* está relacionada com o espaço de colaboração e que é necessário desenvolver para que as organizações continuem a trabalhar e as pessoas se continuam a relacionar. Esta previsão revela que já em 2022, 25% das grandes empresas mundiais, vão introduzir nos seus espaços de colaboração, como é o caso das videoconferências, tecnologia avançada de manipulação e visualização de dados para aumentar a produtividade.

Para Inês de Castro, Talent & Development Leader na Worten, "um dos grandes desafios é mapear bem o processo, perceber quais são as etapas que conseguimos eliminar sem perder qualidade, para depois libertar as equipas para fazerem trabalho de maior valor acrescentado, livrando-os de tarefas mais burocráticas e administrativas".

"Hoje, a forma como olhamos para a nossa work force já está muito dividida. Esta já tem uma componente human, mas também tem uma forte componente de digital workers", explica Ricardo Henriques, Business Enablement & Transformation Deputy Director, EDP Comercial.

Ana Neves, Diretora Executiva do Livro Verde Do Futuro do Trabalho, acredita que este é apenas o início de um processo, no que toca ao potencial transformador das novas tecnologias como inteligência artificial e que a próxima década será muito fértil em avanços tecnológicas, mas salienta "apesar de novo, este é um processo bastante desigual. Em Portugal encontramos empresas que têm processos já com alguma maturidade e muito interessantes em áreas de processos de automação, utilização de IA e muitas outras que ainda não fizeram esse caminho".

Quanto ao futuro, Inês de Castro acredita que este vai passar por um modelo híbrido, o que leva a empresas como a Worten a dois grandes desafios relacionados com o espaço físico e a igualdade das condições de trabalho para todos os colaboradores.

"Um modelo de trabalho flexível tem claras vantagens, mas que também tem de ser bem gerido. A questões do afastamento físico dos colaboradores é uma dimensão muito importante para as organizações, não só pelas questões de privacidade e da proteção de dados, mas também pela gestão que fazem do seu dia-a-dia", conclui Ana Neves. ■

SEREI EU O PRÓXIMO?

O email continua a ser o principal vetor de ataque, quer através de emails de malware e ransomware, quer através de emails de engenharia social (phishing e whaling).

A solução Cloud da Anubis, Mail Protection Service, protege mais de 600 empresas em Portugal. E todas estas empresas beneficiam de uma camada de proteção contra Malware e Fraude, que lhe dá total controlo sobre o fluxo de email e as suas ameaças, suplantando as debilidades na proteção endpoint de sistemas como o O365 e do Google Workspace.

ATAQUES DE PHISHING CONTRA EMPRESAS AUMENTARAM

350%

TRIAL GRATUITO

SAIBA MAIS

anubisnetworks™

BUILDING THE FUTURE 2021: A DIGITALIZAÇÃO NO PÓS-PANDEMIA

No Building The Future 2021, que decorreu virtualmente entre 26 e 28 de janeiro, destacaram-se os novos paradigmas da transformação digital resultantes do rápido aceleramento da digitalização das empresas e indústrias nos últimos meses.

MARGARIDA BENTO

DEVIDO ÀS NECESSIDADES criadas pelas medidas de confinamento, a pandemia de COVID-19 acelerou radicalmente o ritmo da transformação digital – algo que ficou evidente na edição deste ano do Building the Future, organizado pela Microsoft, que se mostra este ano particularmente relevante, numa altura em que as organizações se vêm forçadas começar ou acelerar a sua jornada de transformação digital.

O PONTO DE VIRAGEM DOS SERVIÇOS DIGITAIS

Ao longo do último ano, tornou-se evidente a importância de como as interfaces através das quais os clientes e empresas interagem são concebidas, e o impacto que isto tem na experiência do consumidor, tema abordado por Peter Neufeld, Head of Digital Customer Experience EMEIA da EY, na sua palestra "*The Invisible Interface*".

O responsável cita um estudo recentemente realizado na Europa, que revelou uma adoção acelerada dos serviços digitais no contexto pandémico – o que, alerta, não dispensa a necessidade de refinar estes serviços. Enquanto muitos clientes estão, de facto, a descobrir as vantagens dos serviços digitais e pretendem continuar a utilizá-los, muitos outros apenas o estão a fazer por necessidade, vendo ainda os canais tradicionais, com contacto pessoal, como mais convenientes.

Isto passa, refere o responsável, pela simplificação dos serviços, para que estes possam ser usados facilmente por qualquer utilizador, seja pela correta conceção de interfaces de *self-service* intuitivas ou também por facilitar a interação humana através de canais digitais.

Por outro lado, reforça, é necessário fazer a transição do design *costumer-centric* para um design *human-centric* e *purpose-centric*, focados nas necessidades dos consumidores, não no ato transacional. Por exemplo, um serviço digital de hipoteca, mais do que ajudar o cliente a obter

a mesma, deverá também ajudá-lo, de forma abrangente, a tomar todas as decisões necessárias para o processo de compra de casa.

"Para isto, é necessário criar um *marketplace* integrado, criando redes fora do *core business* das empresas e integrando diferentes setores para criar serviços convergentes que respondam às necessidades dos clientes de forma holística", conclui Neufeld.

DIGITAL TWINS

Como muitas outras tecnologias de digitalização de processos, os *digital twins* estão a ganhar nova relevância no contexto da pandemia, permitindo visibilidade, automação e otimização dos processos numa altura em que as restrições de mobilidade tornam a gestão de ativos desafiante na indústria ou em data centers. Steve Brown, Enterprise Architect na Altran, delineou os principais benefícios desta tecnologia e como está a ajudar as empresas a mitigar riscos, aumentar receitas e reduzir despesas.

"Indo mais além, é possível ter uma visão quase omnisciente sobre tudo o que acontece na organização, da visão global até ao mais pequeno parafuso, podendo assim ter uma visão de raio-X dentro dos ativos que de outra forma não seria possível no mundo real e físico", refere Brown. "Permite também a ter uma visão global do ciclo de vida; não estamos apenas a olhar para uma representação estática no tempo." Isto, por seu lado, permite prever a performance dos ativos no futuro com base nos padrões estabelecidos para, por exemplo, obter resultados de alterações à infraestrutura e determinar o melhor curso a seguir.

A Gartner, explica o responsável, divide os casos de uso de *digital twins* em dois patamares: o primeiro, com melhorias operacionais na ordem dos 10-50%, engloba projetos nos quais digital twins são usados para ganhar visibilidade sobre os sistemas, permitindo assim usar os dados para prever falhas e determinar a longevidade dos equipamentos, bem como criar planos de manutenção preditiva – o que de si traz benefícios, mas pode ser conseguido sem esta tecnologia, através de analítica avançada. No segundo patamar, por outro lado, os digital twins são usados para coreografar processos automáticos para aumentar a eficiência dos processos. "É aqui que os *digital twins* se destacam – não há nenhuma outra ferramenta que possa fazer isto de forma tão eficiente. E é aqui que começamos a ver melhorias operacionais na ordem dos 1.000%".

- Peter Neufeld -
Head of Digital Customer Experience EMEIA da EY

- Steve Brown -
Enterprise Architect na Altran

- Anthony Salcito -
VP Worldwide Education da Microsoft

easyVISTA™

Transform Support.
Delight Customers.

ITSM and Self-Service software that makes it easy to deliver support to employees and customers

EDUCAÇÃO E RESKILLING

Entre as muitas mudanças que trouxe a pandemia, a educação está entre as mais prementes. A necessidade de mover o ensino para um modelo totalmente diferente teve um efeito disruptivo – mas tem também o potencial de mudar o paradigma da educação, em paralelo com as mudanças a ocorrer no mundo.

"Ao expandir os limites do ensino para lá da sala de aula, é essencial ter as ferramentas para saber de que forma é que os estudantes estão a progredir, e extrair *insights* dos dados das plataformas de colaboração, utilizando estas novas fontes de informação para motivar os alunos e compreender de que forma é que os educadores os podem ajudar", refere Anthony Salcito, VP Worldwide Education da Microsoft.

Existe, no entanto, um caminho a percorrer, que Anthony Salcito divide em três etapas.

Numa fase inicial, resultado da necessidade de responder rapidamente às exigências da pandemia, houve um esforço por parte das escolas e governos para garantir as condições mínimas para o ensino remoto.

"Muito rapidamente, os educadores aperceberam-se de que isto não bastava, e é necessário um currículo mais focado e um modelo de ensino mais engaging e flexível na sua abordagem à transição tecnológica".

Esta é a segunda fase, na qual, uma vez estabelecidas as condições tecnológicas adequadas, os educadores começam a repensar o anterior modelo de ensino

A próxima fase será re-imaginar de que forma a educação tem de mudar no futuro, quando voltar a ser possível que os alunos regressem ao ensino presencial.

"Teremos de começar a pensar de que forma é que podemos reter todo este novo potencial que as novas formas de colaboração nos estão a trazer. De momento, o estamos a ver os educadores a usar ferramentas como o Microsoft Flipgrid para permitir aprendizagem assíncrona. Estas experiências têm sido extremamente interessantes em termos de fomentar a curiosidade e criatividade dos alunos, e não queremos perder isto ao voltar ao ensino tradicional. Obviamente, é bom que os alunos voltem para a sala de aula, mas não queremos minimizar esta possibilidade de acelerar a inovação no ensino".

Isto, por seu lado, prevê Anthony Salcito, deverá também ajudar a dar resposta às disrupções no mercado de trabalho causadas pela transformação digital, facilitando o *reskilling* de profissionais afetados pelas mesmas.

À medida que o ensino digital remoto se torna mais comum e ubíquo, surge uma enorme oportunidade para facilitar e flexibilizar o *reskilling*. Ao estabelecer as ferramentas e processos necessários, torna-se muito mais fácil para pessoa – seja por ambição própria ou como colaborador de uma empresa – adquirir as habilitações para acompanhar as mudanças no mercado de trabalho de forma anteriormente dependente de um curso formal, presencial e difícil de integrar na vida da maioria das pessoas profissionalmente ativas. ■

A new identity. For a new reality. The same resolution. There is no evolution without change. We changed. We evolved. We became more digital. More innovative. More sustainable. But not everything changed. Our Business knowledge. Our Customer focus. Our Proven experience. Our Recognized Quality. And the mission of simplifying our customers' business. Stayed the same. Brighten is here to make a statement. It’s got color and a strong personality. It’s got a purpose and a roadmap. To be brighten is to have brighten minds and brighten ideas. To be brighten is to design and deliver brighten solutions. To be brighten is to develop brighten partnerships. brighten is the future and the future is now. SIMPLIFY. YOUR. BUSINESS. TOGETHER.

procensus oak peak is now

brighten

simplify your business.
together.

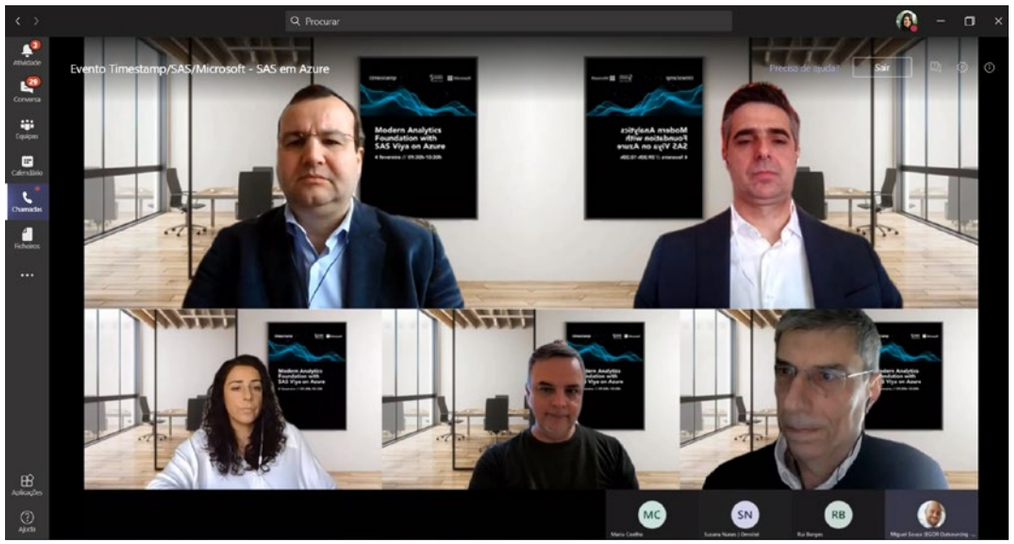
timestamp

MODERN ANALYTICS FOUNDATION COM O SAS VIYA SOBRE AZURE

O lançamento do SAS Viya sobre Azure em modelo cloud veio reforçar as vantagens da parceria SAS e Microsoft que utiliza a analytics para responder a necessidades estratégicas do negócio.

"**O SAS E A MICROSOFT** fazem parte de um grupo estrito de parcerias estratégicas da Timestamp e são tecnologias de eleição para as áreas de *analytics* e de cloud", afirma Luís Leão, Administrador da Timestamp.

O lançamento da plataforma SAS Viya sobre Azure em modelo cloud veio reforçar o anúncio da parceria SAS e Microsoft. Uma plataforma que oferece um conjunto de benefícios significativos para uma estratégia de modernização e transformação digital e que disponibiliza aquilo que são as melhores ferramentas de *analytics* na plataforma cloud líder de mercado, numa solução robusta e *cost-effective*.



VISÃO GLOBAL DA SOLUÇÃO

Para Nuno Almeida, Business Development Director da Timestamp é necessário que as organizações sejam capazes de detetar antecipadamente padrões e eventos que vão ocorrendo nas suas atividades e negócios para que mais facilmente se adaptem a novas oportunidades e até a novas ameaças. É ainda fundamental que tenham a capacidade de agir e de ganhar valor, mostrando diferenciação na informação e nos *insights* que recebem.

Para a obtenção destes *insights* em tempo útil, as organizações necessitam de oferecer uma resposta coesa e completa para os desafios que enfrentam na democratização do poder analítico

que os volumes de informação e de dados que possuem encerram em si.

A plataforma analítica do SAS Viya foi idealizada para simplificar os fluxos de tratamento de dados e em particular, a produção de análises avançadas e de *insights*.

De forma abreviada, os dois processos são conhecidos por Data Ops e Model Ops e são no fundo os dois processos pilares da plataforma de data e *analytics*.

Com a fundação desta oferta analítica do SAS, numa plataforma de cloud pública como é o caso da Microsoft Azure, o mercado passa a ter acesso ao melhor que estes dois conjuntos de ofertas trazem.

VANTAGENS

Em primeiro lugar, existe uma facilidade na democratização e produção de análises que de outra forma estariam encerradas em ferramentas complexas com a capacidade de poderem ser utilizadas de forma intuitiva, mas também sobre enormes volumes de dados de informação.

Por outro lado, existe a integração dos dois pilares da plataforma de *data* e *analytics*. Com a cloud em Microsoft Azure, as organizações passam a ter uma gestão simplificada dos ambientes, tornando-os facilmente implementáveis na sua organização, e com uma capacidade de elasticidade e de crescer consoante as necessidades. Também os custos associados passam a ser adaptáveis à atividade de cada organização, o que permite obter maior agilidade na produção e divulgação de *insights* e um retorno dos investimentos.

"Tudo isto, deve-se ao facto do SAS Viya ser fundado sobre princípios fortes da governação de dados, sendo que os processos que atuam são devidamente governados e auditáveis. Isto é aquilo que se procura numa moderna fundação em *analytics*: que não cumpra só a agilidade de produção de *insights*, mas que o faça de uma forma governada".

O CAMINHO PARA UMA MODERNIZAÇÃO TECNOLÓGICA

A Timestamp concentra todas as valências necessárias para apoiar as organizações em processos de modernização, nomeadamente com soluções SAS e Microsoft Azure.

"Em Portugal fomos o primeiro parceiro SAS a migrar uma solução SAS para SAS Viya e o primeiro parceiro português da Microsoft a disponibilizar uma solução em Azure", refere Nuno Almeida.

A experiência e conhecimento da plataforma SAS Viya e cloud Azure permitem aconselhar com segurança os clientes na infraestrutura de cloud ideal para as suas soluções e processos baseados em SAS, alcançando os objetivos que os clientes procuram neste tipo de processo de modernização.

Tipicamente, este apoio abrange a fase de *assessment*, o desenho de arquitetura inicial, a implementação das aplicações e o processamento dos dados até à própria gestão dos ambientes que estão em produção.

Tudo isto, passando pela implementação de políticas de gestão que hoje são primordiais na disponibilização de aplicações de dados (principalmente as que trabalham com dados pessoais e de clientes) e na escolha dos melhores serviços para fazer esse mesmo tratamento de dados.

"Esta viagem necessária é feita em conjunto com o cliente, juntando aquilo que são as suas expetativas e objetivos com a nossa experiência de como implementar cada caso da melhor forma possível ", garante Nuno Almeida. ■

Quando se trata de Saúde, ninguém quer ficar à espera.

Como gerir as expectativas dos clientes quando o primeiro contacto com o serviço é uma sala de espera? A gestão de atendimento da plataforma **segg** permite a monitorização e recolha de dados para suportar um cuidadoso planeamento dos agendamentos e a redução dos tempos de espera. O **segg** integra a gestão de atendimento e o digital signage numa solução universal, centralizada e escalável de eficácia testada e comprovada. Fale agora com um dos nossos especialistas e não deixe mais ninguém à espera .

segg

the store digital experience by softfinança

+351 214 127 830 • www.segg.pt

O FUTURO DOS CUIDADOS DE SAÚDE É DIGITAL

A pandemia pode ser a alavanca estratégica para a transformação do sistema de saúde, mas ainda falta alinhar modelos de financiamento, integrar soluções tecnológicas e partilhar informação entre prestadores para que a qualidade do serviço ao utente seja efetiva. Tratamento e gestão segura dos dados são dois grandes desafios.

FÁTIMA FERRÃO

A COVID-19 veio acelerar, em poucos meses, a transformação digital no setor da saúde, com impacto direto sobre todo o ecossistema, desde as unidades hospitalares às farmácias. No entanto, como defendem vários especialistas contactados pela IT Insight, esta é uma oportunidade que não deve ser desperdiçada e uma (r)evolução que não pode parar no período pós-pandemia. "Esta onda de aceleração tecnológica, que por norma demoraria anos, deve continuar no momento pós-pandémico com uma arquitetura de referência que defina a resiliência das infraestruturas, a interoperabilidade, a recolha de dados de forma segura e anonimizada e a usabilidade das soluções por parte dos utentes, profissionais de saúde e gestores", defende Paulo Freitas, diretor do serviço de medicina intensiva no Hospital Fernando Fonseca e presidente do Conselho de Administração da Fundação Instituto Marquês de Valle-Flôr. Para o médico intensivista, caberá aos prestadores de serviços tecnológicos na área da saúde e às instituições de saúde trabalhar em conjunto para que esta onda não "morra na praia" até porque, acrescenta José Mendes Ribeiro, membro do Conselho Estratégico do Centro Académico Clínico de Coimbra CHUC/UC, a transformação digital na saúde criará transparência, melhorará o acesso e a qualidade da prestação. "Em termos práticos, podemos acabar com as listas de espera, melhorar a qualidade da gestão e entregar melhores resultados aos cidadãos".

Maria João Campos, diretora do serviço de Tecnologias da Informação e Comunicação no Hospital de S. João, no Porto, recorda que a pandemia obrigou a desafiar a burocracia e algumas barreiras institucionalizadas e a evoluir de uma forma muito rápida, desenvolvendo novos meios para a continuidade de prestação dos cuidados de saúde. E a este nível, destaca, "o trabalho de equipa multidisciplinar foi um aspeto absolutamente essencial". No entanto, para o pós-pandemia, a responsável acredita que "será fundamental trazer a confiança à po-

"a confluência da revolução digital e da revolução genómica criou um espaço de oportunidade para a inovação em saúde sem precedentes"

- David Vieira -

- Paulo Freitas -

pulação para que procure os cuidados de saúde, priorizar os casos mais urgentes, e reduzir a burocracia institucionalizada no SNS".

OPORTUNIDADE PARA INOVAR

A saúde digital, que engloba diferentes áreas como a telemedicina, a telesaúde, a medicina personalizada ou, até, os *wearables*, tem evoluído de forma considerável nos últimos 20 anos. Mais recentemente, e na opinião de Guilherme Victorino, professor auxiliar convidado na NOVA IMS e coordenador do Health & Analytics Lab, "a confluência da revolução digital e da revolução genómica criou um espaço de oportunidade para a inovação em saúde sem precedentes".

Adicionalmente, o contexto do último ano veio demonstrar que muitos dos constrangimentos ao atendimento não presencial e à hospitalização domiciliária não eram reais. Desde março passado, grande parte das consultas passaram a ser realizadas de forma remota, uma tendência que, para Paulo Freitas, pode melhorar o acesso a cuidados de saúde por parte dos cidadãos localizados em geografias mais remotas e com menores condições de acessibilidade e de mobilidade, contribuindo também para o estabelecimento de uma relação de maior proximidade com o doente. "A teleconsulta poupa deslocações ao hospital, que causam desconforto, evitando custos desnecessários e, em caso de pandemia, reduzindo o risco de contágio", defende. "Esta evolução vai obrigar a que as soluções hospitalares se orientem também para a prestação de cuidados de saúde fora das unidades, deixando de estar focadas na prestação presencial", reforça Ricardo Constantino, partner & head of health and public setor da Everis Portugal. Para o consultor, a necessidade de responder de uma forma ágil a

"É PRECISO GARANTIR QUE A LIDERANÇA, PROCESSOS E PESSOAS ESTÃO PREPARADAS PARA LIDAR COM ESTAS TECNOLOGIAS, DE FORMA A DELAS TIRAR PARTIDO E A POTENCIAR O INVESTIMENTO"

estas necessidades irá obrigar a transferir para a cloud uma parte significativa das soluções, e este será um dos desafios nos próximos anos. "Do ponto de vista tecnológico, a utilização da cloud e de machine learning é uma tendência a nível mundial, mas em Portugal têm sido feitas apenas algumas experiências". No entanto, e tendo em conta a flexibilidade que é necessária para a transformação digital, "esta será uma tendência em Portugal nos próximos anos", acredita Ricardo Constantino. No fundo, reforça Guilherme Victorino, "com as alterações, fruto da crise pandémica, há um novo olhar para o potencial transformador destas tecnologias face aos desafios complexos que enfrentamos".

ESTRATÉGIA E LIDERANÇA, PRECISAM-SE!

Mas para que a saúde digital seja uma realidade, não basta investir nos mais complexos e avançados sistemas de informação. É verdade que tecnologias como Inteligência Artificial (IA), machine learning, IoT, ou 5G, vão trazer grandes benefícios. No entanto, como refere Carina Adriano, diretora de sistemas e de tecnologias de informação do Infarmed, "é preciso garantir que a liderança, processos e pessoas estão preparadas para lidar com estas tecnologias, de forma a delas tirar partido e a potenciar o investimento". Uma opinião partilhada por Paulo Freitas que acrescenta que a estratégia para a saúde, nomeadamente para um melhor funcionamento do Serviço Nacional de Saúde (SNS), "terá de sofrer uma reviravolta para, entre outras coisas, permitir a integração e disponibilização da informação sobre cada doente da forma mais imediata possível". Segundo o intensivista, "qualquer tecnologia inovadora deveria permitir que caminhássemos para uma visão centrada nas pessoas que permita a cada um de nós, enquanto cidadão, ser acompanhado ao longo da sua jornada de saúde pela sua informação clínica, ao invés desta estar compartimentada em silos por cada unidade de saúde, especialidade, ou nível de cuidados". Maria João Campos defende igualmente a necessidade de colocar o utente no centro da prestação, considerando que é "uma tendência incontornável. Para a responsável de IT do Hospital de S. João, "os aceleradores de inovação como as aplicações, a IA ou a IoT permitem-nos abordar novos desafios de uma forma disruptiva que promovem uma verdadeira transição digital". No maior hospital da região norte, a tecnologia faz há muito parte da atividade diária e tornou-se numa *commodity*, desde a chegada do utente ao hospital até à realização de exame, consulta ou cirurgia. "Temos atualizado todas as infraestruturas tecnológicas e investido muito em informatização e automação de processos para os tornar mais simples e eficientes", salienta.

"Existe um grande bloqueio de partilhar informação entre o setor público e o privado, e isso não beneficia os cuidados do utente"

Em suma, e como resume Guilherme Victorino, interoperabilidade, centralidade no utente e facilidade de utilização são os fatores essenciais para que o sistema de saúde funcione sem entropia. "Temos de partir de um sistema de saúde com um modelo centrado no prestador de cuidados, onde os doentes são recetores passivos, para ecossistemas de saúde que capacitam as pessoas, aproveitando a infraestrutura e tecnologia digital para apoiar e permitir uma maior participação na gestão da sua saúde e promoção do bem-estar, apoiados por equipas de cuidados de saúde como parceiros".

O DESAFIO DA INTEGRAÇÃO E DA PARTILHA

A falta de comunicação entre sistemas de informação continua, no entanto, a ser uma das grandes lacunas, identificadas pelos especialistas contactados pela IT Insight, no setor da saúde. Uma parte significativa dos hospitais em Portugal tem soluções hospitalares por unidade, "com falhas ao nível da qualidade da informação e capacidades limitadas de integração com as soluções de outras unidades", afirma Ricardo Constantino. Na opinião do consultor, esta é uma das razões pela qual muitas das iniciativas de transformação digital não permitem atingir os resultados pretendidos. "Existe um grande bloqueio de partilhar informação entre o setor público e o privado, e isso não beneficia os cuidados do utente", reforça Pedro Salgado, health solutions manager na F3M.

- José Mendes Ribeiro -

- Maria João Campos -

- Guilherme Victorino -

"Temos o fundamental que são os ingredientes. O que nos falta em muitas circunstâncias é clareza nos objetivos, no planeamento e na liderança"

Na opinião de André Coutinho e Jorge Carvalho, Managing Partners da Brighten, este bloqueio acontece porque ainda existe um parque de soluções neste setor assente em tecnologias ultrapassadas, a par com uma enorme falta de uniformização de processos, e políticas que se traduzem em ineficiências. Além destas, os Managing Partners destacam ainda alguma resistência à transformação digital que ainda existe, sobretudo no setor público, ou a falta de perceção sobre a vertente logística que pode funcionar como catalisadora de eficiência e simplificação, como razões que estão a travar a inovação na saúde. "A capacidade e agilidade de integração de sistemas numa indústria ainda pouco madura tecnologicamente é, e será, nos próximos anos um dos principais desafios no setor da saúde", acrescenta David Vieira, diretor de sistemas de informação no grupo Luz Saúde. Paralelamente, diz Ricardo Constantino, "existe uma necessidade de melhorar a qualidade de informação clínica e administrativa, de forma a criar as bases para a transformação digital necessária".

Já a solução, aponta José Mendes Ribeiro, passará pela criação de uma infraestrutura tecnológica e de comunicações que permita o acesso e a partilha da informação entre todos os operadores do sistema de saúde, em benefício do cidadão. "Temos o fundamental que são os ingredientes. O que nos falta em muitas circunstâncias é clareza nos objetivos, no planeamento e na liderança", reforça.

Recuando umas décadas, Paulo Freitas recorda que o primeiro movimento da informatização visava eliminar o papel nos hospitais. "A informação passou a ser registada de forma eletrónica, mimetizando os processos em papel". Contudo, acrescenta, "cada área do hospital apostou no desenho das suas soluções para servir os seus objetivos, o que levou à multiplicação de inúmeras aplicações, com diversos login e passwords. O resultado foi a criação de torres de comunicação que não comunicavam". Mais tarde, explica o intensivista, acumularam-se erros

"A TECNOLOGIA TEM DE SERVIR COMO UM APOIO, TANTO DO PONTO DE VISTA ADMINISTRATIVO COMO CLÍNICO, MAS AINDA TEMOS UM LONGO CAMINHO PELA FRENTE", CONCLUI O RESPONSÁVEL DO HOSPITAL FERNANDO FONSECA

que levaram à aposta em soluções diferentes em cada instituição que não eram consideradas *user-friendly* para os profissionais de saúde, que sentiam muita dificuldade no acesso a informação de valor. Na prática, o hospital sem papel não se traduziu num aumento de eficiência. Ainda hoje, diz Paulo Freitas, "os profissionais de saúde são subjugados por sistemas de informação, onde perdem seguramente mais de 50% do seu tempo. Lutam por um computador, e acabam por escrever em papéis o que mais tarde transcrevem para um sistema de informação". E este é, precisamente, um dos desafios para o futuro, criando condições para que os profissionais de saúde se possam dedicar aos casos clínicos mais complexos e exigentes. "A tecnologia tem de servir como um apoio, tanto do ponto de vista administrativo como clínico, mas ainda temos um longo caminho pela frente", conclui o responsável do Hospital Fernando Fonseca. Por agora, confirma Guilherme Victorino, há uma grande frustração em torno do digital. "Esta frustração estende-se a profissionais de saúde, onde os processos e a carga burocrática ainda não diminuíram significativamente, e aos doentes onde o acesso e a qualidade dos cuidados ainda apresentam oscilações relevantes". Para o professor da NOVA IMS, o digital continua a ser frequentemente confundido com a simples implementação de sistemas tecnológicos, "em vez de estar relacionado com tornar a experiência de utilização dessas tecnologias mais humana e relevante para cada utilizador final".

PIONEIRISMO VERSUS FALTA DE INVESTIMENTO

Apesar das ineficiências que ainda se verificam no SNS e no ecossistema de cuidados de saúde em Portugal, o país encontra-se "num bom patamar de desenvolvimento tecnológico", afirma Pedro Salgado da F3M que destaca alguns exemplos pioneiros, que têm servido de modelo a outros países europeus, como a receita eletrónica ou os meios complementares

- Ricardo Constantino -

- Carina Adriano -

de diagnóstico eletrónicos. Na área da imagem, complementa Paulo Freitas, as ferramentas de tratamento da Imagiologia e o ECG eletrónico com análise diagnóstica que, entre outros benefícios, permitem comparar a evolução entre exames "representam um impacto positivo muito significativo no dia-a-dia dos profissionais de saúde, nomeadamente, no que respeita à tomada de decisão clínica baseada numa evidência do histórico do respetivo doente". A Linha Saúde 24, que ganhou ainda mais visibilidade durante a pandemia, é outro exemplo positivo referido pelo intensivista do Hospital Fernando Fonseca. "Auxilia o cidadão no diagnóstico bem como permite identificar os casos mais graves que devem seguir para as urgências hospitalares, facilitando o trabalho dos profissionais de saúde e libertando a pressão nos serviços hospitalares tipicamente muito dispendiosos".

