IT Insight

#24 MARÇO **2020**

CX

CUSTOMER [BEST] EXPERIENCE

EY

Building a better working world

No mundo digital será que fazemos melhor ou apenas mais?

Quanto melhor a pergunta. Melhor a resposta. Melhor trabalha o Mundo.

IT Insight

#24 MARÇO **2020**

Ilustração: iStock/shelma1

INSIGHTS | DATA CONVERGE

Plataformas convergentes de dados e a democratização da analítica

COVERAGE

- IDC FutureScape 2020: Reputação e Inovação Digital

- Inteligência artificial em destaque no Building The Future 2020

SECURITY

O futuro do CISO nas organizações

TRANSFORM

BI4ALL aumenta eficácia do Pestana Hotel Group

IN DEEP | CUSTOMER EXPERIENCE

Como a experiência do cliente define a relação com as empresas

FACE 2 FACE | PRIMAVERA

"Queremos trazer ao produto informação sobre o futuro. Essa é a grande diferença, para além da cloud" - José Dionísio

ROUND TABLE | CIBERSEGURANCA

A crescente importância da cibersegurança

SUSTAINABILITY

Um novo mundo elétrico

Fotografias: Jorge Correia Luís

Imagem: iStock/Natali_Mis

DID YOU KNOW?

SAS® BRINGS ARTIFICIAL INTELLIGENCE AND ANALYTICS TO THE CLOUD.

You can run SAS on private, public or hybrid cloud infrastructures to better manage how AI work is done. SAS works with all major cloud providers to give you the power and freedom to innovate and be agile in the cloud.

sas.com/discover

@sas_portugal
company/sas
SAS Portugal - Business Analytics
sasportugal

sas®
THE POWER TO KNOW®

www.sas.com/portugal

IT Insight

#24 MARÇO **2020**

INSIGHTS

sas Cloud

BRANDED CONTENT

easyVISTA "O ITSM deve estar na lista de prioridades das organizações que enfrentam a transformação digital"

infor O casamento perfeito entre BI e Inteligência Artificial

SECURITY

S21SEC Insider Threats: a ameaça crescente para todas as organizações

ROUND TABLE

claranet PME são atrativas para os cibercriminosos

DRC A Governança da Insegurança

multicert O valor de um SOC

warpcom "O desenvolvimento de competências, celeridade de resposta e resiliência das organizações é crucial"

WhiteHat DLP: como proteger a sua empresa com uma abordagem integrada à cibersegurança

IN DEEP

EY Building a better working world Como testar se a sua estratégia de inovação é sustentável?

noesis A era da Experiência Digital

Schneider Electric A importância de colocar o cliente no centro da estratégia de negócio B2B

COVERAGE | IDC FUTURESCAPE

SABIA QUE..?

CIBERCRIME

JÁ É A MAIOR AMEAÇA

QUE AS EMPRESAS ENFRENTAM

NÃO SEJA O PRÓXIMO! ESTEJA PREPARADO.

SECURITY@MULTICERT.COM

HENRIQUE CARREIRO

Ser bom não é suficiente

SE TIVERMOS DE USAR uma palavra para definir a atitude em muitas empresas relativamente à experiência digital dos clientes, essa palavra poderá ser "complacência". Globalmente, as empresas despertaram para a importância do digital na criação de experiências para ganhar, servir e reter os seus clientes, mas demasiadas olham apenas para os concorrentes mais próximos para *benchmark* dos seus esforços, pensando que ser "bom" é suficiente para fazer crescer a sua base de clientes. Mas estes esperam mais: as expetativas são moldadas pelas experiências com as marcas líderes, ainda que noutras indústrias. E se muitas empresas estão a levar a cabo iniciativas de transformação digital, a maioria ainda está longe de procurar sequer otimizar a experiência dos clientes. Muitas vezes, são os processos internos que são expostos externamente, tornando complexas experiências que deviam ser simples. As melhorias incrementais tornam-se incompatíveis com o ritmo de crescimento das expetativas dos clientes, que são impulsionadas pelas melhores experiências e não pelas médias. Há empresas que pensam que estão a obter sucesso por se posicionarem a meio da tabela – infelizmente, tal já não é suficiente. Alguns dos maiores hiatos estão no empenho dos executivos de topo, no próprio nível de entendimento de tais questões, na agilidade, na capacidade de análise e na gestão adequada de parcerias. Todas estas são questões que devem ser endereçadas e resolvidas com celeridade, para que as empresas possam competir com os melhores e não simplesmente com os medianos. No que toca à transformação digital, a experiência do cliente é a pedra de toque, aquilo que não pode deixar de ser constantemente monitorizado, o ponto de aferição constante da estratégia e, eventualmente, o principal determinante do sucesso continuado da empresa. ■

S21 SEC

Complete coverage of cybersecurity risks in the business company processes

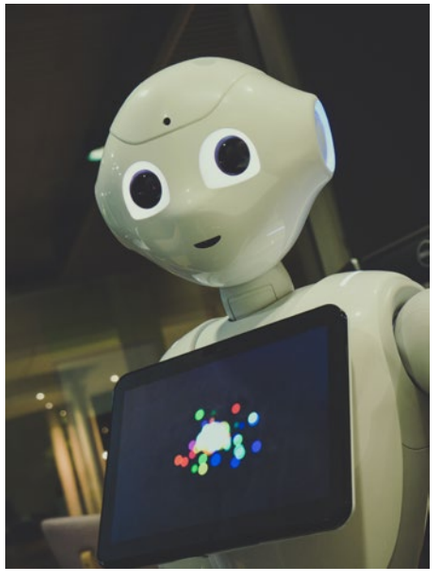

Identification


Protection


Detection


Response


Recovery



EUROPA MARCA POSIÇÃO NO USO DE INTELIGÊNCIA ARTIFICIAL

A Comissão Europeia apresenta novas ideologias para garantir que a Inteligência Artificial (IA) é usada de forma responsável, ao contrário do que acontece noutros países.

OS EUA E A CHINA são os principais responsáveis pelo uso da inteligência artificial e a União Europeia não quer deixar de marcar uma posição. Assim sendo, revelou uma nova abordagem da economia digital através da "Estratégia para moldar o futuro digital da Europa".

Esta nova estratégia da UE tem como principal objetivo estabelecer as regras sobre os dados e a IA europeus – uma regulação que "coloca as pessoas em primeiro lugar" e fomenta a "tecnologia confiável".

A organização europeia ressalva o seu desejo de tornar a tecnologia numa "força para o bem" e não uma que prejudique os cidadãos. Assim, divulgou um artigo sobre inteligência artificial como parte do anúncio da sua nova estratégia.

Este artigo descreve os riscos inerentes ao uso da IA "para rastrear e analisar os hábitos diários das pessoas" e o potencial das autoridades governamentais de explorar a tecnologia para a vigilância em massa. ■

RGPD LEVA A QUE OS HACKERS SEJAM DESCOBERTOS MAIS RAPIDAMENTE

As organizações ainda são muitas vezes vítimas de hackers, mas a FireEye sugere que a legislação de proteção de dados melhorou o tempo de resposta aos ataques cibernéticos.

A QUANTIDADE DE TEMPO que os hackers passam nas redes de organizações comprometidas antes de serem detetados diminuiu significativamente em toda a Europa e o RGPD é a principal razão pelo qual isso acontece.

O Relatório FireEye Mandiant M-Trends 2020 fez uma análise a ataques cibernéticos e revela que o tempo médio desde o início de um ataque até que é identificado caiu de 177 dias para 54 dias, uma redução de 70%.

O RGPD exige que as organizações que descubram uma violação de dados a denunciem à autoridade de proteção de dados num período máximo de 72 horas após o incidente ser descoberto, e caso isso não aconteça pode ocorrer uma penalização financeira significativa.

Toda esta situação levou a que as organizações europeias aumentassem o seu foco na segurança cibernética, levando a que invasões fossem descobertas mais rapidamente. ■

EcoStruxure™
Innovation At Every Level

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

GIGANTES TECNOLÓGICAS PODEM PASSAR A PAGAR MAIS TAXAS

A OCDE anunciou que perto de 140 governos concordaram em reescrever as leis de taxação entre fronteiras.

AS LEIS TRIBUTÁRIAS globais que regulam como as empresas são tributadas através de fronteiras internacionais devem ser reescritas para ter em conta as empresas que agora operam na era digital.

As leis existentes serão reformuladas depois de quase 140 governos concordarem em lançar uma revisão das regras tributárias transfronteiriças para a era digital nos próximos meses. O anunciou foi feito pela Organização para Cooperação e Desenvolvimento Económico (OCDE).

Há muito tempo que as tecnológicas são criticadas pelos governos e reguladores pelas suas práticas tributárias, o que as leva a reduzir as suas contas ao tributar os lucros em países com baixos impostos (como a Irlanda), independentemente da localização do cliente final.

As leis tributárias podem, no entanto, estar perto de mudar, uma vez que um grupo de 137 países e jurisdições concordaram em rever as leis tributárias transfronteiriças com o objetivo de chegar a um acordo até ao final de 2020. ■

INTELIGÊNCIA ARTIFICIAL ANALISA INCÊNDIOS URBANOS

O projeto de investigação da FCT Nova, o AI-4-MUFF, analisa os fogos urbanos para entender o fenómeno e permitir uma melhor gestão dos recursos da administração pública.

A FCT NOVA apresentou na sede da ANEPC o projeto de investigação AI-4-MUFF, onde estão envolvidas a UNIDEMI e a CMA, com a missão de analisar o fenómeno dos incêndios urbanos através da inteligência artificial e metodologias da ciência dos dados. O objetivo é desenvolver uma investigação sobre esta área e criar uma nova ferramenta que permita uma gestão mais eficaz dos recursos da administração pública.

A principal finalidade do projeto de investigação AI-4-MUFF é desenvolver uma ferramenta de apoio à ANEPC e às corporações de bombeiros locais para tomarem decisões tecnicamente mais fundamentadas, como por exemplo, como distribuir melhor os recursos humanos e equipamento, ou até, como definir qual a melhor localização para um quartel de bombeiros. ■

birst
an Infor® company

PLATAFORMA EMPRESARIAL AVANÇADA DE SOFTWARE ANALÍTICO E BI

Análise inteligente: A era da BI possibilitada pela IA

A inteligência artificial é a próxima onda de disrupção na BI e análise. A IA possibilita cumprir a promessa de proporcionar um ROI significativo às organizações, capacitando todos os funcionários a explorar o poder dos dados.

infor.com
Rua Ivens, 42 - 1º e 2º - Sala | 1200-227 Lisboa | 351.21.121.8000

ONU TERÁ ENCOBERTO FALHA DE SEGURANÇA

Uma falha de segurança terá comprometido 20 contas de administrador e terá sido implementado malware em 40 servidores.

A ONU terá sido invadida em 2019, mas a entidade optou por encobrir o incidente de segurança cibernética. Esta é a alegação depois de uma investigação do The New Humanitarian (NH), uma agência de notícias dedicada a assuntos humanitários, depois de supostamente encontrar um relatório confidencial sobre as redes e bancos de dados da ONU.

De acordo com o NH, a ONU tinha conhecimento de uma invasão dos seus sistemas de IT no ano passado, mas optou por não divulgar o assunto. "A ONU não divulgou publicamente um grande ataque de hackers aos seus sistemas de IT na Europa - uma decisão que potencialmente coloca funcionários, outras organizações e indivíduos em risco, segundo os defensores da proteção de dados", afirmou o relatório da NH.

O incidente resultou num "grande colapso", de acordo com um alto funcionário de IT da ONU familiarizado com as consequências, que falou com a NH sob condição de anonimato. Quando o NH pediu à ONU que comentasse, confirmou que manteve o hack em silêncio. ■

RECONHECIMENTO FACIAL PODE SER BANIDO NA UNIÃO EUROPEIA

A União Europeia considera banir a utilização de tecnologia de reconhecimento facial durante cinco anos para que os legisladores possam ter tempo de criar leis.

A UNIÃO EUROPEIA está a discutir uma possível proibição de utilização de tecnologias de reconhecimento facial em áreas públicas. Sistemas equipados com reconhecimento facial, como os encontrados em dispositivos móveis e câmaras, são defendidos pela polícia como uma maneira de seguir pessoas desaparecidas e como ferramentas úteis em investigações criminais.

No entanto, os críticos defendem que essa tecnologia é suscetível a abusos e a sua utilização sem o consentimento do público em geral compromete o direito à privacidade.

A UE está a considerar uma proibição de até cinco anos no reconhecimento facial em áreas públicas para dar aos políticos tempo para elaborar leis para impedir o seu abuso no futuro.

As propostas fazem parte de um *whitepaper* de 18 páginas que sugere que uma proibição poderá permitir a criação de uma "metodologia sólida para avaliar os impactos dessa tecnologia e possíveis medidas de gestão de riscos". ■

MULTAS POR VIOLAÇÃO DE PRIVACIDADE NA EUROPA ATINGEM 114 MILHÕES DE EUROS

Em 2018 entraram em vigor um conjunto de regras mais rigorosas sobre privacidade com diferentes abordagens, consoante o país.

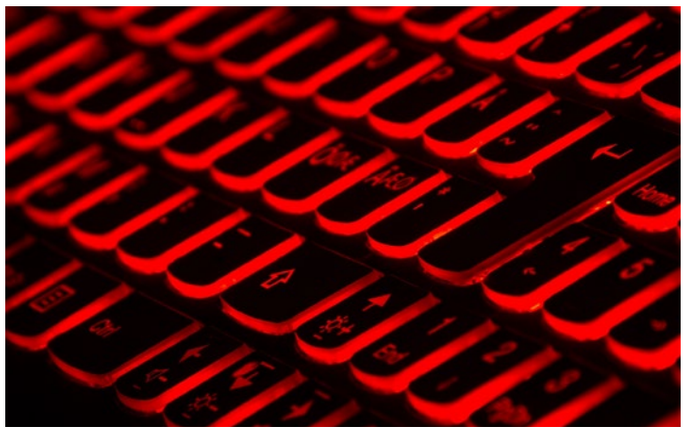
UM RELATÓRIO comunicou que foi em França que se impôs a maior multa individual - de 50 milhões de euros contra a Google -, enquanto Holanda, Reino Unido e Alemanha lideram em termos de número as notificações de violação de dados.

Estas penalizações são aplicadas por escritórios nacionais de proteção de dados em toda a União Europeia, constituídos por 28 membros, com uma responsabilidade desproporcional na Irlanda - país que é o principal regulador dos utilizadores de serviços de Silicon Valley que basearam as operações europeias no país, como o caso do Facebook.

Até ao momento, as multas ainda não tiveram um valor tão significativo, quando comparadas com multas de milhares de milhões de euros impostas a casos antitrust da UE. Uma situação que tende a alterar-se à medida que os recursos sujeitam as sanções a averiguação e a criar precedentes legais. ■

PORTUGAL ENTRE OS PAÍSES MAIS AFETADOS POR CAMPANHA DE MALWARE

A campanha RevengeHotels, direcionada ao setor hoteleiro, colocou Portugal como terceiro país da lista com mais vítimas.



A INVESTIGAÇÃO DA KASPERSKY sobre a campanha RevengeHotels, direcionada ao setor hoteleiro, confirmou que vários hotéis na Europa, América Latina e Ásia foram alvo de ataques de malware dirigidos. Portugal é o 3.º país da lista com mais vítimas que acederam ao link malicioso. Como resultado, a informação de cartões de crédito de hóspedes armazenados em sistemas de reserva dos hotéis, incluindo os recebidos por agências de viagem online, correm o risco de serem roubados e vendidos a criminosos de todo o mundo.

O RevengeHotels é uma campanha na qual participam vários grupos com a intenção de infetar empresas ligadas à hotelaria mediante a utilização de Trojans de Acesso Remoto (RATs). O principal vetor de ataque nesta campanha são emails com ficheiros maliciosos anexados, nos formatos de Word, Excel ou PDF. ■

noesis

Helping your business grow faster

Somos uma **consultora tecnológica** de referência, presente em 5 países, que oferece serviços e soluções para o apoiar na **transformação do seu negócio**.

Fornecemos soluções centradas em **infraestruturas, software, qualidade e pessoas**. Contamos com talentos altamente especializados, trabalhamos com as tecnologias mais inovadoras.

Infrastructure Solutions

Enterprise Solutions

Low-Code Solutions

Data Analytics & AI

ERP

Quality Management

DevOps & Automation

Professional Services

Portugal · Brasil · Irlanda
Holanda · EUA

IDC FUTURESCAPE 2020:

REPUTAÇÃO E INOVAÇÃO DIGITAL

O IDC FutureScape 2020 permitiu perceber de que forma as organizações reinventam os seus departamentos de IT e como se deve abordar tecnologias transformadoras para a criação de mais resultados para o negócio.

NO PASSADO DIA 18 de fevereiro, realizou-se o IDC FutureScape 2020. O evento contou com mais de dez sessões que reuniram os principais *players* do mercado e que teve como objetivo discutir os desafios que a atual transformação digital trouxe à economia.

FUTURE OF TRUST

A reputação das organizações depende cada vez mais da administração e proteção de dados dos clientes e é fundamental que as organizações tomem decisões baseadas na segurança destes, mostrando que estão preparadas para o futuro.

"Durante muitos anos lidámos com a segurança como um fenómeno de compliance. A decisão de risco tem uma grande importância nas organizações, essencialmente pela incerteza e porque nos preocupamos cada vez mais com a segurança para amanhã e não em resolvermos os problemas de ontem", garante Bruno Horta Soares, analista da IDC.

António Gameiro Marques do Ga-

PARA MUITOS, PORTUGAL NÃO É UM PAÍS DE RISCO, MAS A LÍNGUA É UMA DAS MAIS FALADAS NO HEMISFÉRIO SUL E NO CIBERESPAÇO

binete Nacional de Segurança-GNS, Miguel Jacinto do EuroBIC e Paulo Moniz da EDP integraram uma mesa redonda dedicada ao tema de *digital trust*. Paulo Moniz começou por explicar o alinhamento entre o IT e o OT que está presente em empresas como a EDP onde existem sistemas que controlam efetivamente alguma coisa, como por exemplo, abrir e fechar portas.

Enquanto o OT quer ter impacto na vida humana, o lado do IT necessita de confidencialidade. Isto implica que não exista um nível de risco nas infraestruturas críticas pois existe uma necessidade de alinhamento entre eles, sendo que os dois têm interesses diferentes.

Ainda dentro deste tema, António Gameiro Marques alerta que devemos ser cuidadosos quando utilizamos a expressão "integração OT/IT" e defende que cada vez mais os impactos mais fraturantes estão a migrar do IT para o OT e é no OT que o mundo virtual toca o físico e onde tudo acontece em tempo real e daí a gravidade dos ataques, como por exemplo, o roubo de dados.

No que toca à banca, Miguel Jacinto Banco revela que este setor também está preocupado, essencialmente com a monotorização do ciber risco e destaca ainda as competências necessárias para as infraestuturas de SOC.

"Para as organizações como o BIC que estão a implementar as infraestruturas SOC, ainda que os modelos possam ser híbridos, existe muita dificuldade em arranjar profissionais qualificados, sendo preciso recorrer à IA", refere.

"Grandes grupos como a banca, a energia e os portos que utilizam muito OT, deviam evoluir não só para um SOC, mas para um CSIRT (*Computer Security Incident Response Team*) porque o *mindset* de alguém que está num SOC é *in words* e o CSIRT ajuda a organização a agir depois de um ataque, trabalhando na reputação da organização", afirma António Gameiro Marques.

Nos últimos anos, as empresas preocupam-se apenas com o facto de estarem individualmente protegidas e isto acaba por ser um motivo de competição quando, atualmente, já não deveria ser uma questão.

Para muitos, Portugal não é um país de risco. Já para António Gameiro Marques isto não é bem assim, visto que o português é umas das línguas mais faladas no hemisfério sul e uma das mais utilizadas no ciberespaço, sendo assim um veículo de ataque.

Se a IDC tem publicado previsões que reforçam o auxílio das entidades públicas neste contexto, no GNS foi criado um *roadmap* onde se pode verificar o nível de maturidade e o que cada organização pode fazer para chegar ao nível pretendido.

No fim de janeiro, foi publicado o quadro de avaliação de capacidades que reflete, segundo o *framework*, qual o nível em que a empresa se encontra nas cinco componentes da cibersegurança.

Outro dos pontos fulcrais da segurança e da reputação de uma organização é o *phishing* e a evolução dos modelos de autentificação.

"As pessoas já não querem utilizar *passwords*. Preferem utilizar modelos de autentificação moderna. Quanto às mensagens de *phishing*, esta situação só vai mudar quando forem todos nativos digitais", afirma Paulo Moniz.

FUTURE OF DIGITAL INNOVATION

Uma outra sessão que decorreu no IDC FutureScape 2020 foi dedicada ao futuro da inovação digital. Atualmente, as organizações têm de aprender a lidar com a procura de uma personalização extrema do uso da tecnologia.

É necessário que as organizações criem uma maneira de ir ao encontro desta personalização e aprendam a competir neste mercado de forma diferenciada. Para isto, as empresas precisam de se transformar em fábricas de inovação digital, assentes na produção própria de software, sendo necessário uma abertura das empresas para a inovação, bem como uma abertura do ecossistema.

