bilingual edition

# ptsoc{news}

11

Jovens no cibercrime

3 perguntas a Kristof Tuyteleers

Garantir a Resilência Empresarial através da Continuidade de Negócio
por Bruno Morais

Young people in cybercrime

3 questions to Kristof Tuyteleers

Ensuring Business Resilience through Business Continuity
by Bruno Morais

.pt

## Jovens no cibercrime

Há um crescimento do número de jovens a aderir à cibercriminalidade? Não se sabe. Em Portugal, segundo a Polícia Judiciária (PJ), "tem-se observado um crescimento do número de casos de ataques informáticos a in-fraestruturas críticas realizados por jovens adolescentes, não tendo estes sequer noção do impacto dos seus ataques, nem de como estes crimes poderão impactar o seu futuro", por ficarem com registo criminal enquanto ainda são menores.

A declaração foi efetuada em junho passado, na primeira conferência da InterCOP, rede de polícias fundada pela Poliisi (Finlândia) e que tem como parceiros de Portugal a Polícia de Segurança Pública (PSP) e a PJ.

No final de novembro, a segunda conferência da rede internacional acentuou "a tendência crescente de atividade criminosa no cibe-respaço por parte de jovens adolescentes".

A InterCOP, através de campanhas de comu-nicação, pretende desincentivar os jovens de cometerem ações criminosas e informar sobre opções legais alternativas, como o "ethical hacking". Mas alertar para a ilicitude destas ações junto de jovens com elevadas capacidades técnicas e muitos deles já ins-talados em redes internacionais do cibercri-me, terá alguma eficácia?

## Young people in cybercrime

Is there a growing number of young people taking part in cybercrime? We do not know. In Portugal, according to the Polícia Judiciária (PJ) [Portuguese Criminal Police], 'there has been an increase in the number of cases of computer attacks on critical infrastructures carried out by young teenagers, who are not aware of the impact of their attacks or how these crimes could impact their future,' as they will have a criminal record while still minors.

The statement was made last June at the first InterCOP conference, a police network founded by Poliisi (Finland), whose Portuguese partners are the Polícia de Segurança Pública (PSP, Public Security Police) and the PJ.

At the end of November, the second conference of the international network emphasised 'the growing trend of criminal activity in cyberspace by young teenagers.'

Through communication campaigns, InterCOP aims to discourage young people from committing criminal offences and to inform them about alternative legal options, such as ethical hacking. But will it be effective to alert young people with high technical skills, many of whom have already established themselves in international cybercrime networks, to the illegality of these actions?

**O interesse dos jovens pelo hacking ilegal**

Há uma variedade de fatores que captam o interesse dos jovens pelo hacking criminoso, nomeadamente culturais, educativos, tecnológicos ou sociais. O fator geracional não é também de desprezar porque muitos dos jovens hackers têm pais que viveram a primeira geração da informática pessoal, com acesso mais generalizado a computadores para fins profissionais ou lúdicos, na década de 1980.

Um alargado conjunto de filmes - como Tron e WarGames (1982 e 1983, respetivamente) - ajudaram a cimentar esse fascínio e a estimular uma mentalidade de exploração e curiosidade sobre a tecnologia, assim como um inegável interesse pela cibersegurança e os desafios do acesso não autorizado a sistemas informáticos.

"Um hacker é muitas vezes retratado como alguém que, usando um pseudónimo, invade sistemas de computador" de forma ilegal, escreve-se em "The Wachowskis and the hacker as a progressive archetype". Na realidade, a definição de hacker é mais alargada, especificando também quem o faz de forma legal e ajuda a aperfeiçoar programas de software ou sistemas informáticos, redes de telecomunicações e outros em geral, misturando-as com valores da contracultura dos anos de 1960 nos EUA como "a desconfiança no Estado, a salvaguarda da privacidade pessoal, a defesa da liberdade de expressão e a oposição ao capitalismo predatório".

**Young people's interest in illegal hacking**

There is a variety of factors that capture young people's interest when it comes to criminal hacking, including cultural, educational, technological and social factors. The generational factor should also not be overlooked, as many young hackers have parents who lived through the first generation of personal computing, with a more widespread access to computers for professional or recreational purposes in the 1980s

A wide range of films - such as Tron and WarGames (1982 and 1983, respectively) - helped cement this fascination and stimulate a mindset of exploration and curiosity about technology, as well as an undeniable interest in cybersecurity and the challenges of unauthorised access to computer systems.

'A hacker is nearly always depicted as a person who, using an alias, breaks into computer systems' illegally, on can read on "The Wachowskis and the hacker as a progressive archetype". In reality, the definition of a hacker is broader, also encompassing those who do it legally and help improve software programmes or computer systems, telecommunications networks and others in general, mixed with values of the 1960s American counterculture, such as 'distrust of the (deep) State, safeguarding personal privacy, free speech advocacy and an opposition to predatory capitalism.'


My Other Computer (CC)

Atualmente, esses valores são pouco reconhecidos ou assumidos pelos jovens que procuram menos os desafios intelectuais ou o reconhecimento dentro de comunidades online – tanto ligadas aos computadores como aos smartphones – para optarem por um retorno mais financeiro. Essa mudança deve-se também à maior facilidade em obter ferramentas de automatização de ataques.

A estratégia não é nova. Os chamados "script kiddies" usavam técnicas e ferramentas de exploração ("scripts") para perpetrar ataques quando tinham reduzidos conhecimentos técnicos. Agora, o cibercrime avança com a aquisição de software malicioso dedicado a tarefas específicas (Crime-as-a-Service ou

Nowadays, these values are hardly recognised or taken on board by young people who are looking less for intellectual challenges or recognition within online communities - whether linked to computers or smartphones - in favour of a more financial return. This change is also due to the greater ease with which attack automation tools can be obtained.

The strategy is not new. So-called 'script kiddies' used exploitation techniques and tools (scripts) to perpetrate attacks when they had little technical knowledge. Now, cybercrime is advancing with the acquisition of malicious software dedicated to specific tasks (Crime-as-a-Service or CaaS), on Dark

CaaS), em mercados na Dark Web ou fóruns de cibercrime.

Com a proliferação online de livros e cursos, fóruns e comunidades dedicadas à partilha de conhecimento, muitos jovens têm acesso a informações sobre vulnerabilidades informáticas ou de comunicações.

Em resumo, o interesse dos jovens pelo hacking pode passar pelo desafio e curiosidade técnica de como superar sistemas de segurança, participação e integração em comunidade, por motivações políticas ou sociais (hacktivismo), ou por recompensa financeira, normalmente associada a um desconhecimento das consequências e implicações legais, com implicações severas no futuro profissional desses jovens.

**Problemas antigos e efeitos da COVID-19**

Há uma agilização no incremento de ataques usando ferramentas de CaaS, mas o aproveitamento das falhas nas organizações também ocorre pelo laxismo de algumas delas.

Nos EUA, uma análise feita pelo Department of Homeland Security (DHS) detetou que grupos de adolescentes conseguiram explorar falhas de segurança das operadoras de telecomunicações e da cadeia de abastecimento de algumas empresas. Por exemplo, a CVE-2018-13379 é uma falha de segurança crítica descoberta há quatro anos e foi a vulnerabilidade mais explorada em 2022, de-

Web marketplaces or cybercrime forums.

With the proliferation of online books and courses, forums and communities dedicated to sharing knowledge, many young people have access to information about computer or communications vulnerabilities.