Já ao nível do planeamento de cuidados de saúde e decisores políticos, Paulo Freitas destaca o lançamento da ADAPTT Surge Planning Support Tool por parte da Associação Portuguesa de Administradores Hospitalares (APAH), em colaboração com uma multinacional tecnológica portuguesa e a Organização Mundial de Saúde (OMS). A ADAPTT é uma ferramenta gráfica destinada a ser utilizada por especialistas seniores em planeamento. É flexível, permitindo que os utilizadores dos vários países insiram os seus dados epidemiológicos, variem os cenários de mitigação (ao usar o modelo epidemiológico ilustrativo da ferramenta), e adaptem a ferramenta a diferentes *attack rates*. A ADAPTT possibilita a introdução das práticas e atividades hospitalares, assim como a capacidade de diferentes tipologias de camas e de recursos humanos.

No entanto, a adoção de tecnologia inovadora implica um maior alinhamento dos modelos de financiamento do sistema, lembra Guilherme Victorino. "Para acontecer seria necessário centrar o modelo de financiamento no conceito de valor em saúde e não apenas na produção". Na opinião do professor, a implementação de soluções baseadas em saúde digital deve ser acompa-

"faltam meios e investimento em IT na saúde, e o Plano de Recuperação e Resiliência é demasiado centralizador na proposta de investimento, o que deixará de fora muitas das necessidades dos hospitais"

nhada de incentivos financeiros para os prestadores de cuidados de saúde, a fim de eliminar as barreiras financeiras da adoção. "Os sistemas de financiamento devem adaptar-se para facilitar a adoção de soluções digitais em saúde", aponta.

Durante a pandemia, "fizemos muito com muito pouco", diz Maria João Campos. No Hospital de S. João, exemplifica, algum do investimento já estava planeado, mas outro foi alavancado com a pandemia para permitir maior flexibilidade e disponibilização de recursos. Ainda assim, reforça, "faltam meios e investimento em IT na saúde, e o Plano de Recuperação e Resiliência é demasiado centralizador na proposta de investimento, o que deixará de fora muitas das necessidades dos hospitais".

- Pedro Salgado -

TRANSFORMAR DADOS EM INFORMAÇÃO DE QUALIDADE

Nos sistemas de saúde, tal como acontece noutros setores, a multiplicação crescente dos dados está a criar um conjunto de novos desafios. Há mesmo quem diga que os dados são o novo petróleo, mas de nada serve ter sistemas inundados com terabytes de dados, se a informação que deles se extrai não for de qualidade. Para Ricardo Constantino, existe um primeiro desafio estrutural relacionado com a melhoria da qualidade dos dados. "Grande parte das tendências na área da saúde precisam de muitos dados e dados com qualidade. Existe também cada vez mais informação do lado do cliente que é preciso ter em conta e trazer para dentro das soluções. Esta necessidade coloca desafios importantes na verificação da sua qualidade e nos modelos de governação destes dados". Para fazê-lo, é fundamental, na opinião de Pedro Salgado, recorrer a ferramentas de IA, IoT ou de Business Intelligence – que permitem fazer a recolha de informação dos utentes -, com vista a "aproveitar o conteúdo e a dimensão dos atos que temos nas nossas plataformas para ajudar, de alguma forma, o pessoal de saúde a tomar decisões mais rápidas".

- Jorge Carvalho -

MUITAS DAS VEZES TEMOS VISTO NO SETOR DA SAÚDE, UM EXCESSO DE FACILITISMO NA FORMA COMO SE PRETENDE ACELERAR ESTA TRANSFORMAÇÃO, DESCURANDO ASPETOS ESSENCIAIS COMO A SEGURANÇA

Por outro lado, outro grande desafio ao nível dos dados, está relacionado com a sua segurança. A melhoria da segurança dos dados tem sido, para Nuno Bajanca, technical architect consulting - Data Center & Multi Cloud na Warpcom, uma grande preocupação no setor da saúde nos últimos anos. Desde 2018, com a introdução do Regime Geral da Proteção de Dados (RGPD), as instituições de saúde foram obrigadas a reforçar as normas de segurança, a alterar um conjunto de procedimentos que permitam garantir a total confidencialidade aos utentes, recordando o caso de um centro hospitalar multado em 400 mil euros por incumprimento destas práticas. "As empresas do setor de saúde precisam de guardar processos com dados pessoais e clínicos dos seus doentes, cujo acesso rápido e por um grande número de pessoas pode ser crucial para salvar vidas", afirma. No entanto, acrescenta, é preciso garantir que todos os procedimentos são cumpridos, especialmente porque os profissionais de saúde não são utilizadores especializados em sistemas sendo, por isso, pontos frágeis no sistema. "Nunca devemos esquecer a individualidade de cada pessoa, e a segurança dos seus dados. Muitas das vezes temos visto no setor da saúde, um excesso de facilitismo na forma como se pretende acelerar esta transformação, descurando aspetos essenciais como a segurança", salienta David Vieira. José Mendes Ribeiro reforça esta ideia: "a premissa fundamental é respeitar que os dados de saúde são pertença de cada cidadão e devem ser tratados e protegidos com toda a segurança". Para o membro do Conselho Estratégico do Centro Académico Clínico de Coimbra, "esses dados são mais úteis para cada um de nós se ficarem disponíveis num Registo de Saúde Eletrónico (RSE) universal a que o cidadão possa aceder e dar consentimento a que sejam usados de forma útil pelos diferentes parceiros envolvidos na cadeia de valor da saúde".

Mas a questão da confidencialidade dos dados traz também grandes desafios para as aplicações, que ajudam a garantir que esses dados não são partilhados com qualquer tipo de utilizador. O alerta chega pelas palavras de Pedro Salgado que, exemplifica: "nos processos manuais era muito fácil um processo clínico andar de mão em mão e era muito mais difícil garantir esse tipo de segurança". Com o recurso às ferramentas tecnológicas, esta questão tem de manter-se salvaguardada. "Há uma série de desafios gigantes a nível da estrutura tecnológica para suportar todo este volume de dados, mas deve ser o Estado a promover um alinhamento das várias empresas de software para se conseguir fazer este tipo de partilha de informação, por forma a melhorar a forma como prestamos cuidados atualmente", reforça o responsável da F3M.

"a introdução do 5G ao serviço da saúde a par com a capacidade da cloud são componentes decisivas neste grande desafio".

- Nuno Bajanca -

- António Madureira -

FUTURO DA SAÚDE PASSA PELO 5G

Os desafios de alcançar uma medicina mais personalizada e de garantir o acesso aos cuidados de saúde a milhões de pessoas em todo o mundo em geografias mais distantes são, na opinião de José Mendes Ribeiro, concretizáveis com a introdução da tecnologia 5G ao serviço da saúde. "A par com a capacidade da cloud são componentes decisivas neste grande desafio". A capacidade de monitorizar parâmetros clínicos que o IoT e a tecnologia 5G estão a exponenciar, assim como a aplicação de algoritmos (IA) a partir da análise de grandes conjuntos de dados (big data) vão ajudar a uma medicina de precisão e ao desenvolvimento de ferramentas preditivas que permitirão melhorar consideravelmente muitas patologias existentes. "Isso é tão importante para a qualidade de vida das pessoas como para a sustentabilidade dos sistemas de saúde que terão de gerir uma população mais envelhecida e mais exigente", reforça.

Na opinião de David Vieira, este fenómeno na saúde representará, por um lado, "a oportunidade de receber em tempo real os dados dos dispositivos que carregamos connosco ou que interagimos diariamente, mas também de todos os dispositivos médicos que hoje em dia existem nos hospitais e que não comunicam com nada".

Guilherme Victorino tem uma opinião semelhante. "As redes 5G têm o potencial de contribuir para a transformação digital, fornecendo níveis essenciais de conectividade para permitir um novo ecossistema de saúde, que possa satisfazer as necessidades dos doentes e dos prestadores de cuidados de saúde de forma eficiente, rentável e a uma escala substancial". No entanto, acredita o professor, para realizar todo o potencial das redes 5G em áreas como a telesaúde, a cirurgia robótica, o seguimento dos doentes via *wearables* ou a implementação de modelos preditivos para decisão clínica, a segurança e privacidade dos dados são

primordiais. "Ainda há, por isso, desafios éticos, sociais e legais que devem ser endereçados e que devem caminhar a par com a tecnologia".

Ainda no que se refere à ética na utilização de tecnologias exponenciais, António Madureira, diretor do serviço de radiologia no Hospital de S. João, deixa um alerta para a importância da formação de recursos em ferramentas CAD (computed aided-diagnosis), entre as quais a IA será o verdadeiro 'game-changer'. "Será necessário um cuidadoso processo de validação e seguimento numa fase inicial pois como a mente humana não consegue perceber na sua totalidade os algoritmos utilizados, se as 'respostas' forem aceites de modo acrítico podem ser cometidos erros graves".

Para o responsável do Hospital de S. João, estas tecnologias são apenas a porta para um novo mundo que desconhecemos. "Existirão muitas aplicações e ferramentas com as quais nem sequer sonhamos, e que nos próximos dez anos se vão tornar de uso corrente e modificar totalmente a medicina (e a radiologia), tal qual as conhecemos", acredita.

Para já, e de volta ao presente, resta tirar as lições possíveis da pandemia que veio mudar o mundo em geral, e o setor da saúde, em particular. "Uma delas é de que todos somos poucos nestes momentos e por isso se espera que as políticas públicas sejam um fator de agregação de conhecimento, estimulando todos os setores e todos os atores para cooperarem na procura das melhores soluções", afirma José Mendes Ribeiro que espera que, com este objetivo, sejam mobilizadas universidades, centros de inovação, institutos públicos, farmacêuticas, operadores do setor público, privado e social, tecnológicas, empresas de comunicações, investigadores "e, obviamente, os atores políticos, pois cabe-lhes galvanizar os portugueses para esta iniciativa. Seria um excelente legado do Portugal do século XXI", conclui. ■

"EXISTIRÃO MUITAS APLICAÇÕES E FERRAMENTAS COM AS QUAIS NEM SEQUER SONHAMOS, E QUE NOS PRÓXIMOS DEZ ANOS SE VÃO TORNAR DE USO CORRENTE E MODIFICAR TOTALMENTE A MEDICINA (E A RADIOLOGIA), TAL QUAL AS CONHECEMOS"

3 DESAFIOS PARA A TRANSFORMAÇÃO DIGITAL NA SAÚDE

Guilherme Victorino, professor auxiliar convidado na NOVA IMS e coordenador do Health & Analytics Lab, resume os grandes desafios para a transformação digital na saúde em três grandes vetores.

(1) MODELOS DE GOVERNAÇÃO, LIDERANÇA E COLABORAÇÃO. A este nível, os temas críticos estão relacionados com a capacidade de coordenação a nível nacional, alinhando os objetivos de saúde com o apoio político; a promoção, sensibilização e envolvimento das diferentes partes interessadas para o digital; o financiamento alinhado com as prioridades (governo, privado, público, social); a disponibilização de conhecimentos e competências em *eHealth* através de formação e cooperação técnica; a regulamentação legal e aplicada para a privacidade e confiança; e, finalmente, a capacidade de colaboração e de estabelecer parcerias estratégicas;

(2) MODELOS DE DADOS, INFRAESTRUTURAS E INTEROPERABILIDADE. É fundamental atuar sobre os Data Standards; melhorar a infraestrutura de dados; e reforçar a capacidade de análise preditiva nomeadamente através de recursos humanos e tecnológicos;

(3) MODELOS CENTRADOS NOS DOENTES. É fundamental incluir os doentes como parceiros e informar sobre o potencial das tecnologias de saúde, com ênfase na forma como o acesso e a utilização dessas tecnologias devem ser considerados para apoiar os grupos mais vulneráveis; por outro lado, as tecnologias digitais podem fornecer soluções tais como a redução da carga de trabalho relacionada com o tempo gasto em temas administrativos por clínicos, o que lhes permite mais tempo com o doente, apoio ao diagnóstico, melhoria da relação médico-paciente, e fornecimento de meios mais equitativos de prestação de cuidados de saúde.

Alcatel·Lucent Enterprise
inCentea TECNOLOGIA DE GESTÃO

A ÁREA DA SAÚDE NÃO PODE FACILITAR

Cada vez é mais importante priorizar a Cibersegurança, garantindo a operacionalidade e segurança das infraestruturas tecnológicas e dos sistemas de informação da Saúde.

COM OS OLHOS POSTOS em si, os serviços de saúde não podem parar e não são poupados pelos cibercriminosos. Nunca se falou tanto em segurança, mas agora, com um grande número de pessoas em casa e com acessos a dados de qualquer lugar, as portas abertas para uso indevido intensificam-se exponencialmente. Se é verdade que se tem concretizado uma revolução digital, a mesma traz consigo por inerência uma disponibilidade de dispositivos que podem ser atacados e que ficam vulneráveis.

É necessário compreender o valor para o negócio da falta de segurança e não atuar apenas reativamente. Se não quisermos acreditar ou não tivermos consciência dos perigos que corremos com as falhas na segurança digital, podemos deitar tudo a perder.

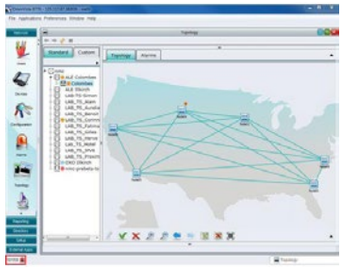
Com o fim das zonas de perímetro controladas, agora é obrigatório mudar comportamentos e desconfiar de tudo. Proteger é a prioridade, mas obriga a um maior controlo e a uma noção de comportamentos para antecipar problemas e ter resultados mais eficazes. Aliado a isto tudo não podemos esquecer a formação das pessoas que precisam de entender que esta mudança de processos é crucial para as organizações. Neste novo mundo transformado digitalmente, tudo é mais rápido e as ferramentas de segurança têm que ter resposta à altura. Os departamentos de IT têm que ser ágeis e eficazes, mas estão numa fase em que não sobra tempo para gerir processos, nem fazer um planeamento rigoroso. O que hoje percebemos é que um planeamento estratégico das infraestruturas, focado na continuidade de negócio, é um objetivo prioritário para qualquer negócio e que se traduz em resultados de produtividade e eficiência. É necessário redefinir processos, reajustar e acrescentar camadas de segurança. Acreditamos que este trabalho tem que ser contínuo e em constante mudança, o que nos obriga a ser mais adaptáveis. Se tivermos uns bons alicerces, ou seja, uma rede estruturada e segmentada, já será um bom princípio.

A rede tem que ser segmentada, protegida e temos mesmo que alcançar níveis maiores de complexidade se queremos olhar de outra forma a segurança.

Alcatel·Lucent Enterprise

Sabemos que uma rede segura, seja de dados ou voz, reduz as vulnerabilidades e que a confiança se ganha com o tempo e por isso contamos com a Alcatel-Lucent Enterprise que nos aporta a experiência de largos anos na saúde e a tranquilidade de ter soluções robustas, flexíveis e adaptadas para trabalhar on-premise, em modo híbrido e na cloud.

Conseguimos excelente capacidade de expansão e políticas de segurança prontas a responder às necessidades atuais e adaptáveis a situações de crise. Equipamentos e software completamente adaptados por forma a assegurar as comunicações de voz, dados, imagem e aplicações com a integridade das redes, dos dispositivos baseados em perfis de utilizadores e com monitorização permanente, quer das aplicações quer da vertente analítica.



No âmbito dos serviços de voz, uma componente crítica na área da saúde, é crucial ter os contratos de manutenção e suporte ativos de forma a possibilitar os vários *upgrades* de segurança e novas funcionalidades, como por exemplo a encriptação de voz. Também aqui existe uma plataforma de gestão centralizada de configuração e monitorização, o Omnivista 8770, por forma a possibilitar a mobilidade, quer dos colaboradores, quer do IT que faz a sua gestão. Estes sistemas têm também a possibilidade de integração com aplicações hospitalares de forma a facilitar a comunicação com o paciente, *staff* e todo o ecossistema de soluções hospitalares.

A inCentea alia a sua vasta experiência em comunicações, colaboração, *networking*, e cibersegurança nas soluções da Alcatel-Lucent Enterprise para conseguir otimizar a realidade de cada organização. A versatilidade das suas equipas, ajuda desde a análise de procedimentos à sua redefinição.

Muitas vezes um olhar externo ajuda a detetar falhas, perceber fragilidades e ajuda a construir uma solução melhor. Ajustamos cada solução para que seja parametrizada de acordo com a utilização real de cada organização e com ferramentas para monitorizar e afinar sempre que seja necessário. Não podemos mesmo deixar que este ciclo de ajustar / monitorizar se quebre e sabemos que a segurança não tem fins de semana, noites ou férias.

Sem dúvida que a tecnologia está hoje a ajudar a criar um mundo novo e que as vulnerabilidades dos sistemas nunca vão terminar. Resta-nos estar atentos, fazer a gestão de risco e monitorizar sempre. Tudo isto com ferramentas e soluções robustas da Alcatel-Lucent Enterprise. ■

INFO
Incentea.com
info.pt@incentea.com
808 222 808

Extreme networks

POR RUI NUNES
Sales Manager Portugal e Angola,
Extreme Networks

A **REDE**, ELEMENTO CRÍTICO PARA A TRANSFORMAÇÃO DIGITAL DO SETOR DA SAÚDE

O setor da saúde começou a sua transformação digital há já algum tempo e tem sido sempre um setor pioneiro na incorporação de novas tecnologias nas suas operações, em todas as áreas.

A TECNOLOGIA está a produzir uma mudança radical na forma como se desenvolve a atividade em hospitais e centros de saúde, com impacto em todos os aspetos da organização, da assistência ao utilizador / paciente ao trabalho dos médicos e do pessoal de saúde, passando para a gestão de todas as operações da organização – administração, serviços gerais, gestão de pessoal, infraestruturas, etc.

Por um lado, houve uma explosão no número de dispositivos médicos ligados à rede, como por exemplo dispositivos de transfusão, analisadores de gases no sangue, sistemas de telemetria, máquinas portáteis de raios-X, unidades de ultrassom, muitos outros e novos dispositivos que também eles vão fazer parte e depender da rede.

Por outro lado, novas tecnologias têm sido incorporadas com o objetivo de melhorar a experiência de uso do paciente, facilitando a comunicação com o pessoal de saúde e familiares e permitindo-lhes usufruir de um ambiente mais confortável durante a sua permanência no hospital ou facilitando as interações com o seu centro de saúde.

Em terceiro lugar, foram adotadas novas tecnologias que melhoram os processos de gestão da própria organização de saúde e que proporcionam eficiência, agilidade e economia de custos, como prontuários médicos digitais – que evitam a duplicação de exames e são acessíveis de forma ubíqua – ou sistemas de telecon-

- Rui Nunes -
Sales Manager Portugal e Angola, Extreme Networks

sulta, que permitem ao paciente maior agilidade na utilização dos serviços e ao sistema de saúde uma melhor gestão dos recursos.

Por fim, o setor de saúde não ficou imune às novas tendências tecnológicas, comuns aos demais setores de atividade, e que foram incorporadas na infraestrutura de IT da organização, como a implementação massiva de dispositivos IoT (videovigilância, controlo de acessos…), mobilidade de funcionários, uso de aplicações na cloud, etc.

Todas estas iniciativas tecnológicas têm um ponto em comum: dependem absolutamente da rede corporativa para serem implementadas. A rede tornou-se o grande facilitador e habilitador da transformação digital, sempre e quando esteja preparada para assumir todos estes desafios.

As tendências tecnológicas que foram incorporadas no setor de saúde nos últimos anos – todas as mencionadas acima, além do BYOD geral, IoT, cloud, Big Data, etc. – exigem uma abordagem de rede que difere radicalmente das arquiteturas tradicionais, projetadas para ambientes de utilização TIC que pouco têm a ver com os atuais. A rede tradicional, monolítica e estática, desenhada para servir *desktops* e conectar data centers físicos, tem que dar lugar a uma rede flexível e ágil, pensada para dispositivos móveis e autónomos (IoT), data centers distribuídos ou na cloud e em perímetro alargado. Ou seja, uma rede preparada para a transformação digital tem que ser flexível, ágil e segura.

Num estudo recente, a Gartner analisa uma série de mudanças e tendências que, na sua opinião, são os elementos que impulsionam esta transformação. Em primeiro lugar, podemos mencionar a necessidade de otimizar os recursos alocados à Saúde. As novas tecnologias permitem fazer mais com menos, facilitam e simplificam a gestão de infraestruturas e otimizam a utilização de recursos. Um exemplo que já é comum no nosso sistema de saúde é a utilização dos registos médicos eletrónicos, que tem permitido economizar muitos recursos em exames repetidos e que estão acessíveis, com as infraestruturas de comunicação adequadas, a partir de qualquer lugar.

Um segundo elemento dinâmico seria a necessidade de oferecer assistência de melhor qualidade ao paciente. Melhorar a qualidade do atendimento continua a ser uma meta urgente que visa melhorar continuamente a saúde dos pacientes e da sociedade em geral. Uma forma de melhorar essa qualidade é facilitar ao máximo o acesso do paciente aos serviços de saúde, minimizando o tempo de espera, etc.

Em terceiro lugar, os requisitos regulamentares devem ser mencionados como um fator para essa mudança. As regulamentações de proteção de dados, necessárias num mundo hiperconectado cheio de ciberameaças à privacidade e confidencialidade do paciente, estão intimamente relacionadas com a gestão da segurança da infraestrutura de IT. ■

glintt

"HÁ ALGO QUE NUNCA SERÁ SUBSTITUÍDO POR MÁQUINAS: O RELACIONAMENTO HUMANO"

Filipa Fixe, Administradora Executiva da Glintt, explica as vantagens da utilização de Inteligência Artificial (IA) na área da saúde para o bem do paciente e para a gestão do hospital.

A IA já é utilizada em Portugal? Quais são os casos de uso presentes em Portugal?

A premissa de que os dados são a nova *healthcare currency* tem culminado numa aposta cada vez mais visível em ferramentas de IA.

Do ponto de vista da gestão hospitalar, temos o exemplo do KnowLogis, desenvolvido pela Glintt em parceria com o INESC TEC e em utilização diária no CHVNGE desde novembro de 2020. O KnowLogis é um sistema de *report* inteligente que, integrado com outras bases de dados, monitoriza e acompanha de forma dinâmica os encargos com os produtos da logística hospitalar, analisa automaticamente a evolução dos seus *stocks*, incorpora dados do histórico e sugere medidas de correção e melhoria. Esta solução transforma o paradigma da logística hospitalar introduzindo a inteligência artificial no processo de decisão.

No âmbito das candidaturas ao *Prémio HINTT*, a Glintt tem tomado conhecimento de inúmeros projetos de reconhecido valor desenvolvidos em contexto nacional. Os projetos

candidatos têm provado que Portugal é uma montra digital na área da saúde.

O público em geral tem a ideia de que os médicos humanos vão desaparecer e ser substituídos por máquinas. Será isto que vai acontecer, ou a abordagem da IA à saúde é de ajuda ao médico?

Há algo que nunca será substituído por máquinas: o relacionamento humano, e esse "pormenor" faz toda a diferença numa relação entre profissional de saúde e doente.

De referir como exemplo a imagem médica – uma das áreas em que a IA se tem mostrado mais promissora. Um estudo recente publicado na Nature em 2020 treinou um modelo de computador em imagens de cerca de 29 mil mulheres. O sistema de IA superou tanto as decisões históricas feitas pelos radiologistas, que inicialmente avaliaram as mamografias, quanto as decisões de seis radiologistas especialistas que interpretaram 500 casos selecionados aleatoriamente num estudo controlado. Aqui conseguimos com relativa facilidade percecionar as potencialidades da IA no que respeita à capacidade de processamento dos dados, considerada fundamental para a tomada de decisão mais ágil e baseada em conhecimento. As potencialidades da IA não contribuem para o desaparecimento dos médicos, representam antes uma mais-valia para a sua prática clínica.

Como é que esta tecnologia pode oferecer conhecimento aos médicos?

O exemplo anterior demonstra as potencialidades da IA para a prática médica. Por outro lado, estamos também a permitir que os médicos, enfermeiros e terapeutas se possam dedicar aos casos que necessitam de mais atenção.

Um exemplo de como um acompanhamento médico pode conferir maior qualidade de vida a doentes oncológicos, com recurso a tecnologia, é o projeto Oncommunities do IPO do Porto, que venceu o Prémio HINTT 2020, na categoria de *Patient Safety*. Esta é uma ferramenta digital inovadora que garante o acompanhamento contínuo e personalizado de mulheres com cancro de mama. Pretende criar um espaço privilegiado para a partilha de dúvidas, de informações, de recursos úteis com carácter psico-educativo e de suporte mútuo.

Uma decisão de um médico pode salvar um paciente. De que maneira é que a inteligência artificial vai apoiar essas decisões?

O Nudge Digital - Redução da sobreprescrição de Antibióticos, projeto vencedor na categoria de *Clinical Outcomes* do Prémio HINTT 2020 desenvolvido pela SPMS ilustra o potencial de novas tendências como IA e *big data* para a aposta no bem-estar e na qualidade de vida dos utentes e realmente como a decisão do médico, com o apoio da tecnologia certa, pode realmente salvar o paciente. O projeto visa reduzir a prescrição inadequada de antibióticos. O conceito é o de comparação interpares, alertando os clínicos que prescrevem mais antibióticos do que outros Profissionais de Saúde da mesma especialidade e / ou da mesma unidade de saúde, por forma a estimular a alteração de comportamentos. Esta solução representa a realização do potencial da *big data* na melhoria de processos terapêuticos. ■

procensus oak peak is now

brighten
simplify your business. together.

POR ANDRÉ COUTINHO
Managing Partner, Brighten

– LOGÍSTICA NO SETOR DA SAÚDE –

A logística no setor da saúde, ao contrário de outras indústrias, é muitas vezes vista apenas como uma função que tem de existir para fazer chegar os fármacos, os dispositivos médicos e tantos outros produtos que são utilizados ou administrados no dia a dia do hospital ou clínicas.

AO NÃO OLHAR para a logística hospitalar como uma função crítica, que pode simplificar e otimizar a cadeia de valor das clínicas e hospitais, o setor da saúde em Portugal está a desperdiçar recursos que, em tempos como os que hoje vivemos, são vitais para salvar vidas.

Como deve, então, o setor da saúde olhar para a sua função logística, e de que forma a digitalização desta função pode trazer valor acrescentado para todos os *stakeholders*?

Na nossa opinião, a logística hospitalar deve ser encarada como uma função crítica e estratégica para este setor. A restruturação das cadeias de abastecimento dos hospitais e a digitalização da função logística são algumas das sugestões que procuramos debater e justificar neste artigo. Se olharmos para a função logística nas várias indústrias, identificamos grandes investimentos, tanto ao nível das infraestruturas como ao nível da tecnologia. Armazéns automatizados, software que permite planear ao ponto de entregar peças quando são precisas na produção (JIT), soluções de *picking* e mobilidade são apenas alguns dos exemplos de investimentos que visam simplificar e otimizar a função logística.

No setor da saúde, porém, em particular no universo nacional, vimos alguns indícios de baixo investimento. Ao visitar vários armazéns centrais hospitalares, facilmente se percebe que funcionam em espaços adaptados para o efeito, que as cadeias de abastecimento e distribuição

- André Coutinho -
Managing Partner, Brighten

não são uniformes e que as soluções de mobilidade são das poucas ferramentas usadas pelos profissionais que, todos os dias, garantem que os serviços hospitalares têm todo o material de que necessitam para tratar os seus pacientes. Esta situação gera ineficiências, desperdício e, mais importante, consome tempo de recursos cujo foco devem ser os pacientes. Quais as iniciativas que, na nossa opinião, podem e devem então ser levadas a cabo neste setor, para elevar a função da logística hospitalar?

Em primeiro lugar, analisar de forma estratégica a criação de centros de distribuição regionais. Se os hospitais não foram desenhados para ter grandes armazéns, porque não montar estruturas regionais que permitam uma maior uniformização e eficiência dos canais de distribuição? Com tal estrutura e com as soluções de tecnologia mais adequadas, seria possível reduzir *stocks* em toda a cadeia ao mesmo tempo que se reduziam as quebras com uma maior flexibilização e agilidade de toda a cadeia. Existem diversos e bons exemplos de tais iniciativas, no setor privado da saúde, implementadas com sucesso.

Em segundo lugar, o setor deverá dotar-se de soluções e tecnologias que permitam implementar esta visão de cadeia de abastecimento. Atualmente, os hospitais usam os seus softwares clínicos para suportar a sua logística hospitalar. Estas soluções, contudo, foram desenhadas, e bem, tendo por base as necessidades clínicas de um hospital e, como tal, carecem de funcionalidades que enderecem as necessidades e complexidades de toda a cadeia de abastecimento.

A implementação de um ERP robusto e com forte capacidade ao suporte da atividade logística, como é, por exemplo o SAP S4/HANA, devidamente integrado com os sistemas clínicos existentes, permitirá ao setor da saúde capacitar-se para a digitalização necessária desta função. Dispor de uma base de dados única de artigos nos vários hospitais, o que permitiria a implementação de uma cadeia de abastecimento com visibilidade total das necessidades, implementar estratégias de reposicionamento dos armazéns avançados e disponibilização de serviços com base nos consumos históricos e, também, na previsão das necessidades futuras, resolver os abastecimentos dos consignados residentes e não residentes nos hospitais, evitar o *maverick buying* dos vários serviços, são apenas alguns dos exemplos de desafios reais que tais soluções ajudam a resolver.