"Os clientes têm de ter noção que o seu negócio tem agora um negócio complementar de desenvolvimento de software com um impacto bastante positivo na sua atividade. Uns chegaram lá por vontade própria e outros porque foram empurrados pelo mercado", conclui Sérgio Viana da Xpand IT.

Para Miguel Sousa do Super Bock Group, a experiência com o consumidor está a sofrer uma transformação e por isso tem explorado o mercado junto da academia e das incubadoras de startups.

"Para esta mudança, o IT é o parceiro ideal para abrir o leque dos inputs que chegam dos negócios", explica Filipe Morla da Mota Engil.

Nuno Matos dos CTT partilha a mesma opinião e garante que é importante "diversificar as novas linhas de negócio, oferecendo uma linha digital e transformação interna".

Ana Rocha de Oliveira da Red Hat discorda e acredita que "não há um modelo que sirva para todos". ■

O FUTURO DAS EMPRESAS

THOMAS MEYER, GENERAL MANAGER E GROUP VICE PRESIDENT, IDC EUROPE

"As empresas precisam de se concentrar no valor que estão a entregar aos seus clientes e colaboradores, mas, obviamente, também aos acionistas. O retorno para eles, mas também o retorno para a comunidade.

É necessário criar uma estratégia, focar em casos de uso que são possíveis por causa da tecnologia. O foco na inovação é muito claro, porque não há muitas organizações a ganhar dinheiro no digital. Este é um foco principal, mas também se concentra no elemento tecnológico para permitir que todos no ecossistema façam parte desse mesmo ecossistema. O aspeto das pessoas é muito importante.

Encorajo todos a pensar no futuro das práticas que construímos em torno da inovação digital, no futuro do trabalho e em todos os diferentes elementos que reunimos e realmente descobrir o que o CEO deseja e como o modelo de negócio irá ser em cinco anos a partir de agora."

O PAPEL DO CIO

MARC DOWD, PRINCIPAL, CLIENT ADVISORY, IDC

"A pergunta sobre o papel do CIO em termos de inteligência, agora e no futuro, é realmente interessante. Acho que se está a tornar mais importante agora. O papel do momento para muitos CIO é realmente sobre a recolha e a gestão de dados, e isso é um problema. Como sabemos através da nossa pesquisa, cerca de 88% dos dados são *dark data* e, na verdade, não são usados para nada, o que é um grande desperdício. A quantidade de dados recolhidos durante todo o tempo está a crescer exponencialmente, o que significa que podem continuar a ser uma função do CIO e fazer o que faziam antes, que está a reunir os dados.

Acredito que o papel mais importante é utilizar esses dados e de repente vejo entre os clientes mais avançados que há um foco em realmente analisar o uso dos dados nos negócios. Muito disto é sobre aprender a utilizar os dados, superando a aversão aos dados que as pessoas têm e que estão em todos os tipos de níveis.

As pessoas gostam de dados para fazer o trabalho, mas às vezes não. Muitas vezes é possível ver pessoas no topo das organizações que tomam decisões instintivamente e o papel do CIO a ajudar realmente a mudar essa maneira de ver os dados no futuro."

DRC®
INSPIRING
DATA
SECURITY

Consultoria

Segurança da Informação
ISO 27001
ISO 22301
RGPD

Auditoria

Gestão de Vulnerabilidades
Testes de Intrusão
Análise Forense
Simulações Phishing
Soluções / Integração

Serviços Técnicos

Recuperação de Dados
Apagar com segurança
Destruição de Dispositivos

Formação

Formação Presencial
Formação e-Learning

DRC

DATA, RISK & CONSULTING

www.drc.pt

Rua Quinta Do Pinheiro, Edifício
Tejo, Nº16 2º E, 2790-143
Carnaxide

TEL.: 214 146 810
FAX: 214 146 819
EMAIL: geral@drc.pt

Descarregue aqui
a brochura completa

INTELIGÊNCIA ARTIFICIAL EM DESTAQUE NO BUILDING THE FUTURE 2020

Como um dos temas mais marcantes da transformação digital, a inteligência artificial e o seu impacto nos negócios foi um dos tópicos centrais do Building the Future 2020, que teve lugar entre 28 e 30 de janeiro em Lisboa

MARGARIDA BENTO

A INTELIGÊNCIA ARTIFICIAL (IA) é um dos maiores desafios que a indústria de tecnologia enfrenta nos dias de hoje. Apesar de ainda estar nas suas fases iniciais já é uma expectativa – quanto mais avançamos na transformação digital cada vez mais se espera que estas soluções tragam valor acrescentado.

Segundo a Gartner, até 2025, cerca de 30% dos negócios irão usar a IA para otimizar alguma atividade dentro da empresa – e 95% das interações de atendimento ao cliente serão potenciadas por esta tecnologia.

"Isto significa que em 2025 será difícil distinguir entre o atendimento realizado por uma pessoa ou um sistema de inteligência artificial", refere Vasco Pedro, CEO e fundador da Unbabel e principal orador na sessão '*Making every business an AI driven business*', que ocupou grande parte da manhã do primeiro dia. "Mesmo hoje, 88% das empresas na Europa já estão a implementar IA na analítica e processos".

Este rápido avanço traz consigo, naturalmente, preocupações, especialmente no que toca ao mercado de trabalho. O refrão da indústria é, de mo-

mento, que a IA vai criar mais empregos que substitui, ou que simplesmente nos vai tornar mais eficientes.

Para Vasco Pedro, a inteligência artificial vai mais além – vai tornar o trabalho mais humano.

NARROW AI E HUMAN AUGMENTATION

Quando falamos em IA, o que a maioria das pessoas pensa é uma réplica da mente humana, que ainda é tecnologicamente impossível. Aquilo a que nos referimos atualmente como IA é a denominada como "Narrow AI", a aplicação de técnicas de machine learning a problemas e tarefas altamente específicos. Através da deteção de padrões em grandes volumes de dados, a Narrow AI permite associar resultados a um grande número de variáveis com relações extremamente complexas entre si. Isto significa que, para alcançar um nível de exatidão aceitável, qualquer aplicação de inteligência artificial tem de ser restrita a uma única tarefa.

"É por isto que estamos a ver impacto em áreas altamente específicas, como atendimento ao cliente e reconhecimento de imagens", explica Vasco Pedro.

Adicionalmente, acrescenta, nenhum sistema de IA verdadeiramente eficaz é autossuficiente. "A IA é muito boa a aprender rapidamente como realizar tarefas numa área muito específica, mas requer enormes quantidades de dados para treinar", refere o CEO. "É por isso que os casos em que a inteligência artificial funciona realmente bem são aqueles em que existe uma interação entre o machine learning e o chamado "*human in the loop*" (...), em que há um humano envolvido, ou a gerir um processo com a assistência da IA, ou a monitorizar e gerar dados para treinar a aplicação".

E aqui, finalmente, entra o conceito de human augmentation. A grande maioria das aplicações de inteligência artificial no presente e no futuro próximo consistem na automação de tarefas repetitivas que constituem parte do trabalho das pessoas, não a sua totalidade.

"As coisas aborrecidas e repetitivas que fazemos hoje em dia vão ser automatizadas, e isto vai libertar as pessoas para serem mais criativas e para terem mais tempo para investir em atividades humanas," explica Vasco Pedro.

- Vasco Pedro, CEO e fundador da Unbabel -

Interações sociais complexas, criatividade, subjetividade, interpretação de nuances – tudo isto se mantém no domínio exclusivamente humano e é indispensável para grande parte das funções que as pessoas representam nas empresas.

Um exemplo já utilizado – e que continuará a crescer nos próximos anos – é o apoio ao cliente. A fase de triagem é totalmente automatizada através de sistemas hierárquicos, o que poupa nos recursos humanos, mas gera

- Sofia Carvalho, vice-presidente, IRN -

grande frustração do lado do cliente, o qual, havendo essa possibilidade, tende a escolher ser atendido por uma pessoa. Com a inteligência artificial, este processo é realizado também de forma automática, mas através de uma interface de voz indistinguível de um humano, e uma vez determinada a necessidade do cliente a chamada é transferida para o agente humano indicado. A IA permite, assim, reinvestir o dinheiro poupado pela automação para criar uma experiência mais humana e, ao mesmo tempo, mais eficiente.

O mesmo se aplica ao atendimento médico. Num esforço para otimizar e agilizar este processo, a digitalização transformou uma situação na qual a comunicação e empatia são extremamente importantes numa interação robótica. Ao libertar o médico da tarefa de inserir manualmente os dados do cliente no sistema informático, interfaces de voz potenciadas por IA vão permitir que exista de facto um diálogo aberto nas consultas médicas, permitindo um melhor diagnóstico e uma melhor compreensão por parte do paciente das instruções e recomendações do médico.

"A questão aqui é como é que nos afastamos dos ecrãs e recuperamos a ligação humana", conclui Vasco Pedro.

Isto não é uma previsão do futuro – espera-se que o mercado das tecnologias de human augmentation chegue a 2,9 biliões de dólares até ao final deste ano.

O CASO DO IRN

A IA já chegou ao Governo português – nomeadamente ao Instituto dos Registos e do Notariado, representado no Building the Future por Sofia Carvalho, vice-presidente.

O projeto apresentado consistiu na utilização de IA para simplificar e agilizar o processo de inventariado das propriedades no território português ao reverter o sistema prévio, que envolvia pedir as informações junto aos proprietários e confirmar posteriormente por imagens aéreas. Através de um sistema de inteligência artificial que, com o contexto de dados prévios, consegue detetar nas imagens aéreas padrões que indiquem com bastante precisão a localização e delimitação de propriedades, o IRN passou a precisar apenas de confirmar os resultados junto dos proprietários, agilizando o processo de tal forma que conseguiu analisar, em 12 meses, 52% das matrizes prediais anteriormente desconhecidas.

"O projeto ainda se encontra de momento em fase de expansão, mas demonstrou que era possível, em 12 meses, marcar a diferença com recurso a esta tecnologia", conclui Sofia Carvalho. ■

WhiteHat®
DESDE 2003

A sua ponte para a cibersegurança

Distribuição de soluções:

- Anti-malware
- Segurança de Perímetro
- Reforço de Autenticação
- Backup e Disaster Recovery
- Encriptação e Protecção de Dados

www.whitehat.pt

ESET
untangle
Macriumsoftware
Your image is everything
peplink
Infrascale™
COSOSYS

PLATAFORMAS CONVERGENTES DE DADOS E A DEMOCRATIZAÇÃO DA ANALÍTICA

As soluções de analítica unificada estão a mudar a forma como as empresas gerem e utilizam os seus dados, levando à democratização das soluções de analítica e inteligência artificial e maximizando o valor que estas trazem ao negócio.

MARGARIDA BENTO

CADA VEZ MAIS NEGÓCIOS procuram usar os dados para otimizar os seus processos, serviços e tomada de decisões através de aplicações de analítica avançada e inteligência artificial.

Contudo, o mesmo volume, variedade e complexidade de dados que possibilitam estas aplicações tornam extremamente difícil para as empresas extrair *insights* e criar valor a partir dos dados. Isto porque o esquema tradicional de gestão de dados dentro das empresas carece da agilidade necessária, o que se prende maioritariamente com três fatores: as fontes dos dados, a sua natureza e as suas aplicações.
Tradicionalmente, o fluxo de dados dentro das empresas é comparativamente simples e estruturado.

Dados provenientes dos sistemas internos como CRM e ERP são armazenados em *data warehouses*, e posteriormente usados para analítica.

Neste modelo, os dados estão estruturados, provêm de um número reduzido de fontes internas de natureza semelhante, e são pré-estruturados para análise. A aplicação de analítica em si é, também, comparativamente estruturada: maioritariamente analítica descritiva e avaliação de resultados para suportar futuras decisões.

Como tal, o isolamento dos dados pode ser considerado coerente com este modelo: cada departamento ou equipa precisa apenas de acesso aos dados que lhes competem e, caso haja necessidade de dados de outras fontes – para apresentar relatórios ou para contextualizar decisões em departamentos sinergéticos como o marketing e as vendas –, não há necessidade de elevados níveis de agilidade e automação. Partindo do princípio que tudo o que a empresa precisa para manter a competitividade é a análise periódica de KPI para suportar decisões com base em instinto e experiência, este fluxo é adequado.

Contudo, no momento em que saímos destas aplicações tradicionais e passamos a incluir analítica avançada, IoT, big data e inteligência artificial, os paradigmas da gestão e processamento de dados tornam-se completamente diferentes.
Em primeiro lugar, as fontes de dados são muito mais variadas; para além dos sistemas da empresa, incluem também novas fontes como sensores de IoT, dados internos anteriormente não utilizados como documentação e emails, dados externos provenientes da Internet e de parceiros, etc..
Assim, onde antes tínhamos pequenos ou médios volumes de dados altamente estruturados passamos a ter grandes volumes de dados pouco estruturados, provenientes de fontes dispersas que, em termos de IT, estão totalmente isoladas entre si.

Por fim, existe também uma enorme diversificação da aplicação destes dados. Onde antes havia apenas aplicações de analítica descritiva, as empresas estão a adotar cada vez mais funcionalidades preditivas e prescritivas. Onde antes se atuava ao nível do mês, trimestre ou ano, cada vez mais aplicações requerem analítica em tempo real ou quase real. Aplicações cada vez mais diversas e sofisticadas, de motores de recomendação à geração de alertas, têm requisitos específicos de gestão de dados e ciclo de vida analítico. Mesmo as simples decisões de negócio requerem mais agilidade e adaptabilidade de forma a que a empresa possa ser competitiva no mercado em que se insere.

Como tal, o armazenamento dos dados em silos deixa de ser sustentável: as aplicações de analítica e inteligência artificial necessitam de todos os dados relativos à empresa para contextualizar as suas conclusões e decisões e a rapidez de resposta exigida requer que o fluxo e gestão dos dados sejam feitos de forma automática e eficiente.

Isto constitui um enorme obstáculo à adoção da analítica avançada e inteligência artificial, uma vez que requerem um forte investimento não só na solução propriamente dita, como também na reestruturação dos processos e infraestrutura de IT, deixando estas tecnologias fora do alcance da maioria do tecido empresarial e reduzindo o apelo do investimento por parte das empresas que podem de facto comportar estes custos.
A capacidade de unificar todo o processo de gestão e análise de dados dentro das empresas, seja ao nível do armazenamento, gestão da analítica ou aplicações específicas, sem os custos e riscos associados à reestruturação do IT, vem

potenciar a adoção e a democratizar o acesso a tecnologias de analítica, IoT, big data e inteligência artificial. Plataformas convergentes de dados permitem agregar dados armazenados em silos, unidades de negócio e equipas diferentes, oferecendo a todos uma visão global e holística do negócio de forma a suportar decisões informadas.

O processo de preparação dos dados para análise é complexo – as organizações passam uma quantidade significativa de tempo a preparar e a contextualizar dados antes mesmo de estes serem processados. Quanto mais avançada a analítica, maior é a importância da qualidade dos dados e, simultaneamente, o volume de dados necessário. Para além de facilitar a criação de *pipelines* de dados entre vários sistemas de armazenamento de dados, plataformas de analítica unificada vão mais além ao automatizar a gestão dos dados através de machine learning, aumentando a eficiência da implementação e manutenção – por exemplo, ao permitir usar o mesmo algoritmo em *datasets* diferentes em vez de desenvolver modelos individuais.

CLOUD E PLATFORM-AS-A-SERVICE

Outra das grandes vantagens das plataformas unificadas é a simplificação da infraestrutura através de serviços cloud. Mais uma vez, a infraestrutura é um dos grandes investimentos e condicionantes destas tecnologias. Ao oferecer serviços cloud de armazenamento e processamento, as plataformas de analítica unificada facilitam a adoção destas tecnologias ao reduzir o CapEx incial. A tendência é que ao longo do tempo as empresas vão formando um *mix* de multicloud e cloud híbrida consoante as suas necessidades, ecossistema pré-existente e "*vendor lock-in*" – pelo menos nas grandes empresas, nas quais o poder de escolha e a necessidade de personalização são maiores.

Soluções cloud, por outro lado, permitem reduzir a complexidade operacional e os requisitos de infraestrutura, proporcionando uma escalabilidade praticamente ilimitada. A adoção de soluções em cloud pública como, por exemplo, as que fazem parte da oferta da Amazon, da Google ou da Microsoft, são um dos principais fatores de democratização da IA e da analítica.

A ESCOLHA CERTA

Ao considerar a adoção de uma plataforma dados, a prioridade deve ser as necessidades do negócio – as soluções devem ser escolhidas com base nos resultados pretendidos, não na tecnologia aplicada. A escalabilidade e a

- Nuno Barreto -
Partner & Big Data Lead da Xpand IT

A CAPACIDADE DE UNIFICAR A GESTÃO E ANÁLISE DOS DADOS, SEJA AO NÍVEL DO ARMAZENAMENTO, DA ANALÍTICA OU DE APLICAÇÕES ESPECÍFICAS, POTENCIA A ADOÇÃO E A DEMOCRATIZAÇÃO DA ANALÍTICA

integração são, assim, prioritárias, de forma a que a solução se possa adaptar à evolução da empresa e do mercado.

"Recomendaria que, em vez de procurar uma solução que resolve tudo agora, garantam que há sempre um futuro", refere Nuno Barreto, Partner & Big Data Lead da Xpand IT. "A melhor abordagem é apostar, primeiro, num conjunto de soluções contido que resolve 80% dos problemas, e a partir daí, ambicionar reduzir o gap dos restantes 20%".

Diferentes plataformas permitem endereçar diferentes níveis deste processo. Algumas, como o Databricks, atuam ao nível da analítica, outras ao nível do armazenamento. Algumas, como o PowerBI da Microsoft, são indicadas para *reporting* e exploração de dados por parte de utilizadores das áreas de negócio, outras são mais adequadas a utilizadores das áreas tecnológicas. Alguns fornecedores, como o SAS, procuram abranger todo um espetro de aplicações com uma única plataforma, enquanto outros se especializam.

"Cada organização deverá procurar o melhor equilíbrio, dentro até da capacidade de gestão operacional que tem em cada momento, entre funcionalidade, limitações e *vendor lock-in*", explica Nuno Barreto.

O último ponto é particularmente importante para questões de escalabilidade. Se uma empresa escolher, por exemplo, uma plataforma de dados que atua apenas ao nível do armazenamento, mas mais à frente começar a investir mais em analítica, é determinante que as duas plataformas sejam integráveis, especialmente se o fabricante da primeira solução não tiver uma oferta de analítica adequada às necessidades específicas do negócio.

A integração e o ecossistema de parceiros do fornecedor são, assim, fatores a ter em conta na escolha de uma solução. É também importante que esta ofereça uma boa integração com o restante ecossistema: plataformas de suporte a armazenamento devem integrar-se bem com os sistemas de segurança da empresa, soluções de exploração de dados devem-se integrar com os motores de *query* existentes, etc..

"Diria que, numa solução completa de *analytics*, a componente que beneficia da consolidação/integração é a fonte de dados sobre o qual a *top layer* da solução assenta, ou seja, é necessário que os dados potencialmente utilizáveis estejam disponíveis, securizados e governados", refere. ■

POR JOÃO OLIVEIRA,
Principal Business Solutions Manager,
Data Management & Decisioning,
SAS Western Europe Customer Advisory

– CLOUD –

Se tivesse que escolher a buzzword do momento seria Transformação Digital, no entanto esta palavra remete-nos de imediato para muitas outras como Cloud, Inteligência Artificial, Machine Learning, Blockchain, Realidade Aumentada e por aí adiante.

CENTREMO-NOS NA CLOUD. Cada vez são mais as organizações que optam pela migração para a Cloud, no entanto há ainda muitos "mas" nesta transição que, acredita-se, representa o futuro...

Quando se fala de Cloud temos de ter em conta que há vários tipos de serviços Cloud, os principais são: **IaaS** – Infrastructure as a Service – que é a disponibilização dos serviços computacionais básicos, ou seja computação, armazenamento, conectividade (virtualizados e/ou não), sendo da responsabilidade do cliente a instalação, operação e manutenção de tudo o que demais necessita, desde o sistema operativo, middleware, aplicações, … ; **PaaS** – Platform as a Service – que é a disponibilização de uma plataforma completa e pronta para o cliente desenvolver / instalar, operar e manter as suas aplicações; **SaaS** – Software as a Service – em que o cliente subscreve a utilização de aplicações como utilizador final. Tais serviços existem em Cloud Pública, mas também podem ser implementados em Cloud Privada, em que a organização se dota de todas as capacidades.

Assim, uma das questões que se levanta é saber o momento certo para avançar com esta mudança e mais importante, qual a estratégia de migração.. que tipo de serviços computacionais (IaaS, PaaS, SaaS), que sistemas, que funcionalidades, quando, como, se tudo em Cloud Pública ou Privada ou Híbrido. Para isso, convém ter presente os benefícios mas também aspectos a considerar que podem limitar ou mesmo impedir a migração para a Cloud.