In short, young people's interest in hacking can be fuelled by the challenge and technical curiosity of how to overcome security systems, participation and integration in the community, political or social motivations (hacktivism), or financial reward, usually associated with a lack of knowledge of the consequences and legal implications, with severe implications for their professional future.

**Old problems and the effects of COVID-19**

There is an obvious increase in the number of attacks using CaaS tools, but the exploitation of organisations' flaws also happens due to the laxity of some of them.

In the US, an analysis by the Department of Homeland Security (DHS) found that groups of teenagers had managed to exploit security flaws in telecoms operators and the supply chain of some companies. For example, CVE-2018-13379 is a critical security flaw discovered four years ago; it was the most exploited vulnerability in 2022, showing how many organisations do not update their software and remain vulnerable to old

monstrando como muitas organizações não atualizam o seu software e continuam vulneráveis a problemas antigos. Outro exemplo é a Shellshock, surgida em 2014, mas que ainda não desapareceu do radar dos atacantes (e dos atacados).

A par dos pedidos para os reguladores norte-americanos penalizarem as organizações com práticas de segurança pouco rigorosas, o Congresso devia considerar o financiamento de programas para afastar os jovens do cibercrime, defende a National Cyber and Workforce Education Strategy.

A aparente descoberta do cibercrime por um crescente número de jovens também ocorre pelos efeitos provocados pela COVID-19. O teletrabalho e as comunicações à distância (para estudar, fazer compras ou aceder a entretenimento, muito dele ilegal) agilizaram a entrada de equipamentos informáticos nos lares. No primeiro semestre de 2020, a venda de smartphones diminuiu globalmente 20%, enquanto a informática cresceu 11,2% no segundo trimestre, segundo a consultora Gartner. O comércio eletrónico aumentou, trazendo potenciais problemas de insegurança a utilizadores pouco conhecedores das alternativas digitais ao dinheiro físico.

No Reino Unido, o total de registos oficiais dos cibercrimes e de fraudes aumentou mas não foi homogéneo e "muitos dos picos de cibercrime e fraude identificados no início da pandemia parecem ter regressado mais

problems. Another example is Shellshock, which appeared in 2014 and has yet to disappear from the radar of attackers (and those attacked).

Alongside calls for US regulators to penalise organisations with lax security practices, the US Congress should consider funding programmes to steer young people away from cybercrime, argues the National Cyber and Workforce Education Strategy.

The apparent discovery of cybercrime by a growing number of young people is also due to the effects of COVID-19. Working from home and the use of remote communications (to study, shop or access entertainment, much of it illegal) have accelerated the entry of IT equipment into homes. According to Gartner Consulting, in the first half of 2020, smartphone sales fell by 20 % overall, while IT grew by 11.2 % in the second quarter. E-commerce has increased, bringing potential insecurity problems for users who are unfamiliar with digital alternatives to physical cash.

In the UK, the total number of official records of cybercrime and fraud increased but was not homogeneous and 'many spikes in cybercrime and fraud identified at the beginning of the pandemic appear to have later dropped back to the longer-term gentler upward trend,' notes the study 'Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19.'

tarde a uma tendência ascendente mais suave a longo prazo", nota o estudo "Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19".

Em março de 2020, a Europol alertou que os cibercriminosos estavam a beneficiar da pandemia e do confinamento. Em agosto, a Interpol notou "um aumento acentuado das atividades cibercriminosas" para, em outubro seguinte, a Europol confirmar que "a COVID-19 causou uma amplificação dos problemas [de cibercriminalidade] existentes" e que tinha aumentado a fraude contra as empresas.

No estudo "Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry", "o FBI declarou que o número de queixas de cibercrime entre janeiro e o final de maio de 2020 foi quase o mesmo que em todo o ano de 2019". Mas, no final do ano, a agência registou 791 790 casos de cibercrimes - mais do dobro dos 300 mil de 2019.

Acompanhando as condições propícias para esta criminalidade, juntou-se a sua evolução para um negócio internacional organizado e publicitado como bastante rentável e de risco mínimo. No final de novembro, por exemplo, uma notícia reportava como o grupo Black Basta teria arrecadado mais de 100 milhões de dólares num único mercado de criptomoeda após ter atacado mais de 90 organizações ao longo de dois anos de atividades de ransomware.

In March 2020, Europol warned that cybercriminals were benefiting from the pandemic and from lockdown. In August, Interpol noted 'a marked increase in cybercriminal activity'; the following October, Europol confirmed that 'COVID-19 caused an amplification of existing [cybercrime] problems' and that fraud against companies had increased.

In the study Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry', 'the FBI stated that the number of cybercrime complaints between January and the end of May 2020 was almost the same as in the whole of 2019.' At the end of the year, the agency reported 791 790 cases of cybercrime - more than double the 300 000 in 2019.

Accompanying the favourable conditions for this crime has been its evolution into an organised international business that is advertised as very profitable and with minimal risk. At the end of November, for example, a news story reported how the Black Basta group had raised more than 100 million dollars on a single cryptocurrency market after having attacked more than 90 organisations over two years of ransomware activity.

**Who are the 'digital bandits'?**

This scenario suggests that only now are more young people getting involved in cybercrime. According to the 2016 'Youth

**Quem são os "bandidos digitais"?**

Este cenário aparenta que só agora mais jovens se dedicam ao cibercrime. Há realmente um maior número de cibercrimes reportados às autoridades mas o fenómeno global e intergeracional não é novo, mostrou o relatório de 2016 "Youth Pathways into Cybercrime".

Wang Zhengyang tinha 13 anos em 2014 quando pirateou o sistema informático da sua escola para aceder às respostas dos seus trabalhos de casa. No ano seguinte, cinco jovens com idades entre os 15 e os 20 anos foram detidos no âmbito de uma investigação ao roubo de dados dos clientes de uma operadora de telecomunicações no Reino Unido. O Information Commissioner's Office multou a empresa e "afirmou que a segurança era tão deficiente que, dada a idade dos detidos, o ataque foi bem-sucedido 'de forma tão fácil'". Nos EUA, num caso mais recente, Joseph Garrison então com 19 anos declarou-se culpado de um ataque de preenchimento de credenciais ("credential stuffing") num site de apostas.

Dois jovens autistas de 17 e 18 anos foram condenados no Reino Unido pelos ataques cometidos pelo Lapsus$, um grupo internacional de cibercrime que visou diversas organizações entre 2021 e 2022. O tribunal apelidou-os de "bandidos digitais".

O Lapsus$ reclamou a autoria de ataques a empresas como a Microsoft, Nvidia, Rocks-

Pathways into Cybercrime' report, there is a greater number of cybercrimes reported to the authorities, despite the global and intergenerational phenomenon not being new.

In 2014, Wang Zhengyang was 13 when he hacked into his school's computer system to access the answers to his homework. The following year, five young people aged between 15 and 20 were arrested as part of an investigation into the theft of customer data from a telecoms operator in the UK. The Information Commissioner's Office fined the company and 'said that security was so poor that, given the age of those arrested, the attack succeeded 'so easily'.' In the US, in a more recent case, Joseph Garrison, then 19, pleaded guilty to a credential stuffing attack on a gambling website.

Two autistic young men, aged 17 and 18, were convicted in the UK of attacks committed by

tar Games ou Uber e, em Portugal, Impresa e Vodafone. No âmbito da subsequente investigação ao grupo, o Cyber Safety Review Board (CSRB) do Department of Homeland Security produziu um relatório onde recomendou o financiamento de programas de prevenção do cibercrime juvenil.