A par da implementação dos ERP (*enabler*), o setor deve ainda garantir que todos os fluxos e registos ocorrem a par dos eventos logísticos relevantes e de forma desmaterializada (*paperless*). Para tal, devem garantir que são desenhadas e implementadas aplicações móveis, como extensões do ERP, devidamente customizadas para o setor e aos vários intervenientes envolvidos em toda a cadeia, desde o técnico do armazém até ao enfermeiro que, por exemplo, administra um fármaco a um paciente. ■

Life Is On Schneider Electric

POR RITA LOURENÇO
Regional Key Account Manager (Iberia), Schneider Electric

EDGE COMPUTING: REDUZIR GASTOS E MELHORAR A SATISFAÇÃO DOS PACIENTES COM SAÚDE DIGITAL

Como seria de esperar com uma pandemia global, as despesas públicas com a saúde dispararam no último ano.

POR OUTRO LADO, muitas instituições de saúde gostariam de reduzir gastos, mas levanta-se uma importante questão: como fazê-lo sem comprometer a saúde dos pacientes?

O DIGITAL É O CAMINHO

Dois fatores principais estão a impulsionar a reinvenção da área da saúde: a busca pela sustentabilidade económica e a disrupção digital. As despesas do setor mantêm-se numa trajetória insustentável, devido a alterações demográficas e à globalização. Felizmente, para ajudar os sistemas de saúde a reduzir custos, surgiu a saúde digital, que permite abordagens substancialmente mais rentáveis. Algo positivo a retirar da pandemia foi a aceleração das iniciativas neste âmbito. A implementação da telemedicina era algo pendente há vários anos e que agora

acontece de forma abrangente; e as tecnologias digitais auxiliaram a comunicação dos resultados dos testes de COVID, bem como o seguimento dos infetados e contactos de risco. Mas é possível fazer ainda mais, nomeadamente para estabelecer sistemas digitais que possam apoiar o setor a longo prazo.

Um dos maiores desafios na transformação do setor da saúde com plataformas digitais é garantir a confidencialidade dos pacientes, e é aqui que os sistemas de IT seguros, fiáveis e robustos se tornam essenciais. Para serem eficazes, os dados têm de estar disponíveis em qualquer momento, para que as equipas médicas possam aceder à informação de cada paciente de forma imediata quando precisam de tomar decisões críticas. A disponibilidade e a operacionalidade dos sistemas são também indispensáveis, exigindo assim a existência de um sistema de *backup* de alimentação elétrica – se houver uma falha no abastecimento, os sistemas têm de voltar ao ativo rapidamente.

COMO PODEM O EDGE, A IA E A IOT AJUDAR O SETOR DA SAÚDE?

O *Edge Computing*, a Inteligência Artificial e a IoT são tecnologias poderosas atualmente utilizadas na digitalização do setor da saúde e que trazem benefícios sem paralelo.

Com o *Edge Computing* garante-se menos latência do que nos serviços baseados na cloud, o que é particularmente importante para a consulta de informações e a tomada de decisões clínicas em caso de emergência. Permite também levar cuidados de saúde a zonas isoladas através de dispositivos *edge* portáteis que podem reunir, armazenar, gerar e analisar dados críticos dos pacientes.

Por seu lado, a IA acelera o processo de investigação dos ensaios de medicamentos – algo que vimos durante a corrida pela vacina da COVID-19. Podendo testar diversos cenários, identificar biomarcadores e reorientar os princípios ativos, as farmacêuticas podem acelerar o desenvolvimento de medicamentos e poupar milhões de euros. A IA também pode ser utilizada em tecnologias de imagem, para automatizar análises e diagnósticos.

A IoT pode favorecer a monitorização dos pacientes com câmaras e sensores para prevenir quedas, alertar os profissionais para mudanças clínicas, ou ainda manter os medicamentos à temperatura adequada e identificar produtos contrafeitos.

CRIAR UM SISTEMA DE SAÚDE RESILIENTE

A pandemia tornou muitas coisas mais claras – e uma das mais importantes foi a necessidade de criar instalações de saúde que possam continuar a operar eficazmente, mesmo em condições de desastre ou emergência.

Cada sistema de saúde deve ser resiliente perante a instabilidade da rede, contar com soluções de *backup* de energia e ser capaz de garantir a prestação de cuidados aos pacientes com segurança e fiabilidade.

A **segurança dos pacientes** deve ser a prioridade número um; segue-se a **eficiência operacional**, que pode ser melhorada através da eficiência energética e da maior produtividade das equipas; e ainda a **satisfação dos pacientes**, que será em última instância o melhor fator de medição de resultados. ■

SoftFinança

POR LUÍS TEODORO
Administrador

FARMÁCIAS DIGITAIS: BEM-ESTAR E ACONSELHAMENTO

"A saúde só é valorizada quando a doença chega"
Thomas Fuller

A TRANSFORMAÇÃO DIGITAL é uma estratégia que as indústrias mais variadas têm iniciado de forma a se reinventarem e serem capazes de oferecer aos seus clientes novos níveis de serviço. A indústria da saúde não é alheia a este facto e se muito se fala do potencial do AI, do AR ou do 5G como tecnologias capazes de revolucionar e aumentar os serviços e as práticas existentes, pouco se tem falado sobre o modo como as farmácias se têm vindo a preparar para fazer face a estas mudanças.

As farmácias têm vindo a estruturar as suas iniciativas de transformação digital em torno de dois eixos estratégicos. O primeiro eixo, alterando a sua tradicional função de aconselhamento e fornecimento de medicação para se tornarem centros de bem-estar e qualidade de vida, oferecendo produtos e serviços capazes de lhes proporcionar conforto e estilos de vida mais saudáveis. O segundo, alicerçando o seu modelo de negócio em função do cliente e da jornada que este enfrenta enquanto paciente.

Normalmente, considera-se que a jornada do paciente é constituída pelas fases de pré-diagnóstico, quando surgem os primeiros sintomas de doença; diagnóstico, quando o paciente já se encontra medicado; tratamento, quando o paciente toma a medicação e segue as indicações médicas; e convalescença, quando o paciente embora considerado curado se encontra ainda debilitado e necessita de acompanhamento próximo.

Esta nova visão centrada no paciente e na sua jornada é garantida através de pontos de contacto físicos, as tradicionais farmácias reconfiguradas para as suas novas e aumentadas funções, e pontos de contacto virtuais, plataformas digitais, que

- Luís Teodoro -
Administrador

permitam às farmácias manter um relacionamento estreito com os seus clientes, e aplicações que permitam aos clientes aceder a novos tipos de serviço mais cómodos e eficientes, quer sejam alertas para a tomada de medicação, encomenda online, troca de mensagens, ou acesso a informação de confiança, e também gerir um vasto conjunto de informação orientada a apoiar o utente na melhoria da sua qualidade de vida.

Ao longo de todas as fases da jornada do paciente, a farmácia digital estará presente, efetuando um rastreamento rigoroso do paciente, tirando-lhe dúvidas, aconselhando-o, tudo fazendo para melhorar a sua jornada, aumentando a utilidade percecionada no dia a dia dos utentes muito para além do suporte à terapêutica curativa que habitualmente caracteriza a relação dos utentes com as farmácias.

Na sua existência, a SoftFinança tem vindo a apoiar as mais exigentes instituições na forma como estas se relacionam com os seus clientes. Dos equipamentos de *self-service*, aos portais, da sinalética digital às aplicações móveis, podemos também apoiar as farmácias na sua transição digital. O SEGG é uma plataforma digital de comunicação e interação entre pessoas e organizações, pensada, de raíz, para dar resposta ao crescente número de canais digitais e ao aumento do volume, e da variedade de conteúdos, presentes nos mais variados dispositivos. Sinalética digital interativa com capacidade para apresentação de diversos tipos de conteúdo, incluindo visualização 3D, *video mapping*, ou experiências de RA são aspetos diferenciadores que a nossa solução torna possível. A nossa experiência em *self-service* permite-nos ainda trazer ao mercado máquinas de venda e cacifos inteligentes, equipamentos que oferecem ao paciente a comodidade de levantar os seus medicamentos, de forma não assistida, a qualquer hora do dia ou da noite.

Em 2019, a SoftFinança foi escolhida pelo Grupo ADDOPHARM para dar início ao processo de pôr em prática os alicerces necessários para garantir aos seus membros uma transição eficaz para as novas missões que o futuro reserva às farmácias, centros de referência na procura de bem-estar, estilos de vida saudável e conselheiros de confiança presentes ao longo de todas as fases da jornada do paciente.

O Grupo ADDOPHARM é um dos maiores grupos de farmácias em Portugal, cerca de 350 totalmente independentes e autónomas, que partilham os mesmos interesses, ideias e práticas de gestão na sua atividade diária.

O primeiro passo deste processo está já lançado, o **Portal Nossa Farmácia** e a **Aplicação Móvel A Nossa Farmácia** são sistemas a partir dos quais os clientes têm já acesso de forma cómoda e eficiente ao inventário de produtos e serviços das farmácias do grupo e onde podem diretamente proceder à sua compra *online*. A aplicação irá ainda permitir ao cliente ter acesso a outros serviços personalizados que irão complementar de forma consistente e valiosa a sua experiência.

Hoje, a saúde já não é só valorizada quando a doença chega, as farmácias digitais já não o permitem! ■

POR NUNO BAJANCA
Technical Architect Consulting
- Data Center & Multi Cloud

NO SETOR DA SAÚDE, A TECNOLOGIA TEM DADO RESPOSTA A GRANDES DESAFIOS

Em entrevista, Nuno Bajanca refere que a experiência de utilização dos profissionais de saúde e a melhoria da segurança dos dados são duas tendências tecnológicas neste setor.

Que tipo de soluções comercializam no setor da saúde?

A Warpcom atua em diversas áreas tecnológicas. No setor da saúde é frequente desenvolvermos projetos de implementação ou melhoria da infraestrutura física de rede, de comunicações unificadas, de virtualização e hiperconvergência, armazenamento e *backup* de dados, postos de trabalho virtuais, cibersegurança e segurança pública.

Especificamente para o setor da saúde, implementamos uma solução de gestão de autenticação e *single sign-on* denominada Imprivata OneSign, cujo objetivo é assegurar um início de sessão simplificado, em computadores e aplicações, através de um acesso rápido, seguro e sem cliques aos dados dos pacientes.

Quais os grandes desafios e tendências tecnológicas deste mercado?

No setor da saúde, a tecnologia tem dado resposta a dois grandes desafios: a melhoria da segurança dos dados e da experiência do utilizador. Com a COVID-19, foi ainda reforçada a necessidade de soluções robustas de videoconferência.

O primeiro desafio está associado às normas de proteção de dados que têm sido introduzidas e que já levaram à aplicação de uma coima de 400 mil euros num centro hospitalar Português.

As empresas do setor de saúde precisam de guardar processos com dados pessoais e clínicos dos seus doen-

- Nuno Bajanca -
Technical Architect Consulting
- Data Center & Multi Cloud

tes, cujo acesso rápido e por um grande número de pessoas pode ser crucial para salvar vidas. No entanto, os profissionais de saúde não são utilizadores especializados em sistemas nem as suas tarefas são completamente compatíveis com uma implementação de técnicas de segurança utilizadas em escritórios.

Já o segundo desafio tem ganho importância num ambiente em que todos os minutos contam. Com uma melhor experiência de utilização, é possível ter colaboradores mais produtivos e motivados, que dedicam mais tempo aos seus pacientes e menos à tecnologia. Como extra, os hospitais asseguram uma maior retenção dos seus profissionais.

Na sua vida pessoal, os profissionais de saúde utilizam dezenas de aplicações que acedem a partir de qualquer dispositivo. Nos hospitais e clínicas, a evolução tecnológica não foi feita com a mesma velocidade, o que deixa os profissionais dependentes de postos de trabalho específicos e do local onde estão fisicamente.

E as oportunidades?

Existem grandes oportunidades de transformação digital introduzindo melhorias nas áreas endereçadas anteriormente. A utilização simultânea da solução da Imprivata e da virtualização do posto de trabalho responde aos desafios de segurança, conformidade e experiência de utilização. Este tipo de soluções contribui também para processos de desmaterialização e simplificação da gestão do ambiente de IT, composto por centenas de computadores de diferentes marcas e gerações.

Com o *single sign-on*, os profissionais de saúde não têm de perder tempo a introduzir diferentes credenciais de autenticação sempre que acedem a uma aplicação. Utilizam ainda o cartão do hospital para iniciar e terminar sessão sem ter de inserir as credenciais, reduzindo o tempo de acesso e motivando a utilização do perfil correto.

Com a virtualização do posto de trabalho, os dados ficam centralizados e menos expostos a falhas de segurança. Os profissionais de saúde acedem às aplicações em qualquer dispositivo e lugar. As equipas de IT atualizam as aplicações uma vez e distribuem-nas por todos os utilizadores.

Pode dar-me alguns exemplos de casos de sucesso?

Apesar dos constrangimentos da pandemia, implementámos a solução Imprivata OneSign num hospital público em Lisboa. Dos 1500 profissionais que vão ter brevemente acesso à solução, 500 já utilizam o seu cartão do hospital para iniciar sessão e aceder, sem colocar as credenciais, a aplicações como o Sclínico, o GHAF e o Sonho.

Realizámos ainda várias provas de conceito em vários ambientes hospitalares públicos e privados, o que nos permitiu conhecer melhor o ambiente aplicacional dos hospitais e demonstrar que as soluções testadas simplificam o trabalho das equipas de IT e melhoram a experiência dos profissionais de saúde.

Além do contexto Imprivata, desenvolvemos regularmente projetos com clientes na área da saúde. A título de exemplo, realizámos em 2020 a renovação tecnológica do ambiente de data center de um centro hospitalar do norte do país, capacitando-o com um ambiente de recuperação a desastres e dotando-o da infraestrutura necessária para a atualização da aplicação Sonho. ■

xerox

INOVAÇÃO COMO ALAVANCA DA TRANSFORMAÇÃO DIGITAL PARA A PRESTAÇÃO DE MELHORES CUIDADOS DE SAÚDE

No início do verão passado, foi publicada uma história no New York Times sobre os desafios que as autoridades de saúde pública enfrentavam no atual contexto de pandemia, incluindo o relato de uma história que mais parecia uma piada dos anos 80.

"Num hospital público nos EUA, um equipamento de fax não parava de imprimir páginas e páginas de resultados de testes à COVID-19. Parecia uma brincadeira, mas não era."

E é uma ilustração eficaz de como sem transformação digital não é possível garantir os melhores serviços de saúde e o melhor atendimento às pessoas no século XXI.

A saúde digital 4.0, ou e-saúde, compreende a aplicação de recursos tecnológicos para otimizar o atendimento, oferecer um serviço mais rápido, integrado e eficiente. É importante entender que a saúde digital é

diferente de apenas digitalizar as informações, trata-se de uma nova mentalidade, da adoção de uma nova abordagem em relação a como encaramos os desafios na saúde.

Muitos estudos indicam claramente que a pandemia veio desacelerar as iniciativas de transformação digital em curso em muitas unidades, pela necessidade premente de re-alocar recursos para outras áreas e assim fazer face aos crescentes custos com a 1ª linha de cuidados de saúde.

Mas o que também se verifica, é que essa desaceleração provoca em paralelo que as organizações de saúde tenham que enfrentar outro desafio acrescido. Num momento crítico em que mais do que nunca é necessário acesso rápido à informação, disponibilidade de dados fiáveis e rapidez na comunicação, as organizações veem-se obrigadas a ter que gerir processos desligados e sem a informação correta, numa abordagem fragmentada de atendimento e suportada por tecnologia desatualizada.

Assim, as organizações de saúde precisam de uma visão clara sobre os sistemas que suportam em paralelo, os melhores cuidados de saúde.

Estão obrigadas a entregar algo que sem digitalização e automação não é possível. Sem acesso rápido ao histórico clínico do paciente, sem registos atualizados ou informação em tempo real e comunicação personalizada às pessoas; no contexto de pandemia actual, **torna ainda mais difícil a concretização da permissa número um: a prestação dos melhores cuidados de saúde.**

INOVAÇÃO COMO ALAVANCA DA TRANSFORMAÇÃO

O investimento contínuo da Xerox em inovação, permitiu-lhe ter vindo a desenvolver soluções adequadas às necessidades do setor da saúde, capazes de acrescentar valor e com a flexibilidade necessária para se adaptar de forma rápida aos desafios que a pandemia trouxe e que ninguém seria capaz de prever.

A capacidade de conectar todas as variáveis e sistemas mesmo em ambientes complexos, digitalizar registos médicos para facilitar a comunicação com as pessoas e fazer a integração de novas ferramentas para a gestão da informação, tem ajudado prestadores de cuidados de saúde em vários países a obter eficiência, personalizar as interações com as pessoas e a garantir a conformidade com todos os regulamentos.

E quando todas estas coisas funcionam em conjunto, o resultado é a melhoria na prestação dos cuidados de saúde, de uma forma global.

IMPERIAL COLLEGE HEALTHCARE NHS TRUST

O desafio do cliente era claro: digitalizar toda a biblioteca de registos e arquivo externo (o número total de páginas rondava os 2,8 mil milhões), ao mesmo tempo que precisava de reduzir os custos relacionados com a gestão dos registos de saúde.

A Xerox respondeu com um serviço de digitalização completo, permitindo que neste momento seja possível alcançar a integração destes registos com a informação nova e adicional que já é 100% introduzida de modo digital.

Implementar uma estratégia digital que englobe todos os dados e toque todos os pontos de interação, acabou por resultar num excelente exemplo de transformação digital global do NHS.

"Pode ser um clichê, mas a Xerox é realmente um parceiro, e não um fornecedor do NHS. Assumiram os nossos objetivos como os deles, e não poderíamos alcançar a nossa estratégia digital tão facilmente sem a Xerox. Juntos, estamos a suportar a melhor prestação de cuidados de saúde em cinco dos hospitais de Londres."

Linda Watts of Imperial College Healthcare NHS Trust

A pressão adicional imposta aos prestadores de cuidados de saúde pela pandemia COVID-19 aumentou a necessidade de estes se certificarem de que os seus sistemas são robustos e adaptáveis, para que os colaboradores possam processar rapidamente grandes volumes de informações críticas para admissão, despiste e tratamento e não menos relevante, para a gestão de comunicações personalizadas, tão cruciais, como por exemplo, para os planos de vacinação de larga escala que estão a ser implementados em todo o mundo.

Num contexto como o atual, o enorme desafio dos provedores de cuidados de saúde é o que resulta da necessidade de manter o equilíbrio entre os deveres de cuidar das pessoas e melhorar o ciclo de interações e de comunicação. ■

Siga a ligação do QR code para saber mais sobre os serviços digitais da Xerox para utentes e prestadores de cuidados de saúde.

Re:imagine!

A **principal responsabilidade** da nossa geração é **re-imaginar** as nossas **empresas e instituições, públicas** e **privadas!**

Tom Peters in Re-imagine! - © Pearson Education

COMO RE-IMAGINAR UMA NOVA ECONOMIA

A pandemia ainda não passou, mas esta é a altura de apostar no futuro. As empresas que começarem agora a investir terão uma maior chance de sucesso. A transformação digital das organizações é a chave para o futuro.

RUI DAMIÃO

NO TERCEIRO TRIMESTRE de 2020, acreditava-se que 2021 seria um ano de voltar ao passado, a pré-2020, em que tudo voltaria aos poucos ao antigo normal. Em Portugal, o crescimento exponencial do número de infetados e mortos levou o Presidente da República e a Assembleia da República a decretar uma vez mais o Estado de Emergência.

Assim, a recuperação que se esperava teve de ser adiada. Os negócios de venda direta ao público voltaram a fechar ou a trabalhar sobre estritas limitações e – na altura de fecho desta edição – ainda não existe data para que voltem a abrir.

TECNOLOGIA E DIGITALIZAÇÃO

Há alguns anos que a tecnologia tem vindo a conquistar uma importância cada vez maior dentro das organizações. O atual estado mostra exatamente isso: é a tecnologia que há muito existia que permitiu que os colaboradores continuassem a trabalhar a partir de casa, por exemplo.

Milton Cabral, Sales Manager na Axians, afirma que, "de um modo geral, todos os setores – económicos e sociais – sofrerão alterações profundas". As alterações que vão existir estão relacionadas "com os nossos hábitos, pessoais e profissionais". O teletrabalho – "que veio certamente para ficar" – é uma dessas alterações; outro são os hábitos de consumo que foram acelerados com a pandemia.

Clara Raposo, Dean do ISEG, indica que há algumas lições que já se aprenderam: "a tecnologia e a digitalização vão ter de chegar a todos os setores de atividade e que os modelos de trabalho mais flexíveis", como o trabalho remoto ou um modelo de trabalho híbrido, "têm de ser bem desenhados, à medida da natureza da função de cada colaborador e da sua própria vida pessoal".

Nuno Vieira da Silva, Head da Google Cloud em Portugal, acredita que "a tecnologia tem sido essencial para muitas empresas e pessoas", indicando que "foram necessários investimentos que levaram a uma digitalização e inovação de diferentes processos que vão desde os modelos de negócio, reconfiguração de espaços físicos, à transformação do ponto

- Carlos Carús, AWS -

- Milton Cabral, Axians -

- Nuno Vieira da Silva, Google Cloud -

- José Manuel Paraíso, IBM Portugal -

de trabalho com a adoção crescente do *home office*".

Na mesma linha, José Esfola, Diretor-Geral da Xerox em Portugal, afirma que "a alteração do local físico de trabalho" é um dos paradigmas que está em mudança. Ao mesmo tempo, "os conceitos de mobilidade e digitalização são um caminho que as empresas estão a entender que ainda não está tudo feito e a perceber que a digitalização é uma coisa, e a alteração de processos e eficácia dos mesmos é outra".

Independentemente do foco das organizações, a cloud tem tido um papel crucial para todas as organizações, independentemente da sua estrutura ou tamanho. Carlos Carús, Diretor de Tecnologia da Amazon Web Services para Portugal e Espanha, explica que a AWS está a "testemunhar como a cloud está a ajudar os nossos clientes a executar planos fiáveis de continuidade de negócio, permitindo o recurso ao teletrabalho, enquanto lançam novos serviços que servem as necessidades reais na otimização dos fluxos de caixa e até mesmo na re-

É PRECISO REVER AVISÃO, A ESTRATÉGIA, AS FERRAMENTAS E AS COMPETÊNCIAS DAS ORGANIZAÇÕES

dução dos custos associados à diminuição da procura.

CENTRADO NO CLIENTE

Com base num estudo do IBM Institute for Business Value (IBV), José Manuel Paraíso, Presidente da IBM Portugal, refere que "os CEO salientaram que se tornou num imperativo focar no que é necessário para se ser essencial para os seus clientes, os seus colaboradores e a sua comunidade", sendo necessário "centrar no que há de mais crítico no próprio negócio, no que realmente diferencia as organizações e permite a entrega de maior valor".

José Tavares, Diretor de Inovação e Soluções da SAP Portugal, refere que há uma necessidade "de se passar além de uma visão única de *Business-to-Business* e *Business-to-Consumer* e ter-se também uma cultura – quiçá preditiva – de *Business-to-Me*, ou seja, um enfoque centrado no cliente".

Depois de uma primeira fase de resposta imediata à pandemia e uma segunda assente na fase de recuperação, de arrancar novamente com a economia ao mesmo tempo que se gere a incerteza, é preciso entrar na re-imaginação. Abel Aguiar, Diretor Executivo para Parceiros e Pequenas e Médias Empresas da Microsoft Portugal, afirma que "temos de preparar hoje o momento pós-pandémico, enquanto gerimos a situação atual. Esta é a fase que começa a ganhar importância neste momento com as vacinas e tratamentos a serem disseminados, mas com taxas de adoção progressivas e distintas, país a país, com novas variantes e estirpes a aparecer mantendo uma estrutura de incerteza latente".

Re-imaginar, explica o executivo da Microsoft, significa "rever a visão, a estratégia, os processos, as ferramentas e as *skills* – da economia e das organizações – com um claro foco no crescimento para identificar vantagens competitivas e tomar, desde já, as ações necessárias para as garantir no pós-pandemia".

DESAFIOS

Milton Cabral menciona alguns dos desafios que as empresas vão enfrentar. O primeiro é "a volatilidade e a indefinição à volta do seu futuro", uma vez que "as variáveis que determinam os comportamentos são imensas". Outro é a "dificuldade de mudança da cultura organizacional".

A incerteza também é um tema referido por José Tavares, da SAP Portugal, para além da resiliência, da agilidade e da flexibilidade, que, diz, "têm de estar baseadas num conhecimento, que não põe em risco os objetivos da nossa empresa, da nossa margem, da nossa rentabilidade. É necessário pegar nesta informação e integrá-la nos processos de negócio, ao longo de toda a cadeia de valor e de todas as áreas de negócio".

José Manuel Paraíso refere que a "agilidade organizacional", ou seja, "a capacidade que uma organização tem para responder rapidamente, com um propósito e capacidade de desempenho" é um dos grandes desafios das organizações, até porque "o contexto empresarial em 2020 viu planos e regras de longa data a serem substituídos por urgências do momento".

"As organizações já estão a ser bem testadas ao limite com esta pandemia", afirma Clara Raposo, explicando que "muitos dos novos desafios que teríamos de enfrentar no futuro foram antecipados e acelerados com a pandemia, na verdade. Temos o grande desafio do *upgrade* tecnológico essencial num mercado internacional competitivo. Isto implica capacitar os quadros das empresas e ter visão quanto à utilização de nova tecnologia de forma inteligente".

- Clara Raposo, ISEG -

- Abel Aguiar, Microsoft Portugal -

SUSTENTABILIDADE DO NEGÓCIO

Nuno Vieira da Silva relembra que "muitas organizações investiram em medidas temporárias" e essa situação "não será sustentável pois os modelos de negócio dos consumidores, clientes e fornecedores também evoluíram e tiveram de se adaptar". Assim, "neste mundo mais competitivo, as organizações têm de ser criativas e descobrir novas formas de encontrar e manter os seus clientes. A diferenciação pode ser através de serviços como: melhorar a experiência na aquisição de bens e serviços, processos de pós-venda, recomendações e incremento da receita por cliente e programas de fidelização".

ATUALMENTE, A TECNOLOGIA TEM UM PAPEL FUNDAMENTAL NAS ORGANIZAÇÕES E É UMA DAS FORÇAS EXTERNAS DE MAIOR IMPORTÂNCIA PARA O NEGÓCIO

Carlos Carús explica que "os maiores desafios na mudança e adoção de novas tecnologias não são técnicos, mas sim desafios relacionados com as pessoas e culturais". O executivo da AWS refere que "a equipa de liderança sénior precisa de estar alinhada e verdadeiramente comprometida com o desejo de acelerar a transformação digital e a adoção da cloud". Só assim é que "essa mesma equipa terá de definir uma direção e expectativas claras com a restante organização para que todos os elementos estejam em sintonia e trabalhar para um bem comum".

Abel Aguiar refere que os desafios estão espalhados por quatro áreas: a capacitação dos colaboradores, a otimização das operações, o relacionamento com os clientes e a transformação de produtos e serviços. Na área da capacitação dos colaboradores, explica, esta foi "uma das maiores áreas de mudança para as organizações e será crítica para o desenho do futuro. Nunca como hoje se falou da dependência das organizações dos seus colaboradores, mas também do seu bem-estar".

José Esfola acredita que o "maior desafio são as pessoas" e reforça que "para as organizações e para o país como um todo, há que agregar a sociedade num esforço conjunto e conseguir uma articulação efetiva entre as pessoas, as empresas e o Estado".

PAPEL DA TECNOLOGIA

Se a "recuperação vai ser longa e desafiante", como diz Nuno Vieira da Silva, também é verdade que "a tecnologia é uma das forças externas de maior importância e com maior impacto em qualquer área de negócio", como referiu José Manuel Paraíso.

Carlos Carús reafirmou que "a tecnologia tem vindo a desempenhar um papel fundamental durante a pandemia e será certamente uma preciosa ajuda na retoma da economia. A crescente adoção da computação na cloud, por diferentes tipos de organizações, irá promover a digitalização e o desenvolvimento económico de Portugal".

Milton Cabral acredita que "o investimento em IT irá acompanhar a tendência" da evolução económica, que apontam para uma retoma. "A transição digital está ainda em curso, Portugal (e a Europa) têm ainda níveis de maturidade digital relativamente baixos e com um potencial de crescimento significativo, acrescendo ainda o facto de que entrará já este ano, e mais fortemente em 2022, o efeito da injeção dos fundos comunitários que, como sabemos, colocam bastante relevância na transição digital", explica.

- José Tavares, SAP Portugal -

- José Esfola, Xerox Portugal -

Nuno Vieira da Silva explica que "A tecnologia irá acompanhar as organizações na sua jornada de transformação e adaptação a esta realidade, mas é também um facto que, para as organizações terem sucesso, têm que ter uma cultura de diálogo, cooperação e colaboração, assegurando que a transformação não é uma barreira, mas sim parte do seu processo evolutivo". No entanto, acrescenta, "um dos fatores de sucesso prende-se com a capacidade de as empresas usarem diferentes serviços com elevada disponibilidade, mas garantindo toda a segurança. Integridade nos negócios é chave, principalmente quando os mundos digitais e físicos finalmente convergiram".

"As empresas devem investir na digitalização e acelerar os seus processos de inovação", afirma José Manuel Paraíso. Isto significa que as organizações devem, por um lado, "caminhar para um modelo tecnológico mais ágil, inclusivo e flexível, que é aquele que facilita a cloud híbrida e, por outro, que devem usar de forma mais intensa as capacidades diferenciadoras de tecnologias-chave como a inteligência artificial, automação ou blockchain. Atualmente, apenas cerca de 20% dos *workloads* foram atualizados para um modelo de cloud e apenas cerca de 14% das empresas começaram a integrar inteligência artificial nos seus processos de negócio".