FOCANDO-NOS APENAS NOS SERVIÇOS DE CLOUD PÚBLICA:

Os principais e mais evidentes benefícios:

Acesso anywhere, anytime, any device. Ou seja, se há uns anos, os sistemas e aplicações estavam somente acessíveis se se estivesse conectado aos sistemas dentro dos "muros" da organização (inclui acesso via VPN) e utilizando

- João Oliveira -
Principal Business Solutions Manager, Data Management & Decisioning, SAS Western Europe Customer Advisory

dispositivos como os PCs ou portáteis. Com os sistemas na Cloud, eles passam a estar disponíveis a toda hora em qualquer lugar com acesso à Internet e com a mesma performance e nível de serviço (dependendo apenas da qualidade da ligação à Internet). Tal disponibilidade faz com que as organizações evoluam na democratização do acesso aos sistemas numa filisofia de self-service. Isto sendo um enorme benefício traz também grandes desafios em relação à gestão da informação (acesso, salvaguarda, qualidade, governação, ..) e também de potenciais violações (vulgo hacking).

ACESSIBILIDADE, DISPONIBILIDADE E ELASTICIDADE.

Trazem um maior controlo dos custos associados com os sistemas de informação devido ao modelo de subscrição *pay what you use*, *pay-per-use*. Em conceito estas são de facto aquilo que aos olhos dos gestores, faz a migração para a Cloud tão atractiva. No entanto há ainda as razões técnicas relacionadas com a manutenção, suporte e garantia de nível de funcionamento e resposta dos sistemas de informação. Por exemplo, instalação de updates e/ou upgrades do software, garantia que o hardware é o mais adaptado às novas versões do software, substituição do hardware em caso de avaria, backups, segurança (encriptação dos dados, tráfego, acessos, etc.). Questões estas que são resolvidas no imediato ao optar por esta via.

Alguns dos obstáculos a considerar:

Todas as organizações têm um passado e com isso múltiplos sistemas de diversas gerações e mais diversas tecnologias, desde mainframes mais ou menos flexíveis até sistemas modernos e modulares. Ora com isso podem existir sistemas que simplesmente não são possíveis de migrar para a cloud, outros que o sendo os custos de o fazer não justificariam os benefícios, outros que devido a obrigações legais ou políticas internas não podem estar numa Cloud Pública. Em qualquer situação de migração para a Cloud há sempre que considerar como garantir a integração e interoperabilidade dos sistemas que irão para a Cloud e os que ficam, ou seja modelo Híbrido.

CONCLUSÃO

Constatamos assim que, passar da plataforma para a Cloud, traz vários benefícios e facilmente podemos considerar que este é o passo mais facilitador para as empresas responderem às atuais exigências do mercado. Há que perceber, contudo, que esta deve ser uma tomada de decisão ponderada e sustentada, não devendo por isso deixar de considerar todos os prós e contras.

O migrar para a Cloud Pública, permite às organizações concentrarem-se cada vez mais no seu negócio e actividades centrais, beneficiando dos serviço dedicados e especializados que respondem às necessidades da organização.

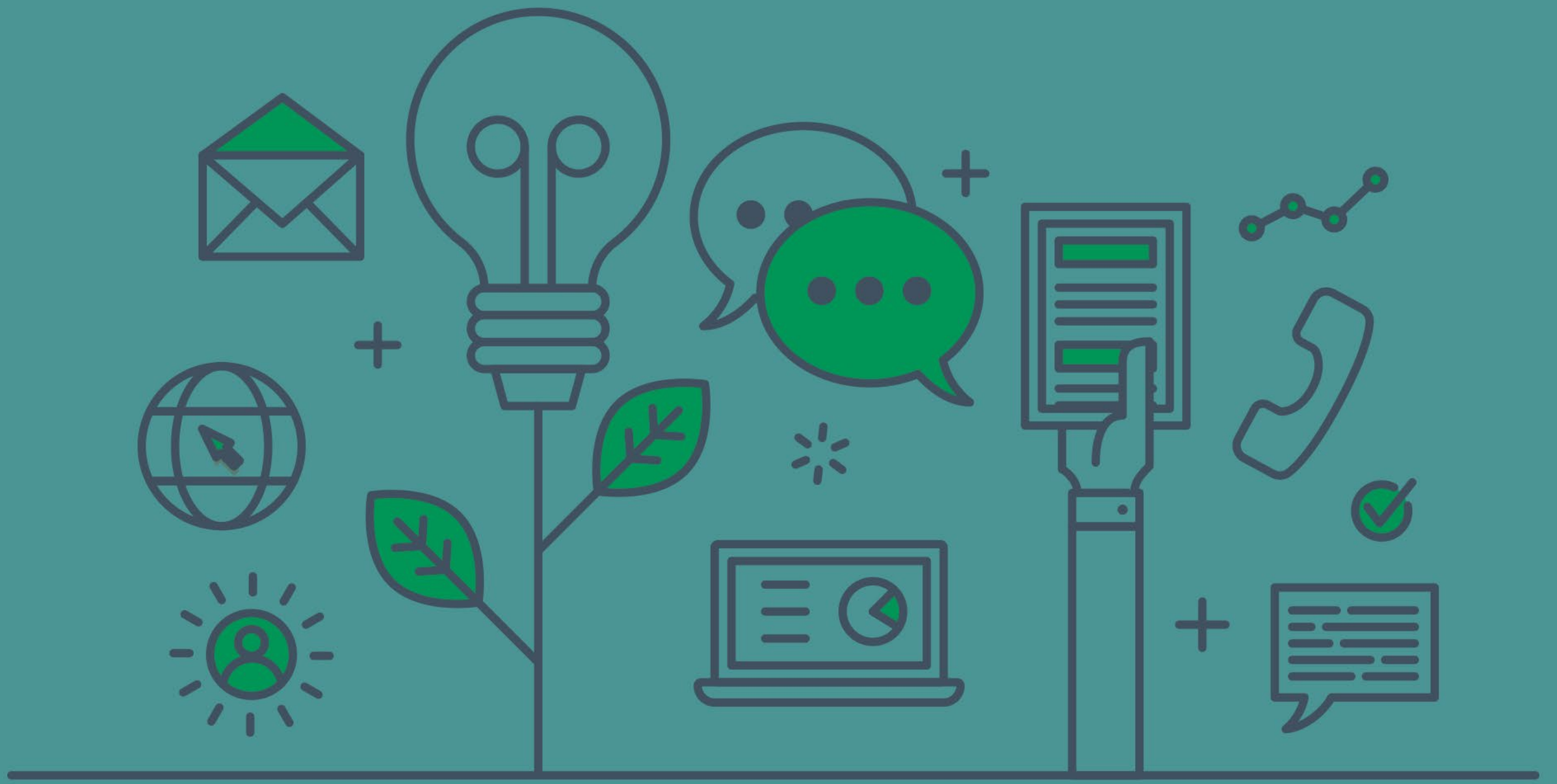
Independentemente da opção tomada, é importante ter noção que as ofertas de Cloud, tal como o mercado, estão em constante evolução, daí ser imprescindível traçar uma estratégia, fazer um planeamento, ter em conta as necessidades presentes e futuras, a configuração que melhor se adapta ao seu caso, os requisitos necessários, averiguar os custos (incluindo os escondidos)... sendo a questão da confiança muitíssimo importante.

A buzzword de que falei acima - Transformação Digital - encontra-se definitivamente no topo das prioridades da agenda de muitos decisores de negócio, e ainda bem pois perante clientes que exigem rapidez, facilidade de uso e agilidade só mesmo a tecnologia para nos ajudar na obtenção de resultados e ganhos de produtividade. ■

easyVISTA™

Transform Support.
Delight Customers.

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



COMO A EXPERIÊNCIA DO CLIENTE DEFINE A RELAÇÃO COM AS EMPRESAS

Se os clientes tiveram uma boa experiência de compra com uma determinada empresa, é expectável que comprem mais, sejam mais leais e partilhem as suas experiências com os seus amigos e colegas. Atingir essa experiência perfeita não é fácil e muitos clientes sentem-se defraudados pela sua experiência e com o facto de uma marca não corresponder às suas expectativas. Quando assim é, as empresas perdem clientes.

RUI DAMIÃO

QUER NA VIDA PESSOAL ou profissional, já todos tivemos algum tipo de relação e/ou experiência com determinadas organizações. Essas relações podem ter sido positivas ou negativas, mas, de alguma maneira, moldaram a perceção que temos dessa empresa.

Essa experiência enquanto cliente não é deixada ao acaso pelas grandes empresas. A perceção que um cliente tem de uma organização é importante; se um cliente tiver uma experiência positiva com um negócio, é mais provável tornar-se num cliente leal. Por outro lado, quanto pior for a experiência, maior é a probabilidade de alguém deixar de ser cliente dessa empresa. Uma empresa não existe sem os seus clientes. Quanto mais feliz uma pessoa estiver com uma determinada marca ou empresa, mais tempo irá permanecer com a mesma. Se uma empresa trata mal os seus clientes ou ignora os seus emails, é mais provável que parem de fazer negócios com a empresa.

Assim, é fácil perceber qual é a importância do customer experience (CX): quanto mais feliz estiver com uma marca, mais provável é o cliente permanecer com a empresa. É por isso que as empresas que oferecem uma melhor experiência ao cliente superam os seus concorrentes.

O QUE É CUSTOMER EXPERIENCE?

De uma forma simples, customer experience é a maneira como os clientes percecionam as suas interações com a empresa. Esta perceção, segundo explica a Forrester Research, é guiada por respostas emocionais e psicológicas aos estímulos apresentados durante a interação entre o cliente, a empresa ou a marca e o ambiente imediato, seja na loja ou online.

Luís Madureira, Managing Partner na Uberbrands, explica que CX "é um conceito muito lato" e que, "quando é referido, pode querer dizer muitas coisas uma vez que o objetivo de todas as companhias é, de uma forma ou de outra, providenciar excelentes experiências aos seus clientes e consumidores".

Naturalmente que a experiência do cliente pode não ir de encontro à expectativa do mesmo, mas, por outro lado, "pode-se dizer que temos uma excelente customer experience quando é

entregue mais valor do que o esperado pelo cliente quando o mesmo escolheu entrar numa relação comercial com a organização, marca ou produto específico", indica Luís Madureira.
Ornella Urso, Research Analyst de Retail Insights na IDC, refere que a CX é, atualmente, "uma grande prioridade de negócio para as organizações". "Quando falamos de customer experience, referimo-nos a diferentes aspetos e dimensões que dizem respeito não só ao *front-end*, mas também a todas as operações que estão no *back-end*", diz.

MANTER A EXPERIÊNCIA

A experiência do cliente deve ser igual em todas as interações que o cliente tem com a marca ou empresa e acontece em toda a jornada. O primeiro contacto entre o cliente e a empresa é importante, mas como é que se desenrola o resto da jornada é, igualmente, fundamental.
Num estudo da PwC, intitulado "Future of Customer Experience", 39% dos clientes mundiais admite deixar de interagir com marcas das quais gostam após uma única má experiência. O número sobe para perto dos 50% quando o cliente tem várias más experiências com a mesma empresa ou marca.

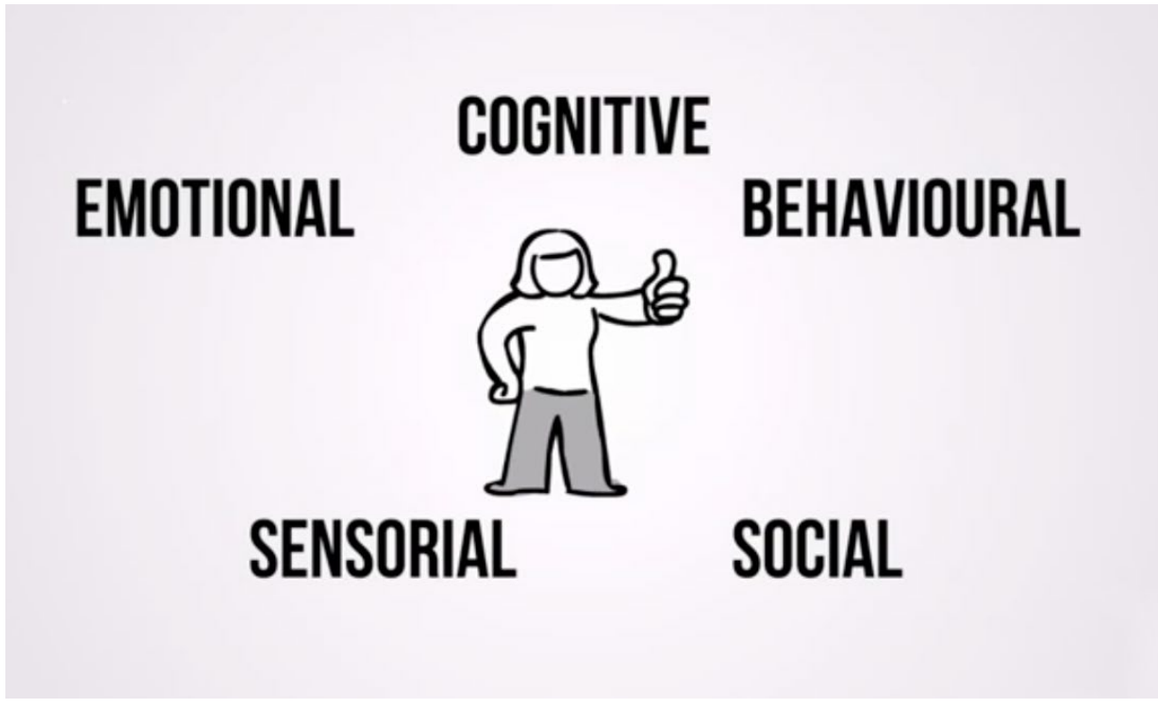
Segundo a PwC, as empresas devem "mudar os objetivos de customer experience para refletir o que é realmente importante para os clientes". Se esses objetivos forem bem implementados, "os clientes sentem-se apreciados" e as empresas colhem "benefícios de negócio".

MEDIR A EXPERIÊNCIA DO CLIENTE

Para saber se qualquer medida de customer experience é eficaz, é preciso ouvir os clientes. Já estão disponíveis no mercado várias formas de monitorizar e medir a experiência dos clientes.
O Managing Partner da Uberbrands partilha que uma das formas utilizadas para "perfilar e compreender a experiência do consumidor de forma mais qualitativa é o uso de Social Web Listening. Esta tecnologia permite-nos, por exemplo, identificar experiências positivas e negativas, os seus atores, o sentimento e as emoções dessas experiências, onde viveu essa mesma experiência, etc.".
"Para dar um exemplo rápido, a experiência de compra pode ter sido ótima, mas a experiência de uso pode ter sido má", explica Luís Madureira.

- Luís Madureira -
Managing Partner,
Uberbrands

- Ornella Urso -
Research Analyst, Retail
Insights, IDC



"Estas experiências podem ter sido vividas num mesmo local (restaurante) ou em locais diferentes (loja de retalho onde o cliente compra o produto para consumir em casa). Esta técnica tem a vantagem de receber *feedback* não enviesado, pois o consumidor embora esteja a partilhar publicamente as suas experiências em redes sociais, blogs, fóruns, etc., não o faz com o objetivo de dar *feedback* à organização". Deste modo, esclarece, "a sua opinião é partilhada na altura em que a experienciou, sendo na maior parte das vezes mais cândida. Permite ainda, caso seja um caso grave de má experiência, abordar este evento antes que o mesmo se torne numa conversa online com repercussões de dimensão elevada, afetando a reputação da empresa".

As empresas focam-se na experiência digital do consumidor e de permitir a melhor experiência possível em todos os canais. Os clientes esperam vários canais que se conectam em perfeita sintonia. Desse modo, os clientes podem continuar num outro canal exatamente onde pararam num outro, tendo uma experiência semelhante seja em que canal for.

Luís Madureira refere que este é "o maior desafio nas organizações". Esta estratégia, no entanto, não deve ser por canal, mas sim uma estratégia multicanal, ou seja, "a entrega da experiência em todos os *touchpoints* ao longo do *customer journey* é desenhada e entregue de forma integrada, sem qualquer disrupção quando são usados diferentes canais".

Ornella Urso explica que "mais de 30% das organizações, atualmente, têm dificuldades em medir a experiência do cliente numa loja e identificar novos KPI que podem ajudar a organização a medir o impacto" dessas iniciativas.

A IMPORTÂNCIA DA INTELIGÊNCIA ARTIFICIAL

A Inteligência Artificial (IA) é de extrema importância na estratégia de customer experience. É esta tecnologia que vai analisar as quantidades massivas de dados que são geradas pelos vários canais de uma empresa e apresentar à organização quão bom – ou quão mau – é a experiência do seu cliente.

AS EMPRESAS DEVEM TER BEM DEFINIDA QUAL A EXPERIÊNCIA QUE QUEREM DAR AOS SEUS CLIENTES

- Marta Piedrafita -
Enterprise Sales Director para Espanha, Itália e Portugal, Qualtrics

- Eduardo Correia de Matos -
Diretor de Customer Service, TAP Air Portugal

Mas a utilização de IA em CX vai para além da análise de dados. Os clientes, muitas vezes sem saberem, também têm interações diretas com a inteligência artificial. Da saúde à moda, passando por muitos outros setores, os chatbots oferecem um suporte inteligente ao cliente. Na maioria dos casos, esta tecnologia é melhor na criação de conteúdo personalizado do que os humanos.

Os chatbots têm acesso a muitos pontos de dados centrados no cliente e também podem combinar solicitações específicas do local para detetar facilmente problemas comuns, identificar padrões e prever o que está a causar problemas para um determinado utilizador.

Os chatbots podem iniciar conversas proativamente com os clientes, fornecendo-lhes as informações necessárias ou ajudando no processo de compra. Também resolvem consultas comuns e transferem as consultas com as quais não podem lidar para a equipa de suporte especializado dentro da organização. Essa equipa de suporte ao cliente lida apenas com as consultas dos clientes que precisam dos seus conhecimentos, aumentando assim a produtividade e melhorando a experiência do cliente.

Depois, e à semelhança da utilização de inteligência artificial noutros casos, à medida que a tecnologia avança, a IA torna-se mais produtiva e ainda mais barata. A tecnologia não precisa de dormir, não descansa e nunca fica doente, algo com que os humanos não conseguem competir. A IA pode aprender facilmente novas competências e ter uma taxa de erro bastante baixa. As máquinas trabalham incansavelmente com eficiência consistente, resultando numa maior produtividade e fornecendo uma melhor experiência de utilização.

CUSTOMER EXPERIENCE B2B

As empresas que vendem a outras empresas também têm de apostar em customer experience. Mesmo a organização B2B mais tradicional deve investir na experiência dos seus clientes, sejam eles pessoas individuais ou outras organizações.

Um estudo da B2B International afirma que apenas 14% das grandes organizações B2B são totalmente centradas nos clientes, ou seja, que as práticas de CX estão enraizadas na cultura da empresa.

Neste campo, Ornella Urso refere que a palavra-chave é "colaboração". "As empresas podem colaborar umas com as outras, podem entender a necessidade do que empresa cliente", mas, indica, "o importante é identificar quais são os tipos de serviços que a empresa pode oferecer aos outros para realmente construir essa plataforma em conjunto, ou co-inovar".

Marta Piedrafita, Enterprise Sales Director para Espanha, Itália e Portugal na Qualtrics, explica que "de uma perspetiva B2B, deve começar a pensar no que sua organização pensa". As empresas têm uma "quantidade limitada de clientes que oferece informações ou oferece serviços". Ao contrário do customer experience mais tradicional, do lado B2B "é mais difícil obter *feedback* e informações sobre o que esses clientes estão a pensar, porque não é possível ter a opinião de todos os pontos de contato, de todas as pessoas presentes".

O público B2B procura soluções ou ofertas para problemas que melhor atendam as suas necessidades, como produtos mais personalizados, melhores sistemas integrados, uma maior capacidade de resposta, um menor custo de utilização ou maior produtividade. Influenciados pelo mundo do consumidor, muitos públicos B2B também estão a procurar uma experiência aprimorada na utilização de um produto ou serviço B2B - uma jornada para o cliente que é perfeita, mais conveniente e sem complicações. Os fornecedores experientes de B2B vendem uma experiência e resultados, não produtos.

TENDÊNCIAS NO MERCADO PORTUGUÊS

Apesar de existirem muitas tendências, nem todas estão a ser adotas pelas organizações portuguesas, seja por falta de políticas na área ou porque ainda não é o momento certo para implementar determinada solução.

Marta Piedrafita refere que o customer experience "era visto até agora como um processo relacionado com o CRM no digital". Agora, diz, a abordagem é diferente: "vem da experiência dos dados".

Para Eduardo Correia de Matos, Diretor de Customer Service na TAP Air Portugal, as empresas devem ter bem definido "o que é um cliente, um *prospect*, uma utilização esporádica dos seus serviços" para depois "definir perfis ou *personas* e jornadas". O responsável diz que, em Portugal, muitas vezes se "começa ao

PORTUGAL AINDA ESTÁ NUMA "FASE MAIS ANALÍTICA" ONDE SE CONSOLIDA A INFORMAÇÃO E SE RETIRA VALOR DA MESMA

contrário", onde se diz que se quer determinada experiência, mas não se "pensou em que tipo de cliente é que estamos a falar e que características é que tem".

Hugo Gonçalves, Head of Marketing da Bizdirect, refere que Portugal está, atualmente, "numa fase mais analítica". "Passámos aqui por um momento em que as organizações tinham o desafio de estruturar a sua informação que criavam todos os dias. Acho que já passamos essa fase". Atualmente, a maior parte das organizações portuguesas "já consolidaram aquilo que era a sua informação de clientes e têm uma necessidade muito grande de retirar valor dessa própria informação".