O grupo também alarmou as autoridades norte-americanas. "É muito preocupante que um grupo de hackers, incluindo alguns adolescentes, tenha sido capaz de invadir de forma consistente as empresas mais bem defendidas do mundo", disse o secretário da Segurança Interna, Alejandro Mayorkas, à CNN. "Estamos a assistir a um aumento da cibercriminalidade juvenil".

No estudo "Understanding cybercrime in 'real world' policing and law enforcement" publicado no ano passado, refere-se que é provável que os hackers se iniciem quando são jovens, "com 61% a começar entre os 10 e os 15 anos e 32% entre os 16 e os 20 anos". A idade média dos suspeitos nas investigações de cibercrime no Reino Unido em 2015 foi de 17 anos.

Um potencial percurso de entrada no cibercrime inicia-se nos jogos online e nas modificações para agilizar os triunfos, evolui naturalmente para os fóruns de pirataria informática, até se estabelecer na cibercriminalidade mais grave. "A cultura do hacking coloca uma forte ênfase nas capacidades e competências que ditam a posição social

Lapsus$, an international cybercrime group that targeted several organisations between 2021 and 2022. The court labelled them 'digital bandits'.

Lapsus$ claimed authorship for the attacks on companies such as Microsoft, Nvidia, Rockstar Games or Uber and, in Portugal, Impresa and Vodafone. As part of the subsequent investigation into the group, the Department of Homeland Security's Cyber Safety Review Board (CSRB) produced a report recommending funding for youth cybercrime prevention programmes.

The group has also alarmed the US authorities. 'It is highly concerning that a loose band of hackers, including a number of teenagers, was able to consistently break into the best-defended companies in the world,' Homeland Security Secretary Alejandro Mayorkas told CNN. 'We are seeing a rise in juvenile cybercrime.'

The study 'Understanding cybercrime in 'real world' policing and law enforcement', published last year, stated that hackers are likely to start whilst they are young, 'with 61 % starting between the ages of 10 and 15 years, and another 32 % starting between 16 and 20 years old.' In 2015, the average age of suspects in UK cybercrime investigations was 17.

A potential route into cybercrime begins with online games and modifications to

no seio destas comunidades, encorajando a aquisição de conhecimentos e a procura de desafios e recompensando o sucesso com estatuto", referem os investigadores.

Na Europa, num inquérito do projeto CC-DRIVER, 69% dos jovens afirmou ter cometido pelo menos uma forma de cibercrime, entre o verão de 2020 e o de 2021. O inquérito não englobou Portugal.

"É mais provável que os homens (74%) do que as mulheres (65%) declarem ter estado envolvidos em pelo menos uma forma de cibercriminalidade", refere-se. Por espaços de risco online, 51,5% utiliza fóruns e chats; 51,2% usa fóruns de jogos online; 19% utiliza redes P2P; 11,8% está em fóruns da Dark Web; e, mais importante, 10,7% em mercados da Darknet".

**A nacional escassez de dados**

Em Portugal, os dados sobre a realidade dos cibercriminosos jovens ou adolescentes é muito escassa, como se nota pela generalização usada na InterCOP. "Para mim é difícil afirmar que se nota uma maior apetência dos mais jovens pelo cibercrime porque não tenho conhecimento de investigação que suporte a afirmação. A investigação geralmente foca-se nos jovens como vítimas do cibercrime e raramente como perpetradores", sintetiza Tito de Morais, fundador do MiudosSegurosNa.Net, projeto que há 20 anos "ajuda famílias, escolas e comunidades

speed up winning, naturally evolving into hacking forums, until it settles into more serious cybercrime. 'The culture of hacking places a strong emphasis on the skills and competences that dictate social standing within these communities, encouraging the acquisition of knowledge and the pursuit of challenges, rewarding success with status,' researchers say.

In Europe, a survey by the CC-DRIVER project showed that 69 % of young people said they had committed at least one form of cybercrime between the summer of 2020 and 2021. The survey did not include Portugal.

'Males (74 %) are more likely than females (65 %) to report having been involved in at least one form of cybercrime,' can be read in the report. By spaces where these online risks are taken, 51.5 % use forums and chats, 51.2 % use online gaming forums, 19 % use P2P networks, 11.8 % are on Dark Web forums and, most importantly, 10.7 % are on Darknet marketplaces.'

**The national lack of data**

In Portugal, data on the reality of young or teenage cybercriminals is very scarce, as can be seen from the generalisation used at InterCOP. 'It is difficult for me to say that there is a greater appetite for cybercrime among young people because I do not know of any research that supports

a promover a utilização ética, responsável e segura das tecnologias de informação e comunicação por crianças e jovens".

"A minha perceção é que há uma maior apetência dos jovens pelo cibercrime que anteriormente e um desconhecimento sobre as penas em que podem incorrer ao praticar um cibercrime", salienta Tito de Morais, considerando que "muitas vezes não têm consciência que estão a cometer um crime e por outro lado há a ideia romantizada que se conseguirem 'hackear' e entrar no sistema de uma grande empresa, podem 'ir parar a uma Big Tech' que os contrate para a equipa de cibersegurança, esquecendo que o mais provável é 'irem parar' à cadeia. E depois não têm

this claim. Research generally focuses on young people as victims of cybercrime and rarely as perpetrators,' summarises Tito de Morais, founder of MiudosSegurosNa.Net, a project that has been, for the last 20 years, 'helping families, schools and communities promote the ethical, responsible and safe use of information and communication technologies by children and young people.'

'My perception is that there is a greater appetite among young people for cybercrime than before and a lack of knowledge about the penalties they can incur by committing a cybercrime,' emphasises Tito de Morais, considering that 'they are often unaware they are committing a crime and, on the


My Other Computer (CC)

noção que uma das causas que leva as empresas a não recrutar alguém é a ligação dos candidatos a comportamentos criminosos".

Nesse sentido, algumas abordagens educativas podem oferecer cursos em cibersegurança, ética hacker e programas de mentoria para redirecionar o interesse dos jovens para atividades legais e carreiras éticas em segurança da informação. O fundador do MiudosSegurosNa.Net vai mais longe e nota que "a atividade no domínio do cibercrime, à semelhança do que acontece com muita da restante atividade criminal, começa a revelar-se na adolescência. Assim, é importante detetarem-se quais os jovens que têm apetência pela aquisição desse tipo de competências para poderem ser enquadrados e acompanhados. Uma das formas que vejo para se detetarem jovens com esse tipo de competências e apetências são competições do tipo 'capture the flag' e a criação de clubes de cibersegurança nas escolas. Por outro lado, a ética, seja ela digital ou não, deve fazer parte do currículo escolar, nomeadamente na disciplina de cidadania, mas também na de TIC".

Entre as 50 recomendações do segundo relatório intercalar da Comissão de Análise Integrada da Delinquência Juvenil e da Criminalidade Violenta, apela-se para "o uso não excessivo/uso racional do digital/tecnologias e a prevenção de comportamentos aditivos" e, entre outras já em execução, "incrementar operações regulares de 'fiscalização'

other hand, there is the romanticised idea that if they manage to hack and get into a big company's system, they can "end up" at a Big Tech company, what will hire them for their cybersecurity team, forgetting that the most likely scenario is that they will "end up" in jail. They do not realise that one of the reasons why companies do not recruit someone is because of an applicant's link to criminal behaviour.'