Clara Raposo relembra que o pacote de medidas e incentivos públicos vão na direção da transformação digital, "o que coloca a tecnologia no centro da economia". Para além disso, as organizações já estavam a fazer "o seu caminho nesta transformação tecnológica", algumas fruto da pandemia, outras que já tinham iniciado o seu percurso. A Dean do ISEG refere que "as organizações retirarão valor do seu conhecimento e investimento em tecnologia, em primeira instância, por ser a forma de competirem com sucesso em negócios globalizados e/ou altamente concorrenciais. Isto aplica-se, claro, a setores de serviços que se prestam em '2D' pela sua natureza, mas também se aplicará a outros setores de atividade que

se transformaram por causa da pandemia". Admitindo que "a tecnologia terá um papel relevante no relançamento económico", Abel Aguiar refere, no entanto, que esta "será apenas um *enabler*". "Para que as organizações possam retirar valor da tecnologia, é crítico que olhem para ela como parte de uma transformação digital. (...) Qualquer transformação digital é uma transformação de negócio suportada em tecnologia, pelo que a criação de valor sustentável passará sempre pela estratégia e cultura da organização".

José Tavares concorda que as tecnologias emergentes e inovadoras "serão certamente um facilitador para a transformação digital e para a sustentabilidade das empresas, abrangendo inúmeras áreas". No entanto, explica, "necessitam de estar embebidas nos processos de negócio que suportam integralmente a cadeia de valor das organizações". O representante da SAP acrescenta que "todas as tecnologias têm uma função fundamental, cada qual de acordo com o seu perfil", mas que todas "visam um objetivo, que é serem capazes de facilitar e capacitar a estratégia das organizações".

José Esfola concorda que a tecnologia terá um papel determinante; no entanto, tão importante quanto as questões da tecnologia são as questões do capital humano "para tornar efetiva a utilização da tecnologia no relançamento da economia". "O desafio está na capacidade de realizar as mudanças necessárias para que o atual local de trabalho seja o centro da transformação tecnológica que as empresas necessitavam para se manter competitivas", conclui.

TRANSFORMAÇÃO DIGITAL

Um dos pontos mais importantes para a economia nacional será a transformação digital das empresas. Os vários entrevistados concordam que este tema é vital para o relançamento económico.

Nuno Vieira da Silva explica que "Portugal cria uma vantagem ao ser um país aberto às colaborações e à cooperação internacional, capaz de atrair investimentos e acelerar o processo de recuperação económica". Além do mais durante o último ano "quase todas as organizações tiveram de se transformar e criar uma identidade digital para se poderem distinguir da concorrência". Neste sentido, "muitas das empresas portuguesas também já têm uma forte presença em diferentes países, por isso, fatores como escalabilidade, agilidade, eficiência operacional e financeira, produtividade e sustentabilidade serão pilares fundamentais no processo de transformação digital".

Clara Raposo refere que, "se já antes da pandemia falávamos abundantemente de transformação digital, atualmente é inconcebível uma economia pós-pandemia que não abrace esta transformação".

A TRANSFORMAÇÃO DIGITAL É UM PONTO IMPORTANTE E FUNDAMENTAL PARA TODAS AS ORGANIZAÇÕES

José Esfola mostra-se "plenamente convicto de a que a transformação digital, ou a aceleração dos processos de transformação digital, é absolutamente crítica para o relançamento da nossa economia". Assim, o desafio que teremos será "o de mitigar as grandes diferenças que temos entre negócios e empresas altamente digitalizadas e as empresas que estiveram e estão mais expostas aos efeitos da pandemia".

Milton Cabral relembra que "quase 70% da riqueza em Portugal é gerada por PME". Um estudo da AEP Link aponta que "25% das PME indicam como principal dificuldade na sua digitalização, a falta de *know-how* específico, 21% aponta o tempo para inovar, 17% a falta de uma estratégia e apenas 12% a falta de capital. Portanto, além dos necessários e importantes recursos financeiros, é necessário sensibilizarmos e apoiarmos as empresas a compreenderem como podem tirar partido das ferramentas digitais, apoiando-as no desenvolvimento de um plano estratégico de transformação digital construído à medida das suas necessidades".

Carlos Carús acredita que "Portugal está no caminho certo para acelerar a transição digital no país". "Com um claro foco em ajudar a acelerar a transição digital como motor de recuperação económica e promover a liderança europeia na inovação digital e na economia digital, Portugal está numa posição muito favorável", explica.

José Manuel Paraíso afirma que "a transformação digital tem tudo a ver com o aproveitamento de tecnologias para reinventar e melhorar os negócios. Sabemos que a tecnologia é agora uma base estratégica central para a maioria das empresas e pode ser um fator determinante para a sua sobrevivência e o sucesso futuro". Ao mesmo tempo, o Presidente da IBM Portugal acrescenta que "a economia nacional pode beneficiar muito com toda esta adaptação e transformação digital".

José Tavares explica que "a transformação digital também deve ser aproveitada para criar novas vantagens competitivas, para apoiar o constante crescimento e gerar maior rentabilidade, assim como deve considerar a implementação de novos modelos de negócio, em busca de mais sustentabilidade".

Abel Aguiar acredita que "se há algo que nos mostraram estes últimos meses, é que a transformação digital é mais urgente do que nunca", até porque "vivemos dois anos de transformação digital em dois meses". No entanto, "este caminho está longe de ter terminado".

Em suma, Clara Raposo afirma que "o relançamento da economia nacional vai exigir que as empresas e outras organizações estejam atualizadas nas suas competências digitais". ■

LAYER8

PROTECTING YOUR BUSINESS

Solutions to address real world problems

DNS8

YOUR BEST FIRST STEP FOR IT SECURITY

VULN8

MITIGATE YOUR IT VULNERABILITIES

LEARNING8

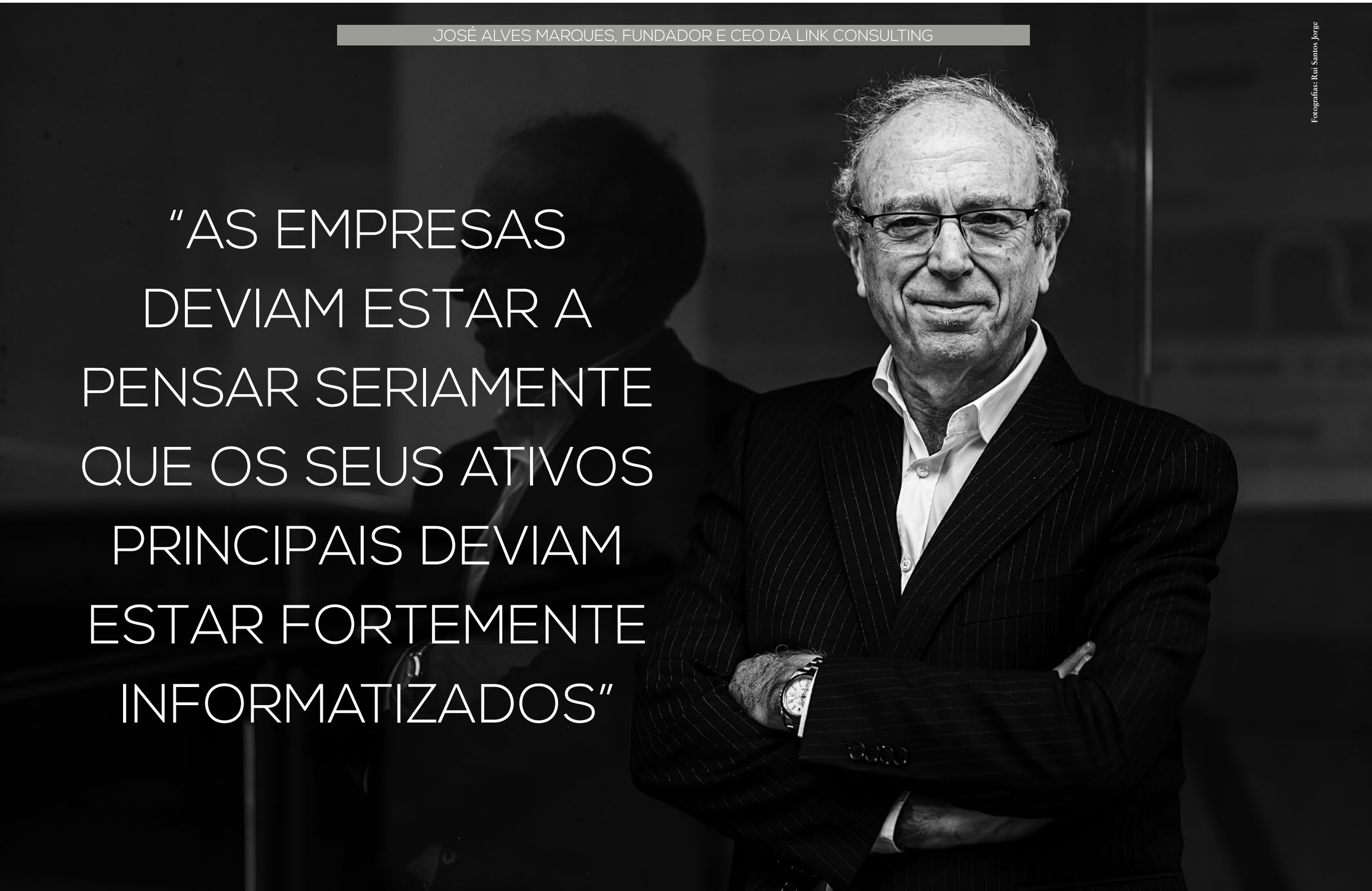
CHANGING HUMAN BEHAVIOUR

FISH8

CATCH YOUR WEAKNESS

FIND OUT MORE AT **WWW.LAYER8.PT**

JOSÉ ALVES MARQUES, FUNDADOR E CEO DA LINK CONSULTING



Fotografias: Rui Santos Jorge

"AS EMPRESAS DEVIAM ESTAR A PENSAR SERIAMENTE QUE OS SEUS ATIVOS PRINCIPAIS DEVIAM ESTAR FORTEMENTE INFORMATIZADOS"

José Alves Marques, Fundador e CEO da Link Consulting, aborda o tema do relançamento da economia nacional e qual será o papel da tecnologia nessa missão.

HENRIQUE CARREIRO E RUI DAMIÃO

Como é que caracterizaria a situação atual nos sistemas de informação empresariais em Portugal, tanto no setor público como no privado, face, sobretudo, aos desafios que este último ano colocou?

A pandemia teve, obviamente, os efeitos todos negativos que conhecemos, mas em determinadas áreas acelerou sete anos o desenvolvimento; todos tiveram que, de alguma maneira, saltar etapas em várias das coisas que faziam normalmente.

Acho que há duas coisas diferentes a distinguir: as empresas e o Estado. Acho que das empresas, se falarmos das grandes empresas, todas elas estavam de alguma forma relativamente evoluídas do ponto de vista dos seus sistemas de informação e do modo como também geriam as suas redes e conseguiram fazer estes saltos com relativa facilidade.

Num patamar mais abaixo, nota-se que muitas empresas não davam realmente valor a qualquer coisa que hoje sentimos que neste ambiente é fundamental. A empresa não pode estar dependente de que os seus processos estejam restritos a uma máquina, a um indivíduo.

A situação no Estado é mais homogénea? Como é que sentiram esta transformação nos organismos estatais?

O Estado tem várias entidades com velocidades muito diferentes. Quando se comparam uma AT ou um Instituto da Segurança Social com outros organismos do Estado, há uma diferença muito significativa. A sensação que tive, pelo menos em alguns aspetos, é que estas questões de confinamento e os impactos que tiveram inicialmente foram mais sentidos em algumas entidades estatais do que propriamente até às vezes nas empresas.

Nas médias e grandes empresas, as plataformas de computação são homogéneas, o modo como o software é feito, o *update*… todas essas coisas estão minimamente estruturadas. Não será a norma, mas no Estado ainda há coisas dificílimas, como conseguir pôr os PC em casa das pessoas, com o software certo. Na realidade, nem havia às vezes um software que era usado por todos e existiam versões diferentes. Aí, notou-se essa menor capacidade que existe dentro do

Estado de olhar para a componente informática como ativo fundamental do seu processo.

Quando começámos há 20 anos aqui na Link, lembro-me que fiz nessa altura uma conferência em que o Estado devia fazer o seu ABC na informática. O A era a administração saber falar com a administração. O B era a administração ser útil e simples para o negócio, para o *business*. O C era dos cidadãos. Acho que nestes três campos, em 20 anos, alguns aspetos não mudaram muito. Acho que o Estado continua a não ter uma visão integrada dos seus sistemas de informação e continua a ter coisas como autenticações diferentes em organismos do Estado. Cada um usa o seu. Há organismos dentro do Estado que têm mais uma visão de competição, uns com os outros até nestas questões de informática. E há uma questão que acho que não andou, ou que andou muito pouco, que era esta fluidez de ter o Estado ligado com o Estado.

Na vertente do Estado com o negócio, o que sinto é que isso não são propriamente os sistemas de informação, mas também lá chega, é que esta questão do *simplex* – que já foi também prometido N vezes – a maior parte das vezes não aconteceu. Se vir qualquer processo de licenciamento camarário, continua a ser aquela coisa de 20 documentos, 30 taxas, para a frente para trás, ninguém sabe bem porquê.

Acho que com os meios que estão hoje à nossa disposição do ponto de vista da informática, quer na estruturação de processos, quer na capacidade de interação com os sistemas dos utilizadores – pelos seus telemóveis, por chatbots, por essas coisas todas – que era o terceiro aspeto, a capacidade que teríamos de ter indicadores podiam ser uma forma de medirmos, quer o Estado quer os intervenientes do lado privado exigirem do Estado que esteja também a mostrar isso.

> // UM ATIVO PRINCIPAL NAS EMPRESAS SÃO OS SEUS PROCESSOS DE NEGÓCIO. OS PROCESSOS DE NEGÓCIO DISTINGUEM UMA EMPRESA DE OUTRA //

Temos quase um ano desde que as pessoas começaram a ir para casa. Neste ano, muita coisa mudou. No final de 2020 todos tinham esperança de que este ano fosse o ano da retoma. Está a passar o primeiro trimestre e voltamos ao confinamento. Neste momento, qual é a perspetiva que tem para o resto do ano?

De certa maneira, acho que as empresas de *core* IT não sentiram muito os efeitos da pandemia. Para mim pessoalmente, que já vi muita coisa, foi uma surpresa.

Um aspeto que acho que melhorou significativamente, pelo menos para nós, é que estávamos a fazer investimentos um bocadinho insípidos; temos um polo em Leiria, outro em Viseu, e outro no Porto. Aquilo que sentíamos quer de clientes, quer equipas, não aceitarem muito bem que a pessoa estivesse a 300km ou 200km, atualmente é o mais natural, não há diferença estar no Porto ou Almada a trabalhar, e isso melhorou.

Acho que esta questão de apostar na universidade e politécnicos dão também essa capacidade. Acho que é um fator de esperança sobre esta discussão de como é que vamos desenvolver o interior… é velha receita. Isto desenvolve-se metendo lá a capacidade universitária, a capacidade de fixar as pessoas pelas boas razões. Do ponto de vista de TIC, isso é positivo, mas também do desenvolvimento do país. Esta questão de estarmos mais despertos e recetivos a trabalhar em rede a nível de organizações no país.

A única questão que fica mais em dúvida, do ponto de vista Link, é se a crise vai afetar ou não os grandes clientes dos mercados TIC; por enquanto, isso não se sentiu. Também sinto que nesta área um conselho de administração de uma grande empresa que pense que o primeiro sítio para cortar é eventualmente no IT é um pouco estranho; todos devem sentir que é dos sítios onde se deve investir mais.

Referiu a questão do interior e do recrutamento. Às vezes pode ser um "pau de dois bicos". Toda a gente está remota e vêm os outros de fora buscar os nossos recursos e não precisam de se mudar para outro país. O remoto é o normal. Sentem de alguma forma isso e essa tendência para o remoto melhora ou piora a nossa posição competitiva enquanto país?

Duas coisas que vimos aqui e que se tem mantido, é que quando nós conseguimos entrar na confiança de clientes internacionais – e neste

- José Alves Marques -

momento estamos a manter clientes na Suíça, Emirados Árabes Unidos, na Arábia Saudita, no Gana, em Jerusalém e por aí adiante –, eles aceitam cada vez mais com alguma naturalidade que as equipas de manutenção evolutiva e mesmo equipas de controlo de redes e de infraestruturas estejam deslocadas porque isto pode funcionar assim. Por um lado, há aqui uma oportunidade. Podemos dizer, e como mostrámos durante a pandemia, que isto se consegue fazer a partir de Portugal, com preços mais interessantes com gente muito boa e, reconhecem pelo menos nas geografias mais avançadas da Europa, que temos outra capacidade de encaixar certas coisas.

Outro ponto do que refere e que não sentimos o impacto, mas é muito óbvio, é que realmente uma pessoa pode perder um bocado a cultura ou a ligação emocional à empresa, porque não está ali no dia a dia. Se calhar, se lhe pagarem um pouco mais, prefere ir para outra situação. É um risco que se pode vir a ter. Acho que o problema entre risco e ameaça existe sempre quando temos situações destas, e que as empresas portuguesas devem tomar uma atitude mais agressiva de ir à procura dos mercados.

Não sabemos exatamente quando, mas isto vai passar. Vamos herdar um problema, mas as empresas têm de olhar para a frente. O que é que as organizações deviam estar a fazer?

Acho que as empresas deviam estar a pensar seriamente que os seus ativos principais deviam estar fortemente informatizados. Um ativo principal nas empresas são os seus processos de negócio. Os processos de negócio distinguem uma empresa de outra.

> // AS EMPRESAS NACIONIS PODEM TIRAR PARTIDO DAS GRANDES EMPRESAS, TÊM É DE TER O STREAMLINE DOS SEUS PROCESSOS PARA INTERLIGAR COM ESSES GRANDES HUBS //

Se isto tiver retoma, os processos de negócio vão ter de acelerar, vão ter de ter outro desempenho. Se aproveitarem o momento para o fazer e pensar significativamente, há imensas hipóteses de melhoria, sobretudo, nas pequenas e médias empresas e mesmo nas grandes. Nas grandes, uma coisa que temos visto nos últimos tempos foram muitas iniciativas de automatização de pequenas partes dos processos, como robôs de software, com os mecanismos digitalização, com o *Business Process Management*, mas quando às vezes se analisam o processo *end-to-end*, de uma ponta à outra, o que se percebe é que existiram ilhas que se tornaram melhores, mas não se tornou tudo.

Se as empresas tivessem este ativo como um ativo principal, o otimizassem e o colocassem em suportes informáticos que funcionem bem – isto pode querer dizer estruturar os processos melhor e aplicar-lhes uma automatização de processos, usarem robôs para tarefas inúteis em que têm pessoas a carregar só em teclas e que poderiam ser feitas automaticamente, ter mecanismos inteligentes de digitalização que evitam estar a copiar informação que é inútil – se fizessem esse investimento, quando os processos acelerarem, não só não precisam tantas pessoas para fazerem o *staffing* desses processos, como eventualmente vão até correr melhor, com menos erros, com menos questões de qualidade para os clientes e coisas desse tipo, porque estão num suporte que pode ser mais bem gerido.

Há uma grande mudança de processos, mas as empresas internacionais têm grandes equipas de desenvolvimento, sistemas próprios, tratamento de dados avançado, mas as empresas portuguesas não.

Não vejo as empresas nacionais a competir nessa liga. Mas as empresas nacionais eventualmente podem tirar partido até dessas empresas, têm é de ter o *streamline* dos seus processos modo para ancorar, para interligar com esses grandes *hubs*, que vão ser usados e que vão decidir eventualmente grande parte da comercialização, tem de ter isso bem feito, porque se não conseguirem ligar-se eles, eles não vão desculpar.

Uma coisa é, eventualmente, as empresas não terem a capacidade de ter os mesmos mecanismos e as mesmas estruturas de ir ao mercado, os canais que essas grandes empresas têm; outra é ficar fora desses, nem sequer lá consegue ir porque não conseguem ancorar nessas nessas plataformas porque não vão aceitar funcionamentos abaixo do nível de *benchmark* que têm.

Sentem, no vosso contacto com clientes, o *benchmark* ativo com o que de melhor se faz lá fora, ou ainda estamos na fase do *good enough*?

Depende das empresas. Na Link, a maioria dos clientes são das áreas financeiras, *utilities* e *telcos*. Aí, fazem os *benchmarks* internacionais e têm uma visão do que é que se está a fazer lá fora; podemos estar ao mesmo nível ou não. Depois há as questões de investimento. Quando se desce patamares realmente é muito mais difícil porque muitas delas ainda não estão aí, se bem que começam a ter esses desafios.

Qual deve ser o foco das empresas?

Acho que a parte positiva na parte empresarial é dizer, apesar de tudo, que as empresas se adaptaram e estão, de uma maneira geral, melhor do que as perspetivas que tinham em março. Acho que é muito positivo porque cria uma lógica que acho que é muito a arrepio do pensamento português, que ficamos logo só a pensar no governo. Avançou-se, fez-se e continuou. Isso é muito positivo.

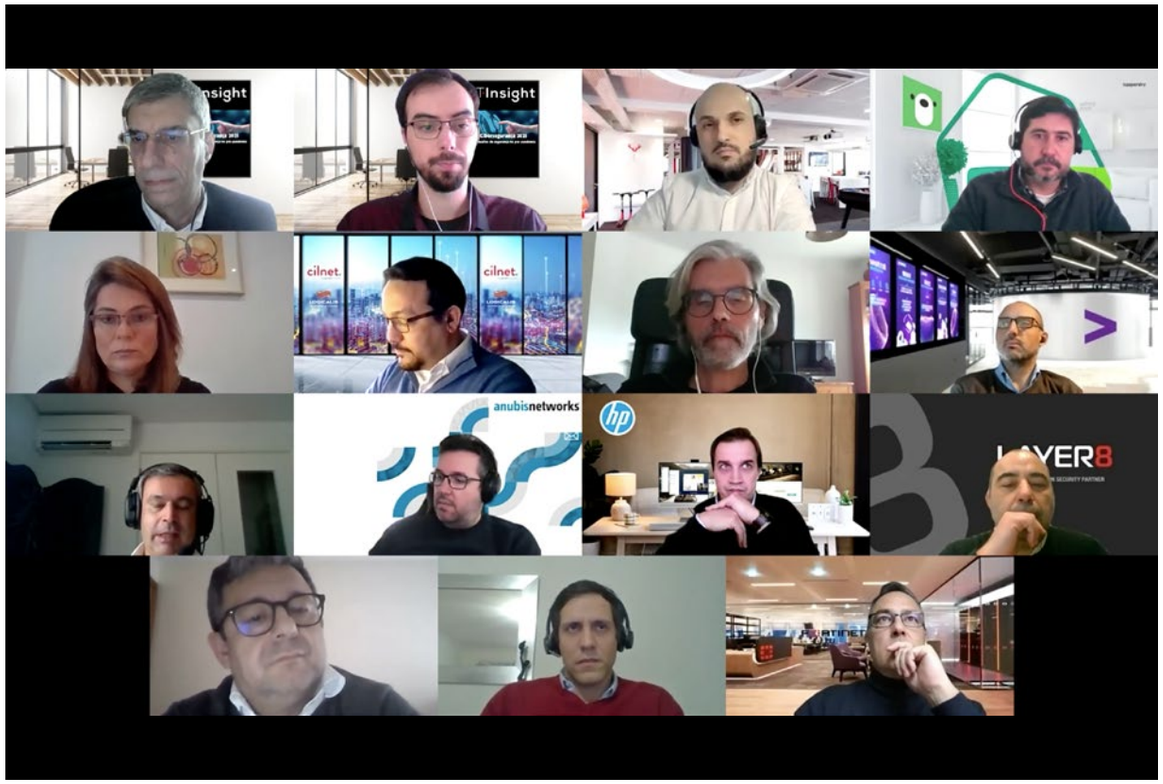
Isto pode ser uma oportunidade para a maior parte das empresas de pensarem realmente que o mundo mudou. Se calhar, andámos sete anos nesta área da digitalização. Como é que vamos tirar partido disso para estar no leque de vencedores, em vez de ficarmos num leque de pessoas que têm um *legacy* que tem de se adaptar a várias coisas que estão no ano passado.

Acho que se devem focar em alguns dos aspetos fundamentais das empresas, que são os seus processos de negócios, estruturação do modo como os fazem, a sua capacidade de interligação informática, esta questão muito falada de que uma empresa que está presa dentro do seu sistema informático, que não tem capacidade de o ancorar, de o ligar a todos estes *players* que vão estar por aí. ■

A CIBERSEGURANÇA DAS ORGANIZAÇÕES É MAIS IMPORTANTE DO QUE NUNCA

Com a transformação digital a acelerar, as organizações devem apostar na cibersegurança, mas, por vezes, acabam por ficar num segundo plano de investimento. Anubis Networks, Accenture, Cilnet, Claranet, Fortinet, HP Inc., IBM, Kaspersky, Layer 8, Nexllence, Noesis, S21sec e Warpcom dão a sua opinião sobre o mercado nacional de cibersegurança.

RUI DAMIÃO



- A IT Insight realizou a sua habitual mesa redonda de forma digital, através de uma plataforma de videoconferência -

A CIBERSEGURANÇA sempre foi importante, mas, depois de os colaboradores começarem a trabalhar a partir de casa, passou a ter outra relevância para as organizações. Num cenário pós-pandémico é, agora, claro que o *workplace* será, sempre que possível, híbrido e móvel.

A responsabilidade de manter as redes seguras, garantir que os sistemas permanecem resilientes contra violações e tomar várias medidas para proteger os dados e a sua integridade de ameaças cibernéticas, é cada vez mais importante, uma vez que os cibercriminosos estão mais ousados nas suas tentativas de invadir os sistemas. Além do mais, a recente pandemia abriu possíveis pontos de brecha que, antes, poderiam não existir na organização.

INVESTIMENTO DURANTE A PANDEMIA

Com os colaboradores a trabalhar a partir de casa, o perímetro de ataque aumentou. Nem todas as organizações estavam preparadas para a realidade e, numa primeira fase, a escolha de investimento não passou necessariamente pela segurança.

O PERÍODO PANDÉMICO OBRIGOU A REPENSAR OS PLANOS DE EMERGÊNCIA E CIBERSEGURANÇA DAS ORGANIZAÇÕES

Pedro Coelho, Computing Area Category Manager da HP Inc., refere que, "para quem olha do ponto de vista dos postos de trabalho pessoais, o que se notou é que o período pandémico obrigou a pensar um pouco melhor quais eram as medidas de proteção. Depois do primeiro impacto em que muitas vezes se ativaram planos de emergência, sentimos – ao longo da segunda metade de 2020 – uma maior preocupação com as questões de segurança e voltou a subir na lista de prioridades dos principais responsáveis de informática".

José Borges Ferreira, CEO da Anubis Networks, indica que "viemos de um mundo muito tradicional onde estávamos habituados a ter a segurança dentro do perímetro. Quando se foi para casa, tudo isso se desmanchou; não havia uma preparação de acessos remotos, de controlo de informação e gestão de acessos. Isso foi a grande diferença do trabalho remoto, não tanto de tecnologia, mas sim de procedimentos. As empresas não estavam organizadas para trabalhar remotamente do ponto de vista de gestão de informação e segurança".

Nuno Baptista, Associate Director e Responsável pela área de Security da Accenture, explica que "há uma necessidade de investir em pessoas especializadas. A complexidade do problema faz com que as organizações tenham muita dificuldade em endereçar todos estes temas. A forma como as empresas encararam o tema difere com a sua maturidade; é um bocado difícil generalizar a forma como as empresas foram impactadas pela pandemia, mas a complexidade é muito grande e nem todas as organizações têm capacidade para o fazer".

INVESTIMENTO ESTRATÉGICO

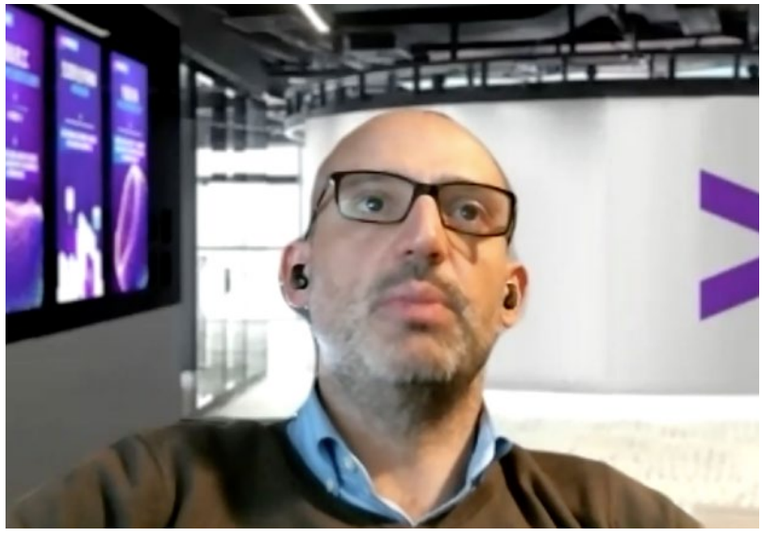
David Santos, BDM de Cybersecurity da Cilnet, afirma que "não existe uma empresa tipo que se consi-

- José Borges Ferreira -
CEO, Anubis Networks

"Os algoritmos vão permitir tomar decisões para algo que não conhecemos"

- Nuno Baptista -
Associate Director, Responsável pela área de Security, Accenture

"Os ataques de engenharia social vão continuar a evoluir e a aproveitar todas as fragilidades"



- Nuno Baptista, Accenture -

- José Borges Ferreira, Anubis Networks -

- David Santos, Cilnet -

ga caracterizar; cada uma tem a sua especificidade. O que temos vindo a verificar é que se começa a ter alguma noção que é preciso apostar na cibersegurança, mas muitos deles sentem-se perdidos porque não sabem por onde começar. Não podemos continuar a manter o diretor de IT a fazer também segurança porque o nível de *skills* são completamente diferentes. Este tipo de transformação é bastante complexo".