Por outro lado, Sérgio Magalhães, diretor no Millenium BCP, indica que a tendência em Portugal está em adotar soluções "que são *mobile first*". Estas soluções já nascem "no âmbito digital" e "todas as interações que são feitas em todos os setores da sociedade são tendencialmente *mobile first*".

Pedro Pinto Lourenço, Business Director da Divisão Dynamics 365 na Microsoft Portugal, refere que, em Portugal, as tendências "prendem-se muito com o tema da personalização" e com "a agilidade". No caso da personalização, as empresas "têm uma preocupação muito grande em utilizar melhor os dados que têm. Há uma preocupação muito grande, também, relacionada com as normativas legais de garantir que as regras são cumpridas e que isso não é, de alguma forma, um obstáculo àquilo que são os dados que têm que ser recolhidos por parte das empresas para melhorar aquilo que é a experiência do cliente".

Por outro lado, explica Pedro Pinto Lourenço, "a perspetiva da agilidade, com o ritmo a que a sociedade e que a economia está a evoluir, garantir que as empresas têm a capacidade de ser ágeis e responder àquilo que são os nossos desafios" é uma preocupação das organizações.

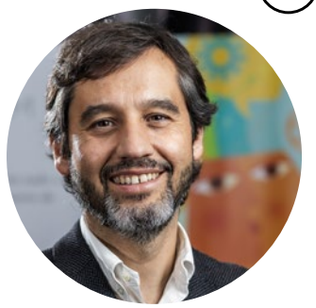
- Hugo Gonçalves -
Head of Marketing, Bizdirect

- Sérgio Magalhães -
Diretor, Millennium BCP

QUEM INVESTE EM PORTUGAL

Desengane-se quem pensa que apenas as grandes empresas portuguesas estão a investir em

NÃO HÁ UM CONSENSO DE QUEM DEVE LIDERAR AS INICIATIVAS DE CX, MAS, GERALMENTE, FICA ALOCADO AO MARKETING OU AO SERVIÇO AO CLIENTE



- Pedro Pinto Lourenço -
Business Director - Dynamics 365 Division, Microsoft Portugal

soluções ou iniciativas de customer experience. "Aquilo que nós sentimos é que muita da transformação vem das grandes empresas, mas também aparecem muito empresas pequenas que já nascem completamente digitais", indica o Business Director na Microsoft Portugal, que acrescenta que essas empresas mais pequenas "muitas vezes (...) desestabilizam aquilo que é o *status quo*".

Hugo Gonçalves afirma que "todas as empresas que têm uma criação e uma dinâmica muito forte e com muitos clientes – e muitas interações – estão a passar por esta transformação". Esta transformação é transversal, ainda que cada uma tenha a sua dimensão. Por outro lado, alerta, esta transformação – que até é um fator competitivo das próprias organizações – é "mais urgente nas empresas que estão com outro grau de maturidade em termos de inovação".

QUEM DEVE LIDERAR AS INICIATIVAS DE CX

O perfil que, dentro de uma organização, deve liderar as iniciativas de customer experience pode não ser o mesmo dentro de todas as empresas. Luís Madureira refere que "deveria estar dentro da direção de marketing, embora em alguns casos esteja no serviço ao cliente e esta função está integrada na direção de operações".

Pedro Pinto Lourenço, da Microsoft Portugal, diz que há uma alteração em curso. Há empresas que começam a apostar na função de Chief Digital Officer que tem uma "estreita ligação com o CIO ou com o CSO, ou seja, com o chefe de vendas, com o diretor de vendas, com o administrador que tem a área de vendas ou que tem a área de marketing". Simultaneamente, também essas funções mais tradicionais começam a sofrer uma fusão, quer nas grandes, como nas empresas mais pequenas.

No caso específico da TAP Air Portugal, Eduardo Correia de Matos partilhou que a área depende do vice-presidente que é responsável por clientes, mas que "tem um envolvimento muito próximo do CEO". "É assim que a vejo", diz o diretor de Customer Service; "quem for o administrador ou diretor que tiver a área de cliente, também deve ser responsável pela experiência, mas o envolvimen-

to do CEO ou da administração é muito importante para dar *empowerement* ao que vai sair daqui".

A Research Analyst da IDC refere que se está a assistir a uma linha ténue "entre o departamento de IT e a linha de negócio". "O importante é que, no nível do CEO, eles tenham a responsabilidade de gerir e impulsionar a inovação e a transformação digital. E como a experiência do cliente é uma das dimensões principais, é necessário ter em conta também esse aspeto".

No entanto, também há outra possibilidade: criar o cargo de Chief Customer Experience. O Managing Partner da Uberbrands diz que "numa empresa que necessite e queira estabelecer o customer experience como a sua maior vantagem competitiva e ponto de diferenciação, pode ter um Chief Customer Experience que reporte diretamente ao CEO".

A IMPORTÂNCIA DO CX

Quase todas – se não mesmo todas – as empresas mundiais reconhecem que os clientes devem estar no centro do negócio. Sem eles, os negócios estão condenados a falhar.

Definir prioridades e as estratégias são de extrema importância para as organizações que querem manter os seus clientes felizes. É de extrema importância manter uma experiência de cliente consistente em todos os canais, sejam online ou offline. Quanto melhor for a experiência do cliente com a empresa, maior será a probabilidade de o cliente gastar dinheiro com essa empresa e de a sugerir aos seus amigos, trazendo, assim, ainda mais negócio para a organização. ■

POR SÉRGIO FERREIRA,
Executive Diretor, EY

COMO TESTAR SE A SUA ESTRATÉGIA DE INOVAÇÃO É SUSTENTÁVEL?

Cada vez mais clientes nos escolhem quando percebem que as antigas aproximações de trabalhar de dentro para fora se tornaram ineficazes para criarem inovação e vantagem competitiva no mercado.

DESTE MODO, temos sido chamados a construir uma ponte entre as equipas de negócio e os seus utilizadores finais e clientes, através de uma metodologia de design centrada no ser humano. Ao entendermos melhor os hábitos, necessidades e aspirações dos clientes, somos capazes de criar soluções que agregam mais valor.

Enquanto Service Designers, frequentemente limitamos a nossa atuação e foco a atender às necessidades dos utilizadores finais, clientes ou principais partes interessadas internas. Até muito recentemente, raramente nos perguntávamos como o processo para chegar a uma nova solução iria afetar o meio ambiente, nem como iria impactar a sociedade em geral.

A razão para normalmente negligenciar estas grandes questões não se prendia apenas com a sua complexidade, mas também porque abordá-las não resultava num retorno imediato do investimento dos nossos clientes. No entanto, tornou-se claro que não podemos mais dar valor aos sucessos de hoje, apenas através de indicadores de curto prazo (Will you be relevant to future consumers if you stay inside your comfort zone?) , quando o bem-estar do nosso planeta e a saúde das gerações futuras estão em jogo. Tornou-se urgente e premente mudar esta aproximação, sendo necessário medir como os negócios e projetos que criamos servem (ou deixam de servir) a nossa sociedade e o nosso planeta.

- Sérgio Ferreira -
Executive Diretor, EY

Nestes últimos dois anos ajudámos clientes a criar novos modelos de negócio, produtos, serviços e processos centrados em pessoas, mas recentemente, percebemos uma crescente necessidade de foco em inovações que contemplem também sustentabilidade. Esta mudança em direção à responsabilidade social e à sustentabilidade é principalmente resultado de os clientes e consumidores quererem cada vez mais produtos ecológicos e marcas que têm práticas sustentáveis, pressionando as empresas a alterarem as suas prioridades (The Elusive Green Consumer).

Muitos líderes e gestores percebem que ativar um propósito na sua empresa teria realmente um impacto positivo no seu desempenho e reputação (e, consequentemente nos seus resultados financeiros), mas eles não têm as ferramentas para medir e demonstrar o potencial sucesso dos seus esforços à prova de futuro.

Foi para responder a esta necessidade que fundimos o EY CUSTOMER LAB com o EY ECO LAB, criando o modelo EY ECO LIVING, o qual cruza as 8 forças de mudança do Consumidor Futuro (FutureConsumer.NOW) com modelos de negócio genuinamente sustentáveis (How an integrated sustainability strategy can help you stand out).

Como vamos viver: a forma como vivemos, onde vivemos, como nos vestimos, que serviços adotamos para o nosso lar (energia, água, etc), refletem um estilo de vida. No modelo Eco-Living, as marcas ouvem as necessidades dos consumidores e posicionam-se como uma extensão dos valores dos consumidores.

Como vamos trabalhar: a forma como trabalhamos, como nos conectamos com os outros, que tecnologias usamos para o trabalho em equipa, são também exemplo de um modelo EcoLiving transversal a todas as áreas da nossa vida.

Como vamos viajar: a forma como são pensados os centros urbanos, as opções de que dispomos para circularmos num mundo globalizado, os meios que usamos no nosso dia a dia são espelho de uma maior consciência face aos problemas ambientais.

Como vamos comprar: a forma como compramos, o formato do que compramos (com ou sem embalagem), a dosagem que escolhemos, as plataformas disponíveis para nos auxiliarem nessas compras, uma maior segurança e privacidade, são também um reflexo do nosso estilo de vida.

Como vamos comer: como procuramos comer melhor, estar mais conscientes dos processos de produção, exigir maior transparência das marcas, é uma forma de "ativismo de consumo".

Como nos equilibramos: a forma como cuidamos de nós e dos outros, como encontramos um equilíbrio mental e físico na nossa vida, também está ligado a valores sustentáveis. ■

#TudoSeTransforma, até o seu negócio!

noesis

POR MIGUEL LOURO
Senior Manager de Enterprise Solutions, Noesis

A ERA DA EXPERIÊNCIA DIGITAL

Não somos todos iguais, mas então porque é que as marcas ainda comunicam como se fôssemos? Uma boa estratégia de Customer Experience (CX) requer uma experiência digital otimizada, esta ocorre quando independentemente do canal de interação com uma marca, sentimos que somos considerados e valorizados.

EM 2020, não vamos ter o tão esperado Quadrante Mágico da Gartner para tecnologias de gestão de conteúdos web (WCM), ao invés, entramos numa nova era de *Digital Experience* (DXP). Os consultores suportam a decisão pela uniformização da oferta e maturidade do mercado, não é um fim, é o início de uma nova definição que considera toda a experiência digital em torno dos conteúdos.

A interação que temos com as marcas nunca foi tão rápida como hoje e, no futuro, a previsão é de que o tempo despendido com um conteúdo específico seja ainda menor! A procura dos clientes centra-se agora em soluções mais complexas e detalhadas nos vários *touchpoints* com o consumidor.

Um exemplo simples é a subscrição de um serviço online e entrada num programa de fidelização, em que no instante seguinte, estamos a receber uma newsletter personalizada com a promoção do mesmo serviço. A estratégia de conteúdo Omnichannel deve ser centralizada e orquestrada com recurso a uma lógica DXP, com uma forte componente de personalização.

O OMNICHANNEL É UMA OBRIGAÇÃO, A PERSONALIZAÇÃO É A SOLUÇÃO.

Se recuarmos uns 30 anos, quando íamos aquela loja perto de casa, sentíamos uma atenção especial, já referia a música do genérico do Cheers – "Everybody knows your name". Isso foi a personalização no mundo físico!

- Miguel Louro -
Senior Manager de
Enterprise Solutions, Noesis

O MERCADO EXIGE A SIMPLIFICAÇÃO DO CAMINHO PARA OS RESULTADOS E A PROCURA DE UMA SOLUÇÃO INTEGRADA QUE, NÃO SÓ PERMITA A PERSONALIZAÇÃO DO CONTEÚDO ONLINE, MAS QUE O FAÇA MONITORIZANDO O COMPORTAMENTO DOS USERS EM TEMPO REAL

Esta proximidade no mundo digital está a ser alcançada através da personalização, a "IA de conversação", através dos já famosos chatbots que alteram automaticamente o conteúdo de um site específico pelo *feedback* recebido dos clientes. Isto é personalização avançada no mundo digital!

Este mundo digital não é algo futurístico, já vivemos nele e até ao final de 2020 a previsão será de existirem 25 mil milhões de dispositivos conectados no mundo. Os negócios estão já a tirar partido do potencial dos dispositivos móveis e a abordar a personalização digital para proporcionar uma imersão profunda na relação com os clientes e, assim, alcançar uma experiência do consumidor otimizada.

Quando falamos em experiência do consumidor, o aspeto crítico é a mensagem personalizada. Os profissionais de marketing estão focados em procurar maneiras de espalhar a mensagem, aumentar presença no mercado e gerar conversões. Todos têm o mesmo *benchmarking*, o que significa que mais de 93% das empresas que usam personalização estão a sentir um aumento nas conversões vindas diretamente do tráfego online.

O mercado exige a simplificação do caminho para os resultados e a procura de uma solução integrada que, não só permita a personalização do conteúdo online, mas que o faça monitorizando o comportamento dos *users* em tempo real.

Existe uma grande diversidade de plataformas, mas muitas falham o match entre flexibilidade e os requisitos necessários para proporcionar uma verdadeira *Digital Experience*. Na Noesis apostamos em Sitecore, uma poderosa solução de DXP que oferece uma visão holística do comportamento do consumidor no mundo digital e que consegue potenciar uma conversão juntando dados recolhidos online com dados recolhidos no mundo físico. Um verdadeiro conceito Omnichanel. As suas *features* de *tracking*, *analytics* e automação permitem que os *marketeers* consigam personalizar as campanhas, captar dados, trabalhá-los, gerar *leads* e obter as tão ambicionadas conversões.

A implementação tem sido transversal a vários setores e com taxas de sucesso incrivelmente positivas, seja na banca, nos seguros ou até no retalho. Hoje, o digital está ao alcance de todos e singrar é uma questão de *mindset*. Está na hora de desenvolvermos estratégias focadas nos nossos *targets* e proporcionar experiências otimizadas aos clientes, consumidores, utilizadores ou parceiros. ■

Schneider Electric

POR RITA LOURENÇO,
Key Account Manager,
Schneider Electric Portugal

A IMPORTÂNCIA DE COLOCAR O CLIENTE NO CENTRO DA ESTRATÉGIA DE NEGÓCIO B2B

Colocar o cliente no centro do negócio é o mote de muitas das grandes empresas globais, que compreendem que o seu sucesso será tanto maior, quanto maior for o conhecimento que têm sobre os seus clientes.

QUE IMPACTO TERÁ, então, esta vontade de dar mais importância ao cliente nas relações B2B, que envolvem sistemas intrincados? O que acontece quando uma cadeia de valor complexa está implicada? Como é que as empresas podem continuar a prestar maior atenção ao valor que trazem ao cliente final?

Para que as suas transações possam focar-se no cliente, as empresas necessitam de mais do que soluções inteligentes e um serviço simpático: devem construir com os clientes uma relação que permita a descoberta, experimentação e o pensamento a longo prazo.

Uma relação empresa/cliente focada neste último constrói-se com base na empatia e na colaboração, eliminando da equação o oportunismo e a persuasão. Uma premissa que soa bem, mas que na prática requer um afastamento da mentalidade de "fechar o negócio, não importa como".

Se analisarmos esta questão de forma mais aprofundada, descobrimos que, ao longo do tempo, o que é bom para o cliente também é bom para a empresa. No que toca à infraestrutura física e de IT, há oportunidades significativas que vão para além da compra inicial; de facto, estima-se que haja um rácio de 5:1 de custos operacionais em relação a custos de investimento, ao longo da totalidade do ciclo de vida de um edifício.

- Rita Lourenço -
Key Account Manager,
Schneider Electric Portugal

NÃO É O FIM DAS VENDAS: É O PRINCÍPIO DAS RELAÇÕES

O novo paradigma dos mercados de edifícios, data centers, espaços industriais e infraestruturas são os sistemas inteligentes e interconectados, que desafiam as empresas a deixar de separar os departamentos de vendas dos restantes. No passado, as empresas respondiam a dez solicitações de proposta com dez equipas de vendas diferentes, o que levava a que se prendessem demasiado em detalhes e perdessem a noção do panorama geral: promoviam os produtos de forma individual, sem uma história global a explicar como podiam trabalhar em conjunto para trazer ainda mais valor ao cliente. Promover a colaboração e articular o seu valor é complexo, mas felizmente há estratégias sólidas para fazer esta gestão; uma delas é a metodologia de arquitetura das soluções.

O MÉTODO DA ARQUITETURA DAS SOLUÇÕES

Para conseguir alcançar a verdadeira integração num projeto de grandes dimensões, o método da arquitetura das soluções pode ser uma ótima opção, procurando unir as várias equipas individuais em torno de uma visão única.

Os arquitetos de soluções fazem a conexão entre a tecnologia e os objetivos dos clientes, focando-se no seu alinhamento com as perspetivas de todas as partes envolvidas. Isto pode ser delicado: por exemplo, os CTO e as equipas de IT compram produtos em ciclos de três a cinco anos, e as equipas de instalação fazem-no em ciclos de 25 anos. Se as decisões forem tomadas apenas a partir de uma ou outra perspetiva, diminuem a eficiência e fiabilidade do sistema e aumentam os custos no geral.

É necessário acautelar também o chamado "dilema CapEx-OpEx". Tipicamente, as equipas de design e construção são incentivadas a entregar os projetos dentro de um prazo e de um orçamento, obrigando-as a fazer escolhas que podem vir a aumentar os custos operacionais, que representam a maior parte dos custos totais ao longo da vida útil de um edifício. Neste sentido, todos os intervenientes da cadeia de valor devem também preocupar-se com os custos do ciclo de vida e a experiência do cliente no projeto – e não apenas com os custos de investimento, que acabam por não pesar tanto no final.

Para coordenar estas perspetivas, o arquiteto de soluções reúne as partes interessadas e define os resultados desejados pelas várias partes. Ao invés de dar prioridade à tecnologia que a empresa oferece, são as necessidades do cliente que determinam a solução a aplicar, garantindo que o projeto vai dar-lhes resposta a longo prazo.

Os benefícios desta metodologia não estão, no entanto, limitados aos objetivos a longo prazo, também criam lucros imediatos: uma maior colaboração e visibilidade entre as equipas pode trazer, desde logo, benefícios na fase do CapEx. Colocar o cliente no foco do negócio requer empatia e humildade por parte das empresas: empatia para com as necessidades dos clientes e a humildade de reconhecer que não têm sempre todas as respostas. Significa ver os clientes como humanos e ver-se a si mesmas como entidades formadas por humanos – que precisam do conhecimento uns dos outros e de se unir em torna de uma mesma visão, para construírem juntos uma infraestrutura preparada para o que o futuro reservar. ■

JOSÉ DIONÍSIO, CO-CEO DA PRIMAVERA

"QUEREMOS TRAZER AO PRODUTO INFORMAÇÃO SOBRE O FUTURO"

HENRIQUE CARREIRO E RUI DAMIÃO

Fotografias: Jorge Correia Luís

José Dionísio, Co-CEO da Primavera, explica o caminho que a empresa tem vindo a fazer ao longo dos anos, desde a transição do DOS para o Windows, até à transição atual dos produtos on-premises para os produtos cloud.

Quando a Primavera nasceu, foi com uma perspetiva de crescimento?

Sim. Começámos vindo de um outro *player*. Eu e o Jorge Baptista quando começámos já tínhamos sete anos de experiência. Éramos uma startup, mas não à saída da universidade. Acho que aquilo que aconselharia a alguém que quer empreender, na medida dos possíveis, é que primeiro vá ganhar uma experiência profissional numa empresa com alguma dimensão. E depois decidir se quer empreender dentro [da empresa], ou se quer empreender por conta própria. Porque também é muito interessante, e pode ser estimulante, empreender dentro de uma boa organização.

O país precisa muito de empreendedores. Se eu quiser trabalhar a escala, o país precisa de empreendedores para as nossas empresas. Se hoje tenho 330 ou 340 pessoas e quero ter amanhã 500, preciso de empreendedores. Nesse sentido, sim, quando nascemos foi para ser logo, pelo menos, da dimensão daquela empresa de onde tínhamos vindo. Saímos e sabíamos o que era uma dimensão de empresa na altura. Não quisemos ser uma empresa internacional e pagámos por isso de alguma maneira, não formatámos tudo isso em função de uma dimensão internacional porque em 1993 não era tema; o mercado interno, por si só, chegava. Mas quisemos ser uma empresa nacional. Construímos uma software house nacional porque a nossa escola tinha sido essa.

Nasceram com o *mindset* de produto?

Exatamente. Um executável para todos. Por isso a Primavera não tem dois executáveis, tem um. O que implica tecnologia para adaptar o produto às necessidades dos clientes, e não fazer vários executáveis e gerir vários executáveis.

Sabíamos o que era software… quando estávamos os dois dentro de uma salinha e ainda mal vendíamos, apareciam-nos pessoas à porta a quererem comprar computadores, na altura em que se ganhava, para aí, 200 contos, mil euros, na altura, num computador. E podíamos mandar vir um computador e fazer-lhe a venda, mas mandávamos ir à porta ao lado porque sabíamos aquilo que tínhamos. Não podíamos desfocar daquele que era o nosso objetivo, que era fazer software de gestão para o Windows e para as empresas.