In this sense, some educational approaches can offer courses in cybersecurity, hacker ethics and mentoring programmes to redirect young people's interest towards legal activities and ethical careers in information security. The founder of MiudosSegurosNa.Net goes even further and notes that 'cybercrime activity, like much other criminal activity, begins to reveal itself in adolescence. If it therefore important to detect which young people have an appetite for acquiring these skills so they can be given training and monitored. One of the ways I see of detecting young people with these kinds of skills and appetites are 'capture the flag'-like competitions and the creation of cybersecurity clubs in schools. On the other hand, ethics, whether digital or not, should be part of the school curriculum, namely in the subject of citizenship, but also in ICT.'

Among the 50 recommendations included in the second interim report by the Commission for the Integrated Analysis of Juvenile Delinquency and Violent Crime, it calls for 'the

do ciberespaço por parte das entidades policiais, em particular sobre a publicitação de atos de violência ou da sua projeção futura, de modo a tornar o ciberespaço mais seguro".

No caso do Relatório Anual de Segurança Interna relativo a 2022, as preocupações com a cibercriminalidade passam pela autoprodução de conteúdos íntimos, partilha de conteúdos ilegais em plataformas sociais e a produção, partilha e alojamento de conteúdos ilegais em redes P2P – um "fenómeno perpetrado por jovens com idades compreendidas entre os 12 e os 16 anos", em que são usadas "plataformas de jogos online para aliciamento de menores à produção de conteúdos íntimos, servindo as plataformas encriptadas para troca e armazenamento de conteúdos ilegais".

No âmbito dos objetivos, prioridades e orientações da política criminal para 2023-2025, em que a cibercriminalidade é considerada crime de prevenção e de investigação prioritárias, os ciberataques a infraestruturas digitais dos Estados e a deslocação de formas de crime tradicional para o ambiente digital, entre outros, "constituem fatores que apontam no sentido da necessidade de manutenção de esforços na prevenção e na repressão do cibercrime e de formas graves de tráfico que lhe estão associadas".

Noutros países, a repressão está a ser substituída por ações mais pedagógicas, como também defende Tito de Morais. A polícia dos Países Baixos lançou o projeto Hack_Right

non-excessive use/rational use of digital/technologies and the prevention of addictive behaviours' and, among others already being implemented, 'to increase regular cyberspace "surveillance" operations by law enforcement agencies, namely on the publicity of acts of violence or their future projection, in order to make cyberspace safer.'

In the Annual Internal Security Report for 2022, cybercrime concerns include the self-production of intimate content, the sharing of illegal content on social media platforms and the production, sharing and hosting of illegal content on P2P networks - a 'phenomenon perpetrated by young people aged between 12 and 16', where 'online gaming platforms are used to entice minors to produce intimate content, using encrypted platforms to exchange and store illegal content.'

Following the objectives, priorities and guidelines of the criminal policy for 2023-2025, in which cybercrime is considered a priority crime for prevention and investigation, cyberattacks on states' digital infrastructures and the displacement of traditional forms of crime to the digital environment are, among others, 'factors that point to the need to maintain efforts to prevent and repress cybercrime and the serious forms of trafficking associated with it.'

In other countries, repression is being replaced by more pedagogical actions, as Tito de Morais also argues. Netherlands


Clark Gu, Unsplash

para jovens entre os 12 e os 23 anos, enquanto o projeto europeu liderado pela Finlândia Next Gen Hack FI vai até aos 25 anos. Outros estão a descobrir o potencial de engenheiros de som e de jogadores para conseguirem "talentos no domínio da cibersegurança".

Com a falta de profissionais na cibersegurança, a requalificação de inesperados talentos para o hacking ético, pode ser benéfica para a sociedade. Ou, como refere o docente Rogério Bravo, podem-se criar e modificar os "cursos existentes (incluindo cursos profissionais) por forma a corresponder àquilo que uns chamam 'necessidades do mercado'".

police has launched the Hack_Right project for young people aged between 12 and 23 years old, while the Next Gen Hack FI European project led by Finland goes up to the age of 25. Others are discovering the potential of sound engineers and gamers to boost the 'cybersecurity talent pool'.

With a shortage of cybersecurity professionals, the retraining of unexpected talent for ethical hacking could be beneficial to society. Or, as lecturer Rogério Bravo says, we need to create and modify 'existing courses (including vocational courses) to meet what some call 'market needs.'

## A universidade e o hacking ético

**Nota-se um maior interesse dos estudantes universitários no cibercrime e, nesse sentido, têm um maior conhecimento sobre as penalizações pela execução destas atividades ilegais?**

A Academia, ao nível das "Engenharias", começou a perceber a vantagem dos alunos aprenderem matérias complementares. As boas práticas internacionais, que faziam parte da "soft law" (análise do risco, criação de listas de "assets" a proteger, notificações de ciber-incidentes, etc.) passaram a fazer parte de diplomas legais.

Por isso, faz sentido que os profissionais da cibersegurança acompanhem diretamente a visão do impacto futuro de legislação na sua organização ou nas suas funções.

Apesar de os gabinetes jurídicos internos o poderem fazer, importa que o "pessoal técnico da área ciber" esteja alinhado com conceitos e procedimentos, para estar mais consciente de limites de atuação (principalmente no "antes" e no "depois" do ciberincidente) e das obrigações para "compliance".

Em tudo isto tem cabimento o interesse pela forma técnica como os académicos passam a "estudar" as técnicas ligadas ao cibercrime. Desta forma, conseguem perceber melhor as ferramentas, as técnicas, as táticas e os procedimentos envolvidos nessas práticas.

## University and ethical hacking

**There is a greater interest among university students when it comes to cybercrime. In this sense, do they have a greater knowledge of the penalties for carrying out these illegal activities?**

The Academia, at the 'Engineering' level, has begun to realise the advantage of students learning complementary subjects. International best practices, which used to be part of the 'soft law' (risk analysis, creation of lists of 'assets' to be protected, notification of cyber-incidents, etc.) are now part of the law.

Therefore, it makes sense for cybersecurity professionals to directly monitor the future impact the law will have on their companies or on their duties.

Although in-house legal teams can do this, it is important for 'cyber technical staff' to be aligned with concepts and procedures, to be more aware of the limits of their actions (especially 'before' and 'after' the cyber incident) and the obligations for 'compliance'.

In all of this, there is an interest in the technical way in which academics 'study' cybercrime techniques. This way, they can better understand the tools, techniques, tactics and procedures involved in these practices. The interest is obvious, but I would highlight two advantages: to understand

O interesse é óbvio, mas destaco duas vantagens: compreender a informação deixada nos sistemas pelas práticas em questão, e perceber melhor a viabilidade e operacionalidade das características técnicas anunciadas por bens e serviços de cibersegurança.

**No caso de existir esse interesse nas diferentes modalidades de cibercrime, quais são as que mais os interessam (financeiras, sexting, outras)?**

Se bem percebo, interessa que a Academia compreenda o espectro de atuação dos atacantes no espaço ciber: desde as motivações de base na personalidade, à situação internacional, até aos fatores externos ligados à estratégia geopolítica. Assim se pode perceber a atuação do atacante e eventualmente estabelecer o seu perfil.

Dentro das possíveis e múltiplas motivações do atacante (dinheiro, ideologia, coação, ego e ressentimento) encontramos as dos defensores. É natural que uns e outros 'estudem' as respetivas motivações. Uns exploram-nas, outros submetem-se e outros ainda, tentam contrariá-las.

**Como é que se pode levar esses jovens a terem um maior interesse no hacking ético, ou é uma "geração perdida"?**

Não acredito em gerações perdidas. Acredito na necessidade de a Academia, com as instituições do Governo e as Ordens, criarem e modificarem cursos existentes (incluindo

the information left behind in systems by the practices in question, and to better understand the feasibility and operability of the technical features advertised by cybersecurity goods and services.

**If there is such an interest in the different types of cybercrime, which ones interest them the most (financial, sexting, others)?**

If I understand correctly, the Academia is interested in understanding the spectrum of attackers' actions in cyberspace: from personality-based motivations to the international situation, to external factors linked to geopolitical strategy. In this way, it can understand the attacker's actions and eventually establish their profile.

Within the attacker's possible and multiple motivations (money, ideology, coercion, ego and resentment) we find those of the defenders. It is only natural for people to 'study' their motivations. Some exploit them, others submit to them and others try to counteract them.

**How can one get these young people more interested in ethical hacking, or is it a 'lost generation'?**

I do not believe in lost generations. I believe the Academia needs, together with government institutions and organisations, to create and modify existing courses (including vocational courses) in order to meet what some call 'market needs' and

cursos profissionais) por forma a corresponder àquilo que uns chamam "necessidades do mercado" e eu gosto de designar por situação internacional da realidade tecnológica.

Uma espécie de "real politik" para a área da formação profissional e das licenciaturas, que englobe os cursos de especialização.

Se a formação for desenhada de raiz para manter a curiosidade e a sensação de criar algo de útil, melhora a prestação académica (em sentido geral).

Juntam-se novos conteúdos aos modelos educacionais "clássicos" como programa nacional, por forma a que, quer no ensino privado, quer no público, se crie e estimule a criação de "talentos".

Isto proporcionaria também, a recuperação do interesse pelo estudo e relançamento de pessoas desapontadas com o sistema de ensino que abrangeu estudantes que se sentiram menos acompanhados durante a época COVID e após.

É aqui que a expressão "visão holística" me faz mais sentido: só tem compreensão genérica da situação ciber e capacidade de atuação qualitativa, quem tem conhecimento e quem tem acesso a mecanismos tecnológicos. É o resultado da experiência com a formação técnica contínua.

**Entrevista a Rogério Bravo,**
**Docente do Instituto Politécnico de Beja**

what I like to call the international situation of technological reality.

A kind of 'real politik' for the area of vocational training and degrees, including specialisation courses.

If training is designed from the ground up to keep students curious and feeling like they are creating something useful, it can improve academic performance (in a general sense).

New content is added to the 'classic' educational models as a national programme, so that both private and public education can create and stimulate the creation of 'talent'.

This would also help people regain interest in studying and reignite a passion in those who were disappointed with the education system, including students who felt less supported during the COVID times and afterwards.

This is where the expression 'holistic vision' makes the most sense to me: only those with knowledge and access to technological mechanisms have a general understanding of the cyber situation and the ability to act qualitatively. This is the result of experience with ongoing technical training.

**Interview to Rogério Bravo,**
**Professor of Polytechnic Institute of Beja**

## Utilização das TIC nas empresas nacionais

## Use of ICT in Portuguese companies

Empresas por tipo de propósito de utilização de *software* ou sistemas de Inteligência Artificial (IA), em % do total de empresas com 10 ou mais pessoas ao serviço que utilizam tecnologia(s) de IA (2023)


**Fonte:** INE, Inquérito à utilização de TIC nas empresas

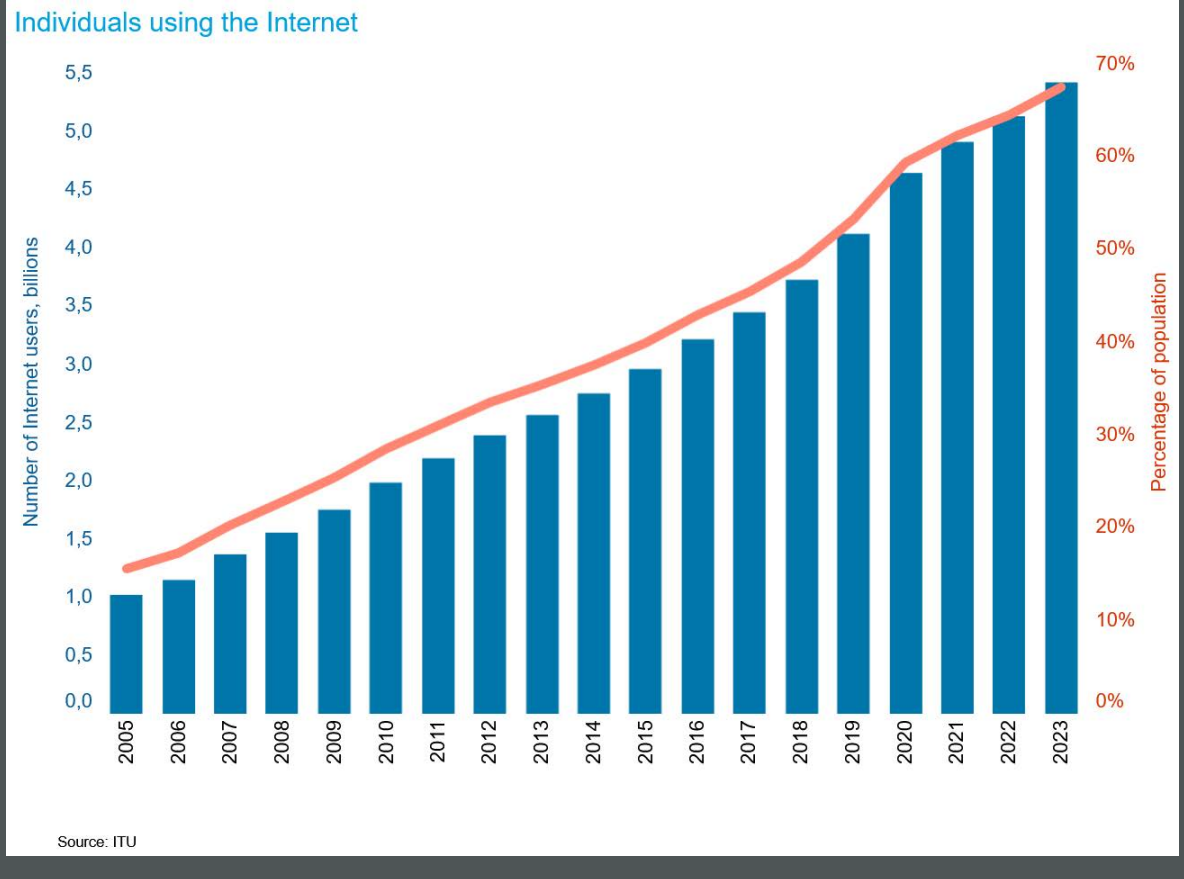
As tecnologias de Inteligência Artificial (IA) nas empresas portuguesas que as utilizam é, em mais de um terço dos casos, dedicada à segurança das tecnologias de informação e comunicação (TIC). Os dados de 2022 do INE revelam que nesse ano 7,9% das empresas utilizava tecnologias de IA, um ligeiro crescimento de 0,7 p.p. relativamente a 2021.

More than one third of Portuguese companies that use Artificial Intelligence (AI) technologies are dedicated to the security of information and communication technologies (ICT). INE's 2022 data shows that, in that year, 7.9 % of companies used AI technologies, a slight increase of 0.7 p.p. compared to 2021.

## ITU Facts and Figures 2023

Cerca de 67% da população mundial (ou 5,4 mil milhões de pessoas) está online, enquanto o número de pessoas offline em 2023 diminuiu para cerca de 2,6 mil milhões de pessoas (33%). O uso da Internet continua ligado ao desenvolvimento de um país. 93% das pessoas dos países com rendimentos elevados utilizavam a Internet em 2023.

Close to 67 % of the world's population (or 5.4 billion people) is online, while the number of people offline in 2023 has decreased to close to 2.6 billion people (33 %). The use of the Internet continues to be linked to a country's development. In 2023, 93 % of people in high-income countries used the Internet.



3

**Kristof Tuyteleers**

**Chair do European TLD ISAC Working Group; CISO, DNS Belgium**
Chair of the European TLD ISAC Working Group; CISO, DNS Belgium

## 1. Quais os principais objetivos do ISAC para os TLD europeus?

O objetivo do European Top Level Domain Information Sharing and Analysis Centre é ser o centro de especialização em cibersegurança para o sistema de nomes de domínio (DNS) em geral e para os operadores de registo de TLD europeus em particular. Pretende servir de ponto de contacto especializado para os decisores políticos relativamente ao ecossistema de DNS e à ciber-resiliência conexa. Além disso, pretende também desempenhar esse papel em iniciativas internacionais focadas na melhoria do intercâmbio de informações e da colaboração intersectorial e inter-ISAC.

Para os seus membros, o TLD ISAC foca-se na partilha atempada de informações de segurança, na análise de ameaças e vulnerabilidades relevantes e em ser uma fonte competente de melhores práticas, normas, métodos e "know-how" relacionados com o DNS.

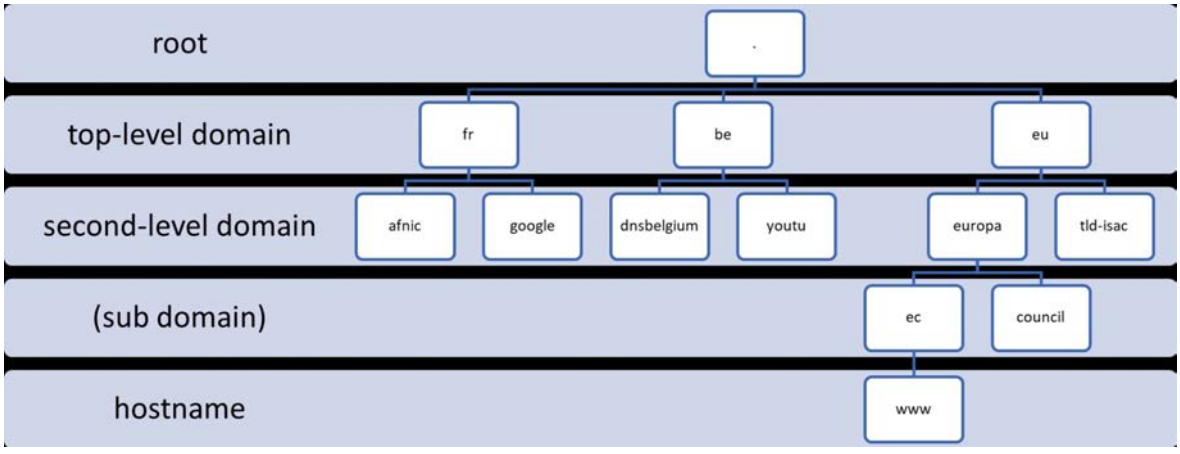
## 1. What are ISAC's main objectives for european TLDs?

The European TLD ISAC's aim is to be the cybersecurity center of expertise for the domain name system (DNS) in general and the European TLD registry operators in particular. It wants to serve as an expert point of contact for policymakers concerning the DNS ecosystem and related cyber resilience. Furthermore, it aims to play that same role in international initiatives aimed at improving cross-sectoral and inter-ISAC information exchange and collaboration.

For its members, the TLD ISAC focusses on the timely sharing of security information, the analysis of relevant threats and vulnerabilities and on being a competent source of best practices, standards, methods, and know-how related to the DNS.

The European TLD ISAC's mission therefore consists in strengthening the cyber security and resilience of the European Top Level Domain infrastructure by providing a platform for collaboration and intelligence sharing, by giving unique insights into the technical and governance aspects of cybersecurity and associated risks for the industry, and by leading the improvement of cybersecurity of TLD registry operators.

Finally, it raises public cybersecurity awareness regarding the secure use of




A missão do TLD ISAC europeu consiste, assim, em reforçar a cibersegurança e a resiliência da infraestrutura dos domínios de topo europeus, fornecendo uma plataforma para a colaboração e partilha de informações, com uma visão única dos aspetos técnicos e de governação da cibersegurança, assim como dos riscos associados para o sector, liderando a melhoria da cibersegurança dos operadores de registo de TLD.

Por último, sensibilizar o público para a cibersegurança relativamente à utilização segura do sistema DNS e protocolos associados através de seminários e publicações.

**2. Com operadores de registo de domínios, especialistas em segurança e outras partes interessadas, não existe sobreposição com outras entidades de cibersegurança europeias, empresas de telecomunicações e terceiras? É este potencial de coopetição saudável?**

the DNS system and associated protocols through seminars and publications.

**2. With domain registry operators, security experts and other interested parties, isn't there an overlap with other entities that bring together European cybersecurity organizations, telecommunications companies and others, and is this potential coopetition healthy?**

Registry operators are part of a specialised sector, so we focus on expanding our cybersecurity capabilities and expertise in that very specific domain. On the intersection between the Top-Level Domain industry and the aforementioned entities, convergence occurs in forums, conferences, and collaborative initiatives aimed at addressing cybersecurity challenges collectively. This overlap can seemingly lead to duplication of efforts, but we believe that each initiative

Os operadores de registo fazem parte de um setor especializado, pelo que nos focamos em expandir as nossas capacidades e conhecimentos de cibersegurança nesse domínio muito específico. Na intersecção entre o setor dos domínios de topo (TLDs) e as entidades acima mencionadas, a convergência ocorre em fóruns, conferências e iniciativas de colaboração destinadas a enfrentar coletivamente os desafios da cibersegurança. Esta sobreposição pode, aparentemente, conduzir a uma duplicação de esforços. Contudo, acreditamos que cada iniciativa tem a sua perspetiva, a sua razão de ser e acrescenta valor a todas as partes interessadas envolvidas.

A troca de informações e a cooperação entre todos estes diferentes "stakeholders" no panorama da segurança são essenciais e geram inúmeros benefícios graças aos conhecimentos especializados de cada um.

**3. Na vossa primeira conferência, em novembro passado, a agenda abrangia "tópicos gerais, técnicos e regulamentares". Quais são os mais difíceis de abordar a curto prazo e, nesse sentido, o que se pode esperar do TLD ISAC em 2024?**

Para enfrentar os desafios da cibersegurança, é necessária uma abordagem multifacetada baseada na colaboração, na partilha de melhores práticas tecnológicas e de medidas de segurança de ponta. Por último,

has its perspective, raison d'être and adds value to all stakeholders involved.

Information exchange and cooperation between the different stakeholders in the security landscape is essential and creates numerous benefits thanks to each other's key expertise.

**At your first conference in last November, the agenda covered "general, technical and regulatory topics". Which do you anticipate will be the most difficult to address in the short term and, in that sense, what can we expect from the ISAC TLD in 2024?**

Addressing cybersecurity challenges requires a multifaceted approach based on collaboration, sharing technological best practices and state of the art

mas não menos importante, é necessária a implementação de quadros regulamentares.

Acreditamos firmemente que os operadores de registo que participam ativamente e tiram partido dos recursos fornecidos pelo TLD ISAC irão reforçar a sua ciber-resiliência face à evolução das ameaças. É por isso que a agenda da nossa primeira conferência abordou todos estes aspetos, destacando todas as facetas de uma estratégia de cibersegurança eficaz.

Os desafios, principalmente em 2024, quando a diretiva NIS2 tiver de ser transposta para a legislação nacional em toda a União Europeia, giram em torno da tradução dos regulamentos em medidas de cibersegurança práticas e compreensíveis que sejam eficientes e exequíveis.

Queremos ajudar os nossos membros neste processo, focando-nos no reforço das suas capacidades para acompanhar os avanços tecnológicos e a evolução das táticas dos cibercriminosos. Iremos intensificar a nossa colaboração para melhor identificar e compreender o atual panorama de ameaças. Por último, pretendemos criar ferramentas valiosas que os membros do ISAC possam utilizar nos seus respetivos departamentos técnicos e de segurança.

security measures, and last but not least, implementing regulatory frameworks. We strongly believe that registry operators that participate actively in and leverage the resources provided by the TLD ISAC will strengthen their cyber resilience in the face of evolving threats. This is why the agenda of our first conference touched all these aspects highlighting all the facets of an effective cybersecurity strategy.

The challenges, particularly in 2024 when the NIS2 directive has to be transposed into national law across the EU, revolve around the translation of regulations into practical and comprehensible cybersecurity measures that are efficient and usable.

We want to assist our members in this by focusing on enhancing their capabilities to keep up with technological advancements and the evolving tactics of cybercriminals. We will intensify our collaboration to better identify and understand the current threat landscape. And finally, we aim to create valuable tools that members of the ISAC can employ within their respective technical and security departments.

**Bruno Morais**

**Analista de Cibersegurança do .PT**
**.PT Cybersecurity Analyst**

## Garantir a Resiliência Empresarial através da Continuidade de Negócio

No cenário empresarial dinâmico de hoje, a capacidade de adaptação a mudanças inesperadas é crucial para a sobrevivência e para o sucesso. A continuidade de negócio emerge como um pilar fundamental na construção da resiliência empresarial. Pretende-se com este artigo explorar a importância prática da continuidade de negócios, destacando as suas fases essenciais e os referenciais que podem guiar as organizações neste mesmo processo crítico.

A continuidade de negócio não é apenas uma precaução contra desastres. É uma estratégia proativa para garantir a operação ininterrupta face a interrupções imprevistas. Vai além da mera recuperação de desastres e abrange a manutenção das operações críticas durante e após eventos disruptivos, como desastres naturais, falhas tecnológicas, ciberataques e pandemias.

A importância de um plano efetivo de continuidade de negócio é inegável, especialmente diante das estatísticas que revelam as consequências severas que as empresas podem enfrentar em caso de uma interrup-

## Ensuring Business Resilience through Business Continuity

In today's dynamic business landscape, the ability to adapt to unexpected changes is crucial for one's survival and success. Business continuity emerges as a fundamental pillar in building business resilience. This article aims to explore the practical importance of business continuity, highlighting its essential phases and the benchmarks that can guide organisations through this critical process.

Business continuity is not just a precaution against disasters. It is a proactive strategy to guarantee uninterrupted operations when facing unforeseen interruptions. It goes beyond mere disaster recovery and encompasses maintaining critical operations during and after disruptive events, such as natural disasters, technological failures, cyberattacks and pandemics.

The importance of an effective business continuity plan is undeniable, especially given the statistics that show the severe consequences that companies can face in the event of a significant interruption without the proper preparation. The lack of a robust

ção significativa sem a devida preparação. A falta de um plano robusto de continuidade de negócio coloca as organizações num terreno instável, frequentemente resultando em sérias repercussões financeiras, operacionais e reputacionais.

*O PTSOC lançou um novo MOOC sobre Gestão da Continuidade de Negócio para o público que pretenda adquirir mais conhecimentos sobre o tema, acessível na plataforma NAU e pelo site do PTSOC.*

A afirmação de que "mais de 50% das empresas sem um plano efetivo de continuidade de negócio acabarão por abrir falência após uma interrupção significativa" reflete a vulnerabilidade inerente a negócios que negligenciam a necessidade de se preparar para eventos imprevistos. Essa percentagem alarmante destaca a fragilidade das operações empresariais quando não há estratégias claras para a resposta a situações de crise como desastres naturais, crises económicas, incidentes de cibersegurança ou qualquer outro evento que possa interromper as atividades normais. Além do risco de falência, a ausência de um plano de continuidade de negócio pode resultar em perda substancial de receitas, danos à reputação da empresa e uma recuperação mais lenta no pós-crise.

Garantir a continuidade de negócio é uma tarefa complexa que envolve as seguintes fases principais:

business continuity plan puts organisations on shaky ground, often with serious financial, operational and reputational repercussions.

*PTSOC launched a new MOOC on Business Continuity Management for the public who wish to acquire more information on this topic, accessible via the NAU platform and the PTSOC website.*

The statement that 'more than 50 % of companies without an effective business continuity plan will end up filing for bankruptcy after a significant interruption' reflects the vulnerability inherent in businesses that neglect the need to prepare for unforeseen events. This alarming percentage highlights the fragility of business operations when there are no clear strategies to address crisis situations such as natural disasters, economic crises, cybersecurity incidents or other events that could interrupt normal activities.In addition to the risk of bankruptcy, the absence of a business continuity plan can result in substantial loss of revenue, damage to the company's reputation and a slower post-crisis recovery.

Ensuring business continuity is a complex task that involves the following main phases:

**Risk and Impact Analysis:**

- Identify potential threats and assess their impact on business processes.
- Prioritise critical assets and essential services.

**Análise do Risco e Impacto:**

- Identificação de ameaças potenciais e avaliação do seu impacto nos processos de negócios.
- Priorização de ativos críticos e serviços essenciais.

**Desenvolvimento de Estratégias de Continuidade:**

- Elaboração de planos detalhados para manter as operações essenciais durante crises.
- Adoção de estratégias como backup de dados, locais alternativos de trabalho e parcerias estratégicas.

**Implementação e Testes:**

- Implementação efetiva dos planos de continuidade.
- Realização de simulações regulares para garantir a eficácia das estratégias.

**Treino e consciencialização:**

- Capacitação dos funcionários para responder adequadamente a situações de emergência.
- Promoção de uma cultura organizacional que valoriza a continuidade de negócio.

**Melhoria Contínua:**

- Avaliação regular do programa de continuidade de negócio.
- Atualização dos planos para refletir as mudanças nas operações e no ambiente empresarial.

Hoje, diversos referenciais internacionais estão disponíveis para introduzir e orientar a continuidade de negócio nas empresas, oferecendo soluções para mitigar a exposição ao risco das empresas e organizações. Estes padrões globais fornecem diretrizes essen-

**Development of Continuity Strategies:**

- Prepare detailed plans to maintain essential operations during crises.
- Adopt strategies such as data backup, alternative work locations and strategic partnerships.

**Implementation and Testing:**

- Effectively implement continuity plans.
- Carry out regular simulations to ensure the effectiveness of strategies.

**Training and awareness-raising:**

- Train employees to respond appropriately to emergency situations.
- Promote an organisational culture that values business continuity.

**Continuous Improvement:**

- Regularly assess the business continuity programme
- Update plans to reflect changes in operations and the business environment.

Nowadays, there are several international benchmarks available to introduce and guide business continuity in companies, offering solutions to mitigate the risk exposure of both companies and organisations. These global standards provide essential guidelines, helping companies implement robust strategies to face challenges and ensure resilience through an environment of disruption.

ciais, auxiliando as empresas na implementação de estratégias robustas para enfrentar desafios e garantir a resiliência através de um ambiente de disrupção.

## Referenciais Importantes

**ISO 22301:2019 - Sistema de Gestão de Continuidade de Negócio:**

- Fornece uma framework internacionalmente reconhecida para a implementação, operação, monitorização, revisão, manutenção e melhoria contínua de um Sistema de Gestão de Continuidade de Negócio.

**NIST SP 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems:**

- Oferece diretrizes detalhadas para o desenvolvimento e manutenção de planos de continuidade de negócio, especialmente voltado para sistemas de informação.

**BIA (Análise de Impacto no Negócio):**

- Uma ferramenta crucial que identifica e avalia os efeitos potenciais de eventos disruptivos nos negócios, auxiliando na priorização de ações de continuidade.

Em suma, a continuidade de negócio não é apenas uma prática teórica, mas uma necessidade premente para as organizações que procuram manter-se resilientes num mundo em constante evolução. Ao seguir as fases essenciais e adotar referenciais sólidos, as empresas podem não apenas resistir a crises, mas também prosperar diante delas. Investir hoje na continuidade de negócio é um investimento vital para o futuro das organizações.

## Important Benchmarks

**ISO 22301:2019 - Business Continuity Management System:**

- Provides an internationally recognised framework for the implementation, operation, monitoring, review, maintenance and continual improvement of a Business Continuity Management System.

**NIST SP 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems:**

- Provides detailed guidelines for developing and maintaining business continuity plans, especially geared towards information systems.

**BIA (Business Impact Analysis):**

- A key tool that identifies and evaluates the potential effects of disruptive events on businesses, helping prioritise continuity initiatives.

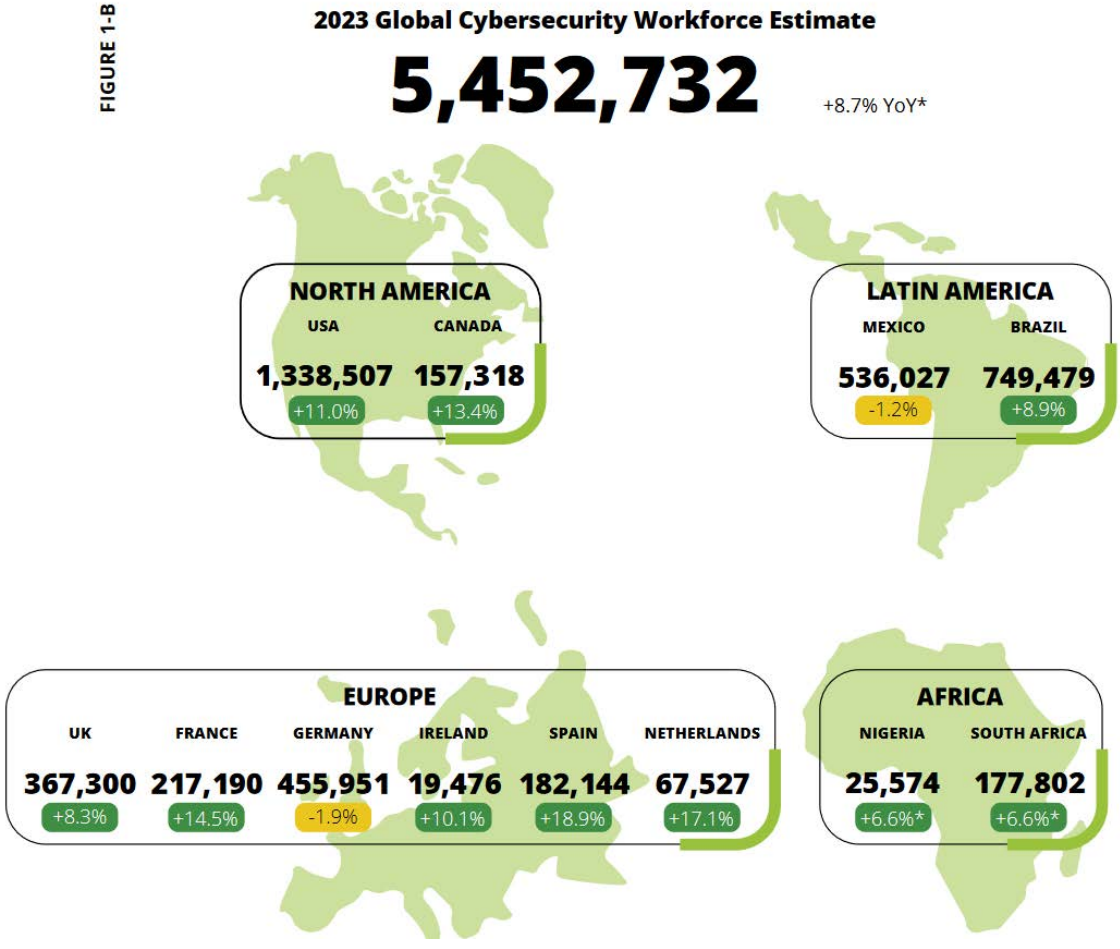
In short, business continuity is not just a theoretical practice, but a pressing need for organisations seeking to remain resilient in an ever evolving world. By following the essential phases and adopting solid benchmarks, companies can not only withstand crises and also thrive in the face of them. Investing in business continuity today is a vital investment for the future of organisations.

## How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce

A força de trabalho global na cibersegurança "atingiu um novo pico de 5,5 milhões de pessoas, um crescimento de 9% desde 2022", mas a procura deve continuar a ultrapassar a oferta durante mais algum tempo.

The global cybersecurity workforce 'has reached a new peak of 5.5 million people, a growth of 9 % from 2022', but demand is still outpacing the supply for a while longer.

FIGURE 1-B



## Cloudzy with a Chance of Ransomware

Relatório com algumas das técnicas usadas para desmascarar os "Command-and-Control Providers" (C2P) - ou fornecedores de comando e controlo -, intervenientes na economia do ransomware e que "vendem serviços a agentes de ameaças enquanto assumem um perfil comercial legal".


Report with some of the techniques used to unmask 'Command-and-Control Providers' (C2P), players in the ransomware economy, who 'sell services to threat actors while assuming a legal business profile'.

## Cyber-attacks: the apex of crime-as-a-service

A evolução dos ciberataques, novas metodologias e ameaças detetadas pela Europol, e a resposta da polícia europeia aos ataques de cibercriminosos "mais profissionalizados" e "a explorar as mudanças na geopolítica como parte das suas metodologias".


The evolution of cyberattacks, new methods and threats detected by Europol, and the response of the European police to attacks by cybercriminals who are 'increasingly professionalised' and are 'exploiting changes in geopolitics as part of their methodologies'

**Diretora | Director**
Inês Esteves

**Edição | Editor**
Pedro Fonseca

**Design Gráfico | Graphic Design**
Sara Dias
Maria Cristóvão

**Tradução | Translation**
Sara Pereira

**Fotografia (capa e índice) | Photography (cover & index)**
Filip Starý/Unsplash
Philipp Katzenberger/Unsplash



Publicação trimestral | Quarterly publication
Dezembro 2023 | December 2023