David Grave, Senior Cybersecurity Consultant da Claranet, diz que "muitas empresas não tinham os seus processos preparados e tiveram de recorrer em muitos casos aos VPN porque ainda tinham os processos dentro de casa; estas foram as empresas que tiveram mais dificuldade em se adaptar". No entanto, é preciso admitir que "o teletrabalho veio para ficar"; para isso, as empresas não podem viver sem a cloud e sem soluções escaláveis se querem manter o teletrabalho a funcionar de forma segura nas organizações.

Paulo Pinto, Business Develop Manager da Fortinet, menciona que, "se inicialmente as empresas se apressaram a confinar e a arranjar soluções mais pontuais para permitir o trabalho remoto, desde o início deste ano que se nota uma abordagem mais estratégica que se foca no médio e no longo prazo. As empresas procuram ser mais abrangentes e incluir todos os elementos do edge, que estão pendurados na cloud

- David Santos -
BDM de Cybersecurity, Cilnet

"Não podemos continuar a manter o diretor de IT a fazer também segurança porque o nível de skills é completamente diferentes"

- David Grave -
Senior Cybersecurity Consultant, Claranet

"É preciso pensar como é que se asseguram as ligações à cloud que já estão fora da infraestrutura"

O NÚMERO DE VIOLAÇÕES DE DADOS E REGISTOS COMPROMETIDOS ATINGIU O NÍVEL MAIS ALTO EM 2020

e nos pontos remotos, e com o requisito de controlo e visibilidade sobre os dispositivos".

TRABALHO REMOTO

Apesar do crescimento contínuo do investimento em cibersegurança ao longo dos últimos anos, o número de violações de dados e registos comprometidos, assim como ataques de ransomware, atingiu o nível mais alto no ano passado. No entanto, é preciso perceber se este crescimento se deveu ao trabalho remoto apenas, ou se às deficiências na segurança das infraestruturas que já existiam no período pré-pandémico.

António Bacalhau, Senior Security Sales Specialist da IBM, explica que "para além da grande maioria das empresas estar muito focada no tradicional, dentro do perímetro de trabalho, assim que começou o trabalho remoto o perímetro mudou e deixou de ser tão controlado. As organizações deixaram de ter tanta visibilidade dos seus ativos digitais e, assim que isso aconteceu, perderam a capacidade de os monitorizar e, à partida, ficaram mais vulneráveis e aumentaram o risco de ataque".

Élio Oliveira, Territory Channel Manager & SMB da Kaspersky, afirma que existiram "muitas decisões *ad hoc*. Muitas decisões tiveram de ser tomadas com as informações que tinham de uma forma muito rápida e espontânea. Quando falamos em colocar o PC debaixo do braço, levar para casa e começar a trabalhar, só foi necessário porque as empresas tiveram de garantir a continuidade do negócio. Também é preciso olhar para o nosso tecido empresarial e perceber quem é que tem um plano de continuidade de negócio e que empresas não têm".

MUITAS VEZES, NÃO HOUVE TEMPO PARA ADAPTAR OU IMPLEMENTAR PROCESSOS E FERRAMENTAS DE CIBERSEGURANÇA

Fernando Cardoso, COO da Layer 8, refere que, "de facto, existiu um aumento de ciberataques feito por cibercriminosos que são oportunistas; aproveitam um momento de maior fragilidade e incerteza para nos atacarem. Acho que ninguém tem dúvidas que a maioria dos ataques não são direcionados a sistemas, mas às pessoas; quando as pessoas estão mais frágeis e a viver momentos de maior incerteza, é aí que os atacantes conseguem ter mais êxito. Houve um aproveitamento do que está a acontecer para criar várias campanhas de cibercrime".

FRAGILIDADES ANTIGAS

Alexandre Costa, Head of Industry Executive da Nexllence, indica que, "em casa, o nível de segurança é muito mais baixo do que numa empresa. Notámos foi um aumento exponencial de vendas de licenciamento de VPN o que mostra que a maior parte das empresas em Portugal não estavam preparadas para esta mudança repentina. Há vários tipos de empresas que têm infraestruturas críticas para o Estado tem um nível de maturidade de segurança superior que a maioria do tecido empresarial português não tem".

Nuno Cândido, Infrastructure Solutions Senior Manager da Noesis, diz que "um grande número de ataques do ano passado não se deu apenas por causa da pandemia ou ao facto das pessoas trabalharem remotamente, mas a um conjunto mais diverso de fatores. Em termos de segurança, não houve tempo para adaptar ou implementar processos e ferramentas que permitissem suportar esta mudança tão repentina; tem de existir prioridades e isso levou a que as empresas ficassem mais desprotegidas, causando mais ataques".

Carla Zibreira, Head of Consulting da S21sec, menciona que "não houve uma alteração do contexto de risco; o que houve foi uma alteração brutal do ecossistema de riscos das organizações perante o cenário da pandemia. A pandemia trouxe alterações muito específicas – nomeadamente nos processos de negócio e à forma como são desempenhados e implementados. Isto veio alterar o equilíbrio dos vários riscos e da probabilidade que os riscos tinham de acontecer. Também existiu pouca preparação das organizações para responder a estes riscos".

- Paulo Pinto -
Business Develop Manager, Fortinet

"A automação e o machine learning vão ter um papel primordial no apoio às equipas de cibersegurança"

- Pedro Coelho -
Computing Area Category Manager, HP Inc,

"Quem está a pensar em como se vai proteger deve considerar em se proteger para o que existe e para o que não existe"

O TEMA DA PANDEMIA FOI UM DOS TEMAS MAIS UTILIZADOS PARA REALIZAR CIBERATAQUES CONTRA OS COLABORADORES DAS ORGANIZAÇÕES

EVOLUÇÃO DAS CIBERAMEAÇAS

Ao longo dos anos, as ameaças foram evoluindo. As empresas e os utilizadores já não têm de se preocupar com o 'simples' vírus informático, mas sim com uma miríade de ciberameaças cada vez mais complexas.

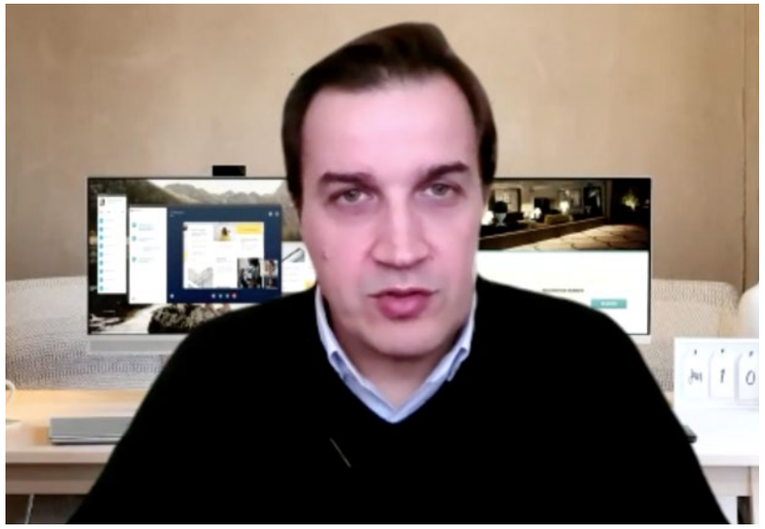
Nuno Baptista, da Accenture, explica que "os ataques de engenharia social, o phishing, vão continuar a evoluir e a aproveitar todas as fragilidades acrescidas que as pessoas têm sentido. Por outro lado, vemos que as táticas, as técnicas e os procedimentos dos atacantes estão a evoluir, ameaçando muito a continuidade do negócio. Vemos ataques direcionados e muito sofisticados que colocam em risco os dados da organização; antigamente, via-se a encriptação dos dados, mas agora vemos a exfiltração dos dados".

Bruno Gonçalves, Business Unit Manager – Cybersecurity & Public Safety da Warpcom, afirma que "todos os dias nos deparamos com ataques mais sofisticados e avançados e com um impacto brutal para as organizações. Atualmente, a indústria responde tendo em conta a sua maturidade. Dependendo dos setores e das organizações, há quem tenha uma maturidade grande e uma perceção do risco, analisando e percebendo as ameaças que existem para criar controlos efetivos para dar resposta, mas uma grande parte das organizações ainda não tem esta maturidade".

Focando-se nos emails, José Borges Ferreira refere que, "às vezes, o aumento da sofisticação é contraprodutivo; as coisas simples funcionam. A evolução passa por mecanismos de machine learning que permitam ler e analisar o conteúdo do email para perceber se o que está nos anexos são ameaças ou não. É preciso subir o jogo onde estes processos automáticos permitem, também, criar algumas

- David Grave, Claranet -

- Paulo Pinto, Fortinet -



- Pedro Coelho, HP Inc -

- António Bacalhau, IBM -

defesas" contra as ameaças que chegam às organizações diariamente.

FOCO NO UTILIZADOR

David Grave, da Claranet, indica que "nem todas as clouds são iguais; podemos estar num cloud provider de excelências e as configurações não serem as melhores. Gerir uma infraestrutura *on-premises* é muito diferente de gerir uma infraestrutura na cloud. A cloud não é simplesmente pegar nos nossos servidores, virtualizá-los e fazer a transposição para a cloud. É preciso pensar como é que se asseguram as ligações à cloud que já estão fora da minha infraestrutura; não posso apenas colocar uma firewall à frente dos servidores".

Paulo Pinto diz que "com a capilaridade das redes, com os *smart devices* que se usam e com os sistemas que já temos em casa, há uma maior porta de entrada. O que se coloca em casa é vantajoso, mas é uma porta de

MINIMIZAR OS RISCOS DE UM CIBERATAQUE É UMA PRIORIDADE PARA A MAIORIA DAS ORGANIZAÇÕES MUNDIAIS

entrada muito grande para se conseguir um conjunto de informações sobre o sujeito para depois ou tentar entrar dentro destes dispositivos, ou saltar para os dispositivos corporativos. Isso é uma das portas mais capilares para entrar atualmente e que é difícil de contornar porque não é uma questão tecnológica".

David Santos, da Cilnet, menciona que "as coisas estão cada vez mais específicas. O diferente tipo de ataque existente ou é o direcionado para a empresa, ou é através de phishing. No entanto, é preciso não esquecer que a entrada de qualquer ataque ou é de dentro para fora ou de fora para dentro e as medidas que temos de tomar têm de ser completamente diferentes. A primeira capacidade onde todas as empresas devem atuar é a formação ao utilizador; é preciso dotar todos os colaboradores de todos os tipos de ataques existentes".

Pedro Coelho aponta que "nestas questões da segurança, são sempre bem-vindos conceitos como sobreposição de várias camadas de proteção; a redundância acaba por ser bem-vinda nesta ótica da segurança. Outro conceito que faz sentido é planear para o pior cenário; se estivermos a planear para o pior cenário, estamos muito mais bem preparados para todos os outros. Quando se fala em evolução das ciberameaças, quem está a pensar em como se vai proteger deve considerar em se proteger para o que existe e para o que não existe".

MINIMIZAR OS RISCOS

Um estudo realizado por uma empresa do setor de cibersegurança indica que 51% das empresas consideram que minimizar os riscos de ciberataque são uma prioridade para as organizações mundiais.

- António Bacalhau -
Senior Security Sales Specialist, IBM

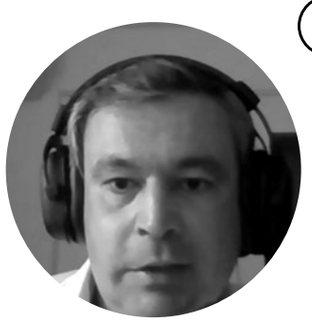
"As empresas estão mais conscientes dos impactos financeiros e reputacionais que os ataques podem ter"

- Élio Oliveira -
Territory Channel Manager & SMB, Kaspersky

"Muitas decisões tiveram de ser tomadas com as informações que tinham de uma forma muito rápida e espontânea"

- Fernando Cardoso -
COO, Layer 8

"A maioria dos ataques não são direcionados a sistemas, mas às pessoas"



- Alexandre Costa -
Head of Industry Executive, Nexllence

"DevSecOps é vetor de investimento muito forte nas empresas que têm uma maturidade maior em cibersegurança"

É EXPECTÁVEL QUE O RANSOMWARE CONTINUE A SER UMA AMEAÇA PARA AS ORGANIZAÇÕES

Fernando Cardoso afirma que "tudo tem a ver com a maturidade que as empresas têm e, de certo modo, a apetência ao risco. Quando fazemos bem o nosso trabalho em cibersegurança, os nossos sucessos são invisíveis; quando falhamos, o nosso trabalho é altamente visível. Ou há esta maturidade para a cibersegurança, ou as empresas só acordam para a prioridade de minimização de riscos quando algo acontece e as ciberameaças estão a evoluir a um bom ritmo, também com a massificação da utilização de dispositivos".

António Bacalhau sente que "há uma estabilização dentro do 'novo normal'. As empresas estão mais conscientes dos impactos financeiros e reputacionais que os ataques podem vir a ter dentro das suas organizações. Temos vindo a assistir a uma transformação digital quase global na maioria das empresas. No entanto, é preciso mostrar às empresas como se deve investir em cibersegurança; acho que a aproximação correta é que conseguimos fazer uma gestão completa, mas é preciso explicar como devem investir o seu *budget* em cibersegurança".

Pedro Coelho (HP) indica que, "em termos de investimento nesta área, é preciso ter uma abordagem estruturada que terá de começar pelos *endpoints*. Os próprios dispositivos IoT podem ser veículos de propagação de ameaças" e também devem ser protegidos. "Temos de nos preparar para um cenário em que o ransomware continuará a ser uma realidade muito pertinente, não só na ótica de exfiltração de dados, como também aliado aos desafios que o RGPD coloca, com o perigo desses dados se tornarem públicos".

INVESTIMENTO ESTRUTURADO

Alexandre Costa refere que, "este ano, tem existido um forte investimento em *Security-as-a-Code*, no-

meadamente na parte de DevOps. Os clientes procuram automatizar o processo de DevSecOps, que é uma área que traz grandes vantagens não só na parte de perímetro, mas também na parte de desenvolvimento de software e a segurança de software e API. Este é um vetor de investimento muito forte nas empresas que têm uma maturidade maior na área de cibersegurança".

Nuno Cândido, da Noesis, revela que "o mercado nacional ainda está atrás do mercado internacional. No entanto, temos assistido a um aumento significativo da prioridade do investimento em cibersegurança. Também vejo que temos um país que navega a várias velocidades, ou seja, as grandes empresas têm consciência e investimento de forma estruturada, e depois temos o mercado mais baixo em que a situação é muito diferente e onde é preciso um amadurecimento para que seja possível implementar processos eficazes".

Élio Oliveira nota que "há uma intenção das empresas para minimizar o impacto dos riscos e procuram proteger-se contra ameaças externas. Mas, até à data, as coisas têm sido feitas um pouco *ad hoc*. As empresas começam a olhar para a cibersegurança com uma estratégia já identificada. Enquanto fabricantes, temos o papel de evangelizar os clientes e explicar as necessidades que existem e porque se deve ir por um determinado caminho, porque é que é importante, por exemplo, a resposta automática a incidentes, entre outros".

- Élio Oliveira, Kaspersky -

- Fernando Cardoso, Layer 8 -

- Alexandre Costa, Nexllence -

AINDA QUE A INTELIGÊNCIA ARTIFICIAL NÃO SEJA ALGO NOVO, SÓ AGORA É QUE ESTÁ A SER UTILIZADA REGULARMENTE EM CIBERSEGURANÇA

INTELIGÊNCIA ARTIFICIAL

A Inteligência Artificial (IA) é cada vez mais utilizada em todo o IT. Na cibersegurança, terá um papel fundamental tanto para quem defende, como para quem ataca.

Carla Zibreira explica que "começamos a olhar para a inteligência artificial como uma solução que nos vai ajudar na capacidade de inteligência e na interpretação dessa inteligência ao nível da segurança, para além de ajudar na análise de informação massiva, por exemplo, de malware. Este tipo de ferramentas têm sido implementadas nesse sentido, no apoio e na ajuda" que podem dar às equipas de cibersegurança das organizações. Por outro lado, ainda se está a perceber o real alcance que estas ferramentas podem ter na proteção das empresas.

Bruno Gonçalves diz que "esta nova realidade de machine learning e inteligência artificial já começa a ser utilizada como ferramenta para ataques e defesa. Traz uma nova realidade para nós, será um novo desafio. Antes de chegarmos à parte de conseguir responder, temos de ganhar visibilidade e isso é um caminho que tem de ser feito. Vamos precisar de ganhar rapidamente maior visibilidade daquilo que está a acontecer dentro da infraestrutura das organizações e são precisas tecnologias que permitam suportar esta resposta".

António Bacalhau (IBM) indica que "a inteligência artificial já não é uma coisa nova. Há 20 anos, já programávamos sobre isso; não havia era capacidade. A cloud e o preço do *data storage* a baixar aumentou bastante esta capacidade. O que acontece é que à medida que os ataques cibernéticos têm vindo a aumentar, tem aumentado o volume e a complexidade dos mesmos. A inteligência artificial vai ajudar as operações de segurança – principalmente as que têm menos recursos – a ficarem à frente dessas ameaças".

APOIO ÀS EQUIPAS

Nuno Baptista (Accenture) afirma que "a inteligência artificial e o machine learning são um suporte daquilo que fazemos atualmente – e vamos continuar a fazer – não só na cibersegurança, mas também de uma forma mais transversal. Ao nível das pessoas e dos processos, tudo o que é análise comportamental

- Nuno Cândido -
Infrastructure Solutions Senior Manager, Noesis

"Temos assistido a um aumento significativo da prioridade do investimento em cibersegurança"

- Carla Zibreira -
Head of Consulting, S21sec

"Houve uma alteração brutal do ecossistema de riscos das organizações perante o cenário da pandemia"

relativamente à forma como utilizamos os dispositivos e os dados, gera tanta informação que a única forma de a trabalhar é com tecnologias de machine learning e inteligência artificial que nos permitem prever comportamentos potencialmente perigosos e atuar em conformidade".

David Santos (Cilnet) refere que "é cada vez mais utilizado pelos atacantes a orquestração e o machine learning. Prevejo que, num curto espaço de tempo, vão ser submetidos no mercado produtos com novos mecanismos de defesa. Se contabilizarmos de tempo, a utilização destes mecanismos pelos atacantes não serve mais do que para primeiro orquestrarem, e depois fazer uma redução substantiva do tempo. Se utilizarmos os métodos tradicionais, será completamente impossível colmatar seja o que for deste tipo de ataques".

Paulo Pinto (Fortinet) diz que "no contexto das infraestruturas digitais e no posicionamento no ciberespaço, as pessoas, por si próprias, não vão ser capazes de lidar com a quantidade de alertas que vão chegar dos diversos sistemas. De uma forma muito simples, a automação e o machine learning vão ter um papel primordial no apoio às equipas de cibersegurança. A forma como vai ser aplicado exige cuidado porque estes algoritmos precisam de uma grande quantidade de dados para que possam produzir informação prática".

David Grave (Claranet) explica que "é necessário esse poder de computação para analisar a quantidade e a qualidade dos dados. Podemos treinar os elementos cognitivos, mas são precisos dados de qualidade. Isto é crítico. Para os clientes mais pequenos, é preciso dar acesso a esse poder de computação para ter acesso a uma enorme quantidade de dados que o cliente, de outra forma, não teria. A inteligência artificial é um serviço para os analistas altamente especializados que vão passar a ter informação de qualidade para trabalhar".

TENDÊNCIAS PARA 2021

Com um mundo em constante mudança, muitas são as tendências que existem à volta dos sistemas de informação. Na cibersegurança não é exceção e as organizações devem adaptar-se a novas realidades neste segmento.

Nuno Cândido (Noesis) refere que "se vai dar continuidade à adaptação à realidade de teletrabalho e são esperados investimentos em soluções empresariais para dar resposta a este novo paradigma. Creio que as PME vão ter de aumentar bastante o investimento em cibersegurança; muitas delas tiveram de aumentar a sua exposição online e o segundo passo é começarem a sofrer ataques, perdas de negócio, e terão de começar a ter muita atenção à questão da segurança".

Alexandre Costa (Nexllence) explica que "as principais tendências continuam a ser os ataques de ransomware, de DDOS e de *Advanced Persistent Threats*. A dark web irá permitir cada vez mais aos cibercriminosos aceder a dados sensíveis de redes das organizações. Acho que vão continuar a existir cada vez mais produtos e serviços de segurança que vão trazer uma gestão mais complexa às corporações. Depois, as próprias fusões e aquisições nesta área vão ser uma tendência nos próximos anos".

- Nuno Cândido, Noesis -

- Carla Zibreira, S21sec -

José Borges Ferreira (Anubis Networks) menciona que, "ao longo dos anos, a evolução de classificação de eventos foi interessante. Passámos da evolução simples, para a classificação com machine learning com base nos dados recolhidos, para as redes neurais onde já não é preciso um grande *data set* de treino. São estes algoritmos que nos vão permitir tomar decisões para algo que não conhecemos. Estamos a tentar prever o que vem por aí, mas devemos estar preparados para o que não conhecemos".

- Bruno Gonçalves, Warpcom -

FOCO NO *ENDPOINT*

Élio Oliveira (Kaspersky) afirma que "é preciso haver um foco no *endpoint*, e não falamos apenas na componente do antivírus, mas numa componente mais avançada como a resposta automática a incidentes, o vulgo EDR. Depois, também é preciso consciencializar os utilizadores, o *awareness*, para os perigos da cibersegurança. A autenticação multifator e o acesso à cloud vão ser tendências no mundo da cibersegurança nos próximos anos".

Fernando Cardoso (Layer 8) indica que "as tendências para 2021 vão estar intimamente ligadas à pandemia e ao paradigma de teletrabalho. Vão acontecer mais ataques nos computadores e redes domésticas, onde os criminosos vão utilizar esses equipamentos para saltarem para as redes empresariais ou para as clouds onde os utilizadores estão ligados. Terá de existir, necessariamente, um investimento maior na segurança do *endpoint*, dos EDR e em abordagens *zero trust*".

Bruno Gonçalves (Warpcom) diz que "este ano vamos continuar a assistir e o foco será criar mais resiliência. As organizações vão estar focadas em criar mais resiliência nas suas infraestruturas que toca em vários pontos: no *awareness* dos colaboradores, num maior controlo dos processos, nos *endpoints* e na gestão de identidades. Por último, é a questão das redes quânticas que vai trazer uma nova realidade e uma nova capacidade para os atacantes".

Carla Zibreira (S21sec) refere que "a pandemia veio transformar a forma como as organizações fazem aquilo que é o seu negócio e, como tal, há uma maior exposição por parte desses processos à Internet. Aí, o *compliance* – ao contrário do que inicialmente se podia pensar – não aligeirou e as reguladoras continuaram atrás das empresas, a exigir o cumprimento dos *timings*, a certificação ou a entrega de evidências de cumprimento em relação a um *framework*. Quando falamos em segurança também falamos em confiança; quando viramos o negócio para o exterior, essa é a palavra-chave". ■

- Bruno Gonçalves -
Business Unit Manager – Cybersecurity & Public Safety, Warpcom

"Todos os dias nos deparamos com ataques mais sofisticados com um impacto brutal para as organizações"

accenture

O NOVO PANORAMA DA SEGURANÇA NA CLOUD

O período pós-pandémico trouxe consigo uma mudança radical de paradigma para a cibersegurança. Nuno Cerdeira Baptista, Associate Director responsável pela área de Security da Accenture Portugal, delineia o atual panorama de cibersegurança e de que forma as organizações podem responder a estes novos desafios.

Como é que a pandemia mudou o panorama da cibersegurança?

No que diz respeito às organizações e para aquelas que tiveram de efetuar uma transição forçada para trabalho remoto, o panorama da cibersegurança, sem dúvida, que mudou. O aumento da superfície de ataque, agora estendida a dispositivos e redes domésticas, criou novos e difíceis desafios para as organizações que não estavam preparadas. E a grande questão parece-nos ser mesmo a da preparação, pois a forma como as organizações abordam a gestão de identidades e de dispositivos veio condicionar, em grande medida, a sua preparação para poderem fazer, ou não, uma transição efetiva e segura para o trabalho remoto. Mais do que falar de VPNs ou simplesmente de tecnologia, é preciso falar de como é que uma identidade é encarada e gerida pela organização, pois com a estratégia adequada é possível abordar trabalho, em escritório ou remoto, exatamente da mesma forma.

De que forma é que as empresas estão de momento a responder a estes novos desafios?

Depende do estado de maturidade da cibersegurança e necessidades de cada empresa. Estamos, por isso, perante dois tipos de organizações: as que estavam preparadas para os desafios da pandemia em termos de maturidade tecnológica e de cibersegurança, sendo que nestes casos trata-se apenas de continuar a desenvolver a estratégia existente e, eventualmente, reforçar as componentes de prevenção e resposta a incidentes adaptadas ao ambiente da pandemia; e, em segundo lugar, as organizações que não estavam preparadas para estes desafios, como por exemplo, o trabalho remoto em escala e, nesse caso, a capacidade de resposta será, sobretudo, reativa e de gestão de crise, sendo que a dificuldade vai estar relacionada com a capacidade de adaptação da estratégia à nova realidade, que vai ser influenciada por recursos disponíveis, quer ao nível das pessoas, quer ao nível do investimento.

Como é que a Accenture está a ajudar as empresas a enfrentar esta situação?

A par de projetos mais tácticos e pontuais, o nosso principal objetivo para com os clientes é o aumento da sua ciber-resiliência através da transformação dos programas e estratégias de cibersegurança das organizações, no sentido de os adaptar à realidade atual e ao que se perspetiva que seja a realidade futura. Esta ajuda parte muitas vezes de uma análise inicial que permita perceber e fazer benchmarking do estado de maturidade atual da organização.

Como prevê que esta situação evolua no futuro próximo, e quais deverão ser as prioridades das empresas para garantir a segurança e continuidade de negócio?

Por um lado, o fator humano, em que ataques de engenharia social como o phishing vão continuar a evoluir e a aproveitar a fragilidade acrescida das pessoas nestes tempos conturbados. Por outro lado, as táticas, técnicas e procedimentos dos atacantes estão a evoluir, ameaçando a continuidade dos negócios numa altura em que a mesma já foi ameaçada pela disrupção causada pela pandemia.

Ataques direcionados e sofisticados combinados com ransomware colocam em risco não só a continuidade do negócio mas também os dados da organização, pois se antes o foco destes ataques estava no resgate propriamente dito, atualmente tem estado na remoção de dados críticos da empresa como forma adicional de chantagem, levando as organizações a pagarem o resgate, não para recuperar os dados, mas para evitar que sejam divulgados.

O aumento da superfície de ataque devido ao trabalho remoto vem potenciar um movimento dos atacantes para a cloud, fazendo com que a adoção de uma estratégia de cloud segura seja de extrema importância, especialmente considerando que as competências necessárias ao nível de segurança da cloud são diferentes quando comparadas com as de gestão de infraestruturas mais tradicionais. ■

anubisnetworks

POR JOSÉ BORGES FERREIRA
CEO, Anubisnetworks

O (SEU) ECOSSISTEMA DE E-MAIL ESTÁ SOB ATAQUE

Todas as empresas são diariamente atacadas por Cibercriminosos. Informando-se e agindo sobre o seu ecossistema de e-mail, terão mais possibilidades de se defenderem.

OS CIBERATAQUES, por motivos financeiros, geopolíticos, por dano (*hackers*, mas também, por exemplo, funcionários descontentes), e por motivos de espionagem industrial privada e soberana, são, obviamente, a ação que causa a reação – o investimento em cibersegurança motivado pelas empresas que estão muito mais informadas e, muitas delas, sofreram já com ataques bem sucedidos – implicando perda de dados privados, perdas económicas diretas, e indiretas – por dano de reputação e pelos custos da recuperação dos sistemas afetados.

De todos os tipos de ciberataques, o *e-mail é um denominador muito comum*, e em dois aspetos:

• **A parte de fraude** (recorrendo a engenharia social), onde se "enganam" as vítimas, simulando ser outra pessoa ou entidade, por forma a que a vítima tome determinada ação (por exemplo, fornecer informação, abrir um documento, clicar num link, fazer uma transferência bancária).

• **A parte tecnológica**, quase sempre associada a engenharia social, e que implica enviar o e-mail de modo a que este pareça legítimo na sua origem e intenção, podendo conter links, imagens, ou anexos maliciosos. O malware que posteriormente é despoletado cumpre outras funções – por exemplo ransomware e spyware, ou facilitar a entrada de outro malware.

A taxa de sucesso destes ataques varia do residual (atacantes pouco inspirados, que enviam spam massivamente) ao quase garantido, bastando que os ata-

- José Borges Ferreira -
CEO, Anubisnetworks

cantes (e existem equipas altamente proficientes no mundo) se dediquem a dirigir o ataque para determinada(s) pessoa(s) (aprendendo os seus hábitos, perfil social, e acessos) e / ou sistema(s) (descobrindo as vulnerabilidades do software e dos processos humanos). Seja como for, a atividade é lucrativa (estima-se um retorno médio *de quase 1500%*) ou não estivesse a aumentar ano após ano (em 2020, os *ataques de phishing terão aumentado 350%*).

Cruzando a escalada de ataques que vivemos com a enorme dependência, agudizada pela pandemia, relativa aos sistemas tecnológicos de comunicação (com destaque para o e-mail) – não é incomum existirem empresas a investir fortemente na sua proteção. Este investimento assenta (ou deve assentar) em:

• **Recursos Humanos** Melhor formação de segurança (e contínua), melhor disciplina de trabalho, e uma postura de "Zero Trust" (tudo pode ser perigoso) face a comunicações externas, mas também internas (o número de *Insider Threats* continua a crescer!), evitando, por exemplo, divulgar informação institucional ou pessoal que pareça desnecessária, suspeitar de ações demasiado proveitosas ou rápidas, e tentar perceber o potencial de fraude em cada comunicação recebida – por exemplo marcações para chamadas de videoconferência com um anexo que afinal esconde malware (*o Zoom foi mesmo a empresa mais "Brand Impersonated" de 2020*).