Começámos por onde o Windows andava, nos profissionais liberais; fez-se ali um *bestseller* sem sabermos. Vendeu cem mil euros, 20 mil contos na altura. Tenho a primeira fatura no meu gabinete e, por isso,

eram caixinhas que eram vendidas a 14 contos, 70 euros, e que ainda tinha a margem de revenda, para aí 30 ou 40 euros, que dávamos a quem vendia.

Andava a vender pelas lojas, na altura. Hoje ando a tentar ver se estes jovens faturam 50 mil euros no primeiro ano. Por isso nós de facto, fomos privilegiados ali por mérito, sorte, momento, *time-to-market*... eu sei lá. Aparecemos com um produto bem trabalhado também do ponto de vista da imagem; as caixas eram bonitas, atrativas. Ocupámos um espaço no mercado de lojas português que nos deu esse volume de negócio. Cem mil euros no primeiro ano, depois 250 mil euros no segundo, 535 [mil] no terceiro.

Não tendo sido os primeiros com este tipo de software, qual foi o fator distintivo?

Foi o Windows, fomos os primeiros. A Primavera foi a primeira empresa em Portugal a apresentar produtos para Windows.

Nativos para Windows?

Sim, essa foi a diferença. À luz da transformação que estamos hoje a fazer para a cloud, essa era uma transformação mais fácil, na altura. Esta é muito mais desafiante, sem dúvida. O que nós fizemos foi produtos que existiam em DOS e passámo-lo a fazer em Windows. Com todas as dúvidas que havia na altura, se alguém ia trabalhar no escritório, fazer faturação com um rato, com janelas. Mas esses tabus, essas fobias, foram desaparecendo, muito com a ajuda, também, da própria força do marketing, da Microsoft sobre o Windows.

O que havia na altura em Windows era o Office. O nosso software era comparado com um produto altamente profissional. Tínhamos que fazer um software muito bom, o cursor tinha que rodar. Imaginem trabalhar num Windows que não tem uma ampulheta. Carregava-se e atuava. E na altura não havia componentes para fazer os botões automáticos, apareceram um ano depois. Eram produtos o mais sofisticados

possíveis para aquela tecnologia e para o nosso comparativo, felizmente, era com uma marca boa, e por isso, isso desafiou-nos a fazer coisas que víamos nesses produtos que também nós tínhamos que o fazer, apesar de ser mais complicado, levar mais tempo, e assim aconteceu.

Eu e o Jorge fechámo-nos num quarto do apartamento onde ele vivia na altura, fizemos daquilo um escritório, e entre setembro e de dezembro [de 1993], a trabalhar 16 ou 18 horas por dia, fizemos o Contalib, uma contabilidade para profissionais liberais. Basicamente, substituía os livros pretos de receitas e despesas e tratava do IVA e das amortizações aos profissionais liberais, que é onde o Windows começava a entrar. Não tanto ainda nas empresas. Esse produto foi pagando tudo, depois criou-se outro para empresários em nomes individuais e, entretanto, fomos fazendo a faturação, a gestão de stocks, etc..

Sendo que inicialmente não estava previsto, a partir de que altura é que começaram a pensar em expansão internacional?

A internacionalização para os PALOP, primeiro para Angola e para Moçambique, quase em simultâneo, deu-se por acaso. Em Angola, contactámos com um empresário angolano, que queria representar os produtos da Primavera nesse país. Do ponto de vista da legislação, os PALOP estão na penúltima ou antepenúltima versão da nossa. Tivemos um distribuidor que fez a marca em Angola, desde logo em Luanda. Foi um distribuidor exclusivo durante uns cinco ou seis anos. O mercado ganhou uma determinada dimensão e os clientes começaram a exigir outro modelo e então adotámos lá o modelo português. Com um canal aberto, com parceiros que estão certificados de acordo com as suas competências e o número de técnicos que têm com certificações.

Em Moçambique aconteceu exatamente o mesmo. Primeiro tivemos um distribuidor e depois passámos a ter um canal aberto. E hoje a Primavera gere cerca de 350 parceiros, entre parceiros com quem tem uma ligação direta e uma rede, também, de subdistribuidores, que adquirem alguns dos nossos parceiros distribuidores.

Este tipo de produtos permite, agora, uma expansão internacional a uma outra escala ou ainda não está exatamente no âmbito da empresa?

Caracterizo [a Primavera] como uma pequena multinacional que está presente em Portugal, no seu mercado, que significa 70% da sua faturação. E está presente nos PALOP, com 30% da sua faturação, sendo o segundo maior mercado, de longe, o mercado angolano. Depois, há cerca de dez anos, entrámos em Espanha, com o Windows, mas não tivemos sucesso significativo. Temos um conjunto de clientes em Espanha, continuamos a mantê-los, mas estamos à espera, hoje, das soluções cloud para podermos dar outra passada. Desde logo, esperamos, com o Jasmin, que é o produto para as micro e pequenas empresas, chegar em tempo de novidade ao mercado espanhol que é um mercado, que tudo indica, está menos preparado para a cloud do que está o mercado português.

Quando a Primavera fez, quer no Dubai, quer em Espanha, as suas entradas com produtos Windows, a verdade é que não levou diferenciação. Já existia muita coisa em Windows, por isso era exatamente como se estivéssemos em 1993 com um software para DOS quando já havia tudo em DOS. Acho que essa é a explicação pelo qual não conseguimos ganhar atração e interesse de um canal [de parceiros] – temos primeiro que conquistar os parceiros para eles venderem – porque não tínhamos, de facto, diferenciação.

Em Espanha, juntou-se o facto de entrarmos, precisamente, numa grande crise e quando Espanha ainda tinha uma crise maior que a portuguesa; pedir a parceiros, que já têm dificuldade em tomar conta de uma marca, que invistam na formação de pessoas numa segunda marca, também dificultou. Mas ficou-nos imensa aprendizagem sobre as características do mercado espanhol que é um mercado muito mais difícil do que, à primeira vista, parecia. Independentemente disso, há que ter consciência que para se fazer internacionalização hoje é preciso dinheiro. É preciso muito capital e muito investimento. É isso que nos diz o *benchmark* que se pode fazer do mercado mundial onde vemos, de facto, *players* ao nível das soluções para microempresas a se internacionalizarem, que era uma coisa que não acontecia no *on-premises*.

Para uma empresa como a Primavera, a cloud é um *enabler* ou abre a porta à entrada de concorrentes que, de outra forma, não entrariam no mercado?

Acho que é um *enabler,* agora... não deixa de exigir um investimento muito considerável que, provavelmente, a Primavera, com a sua atual estrutura de capital, pode não ter condições para o fazer. Fazer vingar uma marca em Inglaterra onde uma visualização através de AdWords do Google custa cerca de 30 euros, quando em Portugal é um ou dois... é preciso de facto muito dinheiro, muita capacidade financeira para nos afirmarmos dessa maneira.

Acho que o espaço de crescimento da Primavera, neste momento, passa pela questão espanhola. É onde temos recursos e é onde queremos insistir, agora com soluções mais inovadoras para o mercado espanhol. Para já, não seremos os primeiros, já há vários fabricantes em Espanha, como já há 24 em Portugal com soluções para pequenas empresas; isto aconteceu assim com o DOS e agora volta a acontecer. Há novas empresas, novos programas de faturação, com stock, gestão de contas correntes. São 'novas Primaveras' que podem vingar ou não, depende agora da capacidade desses empreendedores de fazer um projeto de sucesso.

Falando de cloud, como é que a Primavera está a endereçar este mercado? Com produtos próprios ou a estender o seu produto a parcerias? Como é que a Primavera vê esta transição?

Vemos de forma super prioritária em investimentos muito próprios nessa área.

O Rose — que é o produto que vai ser lançado agora, muito brevemente —, tem a assinatura de *Intelligent by Design*, o que é significativo. Temos um grupo que se dedica à inteligência dentro do produto. Estamos a construir as coisas de modo a desenvolvermos um outro tipo de produto. Partindo deste princípio, já não temos mais nada a acrescentar sobre a situação atual de uma empresa. Isso é o que fizemos estes 30 anos, quer em DOS, quer em Windows. Isto é, qualquer produto no mundo diz "olha, hoje estás a vender X, este mês estás a vender Y". Se estou em março tenho isto aqui preenchido até março. Tudo o que está para a frente, estava sempre em branco. Chega a janeiro, fica tudo em branco outra vez. Aquilo que queremos fazer é, digamos, uma bola de cristal. Queríamos trazer ao produto informação sobre o futuro. Essa é a grande diferença, para além da questão tecnológica da cloud.

Com as novas ferramentas, e a partir dos dados de cada uma das empresas clientes e, também, dos dados de uma comunidade muito alargada, podemos dar indicação sobre o futuro a curto, médio e longo prazo. O que hoje já se vê a sair no Jasmin são *insights* que está a receber; recebe informação sobre se o senhor não fizer isto, os seus resultados no final do ano vão ser assim. Se não comprar, vai ter rutura de stock em outubro, e estamos em junho, por exemplo. A inteligência que estamos a trazer ao produto está a ser fruto dessa investigação.

Com o conhecimento que tem do mercado, quais são os pontos que um gestor tem que ter em conta, agora? O que é que não pode deixar passar em branco?

Não há dúvida nenhuma que as dinâmicas de mudança, em tudo, são imensas. Tudo é diferente do que se passava há dois ou três anos. O conselho que dou é que têm que ter consciência de que têm que se informar. A realidade alterou-se muito nos últimos anos, coisas que não se viam e que agora são banais. Hoje, nenhum gestor pode dizer para si próprio "eu estou descansado, eu sei o que se passa".

Depois, é preciso ter em conta a satisfação das pessoas que trabalham na empresa. As pessoas valorizam muito trabalhar na Primavera porque tudo o que pedem - nomeadamente os mais responsáveis - para trabalhar, nós dizemos "compre". As tecnologias de informação são imprescindíveis e acabam por ser uma *utility*, como é o programa de faturação, por exemplo. ■

easyVISTA™

"O ITSM DEVE ESTAR NA LISTA DE PRIORIDADES DAS ORGANIZAÇÕES QUE ENFRENTAM A TRANSFORMAÇÃO DIGITAL"

Tendências, Service Desks e chatbots são alguns dos temas discutidos por Paulo Magalhães, Vice-Presidente do Sul da Europa da Easy Vista, de maneira a tentar agilizar e melhorar o trabalho das organizações.

O MERCADO ITSM levou alguns anos a atingir uma maior eficiência nos processos. Hoje, um dos seus grandes objetivos é garantir o *compliance* dos processos, tentando sempre agilizar e melhorar o trabalho das organizações. Quanto ao acesso à informação, com toda esta evolução, foi criada uma gestão de eficiência, pedidos, CMDBs e gestão de ativos, acabando por negligenciar a base do conhecimento e gestão de conhecimento, cada vez mais

- Paulo Magalhães, Vice-presidente do Sul da Europa, EasyVista -

importante no processo de ITSM. Primeiro, vivemos um momento de *turn over* dos recursos. Isto porque existem recursos a entrar e a sair.

Quando os recursos saem, existe um prejuízo para as organizações pois há sempre conhecimento que se perde e também porque há a necessidade fazer projetos diferentes e exemplo disso são os chatbots, que poderão correr mal, pois sem uma base de conhecimento bem estruturada, dificilmente vamos

conseguir ter e ensinar um Chatbot de forma eficiente e eficaz.

Existe uma evolução em termos de ITSM. Todos estes projetos foram pensados em 2019, estão a ter continuidade no ano de 2020 e, muito provavelmente, muitos deles ainda terão muitas consequências em 2021. Tudo isto faz parte de um processo de melhoria contínua.

Quando questionado sobre como as organizações podem melhorar os seus *service desks*, Paulo Magalhães, Vice-Presidente do Sul da Europa, destaca dois temas fundamentais: Autonomia e automatização.

É necessário fazer o *shift left*, de forma a conseguir levar para o lado do utilizador final a capacidade de conseguir encontrar soluções para esse tipo de questões que têm zero de valor acrescentado quando são executados por uma pessoa. Exemplo: em 80% das organizações, o *reset* da *password* é feito por uma pessoa, se não mais. O valor acrescentado de ter uma pessoa a fazer um *reset* de uma *password* é zero. É evidente que é preciso garantir confidencialidade, automatização, mas também é preciso ter atenção que 30% ou 40% dos incidentes de uma organização são *resets* de *password*.

Por outro lado, quando se desenvolve um projeto é preciso ter em mente que é preciso automatizá-lo num curto espaço de tempo e que existem desafios que têm em conta uma lógica de custo-benefício.

"O ITSM deve estar na lista de prioridades das organizações que enfrentam a transformação digital", mas existem ainda empresas que não investem neste tipo de soluções.

A transformação digital impõe uma pressão enorme nos sistemas de informação que passam a ser um pilar estratégico nas organizações. O número de pedidos é tão grande que a capacidade de resposta é limitada, sendo precisos cada vez mais recursos e profissionais especializados. Em muitas organizações, as áreas de negócio a fazer *shadow IT* e a procurar soluções externas, porque o departamento de IT não lhes consegue dar resposta.

Quando questionado sobre os chatbots, Paulo Magalhães, afirma que "são e serão uma mais valia, entroncando no que foi falado antes. Vamos ter que ter a capacidade de fazer o *shift left*, de transferir para os utilizadores finais a sua capacidade para aceder a determinados serviços e conseguir disponibilizar esses serviços onde quer que seja, a que horas seja, e pelo canal que for".

"Nós temos apresentado soluções interessantes aos nossos clientes, como é o caso do Teams, que nos responde ao 'o que é que eu tenho que fazer hoje?' com uma lista de tarefas".

Os chatbots são mais um canal e um serviço para poder dar esta resposta aos clientes, principalmente aos da geração milénio. É ainda importante que este esteja alinhado a uma estratégia global, bem como uma base de conhecimento.

"No ponto de vista do utilizador final, mas também para os técnicos de primeira linha e segunda linha, que vão ter que responder aos seus utilizadores. Também para esses, o chatbot é importante porque é uma forma de conseguir ter acesso a informação que permite, rapidamente, dar uma resposta aos utilizadores. E, portanto, o chatbot vai ter aqui dois contextos importantes, em termos de utilização", conclui Paulo Magalhães. ■

Imagem: iStock/Natali_Mis

A CRESCENTE IMPORTÂNCIA DA CIBERSEGURANÇA

As recentes fugas de dados colocaram definitivamente a cibersegurança na agenda de todas as organizações. No entanto, muitas empresas ainda veem a cibersegurança como um custo e não como um investimento. Claranet, DRC, Multicert, Noesis, Warpcom e WhiteHat partilham a sua visão sobre o mercado de cibersegurança português, os seus desafios e as suas oportunidades.

RUI DAMIÃO

Fotografias: Rui Santos Jorge

DE HÁ UNS ANOS a esta parte que o mercado de cibersegurança em todo o mundo está a crescer. Portugal não é exceção; com as empresas a passarem pelos seus processos de transformação digital, torna-se premente investir em cibersegurança. Nenhuma empresa é demasiado pequena para ser atacada.

Alterar mentalidades é, assim, essencial. A evangelização já acontece há vários anos, mas a mensagem ainda não chegou a todos os decisores das pequenas empresas. Uma falha de segurança numa pequena empresa pode, em determinados casos, colocar organizações maiores em risco.

CRESCIMENTO NO MERCADO PORTUGUÊS

Os dados mais recentes da IDC sobre o mercado português de cibersegurança, referentes ao ano de 2018, mostram que o mercado cresceu 3,6% neste período. No total, o mercado português atingiu os 135,97 milhões de euros.

A IDC estima, também, que Portugal tenha um crescimento positivo de 6,71% entre 2018 e 2022 neste mercado. Em comparação, a mesma entidade espera que o mercado de cibersegurança na região do oeste da Europa tenha um crescimento ligeiramente superior – 7,37%.

Bruno Rodrigues, Cybersecurity Specialist da Noesis, defende que, apesar de o que é o mercado de cibersegurança ainda não estar totalmente definido, a procura tem, de facto, vindo a crescer. "As empresas estão mais sensíveis, já disponibilizam dinheiro para isso", indica. "O que se tem vindo a assistir é que a cibersegurança informática fazia parte dos custos e dizer aos gestores que é mais um custo é uma chatice; ninguém gosta". Na opinião de Bruno Rodrigues, o mercado português vai assistir a "uma integração da cibersegurança nos processos da empresa e a fazer parte do negócio". Deste modo, a procura vai subir e o mercado, em termos de valor, irá aumentar.

Nuno Mendes, CEO da WhiteHat, concorda que tem existido um crescimento no mercado português. Esse crescimento, diz, estará relacionado com uma "maior perceção para o risco, fruto da comunicação que tem existido nos media e a emergente quantidade de fuga de informações de empresas de todas as dimensões". Nuno Mendes acredita que estas situações "são a prova que as pequenas e as médias empresas também têm que se preocupar de igual forma com a segurança da sua informação".

Por outro lado, o CEO da WhiteHat salienta que ainda há uma mentalidade de a cibersegurança estar no segundo plano da estratégia de muitas organizações. "Se um seguro não for obrigatório passa a ser uma opção e é um investimento a evitar; raramente é considerado um investimento. É necessário existir mais formação e sensibilização nesta área junto das empresas".

Na perspetiva da Warpcom, representada na mesa redonda por Manfred Ferreira, Technical Architect Consulting, o mercado assistiu a "um crescimento muito acentuado" em termos de requisitos de cibersegurança. A empresa detetou que apesar de existi-

- Bruno Rodrigues -
Cybersecurity Specialist, Noesis

"Nos próximos anos vamos ver uma integração da segurança nos processos da empresa e a fazer parte do negócio"

- António Ribeiro -
Head of Cybersecurity, Claranet

"Não adianta ter uma boa solução, é preciso ter as pessoas certas"

- Bruno Rodrigues, Noesis -

- António Ribeiro, Claranet -

- Luís Martins, Multicert -

rem solicitações proativas, grande parte foram reativas, tanto de setor público como setor privado. "Detetamos um forte crescimento e solicitações nesta área, não só de soluções, mas também de consultoria e identificação, análise e deteção" de falhas dentro das infraestruturas das várias organizações. Com as várias fugas de informação que têm acontecido nos últimos tempos, Manfred Ferreira estima que o crescimento possa ser superior ao que é estimado pela IDC.

David Marques, Information Security Manager da DRC, salienta que existe não só um crescimento efetivo do mercado, como também uma maior procura por este tipo de soluções. No entanto, essa procura "já não vem só do departamento de IT ou de segurança". A procura por soluções de cibersegurança chegava essencialmente pelo departamento de IT que tinha determinadas preocupações, "e agora nota-se que a procura vem por outros canais, pela gestão de topo, que já há muitas vezes o *driver* para a procura de soluções" de segurança. David Marques refere que muitas organizações têm uma preocupação com este tipo de serviços ou soluções, mas que nem sempre existe "uma estratégia que consiga levar a que essa preocupação seja satisfeita, fazendo com que os investimentos não sejam estruturados".

António Ribeiro, Head of Cybersecurity da Claranet, explica que, na sua perceção, há um crescimento no mercado português superior ao que é indicado pela IDC. Se antes as organizações olhavam para estas questões exclusivamente como um custo, atualmente "já é um *enabler*, a segurança já faz parte do negócio em si".

- Luís Martins -
Head of Cybersecurity, Multicert

"Tem de se mostrar com factos que um determinado serviço é mais eficaz do que comprar uma solução ou produto que não lhe vai resolver o problema"

- David Marques -
Information Security Manager, DRC

"É muito difícil para o decisor saber como vai priorizar o investimento; ele tem um budget, mas não sabe ao certo onde e como o vai gastar"

É NECESSÁRIA UMA ALTERAÇÃO NO MODELO DE VENDA, PARANDO DE VENDER PRODUTOS PARA VENDER SERVIÇOS

"Não adianta ter uma boa solução tecnológica", alerta António Ribeiro, que diz que "é preciso ter as pessoas certas". Simultaneamente, é preciso fazer uma alteração do produto para o serviço, onde as empresas deixam de vender apenas um produto, como uma firewall, para passar a vender serviços que de facto tragam mais valor para o cliente. Esta alteração no modelo de venda é essencial tendo em conta que "não há recursos". Muitos dos clientes viram-se, assim, para os serviços geridos para colmatar a falta de talento nas empresas.

Em relação ao estudo da IDC, Luís Martins, Head of Cybersecurity da Multicert, refere que há uma diferença entre software, hardware e serviços e os números mostram que os serviços têm um crescimento muito menor, mesmo tendo em conta que esta é a evolução natural no setor.

O Head of Cybersecurity da Multicert refere que haverá, certamente, um caminho ao passar de produtos para serviços, mas que parece que essa alteração ainda não está a acontecer no mercado português.

CONVENCER QUEM DECIDE

As organizações mudaram. As empresas mais avançadas que entendem o papel da cibersegurança já não delegam no responsável de IT ou no CISO – quando existe – a função de escolher a melhor solução. Em vários casos, é o CFO ou mesmo o CEO a dar a cara e a estar presente no processo de seleção da solução de cibersegurança adequada para a organização.

Se as grandes empresas têm interlocutores especializados nas áreas de segurança, a larga maioria das PME não. Luís Martins (Multicert), indica que "faltando recursos" nas pequenas empresas, muitas vezes é o responsável de IT que é o ponto de contacto para questões sobre a segurança da organização. "Do ponto de vista da abordagem, tem de se mostrar com factos que um determinado serviço é mais eficaz do

que comprar uma solução ou produto que não lhe vai resolver o problema. Tem de ser seguramente essa a lógica de conversa com as PME".