• **Processos** Uma cultura empresarial que balanceie agilidade com o rigor da segurança (por exemplo: utilizar sempre VPNs ou autenticação multifator para acessos corporativos, não solicitar operações bancárias por e-mail ou IM sem outro tipo de confirmação, não partilhar credenciais, manter um DPO ativo).

• **Tecnologia** Assegurar que quaisquer sistemas possuem funcionalidades inerentes de segurança (por exemplo: *auditing*, controlo de acessos, encriptação de dados), e dotar a organização com múltiplos sistemas de segurança, complementares e, de preferência, redundantes em termos de fabricante, nações de origem e geografias – recentemente, diversos ataques a empresas tecnológicas (por exemplo, à Solarwinds, com acesso a dados de milhares dos seus clientes, incluindo *empresas de cibersegurança*) demonstram que nenhum sistema é autónomo na sua segurança. O maior exemplo de complementaridade de segurança vem do Exchange / O365 e do Google Workspace – ferramentas críticas de trabalho – com diversos componentes de segurança – mas que, dada a predominância no mundo empresarial, são os maiores alvos mundiais de ataques direcionados, explorando constantemente as suas vulnerabilidades e funcionalidades (nomeadamente as funcionalidades "*cross-app*", como linkar e abrir ficheiros) – não é incomum as empresas mais sofisticadas criarem "camadas de segurança" sobre estes sistemas, ativando segurança de e-mail, VPNs, Firewalls, ou arquivos de dados, que possam em conjunto mitigar mais ameaças, afastando-se assim do oportunismo dos atacantes – que tendem a explorar os ecossistemas mais expostos e mais populares. ■

www.anubisnetworks.com/contacts

cilnet. a Logicalis company

POR DAVID SANTOS
BDM de Cybersecurity,
Cilnet a Logicalis Company

– RUMO À SEGURANÇA DE IOT –

O ano de 2020 foi profundamente marcado pela situação pandémica e pelo seu consequente impacto na continuidade dos negócios, e nos ambientes de segurança das organizações. Este cenário, combinado com diversos avanços tecnológicos sugere algumas tendências de segurança, que esperamos ver refletidas nos próximos 24 meses.

À MEDIDA QUE AS ORGANIZAÇÕES abraçam o IoT por questões de eficiência e evolução dos próprios negócios, é crucial que haja uma consideração abrangente de todas as implicações de segurança.

É por isso expectável que a relação da Segurança com o IoT seja cada vez mais indissociável e que estas três *trends* que apresentamos de seguida, venham para ficar:

1: Proteção da tecnologia operacional (OT)

O nível de risco cibernético em ambientes industriais vai continuar a crescer, fazendo com que os diferentes departamentos e responsáveis tomem medidas mais avançadas, de modo a proteger a rede operacional (OT). Será necessário ter uma postura mais ousada para as novas ameaças, pois será imperativa a validação da existência de *backdoors*, ou outro tipo de vulnerabilidades. O fornecimento de acessos remotos para a atualização de sistemas, máquinas e dispositivos ou outras operações, deverão ser considerados numa nova estratégia. O sucesso das boas práticas e melhoria da proteção das redes operacionais só vai funcionar em harmonia com a rede IT.

Qual será o resultado esperado?

As empresas vão necessitar de soluções que por um lado aumentem a proteção, e por outro reduzam o risco associado, tendo ao mesmo tempo de responder às necessidades das redes IT e OT onde a visibilidade terá um papel preponderante.

- David Santos -
BDM de Cybersecurity,
Cilnet a Logicalis Company

2: Operações remotas

Com o aumento da necessidade de **resiliência operacional,** torna-se imperativa a implementação de operações remotas e autónomas.
As mudanças que surgiram em 2020 estão a levar as organizações a utilizarem cada vez mais tecnologias IoT com vista à resiliência operacional. Afinal, os elementos que compõem o IoT ajudam a manter uma empresa em funcionamento quando as pessoas não estão presentes, ao mesmo tempo que ajudam a melhorar a segurança e a eficiência, evitando visitas desnecessárias aos diferentes locais e reduzindo a movimentação dos colaboradores às instalações.
Veremos de 2021 em diante mais implementações destinadas a operações remotas sofisticadas, que vão incluir controlos operacionais autónomos para partes de um processo operacional. Todos os novos *use cases* vão carecer de dados instantâneos e de forma massiva, exigindo uma rede que possa não só suportar essa quantidade de dados, mas ainda entregar a velocidade necessária para análise.
A classe de rede industrial deverá: fornecer maior largura de banda; latências próximas a zero; suportar computação avançada; dotar-se de segurança e escala para se adaptar rapidamente (garantindo a operacionalidade do negócio).

3: Gestão tecnológica de acesso múltiplo

As organizações vão operar tecnologias de acesso múltiplo para obter agilidade e flexibilidade operacional. Embora a Ethernet sempre tenha sido a base para a conectividade em espaços **IoT industriais,** essa conectividade está a ser expandida rapidamente para o *wireless*. A tecnologia sem fios fornece versatilidade para atualizar, implementar e reconfigurar a rede com menos tempo de inatividade. As tecnologias *wireless* mais recentes, como o **Wi-Fi 6** e **LoRaWAN**, também potenciam *use cases* que não eram possíveis no passado (ou possíveis apenas com conectividade com fio). Conforme as organizações expandem as suas implementações de IoT, a necessidade de gerir várias tecnologias de acesso vai aumentar.

A CONFIANÇA NO IOT, ATRAVÉS DA SEGURANÇA

A confiança é absolutamente essencial, não apenas para que os processos de transformação digital possam ter êxito e ser otimizados, mas também para retirar o máximo partido das tecnologias de IoT.
A Cilnet a Logicalis Company disponibiliza soluções que ajudam as organizações a melhorar a conectividade, a obter melhores *insights* e a potenciar os seus serviços, de forma segura.

Para mais informações e para saber como podemos ajudar a sua organização, fale com o nosso especialista: *david.santos@cilnet.pt* ■

claranet

POR DAVID GRAVE
Cybersecurity Consultant,
Claranet Portugal

O PODER DA AUTOMAÇÃO NA CLOUD AO SERVIÇO DA CIBERSEGURANÇA

A adoção dos microserviços pode fazer toda a diferença na hora de as organizações pensarem numa solução de cibersegurança robusta para a cloud, como forma de proteger os seus serviços disponibilizados online.

COM A COMPLEXIDADE crescente das aplicações que suportam os serviços online disponibilizados por empresas das mais diferentes áreas de atuação, torna-se cada vez mais importante a gestão dessa complexidade do ponto de vista do *deploy*, da atualização dos sistemas e, claro, da sua segurança.

Neste contexto, uma das abordagens que tem ganho relevância na agilização desses processos é a implementação de microserviços, recorrendo a *containers* e à metodologia SecDevOps, possíveis com a evolução de uma SOA (Service Oriented Architecture) suportada nos vários operadores de cloud.

Em termos práticos, ao dividirmos estas soluções complexas em conjuntos de microserviços que correm os seus próprios processos em *containers* isolados, mantendo a integridade dos seus dados e comunicando entre si por API's, podemos fazer o *deploy* e a atualização independente e automatizada de partes individuais das aplicações de suporte ao negócio.

Isto permite endereçar vários desafios que as empresas encontram de forma recorrente – concretamente implementar e atualizar aplicações cada vez mais complexas, responder rapidamente a funcionalidades requeridas pelo negócio mantendo elevados padrões de segurança, sem perder flexibilidade e capacidade de usar diferentes tecnologias. Adicionalmente, a divisão em

- David Grave -
Cybersecurity Consultant,
Claranet Portugal

microserviços possibilita da mesma forma escalar rapidamente a operação, através do *deploy* de várias destas instâncias de forma totalmente *automatizada*.

MAIS TRANSPARÊNCIA, MAIOR SEGURANÇA

Embora esta abordagem possa parecer complexa, a realidade é que, com a adoção que estas soluções estão a ter, assistimos a um desenvolvimento acelerado de ferramentas que permitem fazer uma gestão transparente para o cliente em modelos de Software-as-a-Service (SaaS), ou Containers-as-a-Service (CaaS). Tal é possível, por exemplo, recorrendo a *Kubernetes*, *Containers* e adotando metodologias SecDevOps, assentes nas melhores práticas de *cibersegurança* durante os processos de desenvolvimento e *deployment*.

A conjugação de todas estas soluções permite a adoção de políticas de segurança mais flexíveis e precisas, que podem ser atribuídas até o nível do *workload*. E esta granularidade garante que os cibercriminosos encontrarão potencialmente menos vulnerabilidades para explorar, apesar do aumento teórico da superfície de ataque.

REBUILD AUTOMÁTICO

Exclusivamente do ponto de vista da segurança, é enorme a diferença para os modelos *legacy* baseados nas aplicações cliente-servidor, assentes em máquinas dedicadas nos data centers. E isto porque falamos de máquinas que requerem constante atenção, processos permanentes de *patching* e em que, muitas vezes, qualquer intervenção implica um *downtime* para o negócio – e que são maioritariamente o alvo primário e persistente dos cibercriminosos.

Ao migrarmos para um modelo em que a sua flexibilidade e eficiência permitem fazer o *rebuild* diário automatizado, a partir de código de todo o *footprint* visível – por exemplo, eliminando a persistência de um ataque e limitando o mesmo à vida útil de um *container* – conseguimos um processo realmente disruptivo: não só do ponto de vista das operações e da cibersegurança, mas também do próprio negócio.

Deste modo, a conjugação de SecDevOps, *containers* e microserviços, associados ao poder da automação na cloud, garantem alta disponibilidade e um incremento significativo da resiliência, escalabilidade e segurança, permitindo que os objetivos do negócio sejam atingidos de forma mais eficiente.

Resta às organizações adotarem uma abordagem holística na escolha deste tipo de solução, bem como na escolha do *Service Provider* que fará a gestão da cloud a todos os níveis. Apenas com um olhar transversal sobre todo o *workload* de uma empresa será possível implementar as melhores soluções de compartimentação, de acordo com as necessidades de cada processo, em todas as fases de um projeto. ■

FORTINET

POR JOÃO ABREU
Systems Engineer Manager, Fortinet

OS NEGÓCIOS DA PRÓXIMA GERAÇÃO EXIGEM UMA REDE ORIENTADA A SEGURANÇA

As redes de hoje estão distribuídas por tantos dispositivos e ambientes, que a noção de perímetro foi praticamente abandonada.

ESSA TRANSIÇÃO foi, em grande parte, o resultado de um modelo de negócios baseado em aplicações. Os utilizadores – funcionários e consumidores – exigem acesso imediato e fiável a aplicações essenciais e serviços de *streaming* a qualquer momento, em qualquer lugar, em qualquer dispositivo.

A maioria das organizações transformou as suas redes num conjunto de edges: Além da LAN edge, há a nova WAN edge, a multicloud, a do data center distribuído, a móvel e, mais recentemente, devido à rápida adoção do teletrabalho, um grande aumento das edges nas residências. E a computação multi-edge (MEC) – uma arquitetura de IT aberta e distribuída que apresenta poder de processamento descentralizado e uma plataforma de rede virtualizada – está ao virar da esquina. Alimentado por dispositivos e infraestrutura preparados para 5G, o MEC aproveita as tecnologias de computação móvel e *Internet of Things* (IoT) para processar dados localmente, em vez de serem transmitidos para um data center.

Este nível de inovação transformou as redes de uma forma tão completa e rápida que as ferramentas de segurança tradicionais não são capazes de fornecer a segurança consistente que as redes exigem. As soluções de segurança tradicionais, geralmente implementadas após a instalação de uma rede, foram desenvolvidas para proteger perímetros fixos e monitorizar níveis previsíveis de tráfego e fluxos entre servidores e dispositivos de rede.

- João Abreu -
Systems Engineer Manager,
Fortinet

Esses dias acabaram. A coleção atual de ambientes de edge está num estado de fluxo constante. Não estão apenas a adicionar e a descartar continuamente dispositivos físicos e virtuais, mas também criam redes temporárias e ajustam-se constantemente. E à medida que o Big Data, arquiteturas de Hiper escala, SD-WAN, 5G, redes Edge e sistemas inteligentes (carros, cidades e infraestruturas) se tornarem comuns, essas redes vão ser forçadas a mudar ainda mais. A geração atual de soluções de segurança implementadas simplesmente não consegue acompanhar.

AS REDES ORIENTADAS A SEGURANÇA SÃO DESENHADAS PARA OS NEGÓCIOS DIGITAIS ATUAIS

Felizmente, existe uma nova geração de segurança desenhada para os ambientes atuais complexos, distribuídos e dinâmicos. Tudo começa com a rede orientada à segurança, uma abordagem que integra totalmente a infraestrutura de rede e a arquitetura de segurança de uma organização numa única solução, essencial para defender com eficácia os ambientes altamente dinâmicos de hoje.

Três etapas críticas para implementar uma rede orientada a segurança:

PDIO seguro: uma estratégia de rede orientada à segurança deve fazer parte de todo o ciclo de vida do planeamento, *design*, implementação e otimização da rede, mas começa na fase de planeamento, antes que haja decisão sobre que novas infraestruturas, aplicações e dispositivos vão ser necessários.

Controlo de acesso e segmentação: quando novos dispositivos são adicionados à rede, o sistema de segurança integrado precisa identificá-los automaticamente e aplicar regras antes de conceder acesso aos recursos da rede. Isso inclui a atribuição automática de dispositivos a segmentos de rede protegidos que foram melhorados com autenticação para maior controlo. Esses segmentos de rede são monitorizados pela estrutura de segurança para evitar comportamentos não autorizados, inspecionar aplicações e proteger *workflows*.

Proteção consistente em todos os lugares: os dados nunca ficam num só lugar. Eles são partilhados, comparados, extraídos e processados. A rede orientada à segurança protege continuamente os dados, aplicações e *workflows* por meio da implementação de um único Security Fabric integrado, garantindo segurança ao longo de todo o caminho.

INOVAÇÃO DIGITAL EXIGE REDE ORIENTADA À SEGURANÇA

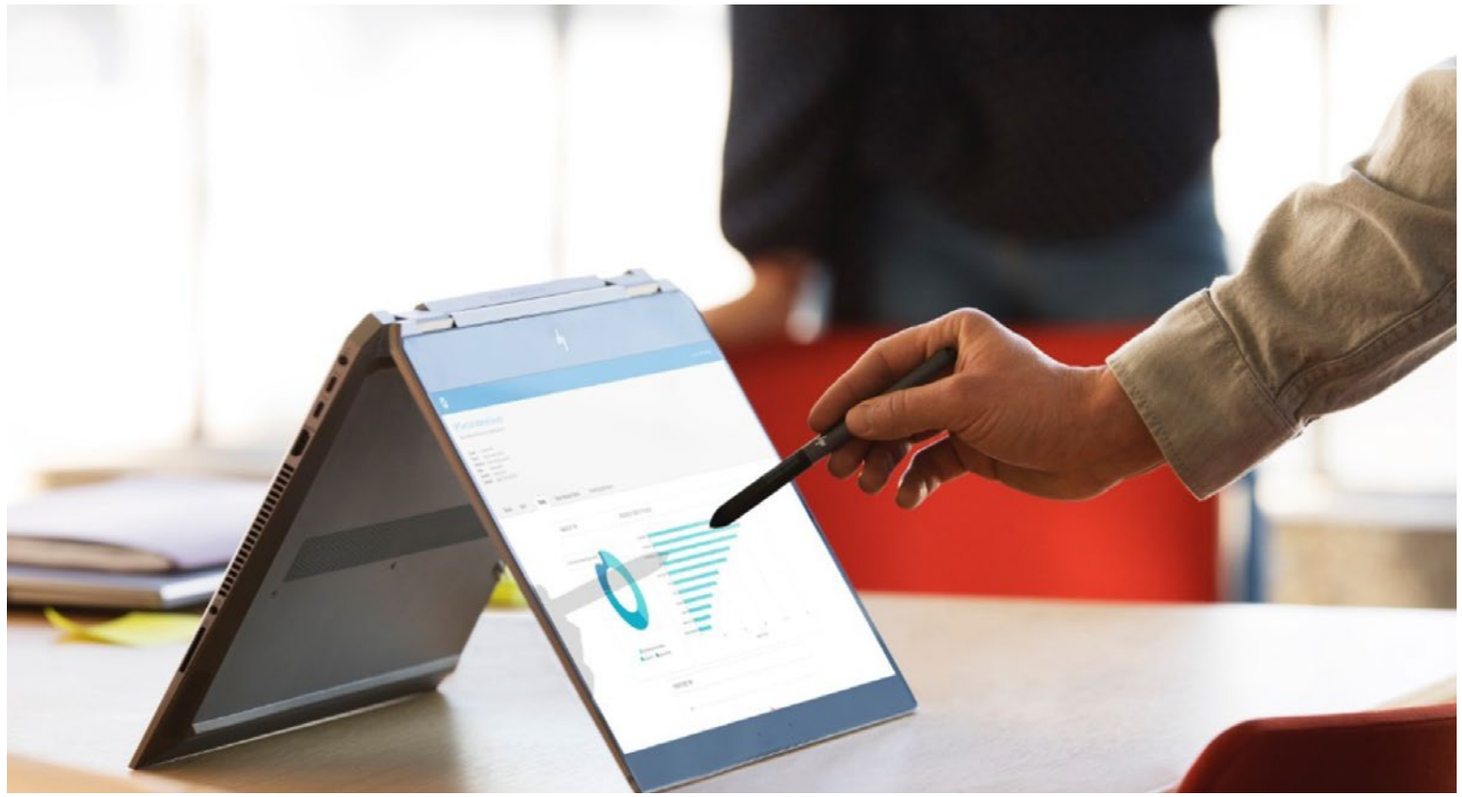
A rede orientada à segurança é um próximo passo essencial para proteger as atuais infraestruturas digitais dinâmicas e em evolução. As plataformas de segurança integradas numa estrutura de segurança unificada e criadas na infraestrutura de rede permitem que as organizações adotem a inovação digital e expandam a sua pegada digital sem expor recursos críticos a novos riscos agravados pela perda de visibilidade e controlo. A rede orientada à segurança foi desenvolvida para expandir e adaptar-se em sincronia com a rede, fornecendo proteções e controlos flexíveis que os negócios digitais de hoje exigem. ■

POR PEDRO COELHO
Lead de Computação Pessoal, HP Portugal

A SEGURANÇA É ESSENCIAL. A SEGURANÇA COMEÇA NO PC

O período pandémico acentuou a preocupação com as soluções de segurança implementadas ao nível do computador pessoal.

COM COLABORADORES remetidos para fora do escritório, a maioria dos quais ainda sem conhecer as diferentes facetas do cibercrime, criou-se um enquadramento quase perfeito para a proliferação de ataques à segurança do PC, com o objetivo de aceder ilicitamente a dados, aplicações e credenciais de utilizador.



SEGURANÇA – SEMPRE E CADA VEZ MAIS *"BY DESIGN E BY DEFAULT"*

Na perspetiva de cada um de nós, como utilizadores, o PC é a primeira frente de exposição a riscos de cibersegurança. É urgente reforçar as soluções e ferramentas que protegem os utilizadores de ataques

cibernéticos e que, idealmente, operem sem a sua intervenção e possam bloquear ataques de diferentes origens e em constante mutação. Para isso, a segurança tem de constar "*by design*" e "*by default*" em qualquer nova iniciativa digital ou em qualquer arquitetura tecnológica.

Inclusivamente, ao nível do PC onde a segurança tem de estar embutida no equipamento e não ser remetida para um *add-on* ou *upgrade* de software.

A proteção contra ataques à BIOS, a deteção de malwares, a monitorização da integridade dos processos de anti-vírus, os métodos reforçados de autenticação e as tecnologias de privacidade sobre os dados pessoais, entre outras soluções, devem integrar nativamente os nossos equipamentos pessoais e constituir camadas de proteção que, de modo automático, inteligente e evolutivo, assegurem a integridade do dispositivo, das nossas credenciais, dos dados pessoais e da camada aplicacional. Com 350.000 novos malwares por dia, é igualmente relevante que o nosso computador, o nosso posto de trabalho, consiga detetar ameaças sem a nossa intervenção, inibindo estes "*zero-day attacks*" recorrendo a técnicas de Inteligência Artificial que conseguem deduzir os padrões de comportamento destas tentativas de intrusão e roubo.

Deixou de ser suficiente definir o PC pelo processador, memória ou disco; é crítico estabelecer requisitos mínimos de segurança que integrem o PC para que este seja, de facto, a primeira linha de defesa e não apenas um ativo desprotegido que obrigará o IT a implementar outras camadas de proteção, já ao nível das infraestruturas corporativas ou de acesso à cloud.

O PC É ESSENCIAL

O PC tem-se revelado essencial. Essencial para trabalhar em qualquer lugar, essencial para aprender e ensinar, essencial para nos mantermos conectados, colaborativos e criativos.

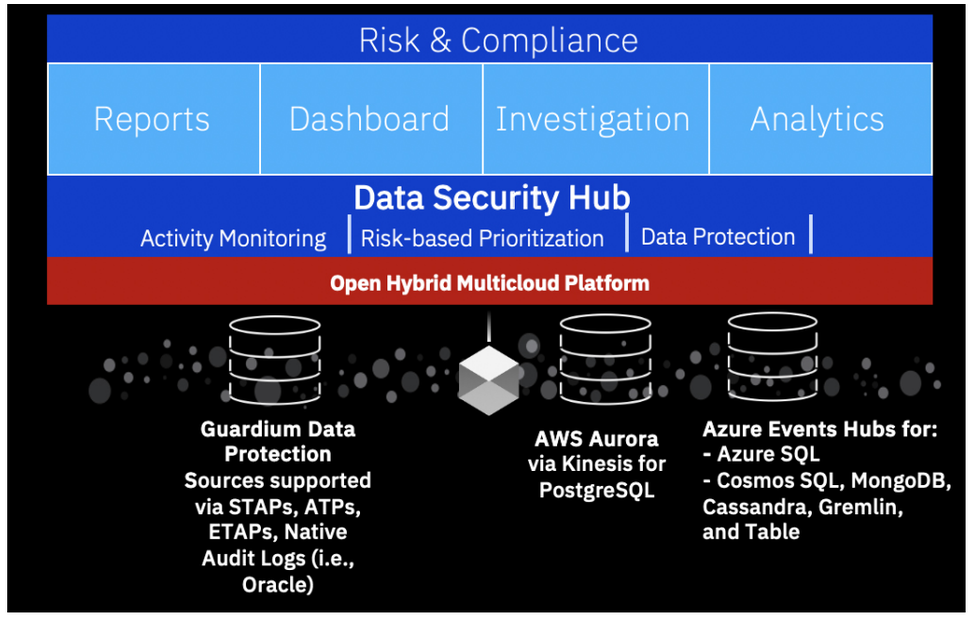
No que respeita à **segurança**, já há vários anos que ela consta do DNA dos PCs HP, com tecnologias embutidas que implementam diferentes camadas de defesa. Soluções como o HP Sure Start protegem o PC desde um nível de firmware, monitorizando o comportamento da BIOS e com capacidade de autorrecuperação para minimizar o *downtime* que os utilizadores possam sofrer. Ou soluções como o HP Sure Sense que utiliza técnicas de IA (*deep learning*) para detetar ataques no próprio dia do seu lançamento, atribuindo a ficheiros e aplicações uma probabilidade de esconderem uma ameaça à integridade do PC e forçando o respetivo bloqueio quando essa probabilidade é elevada. Os computadores profissionais da HP constituem assim uma importante primeira linha de defesa de utilizadores e organizações, porque na HP acreditamos que a segurança é essencial e ela deve começar no PC. ■

IBM

AJUDAR AS ORGANIZAÇÕES A PROTEGER OS SEUS PRINCIPAIS ATIVOS

O IBM Security Guardium oferece um conjunto abrangente de produtos e foi projetado para ajudar os clientes a proteger os seus principais ativos de dados.

A SEGURANÇA DE DADOS cresceu em importância à medida que o escrutínio sobre as práticas de recolha de dados aumentou. O custo de não proteger os dados de alguém expande-se muito além do esforço que as empresas colocam para recuperar as informações perdidas. Multas regulatórias, IP roubados e danos à reputação podem aumentar consideravelmente o custo de uma violação.



Conforme as organizações crescem, o mesmo acontece com os seus ambientes de dados, aumentando a área de superfície potencial para ataques de cibercriminosos. O IBM Security Guardium providencia aos clientes a capacidade de proteger os seus ambientes de dados cada vez maiores sem limitar a sua capacidade de navegar e analisar as informações que armazenam. A solução fornece aos clientes um conjunto de produtos que aumenta a sua capacidade de monitorizar e proteger os seus fluxos de trabalho eficientes para provar a conformidade numa variedade de ambientes.

Para entender melhor os benefícios, custos e riscos associados a esse investimento, a Forrester entrevistou decisores de uma organização com experiência na utilização do Guardium Data Protection.

Antes de usar o Guardium Data Protection, o cliente esperava que cada proprietário de dados na organização mantivesse e protegesse os seus

ambientes de dados separadamente. Isso deixou a empresa sem estratégias de segurança de dados coerentes e forçou os proprietários de dados a utilizar processos manuais demorados para provar que podiam atender aos padrões de conformidade regulamentar.

Este investimento permitiu à organização automatizar muitos dos processos manuais necessários no seu *legacy*, proteger os seus dados numa solução unificada e provar a conformidade com muito mais rapidez.

BENEFÍCIOS

Antes de investir no IBM Security Guardium, a empresa analisada pela Forrester encarregou a sua equipa de administração de *database* de correlacionar e ajustar manualmente os dados para realizar relatórios de análise sobre a saúde do seu ambiente de dados. Ao usar os recursos fornecidos pela solução, foi possível automatizar esses processos, economizando um tempo significativo.

A organização relatou que, desta forma, poderia agilizar os fluxos de trabalho que seguiu para concluir as auditorias dos seus ambientes de dados. No seu *legacy*, a organização exigia uma grande equipa para recolher, analisar e apresentar as informações necessárias para passar por uma auditoria. A solução eliminou a necessidade de recolha de dados de fontes distintas e fornece um local central com todas as informações necessárias prontamente disponíveis.

Isto ajudou a organização entrevistada a obter visibilidade no seu ambiente de dados, permitindo-lhe identificar potenciais ameaças internas e externas. Os recursos de gestão de vulnerabilidade, monitorização e deteção de ameaças e priorização de ativos fornecidos pela IBM permitiram ao cliente evitar os custos potencialmente significativos de uma violação de dados.

PRODUTOS

O IBM Security Guardium inclui (mas não está limitado a) produtos como Guardium Data Protection, Guardium Insights para IBM Cloud Pak for Security, Guardium Data Risk Manager e Guardium Data Encryption.

Estes produtos são projetados para capacitar os clientes a centralizar os seus ambientes de dados, provar de forma rápida e fácil que os seus ambientes estão em conformidade com vários regulamentos, expor potenciais riscos dentro desses ambientes e acelerar a resposta a essas ameaças.

O conjunto de produtos da solução integra-se às plataformas nativas em cloud da IBM para segurança, dados e análises, IBM Cloud Pak for Security e IBM Cloud Pak for Data. A integração com essas plataformas estende a segurança de dados, análise de ameaças e relatórios de conformidade entre os ambientes de IT das organizações. ■

POR JOÃO MARQUES
Cybersecurity Sales Specialist

A IMPORTÂNCIA DA **ELIMINAÇÃO SEGURA DOS DADOS** NUMA ORGANIZAÇÃO

A polÍtica de gestão do ciclo de vida dos dados de uma organização define as regras de governação do fluxo dos dados desde a sua criação até à sua eliminação.

SEGUNDO A GARTNER, este ciclo comporta sete fases: criação, utilização, partilha, atualização, arquivo, armazenamento e eliminação segura de dados.

Para além das boas práticas do tratamento e segurança dos dados, a aplicação do RGPD – Regulamento Geral de Proteção de Dados – também introduz às organizações obrigações relativamente à eliminação definitiva de dados. Fase esta que pode ser equivocadamente percebida como de pouca importância e ocasionar riscos à segurança de confidencialidade para além de coimas pela infração ao correto tratamento previsto pelo RGPD.

Esta fase do ciclo de vida dos dados pode ser exposta a falhas de segurança de confidencialidade se coincidir com o fim do ciclo de vida do suporte em que os dados estão armazenados; confundindo-se assim as regras de gestão de vida dos dados com a gestão de vida dos ativos onde estão armazenados.

A não separação destes dois conceitos pode comprometer a segurança dos dados, originando situações amplamente publicitadas em que equipamentos comercializados em 2nd *market* revelam dados confidenciais. Sobretudo no interior das organizações, estes conceitos também devem ser geridos de forma especializada, por exemplo: a transferência de um ativo de *endpoint* deve garantir a eliminação segura dos dados devendo ser reduzido o espaço temporal entre a tomada de decisão da sua transferência e a execução do procedimento de eliminação segura dos dados.

- João Marques -
Cybersecurity Sales Specialist

A DRC – Data Risk and Consulting, como detentora de um conjunto de certificações de segurança, ferramentas, processos e pessoas, oferece um processo de eliminação deliberada, irrecuperável e irreversível de dados, chamado *Data Sanitizing*, garantindo assim a confidencialidade da informação que está presente nos suportes de armazenamento e que não existem fugas internas ou externas, mesmo recorrendo a ferramentas avançadas de recuperação de dados.

Esta metodologia pode ser aplicada em dois cenários. A **destruição física**, também conhecida por ***data destruction*** aplica-se quando se pretende destruir dados muito sensíveis ou dados alocados em equipamentos antigos e sem valor comercial. Neste método, os suportes de armazenamento são fisicamente destruídos deixando o suporte inutilizável e garantindo a impossibilidade de recuperação da informação.