As pequenas e médias empresas portuguesas continuam a não ter uma abordagem de preocupação e há organizações que, mesmo tendo conhecimento das notícias de fugas de dados, acreditam que não são um alvo.

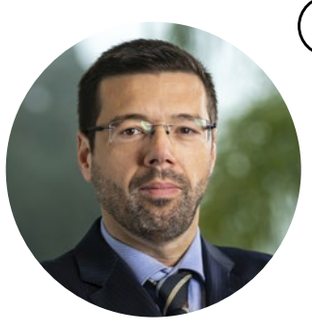
António Ribeiro, da Claranet, refere que a maneira mais fácil de convencer uma PME a adotar serviços de segurança é depois de a organização sofrer um ataque. Esta mentalidade deve-se muito ao conhecimento – muitas vezes limitado – que as empresas têm sobre estes temas e por não perceberem a necessidade que existe em proteger a sua infraestrutura, as suas operações e o seu próprio negócio. "A principal questão numa PME está relacionada, mais uma vez, com recursos; na melhor das hipóteses, têm um IT manager, mas não há pessoas dedicadas que consigam ver o puzzle todo", refere. Tendo em conta esta falta de recursos, as empresas devem contratar serviços externos para gerir a segurança das suas infraestruturas para que se possam concentrar no seu negócio e naquilo que fazem bem.

"Hoje em dia não é difícil falar com os decisores sobre segurança; há preocupações muito específicas nesse sentido", indica David Marques (DRC), que acrescenta, no entanto, que existe uma "dificuldade enorme em priorizar os investimentos. O orçamento é limitado e muitas vezes é culpa nossa, por causa das so-

- David Marques, DRC -

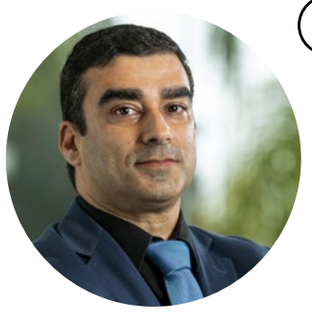
- Nuno Mendes, WhiteHat -

- Manfred Ferreira, Warpcom -



- Nuno Mendes -
CEO, WhiteHat

"É preciso passar a mensagem de cibersegurança desde o topo – onde já há um domínio completo sobre o tema –, até ao elemento que está em contacto com o cliente. Esse é um desafio grande"



- Manfred Ferreira -
Technical Architect Consulting, Warpcom

"A inteligência artificial ainda está bastante atrasada e o boom vai dar-se agora com o 5G, onde vamos ter acessos a dados massivos"

luções e dos serviços, com conceitos novos e diferentes. É muito difícil para o decisor saber como vai priorizar o investimento; ele tem um *budget*, mas não sabe ao certo onde e como o vai gastar". David Marques refere que é importante, também, que as várias empresas que trabalham com cibersegurança descompliquem os conceitos o máximo possível para que quem está do lado da decisão os possa perceber de uma forma fácil.

"A nossa abordagem não é vender cibersegurança; a nossa abordagem é ir a clientes e perceber as suas dores, as suas necessidades e o nível de maturidade" para poder ajudar o cliente, explica Manfred Ferreira (Warpcom). Também é preciso ter em conta que os clientes "não vivem as mesmas preocupações que nós", mas as empresas que vendem serviços ou produtos de cibersegurança têm que "calçar os sapatos" dos clientes e perceber quais são as suas necessidades e ajudar no investimento das soluções ou serviços que devem investir.

Nuno Mendes, da WhiteHat, relembra que a grande maioria do tecido empresarial português são as PME e que é necessário sensibilizar para a matéria relacionada com a cibersegurança. "É preciso passar a mensagem de cibersegurança desde o topo – onde já há um domínio completo sobre o tema –, até ao elemento que está em contacto com o cliente. Esse é um desafio grande". O CEO da WhiteHat indica que tudo se resume à sensibilização das empresas e dos decisores dentro das PME, a fazer uma análise de risco para que as organizações consigam perceber onde estão expostas, onde devem fazer os seus primeiros investimentos e como devem abordar o tema da melhor forma possível.

Bruno Rodrigues, da Noesis, explica que não deveria ser necessário convencer uma PME de que é preciso investir em cibersegurança. Sobre a sensibilização, Bruno Rodrigues defende que "não é necessário mais *awareness*". "As empresas não têm que ser especialistas em cibersegurança, a temática é demasiado vasta. Infelizmente as ameaças evoluem demasiado rápido, mas não tem de existir mais *awareness*; tem de existir bom senso", indica.

A INTELIGÊNCIA ARTIFICIAL ESTÁ A SER UTILIZADA POR QUEM DEFENDE E POR QUEM ATACA, QUE ESTÁ, POR NORMA, SEMPRE UM PASSO À FRENTE

Por outro lado, a cibersegurança não é um "tema sexy" e, possivelmente, é necessário que a indústria transforme o tema mais atrativo para que as várias organizações invistam mais nestes temas dentro do seu negócio.

INTELIGÊNCIA ARTIFICIAL APRESENTA-SE AO SERVIÇO

É sabido que a Inteligência Artificial (IA) está cada vez mais presente nas operações diárias das organizações e na vida das pessoas de uma forma geral. Na cibersegurança não é exceção. É a IA que permite analisar uma grande quantidade de dados de ataques e perceber padrões, identificar os principais alvos de ataques e auxiliar na defesa dos sistemas.

Simultaneamente, a inteligência artificial pode – e é – utilizada do 'lado de lá'. Não é só quem defende que tem IA ao seu dispor; também o lado negro utiliza inteligência artificial para um sem número de possibilidades num ataque a uma ou mais organizações.

Luís Martins (Multicert) acredita que a inteligência artificial "é o caminho inevitável" para a cibersegurança. No entanto, relembra, a diferença entre quem defende e quem ataca é que quem defende "está sempre um bocadinho atrás". "Qualquer atacante mais empenhado utiliza técnicas de *data analysis* para chegar a informação que está exposta. É possível fazer *scripts* fáceis para chegar a conclusões rápidas" para ter uma "base de dados interessante" para fazer um ataque a uma organização. Quem defende, por outro lado, ainda não está a utilizar todo o potencial para se proteger da melhor forma e ainda há um "caminho de estruturação" a percorrer para atingir todo esse potencial.

Os dispositivos IoT alargaram a base de possíveis portas de entrada para todas as empresas. Assim, é necessário um modelo de automação de análise de incidentes para que seja possível analisar a grande quantidade de dados gerados. António Ribeiro (Claranet) diz que a inteligência artificial pode ajudar muito numa primeira linha de ataques, onde pode não existir sequer intervenção humana e ser endereçado de forma totalmente automática. O próximo passo serão os modelos preditivos onde se pode deixar de falar de "*zero days*" e passar a falar "*negative days*". Estes modelos, aliados à inteligência artificial, vão perceber determinados padrões que levam a um ataque cibernético.

O Cybersecurity Specialist da Noesis refere que a IA "é um tema sexy" onde "toda a gente quer saber, mas quase ninguém vai implementar". A

SÓ FAZ SENTIDO FALAR DE IA DEPOIS DAS ORGANIZAÇÕES TEREM O BÁSICO. É PRECISO, PRIMEIRO, TER AS BASES DE CIBERSEGURANÇA

luta entre defensores e atacantes neste campo é "extremamente desigual". Enquanto quem defende tem uma tarefa difícil para conseguir *datasets* para machine learning, os hackers, alguns que têm várias redes infetadas, têm acesso a uma quantidade quase infindável de dados.

Em vez de inteligência artificial, a Noesis prefere o termo "inteligência assistida" que analisa as informações e entregam à pessoa o que é mais relevante para que o colaborador possa proteger da melhor forma a organização que está a sofrer um ataque, distribuindo o seu esforço consoante a gravidade dos ataques.

O Technical Architect Consulting da Warpcom revela que a transformação digital faz com que exista cada vez mais informação que nem sempre é válida, e onde o tempo de validade dessa informação é cada vez mais reduzido. "A inteligência artificial ainda está bastante atrasada e o *boom* vai dar-se agora com o 5G, onde vamos ter acessos a dados massivos, conseguir extraí-los e analisá-los em tempo real para tomar ações", refere Manfred Ferreira, acrescentando que "aí sim, a inteligência artificial vai ser mais uma componente, não vai ser o único".

O Information Security Manager da DRC acredita que o mercado "ainda está numa fase muito embrionária de exploração da potencialidade" do que a IA pode fazer. No entanto, alerta, "se a maioria das organizações não têm o básico, quanto mais estarmos a falar de machine learning e inteligência artificial". "Há áreas onde faz todo o sentido a automação, a orquestração e a questão da mudança de força de trabalho. Por causa de tudo aquilo que estas novas capacidades trazem para as organizações, é bem provável que aquilo que são os SOC 24/7 se transformem", onde a inteligência artificial terá, certamente, um papel importante. "Agora, até chegarmos lá, há um trabalho humano muito, muito grande para poder potenciar estas capacidades de forma efetiva", diz.

O CEO da WhiteHat afirma que, em termos práticos, o que se assiste em Portugal são ações mais simples que não envolvem inteligência artificial, mas que deixam um impacto severo em cada organização. "Existe, contudo, outros vetores de ameaça que tiram proveito de ataques massivos que não carecem de um *profiling* e reconhecimento no sentido de perceber quais são as vulnerabilidades", indica Nuno Mendes. Por norma, refere, os ataques em Portugal aproveitam vulnerabilidades já conhecidas e ameaças *zero days* e é necessário que existam sistemas que consigam identificar esse tipo de ameaças. ■

claranet

POR ANTÓNIO RIBEIRO
Head of Cibersecurity, Claranet Portugal

PME SÃO ATRATIVAS PARA OS CIBERCRIMINOSOS

Existe uma perceção no mercado de que quanto mais pequenas forem as empresas, menos atrativas serão para os cibercriminosos. Nada está mais longe da realidade.

SE ESTA PERCEÇÃO poderá ter feito sentido a dada altura – seguindo até a filosofia da criação dos "vírus", que visavam alcançar o máximo denominador comum -, atualmente não o faz, até porque os criminosos evoluíram de forma a tornar mais eficientes as suas operações. Sigamos esta premissa: quais os custos para um criminoso de atacar uma grande organização com inúmeras defesas de segurança (ao nível de tecnologia, de recursos humanos e de processos), quando comparável com o ataque a uma PME que, na maioria das vezes, não possui sequer colaboradores especialmente dedicados a cuidar da segurança da informação?

Mesmo nos casos de ataques com técnicas de ransomware, em que fará sentido pensar que será tanto maior o prémio quanto maior for a organização, de uma forma geral a relação custo/benefício sai melhorada nos ataques às organizações de menor dimensão e, na maioria dos casos, mais desprotegidas. Até porque a proporção dos danos, face à escala da própria empresa, pode fazer toda a diferença.

A verdade é que os atacantes sabem isso: quem pagaria mais rapidamente um resgate? Uma pequena indústria com a produção parada e sem preparação para responder a estes ataques, ou uma grande organização que está preparada para este tipo de situações?

Os atacantes escolhem os alvos que melhor servem os seus propósitos e esses alvos nem sempre serão os mais óbvios. Por exemplo, para atingir uma grande organização,

- António Ribeiro -
Head of Cibersecurity,
Claranet Portugal

poderá ser mais eficaz atacar e comprometer um dos seus fornecedores. Esta ação poderá ter um impacto tal que levará eventualmente o fornecedor a fechar o seu negócio, criando uma dificuldade significativa no seu verdadeiro alvo - mesmo que de forma indireta.

De acordo com dados do Parlamento Europeu, o tecido empresarial da União Europeia (UE) é composto em 99% por micro, pequenas e médias empresas, que contribuem para mais de metade do valor acrescentado total criado pelas empresas na UE. Ou seja, não só o ataque é mais fácil, como alvos não faltam...

A cultura de ocultação dos ataques, que teima em existir, transmite uma falsa perceção de normalidade, contribuído também para tornar as PME atrativas aos cibercriminosos. Seja por questões de proteção da marca, para manter os clientes ou, em última instância, para garantir que o negócio não fecha, a realidade é que - e a menos que seja estritamente necessário por questões legais -, os ataques não são comunicados. Esta perceção de que "está tudo bem", leva as PME a negligenciar a segurança da sua informação.

Apesar de tudo, progressivamente vamos assistindo a alguns bons exemplos nesta área, como aconteceu em 2019 com a Norsk-Hydro - uma empresa norueguesa que viu as suas ações subirem após sofrerem um ciberataque massivo, tudo devido à preparação que foi feita e a uma estratégia adequada de comunicação. Não sendo uma PME, esta empresa foi pioneira na forma de comunicar um ciberataque, dando o exemplo a outras organizações e abrindo o caminho para a forma correta de agir nestas circunstâncias.

O que podem então fazer as PME, tendo em conta os escassos recursos que normalmente dispõem nesta área?

Não existe uma fórmula que sirva a todos. Ainda assim, da mesma forma que estas organizações externalizam serviços que não fazem parte do seu *core-business*, poderão fazer o mesmo no que respeita à segurança da informação. Enquanto planeiam uma estratégia de ciberdefesa de longo prazo, o recurso a especialistas externos que podem monitorizar e reduzir as ameaças a que estão sujeitas é um *quick-win* com resultados imediatos.

A utilização destes serviços dificilmente poderá resolver todos os problemas. Mas permitirá reduzir de imediato o risco a que as PME estão sujeitas e, progressivamente, introduzir uma cultura de cibersegurança como parte de um processo de melhoria contínua.

Ao lidar regularmente com especialistas em cibersegurança, as próprias organizações introduzem novos processos e eliminam os antigos que as deixavam mais expostas. Tornam-se assim mais resistentes a novos ataques, compreendem a importância de comunicar e partilham a experiência com o setor, fazendo com que todo o ecossistema se torne mais resiliente. ■

DAVID MARQUES,
Information Security Manager,
DRC

– A GOVERNANÇA DA INSEGURANÇA –

Já quase não é necessária introdução ao tema da segurança da informação ou cibersegurança, e explicar a necessidade que existe nas organizações de se focarem naquilo que hoje, pela relevância que tem, deixou de ser apenas uma questão de proteção dos ativos de uma organização, mas um business enabler, que permita de uma forma mais rápida tornar algo reativo em algo proativo

AS NOTÍCIAS NOS MEDIA são frequentes sobre os problemas que a insegurança traz, desde perdas financeiras diretas e indiretas, danos reputacionais difíceis de medir, entre outros, e aquilo que sabemos pelos media são apenas a ponta do iceberg.

Assim como qualquer organização real que conhecemos, as organizações que operam no mundo do cibercrime são em tudo semelhantes no seu objetivo mais básico, que é obter determinado lucro financeiro. A diferença é que as últimas não têm de cumprir determinadas regras, operam em horários que nós não operamos e são especializadas naquilo que é o seu *core business*, o que torna muitas vezes complicado o desafio de quem tem de proteger os seus ativos. Pior ainda estão as nossas PME, que são a maioria do nosso tecido empresarial, mas na maioria dos casos com uma dimensão reduzida que não lhes permite ter recursos dedicados e focados em cibersegurança.

Será que o problema está no facto de os criminosos serem tecnologicamente mais avançados do que nós? Será que têm ferramentas extremamente complexas que mais ninguém tem? Dificilmente isso acontece e, quando acontece, raramente utilizam essas ferramentas para a realidade que aqui se discute, poderá ser uma realidade em situações de ciberguerra entre estados ou espionagem ao mais alto nível. Se o nosso problema não é a tecnologia que temos, qual é?

- David Marques -
Information Security
Manager, DRC

Governança! Se não sabemos qual é o nosso objetivo, dificilmente vamos conseguir decidir qual é o caminho a seguir, porque não sabemos ao certo para onde vamos. Se não temos uma estratégia, não conseguimos traçar objetivos e, sem objetivos, a forma como gerimos a cibersegurança corre o risco de ser apenas um conjunto de atividades desagregadas, que trazem um valor muito limitado para a organização, que na realidade já tem um *budget* limitado. Uma tecnologia, por muito melhor que seja, não traz um grande valor para a organização, se não for implementada, gerida e monitorizada de forma adequada.

Quando damos algum tipo de resposta a incidentes de cibersegurança, é comum encontrarmos situações em que o cliente tem muita e "boa" tecnologia, mas não faz ideia de como está implementada, com que lógica e sem qualquer tipo de monitorização. Ou seja, o investimento não lhe deu o retorno que esperava, porque na realidade, em muitos casos, tinha uma expectativa irrealista sobre cibersegurança.

Portanto, na realidade, em muitos casos, aquilo que fazemos é Governança da Insegurança em vez de Governança da Segurança ou Cibersegurança. O que necessitamos é subir um degrau, olhar de uma posição mais elevada e definir uma estratégia para a cibersegurança. A estratégia não tem de ser algo complexo, fruto de um processo longo e oneroso de consultoria, mas pode ser algo simples e realista tendo em conta o contexto da organização em que estamos. A questão de "olhar" para o contexto é fundamental, pois não existem duas organizações iguais, e os desafios e necessidades diferem muito dependendo do contexto em que estamos. Este tema do contexto é bem mais importante do que a dimensão da organização, pois algumas vezes organizações pequenas, dependendo da sua área de atuação, exposição pública, complexidade do ecossistema de IT, podem ter necessidades de cibersegurança bem mais complexas que outras organizações maiores em contextos distintos.

Não precisamos de complicar para definir uma estratégia. Nem precisamos de inventar a roda novamente. Temos *frameworks*, como por exemplo NIST, ISO 27001, CIS20, que nos ajudam a ter uma abordagem muito mais holística à cibersegurança. Ainda mais, temos uma *framework* criada em Portugal, pelo CNCS, adaptada em boa parte à realidade do nosso mercado mais centrado em PME, que pode ser uma base para a avaliação do nosso estado atual e para a definição de uma estratégia simples, mas com objetivos específicos ao longo de um período (anual ou bianual), que permita aumentar realmente os níveis de maturidade das organizações.

Para as organizações que não têm capacidade de ter recursos internos para alocar a este tema da cibersegurança, é necessário recorrer a MSP, empresas focadas em Segurança da Informação ou Cibersegurança, assim como atualmente recorremos a serviços externos para áreas não core das empresas, como contabilidade, IT, etc.. Essa visão de especialistas pode ajudar a ter uma perceção real do estado atual de maturidade e ajudar as organizações a definirem estratégias simples, mas coerentes e com objetivos definidos, que servirão para existir uma real Governança da Segurança em vez de Governança da Insegurança. ■

multicert

POR LUÍS MARTINS
Head of Cybersecurity da Multicert

– O VALOR DE UM SOC –

Com o crescimento do número e severidade dos ciberataques, as estratégias exclusivamente focadas na prevenção de incidentes de segurança já não são uma opção. O que exige uma mudança de mentalidade: as organizações têm de deixar de pensar "se vão ser atacadas" e adotar uma abordagem de "quando forem atacadas".

EXIGE, IGUALMENTE, AÇÃO. O tempo e os recursos disponíveis na deteção e resposta aos incidentes são fundamentais para, se não impedir, pelo menos limitar e atenuar os efeitos de um incidente grave de segurança.

Os Security Operations Center (SOC) são, por isso, um tema crucial para se endereçar as ciberameaças crescentes. Servem como um ponto de coordenação central para a recolha e análise de informações de segurança, bem como para a resposta aos incidentes de segurança.

AS AMEAÇAS NÃO DORMEM, LOGO UM SERVIÇO DE SOC TAMBÉM NÃO O PODE FAZER

Porque o cenário de ciberameaças de hoje se transforma a grande velocidade e os atacantes são capazes de comprometer uma organização rapidamente, aceder e extrair informação valiosa.

Assim, **o tempo é essencial** quando uma organização é atacada.

As equipas de segurança devem detetar e bloquear o ataque o mais rapidamente possível para terem alguma hipótese de minimizar os danos, fazendo uso de monitorização 24 x 7 x 365 dos ativos críticos.

O SERVIÇO DE SOC CONTRIBUI PARA A CRIAÇÃO DE VALOR NA ORGANIZAÇÃO

O tema do digital - e da segurança em particular - há muito que deixou de ser um assunto interno às organizações e específico das equipas de IT, e passou

- Luís Martins -
Head of Cybersecurity da Multicert

a ser sobretudo um fenómeno de contexto. As organizações como um todo procuram aproveitar o tema da segurança - e da confiança que lhe é inerente - para **trabalhar a reputação e explorar novas oportunidades de negócio.** Mas também se expõem a um conjunto de novas ameaças que estão longe de controlar.

Desta forma, não só este fator contribui cada vez mais para a criação de valor nas organizações – estando cada vez mais associado à satisfação das necessidades das partes interessadas (internas e externas) - como é um **recurso fundamental para a minimização dos riscos** – reputacionais, financeiros e operacionais.

A IMPORTÂNCIA DE RECOLHER OS DADOS RELEVANTES

Um SOC depende de um fluxo constante de dados fiáveis e relevantes de uma ampla variedade de soluções - de segurança, aplicações e componentes de infraestrutura. Na maioria das organizações, os dados exigidos pelo SOC são armazenados em diferentes sistemas e são muitas vezes inacessíveis aos analistas de segurança.

A IMPORTÂNCIA DE ESCOLHER O PARCEIRO CERTO PARA A GESTÃO DO SERVIÇO DE SOC

Os fornecedores de serviços oferecem uma variedade de serviços de suporte ao SOC, podendo as organizações decidir contratar um parceiro para desempenhar várias funções no contexto de um SOC. O envolvimento de um parceiro pode incluir várias abordagens:

- Apoio no design do SOC ou de uma função em particular, nomeadamente na definição de requisitos, seleção de soluções tecnológicas e design de uma arquitetura SOC;
- Desenhar, configurar e implementar recursos do SOC;
- Disponibilizar uma equipa operacional para o SOC, quer seja na fase inicial para colocar o SOC em funcionamento ou posteriormente como um serviço de capacitação da equipa a longo prazo.

Há algumas considerações a ter, no momento da escolha de um parceiro:

- Serviços avançados.
- Automação e orquestração.
- Utilização de Inteligência de ameaças.
- Segurança na nuvem.
- Portais de serviços de segurança.

EM RESUMO:

O serviço SOC fornece às organizações um centro de excelência para operacionalizar atividades de segurança, responder a incidentes, recolher e analisar inteligência sobre ameaças e monitorizar a segurança. A decisão de selecionar um parceiro de serviços de segurança é estratégica, com implicações até o nível executivo, podendo ter ramificações para questões críticas do negócio, como gerir riscos corporativos e permitir o sucesso de estratégias de transformação digital. ■

warpcom

"O DESENVOLVIMENTO DE COMPETÊNCIAS, CELERIDADE DE RESPOSTA E RESILIÊNCIA DAS ORGANIZAÇÕES É CRUCIAL"

Manfred Ferreira aborda o mercado de cibersegurança e os principais benefícios e riscos das organizações.

Como vê o mercado de cibersegurança?

No mercado de cibersegurança Ibérico, os clientes focam-se essencialmente no seu core business. Tal implica, num plano técnico-operacional, a passagem para a lógica de serviço e operações automatizadas em ambientes partilhados. Estamos a falar num modelo híbrido, que já desenvolvemos há cerca de cinco, sete anos, e de uma seleção natural de parceiros de confiança na criação de políticas proativas e transversais.

De que forma as organizações ficam expostas quando globalizam os seus serviços e evoluem na transformação digital do seu negócio?

A maioria das entidades em Portugal não se cinge a responder a normas e regulamentos nacionais, mas sim a normativas do mercado europeu e, em alguns casos, mundial. Este aumento de exigência, acarreta uma maior exposição a riscos de maior diversidade e complexidade. Neste contexto, o desenvolvimento de competências, celeridade de resposta e resiliência das organizações é crucial. Para tal, é aconselhável recorrer a soluções híbridas e serviços geridos que permitam ter a "visibilidade" para a tomada de decisão e a serviços complementares na cloud e data centers que garantam a "disponibilidade" necessária. Por último, deve ser garantida a cibersegurança destas soluções e serviços através de múltiplas camadas. No caso dos ambientes partilhados e distribuídos

- Manfred Ferreira -
Technical Architect
Consulting, Warpcom

como na Amazon, Azure ou Google ou através de ambientes em Cloud privada e micro redes assentes em IaaS, PaaS, DaaS e FaaS, há que garantir também a proteção dos endpoints e respetivos dados. As soluções de EPP e DLP são imprescindíveis, uma vez que asseguram a proteção contra exfiltração dos dados e documentos, aportando valor e sustendo a base da transformação digital num contexto de trabalho em qualquer localização e momento.

Como se posiciona a Warpcom face ao gap de competências existente?

A capacitação contínua dos seus especialistas é uma das fortes apostas da Warpcom. Cientes da importância dos processos de identificação de tendências e riscos de exposição das organizações, é feito um forte investimento em constantes atualizações tecnológicas juntos de parceiros de renome de cibersegurança. Do ponto de vista da oferta, detemos serviços especificamente desenvolvidos para capacitar as organizações de destreza e celeridade de reação e tomada de decisão, i.e. formação empírica com base na simulação de cenários para aplicação de técnicas de defesa e ataques cibernéticos num contexto de Cyber Range e War Game, investigação e análise forense e também a presença em grupos chave que permitem extrair previsões de antecipação de movimentos e tendências. Deste último ponto, resultam ações de mitigação dos riscos emergentes e soluções especificamente desenvolvidas para a realidade de cada organização.

Quais as principais soluções da Warpcom para o mercado de cibersegurança?

As nossas soluções de cibersegurança dividem-se, de uma forma geral, em:

- **Strategic Services** – serviços de consultoria tecnológica especializada que visam avaliar a capacidade de resposta das organizações, nomeadamente através de assessments de segurança, desenvolvimento de políticas de navegação na internet, gestão de acessos e de identidades. Também o desenvolvimento de planos de gestão de incidentes, gestão e otimização do parque e arquitetura e a revisão das soluções e de código num ciclo de CD/CI são considerados.

- **Serviços Geridos** – o Warpcom Command Center apoia na transformação e automatização de processos proativos de gestão (NOC) e proteção (SOC) das redes das empresas. Ao serem prestados por um parceiro especializado, estes serviços permitem que as organizações foquem o seu esforço e investimento no seu core business.

- **Warp Academy** – treino especializado de capacitação das equipas do cliente na resposta a incidentes, na resiliência e no apoio à continuidade do negócio. Esta tipologia de treino expõe os seus formandos a uma experiência híper-realística, baseada em cenários complexos com diferentes densidades de equipamentos, aplicações e serviços. Desta forma as equipas adquirem competências empíricas sobre como se proteger e atuar quando deparadas com ataques externos, e como conter e reverter a propagação de malwares, trojans e especificamente a proliferação de ransomware. ■

WhiteHat

POR NUNO MENDES
CEO da WhiteHat

DLP: COMO PROTEGER A SUA EMPRESA COM UMA ABORDAGEM INTEGRADA À CIBERSEGURANÇA

A prevenção de perda de dados, ou DLP (Data Loss Prevention) é uma abordagem integrada e consolidada da segurança da informação.

MAIS DO QUE SIMPLESMENTE erguer "barreiras", coloca em prática uma série de regras através das quais é possível assegurar a confidencialidade, integridade e disponibilidade da informação.

O ano de 2019 foi marcado por constantes notícias de fugas de dados em grandes organizações, que deram a conhecer a perda de milhões de registos com informação sensível (ex.: dados médicos, financeiros, pessoais, entre outros) e milhões de euros de prejuízo.

As empresas começam a estar mais conscientes da importância de implementar uma tecnologia DLP para protecção da sua informação e propriedade intelectual. De acordo com a Gartner, prevê-se que até 2021, cerca de 90% das organizações irão implementar pelo menos uma forma de DLP, o que representa um acréscimo na ordem dos 50% face à situação registada em 2019.

O desafio nem sempre é fácil para as organizações, principalmente para as PME. Existem dificuldades em identificar a melhor abordagem para implementar uma estratégia de DLP adequada, seja pela falta de conhecimento, recursos ou nível de sensibilidade e importância dos dados a proteger. É também importante que os decisores encarem esta implementação de segurança da sua informação como um investimento e não como um custo.

- Nuno Mendes -
CEO da WhiteHat

O DLP É UMA MEDIDA ESSENCIAL PARA A PROTEÇÃO DA INFORMAÇÃO E PROPRIEDADE INTELECTUAL.

A tecnologia DLP é a melhor medida para prevenir e antecipar diversos riscos, nomeadamente: roubo de dados por parte de colaboradores internos ou externos e ainda perda / roubo físico de equipamentos portáteis. A proteção de vetores de fuga vai desde o email, messaging, redes sociais, serviços de cloud, dispositivos USB, entre outros.

DESAFIOS DAS ORGANIZAÇÕES

PERDA/ROUBO FÍSICO

Tomemos como exemplo uma empresa com uma equipa de vendas com trabalhadores em mobilidade. Os seus equipamentos contêm certamente dados sensíveis de clientes, fornecedores e até credenciais de acesso a sistemas. Numa situação de perda ou roubo destes equipamentos é necessário assegurar que toda a informação que armazenam está protegida com tecnologia de encriptação (vertente de DLP) capaz de impossibilitar o acesso indevido aos dados.
A WhiteHat tem várias propostas de DLP adequadas a organizações de qualquer dimensão. Uma das soluções, foca-se no risco de perda ou roubo físico de computadores. Trata-se do ESET Full Disk Encryption que funciona em conjunto com as soluções de protecção de endpoints (ex.: ESET Endpoint Protection Advanced).

Para organizações com requisitos de encriptação mais abrangentes, o ESET Endpoint Encryption, disponibiliza encriptação integral de discos, pastas, ficheiros e dispositivos externos. A aplicação de regras e políticas de segurança é efectuada através de uma consola dedicada que permite a gestão completa de computadores, chaves de encriptação e partilha de chaves mesmo entre utilizadores em mobilidade.

FUGAS DE DADOS

A fuga de dados por colaboradores é outro desafio no quotidiano das empresas, bem como a exfiltração de informação por parte de agentes externos.
O Safetica Full DLP é uma solução que evita a fuga indevida de informação confidencial através da aplicação de regras definidas pela organização. Processos simplificados de classificação de documentos e identificação de vectores de fugas, permitem uma fácil implementação de um plano eficaz de segurança da informação.
A WhiteHat e a sua rede de parceiros estão disponíveis para dar resposta a qualquer organização que pretenda avaliar e implementar a tecnologia DLP. ■

BI4ALL AUMENTA EFICÁCIA DO PESTANA HOTEL GROUP

O Pestana Hotel Group implementou a estratégia de analytics da BI4ALL nos departamentos de IT e de Business Intelligence, conseguindo acesso aos dados de forma estruturada, retirando todo o potencial da informação agregada.

O DESAFIO

O Pestana Hotel Group, passou por uma fase de grande crescimento nos últimos anos e também por uma transformação do modelo de negócio do setor da hotelaria.

Esta cadeia de hotéis, tinha o processamento de grandes quantidades de dados oriundos de múltiplas fontes independentes e cada uma das suas equipas trabalhava de forma independente e produzia os seus próprios *dashboards* e *reports*, o que resultava em várias versões do mesmo conteúdo. O facto da informação estar dispersa conduzia a discrepâncias nos dados e dificuldade na geração de informação que não existia ou era muito difícil de obter, o que resultava numa falta de eficácia. No passado, o grupo tinha várias equipas a fazer recolha e tratamento de dados de vários sistemas, sem que houvesse uma plataforma ou sistematização da recolha dos dados. Foi então que o Pestana Hotel Group implementou a estratégia de Analytics da BI4All, nos departamentos de IT e de Business Intelligence, mas também as áreas operacionais para garantir um alinhamento entre os dados produzidos e as necessidades da operação.

Atualmente, presente em 16 países, o grupo depara-se com mais informação e modelos de negócios sendo por isso, bastante importante obter os dados de forma concisa e constante para as mais de cem unidades e regiões.

AS SOLUÇÕES

As soluções de Analytics permitem que qualquer organização seja mais ágil e competitiva, conseguindo acesso aos dados de forma estruturada e assim retirar todo o potencial da informação agregada. Ao adotar tecnologias disruptivas, possibilita o acesso mais rápido à informação, tomadas de decisões estratégicas mais eficientes, baseadas em informação fidedigna e em tempo real, uma resposta mais eficaz aos constantes desafios da atividade. Um maior conhecimento do cliente, possibilidade de antecipar tendências, gestão mais eficiente de todos os recursos e uma visão completa de toda a organização são algumas das principais vantagens desta solução.

"A solução do Pestana Hotel Group é uma solução em constante evolução, sendo que o grupo tem recursos internos sempre a fazer pequenas evoluções e conta com a BI4All para desenvolvimentos também de novas áreas ou adições disruptivas. A solução é constituída por um base comum baseada na framework BI4All para *hospitality* e que foi posteriormente personalizada para as necessidades do cliente", explica José Oliveira, CEO da BI4All.

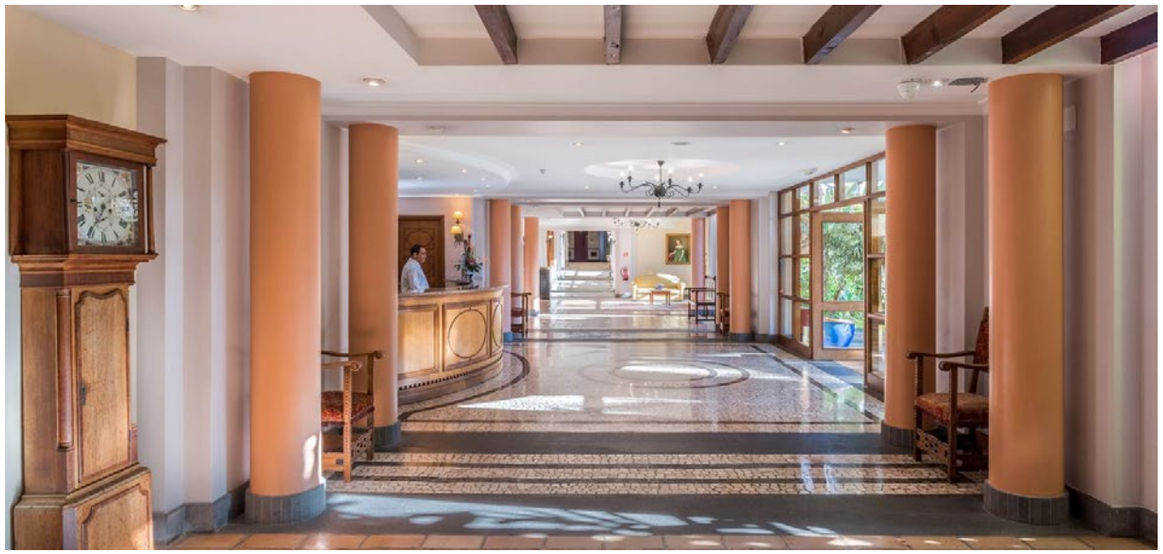
Com a implementação da solução de Analytics com a BI4All, o Pestana Hotel Group passou a dispor de um único repositório de dados centralizado, o que lhe possibilita analisar mais informação e de forma mais rápida, conseguindo inclusive cruzar os dados oriundos das operações, das receitas ou dos diversos produtos que oferece, das diversas áreas do grupo. Hoje, a informação está consolidada e é atualizada diariamente em *dashboards*, onde é possível consultar toda a informação agregada, bem como a respetiva análise até ao detalhe máximo, permitindo assim retirar os maiores *insights* possíveis de análises de desempenho por mês, região, hotel, etc..

"A solução desenvolvida pela BI4All foi a melhor opção uma vez que se enquadrava perfeitamente nos nossos objetivos. A solução é composta por um conjunto de processos de recolha e tratamento de informação que recolhem num único repositório toda a informação das diversas áreas do grupo, culminando na disponibilização de um conjunto de *dashboards* facilmente acessíveis por toda a organização", afirma Verónica Soares Franco, Executive Committee Member do Pestana Hotel Group com os pelouros de BI, Inovação e Recursos Humanos.

Atualmente, o grupo depara-se com mais informação e modelos de negócio sendo importantíssimo obter os dados de forma concisa e consistente para todas as unidades e regiões.

"Neste momento, através da solução imple-

mentada, conseguimos cruzar inúmeras fontes de dados e assim tornar o fluxo de trabalho muito mais rápido e ágil. Temos uma única fonte o que simplifica e otimiza o trabalho de todos dentro da organização tendo também a informação mais estruturada e organizada numa única plataforma, o que simplifica e otimiza o trabalho de todos dentro da organização. Ganhou-se em eficácia, rapidez na tomada de decisão, em produtividade e num aumento do grau de confiança dos dados que usamos para as tomadas de decisão", garante Verónica Soares Franco.



OS RESULTADOS

A BI4All, através de soluções de *analytics* adaptadas às necessidades do cliente, permitiu que o Pestana Hotel Group conseguisse retirar o máximo partido dos dados gerados para que a gestão se foque mais na análise e nos resultados.

As vantagens desta solução para o Pestana Hotel Group são o exemplo claro de como as soluções de *data analytics* acrescentam valor para as organizações e são de facto uma mais valia para o sucesso do negócio. O mercado português tem apresentado uma crescente recetividade para projetos na área de *data analytics* e inteligência artificial, apesar de ainda haver um longo caminho a percorrer, já são muitas as empresas que apostam numa estratégia *data-driven*.

As áreas de *analytics* e big data têm sido áreas de profundo crescimento e de rápida evolução, fruto do seu potencial de transformação da gestão com dados relevantes para a tomada informada de decisões, em tempo real. Antecipar tendências de consumo, perceber mudanças de mercado antes que estas se tornem evidentes, tudo isto é possível com as mais avançadas soluções de analítica disponíveis.

"O grupo reconhece que as equipas da BI4All têm um elevado conhecimento técnico, bem como experiência nos vários tipos de negócio, o que é de facto determinante para perceber as principais necessidades do cliente e obter resultados de excelência que influenciam diretamente os resultados do negócio", conclui José Oliveira. ■

– O CASAMENTO PERFEITO ENTRE BI E INTELIGÊNCIA ARTIFICIAL –

"O melhor ainda está por vir", a frase que marca o brinde dos noivos também se aplica à BI e IA – tecnologias que uniram forças para empoderar empresas através do uso de dados.

AO AJUDAR NA TOMADA DE DECISÕES e permitir a competição no mundo digital, a AI deve ultrapassar os limites do tradicional BI transformando a ferramenta que disponibiliza relatórios padrão, numa solução para a tomada de importantes decisões de negócios baseadas em dados.

Ilustração: Designed by starline / Freepik

Tal deve-se ao facto de as indústrias de BI e analytics se encontrarem numa nova onda de disrupção por causa da inteligência artificial e machine learning. No estudo apresentado no ano passado, o 'Augmented Analytics', ou a Análise Aumentada, como é chamada pelo Gartner, foi apresentado o futuro da análise de dados que, na prática, é capaz de automatizar os *insights* através de machine learning e geração automática de texto. No evento, empresas novas e antigas demonstraram que a AI, quando influenciada por essas análises, como a linguagem de processamento natural (NLP, em inglês), pode recomendar *insights* até em forma de texto.

É essa linguagem de processamento natural que permite aos utilizadores de ferramentas de BI e analytics criar relatórios usando comandos

de voz, fazer perguntas e até mesmo declarações. Os *insights* gerados vão para além de fazer recomendações "pré-formatadas" aos utilizadores. É possível prover dados adicionais, dado que estas ferramentas contam com a inteligência para responder a questões importantes sobre os negócios e produtos, sem exigir muito do utilizador.

Essas narrativas são automatizadas e usam a linguagem natural para fornecer uma resposta baseada na análise de dados. Por exemplo, para o questionamento sobre vendas, o sistema de BI pode adicionar textos descritivos como "este trimestre a receita foi de X, um aumento de Y por cento se comparado com o trimestre anterior. Dessa forma, a receita do próximo trimestre será de Z €". E já existe um número considerável de empresas usando ferramentas que perguntam às máquinas para conseguir as respostas mais rápidas.

SALTANDO DA ERA DOS RELATÓRIOS PARA A DOS INSIGHTS

Mesmo com múltiplos exemplos destas tecnologias, o BI ainda exerce a função antiga de criar e gerar relatórios nas empresas, e o problema está na falta de análise de dados. Os utilizadores de negócios e executivos querem respostas rápidas.

Soluções de BI e analytics podem entregar essa lista ambiciosa de capacidades e definitivamente acabar com o estigma do BI ser uma ferramenta apenas para geração de relatórios e transformá-lo em algo mais preditivo, capaz de "prescrever" o futuro. Ao invés de oferecer ferramentas de análises para gerar relatórios, as plataformas de analytics e BI aumentada por AI, permitirão que os executivos possam fazer perguntas usando a linguagem de negócios do dia a dia, e receber recomendações sobre possíveis ações.

O BI PRECISA DA AI

No entanto, até a mais moderna ferramenta de BI ainda necessita de um *expert* para encontrar o dado certo, perguntar a questão certa e interpretar os resultados corretamente, por forma a atingir resultados de negócios tangíveis. A pesquisa Global Business Technograph survey afirma que grande parte dos tomadores de decisões de dados e analytics estão 52% do lado do negócio e 63% da tecnologia e planeiam contratar pessoas com habilidades de dados avançadas para apoiar as empresas nas iniciativas direcionadas a dados.

A Forrester aponta que aceder a dados não é suficiente. É igualmente necessário o recurso a especialistas para escolher o dado correto e fazer perguntas, e a AI desempenha um papel importante em identificar o dado correto e surgir com resultados relevantes para todos os acionistas de negócios.

Não há dúvidas, portanto, que a AI-aumentada "Analytics Inteligente", é a próxima onda da disrupção na indústria de business intelligence. Para os utilizadores de negócio, essa trajetória de inovação é ampla, e uma prova disso é que, de facto, o melhor ainda está por vir. ■

Ilustração: Designed by makyzz / Freepik

O FUTURO DO CISO NAS ORGANIZAÇÕES

Nem todas as organizações têm o cargo de CISO, mas a aposta na cibersegurança é necessária. A segurança da informação não deve ficar a cargo exclusivamente do CIO ou do IT manager.