Para atestar a fiabilidade do método e implementar um fluxo de trabalho seguro, a DRC desenvolveu um **laboratório móvel** o qual permite:

- **Recolha dos Dados Identificativos do Ativo:** número de série, marca, etc;
- **Destruição Física:** este processo pode ser acompanhado pelo cliente final;
- **Produção de Evidência:** é entregue ao cliente um filme da execução do processo;
- **Reciclagem:** os resíduos são geridos por uma entidade gestora certificada.

Já a destruição lógica, também conhecida por ***data erasure*** ou ***data wiping***, é utilizada quando se pretende destruir dados importantes no fim de vida da máquina ou quando a máquina terá um novo utilizador. Portanto, este método permite a reutilização dos dispositivos além de emitir um relatório com o ***serial number*** do ativo e a norma utilizada na eliminação dos dados.

Como uma empresa especializada em Segurança da Informação e que está no mercado desde 1989, a DRC promove diariamente através da alta qualificação do seu corpo técnico um conjunto de serviços a fim de estabelecer um fluxo de trabalho seguro para qualquer organização nas mais diversas vertentes:

- **Recolha dos Dados Identificativos do Ativo:** número de série, marca, etc;
- **Destruição Lógica:** utilização de normas de segurança internacionais: Departamento de Defesa ou Departamento de Energia dos Estados Unidos, HIPAA, NIST, etc;
- **Auditoria:** o processo inclui uma etapa de verificação da boa execução da eliminação dos dados através de uma tentativa de recuperação de dados que é efetuada em todos os ativos;
- **Produção de evidência:** emissão de um certificado de destruição segura de dados que inclui informação sobre o ***serial number***, norma utilizada, data e tempo de duração, nome do técnico, etc.
- **Formação:** introdução à segurança da informação, RGPD, Navegação Segura e etc.
- **Reutilização de equipamentos:** após emissão do certificado de eliminação dos dados, os ativos podem ser reutilizados ou reciclados.

Construir um programa de cibersegurança adequado à sua realidade e contexto muito particular, torna a DRC um parceiro de confiança para suportar as organizações neste momento de transformação digital. ■

kaspersky

POR ALFONSO RAMIREZ,
Diretor Geral da Kaspersky Ibéria

A PANDEMIA CONTINUA EM 2021. E OS DESAFIOS DE CIBERSEGURANÇA TAMBÉM

Já todos sabemos – e muitos chegámos mesmo a sentir – as dificuldades que a pandemia trouxe a todos os países e populações.

NADA, NEM NINGUÉM, ficou indiferente ao seu impacto, que ainda se vai sentir por muito tempo. No entanto, para os profissionais de cibersegurança, a pandemia continua a criar novos desafios, principalmente com o crescente aumento do cibercrime a todos os níveis. Cibercriminosos e grupos organizados têm aproveitado os vários momentos de desarmonia global para desenvolver novos métodos e vetores de ataque.

Em março de 2020, os ataques relacionados com a Covid-19 atingiram o pico de um milhão por dia e o *phishing*, sites web maliciosos e o malware dirigido a utilizadores remotos cresceram 30.000%. E agora a situação não está melhor. Com o regresso ao ensino online, plataformas como o Zoom, o Moodle e o Google Meets, utilizadas para lecionar as aulas à distância, continuam a estar sob o olhar atento dos cibercriminosos.

Quanto às empresas, que tiveram que lidar, numa fase inicial, com uma mudança abrupta que incluiu uma transição rápida para a conexão de todas as suas infraestruturas e colaboradores online, a necessidade de proteger todas as atividades do negócio continua a ser uma prioridade. Apesar das manobras e do desinvestimento que aplicaram em muitas áreas para reduzir o impacto económico da crise pandémica, a cibersegurança está, pelo contrário, a tornar-se cada vez mais uma área prioritária para muitas delas. Inclusive, de acordo com um estudo da *Kaspersky*, 67% das mesmas a nível europeu espera aumentar o seu orçamento nos próximos três anos neste âmbito.

- Alfonso Ramirez -
Diretor Geral da Kaspersky Ibéria

Isto torna-se extremamente importante, uma vez que 2021 também traz muitos – e novos – desafios para os quais devem estar preparadas. É muito provável que a crise origine uma onda massiva de pobreza, o que leva a que, inevitavelmente, um maior número de pessoas recorra à delinquência, incluindo a cibernética. No campo das ciberameaças financeiras, estão a surgir novas tendências, principalmente no que respeita às mais perigosas, as que afetam o bem-estar económico das vítimas. O colapso de algumas economias e moedas tornará o roubo de *bitcoins* muito mais atraente e, por isso, é expectável que mais fraudes dirigidas a estas moedas ocorram, uma vez que são as criptomoedas mais difundidas.

Desta forma, torna-se muito provável que surja um crescimento das tentativas de extorsão, seja através de ransomware, ataques DDoS ou ambos. Explorações avançadas estão a consolidar-se entre os atacantes e os grupos de ransomware, com destaque para aqueles que possuem mais fundos, irão continuar a diversificar e a escalar os seus ataques, algo que se torna particularmente crítico para as empresas mais sensíveis à perda de dados, tendo que passar por um processo de recuperação esgotante e pela interrupção das suas operações online.

Além destas ameaças, poderemos também assistir a uma alteração na forma como os cibercriminosos passarão a exigir pagamentos às vítimas. Para garantir a sua privacidade e atuar sem deixar rasto, poderão servir-se de outras criptomoedas mais "discretas" enquanto primeira moeda de transição, como as Monero, convertendo-as depois em outras criptomoedas mais populares, como são exemplo as *bitcoin*.

Estes são apenas alguns exemplos do que ainda poderá vir a acontecer nos próximos meses. Vivemos tempos complexos, que urgem pela necessidade de uma maior colaboração entre as instituições públicas e o setor privado, e pela criação de uma relação de partilha de inteligência e recursos, que permita redobrar os esforços em cibersegurança. Existem já várias iniciativas a serem criadas com este objetivo, incluindo o projeto *NoMoreRansom* fundado pela Kaspersky, que já permitiu evitar pagamentos no valor de 643 milhões de euros.

Este é apenas mais um passo, num caminho que ainda tem muito por percorrer. Mais unidades de ação e transparência serão fatores essenciais para dar resposta a todos os novos desafios relacionados com cibersegurança. E não nos podemos esquecer que quanto maior a digitalização, maior atenção devemos prestar a esta área, de forma a podermos utilizar e beneficiar por completo das mais-valias da evolução tecnológica. ■

LAYER8

POR FERNANDO CARDOSO,
COO, Layer8

– A PRIMEIRA VEZ –

A primeira vez é sempre especial. Lembram-se do vosso primeiro beijo? Da vossa primeira paixão? Da primeira casa? Do primeiro filho? É sempre um momento especial. Nem sempre estamos preparados para a ocasião, nem para as responsabilidades ou dificuldades que se seguem, mas são acontecimentos marcantes e inesquecíveis.

E DO VOSSO PRIMEIRO INCIDENTE DE SEGURANÇA? Alguém se lembra? No meu caso, se não contar com os bloqueios de terminais aos colegas no Secundário (uma espécie de DoS primitivo…) ou a roleta russa que era meter uma *floppy* num computador na Universidade e não sair de lá com o Barrotes, foi algures em 1998, quando administrava, entre outras coisas, uma Sun SPARCstation 5. Era, na altura, um dos nossos servidores de DNS e de e-mail e foi só quando deixou de resolver nomes que notei que algo de estranho se passava. Foi então que os "vi": alguém, a partir da Roménia, tinha conseguido entrar na máquina e posto um *bot* de IRC a correr que estava a arrasar com o servidor. Foi o "*click*" que me fez mergulhar no mundo da segurança. Como é que entraram? Como é que me posso proteger? Como é que posso ser alertado quando tentarem novamente? Num curto espaço de tempo devorei tudo o que havia para ler sobre segurança, instalei IDSs, criei *honeypots*, defini *baselines* para *hardening* de sistemas, enfim, todo um mundo novo para o qual fui empurrado e que, tal como a Alice, fui obrigado a compreender para conseguir sobreviver às várias Rainhas de Copas que, disfarçadas de IPs, iam aparecendo.

O momento que estamos a viver com a pandemia é também uma primeira vez, não para um,

- Fernando Cardoso -
COO, Layer8

mas para todos. Tivemos que, num espaço de tempo muito limitado, compreender, adaptar e implementar um novo conceito de trabalho que nos permitisse ter os processos de negócio a funcionar.

A segurança teve, também, que obrigatoriamente entrar na ordem do dia. A mudança do paradigma de funcionamento das empresas, cuja face mais visível foi a adoção maciça do teletrabalho, obrigou a um conjunto de investimentos, nomeadamente no que diz respeito ao reforçar das infraestruturas de VPN e de MFA, à adoção de soluções *cloud-based* e ao focar na segurança do *endpoint* através de, por exemplo, soluções de EDR (*Endpoint Detection and Response*).

A boa notícia é que, apesar de haver sempre uma primeira vez para tudo, aquilo que eram as melhores práticas em 1998, também são hoje aplicáveis. Na realidade, as salvaguardas que temos de ter, já as conhecemos desde sempre, e mais, estão bem definidas em *standards* e regulamentos, desde a família ISO 27000, aos NIST 800, passando, no nosso caso, pelo Quadro Nacional de Referência para a Cibersegurança do CNCS. Está lá tudo, desde a governação à gestão de risco, da formação à sensibilização, passando por uma panóplia de controlos procedimentais e técnicos que (já) deveriam estar implementados.

O que mudou então de 1998 para 2021? Essencialmente o onde aplicar. Se no passado, o IT estava circunscrito a um ou dois processos de negócio, hoje em dia praticamente todos estão dependentes de alguma forma dos sistemas de informação que, por sua vez, são acedidos a partir de uma panóplia de dispositivos que são controlados por pessoas com mais ou menos conhecimentos em informática ou, em particular, segurança. Para além disso, as redes eram relativamente estanques e apostava-se na segurança do perímetro. Nos tempos que correm, onde está o perímetro? Em casa, na cloud, no *wired*, no *wireless*?

Devemos, como sempre, concentrar-nos naquilo que queremos proteger e, em função do nosso apetite ao risco, implementar os controlos necessários. Temos de estar preparados para, em contínuo, avaliar ameaças, venham elas de onde vierem, e da forma mais automática possível, responder em tempo real.

Se 2021 traz mais desafios, sim. Vão acontecer mais ataques aos computadores e redes domésticas, o ransomware e o BEC (*Business Email Compromise*) vai continuar a crescer, os dispositivos móveis vão continuar a ser alvo de ataques via *apps* maliciosas nas *stores* e IoTs e OTs vão continuar a ser um alvo apetecível, ainda para mais quando conjugados com tecnologias emergentes como o 5G.

Mas para uma organização que tenha uma cultura de segurança e tenha assumido uma postura de *zero trust*, o identificar, proteger, detetar, responder e recuperar, que era válido em 1998, continuará a sê-lo no presente e no futuro. ■

nexllence
POWERED BY GLINTT

"A PERSPETIVA DE CIBERSEGURANÇA MAIS EQUILIBRADA SERÁ A DE TRABALHAR PARALELAMENTE EM DUAS FRENTES"

David Faustino, Manager Director da Nexllence, aborda o tema da cibersegurança e de como um ciberataque pode ter custos financeiros e reputacionais elevados para uma organização.

Como se podem endereçar as preocupações dentro de uma organização relativamente a potenciais fugas de informação?

É hoje sabido que as fugas de informação dentro das organizações são, na sua esmagadora maioria, involuntárias e inusitadas, causadas por ações descuidadas dos utilizadores. A título de exemplo, todos nós já enviámos um e-mail para a pessoa errada sem qualquer intenção maliciosa; este e-mail poderá conter informação sigilosa, que deste modo irá ser recebida por uma pessoa que não deveria ter acesso à referida informação.

No entanto, também há fugas de informação de cariz intencional e pernicioso. Assim, o tema deverá ser endereçado nas suas diversas vertentes: deverão ser promovidas campanhas regulares para a sensibilização dos utilizadores para este tema; deverá ser implementada e operacionalizada uma política rigorosa de gestão de privilégios de acesso aos recursos da organização; e finalmente, como última linha de defesa, deverá ser implementada uma solução de DLP (*Data Leak Prevention*).

As lideranças de topo das empresas e entidades públicas têm literacia digital e percebem as ameaças que podem existir numa organização caso não se invista em cibersegurança?

A gestão de topo na maior parte das médias e grandes empresas e organismos públicos tem hoje consciência das ameaças existentes e do seu impacto para o negócio. Observamos três grandes dificuldades para que as empresas robusteçam mais a cibersegurança do seu negócio:

1. Uma visão parcial do que é a cibersegurança, preocupando-se apenas com parte do desafio;

2. A (falsa) sensação de que a empresa não é suficientemente grande ou interessante para ser atacada;

3. A disponibilidade financeira para implementar um plano holístico de cibersegurança. Sendo esta uma decisão da gestão, assistimos infelizmente a inúmeros casos em que o investimento considerado impossível é efetivamente realizado após um ciberataque, devido aos consequentes (e usualmente muito significativos) custos financeiros e reputacionais, pela paragem de atividade da empresa e degradação de imagem ocasionada.

É preciso investir em infraestruturas de IT, nos processos, na componente aplicacional e nos dados. Qual deve ser o ponto de partida no investimento?

Todas as empresas têm uma *baseline* de cibersegurança atual. A perspetiva mais equilibrada será a de trabalhar paralelamente em duas frentes:

a) A curto-prazo, identificando as vulnerabilidades mais graves de cibersegurança (através de auditorias a processos e testes de penetração e vulnerabilidades) e resolvê-las se possível no imediato;

b) A médio-longo prazo, criando um plano plurianual que calendarize o investimento com base em critérios bem definidos, como criticidade, literacia de cibersegurança dos colaboradores da empresa, impacto no negócio, dinâmica de negócio, cumprimento de pré-requisitos e/ou normativos para iniciativas mais sofisticadas e disponibilidade de investimento.

São necessárias cada vez mais competências para tornar uma organização o mais segura possível. De que maneira é que a Nexllence pode ajudar as organizações?

A Nexllence tem características únicas em cibersegurança, uma vez que detém internamente todas as competências dos quatro pilares da cibersegurança: experiência no desenvolvimento e evolução de aplicações, onde utilizamos *frameworks* como *security by design* e DevSecOps, entre outras; grande capacidade na implementação e operação de infraestruturas de segurança perimétrica, na cloud e do utilizador final, assentes numa experiência de mais de 20 anos em setores críticos como banca, telecomunicações ou *utilities*; e através de um conhecimento profundo dos dados, sejam nos seus sistemas de armazenamento, *backup*, como nos sistemas de gestão de bases de dados e gestão de identidades, em contexto de data center físico ou na cloud. No quarto pilar, a definição de políticas e processos de segurança, temos também importantes referências, nomeadamente ao nível dos setores da saúde, retalho e distribuição. ■

noesis
an Altia Company

POR NUNO CÂNDIDO,
IT Operations, Cloud & Security Associate Director, Noesis

INTELIGÊNCIA ARTIFICIAL: UM FORTE ALIADO AO SERVIÇO DA CYBERSEGURANÇA!

Vivemos tempos de forte aceleração digital. Por um lado, a evolução da tecnologia trouxe um aumento da utilização dos dispositivos móveis e democratizou-se o acesso à Internet, por outro lado, a diversidade de plataformas, dispositivos e redes que utilizamos faz com que fiquemos progressivamente mais conectados com o mundo.

A TRANSFORMAÇÃO DIGITAL aumentou a complexidade, levando a uma degradação do perímetro de segurança e à necessidade de adoção de novas ferramentas e soluções. Para adensar ainda mais a criticidade deste contexto, a pandemia COVID-19, com a consequente adoção de teletrabalho, veio adicionar maior dificuldade de segurança de informação das nossas empresas.

De igual forma, a escassez de talentos, de profissionais qualificados. Esta aceleração digital e as alterações tecnológicas acima descritas, conjugadas com uma maior perceção, por parte das organizações, para a importância de protegerem as suas infraestruturas, dados e sistemas, tem provocado uma procura crescente de profissionais experientes. A escassez destes profissionais, aliada à não-inesgotabilidade dos departamentos de IT, que como sabemos não podem dedicar todo o seu tempo ao tema da segurança informática, agrava a vulnerabilidade das organizações. Este é um problema premente, mas tem sido também um motor de inovação no mercado dos fornecedores e fabricantes, que procuram desenvolver soluções que garantam segurança e, em simultâneo, otimizem a intervenção de recursos humanos.

- Nuno Cândido -
IT Operations, Cloud & Security Associate Director, Noesis

Por último, a crescente sofisticação dos cibercriminosos, o aumento exponencial do número de ataques, cada vez mais complexos e diversificados, a sofisticação crescente das técnicas de ataque, são uma realidade, comprovada por inúmeros relatórios e, inclusive, objeto de cada vez maior atenção mediática. Só entre fevereiro e março de 2020, por exemplo, registou-se um aumento de 84% do número de incidentes de segurança reportados em Portugal, tendo-se registado um aumento de incidentes de mais de 150% em 2020, face ao ano anterior.

As ameaças estão bem presentes, em constante mudança e cada vez mais diversificadas. Ataques *machine-to-machine* (M2M), ataques silenciosos, altamente personalizados, ataques de *phishing*, entre outros, a que as abordagens tradicionais de segurança, não são capazes de responder. A abordagem tradicional, com base em padrões e assinaturas, focada na deteção de ações e comportamentos maliciosos, revela-se lenta e incapaz de se adaptar a estas novas ameaças.

É por isso que a aposta em cibersegurança se assume, cada vez mais, como uma das preocupações centrais das organizações. De acordo com o mais recente estudo da IDC – Security Market in Portugal, 2020 – A despesa com segurança da informação vai ultrapassar 197,3 milhões de euros em 2024, o que corresponde a um crescimento anual médio de 6,3% entre 2019 e 2024. Estima ainda a IDC que a despesa com segurança de informação representará cerca de 4,7% da despesa total com IT em 2024.

É necessário mudar o paradigma – procurar comportamentos anómalos, ao invés do foco na procura de comportamento malicioso e adotar estratégias de reforço da confiança digital, que envolvam atributos como o risco, a conformidade regulamentar, a privacidade e a ética de negócio.

E esta mudança de paradigma está mais próxima do que possamos pensar. As previsões para a próxima década são a prova disso, de acordo com um estudo da Trend Micro, os algoritmos de inteligência artificial vão ser dos pilares fundamentais para a automatização da cibersegurança, e uma resposta aos limites da capacidade humana.

A inteligência artificial é uma forte aliada ao serviço da cibersegurança e um investimento essencial para aumentar a segurança nas organizações e para dotar as próprias equipas de IT, retirando-lhes grande parte do esforço de análise e permitindo-lhes um maior foco no que é importante, o negócio e os objetivos da organização.

Poder analisar informações e eventuais anomalias sem a sobrecarga dos recursos humanos é uma das perspetivas que a visão de inteligência assistida permite alcançar. Com pouco esforço, passa a ser possível monitorizar as redes de forma completa e, dessa forma, atuar em *real time* sobre as ameaças externas ou internas que afetam as organizações.

As soluções baseadas em IA utilizam tecnologia que permite analisar padrões de comportamento em qualquer rede, dispositivo ou utilizador numa organização, independentemente da escala, através de algoritmos de IA e *Machine Learning*, permitindo assim detetar, com elevados níveis de eficácia, qualquer alteração no padrão e, desta forma, identificar possíveis ameaças de forma muito mais rápida.

Este tipo de assistência, baseada em modelos de AI e ML é o futuro das organizações que se querem manter na vanguarda da tecnologia com segurança. ■

POR CARLA ZIBREIRA,
Head of Consulting, S21sec Portugal

A CIBERSEGURANÇA NA CONSTRUÇÃO DA CONFIANÇA DIGITAL

A forma holística como as tecnologias emergentes, o datamining e os algoritmos entraram no nosso quotidiano, moldando a nossa existência política, social e moral, é uma realidade difícil de ignorar, fazendo surgir sérias preocupações sobre quais os impactos que podem ter em gerações atuais e futuras.

A TECNOLOGIA que criámos fez surgir novos casos de uso, oportunidades, mas também, e não menos importante, perigos que podem comprometer infraestruturas críticas, dados pessoais, diversos serviços disponibilizados no ciberespaço e, acima de tudo, a confiança do cibernauta consumidor.

Ao longo dos anos, os governos, a indústria e a comunidade científica têm estudado estratégias e soluções com o objetivo de enfrentar esses perigos e impactos. No entanto, a maturidade em relação ao ecossistema de riscos que a tecnologia apresenta não é consensual nem homogénea, levando a comportamentos maliciosos (intencionais ou não) que podem comprometer vidas, negócios e sociedades em geral. Nesse sentido, é fundamental compreender que a tecnologia e a sua aplicabilidade são aspetos dissociáveis que influenciam de forma distinta a implementação da ética e da confiança digital.

Deste modo, como consequência da crise pandémica que atravessamos, as organizações nos vários setores de mercado, e independentemente da sua dimensão, foram forçadas a repensar os seus modelos de negócio de modo a responder ao cenário de contingência vivido. Essa reflexão levou à necessidade urgente e prioritária de recorrer à utilização de recursos digitais para uma

- Carla Zibreira -
Head of Consulting,
S21sec Portugal

transformação estratégica dos seus processos de negócio no ambiente digital. É assim fulcral e prioritário que as organizações entendam:

• Os fatores que influenciam e impulsionam a confiança do cibernauta
• O grau de confiança real nos seus produtos e serviços
• O impacto que a perda de confiança tem para o negócio

Adicionalmente, compreender que a construção de uma cultura de confiança no digital é um processo complexo que implica endereçar, não só aspetos tecnológicos, mas também sociológicos. Aspetos que conjugados se apresentam como verdadeiros desafios num mercado em que os níveis de maturidade, quer das organizações quer dos cibernautas, são ainda bastante heterogéneos.

Deste modo, e nos aspetos sociológicos, é importante realçar a forte influência que as crenças e os aspetos culturais têm naquele que é o conceito de perceção de confiança de cada indivíduo.

Nos aspetos tecnológicos, é importante que sejam considerados os seguintes fatores:

• A definição de requisitos de cibersegurança e privacidade dos dados são críticos, cruciais e chave na conceção e implementação de novos produtos e serviços para que a confiança do cibernauta saia reforçada, uma vez que o preço, a qualidade, a experiência e o compromisso passaram a ser fatores secundários na diferenciação das organizações e dos seus produtos no ciberespaço.
• O conhecimento e a compreensão do ecossistema de ciber riscos para que o tratamento da informação do cliente através da gestão do ciber risco seja efetiva.
• A nomeação de um *Chief Trust Officer* (CTrO) com fortes conhecimentos em operações de segurança da informação, privacidade e conformidade, e que complemente as funções de um DPO, CISO, CIO e CTO.
• A demonstração de conformidade regulamentar e normativa como estratégia de demonstração de ética e selo de confiança digital.
• A sensibilização interna de todas as estruturas orgânicas (i.e., negócio e suporte) para a importância da definição de uma estratégia para a construção da confiança digital e do papel da segurança na implementação dessa estratégia.
• A sensibilização do cliente final para aspetos relacionados com a utilização segura dos seus serviços e infraestruturas assim como do tratamento em conformidade dos seus dados no ciber espaço.
• A implementação de controlos tecnológicos de segurança que visem salvaguardar: as infraestruturas de perímetro, *endpoint* e cloud; a gestão de identidades e acessos; a resiliência da tecnologia para suportar a estratégia do negócio; a capacidade de prevenção e resposta perante incidentes de segurança.

À medida que as ciber ameaças se tornam mais conhecidas, os cibernautas tornam-se mais conscientes de temas como a privacidade dos seus dados e, deste modo, mais comprometidos com a cibersegurança.

Deste compromisso nasce a oportunidade de as organizações se diferenciarem da concorrência, melhorando a sua relação com novos e atuais clientes através da confiança digital! ■

powered by IT SECURITY

CIBERHIGIENE: A BASE DA SAÚDE DE UMA ORGANIZAÇÃO

Ilustração: Designed by slidesgo / Freepik

Os utilizadores devem adquirir um conjunto de práticas para garantir que utilizam a Internet sem problemas nas suas rotinas, para além de saber identificar potenciais ameaças como emails de phishing.

RUI DAMIÃO

É SABIDO QUE O PONTO MAIS FRACO da cibersegurança é a componente humana, mas, simultaneamente, é impossível retirar as pessoas por completo dos sistemas. A partir do momento em que existem colaboradores, existe uma possível porta de entrada.

O trabalho remoto cresceu com a pandemia. Também é sabido que as organizações abriram os acessos aos seus colaboradores e que as ameaças cresceram durante o período de confinamento. Ao verem-se no conforto das suas casas, muitos relaxaram a atenção dada a potenciais emails de phishing que podem ser o primeiro ponto de entrada para um ataque cibernético de larga escala.

Cabe às organizações formar e alertar os colaboradores para as ameaças existentes. O phishing é apenas um deles, mas há mais. Assim, todos os utilizadores de Internet – seja num contexto profissional ou pessoal – devem adquirir um conjunto de práticas para garantir que utilizam as várias ferramentas online existentes sem problemas nas suas rotinas, para além de saber identificar potenciais ameaças.

PONTOS CRÍTICOS PARA UMA CIBERHIGIENE

O Centro Nacional de Cibersegurança (CNCS) publicou no seu site uma série de recomendações que os utilizadores devem ter em conta quando navegam na Internet. No caso da navegação, devem ser utilizadas firewalls, privilegiar endereços 'https', desconfiar de ofertas demasiados boas na Internet e, ao máximo, recolher informação sobre o vendedor, utilizar formas de pagamentos seguras e guardar o registo das transações.

Com o aumento de trabalho remoto, aumentou, também, a utilização dos dispositivos corporativos para temas pessoais. No caso de o dispositivo ser utilizado por terceiros – algo que não deve ser feito – deve ser acompanhada a navegação dessa pessoa para garantir que não prejudica o dispositivo e os sistemas.

Os emails são uma conhecida porta de entrada para vários ciberataques. Assim, os utilizadores devem abrir emails apenas de origem conhecida e, no caso de abrir um email de origem desconhecida, não devem carregar em nenhuma ligação ou anexo.

OS COLABORADORES E AS ORGANIZAÇÕES DEVEM TER EM CONTA UMA SÉRIE DE PROCEDIMENTOS PARA GARANTIR A SUA CIBERHIGIENE

Simultaneamente, deve-se verificar o endereço e a veracidade dos emails conhecidos, não enviar informação sensível por email, identificar SPAM para que o sistema faça uma seleção prévia e terminar sempre a sessão quando se finaliza a utilização do email.

Também as redes sociais são não só um ponto de entrada para um ciberataque, como uma ferramenta para retirar informação que pode ser utilizada para realizar um ciberataque direcionado. Assim, mesmo numa componente mais pessoal, os utilizadores só devem aceitar ligações apenas de pessoas conhecidas e nunca partilhar telefone ou moradas no seu perfil. Ao mesmo tempo, deve-se evitar partilhar locais, imagens de crianças ou dados sensíveis e não carregar em publicações suspeitas, uma vez que pode ser uma campanha de phishing.

CUIDAR DOS DISPOSITIVOS

Os colaboradores e as organizações devem ter em conta uma série de procedimentos para garantir uma ciberhigiene do equipamento. Assim, só devem ser utilizados dispositivos autorizados pela organização e, em caso de perda, informar o responsável de cibersegurança. Para além de não deverem ser utilizado por terceiros ou para tarefas pessoais, o utilizador também deve utilizar apenas pens USB confiáveis, utilizar um filtro no ecrã do portátil e ativar o bloqueio automático dos dispositivos e utilizar um PIN ou uma palavra-passe para desbloquear o dispositivo.

CURSO CIDADÃO CIBERSEGURO

O Centro Nacional de Cibersegurança conta com um curso que "visa garantir um conjunto de competências que permitam que o cidadão, enquanto utilizador do ciberespaço, se sinta apto a navegar de forma segura".

Este curso gratuito – *disponível até ao final de março de 2021 no site do CNCS* – tem uma carga total de cerca de três horas, divididas em três módulos e que inclui uma avaliação. Os módulos dizem respeito à casa, ao trabalho e ao exterior e, cada um deles, se foca na identidade, nas redes e na navegação, no comportamento social e no posto de trabalho ou posto doméstico. ■

BRANDED CONTENT

easyVISTA

POR HUGO BATISTA,
Pre Sales and Delivery Director Southern Europe

DEVEMOS AUTOMATIZAR A GESTÃO DE ATIVOS DE IT?

À medida que uma empresa cresce, mais difícil é rastrear o uso de ferramentas e equipamentos de IT fornecidos aos seus colaboradores.

QUANDO A ORGANIZAÇÃO tem menos de dez colaboradores, a memória corporativa pode ser suficiente. De dez a 100, é comum ficar satisfeito com um Excel. Mas para números superiores, uma ferramenta dedicada deve ser essencial, em particular para organizações com várias localizações. E como a gestão de ativos de IT não se contenta apenas em listar e referenciar hardware e software de acordo com os colaboradores, é acima de tudo uma ferramenta estratégica que desempenha um papel importante no acompanhamento de *tickets*, na gestão e antecipação de incidentes de segurança e no desempenho da sua organização, qualquer que seja o setor de atividade.

O QUE É UM SISTEMA DE GESTÃO DE ATIVOS DE IT?

É uma plataforma web ou software cujo objetivo é relacionar todos os seus ativos estratégicos, gerindo-os ao longo do seu ciclo de vida. A Gartner define como um método para "fornecer uma visão precisa dos custos e riscos dos ativos de tecnologia para maximizar o valor agregado das decisões em termos de estratégia, arquitetura, financiamento, contrato e aquisições da empresa". Mais concretamente, é uma ferramenta que permite responder às seguintes questões:

- Quais os computadores em fim de vida e que precisam de ser substituídos?
- Onde estão as licenças de software usadas por determinado departamento?
- Quanto custa todo o software da organização?
- Quais os ativos que ainda estão na garantia?