RUI DAMIÃO

DESDE A CRIAÇÃO da posição de Chief Information Security Officer (CISO) dentro das organizações há mais de uma década que o cargo fica situado algures entre a equipa de IT e o *board*.

Com a crescente importância da cibersegurança, é normal que se discuta qual é a posição do CISO dentro da organização. As empresas são cada vez mais digitais, têm uma superfície de ataque cada vez maior e as ameaças são, também elas, cada vez maiores e mais impactantes para o negócio.

Enquanto o papel do CISO pode não ter sofrido uma grande mudança nos últimos anos, a perceção da sua importância dentro das organizações e para o negócio mudou. Entre as grandes empresas, já são poucas as que não contam com alguém dedicado para a segurança da informação da organização.

As empresas têm vindo a digitalizar os seus ativos e, com essa digitalização, a importância de os proteger torna-se cada vez mais importante. Depois, as notícias de grandes empresas – algumas tecnológicas – que foram vítimas de ataques cibernéticos e que viram a sua informação exposta na web aumenta a necessidade interna de proteger os seus sistemas – até para que o nome da sua empresa não figure entre a lista de organizações que sofreu uma fuga de dados massiva.

NA LUZ DA RIBALTA

O relatório "The Future Of The CISO" da Forrester Research indica que o cargo do CISO "evoluiu de um líder de equipa ignorado e subestimado e passou a tornar-se, em muitos casos, um membro vital e envolvido da equipa executiva".

A atenção dada pelas organizações coloca o CISO cada vez mais no centro das atenções não só dos investidores, mas também dos clientes. Por outro lado, esta atenção repentina e a falta de entendimento do que é a segurança pode diminuir o papel do CISO, tornando o profissional "mais num artista do que num líder", refere a Forrester Research.
Este tipo de CISO é um "executivo de segurança simbólico" que é cha-

mado para “discutir segurança, ética e privacidade quando é conveniente”, mas internamente ainda “enfrenta obstáculos” e a “falta de adesão das partes interessadas”.

Quando assim é, o CISO “concentra-se na promoção da cibersegurança como um tópico moderno, interna e externamente”, mas “não lidera a transformação da segurança”, não protege a organização, nem defende a marca.

BODE EXPIATÓRIO

No entanto, ser a cara da segurança de uma organização nem sempre é positivo; em caso de uma fuga de informação ou de uma violação de segurança, também é automaticamente o culpado.
A cibersegurança a nível corporativo é uma iniciativa de várias partes interessadas, mas, ao tornar-se o rosto da cibersegurança para uma empresa, faz com que o CISO seja automaticamente o bode expiatório, danificando a reputação do profissional e do papel dos CISO como um todo.

FUTURO DO CARGO

Para além destes dois tipos de CISO, a Forrester Research refere outros tipos de líderes de segurança dentro das organizações.

Um deles é o CISO que já não tem contacto diário com a sua equipa e que já não sabe exatamente o que é que as suas equipas precisam para atingir o sucesso e os objetivos propostos.

Um outro tipo de CISO é aquele que no papel é, de facto, o CISO, mas quem manda é outro líder mais poderoso dentro da organização. Por norma, esta situação acontece com executivos que adotam o papel pela primeira vez; que ganham o título, mas não a autoridade dentro da empresa.

Se os líderes de segurança permitirem que estas e outras situações aconteçam, ignorando o que efetivamente está em jogo ao mesmo tempo que fazem más escolhas ou falsas promessas que não correspondem à sua autoridade real dentro da organização, o CISO estará condenado ao fracasso.

Por outro lado, os líderes de segurança devem apostar naquilo para o qual foram contratados e defender a informação da sua empresa. Dentro das organizações, o CISO pode – e deve – informar quais as decisões para a organização em termos de segurança, em que atividades externas deve estar envolvido e qual a autoridade esperada e exigida internamente para fazer promessas externas. ■

INSIDER THREATS: A AMEAÇA CRESCENTE PARA TODAS AS ORGANIZAÇÕES

As Insider Threats são um risco de segurança que tem a sua origem dentro de uma organização, mais concretamente através de colaboradores, ex-colaboradores, subcontratados, consultores ou parceiros de negócio.

SÃO RECURSOS que dispõem de acesso a informação confidencial e a sistemas de informação críticos e que, de forma intencional ou acidental, colocam em risco essa informação e a reputação da sua organização. Com regularidade, informação de cariz confidencial acaba nas mãos de concorrentes, ou são divulgadas para o domínio público (*data breaches*), com graves implicações em contexto do RGPD ou do segredo de negócio. De acordo com o Data Breach Investigations Report da Verizon, 34% dos *data breaches* identificados em 2019 envolveram atores internos.

Mas como detetar comportamentos que indiciem práticas que possam lesar a sua organização, no meio de centenas ou milhares de pessoas que interagem diariamente, de forma benigna, com estes sistemas?

Fotografia: arlington-research-unsplash

Os comportamentos humanos são os principais indicadores de possíveis ameaças internas. Existem alguns comportamentos comuns que sugerem a sua presença dos quais se destacam apenas alguns: *download* ou acesso a quantidades substanciais de dados, acesso (ou tentativa de acesso) a dados confidenciais não associados à sua função de trabalho ou a dados que estão fora do seu perfil comportamental exclusivo, utilização de dispositivos de armazenamento não autorizados (por exemplo, unidades USB), cópia de arquivos de pastas confidenciais, envio de dados confidenciais por e-mail para fora da organização ou até acesso aos sistemas de informação em horários não habituais para aquele utilizador.

No entanto, é importante frisar que nem sempre estas ameaças acontecem de forma intencional e muitas vezes os colaboradores são apenas peões de um atacante externo. Um colaborador pode ser vítima de um ataque e ver os seus dispositivos ou as suas contas de acesso comprometidas por um atacante, que as utiliza para levar a cabo o roubo de informação ou o comprometimento de dados. Exemplos disto são a abertura de documentos Word com macros maliciosas, o comprometimento de credenciais através de ataques de phishing ou a execução de um ransomware. Por último, temos ainda os utilizadores que, por engano, partilham um documento confidencial por correio eletrónico com um (ou vários) destinatário errado.

PRÁTICAS RECOMENDADAS

Para se proteger face a este tipo de ameaças, é essencial que o foco da organização esteja na proteção dos ativos críticos, no reforço das políticas de segurança e na promoção de uma cultura de segurança na sua organização. A isto deve associar-se uma total visibilidade, através da monitorização contínua de toda a atividade dos seus colaboradores e dos dispositivos que acedem à informação e da correlação de eventos através de múltiplas fontes de informação.

Como se tratam de ameaças internas, não é possível confiar nas medidas tradicionais de segurança para proteger a sua empresa. Um sistema eficaz de deteção de insider threats combina várias ferramentas para monitorizar o comportamento interno, filtrar o grande número de alertas e eliminar falsos positivos. As ferramentas de UBA (*User Behavior Analytics*) e a análise de ameaças (*Threat Hunting*) ajudam a detetar possíveis ameaças internas, alertando as equipas quando um utilizador se comporta de forma suspeita ou fora do seu comportamento típico. Por último, a análise forense digital é a forma mais eficaz de confirmar a presença de uma insider threat. Estes processos e tecnologias, aliadas a um plano de resposta a incidentes eficaz são a chave para a deteção e contenção destas situações. Só assim as organizações conseguirão efetuar uma análise eficiente e agir atempadamente. ■

CIONET

Em parceria com a CIONET Portugal

POR MIGUEL PIRES MARINHO E PAULO,
Global Digital Enablement IT Lead, Siemens

REALIDADE MISTA (XR), ONDE ESTAMOS EM 2020?

A REALIDADE AUMENTADA (AR) a par da virtual encontra-se num processo de crescimento. De acordo com a PricewaterhouseCoopers (PWC) é esperado que em 2030 a capitalização de mercado para estas tecnologias ascenda aos 1,5 triliões de dólares impactando assim cerca de 23 milhões de empregos. O grande crescimento será na área de realidade aumentada cuja capitalização de mercado prevista é de 67,9 biliões de dólares já em 2020, com especial incidência no mercado americano e japonês. Desta forma, quais serão as tendências tecnológicas para esta área e em quais podemos esperar este crescimento?

Indústria: Sabemos hoje que ainda teremos de esperar até provavelmente 2023, para termos os novos aparelhos num formato que permita a adoção em massa dos consumidores finais. As grandes marcas têm vindo a partilhar, umas vezes mais, outras menos, a sua previsão para lançarem os seus próprios aparelhos nesta altura.

Hardware: Os nossos fiéis telemóveis poderão contar com processadores e sensores ainda mais potentes capazes de incorporar novas funcionalidades, tornando-se assim o aparelho de eleição para a maioria dos casos de uso em AR. Teremos também opções mais leves e apelativas, especialmente no setor da moda com a inclusão de "mini-computadores" nos óculos tradicionais permitindo numa primeira fase atingir a chamada realidade assistida com sobreposição de informação no nosso campo de visão. Faça-se a ressalva que o preço e o entendimento do público em geral, poderão influenciar o desenvolvimento deste conceito. Com os desenvolvimentos tecnológicos feitos nas áreas da ótica e fotónica, será de esperar um decréscimo do preço de produção, um aumento do campo de visão e uma diminuição da espessura das lentes em aparelhos com menor qualidade. Na vertente empresarial, à semelhança de 2019, será expectável a entrada de mais empresas à procura de configurar os aparelhos já existentes à sua realidade. Para finalizar, um

- Miguel Pires Marinho e Paulo -
Responsável Global da Siemens para Realidade Aumentada e Virtual

dos cenários que causará mais impacto para os consumidores e para os eventos será a massificação dos espetáculos holográficos.

Plataformas e infraestrutura: Já com alguns standards de desenvolvimento como WebAR, teremos vários programadores em busca de novas formas de captar a atenção de mais utilizadores e com maior facilidade. Para o atingir, com novas formas de criação de conteúdo e manipulação de objetos digitais, podemos esperar uma interação direta através do nosso browser e bastante enfâse na criação deste tipo de experiências. Pensando no enorme crescimento dos filtros de AR, já existentes em aplicações como Facebook e TikTok, assistiremos à promoção da interação com o mundo exterior, através de outras partes do nosso corpo – as mãos, além do tradicional rosto - abrindo assim portas para experiências mais imersivas. Uma tendência em crescendo continuará a ser o 5G, que terá em plataformas como AR cloud uma oportunidade de demonstrar o seu potencial, permitindo executar modelos bastante complexos e "pesados" diretamente da cloud, algo que poderá servir de motor para as operadoras de telecomunicações mais vanguardistas que o queiram promover.

Mercado de Consumo: Com toda esta tecnologia já disponível, será de esperar um investimento crescente em marketing e publicidade por parte de agências e no mercado de retalho. Será expectável também um aumento de consumo feito com recurso a experiências de AR que permitem ao consumidor experimentar o produto com maior eficácia para seguidamente efetuarem a sua compra. Estes cenários poderão ser aplicados a roupa, jóias, óculos, etc.. Outro setor em expansão, é o da navegação em 3D, com vários fabricantes de automóveis a incorporarem AR no vidro dianteiro do carro em detrimento de painéis no centro da viatura. A par da versão 3D do Google Maps teremos todo um outro conjunto de aplicações e grandes marcas à procura de encontrar formas de capitalizar neste mercado, nomeadamente na navegação indoor. Alguns destes cenários permitirão ao consumidor encontrar locais dentro de aeroportos, centros comerciais e até parques de estacionamento.

Dentro das empresas: Para as empresas, continuaremos a apurar a fase de prova de conceito, aumentando os casos de estudo feitos pontualmente, com vista a maximizar o retorno do investimento feito. Apesar de retornos bastante significativos em diversas indústrias, os desafios recaem na possibilidade de escalar este tipo de soluções, bem como no processo de integração, na segurança e na vontade interna para se adaptarem a esta tecnologia. Os que conseguirem reunir todos estes critérios estarão certamente posicionados para recolher os inúmeros benefícios explicados no início deste artigo.

Em suma, 2020 não deverá ser o ano em que a realidade aumentada e virtual fica *mainstream*, mas deverá certamente continuar num crescimento exponencial e sustentado. Teremos igualmente a possibilidade de medir o pulso a este sector com a vinda para Lisboa, pela primeira vez, do European Summit da VRARA - uma das maiores associações mundiais de realidade aumentada e virtual - que será realizado nos dias 1 e 2 de junho no LX Factory e que deverá contar com cerca de 500 empresas participantes. ■

– UM NOVO MUNDO ELÉTRICO –

As respostas aos desafios ambientais, a descarbonização das fontes energéticas e o aumento da eficiência na sua utilização encontram a sua resposta na inovação tecnológica.
As empresas de base europeia lideram mundialmente em muitos destes setores energéticos, da produção renovável à distribuição e a sua utilização de forma mais racional e eficiente.
Um dos exemplos na liderança da inovação energética é a francesa Schneider Electric. Falamos com o seu recém nomeado vice-presidente Pankaj Sharma sobre os desafios do crescimento sustentável.

JORGE BENTO

SEPARAR o crescimento económico do crescimento do consumo energético (*energy decoupling*) está a ser conseguido no velho continente há várias décadas, primeiro por uma alteração dos modelos económicos de produção, e, na última década, por uma otimização do consumo, ou eficiência energética.
Dito de outra forma, nos últimos 30 anos a Europa cresceu a um ritmo médio de 1,7% ao ano independentemente do consumo energético e na última década com uma ligeira redução nominal da energia consumida.
Mas diminuir a intensidade energética é manifestamente insuficiente; é preciso diminuir significativamente o próprio consumo nominal sem afetar a economia.

Do ponto de vista mais holístico, como situa a sua empresa no atual desafio das metas ambientais?

Pankaj Sharma — A missão da Schneider é ajudar a construir um novo mundo elétrico.
A descarbonização das indústrias é fundamental para um planeta sustentável. A questão é como o fazer.
Do nosso ponto de vista, isto passa por migrar do consumo de carvão e petróleo para formas diretas de produção de eletricidade e simultaneamente digitalizar as indústrias, porque digitalização significa eficiência.

Esta é a missão da Schneider Electric: tornar o mundo mais sustentável.

- Pankaj Sharma -
Executive Vice president
da divisão Secure Power
Schneider Electric

Se virmos do lado mais prático da divisão Schneider Power Secure, onde temos a maioria da atividade no data center, dos gigantes, passando pelo edge até aos micros [data centers] e ao IT distribuído, o nosso foco é na eficiência.

No caso da eficiência da infraestrutura, com as nossas soluções conseguimos baixar o seu PUE (*Power Usage Effectiveness*), que tipicamente estava entre 1.8 e 1.9, até 1.17 e isto traduz-se numa redução do consumo energético através da eficiência.

Já no lado do digital, o que estamos a desenvolver são aplicações de software e produtos conectados, o que se traduz em mais informação sobre a utilização da energia, o que significa que o utilizador pode tomar decisões melhores, o que resulta também numa maior eficiência.

O edge computing, alavacado também pelo IoT, é uma das grandes tendências no IT. Quais são os desafios específicos ?

O edge pode ser uma grande fonte de desperdício de energia, porque ao contrário do data center central, que é concebido de raiz para ser energeticamente mais eficiente, no Edge, quando uma empresa tem centenas de locais onde precisa de ter capacidade de computação, estes locais normalmente não foram pensados do ponto de vista da eficiência energética.

Por isso e do ponto de vista da missão para um novo mundo elétrico, queremos ter a eficiência *by design*, para que quando se multiplica este modelo para centenas de localizações seja possível garantir a melhor eficiência possível, independentemente das condições ambientais de cada local.

A segunda grande vantagem da nossa tecnologia edge é que todas as nossas soluções são do tipo *Plug & Play*. Exemplo disto são os micro data centers, mesmo os pequenos de 6U, que são fáceis de implementar e têm a eficiência energética garantida.

Como se gere com eficiência essa dispersão no IT?

Para o Edge, a Schneider Electric tem como resposta o EcoStruxure IT, que é a visão centralizada da totalidade do edge computing. Com uma única visualização, o gestor pode intervir, por exemplo, quando um local está subaproveitado, ao descolar para lá *workloads* de computação de outros sites sobreocupados, e isso é importante para aumentar a eficiência geral.

Isto permite aos nossos clientes terem uma visão geral dos ativos, bem como acompanhar o ciclo de vida dos mesmos.

O edge e IoT vão aumentar exponencialmente a quantidade de dados gerados. A Gartner prevê que 75% dos dados estarão no edge em 2025, e todas estas soluções de data center descentralizado necessitam de incorporar uma melhor eficiência energética. ■

Fontes:
European Environment Agency
Eusostat

- THE FUTURE OF ROBOTICS -

03 - 03 - 2020

Lisboa

O Nova Tech Club traz o N3E Robotics, o clube do Instituto Superior Técnico, que fará uma palestra sobre a tecnologia avançada, mostrando onde estamos e o que está prestes a chegar. Os projetos estarão do N3E Robotics estarão disponíveis para os participantes testarem durante o evento.

- IDC MULTICLOUD CONFERENCE -

12 - 03 - 2020

Lisboa

As empresas têm vindo a abraçar a transformação digital e as iniciativas associadas à cloud, sempre com um objetivo comum: o aumento da eficiência, quer no que diz respeito ao IT, quer também aos processos, assegurando-se ainda que estes se encontram em comunhão com as inovações do negócio.

- NDC PORTO -

21 a 24 - 04 - 2020

Porto

O NDC Porto é um evento de quatro dias que vai ser dedicado a vários temas, como .NET, IA, big data, cloud, DevOps, Machine Learning, e UX, entre muitos outros. No total, terá 60 oradores, 62 palestras, irá abordar 29 tecnologias e conta com sete workshops. O evento terá lugar na Alfândega do Porto.

- POWER BI PORTUGAL DAY -

30 - 04 - 2020

Lisboa

O Power BI Portugal Day vai concentrar-se na tecnologia mais emergente e de ponta em Data, Analytics e Data Science, reunindo empresas de tecnologia, empresas líderes e os cérebros mais brilhantes de todo o mundo. O evento terá lugar na reitoria da Universidade Nova de Lisboa, em Campolide.

- Miolo conta com vários clássicos portugueses -

ABRIU EM LISBOA um novo espaço com apenas 15 metros quadrados que conta com uma série de sandes criativas, assim como alguns clássicos portugueses. No menu é possível encontrar sandes de bochecha de porco, estufada a baixa temperatura com vinho do Porto, ou a sandes aberta de salmão fumado com queijo creme, espinafres, rabanete, ou, ainda, a sandes de vegetais do Miolo. Um dos grandes destaques é o hambúrguer vegan que combina maionese de abacate com cebola roxa, tomate, agrião e lascas de parmesão. O espaço conta, também, com bolos caseiros que mudam todos os dias, pão de banana com lascas de amêndoa, chás frios, sumos e limonadas.

- 1905 Zino's Palace é o novo hotel da Madeira -

LOCALIZADO NA PONTA DO SOL, a cerca de 22 quilómetros do Funchal, é possível encontrar o 1905 Zino's Palace. Inaugurado durante a semana do dia dos namorados, este edifício é um dos poucos imóveis de estilo romântico na Madeira, sendo um importante exemplar do património arquitetónico do Arquipélago. O Palacete e a capela anexa foram construídos no final do século XIX com a finalidade de serem usados como casa de verão da família Zino. Mais tarde o palacete chegou a ser utilizado pelo estado como Escola Prática Elementar de Agricultura da Madeira e como Escola Primária.

- Stomp em exibição em Lisboa e no Porto -

LISBOA E PORTO vão receber várias exibições do espetáculo internacional *Stomp*. Em Lisboa, o Teatro Tivoli BBVA recebe diariamente, com exceção de segunda e terça, o espetáculo entre os dias 4 e 29 de março. Já o Porto, no Coliseu Porto Ageas, recebe Stomp entre os dias 2 e 4 de abril. Mestres da percussão e humor, para os Stomp tudo tem um movimento e som próprios. Das botas aos baldes, das tampas dos caixotes de lixo aos isqueiros e vassouras, dos lava-loiça aos garrafões de água, a sua originalidade é incrível e o humor contagiante.

O Banco Central da Suécia (Riksbank) está preocupado com o desaparecimento da moeda física, que neste país nórdico está já em total desuso, substituindo-a por uma app privada denominada de Swish Payments. As previsões apontam que em 2022 a maioria dos comerciantes não aceitarão pagamentos em numerário. De forma a manter o dinheiro em circulação como um meio de pagamento em mãos públicas, e dado o pouco interesse dos cidadãos em usarem porta-moedas, o banco central iniciou o processo de investigação tecnológica para a criação de uma moeda virtual nacional, o E-Krona, baseado em blockchian, mas distinto das regras das habituais criptomoedas, uma vez que será uma moeda digital soberana e em paridade com a Coroa Sueca. Não existe ainda uma decisão final do Riksbank sobre a data para o eventual lançamento do E-Krona.

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
COPYDESK: Lara Fonseca
GESTÃO DE PARCEIROS:
João Calvão - joao.calvao@medianext.pt
Rita Castro - rita.castro@medianext.pt
ARTE E PAGINAÇÃO: Teresa Rodrigues
FOTOGRAFIA: Jorge Correia Luís, Rui Santos Jorge
WEB: João Bernardes

DESENVOLVIMENTO WEB: Global Pixel
COLABORARAM NESTE NÚMERO: Miguel Pires Marinho e Paulo
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