- Hugo Batista -
Pre Sales and Delivery Director
Southern Europe

• E quais os que já não têm cobertura?
• Os servidores internos ainda têm capacidade para lidar com novas tarefas?
• Qual é a vida útil média de um ativo específico?
• Quais são as relações de dependência que existem entre os ativos?

É também uma ferramenta muito importante para facilitar o dia a dia do seu CIO. Um novo colaborador chega ao departamento de marketing? É fácil atribuir-lhe um computador ou tablet e um telemóvel. Um vendedor está a sair da sua organização? Com alguns cliques, tem a lista detalhada de ativos de IT que ele terá de entregar quando sair. Uma vulnerabilidade de segurança é descoberta num programa na versão 10 do Android? A sua plataforma informa imediatamente quais os tablets e smartphones em risco e quais devem ser intervencionados. Com o trabalho à distância, a gestão de ativos de IT é uma solução altamente estratégica para administrar a sua organização com diligência e responsabilidade. Com a automação, é fácil responder rapidamente, receber alertas em tempo real, provisionar hardware ou software e gerir reparações ou substituições.

OS IMPACTOS DA GESTÃO DE ATIVOS NA SUA ORGANIZAÇÃO

Graças à gestão de ativos, pode ter uma visão holística da sua organização. É uma forma eficiente de controlar atualizações de programas e equipamentos, padronizar a sua frota para limitar o desperdício de recursos e processar solicitações de serviços personalizados e contextualizados de acordo com o perfil do colaborador. Mas também existem muitos outros impactos:

• Gastos indiretos reduzidos, maior eficiência na reutilização de ativos e fácil acesso às informações.
• Maior visibilidade para saber o que está em circulação, onde está, se é útil, quais são os riscos e o ciclo de vida.
• Melhor gestão de conformidade de licença de software: o que é usado? Por quem? Quanto custa? Quais as atualizações mais recentes?
• Rastreie o inventário da sua propriedade para ajudá-lo a gerir roubos, perdas, seguros e evitar compras desnecessárias.
• Monitorize os seus indicadores chave de desempenho para controlar os seus gastos, o valor da frota ou a qualidade do seu serviço.
• Otimize a sua política de segurança (atualização de software, sistemas operacionais, antivírus, etc.)

Com a gestão de ativos de IT, economize tempo e dinheiro, obtenha maior eficiência operacional e melhor experiência de utilizador, com rapidez de execução e otimização de recursos ... Além disso, com a gestão de ativos de IT pode reduzir a sua pegada de carbono, pois será mais fácil e rápido reaproveitar um ativo existente ao invés de fazer novas aquisições. ■

ALTRI OTIMIZA M365 E CULTURA DIGITAL COM CMAAS

Com o serviço de Change Management-as-a-Service (CMaaS) da Claranet, foram identificados os temas de trabalho e consequentes iniciativas que suportaram a transição e criação de uma cultura digital.

COTADA NA BOLSA DE VALORES de Lisboa, onde integra o seu principal índice, o PSI-20, a Altri é apresenta-se como um produtor europeu de referência no setor de pasta de papel, sendo um dos mais eficientes produtores da Europa de pasta de eucalipto branqueada.

Atualmente, contabiliza três fábricas de pasta de papel – a Celbi, a Caima e a Celtejo – com uma capacidade anual nominal superior a um milhão de toneladas.

A gestão florestal é outra atividade central da Altri que tem em Portugal sob gestão cerca de 83,5 mil hectares de floresta certificada. A autossuficiência florestal é da ordem dos 20%.

Paralelamente, a empresa é excedentária na produção de energia elétrica através da cogeração industrial de base renovável e vende anualmente cerca de 500 GWh de energia elétrica, a partir do processo de cogeração.

A ALTRI PROCUROU CONSOLIDAR O SEU LOCAL DE TRABALHO DIGITAL E OTIMIZAR A COMUNICAÇÃO, COLABORAÇÃO E MODERNIZAÇÃO DOS SEUS PROCESSOS DE TRABALHO

O DESAFIO

A par das tendências atuais e partindo do princípio de que as empresas estarão cada vez mais dependentes das plataformas digitais, a Altri procurou consolidar o seu *workplace* digital, otimizando a comunicação, colaboração e modernização dos processos de trabalho.

Assim, tendo em conta os diferentes perfis de trabalho na Altri, distribuídos por diferentes geografias e considerando as pequenas iniciativas de introdução à ferramenta já realizadas anteriormente, o desafio prendeu-se com a gestão da mudança e adoção da tecnologia num modelo de as-a-Service, que garantisse não só a adoção da tecnologia, mas também a transição para uma cultura de organização cada vez mais digital.

Com o serviço de CMaaS (*Change Management-as-a-Service*), foram identificados os temas de trabalho e consequentes iniciativas para abordagem aos mesmos:

- Aumentar a produtividade dos colaboradores através da utilização do Microsoft Teams, OneDrive, Planner;
- Garantir a mobilidade dos colaboradores - *First Line Workers*;
- Inovar e automatizar os processos de negócio com base no Power Platform;

"O CMaaS permite trabalhar os diferentes temas com recurso a diferentes iniciativas ao longo de um ano e de forma contínua", garante Miguel Coelho, Diretor de IT da Altri.

A SOLUÇÃO

A Claranet dispõe de um programa de transformação de *workplace*, num modelo as-a-service, suportado por uma metodologia de Change Management, certificada pela PROSCI. Alinhado com esta *best practice*, o programa de transformação identifica as necessidades em cinco fases distintas: *awareness*, *desire*, *knowledge*, *ability* e *reinforcement*.

Sendo um modelo de as-a-Service, o CMaaS, permite definir temas concretos de trabalho que suportam a transição e criação de uma cultura digital.

Paralelamente, e contemplando um trabalho estruturado e contínuo, permite promover esta transição com maior impacto, eficiência e índices de adoção.

Para Miguel Coelho, "a solução passou pela adoção, de forma contínua e estruturada, de uma ferramenta já presente na organização, o Microsoft 365".

Definiu-se um período inicial de meio ano, para trabalhar os principais temas associados

ao Microsoft 365 abrangendo temas específicos através de iniciativas regulares.

A familiaridade com outras aplicações Microsoft ajudou os 652 colaboradores do grupo a tirarem um maior potencial destas ferramentas colaborativas, juntamente com a experiência em projetos de adoção de M365 que dão uma maior garantia do incremento do trabalho colaborativo e da forma e eficiência como são usadas.

O RESULTADO

Para o Diretor de IT da Altri, a parceria com a Claranet tem como objetivo aumentar a capacidade de inovação e de divulgação das boas práticas da empresa.

"A Claranet tem sido um parceiro desde há vários anos para o desenvolvimento de projetos em tecnologias Microsoft com excelentes resultados nestas áreas", afirma.

Com a adoção do Microsoft 365 em modelo CMaaS, muitos processos internos passam agora a ser executados de uma forma mais célere, e as comunicações e informações passam também a ser partilhadas de forma imediata e descentralizada.

Para a Altri é fundamental criar uma dinâmica de transformação nos processos de trabalho onde a inovação promove mais inovação e existe

um ganho considerável de agilidade, escalabilidade, mobilidade, e paralelamente de aumento de segurança e resiliência.

Com esta adoção num modelo de as-a-Service, a Altri ganha capacidade de organização dos temas a serem abordados e, simultaneamente, promove uma cultura de mudança e aprendizagem contínua, aumentado assim a adoçao da tecnologia e destreza tecnológica dos seus colaboradores, abrindo portas a outros projetos de transformação digital. ■

"O QUE CRIA REALMENTE VALOR NAS ORGANIZAÇÕES SÃO OS PROJETOS INOVADORES E DE TRANSFORMAÇÃO"

António Monteiro entrou no Grupo Brodheim em 2018 para liderar o processo de transformação digital e tem com principal objetivo definir e implementar a estratégia de IT Governance. O Head of IT & Innovation do Grupo Brodheim considera que identificar as necessidades de negócio é fundamental para o sucesso de uma organização.

- António Monteiro, Head of IT & Innovation do Grupo Brodheim -

O GRUPO BRODHEIM conta já com mais de 70 anos de história e atua em dois grandes sectores: o *fashion retail*, onde o grupo detém mais de 65 lojas e tem vindo a expandir a sua cadeia de lojas próprias, sendo um representante exclusivo das mais prestigiadas marcas do mundo da moda premium (Guess, Furla, Timberland e Vans) e de luxo (Burberry, Tod's e Betrend). Inclui ainda o Wholesale (B2B) com representação de marcas cuja venda das coleções se destina ao comércio multimarca.

Já no setor da ótica, o Grupo Brodheim possui o grupo Optivisão que há mais 30 anos contribui ativamente para a prevenção dos problemas de saúde visual de todos os portugueses. Atualmente com dez lojas próprias e 250 lojas franquiadas, inclui ainda a Modavisão (B2B) que tem a representa-

ção de prestigiadas marcas internacionais de armações e óculos de sol (Silhouette, Neubau, ProDesign, Benetton, Porche Design).

EVOLUÇÃO E PERCURSO

Nos últimos anos, o grupo tem registado um crescimento muito acentuado devido à abertura de várias lojas de retalho no setor da moda e à aquisição do grupo Optivisão em 2016.
Toda esta situação criou uma enorme pressão nas tecnologias de informação do grupo.
António Monteiro, entrou no Grupo Brodheim em 2018 para liderar a transformação digital do grupo, com a missão de definir e implementar a estratégia de IT Governance que resultou na reorganização das funções de IT, contratação de novos colaboradores e elaboração e negociação de contratos de outsourcing com os seus parceiros.
"Desde essa altura temos vindo a consolidar uma estrutura mais eficiente que responde com eficácia aos desafios que são constantemente colocados pelo negócio", afirma António Monteiro, Head of IT & Innovation do Grupo Brodheim.

A ESTRATÉGIA DE TRANSFORMAÇÃO DIGITAL

O setor do retalho conta com lojas abertas a partir das 06h (no aeroporto) e que fecham às 24h (nos centros comerciais), numa operação praticamente "*non stop*" ao longo de 365 dias por ano.
Esta é uma atividade muito exigente no suporte às operações de negócio, e que obriga a uma constante monitorização dos equipamentos e sistemas para que o grupo possa estar preparado para uma reação imediata em caso de avaria de equipamentos e sistemas de loja.
"Esta foi uma componente muito importante. Dotar o setor de IT do grupo com ferramentas e sobretudo com bons parceiros que nos assegurem que somos eficientes na gestão e suporte às operações de negócio", explica.
Por outro lado, e o que na visão de António Monteiro, cria realmente valor nas organizações, "são os projetos inovadores e de transformação".
"Tivemos a preocupação de capacitar a organização com uma estrutura de IT, não só no apoio aos projetos desenvolvidos pelos nossos parceiros, mas também com a capacidade de desenvolver com autonomia alguns projetos internos".
Numa primeira fase foi efetuada uma avaliação aos processos, pessoas e tecnologias do grupo e foi ainda realizada uma cuidadosa avaliação do modelo de negócio e das necessidades a curto/médio prazo e de longo prazo, o que resultou na definição de um *roadmap* de transformação digital.
Foram então criadas várias iniciativas que se traduziram na implementação de projetos de transformação digital tendo sido criados dois grandes blocos: os projetos de eficiência operacional, que estão relacionados com a automação e digitalização de processos e que normalmente são projetos de duração mais reduzida, numa ótica de fazer mais e melhor, e se possí-

> // É IMPORTANTE PROCURAR AVALIAR EM CDA MOMENTO QUAL A MELHOR SOLUÇÃO E DE QUE FORMA ELA PODE CONTRIBUIR PARA MELHORAR O NEGÓCIO //

vel com redução de custo. Existem ainda os projetos mais estratégicos e inovadores que incorporam um maior valor para a organização e que estão associados a potenciar o aumento de vendas e apoiar novos modelos de negócio.

Nos últimos tempos e em virtude do contexto pandémico atual foram ainda desenvolvidas iniciativas de e-commerce, projetos de mobilidade e ligação do online às lojas físicas com o objetivo de proporcionar uma melhor experiência aos clientes.

A CHAVE

O Head of IT & Innovation do Grupo Brodheim considera que o fator-chave para uma empresa ser bem-sucedida no processo de transformação digital passa por uma boa identificação das necessidades de negócio, ou seja, uma boa especificação e uma criteriosa seleção dos projetos que possam contribuir para a organização com um ROI mais elevado, sendo ainda fundamental avaliar em cada momento de decisão o que melhor se ajusta ao processo de transformação digital.

"Muita resiliência, capacidade de adaptação constante aos fatores externos, muito critério nas propostas de investimento tecnológicas", estas são, para António Monteiro, as principais preocupações para um CIO numa perspetiva a curto prazo.

Por outro lado, acredita que também é necessário ter presente que este contexto estará ultrapassado dentro de alguns meses e é necessário preparar as organizações para o pós-covid com novos métodos, com novas ferramentas e mais digitalização, o que lhes permitirá, na altura do "arranque", estarem bem posicionadas.

Para o futuro, António Monteiro admite que existe uma grande expectativa em retomar rapidamente à "vida normal" e em receber os turistas que visitam Portugal e que representam uma fatia muito importante das vendas.

O objetivo é continuar a apostar no caminho da transformação digital, onde o grupo tem vários projetos em curso e outros previstos a curto e médio prazo.

"É importante procurar avaliar em cada momento qual a melhor solução e de que forma ela pode contribuir para melhorar o negócio", conclui. ■

CIONET

Em parceria com a CIONET Portugal

POR JOÃO FIGUEIREDO,
Diretor de Sistemas de Informação da
Santa Casa da Misericórdia do Porto (SCMP)

PANDEMIA 2.0 – CYBER ATAQUE ÀS INFRAESTRUTURAS CRÍTICAS DA SAÚDE?

Os processos de transformação digital em curso nas organizações, bem como a necessidade crescente de garantir a proteção contra os riscos digitais tem vindo a impulsionar a necessidade de mais profissionais e de novas competências.

A ESCASSEZ DE TALENTOS é um fenómeno global que está relacionado com os temas digitais de forma geral, mas em particular com as áreas de segurança de informação, levando as organizações a encontrarem novos modelos de colaboração com os fornecedores de segurança. Continuamos a assistir a um aumento do nível de sofisticação e do nível de determinação dos ataques. Os agentes de ameaça são de uma forma geral cada vez mais sofisticados, podendo enquadrar-se em quatro principais categorias – 1) Hacktivismo; 2) Espionagem industrial; 3) Cibercrime organizado; e 4) Estados-nação.

Nos últimos anos, com a proliferação das comunicações internet e da migração para a cloud, as organizações têm assistido a uma degradação do perímetro de segurança, sendo necessário cada vez um número mais alargado de equipamentos e ferramentas para proteger todos os novos ambientes.

A complexidade do ambiente de segurança da informação é em si mesmo, sendo cada vez mais necessários processos de gestão e integração que permitam uma visão global do ciclo de ameaça.

A introdução de tecnologias de 3.ª plataforma nas organizações, designadamente cloud, big data, mobile e *social business*, tem contribuído para uma maior complexidade dos ambientes

- João Figueiredo -
Diretor de Sistemas de Informação da Santa Casa da Misericórdia do Porto (SCMP)

de informação e tecnologias, obrigando à melhoria das práticas de operação e também das práticas de governança e gestão.

Neste contexto, tem-se verificado um fator crítico de sucesso a integração do tema da segurança da informação numa visão mais alargada do sistema de informação. Os fornecedores de serviços de segurança procuram cada vez mais integrar componentes de processos, pessoas e tecnologias nas suas ofertas, passando a existir uma cada vez maior dependência dos serviços de gestão de segurança na segurança geral das organizações e, consequentemente, uma necessidade cada vez maior de partilha de responsabilidades.

O aumento dos ativos conectados levou à necessidade de uma visão integrada da segurança que permita não apenas a proteção do sistema de informação, mas de todos os ativos conectados. À medida que as medidas de segurança centradas na rede e no perímetro ficam mais permeáveis, os investimentos em cibersegurança concentram-se em quatro pontos essenciais – identidades, aplicações, dados e dispositivos.

Atualmente, a segurança e a cibersegurança das SI/TIC são das maiores preocupações não só dos responsáveis de sistemas de informação das organizações, mas cada vez mais dos líderes empresariais e da própria população em geral. Com o aumento exponencial de ataques informáticos, o mercado denota uma notória falta de profissionais qualificados na área de especialidade de segurança informática, pelo que é fundamental que as organizações, recrutem no mercado colaboradores com perfis de segurança informática e *Ethical Hacking* visando dotar os departamentos de IT dos conhecimentos e ciberferramentas que permitam analisar e corrigir vulnerabilidades em sistemas de informação pessoais e de suporte às atividades das várias áreas de negócio da SCMP fundamentalmente na área da Saúde, onde os impactos podem ser de elevado prejuízo.

A título de exemplo apresentamos os últimos acontecimentos de agosto/2018, no grupo privado Hospitalar em Portugal afetado por SamSam ransomware. Este ransomware foi especialmente desenhado para atacar grandes infraestruturas, como os hospitais e sistemas *healthcare*, que são a principal vítima de ataques de ransomware realizados pelos *cyber actors*. [comunicado do grupo: "*no final do dia de ontem surgiram dificuldades no acesso ao sistema informático, motivadas pelo aparecimento de um vírus, prontamente detetado e controlado. Desde o primeiro momento estamos em estreita articulação com todas as autoridades competentes, nomeadamente com o Centro Nacional de Cibersegurança, estando igualmente a trabalhar proximamente com todos os nossos parceiros na resolução desta situação*."]

Informações reveladas, indicam que o grupo de hackers responsável por este malware consegue faturar atualmente cerca de 300 mil dólares por mês (o pedido de resgaste neste caso chegou aos 10 milhões de euros) e que o continua a desenvolver no sentido de lhe adicionar novas funcionalidades, sendo que o processo afetou toda a infraestrutura incluindo os processos de *backup*, pelo que o impacto à data de hoje, ainda se encontra por avaliar em termos de dimensão, ou seja, passados cerca de 20 dias, ainda não tinham sido repostos o normal funcionamentos dos suportes

aplicacionais, o que reforça a necessidade de antecipar temporalmente a elaboração de *Disaster Recovery Plan* e *Business Continuity Plan* para a área da saúdem em Portugal, investindo nestes pressupostos com elevada prioridade para o próximo triénio.

Assim deve ser previsto e implementada nova estrutura de segurança bem como no programa de segurança da informação da saúde com as seguintes componentes:

A. Gestão de serviços externos recorrendo a parceiro que apoiará no desenho e execução do Sistema de Gestão de Segurança da Informação (SGSI) e do plano de testes de segurança, promovendo paralelamente a melhoria contínua em alinhamento com os requisitos normativos e de documentação relativos à segurança da informação.

B. e integração na implementação de SOC (Security Operations Center), com foco a apoiar e proteger pro-ativamente a saúde contra as mais avançadas ciberameaças, incluindo malware, ransomware, fugas de informação, (data breaches), abusos de marca, e fraudes informáticas com impacto financeiro ([spear] phishing e CEO Fraud).

C. Articulação direta com o CNCS (Centro Nacional de Ciber Segurança) na perspetiva, de cumprir os requisitos do protocolo celebrado, formação e estreitar o modelo de relacionamento e cooperação entre ambas as entidades.

D. Integrar as estruturas de segurança, risco e compliance, marketing digital e DPO no projeto no sentido de garantir modelos de governação com sucesso.

A integração da gestão de identidade nas iniciativas de transformação digital é um fator crítico para a segurança da informação e tecnologias, melhorando a integridade das interações, reduzindo a dependência da segurança de rede e possibilitando medidas de segurança ao nível dos dados e das aplicações, com foco na área da saúde.

O "tribunal" da opinião pública funciona 24X7. Apesar das "massas" acreditarem que é possível obter segurança a 100%, os profissionais e as organizações sabem que tal não é possível de alcançar. Neste contexto, o diferencial entre as estratégias de segurança de duas organizações pode estar diretamente relacionado com o marketing e pelas relações públicas das organizações.

A confidencialidade, integridade e disponibilidade necessitam de outro objetivo – proteção física. Os ataques já não afetam apenas a Informação utilizada para a tomada de decisão, podendo afetar a disponibilidade de ferramentas, equipamentos, máquinas ou infraestruturas e consequentemente a operacionalidade de uma organização.

A penetração da robótica e das tecnologias IoT e a dependência de utilização destes ativos em tempo real leva a que a segurança física passe a ser um novo objetivo fundamental de controlo.

A confiança é conquistada quando as ações se juntam às palavras. Por isso fica a questão PANDEMIA 2.0: um *shutdown* das infraestruturas críticas da Saúde? ■

- IDC MULTICLOUD CONFERENCE -

10 e 11 - 03 - 2021

Digital

A IDC vai organizar a Multicloud Conference que irá conter com uma agenda dinâmica conduzida por analistas seniores da IDC, pioneiros da transformação digital e peritos em cloud híbrida. Será possível descobrir, por exemplo, as últimas novidades do mercado de multicloud híbrida.

- TRANSFORMAÇÃO DIGITAL -

25 - 03 - 2021

Digital

Em parceria com a IT Insight, a Infor e a Extreme Solutions vão apresentar como é possível apoiar há mais de 15 anos milhares de organizações a nível mundial a tomar mais e melhores decisões, a reportar a confiança e a medir e a planear o negócio com inteligência artificial.

- SMARTPAYMENTS CONGRESS -

01 - 06 - 2021

Digital / Oeiras

O SmartPayments Congress volta em 2021 para debater o que se pode esperar do setor financeiro. Numa edição híbrida, o SmartPayments Congress – que já vai para a 19.ª edição, vai continuar a desvendar as principais tendências na inovação bancária e dos meios de pagamento.

- THINK CONFERENCE -

24 a 26 - 06 - 2021

Leiria

A Think Conference é uma das principais conferências de marketing digital e empreendedorismo em Portugal, especialmente depois do sucesso das duas primeiras edições. A Think Conference tem como objetivo reunir os melhores especialistas destas duas áreas.

- Dormir numa estação de comboio -

A ESTAÇÃO DE COMBOIOS do Carregado tem 164 anos e foi transformada num hostel. A temática do hostel Estação Real está ligada ao universo ferroviário das viagens e da história que coloca a Estação do Carregado num lugar de destaque no panorama nacional.

O hostel tem capacidade para receber seis hóspedes e cada quarto é alusivo a uma figura de relevo para a história dos comboios em Portugal.

Ficar hospedado neste hostel custa entre 35 e 50 euros por noite e a reserva pode ser feita através do site de reservas Booking.

- A linha de roupa desportiva sustentável -

A BREATHE SPORTSWEAR é uma marca de roupa de desporto sustentável e 100% portuguesa.

Os responsáveis pela marca recorreram a matérias naturais como o Algodão BCI (*Better Cotton Iniciative*) e o Lyocell (Tencel), sem plásticos, promovendo um comércio justo e um menor desperdício e consumo de água.

Todos os tecidos produzidos são tingidos de forma natural sem recurso a produtos químicos, através dos extratos de plantas e cogumelos.

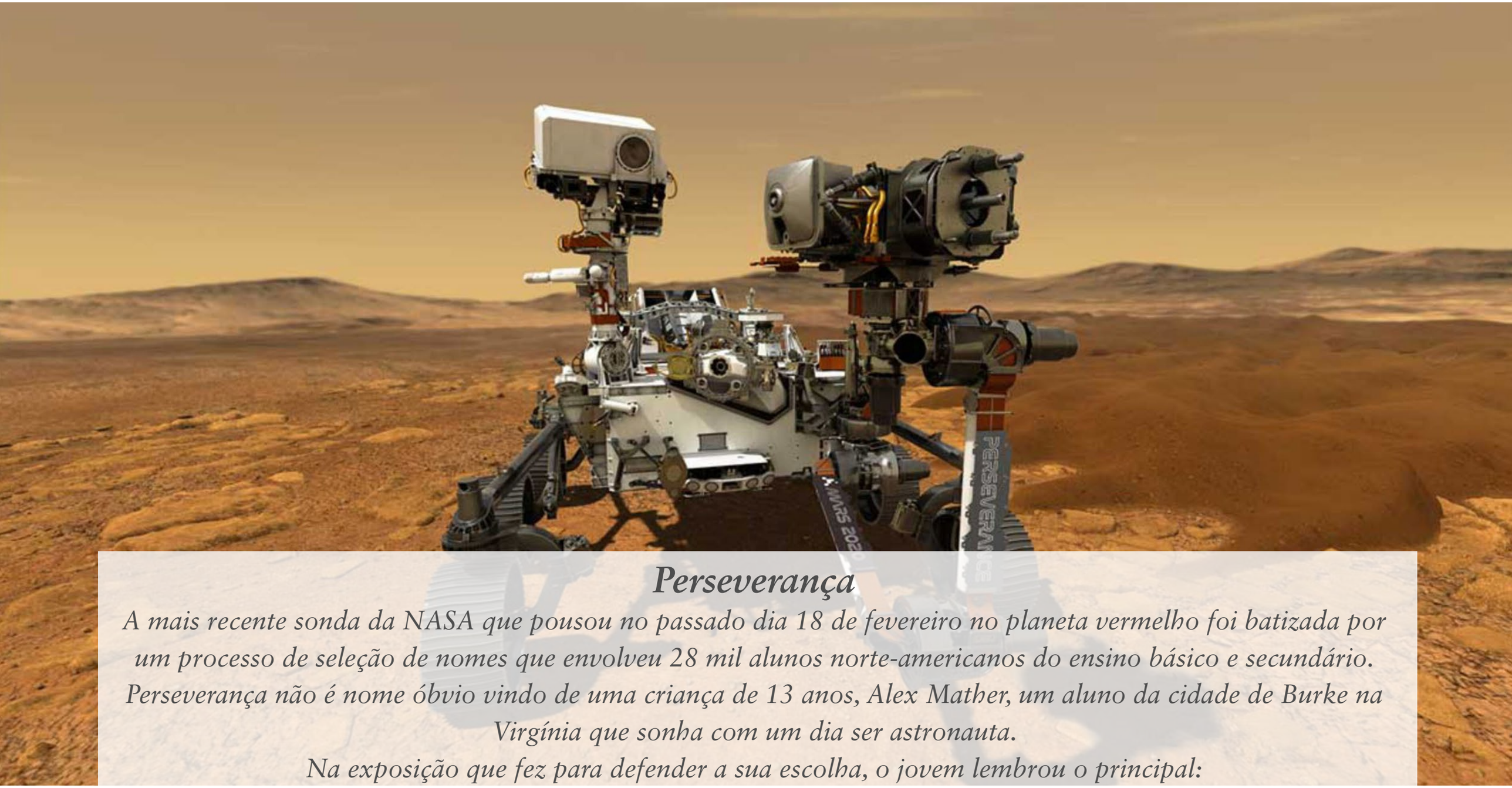
As peças estão apenas disponíveis no site e Instagram da marca portuguesa e fazem entregas para todo o mundo.

- Teleconsultas SOS Pediatria -

DEVIDO AO CONTEXTO PANDÉMICO atual e à situação de confinamento, a Lusíada Saúde lançou um serviço de videoconsultas para crianças até aos 17 anos de idade com o objetivo de dar uma resposta rápida e eficaz a episódios de urgência.

As teleconsultas podem ser marcadas no próprio dia, através da App, do Portal +Lusíadas ou através dos contactos das várias regiões.

O novo serviço de Teleconsultas SOS Pediatria está disponível em todo o país, 24 horas por dia e integra os acordos com as principais entidades seguradoras.



Perseverança

A mais recente sonda da NASA que pousou no passado dia 18 de fevereiro no planeta vermelho foi batizada por um processo de seleção de nomes que envolveu 28 mil alunos norte-americanos do ensino básico e secundário. Perseverança não é nome óbvio vindo de uma criança de 13 anos, Alex Mather, um aluno da cidade de Burke na Virgínia que sonha com um dia ser astronauta.

Na exposição que fez para defender a sua escolha, o jovem lembrou o principal:

- "Não há exploração sem perseverança", disse ele.

Na verdade, não há desenvolvimento cientifico e tenológico sem muita perseverança, porque sempre que rasgam horizontes, aumentam os obstáculos e a probabilidade de falhar .

Obrigado a Mather por nos lembrar.

#30 MARÇO **2021**

OBRIGADO POR TER LIDO A IT·Insight

*Para continuar a receber regularmente a sua IT Insight, por favor atualize os seus dados profissionais **aqui***

*Conheça a política de privacidade da IT Insight **aqui***

IT·Insight

DIRETOR: Henrique Carreiro
CHEFE DE REDAÇÃO : Rui Damião - rui.damiao@medianext.pt
REDAÇÃO: Diana Ribeiro Santos, Margarida Bento
JORNALISTA CONVIDADO: Fátima Ferrão
CONTENT PRODUCER : Lara Fonseca
GESTÃO DE PARCEIROS:
João Calvão - joao.calvao@medianext.pt
Rita Castro - rita.castro@medianext.pt
ARTE E PAGINAÇÃO: Teresa Rodrigues
FOTOGRAFIA: Rui Santos Jorge
WEB: João Bernardes
DESENVOLVIMENTO WEB: Global Pixel
COLABORARAM NESTE NÚMERO: João Figueiredo

A REVISTA DIGITAL INTERATIVA IT INSIGHT É EDITADA POR:
MediaNext Professional Information Lda.
PUBLISHER: Jorge Bento
CEO: Pedro Botelho
SEDE: Largo da Lagoa, 7c, 2795-116 Linda-a-Velha, Portugal
TEL: (+351) 214 147 300 | **FAX**: (+351) 214 147 301

IT INSIGHT está registada na Entidade Reguladora para a Comunicação Social nº127295

Consulte aqui o Estatuto Editorial

Editado por:

IT Insight é membro de: