INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Employer Branding em Profissionais de Cibersegurança

Andreia da Silva Nunes

Mestrado em Gestão de Recursos Humanos e Consultadoria Organizacional

Orientador:
Prof. Doutor Aristides Ferreira,
Professor Associado, ISCTE-IUL

Outubro, 2022

BUSINESS
SCHOOL

Departamento de Recursos Humanos e Consultadoria Organizacional

Employer Branding em Profissionais de Cibersegurança

Andreia da Silva Nunes

Mestrado em Gestão de Recursos Humanos e Consultadoria Organizacional

Orientador:
Prof. Doutor Aristides Ferreira,
Professor Associado, ISCTE-IUL

Outubro, 2022

Agradecimentos:

Agradeço primeiramente ao meu orientador, Professor Doutor Aristides Ferreira pelo acompanhamento e orientação.
Ao meu marido por me ter inspirado a escrever esta dissertação.
À minha mãe e irmã por todo o apoio incondicional durante toda a minha vida.
Ao meu pai, embora com cancro sempre esteve presente. A ele dedico esta dissertação.
Finalmente, gostaria de agradecer a todos os que responderam e participaram nesta investigação.

Resumo:

O *employer branding* é um processo estratégico de construção de imagem, que permite às empresas que a implementam construir uma imagem de boa referência empregadora, e atrair, sobretudo, perfis tecnológicos como os profissionais de cibersegurança, cuja procura atualmente está a aumentar consideravelmente, gerando ainda mais significado na capacidade de reter este tipo de talento, para a realização dos objetivos do negócio. Atualmente, as empresas que têm a capacidade de se tornar referência no mercado de trabalho passam por um processo de transformação bastante trabalhoso, que pode levar tempo e exigir colaboração e recursos, ao invés de trazer grandes benefícios de longo prazo em termos profissionais e comerciais, atraindo e retendo os melhores profissionais em diferentes áreas, como cibersegurança. Com isso em mente, a fim de desenvolver uma dissertação válida, com base literária, análise crítica qualitativa, análise quantitativa e estatística, foi desenvolvida uma série de questões de pesquisa sobre os procedimentos utilizados nas técnicas e instrumentos de recolha de dados, a fim de determinar a eficácia da implementação do *employer branding* como estratégia de atração de talentos e profissionais de cibersegurança na era atual. Para tal a presente investigação contou-se com a participação de 12 participantes no estudo qualitativo e com cerca de 127 participantes no estudo quantitativo. Uma vez aplicadas estas últimas, torna-se estatisticamente evidente que o *employer branding* é atualmente uma alternativa eficaz para atrair e reter profissionais de cibersegurança.

Palavra-chave: *Employer Branding*, Tecnologia de Informação, Retenção

Classificação JEL:

O15: Human Resources

L86: Information and Internet Services/ Computer Software

Abstract:

Employer Branding is a strategic image-building process, which allows companies that implement it to build an image of good employer reference, and to attract, above all, technological profiles such as cybersecurity professionals, whose demand is currently increasing considerably, still generating more meaning in the ability to retain this talent, for the achievement of business objectives. Currently, companies that have the capacity to become a reference in the job market go through a very laborious transformation process, which can take time and require collaboration and resources, rather than bringing great long-term benefits in professional and commercial terms, attracting and retaining two best professionals in different areas, such as cybersecurity, a priority in this process. With that in mind, to develop a valid dissertation, with a literary basis, qualitative critical analysis, quantitative and statistical analysis, a series of research questions were developed about the foramina used in the techniques and instruments of data collection, in order to determine the effectiveness of implementing *employer branding* as a strategy for attracting cybersecurity talent and professionals in the current era. For this, the present investigation had the participation of 12 participants in the qualitative study and with about 127 participants in the quantitative study. Once these last forms are applied, it becomes statistically evident that *employer branding* is currently an effective alternative to attract and retain cybersecurity professionals.

Keywords: *Employer Branding, Information Technology, Retention*

JEL Classification:

O15: Human Resources

L86: Information and Internet Services/ Computer Software

Índice

Índice de tabelas

Índice de figuras

Introdução

Discutir a atração e retenção de talento humano implica entender que esses processos representam os dois fatores mais importantes para a área de recursos humanos de qualquer organização, principalmente a procura por novos colaboradores que contribuam positivamente para os objetivos do negócio. A tarefa de recrutar profissionais tecnológicos torna-se fundamental numa perspetiva funcional.

Sabemos que no passado a competição empresarial decorria perante o capital investido da empresa e em estratégias de *marketing*, atualmente com a globalização e com a digitalização a competição decorre ao nível da atração, motivação e retenção dos talentos que são vitais para as organizações (Aggerholm *et al.,* 2011; Joo *et al*., 2006).

Uma vez que capital humano é o verdadeiro diferenciador das organizações é necessário recorrer a ferramentas que conduzam a um pacote salarial e de benefícios exclusivos aliciantes ao colaboradores (Hillebrandt *et al*., 2013; Sokro, 2012) que têm como foco, além de atrair potenciais talentos, também tentar contrabalançar a decisão do colaborador quando este recebe ofertas de outras organizações (Hillebrandt *et al*., 2013).

Sabendo que o mundo está cada vez mais digital e as organizações enfrentam uma elevada competitividade doravante mundial, esta mudança obriga as mesmas a reverem os seus posicionamentos estratégicos bem como as políticas organizacionais. Ao longo dos últimos anos, temos vindo a observar a elevada expansão do setor das tecnologias de informação onde se consegue notar que existiram algumas profissões que se extinguiram mas tantas outras dentro deste setor floresceram devido ao desenvolvimento mundial.

Devido à enorme escassez de recursos especializados no mercado de trabalho em cibersegurança em comparação com outras áreas de tecnologias de informação (i.e. programadores) (Bureau of Labor Statistics, 2022), bem como da existência de pouca formação académica disponível para formar massivamente recursos nesta área (Observatório de Cibersegurança, 2022), estes recursos especializados são disputados com muita frequência (ISC² 2022) neste setor volátil (Agrawal *et al*., 2009).

É assim importante que as empresas utilizem o *employer branding* para lhes permitir construir uma boa referencia de entidade empregadora para atrair futuros candidatos e reter os profissionais atuais (Ahmad *et al*., 2016).

As empresas que implementam o *employer branding* nos seus processos estratégicos são capazes de gerar emoções e sensações nos futuros colaboradores e/ou atuais colaboradores, associando-se à marca, à filosofia e imagem alicerçada em valores éticos e morais da empresa (Rampl *et al*., 2016). No entanto, é preciso estar ciente de que, para implementar este processo estratégico, é necessário que diversos departamentos das organizações colaborem para melhorar o posicionamento organizacional no mercado de trabalho, atuando com base na cultura e clima organizacional (Heilmann *et al*., 2013), com vista a garantir a satisfação dos primeiros e mais eficientes embaixadores da imagem da empresa na captação de novos talentos, os próprios colaboradores atuais da empresa.

No caso particular dos profissionais de cibersegurança, é muito importante que as empresas se concentrem nos salários (Döckel, 2003), que obviamente devem estar de acordo com o trabalho solicitado, mas também na valorização do talento e das habilidades humanas, qualidade dos projetos, oportunidades de crescimento, flexibilidade, entre outros fatores que não seriam levados em conta aparentemente, na categoria de *employer branding.*

Com vista à compreensão quais são aos motivações de employer branding que são condutoras das decisões deste setor profissional, durante o presente estudo pretende-se assim responder às seguintes questões de investigação:

1. Quais as motivações que levam os profissionais de cibersegurança a mudar de organização?
2. Quais as motivações que levam os profissionais de cibersegurança a preferir trabalhar nesta área face a outras de tecnologias de informação?
3. Quais as motivações que levam os profissionais de cibersegurança a continuar na empresa onde desempenham funções atualmente?
4. Quais os fatores de *employer branding* interno que explicam uma maior integração (*job embeddedness)* no trabalho?

Sabendo que uma dissertação é uma reflexão baseada em informação, argumentação e conclusão sobre uma ou mais hipóteses de investigação a presente dissertação irá analisar a atração e retenção nos profissionais de cibersegurança.

Seguidamente, será apresentada a revisão de literatura científica que foi considerada pertinente para o presente estudo, bem como as questões de investigação, seguido da metodologia utilizada durante a presente dissertação, depois os resultados e discussão, terminado com as conclusões da investigação. Depois poderão ser encontradas as referências utilizadas para a presente dissertação e os anexos para melhor compreensão do presente estudo.

Revisão de Literatura

Employer Branding nos Profissionais de Cibersegurança

Conforme citado em Campanário (2014), o termo *employer branding* teve sua primeira aparição histórica na década de 1990, quando Ambler *et al*., (1996) define o *employer branding* como uma aplicação de estratégias de mercado dentro da área de recursos humanos, que procura atrair e reter talentos em prol dos objetivos organizacionais estabelecidos.

O *employer branding* nasceu como base num interesse genuíno das organizações em comunicar e procurar novos colaboradores para as suas empresas, colaboradores estes que estejam alinhados com os objetivos estratégicos, pontos fortes e proposta de valor que a empresa tem (Barrow *et al*., 2011). Campanário (2014), afirma ainda que o *employer branding* procura atrair novos talentos com estratégias claramente semelhantes às utilizadas por um Departamento de *Marketing* para atrair e reter clientes. A esse respeito, Jimenez *et al*., (2010), explicam que o *employer branding* é desenvolvido a partir da cultura organizacional estabelecida na organização, sendo um processo onde várias estratégias de *marketing* interno são aplicadas para atrair novos futuros talentos que se interessem e identifiquem com a organização em causa.

De fato, Laínez (2016), explica que a essência do termo é justamente a expressão ou exposição externa da cultura interna, incluindo fatores que vão desde o trabalho, ao clima organizacional e até a cultura. Blasco-López *et al*., (2015), por outro lado mostram que o *employer branding* não utiliza apenas estratégias de *marketing* interno, como afirmam Jiménez *et al*., (2010), mas representa uma técnica em que estas são complementadas pela "marca da empresa", onde o principal objetivo é realmente atrair e reter potenciais talentos humanos durante o máximo de tempo possível. A isto acrescentam que, para implementar o *employer branding* com sucesso numa organização, deve haver uma transmissão de valores e benefícios aos colaboradores atuais e futuros, bem como uma boa comunicação interna e gestão do sentimento de pertença à organização. Por sua vez Foster *et al*., (2010) defendem que o *employer branding* surge da necessidade das empresas criarem equipas de trabalho mais competitivas interna e externamente, e que por isso, investe-se inúmeros recursos de diversos tipos para posicionar a reputação da organização no mercado em que se atua, na premissa de promover um bom ambiente de trabalho.

Atualmente, atrair e reter talentos para as organizações é um grande desafio, uma vez que é uma variável crítica de competitividade e as organizações deixam de estar somente

preocupadas com a reputação junto dos clientes para também consolidar a sua reputação junto dos colaboradores atuais (Jiménez *et al.,* 2015). As empresas de hoje procuram tornar-se uma marca empregadora atrativa para os atuais e futuros talentos, compreendendo as capacidades e as ferramentas que podem contribuir para o desenvolvimento organizacional (Di Girolamo, 2015).

A Geração X e Millennials são aqueles que atualmente entram no mercado de trabalho em 2022, e as empresas que procuram aumentar talento destas idades devem ter em mente o seu desejo de equilíbrio entre vida profissional e pessoal. Estas gerações valorizam um clima organizacional onde seja valorizado o tempo, o esforço, o poder aquisitivo e as oportunidades de crescimento profissional. (Gilley *et al.,* 2015). Quando isso não acontece e as atividades profissionais não apresentam boas condições de trabalho, como um bom salário, bónus, entre outros, estas organizações são vistas apenas como uma ponte para chegar a uma nova organização que ofereça as condições esperadas por estas novas gerações, pois as primeiras organizações são apenas um processo transitivo de aquisição de experiência, mas nunca uma opção de fidelização, que é o principal objetivo do *employer branding* (Gomes *et al.,* 2010). Consequentemente, o fato dos colaboradores estarem separados das organizações representa, por sua vez, uma perda de tempo e dinheiro, pois significa instabilidade nos processos de formação e recrutamento (Álvarez *et al.,* 2017).

Com o *employer branding*, surgem novas estratégias e esforços para a retenção dos talentos, onde a competitividade dos profissionais no mercado de trabalho também desempenha um papel importante, uma vez que para organizações à procura de crescimento e posicionamento, atrair talento humano com elevada capacidade e competências excecionais é de especial interesse dado que o sucesso empresarial está relacionado com o recrutamento de pessoas com elevados níveis de motivação e com elevadas *skills (*Figurska *et al*., 2013).

Em suma, o *employer branding* procura conceber, promover e implementar ações eficazes e inovadoras nas organizações de acordo com as necessidades atuais dos recursos humanos para gerar uma cultura organizacional que predisponha desenvolvimento profissional, bom clima organizacional, comunicação interna, equipamentos de trabalho e condições de trabalho ideais que ajudam os atuais colaboradores e futuros a se comprometerem com a empresa (Shuck *et al.,* 2011).

Segundo Jaimes *et al.,* 2017, detalham as vantagens da implementação do *employer branding* internamente, que podem ser resumidas da seguinte forma:

- Aumento do desempenho financeiro;
- Aumento do potencial dos colaboradores;
- Satisfação e melhoria do ambiente de trabalho;

- Orientação ao cliente;
- Compromisso organizacional.

Relativamente às vantagens da implementação do *employer branding* externamente, Sousa *et al.,* 2017, destacam como vantagem as ofertas de emprego tornarem-se mais atrativas e com maior número de candidaturas.

Importância do *employer branding* no posicionamento empresarial

A importância do *employer branding* reside principalmente na forma como permite que as empresas atuem para se mostrarem ao mercado de trabalho de forma visível, onde os futuros colaboradores têm acesso à informação sobre a missão e visão da empresa, bem como a sua cultura, metodologia de trabalho, interesses e talentos, e ainda, desperta afinidade com os futuros talentos que as organizações pretendem recrutar para melhorar a sua força de trabalho, tornando assim uma vantagem competitiva face a outras organizações (Sehgal, 2013). Duarte (2016), explica que hoje em dia é muito comum ter uma estratégia de comunicação clara nas redes sociais e noutros aplicativos especializados. Devido ao grande *boom* digital é importante as organizações estarem presente nas redes sociais e aplicações onde os futuros colaboradores também estejam.

Campanário (2014) defende que os benefícios do *employer branding* são significativos e têm impacto na produtividade da empresa, defende também que com a orientação dos especialistas, este processo melhora a reputação da empresa em questão e reduz o custo de recrutamento, reduzindo gradualmente o absentismo e o *turnover* excessivo uma vez que os colaboradores sentem-se mais motivados e tornam-se os principais embaixadores da empresa.

Existe um ditado popular na sociedade atual que nos diz que não há melhor publicidade externa do que um cliente satisfeito que recomenda a empresa a outros clientes. Da mesma forma, internamente, não há melhor divulgação interna do que um colaborador satisfeito que recomenda a empresa a outros futuros colaboradores que também podem vir a contribuir com os seus talentos para o alcance dos objetivos. Assim, as estratégias de *employer branding* visam promover internamente as “vantagens da empresa", os salários e os benefícios psicológicos e emocionais tão importantes na era atual para atrair novos talentos.

Corral (2007) indica que o plano de *employer branding* deve ser pensado como uma proposta de valor dirigida aos atuais trabalhadores e futuros colaboradores, quer em termos da marca interna quer em termos de marca externa. Portanto, para colocar estas estratégias em prática, além de elaborar um projeto base bem estruturado, também é essencial que as áreas de recursos humanos, comunicação interna e administração estejam em concordância (Figurska *et al*., 2013).

Em todas as questões de *employer branding* é necessário, para a sua implementação, posicionar a empresa. Para tal é indispensável compreender o conceito de cultura organizacional. Este é considerado como um conjunto de significados e crenças partilhados por um grupo de pessoas, que permitem que as organizações tenham um impacto positivo na sua produtividade (Cújar, 2013). Neste sentido, Estrada *et al*., (2009) argumentam que a cultura organizacional representa um conjunto de valores, necessidades, expetativas, crenças, normas, políticas, clima e comportamentos que estão constantemente a surgir dentro da empresa, o que significa que as pessoas que constituem uma organização são quem determina a cultura organizacional da mesma. Neste sentido, a cultura organizacional proporciona uma identidade organizacional e está também relacionada com os objetivos estratégicos da empresa, gestão e desempenho dos trabalhadores (Gutiérrez *et al*., 2017; Williams, 2013). Naturalmente, a cultura organizacional está também relacionada com o *employer branding*, uma vez que a cultura organizacional desempenha um papel fundamental na reputação interna das empresas. Outro termo importante a ser desenvolvido para a compreensão do assunto a ser tratado, é que o clima organizacional representa todo ou o contexto social onde fazem parte as pessoas que pertencem à organização, bem como as suas perceções políticas, práticas e processuais (Chiang Vega *et al*., 2008). Bernal *et al*., (2015) acrescentam ainda que o clima organizacional é um dos dois fatores que mais influencia a perceção das pessoas sobre a reputação das empresas e é composto pela perceção que cada trabalhador tem de uma empresa, a partir de uma avaliação crítica de condicionantes como relações sociais, comunicação, tomada de decisão, entre outros (Williams, 2013). O clima organizacional está ainda relacionado com a motivação e o comportamento dos membros de uma empresa e, portanto, refletindo-se diretamente na sua produtividade (Iglesias *et al*., 2015).

Os autores Estrada *et al*., (2009) propõem que o clima organizacional apresenta uma noção multidimensional, baseada no ambiente físico, que é constituído pelas instalações e ferramentas de trabalho da empresa; o ambiente social, que engloba aspetos de comunicação, companheirismo e possíveis conflitos entre trabalhadores; e o ambiente estrutural, as características que definem as hierarquias organizacionais, bem como as características pessoais de cada indivíduo, onde se destacam elementos como aptidões, atitudes, expetativas e motivação. Por fim, o estudo menciona ainda que o clima organizacional, está relacionado com a produtividade, rotatividade, satisfação profissional, entre outros. Tendo isso em mente, fica claro que para implementar o *employer branding* como estratégia organizacional, é necessário identificar e cultivar um bom clima organizacional que influencie a eficácia dos resultados a curto, médio e longo prazo.

Employer branding e cibersegurança

Para compreender a atual relação entre o *employer branding* e cibersegurança, é necessário conhecer ambos os termos em profundidade, razão pela qual até esta parte explicámos muitos pontos importantes a ter em conta no que concerne ao *employer branding*. No entanto, é agora tempo de aprofundar o conceito de cibersegurança, e para começar, o termo pode ser definido de acordo com as diretrizes do Centro Nacional de Cibersegurança (2019) como um conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem.

É importante ter em mente que o principal objetivo da contribuição dos profissionais de cibersegurança nas organizações é precisamente minimizar os riscos de possíveis acessos a dados de outros utilizadores, expondo informações que devem ser confidenciais (Austin *et al*., 1992). O domínio da cibersegurança representa assim atualmente um terreno fértil onde as atitudes podem gerar resultados positivos ou negativos.

Atualmente, em muitos países do mundo, a crescente necessidade de salvaguardar dados, bem como os contínuos casos de roubo de informação (Cremer *et al*., 2022), tornaram essencial para as empresas o recrutamento de profissionais com experiência em cibersegurança, e é aqui que se concentra a relação com o *employer branding*. Por outro lado, as empresas têm cada vez mais dados de utilizadores "na ponta dos dedos", e esta informação é também uma grande fonte de oportunidades a explorar (Cremer *et al*., 2022).

A curto prazo, não se espera que a procura de profissionais de cibersegurança diminua, mas pelo contrário, estamos perante um processo crescente em que novas empresas e outras fora do setor das tecnologias de informação continuarão a crescer e terão de passar por um processo de digitalização para serem competitivos numa era puramente digital (Brynjolfsson, 1993) onde o salário não é um fator aparentemente predisponente na tomada de decisões quando estes profissionais mudam de emprego, uma vez que os profissionais de cibersegurança procuram outros benefícios de maior importância na sua qualidade de vida (Haney *et al.,* 2019).

Atrair e reter profissionais de cibersegurança nas organizações

Dada a importância destes profissionais, existe uma constante procura por estes recursos fazendo com que um dos desafios cruciais em cibersegurança seja atrair e reter talentos (Caldwell, 2013; Pretorius *et al.,* 2015).

De acordo com relatórios regulares emitidos pela Cisco Systems, uma empresa americana envolvida no fabrico, venda, manutenção e consultoria de equipamento de telecomunicações, a pandemia de Covid-19 marcou uma mudança significativa na área da cibersegurança, gerando uma transição nas empresas de todo o mundo do ambiente de trabalho familiar face-a-face para o ambiente de trabalho remoto que é hoje popular, a uma velocidade e escala sem precedentes.

Com os períodos de confinamento gerados pela pandemia covid-19, o que antes era uma modalidade opcional para colaboradores de organizações a nível global, tornou-se agora essencial em muito pouco tempo, uma vez que as organizações em praticamente todos os países implementaram disposições de trabalho remoto para toda a sua força de trabalho, num processo de transição, no qual tiveram de se adaptar, desenvolvendo abordagens, soluções e políticas de cibersegurança para permitir aos seus colaboradores trabalharem remotamente, aceder aos recursos da empresa com segurança e assegurar a continuidade dos objetivos empresariais.

Esta tendência, no sentido de um futuro de trabalho flexível e híbrido, originou com que os colaboradores de diferentes empresas tivessem horários flexíveis e a capacidade de trabalhar a partir de qualquer lugar, em qualquer altura e com qualquer dispositivo, de modo a que estes valores, que giram em torno da flexibilidade laboral, sejam então parte dos fatores motivacionais atualmente utilizados nas empresas para atrair talento em cibersegurança, bem como noutras áreas (Cisco, 2021). O mesmo relatório afirma que os líderes das tecnologias de informação são obrigados a adotar uma nova mentalidade, com ênfase na agilidade das tecnologias de informação necessárias para alcançar a resiliência empresarial, em vez do planeamento tradicional da continuidade empresarial, mesmo em preparação para o inesperado (Cisco, 2021).

É possível compreender que a maior utilização de dispositivos e ligações pessoais para aceder a aplicações e dados empresariais, torna os colaboradores remotos mais vulneráveis a ciberataques (Cisco, 2021). Nos últimos anos, registaram-se ataques na Europa e em muitos países em todo o mundo que comprometeram a cibersegurança dos dados governamentais e do setor privado mostrando ao mundo uma realidade inegável (União Europeia, 2022), e isto é a prova de que os profissionais em cibersegurança são uma tendência crescente nas organizações (ISC², 2022). Com estes fatos, muitas organizações entraram numa fase de competição por especialistas de cibersegurança (Ishmael *et al*., 2022), porque precisam destes profissionais para prevenir ciberataques às suas próprias organizações (Fortinet, 2022).

A luta de que se fala, contudo, deve-se ao fato de não haver talento suficiente para satisfazer a procura que existe atualmente para estas organizações, e o fosso entre a oferta e a procura neste caso está longe de deixar de crescer desde 2017. Nesse ano, a ISC² (2017) já previa que este fosso entre o que as organizações precisam e o que o mercado de trabalho oferece iria

aumentar com o tempo, estimando-se que 1,8 milhões de posições de profissionais de cibersegurança permaneceriam por preencher até 2022. Segundo a mesma fonte, serão necessários cerca de 3,2 milhões de especialistas em cibersegurança a nível mundial na próxima década e as ofertas de emprego triplicarão nos próximos dois anos. Isto levanta muitas questões para as organizações sobre como podem atrair talento especializado em cibersegurança, mas especialmente sobre como o podem reter.

Um dos passos para atrair talento em cibersegurança está relacionado com o salário, já que uma das consequências do elevado nível de concorrência no setor tem sido o aumento dos salários, e isto deve-se principalmente ao fato do salário continuar a ser a principal motivação para escolher uma empresa em detrimento de outra (ISC², 2022), e não é segredo que hoje em dia os especialistas em cibersegurança estão entre os empregos mais bem pagos e mais procurados do mundo (Bureau of Labor Statistics, 2022).

Contudo de acordo com ISC² (2017), não se trata apenas do dinheiro ou dos recursos materiais que uma empresa pode oferecer ao talento de cibersegurança; a falta de compreensão do seu trabalho, bem como a falta de apoio dos diretores e gestores organizacionais, são razões pelas quais os especialistas em cibersegurança deixam as empresas, uma vez que são fatores que limitam a sua capacidade de crescer profissionalmente e causam desmotivação e fraturas no clima e cultura organizacionais. As oportunidades de crescimento interno, desenvolvimento e aquisição de conhecimento, a possibilidade de ir a eventos no setor e entrar em contato com outros profissionais, o trabalho flexível e remoto, e o acesso a ferramentas tecnológicas inovadoras estão entre os elementos do chamado salário emocional que são mais importantes para este tipo de profissionais (ISC², 2017). Portanto, na maioria dos casos, o salário emocional é mais importante do que o salário monetário, dado que a maioria dos profissionais de cibersegurança estão mais concentrados na qualidade de vida e em tudo o que isto representa em termos de tempo, estabilidade emocional e equilíbrio do que no que podem adquirir monetariamente com o seu trabalho (Cisco, 2021).

É também importante que as empresas tenham uma cultura empresarial que apoie e proteja a diversidade na organização, pois ajuda a trazer perspetivas diferentes à equipa de cibersegurança numa área de trabalho que está em constante evolução, especialmente na era digital atual. De acordo com o relatório elaborado pela Mercer Marsh Benefits (2021), atualmente, a cibersegurança, a atração, a retenção, o *engagment* dos colaboradores e a proteção de dados são alguns dos maiores desafios que as empresas enfrentam a nível global. As suas conclusões, baseadas no inquérito a 1.380 profissionais, em primeiro lugar, globalmente, tanto os diretores de Recursos Humanos (46%) como os Gestores de Risco (54%) concordam que cibersegurança e talento são os dois riscos-chave.

Portugal, tal como outros países da Europa, está a desenvolver novas políticas de trabalho que permitirão às organizações atuais evoluir de acordo com as novas tecnologias. É por isso que o governo português está a atribuir pelo menos 130 milhões de euros de fundos europeus para aumentar a segurança na utilização de sistemas e dados digitais, ou seja, para fins de cibersegurança. Como noticiado por Rodrigues Varela, (2021) no Jornal Económico, o reforço da proteção da infraestrutura informática do Estado tornou-se uma das prioridades do Governo português no Plano de Recuperação e Resiliência, constituído por 36 reformas e 77 investimentos com um orçamento de 13,9 mil milhões de euros que serão utilizados para retomar o crescimento económico do país nos próximos cinco anos. Cerca de 83 milhões de euros serão investidos em infraestruturas críticas digitais eficientes, seguras e partilhadas com o objetivo de tornar a rede informática do governo mais resiliente e digital. Do mesmo modo, 47 milhões, irão para a criação de um Sistema Nacional de Certificação de Cibersegurança, um sistema que que tem como objetivo fazer face a quaisquer ciberataques a nível estatal ou à indústria privada.

O estudo de Fitzgerald *et al.,* (2013) descreve Portugal como um centro para grandes empresas tecnológicas internacionais, descrevendo como Portugal aborda especificamente os desafios da proteção de dados e da cibersegurança que surgem quando confrontado com uma elevada procura de serviços digitais, investindo grandes somas de dinheiro e esforço no desenvolvimento de cibersegurança. Segundo o mesmo estudo Portugal adere às melhores práticas mundiais em matéria de proteção de dados e cibersegurança, alinhando o seu quadro de cibersegurança com as normas e certificações internacionais mais importantes do setor europeu, refere também que Portugal está bem posicionado não só para acompanhar a transformação digital, mas também para continuar o seu caminho como um dos pioneiros da Europa na inovação tecnológica de cibersegurança e da proteção de dados.

Contudo, para que tal seja possível, é necessário estabelecer novas abordagens na gestão do talento humano nas empresas, que estejam relacionadas com as metas e objetivos na direção estratégica das organizações (Cano, 2020). No processo, deve também ter-se em conta que a economia e a sociedade do conhecimento se caracterizam pela globalização económica e pela emergência de avanços tecnológicos em vários domínios industriais e científicos (García, 2021). Neste sentido, o reforço das competências do talento humano também assegura que a utilização dos recursos tecnológicos seja otimizada e minimiza o risco de danos e perdas de informação, sistemas e equipamentos devido a uma utilização inadequada (García, 2021). Com isto e a adoção de normas internacionais sobre boas práticas para a prevenção de riscos, as empresas poderão selecionar profissionais com competências, capacidades e conhecimentos

para compreender e gerir adequadamente os sistemas de gestão de cibersegurança (Díaz, *et al.,* 2018).

A era digital, que até há poucos anos era um sonho do futuro, é agora uma realidade presente; inteligência artificial, *big data*, agilidade, mudança organizacional são uma parte essencial de uma nova etapa, e as organizações devem embarcar na transformação digital uma vez que se mantiverem os métodos tradicionais arriscam-se a desaparecer no tempo. Segundo Valderrama (2019), a era digital forçou as empresas a reinventarem-se e a conceberem novos modelos de negócio, uma vez que os avanços tecnológicos mudaram as competências e os conhecimentos dos indivíduos, influenciando significativamente o seu desempenho profissional.

Questões de investigação

Sabendo que as organizações podem melhorar o processo de reter os colaboradores através da criação de um local de trabalho que oferece os meios necessários para os colaboradores serem eficientes (Nguyen, 2020), é imperativo estudar quais os fatores do *employer branding* que os profissionais de cibersegurança valorizam nas organizações para potenciar a retenção deste setor profissional.

Uma vez que as empresas apresentam dificuldades em atrair, reter, recrutar e motivar os trabalhadores com maior talento (Hanin *et al.,* 2013) dada a concorrência que se tem manifestada acentuadamente (Alnıaçık *et al*., 2012) é imperativo encontrar quais as motivações que levam estes profissionais a deixar as organizações atuais.

Sugere-se assim o estudo da seguinte questão de investigação:

1. Quais as motivações que levam os profissionais de cibersegurança a mudar de organização?

É importante saber quais as motivações que levam os profissionais a optar pela cibersegurança face a outras áreas de tecnologias de informação para que possamos entender o que eles procuram quando enveredam por este setor dentro das tecnologias de informação, esta é uma questão pertinente uma vez que permite às organizações terem a oportunidade de criar *job description* adequadas (Stanca *et al*., 2020).

Assim, sugere-se o estudo da seguinte questão de investigação:

2. Quais as motivações que levam os profissionais de cibersegurança a preferir trabalhar nesta área face a outras de tecnologias de informação?

Sabendo que as organizações atuais concorrem para conseguir ter o máximo de sucesso nos processes de atração e retenção para que consigam criar mais valor para a organização (Younas *et al*., 2020), e que para atingirem este máximo de sucesso nos processos de atração e

retenção as organizações devem melhorar a sua gestão de recursos humanos (Kashyap *et al*., 2018), assim como compreender o que os colaboradores atuais preferem de forma a atrair futuros colaboradores e a reter os atuais (Bethke-langenegger *et al*., 2011), sugere-se o estudo da seguinte questão de investigação:

3. Quais as motivações que levam os profissionais de cibersegurança a continuar na empresa onde desempenham funções atualmente?

O *employer branding* é um dos "tópicos mais relevantes das práticas de recursos humanos" (Lievens *et al*., 2016, p. 408) para atrair candidatos e reter os atuais colaboradores, sabe-se também que uma imagem positiva da organização no mercado de trabalho terá um custo de recrutamento muito mais reduzido comparativamente a uma organização no mercado de trabalho com uma imagem negativa (Grzesiuk *et al*., 2018), sabendo também que existem estudos que referem a integração no trabalho (*job embeddedness)* como uma força psicológica que tem o potencial de impedir que os colaboradores deixem a organização (Allen 2006; Holtom *et al,* 2006; Mitchell *et al.,* 2001), sugere-se o estudo da seguinte questão de investigação:

4. Quais os fatores de *employer branding* interno que explicam uma maior integração (*job embeddedness)* no trabalho?

Seguidamente poderá então encontrar a metodologia utilizada para uma resposta eficaz a estas questões de investigação.

Metodologia

A fim de fazer uma dissertação válida, baseada numa reflexão crítica bem fundamentada e verificada, foram utilizados alguns métodos e instrumentos de investigação.

Amostra

- **Entrevistas de saturação**

A amostra foi constituída entre os meses de Março e Abril de 2022 utilizando apenas um critério: serem profissionais de cibersegurança. De acordo com os aspetos definidos, participaram nas entrevistas de saturação 12 profissionais de cibersegurança do sexo masculino, onde 67% dos entrevistados referem ter qualificações superiores ao nível de licenciatura, 8% dos entrevistados referem ter mestrado e 25% dos entrevistados referem ter pós-graduação. Em relação às idades, 25% dos entrevistados referem ter entre os 25 e os 34 anos, 58% dos entrevistados r referem ter entre os 35 e 44 anos, 17% dos entrevistados referem ter entre os 45-54 anos. Todos os entrevistados estão a trabalhar por conta de outrem e efetivos.

Dos participantes, 41,66% dos entrevistados trabalham em cibersegurança há 15 anos, enquanto outros 41,66% trabalham em cibersegurança há 4 anos e 16,68% trabalham na área há mais de 20 anos. Da amostra 58,33% dos entrevistados referiram que já mudaram de emprego apenas três vezes, enquanto 25% já mudaram de emprego seis vezes e 16,67% já mudaram de emprego quatro vezes. Por fim, 50% dos entrevistados referiram que trabalhavam na organização atual há três anos, enquanto 41,66% trabalhavam há um ano e meio e 8,34% há apenas seis meses.

- **Questionário**

A amostra participantes foi constituída entre os meses de Abril a Julho de 2022 utilizando apenas um critério: serem profissionais de cibersegurança. Neste caso a amostra contou com 127 participantes, onde apenas 13 dos participantes pertencem ao sexo feminino. Na análise dos dados sociodemográficos é possível constatar que 39,4% dos inquiridos têm mestrado, 35,4% dos inquiridos têm licenciatura, enquanto 14,2% dos inquiridos têm ensino técnico-profissional, 6,3% dos inquiridos têm qualificações ao nível do ensino secundário via profissional e 4,7% dos inquiridos têm ensino secundário via ensino.

O questionário foi respondido maioritariamente pelo sexo masculino (89,8%) enquanto 10,2% foram respostas do sexo feminino. No que concerne à idade 15,7% dos inquiridos têm

entre 18 e 24 anos, 48% dos inquiridos têm entre 25 e 34 anos, 24,5% dos inquiridos têm entre 35 e 44 anos, enquanto 11,8% dos inquiridos têm entre 45 e 54 anos. Relativamente à situação profissional dos inquiridos, 1,6% encontram-se desempregados, 7,9% a trabalhar por conta própria, 22,8% a trabalhar por conta outrem a prazo e 67,7% a trabalhar por conta outrem efetivo.

No que diz respeito aos anos de experiência profissional em cibersegurança dos inquiridos 37,8% dos inquiridos têm até 2 anos de experiência, 29,8% dos inquiridos têm entre 2 anos e 5 anos, 17,4% dos inquiridos têm entre 6 anos e 9 anos, 6,4% dos inquiridos têm entre 10 anos e 14 anos, 4,7% dos inquiridos têm entre 15 anos e 19 anos, 3,1% dos inquiridos têm entre 20 anos e 24 anos enquanto 0,8% dos inquiridos têm mais de 25 anos de experiência profissional em cibersegurança. Relativamente ao número de vezes que os inquiridos mudaram de emprego desde que desempenham funções em cibersegurança 76,4% dos inquiridos referem entre 1 e 2 vezes, 16,5% dos inquiridos referem entre 3 e 4 vezes, 6,3% dos inquiridos entre 5 e 6 vezes e 0,8% dos inquiridos entre 7 e 8 vezes.

Com relação à antiguidade na empresa atual onde os inquiridos desempenham funções de cibersegurança, 49,6% dos inquiridos referiram entre 1 mês e 1 ano, 23,6% dos inquiridos referiram entre 1 ano e 2 anos, 15% dos inquiridos referiram entre 3 anos e 4 anos, 3,1% dos inquiridos referiram entre 5 anos e 6 anos, 2,4% dos inquiridos indicaram entre 6 anos e 8 anos enquanto 6,3% referem mais de 9 anos.

Podemos concluir que estamos perante uma amostra com qualificações ao nível do ensino superior (74,8%), maioritariamente do sexo masculino (89,6%), no que concerne à idade estão entre os 25 e os 44 anos (72,4%), predominantemente trabalhadores por conta de outrem em regime efetivo (67,7%), com experiencia profissional em cibersegurança até 5 anos (67,7%), que mudou de emprego desde que desempenha funções em cibersegurança entre 1 e 2 vezes (76,4%) e que está na empresa atual onde desempenha funções em cibersegurança entre 1 mês e 2 anos (73,2%).

Procedimento

- **Entrevistas de saturação**

Para o presente estudo, o método de amostragem selecionada para estas entrevistas foi o método de amostragem não aleatório por conveniência. Deste modo as respostas foram obtidas

por meio de contactos pessoais. O único requisito obrigatório para participarem na pesquisa é ser profissional de cibersegurança.

Realizaram-se as entrevistas de saturação com 12 indivíduos que desempenhassem funções em cibersegurança onde foi claramente possível analisar a saturação das respostas obtidas. Estas entrevistas foram realizadas individualmente via *Zoom,* foi gravado o áudio e demoraram em média 30 minutos cada uma.

- **Questionário**

Para o presente estudo, o método de amostragem selecionada para o questionário foi o método de amostragem não aleatório por conveniência em que a divulgação do questionário foi feita em redes profissionais, nomeadamente *LinkedIn* e contou-se ainda com a divulgação no *Twitter* da AP2SI – Associação Portuguesa para a Promoção da Segurança da Informação. O único requisito obrigatório para participarem na pesquisa é ser profissional de cibersegurança.

Para a elaboração das questões do questionário foram utilizados dados recolhidos nas entrevistas de saturação e decidiu-se incluir também a Escala de Integração (*job embeddedness)* no Trabalho de Crossley *et al.,* (2007).

Utilizou-se ainda a ferramenta *GoogleDocs* para alojamento do questionário e ao abrir o *link* para o questionário, os inquiridos foram informados sobre o objetivo e o propósito do estudo. Após concordarem com todas as informações poderiam avançar para a realização do questionário ou para a sua desistência, garantindo assim liberdade de escolha a todos os participantes. Os questionários demoravam em média 10 minutos a serem preenchidos.

Todas as respostas não tratadas são confidenciais, apresentando na presente dissertação os dados recolhidos já tratados pelo programa de análise estatística *IBM SPSS Statistics*.

Seguidamente poderá encontrar os resultados obtidos quer das entrevistas de saturação quer do questionário e a discussão dos mesmos.

Instrumentos

Para a presente investigação usaram-se dois instrumentos de análise.

- **Entrevistas de saturação**

As entrevistas são uma técnica prática de recolha de dados qualitativos, aplicável a pequenas populações, em que são feitas perguntas abertas ou fechadas, nas quais existe uma gama mais vasta de respostas (Kabir, 2016). São utilizadas principalmente para fazer uma análise qualitativa e crítica do tema do estudo.

Realizaram-se estas entrevistas sob forma de se conseguir explorar alguns temas no setor profissional em análise, que viriam depois a constituir questões no questionário posterior.

As primeiras questões feitas nas entrevistas de saturação abordam dados sociodemográficos e caracterização da amostra, sendo que as seguintes questões abordam temas concretos do *employer branding* nas organizações. A primeira questão refere-se ao nível de qualificação, a seguinte ao sexo, posteriormente à idade, seguida do vínculo laboral. Posteriormente questionou-se a cada entrevistado há quanto tempo trabalha em cibersegurança, quantas vezes mudou de emprego desde que desempenha funções em cibersegurança, o que levou a integrar a empresa atual onde desempenha funções de cibersegurança, antiguidade na empresa atual, o que motivou os entrevistados a trabalhar em cibersegurança face a outras áreas de tecnologias de informação, quais as características que procuram numa empresa para terem interesse em trabalhar em cibersegurança nela, se os limites éticos da empresa atual fazem sentir os entrevistados mais ou menos atraídos pela empresa assim como se os limites éticos da empresa os impedem de desempenhar adequadamente as funções de cibersegurança. Seguidamente perguntou-se aos entrevistados se são contactos com frequência com ofertas de empresa, o que os estimula a continuar na empresa atual onde desempenham funções de cibersegurança, os que os fez sair de cada empresa onde já desempenham funções em cibersegurança e que condições são cruciais que a empresa atual deve facultar para continuar a desempenhar funções na mesma. Por fim, perguntou-se também se queriam continuar a desempenhar funções na empresa onde estão atualmente e o que seria necessário existir noutra empresa para deixar aquela onde está atualmente. No anexo A pode encontrar-se o guião das entrevistas de saturação enquanto no anexo B pode ser encontrado os resultados gerais das entrevistas de saturação.

- **Questionário**

O segundo instrumento de investigação foi a realização de um questionário realizado através de um formulário, onde foram feitas perguntas fechadas aos indivíduos em estudo, com menor amplitude de resposta e escalas numéricas claras. As questões presentes no questionário foram obtidas a partir das entrevistas de saturação.

Os questionário s são muito funcionais para quantificação e análise estatística e gráfica de dados, especialmente quando a amostra é de uma população considerável. O instrumento de pesquisa pode ser encontrado no anexo C.

O questionário tem 5 núcleos de questões, tendo o primeiro como propósito avaliar a "atração" numa escada de 5 itens, através dos seguintes preditores:

“Salário acima do valor médio praticado na empresa”; “Suporte da equipa de gestão”; “Projeto aliciante e desafiador”; “Projeto começado de raiz”; Projeto que o fizesse evoluir mais profissionalmente”; “Flexibilidade; “Progressão de carreira”; “Limites ético impostos pela potencial empresa” e “Funções rotineiras na empresa atual”.

No núcleo seguinte tem como propósito avaliar a “motivação” através de uma escala de 5 itens, através dos seguintes preditores:
“Paixão”; “Possibilidade de estar em contacto com os avanços tecnológicos”; “Integração possível com as restantes áreas de tecnologias de informação”; “Aprendizagem continua”; “Gestão de topo desenvolver cibersegurança a par com o negócio” e “Valorização do seu conhecimento”.

Para avaliar a “retenção” numa escala de 5 itens, utilizaram-se os seguintes preditores no instrumento:
“Progressão de carreira”; “Suporte da equipa de gestão”; “Progressão salarial” e “Oportunidades de formação pela empresa”.

Seguidamente utilizou-se o instrumento de Crossley *et al.,* (2007) que pretende medir a integração (*job embeddedness***)** na empresa, também com uma escala de 5 itens, que apresenta as seguintes questões:
“Sinto-me ligado/a a esta organização”; “Seria para mim difícil deixar esta organização”; “Estou demasiado envolvido/a nesta organização para a deixar”; “Sinto-me vinculado/a a esta organização”; “Simplesmente não conseguiria deixar a organização onde trabalho”; “Seria muito fácil para mim deixar esta organização” e “Estou intimamente ligado/a a esta organização”.

No presente instrumento de Integração (*job embeddedness*) no Trabalho de Crossley *et al*. (2007) com uma escala de 1 a 5, onde 1 significa “discordo totalmente”; 2 “discordo”; 3 “não concordo, nem discordo” 4 “concordo” e 5 “concordo totalmente”, após recodificação da variável “Seria muito fácil para mim deixar esta organização”, optou-se também por retirar a variável “Seria para mim difícil deixar esta organização” uma vez que esta apresentava valores muito próximos que comprometiam a investigação.

Seguiu-se assim para a analise fatorial, da qual resultou 1 único fator que explica 44,65% da percentagem de variância explicada e apresenta um Alpha de Cronbach de 0,809. Perante estes dados optou-se por utilizar a regressão linear para avaliar a escala de Integração (*job embeddedness*) no Trabalho de Crossley *et al.,* (2007) com as questões que avaliam os fatores que os profissionais de cibersegurança têm em conta para continuar a desempenhar funções na empresa atual.

Resultados

Primeiramente começaremos por apresentar os resultados das entrevistas de saturação, sendo estes seguidos pelos resultados dos inquéritos.

- **Entrevistas de Saturação**

As características que estes profissionais esperam encontrar numa empresa para motivá-los a desempenhar funções em cibersegurança nessa empresa 58,34% dos entrevistados referiram a flexibilidade, autonomia e suporte da gestão como se pode ler na seguinte transcrição*"(...) a flexibilidade e a autonomia que tenho assim como o suporte da gestão é o que me motiva a continuar as minhas funções na empresa atual, repare que esta profissão é muito critica e se a equipa de gestão não entender as necessidades não conseguimos estar motivados (...)"* enquanto os restantes 41,66% referiram o suporte da equipa de gestão como se posso observar na seguinte transcrição *"(...) o que dita as regras da motivação na empresa é o fato da equipa de gestão apoiar e seguir as nossas recomendações, porque se recomendarmos algo mas a gestão não seguir como podemos continuar motivados se não se interessam pelo que alertamos? (...)"*.

De facto, quando questionados sobre o que os motiva a permanecer nestas empresas, 58,34% dos entrevistados afirmaram o fato da gestão da empresa compreender a importância da cibersegurança e desenvolvê-la a par do negócio como se pode ler nas seguintes transcrições*"(...) a gestão da empresa tem que compreender que cibersegurança é um novo requisito organizacional, sem a gestão compreender a nossa importância não estamos ali a fazer nada (...)"* e *"(...) cibersegurança é tão importante quanto o próprio negocio da empresa, porque sem ciber o negócio pode acabar em segundos caso exista algum ataque* (...)" , enquanto os restantes 41,66% dos entrevistados referem que o que os motiva a permanecer na empresa é a aprendizagem continua como é possível ler nas seguintes citações: *"(...) o que me faz permanecer na empresa atual a aprendizagem contínua no meu dia a dia (...)"* e "*(...) a aprendizagem continua que a empresa me oferece é o que me faz ficar (...)"*. Ainda, o fator que motivou a deixar organizações anteriores 58,34% dos entrevistados referem ter sido o salário como é possível ler na seguinte transcrição: *"(...) o salário foi o que me fez mudar, em todas as empresas onde estive o salário sempre foi o que levou a mudar de empresa para empresa (...)"*, para os outros 25% dos entrevistados a falta de projetos que lhes permitam continuar a crescer profissionalmente como se pode ler na seguinte transcrição "*(...) o que me fez deixar as antigas empresas foi o fato de estar estagnado no projeto em que estava e sempre*

que falava com as chefias negavam-me oportunidades de crescimento, então decidi sair (...)" e 16,66% dos entrevistados mencionaram falta de apoio da gestão *"(...) a falta de apoio da equipa que te lidera corrói a tua motivação e começas a olhar para outras oportunidades (...)"*.

Quando questionados sobre o que os levou a integrar a empresa atual onde desempenham funções de cibersegurança, 92% dos entrevistados referiram o fato de ser um projeto desafiador a par de um salário adequado e do suporte da equipa de gestão *"(...) o que trouxe para esta empresa foi a conjunção de uma serie de fatores, o suporte da chefia que é incrível, o projeto ser totalmente desafiador e a par com isso um salário adequado à minhas atuais funções e experiência (...)"* e *"(...) além de um salário e um projeto que seria impossível recusar, o fato da equipa de gestão apoiar incondicionalmente e ser como um conselheiro de segurança para a gestão é o que me levou a integrar a empresa onde estou (...)"*, enquanto 8% dos entrevistados referiram começar um projeto de raiz como é possível observar na seguinte transcrição *"(...) iniciar algo de raiz foi o que me motivou e me trouxe para esta empresa, foi algo que sempre quis fazer dedicar-me a um projeto começado do zero (...)"*. Em relação ao que os motiva face a outras áreas de tecnologias de informação para preferirem trabalhar em cibersegurança todos os entrevistados referiram a paixão pela área, sendo que é das poucas onde têm a possibilidade de estar em contato com os avanços da tecnologia e ao mesmo tempo ter interação com as restantes áreas de tecnologias de informação como é possível ler nas seguintes citações *"(...) prefiro cibersegurança a outras áreas de tecnologias de informação primeiro porque consigo estar em contato com as novidades tecnológicas e continuar a par dos desenvolvimentos das outras áreas e também porque sou apaixonado por esta área (...)"* e *"(...) o fato de estar em cibersegurança e poder estar com contacto com as outras áreas e trabalhar em conjunto com elas durante os projetos é algo que me fascina, porque não estou colocado apenas numa área onde só me relaciono dentro dela e com as tecnologias dela. Estou em contato permanente com outras áreas e desenvolvo projetos com elas, o que me permite conhecer novas tecnologias, além disso esta área sempre foi o meu sonho sou completamente apaixonado por tudo o que cibersegurança representa (...)"*.

Quando inquiridos sobre se os limites éticos da empresa em que estão os fazem sentir-se mais ou menos atraídos pela empresa todos referiram sentir-se mais atraídos como é possível ler na seguinte transcrição *"(...) os limites éticos das empresas são muito importantes e valorizados, não vale tudo numa guerra cibernética (...)"*, enquanto que quando inquiridos se os limites éticos se tornavam impeditivos para desempenharem as funções adequadamente todos referiram que não, como é possível observar *"(...) os limites éticos não são impeditivos para desempenhar as tarefas até porque nunca me pediram para fazer nada que metesse em risco os mesmos (...)"*.

Sobre as condições cruciais que a empresa atual deve facultar para continuarem a desempenhar as funções em cibersegurança 84% dos entrevistados referiram a progressão salarial, as perspetivas de progressão de carreira e o suporte das equipas de gestão, como é possível observar na seguinte transcrição *"(...) manter o suporte da gestão é essencial, assim como dado o mercado competitivo em que estou e que sou aliciado várias vezes é importante que a empresa não fique parada no tempo sem rever a progressão de carreira e a progressão salarial, são os meus 3 tópicos essenciais para continuar na empresa atual em cibersegurança (...)"* e *"(...) é necessário que todos os anos continuem a rever a progressão salarial e a progressão de carreira, bem como a gestão mantenha interesse e apoie o departamento de cibersegurança (...)"* enquanto que 16% dos entrevistados referiram o fato de continuarem a ter oportunidade de fazer formação na área pela empresa onde trabalham, como possível ler na transcrição *"(...) as oportunidades de formação em cibersegurança são, para mim, o que me faz continuar na empresa porque são formações de valores económicos muito elevados e para continuar a fazer um bom trabalho preciso destas formações (...)"*. Por fim, todos os inquiridos referem que querem continuar na empresa atual e que o que seria necessário para sair da entidade onde estão atualmente seria um melhor kit salarial e um projeto que os permitisse evoluir mais profissionalmente, como se pode ler nas seguintes transcrições "*(...) tenho todas as condições na empresa atual e só me vejo a sair no caso de surgir um projeto que me permita evoluir mais e ter um melhor salário (...)"* e *"(...) não quero sair da empresa porque me sinto bem onde estou e tenho todo o suporte necessário para desempenhar as minhas tarefas mas se saísse seria certamente por ser um projeto mais desafiante e por um salário melhor."*

- **Análise quantitativa**

Para analisar os resultados do questionário, a primeira coisa a considerar são as questões do instrumento de pesquisa.

No primeiro conjunto de questões, referente à atração, após ser feita uma análise fatorial exploratória e análise de consistência interna os resultados apresentaram dados que não sugeriam o agrupamento de fatores, deste modo, optou-se pela análise de item a item.

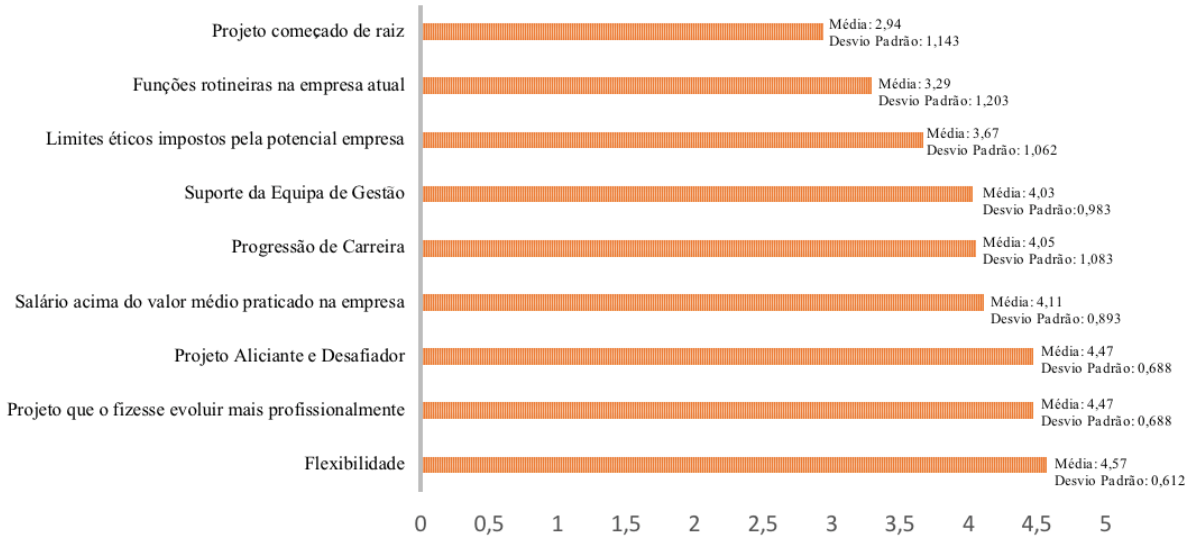

Figura 1 Quais as motivações que levam os profissionais de cibersegurança a mudar de organização?

Fonte Própria

De acordo com a figura 1 apresentada acima é possível afirmar-se que de acordo com os dados recolhidos as motivações em ordem decrescente que levam os profissionais de cibersegurança a mudar de organização são primeiramente questões de "flexibilidade" (M ≈ 4,57); inferiormente "projetos que fizessem evoluir mais profissionalmente" (M ≈ 4,47) e "projetos alicantes e desafiadores" (M ≈ 4,47); seguidamente "salário acima do valor médio praticado na empresa" (M ≈ 4,11); segue-se "progressão de carreira" (M ≈ 4,05); depois "suporte da equipa de gestão" (M ≈ 4,03); para finalizar as 3 últimas motivações que menos influenciam os profissionais de cibersegurança a mudar de organização são "limites éticos impostos pela potencial empresa" (M ≈ 3,67); seguido de "funções rotineiras na empresa atual" (M ≈ 3,29) e por fim, a motivação que menos influência os profissionais de cibersegurança a mudar de organização é o "projeto começado de raiz" (M ≈ 2,94).

No segundo conjunto de questões, referente à motivação, após ser feita uma análise fatorial exploratória e análise de consistência interna os resultados apresentaram dados que não sugeriam o agrupamento de fatores, deste modo, optou-se pela análise de item a item.

Com esta análise pretende responder-se à seguinte questão de investigação:

1. Quais as motivações que levam os profissionais de cibersegurança a preferir trabalhar nesta área face a outras de tecnologias de informação?

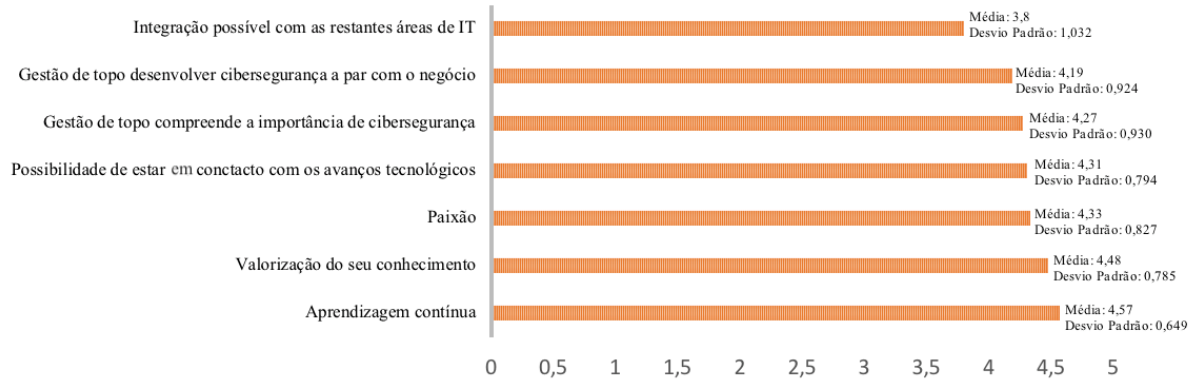

Figura 2 Quais as motivações que levam os profissionais de cibersegurança a preferir trabalhar nesta área face a outras de tecnologias de informação?

Fonte própria

De acordo com a figura 2 apresentada acima é possível afirmar-se que, de acordo com os dados recolhidos as motivações em ordem decrescente que levam os profissionais de cibersegurança a preferir trabalhar nesta área face a outras das tecnologias de informação são primeiramente questões de "aprendizagem contínua" (M ≈ 4,57). Seguidamente "valorização do conhecimento" (M ≈ 4,48); seguido da "paixão" (M ≈ 4,33). Posteriormente a quarta motivação que menos influencia os profissionais a preferir trabalhar nesta área face a outras de tecnologias de informação é a "possibilidade de estar em contacto com os avanços tecnológicos" (M ≈ 4,31); seguido da "gestão de topo compreender a importância de cibersegurança" (M ≈ 4,27); posteriormente da "gestão de topo desenvolver cibersegurança a par com o negócio" (M ≈ 4,19) e por fim, a "integração possível com as restantes áreas de tecnologias de informação" (M ≈ 3,80).

No terceiro conjunto de questões, referente à retenção, após ter sido realizada a análise fatorial exploratória e a análise de consistência interna, foram apresentaram dados que não sugeriam o agrupamento de fatores, assim irão ser analisados item a item.

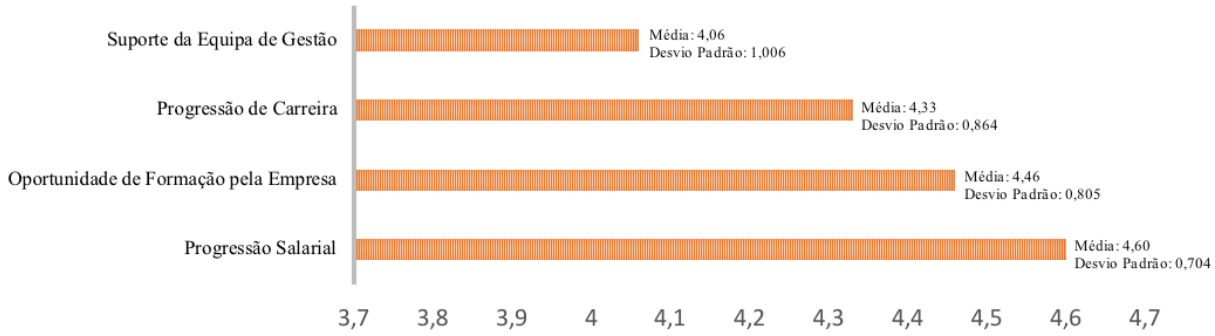

Figura 3 Quais as motivações que levam os profissionais de cibersegurança a continuar na empresa onde desempenham funções atualmente?

Fonte própria

De acordo com a figura 3 apresentada acima é possível constatar que, de acordo com os dados as motivações em ordem decrescente que levam os profissionais de cibersegurança a continuar na empresa onde desempenham funções atualmente são primeiramente questões de "progressão salarial" (M ≈ 4,60); seguida de "oportunidades de formação pela empresa" (M ≈ 4,46); posteriormente "progressão de carreira" (M ≈ 4,33) e por fim o "suporte da equipa de gestão" (M ≈ 4,06).

		B	**SE**	**β**	**t**	***p***
Integração (*job embeddedness*) no Trabalho		2,207	0,664		3,323	0,001
	Progressão de Carreira	0,005	0,116	0,005	0,043	0,965
	Suporte da Equipa de Gestão	0,200	0,096	0,210	2,074	0,040
	Progressão Salarial	-0,080	0,131	-0,059	-0,609	0,544
	Oportunidades de Formação pela Empresa	0,161	0,117	0,135	1,374	0,172

Nota: R^2= 0,273, Δ R^2=0,075

Nota: B = coeficientes não padronizados; *β* = coeficientes padronizados; SE = desvio-padrão; t = teste t; *p* = teste de significância

Tabela 1 Regressão Linear entre a Integração (job embeddedness) no Trabalho e os fatores que os profissionais de cibersegurança têm em conta para continuar na empresa atual (employer branding interno).

Fonte própria adaptado do SPSS

Para responder a esta questão, foi necessário efetuar uma regressão linear que analisa a escala de Integração (*job embeddedness*) no Trabalho de Crossley *et al.,* (2007) com as questões realizadas no terceiro conjunto de questões que avaliam os fatores que os profissionais de cibersegurança têm em conta para continuar a desempenhar funções na empresa atual (*employer branding interno*).

Através dos dados obtidos consegue-se observar que o que único fator que influencia a integração (*job embeddedness*) no trabalho e está correlacionada é o suporte da equipa de gestão (*β*=0,200, *p*=0,040). Visto que o valor de "*p*" se apresenta inferior ao alfa (α=0,05), portanto destas variáveis dependentes apenas uma possui capacidade explicativa da variável

integração no trabalho. A variância da variável dependente (i.e. integração no trabalho (*job embeddedness*)) explicada pelo modelo é pequena, igual a 2,7% (R^2= 0,273).

Seguidamente poderá encontrar a discussão dos resultados.

Discussão dos Resultados

A presente investigação pretende avaliar o que é mais valorizado pelos profissionais de cibersegurança relativamente a algumas preditores de *employer branding* de forma a compreender os fatores que são mais valorizados pelos profissionais em questão. Pretende-se também que com o presente estudo entender quais os preditores que levam os profissionais de cibersegurança a deixar as suas empresas atuais uma vez que cada saída de uma organização representa um elevado custo no processo de recrutamento e formação de um novo profissional (Pflügler *et al.,* 2018) e existe uma elevada dificuldade em atrair e reter talentos na área das tecnologias de informação (Hanin *et al.,* 2013).

Relativamente à primeira questão de investigação ("Quais as motivações que levam os profissionais de cibersegurança a mudar de organização?") é possível observar no gráfico que o mais valorizado é a "flexibilidade" ($M \approx 4,57$). Uma organização ao ser flexível no trabalho oferece aos colaboradores flexibilidade durante o horário laboral. Sabemos que flexibilidade numa organização permite aos trabalhadores escolher onde e quando o trabalho é realizado, e quem toma essa decisão é o empregado e não o empregador. Os dados apresentados corroboram com o estudo de Ishmael *et al.,* (2022), onde 100% dos seus inquiridos afirmam que o principal fator para continuar ou mudar de organização é justamente a flexibilidade permitida pelo empregador. Ainda no estudo de Ishmael *et al.,* (2022), 94% dos inquiridos referem que sentirem-se honrados e orgulhosos com o seu trabalho é o segundo maior fator de retenção de talento, isto vai de encontro aos dados do questionário realizado na presente investigação em que "projetos que fizessem evoluir mais profissionalmente" ($M \approx 4,47$) e "projetos aliciantes e desafiador" ($M \approx 4,47$) são as duas motivações, após a flexibilidade, que levam os profissionais de cibersegurança a mudar de organização. Pelo que se estes estiverem envolvidos em desafios aliciantes e que os façam evoluir mais irão sentir-se orgulhosos e honrados.

Também Singh (2019) refere que os acordos de trabalho flexíveis ajudam a retenção dos colaboradores e ajudam os mesmos a equilibrar a vida pessoal com a profissional assim como promover a felicidade. O mesmo autor afirma que flexibilidade resulta ainda em menos absentismo dos trabalhadores. Atualmente as organizações tentam recrutar e ter o melhor talento numa ambiente que se encontra extremamente competitivo, pelo que devem melhorar os seus processos de recrutamento (Hanin *et al.,* 2013), sabendo que o objetivo de atrair e reter os colaboradores está inteiramente relacionado com compreender as necessidades destes (Bethke-langenegger *et al.*, 2011) consegue entender-se que é crucial que as organizações que

visam reter os seus talentos em cibersegurança devem adotar primeiramente estratégias de flexibilidade como principal ajuda para os reter, seguido de projetos que os fizessem evoluir mais profissionalmente a par com projetos aliciantes e desafiadores. Estas estratégias devem ser utilizadas no *employer branding* interno na organização para reter talento, mas também devem ser comunicadas para atrair cada vez mais talento.

Na segunda questão de investigação ("Quais as motivações que levam os profissionais de cibersegurança a preferir trabalhar nesta área face a outras de tecnologias de informação?") é possível observar na figura que a principal motivação destes profissionais para preferirem trabalhar nesta área face a outras dentro das tecnologias de informação é primeiramente a "aprendizagem continua" ($M \approx 4,57$) , seguido da "valorização do seu conhecimento" ($M \approx 4,48$).

Embora exista pouca literatura dedicada a cibersegurança que consiga apoiar os resultados obtidos, Oltsik (2017) identifica o que levou os atuais profissionais de cibersegurança a entrarem para esta área. Nessa investigação é possível constatar que quase metade (47%) dos participantes ingressaram para cibersegurança face a outras áreas das tecnologias de informação para ter oportunidade para desenvolver as suas habilidades e curiosidades, o que está alinhado com o fator da aprendizagem contínua ser algo que motiva os profissionais de cibersegurança a preferir trabalhar na área comparativamente a outras de tecnologias de informação. Embora esta questão não esteja relacionada com o *employer branding* tal permite-nos rastrear e entender o que atrai os profissionais para esta área em questão.

Perante a terceira questão de investigação ("Quais as motivações que levam os profissionais de cibersegurança a continuar na empresa onde desempenham funções atualmente?") sabendo que o que conduz os profissionais a ficarem na empresa atual deve-se primeiramente a questões de "progressão salarial" ($M \approx 4,60$), seguidas de "oportunidades de formação pela empresa" ($M \approx 4,46$) conseguimos constatar que estes dois temas são algo que devem requerer uma atenção especial para reter estes profissionais. Segundo Ishmael *et al.,* (2022), a sua investigação demonstra existirem 4 pilares de retenção de profissionais de cibersegurança: apoio e compromisso organizacional; oportunidades de formação e progressão de carreira; flexibilidade e reconhecimento. A investigação de Orye *et al.,* (2021), indica-nos que as respostas mais respondidas pelos profissionais de cibersegurança quando perguntados sobre as motivações para permanecer numa organização primeiramente referem as oportunidades de formação pela empresa e seguidamente a progressão salarial, o que vai de encontro ao presente estudo embora neste esteja primeiramente referenciada a progressão salarial seguida das oportunidades de formação pela empresa.

Em relação à quarta questão de investigação ("Quais os fatores de *employer branding* interno que explicam uma maior integração (*job embeddedness)* no trabalho?") é possível observar que o "suporte da equipa de gestão" (β=0,200, p=0,040) é o principal fator que explica uma maior integração (*job embeddedness)* no trabalho. Tais dados são também suportados pela ISC² (2022), em que suporte da equipa de gestão é o segundo motivo que os profissionais de cibersegurança consideram afetar mais negativamente a sua satisfação no trabalho, podendo influenciar a sua decisão de permanecer na empresa.

Perante estes dados consegue identificar-se que, em média, os fatores de *employer branding* que as organizações devem ter em atenção para atrair e reter estes talentos são flexibilidade, projetos que os fazem evoluir mais profissionalmente, projetos aliciantes e desafiadores, progressão salarial, oportunidades de formação pela empresa e o suporte da equipa de gestão.

Seguidamente poderá encontrar as implicações da investigação.

Implicações da investigação

Uma vez que as organizações necessitam de um ambiente colaborativo que vise reter os atuais talentos (Nayak, 2017) é importante compreender as motivações que conduzem os profissionais de cibersegurança. Deste modo, esta investigação apresenta contribuições teóricas para este setor profissional, uma vez que acrescenta informações sobre um setor profissional ainda pouco estudado cientificamente.

O presente estudo não apresenta hipóteses de evidência empírica, mas com recurso a médias é possível observar os preditores que são mais valorizados por este setor profissional. Este estudo pretende assim alertar as organizações que têm profissionais de cibersegurança na sua estrutura e dar-lhes ferramentas para que possam melhorar a atração de potenciais colaboradores e reter os atuais talentos. Estes resultados podem conduzir as organizações a vantagens competitivas perante outras que não disponham de tais informações (Bohlmann *et al*., 2016).

De acordo com os métodos de pesquisa aplicados, desde a revisão de literatura até aos instrumentos de pesquisa, cujos resultados foram analisados e discutidos anteriormente, conseguimos constatar que este estudo apresenta várias implicações práticas. É possível observar que as motivações mais valorizadas pelos profissionais de cibersegurança nas empresas, e que são por isso, as ferramentas fundamentais para atrair e reter este tipo de talentos, são principalmente a flexibilidade, a progressão salarial e a aprendizagem contínua.

Nos fatores analisados de *employer branding* interno comparativamente entre progressão de carreira; suporte da equipa de gestão; progressão salarial e oportunidades de formação pela empresa, o fator que explica maior integração (*job embeddedness)* no trabalho é o suporte da equipa de gestão. Podemos assim verificar que dos fatores analisados o suporte da equipa de gestão é o que se destaca para que os profissionais de cibersegurança não saiam das suas organizações atuais. Desta forma, o presente estudo indica que para atrair e reter estes profissionais é necessário promover flexibilidade, políticas de progressão salarial e aprendizagem continua assim como incutir às lideranças que estes profissionais vêm o suporte das mesmas como um fator crítico que os pode conduzir à saída da organização.

Seguidamente poderá encontrar as limitações do presente estudo e sugestões para futuras investigações.

Limitações e Sugestões

Apesar do presente estudo contribuir para um avanço na literatura, na fase final desta investigação, consegue-se identificar algumas limitações encontradas ao longo da investigação bem como identificar algumas recomendações e sugestões para futuras investigação relacionadas com este tema.

A presente pesquisa teve um conjunto de limitações operacionais que podem levar à existência de alguma margem de erro nos resultados obtidos. Tais limitações podem ser resumidas, em primeiro lugar, ao número reduzido da amostra em estudo (N=127). O facto de estarmos dentro do ramo de tecnologias de informação que só por si apresenta poucos estudos sobre a retenção destes profissionais (Kori *et al.,* 2018) e limitarmos ainda mais a pesquisa apenas para o setor profissional de cibersegurança fez com que não fosse possível chegar a um número maior de inquiridos, certamente os resultados poderiam ter algum padrão diferente com uma amostra maior com menor margem de erro.

O questionário ter derivado das entrevistas de saturação pode constituir também outra possível limitação, em que dada a amostra ser reduzida e o método de amostragem não probabilístico por conveniência, pode originar qualquer tipo de enviesamento nas entrevistas de saturação que condicionam o instrumento de investigação do questionário (Elliott *et al*., 2007) .

O fato do questionário ter sido disponibilizado apenas na língua portuguesa o que fez com que só respondessem pessoas que dominavam ao supra citada língua, pelo que para uma investigação futura poderá ser utilizada a tradução do questionário (Schmidt *et al*., 2016) para

que se possam analisar e comparar diferenças face a outros países. Sem um maior número de inquiridos e respostas de outros países não é possível generalizar os resultados obtidos no presente estudo (Bettencourt *et al*., 2003; Karatepe *et al.,* 2012; Singh, 2000).

Pode ser também considerada uma limitação o fato de termos poucas profissionais do sexo feminino (N=13), a responder ao questionário (N=127), contudo é uma limitação existente no mercado de trabalho atual onde este setor profissional é maioritariamente composto por profissionais do sexo masculino (ISC², 2022).

Uma vez que este setor profissional é recente (Haney *et al.,* 2019) a falta de estudos aplicados aos profissionais de cibersegurança limitou a revisão de literatura e a discussão de resultados. Deste modo, sugere-se que sejam realizadas mais investigações neste setor profissional sob forma de colmatar esta falha literária.

Poderá ser interessante analisar numa futura investigação se as diferenças entre gerações representam alterações nos resultados das questões de investigação, sabendo que atualmente são várias as gerações que se cruzam no mercado de trabalho será vantajoso saber quais os preditores mais valorizados de *employer branding* por cada uma das gerações para que as organizações possam adequar as suas estratégias de *employer branding* por classes geracionais.

Deverá ser também interessante analisar se as respostas conforme a nacionalidade dos inquiridos apresenta algum padrão nos resultados das questões de investigação para se conseguir assim entender o que os profissionais de cibersegurança mais valorizam em termos de preditores do *employer branding* em cada país comparativamente com outros.

Apesar das limitações referidas acima, considera-se que os resultados deste estudo potenciam novos conhecimentos acerca deste setor profissional, que comparativamente com o setor de tecnologias de informação encontra-se ainda pouco estudada.

Seguidamente poderá encontrar as conclusões do presente estudo.

Conclusões

Uma dissertação, desenvolve-se como uma oportunidade de questionar se algo é um fato existente e se conseguimos comprovar o mesmo. Representa um exercício de reflexão científico, com a qual se procura responder a uma questão colocada ou, como neste caso, a várias questões de investigação. É também um exercício informativo, argumentado através de referências bibliográficas de diversas fontes de autores reconhecidos na área.

Em relação ao tema abordado, pode-se dizer que devido à crise económica global originada pela pandemia covid-19, as formas de retenção do talento interno das empresas foram transformadas, bem como aquelas para atrair e reter os melhores profissionais de diferentes áreas. Foi nesta fase histórica sem precedentes que o *employer branding* voltou a ser uma tendência, tendo como principal objetivo posicionar as organizações como empregadores atrativos no mercado de trabalho atual, cada vez mais digitalizado e diversificado.

O mercado de trabalho está cada vez mais complexo e exigente, principalmente quando se trata das áreas tecnológicas onde a procura por profissionais qualificados aumenta cada vez mais, enquanto em comparação, o número destes profissionais não é suficiente para fazer face à procura. Dado isto, é muito importante que as organizações de hoje, se quiserem permanecer ao longo do tempo em vez de desaparecerem no meio de tantos avanços tecnológicos, desenvolvam a capacidade de se adaptar aos novos formatos de trabalho digital e às necessidades dos futuros colaboradores e das novas gerações, que procuram uma oferta de trabalho abrangente que lhes permita estabilidade económica, emocional, mental e social.

Da mesma forma, estas empresas devem focar-se no desenvolvimento de um processo estratégico que posicione a sua marca como uma boa referência para trabalhar no mercado de trabalho, não sendo apenas boas no que vendem, mas também no que representam como entidade empregadora.

Sabendo que estamos numa era digital onde a informação é constantemente partilhada e o bem mais valioso, espera-se com o presente estudo conseguir ajudar as empresas a conhecerem exatamente o que os profissionais de cibersegurança mais valorizam para que estas consigam ajustar o que oferecem a este setor profissional e consequentemente atrair e reter talento deste setor profissional.

Referências

Aggerholm, H., Andersen, S. E., & Thomsen, C. (2011). Conceptualising employer branding in sustainable organisations. *Corporate Communications*, 16(2), 105-123. Doi: 10.1108/13563281111141642

Agrawal, R. K., & Swaroop, P. (2009). Effect of Employer Brand Image on Application Intentions of B-SchoolUndergraduates. *The Journal of Business Perspective*, 13(3), 41–49.

Ahmad, N. A., & Daud, S. (2016). Engaging people with employer branding. *Procedia Economics and Finance*, 35, 690-698.

Ainspan, N. & Dell, D., (2001). "Engaging employees through your brand. In: *Conference Board Report*, Washington, D.C., No. R- 1288-01 RR.

Allen, D. (2006) "Do organization socialization tactics influence newcomer embeddedness and turnover?". *Journal of Management*, (32), 237-256.

Alniaçik, E., & Alniaçik, U. (2012). Identifying Dimensions of Attractiveness in Employer Branding: Effects of Age, Gender, and Current Employment Status. *Procedia - Social and Behavioral Sciences*. 58. 1336-1343. Doi:10.1016/j.sbspro.2012.09.1117.

Álvarez, D., & Ojeda, F. (2017). Labor branding a factor considered for the attraction and retention of personnel in Celaya Guanajuato. *Caderno Professional Marketing Magazines* - Unimep, 05 (02), 1 - 14. Retrieved from http://www.cadernomarketingunimep.com.br/ojs/index.php/cadprofmkt/article/view/101/80 (visitado em 05 de abril , 2022).

Ambler, T., & Barrow, S. (1996). The employer brand. Journal of brand management, 4(3), 185-206.

Austin, J. T., & Villanova, P. (1992). The criterion problem: 1917–1992. *Journal of Applied Psychology*, 77(6), 836.

Barrow, S. & Mosley, R. (2005). The employer brand. Bringing the best of brand management to people at work. London: Wiley & Sons, Ltd.

Barrow, S., & Mosley, R. (2011). The Employer Brand (1st ed.). *Wiley*. Retrieved from: https://www.perlego.com/book/1005944/the-employer-brand-bringing-the-best-of-brand-management-to-people-at-work-pdf (visitado em 10 de Março , 2022).

Beauregard, T. & Henry, L. (2009). Making the Link between Work-Life Balance Practices and Organizational Performance. *Human Resource Management Review*. 19. 9-22. Doi:10.1016/j.hrmr.2008.09.001.

Bernal, I., Pedraza, N. A., & Sánchez, M. L. (2015). The organizational climate and its relationship to the quality of public health services: Design of a theoretical model. *Estudios Gerenciales,* 31(134), 8-19.

Bethke-langenegger, P., Mahler, P., & Staffelbach, B. (2011). Effectiveness of talent management strategies. 5(5), 524–539

Bettencourt, L. A., & Brown, S. W. (2003). Role stressors and customer-oriented boundary-spanning behaviors in service organizations. *Journal of the Academy of Marketing Science*, 31(4), 394–408. Doi:10.1177/0092070303255636

Blasco-López, M.F., Rodríguez-Tarodo, A. & Fernandez-Lores, S. (2014). Employer branding: A multinational research on the construction of employer brand. *Universia Business Review*. 34-53.

Bohlmann, C., Krumbholz, L. & Zacher, H. (2018). The Triple Bottom Line and Organizational Attractiveness Ratings: The Role of Pro-Environmental Attitude. *Corporate Social Responsibility and Environmental Management*. 25. Doi:10.1002/csr.1507.

Brynjolfsson, E. (1993). The productivity paradox of information technology. *Communications of the ACM*, 36(12), 66-77.

Bureau of Labor Statistics (2022). *US Department of Labor, Occupational Outlook Handbook , Information Security Analysts. R*etrieved from: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm (visitado em 05 de outubro , 2022).

Caldwell, T. (2013). Plugging the cyber-security skills gap. *Computer Fraud & Security*. 2013. 5–10. Doi:10.1016/S1361-3723(13)70062-9.

Campanário, C. (2014). Employer Branding: "Make" the difference as an employer to retain and attract the best talent. Retrieved from: http://carmencampanariolopez.blogspot.com/2014/06/employer-branding-marca-la-diferenca.html (visitado em 05 de outubro, 2022).

Cano, J. J. (2020). Retos de seguridad/ciberseguridad em el 2030. *Sistemas,* (154), 68-79.

Centro Nacional de Cibersegurança. (2019). Estratégia Nacional de Segurança no Ciberespaço. Retrieved from: https://www.cncs.gov.pt/docs/cncs-ensc-2019-2023.pdf (visitado em 05 de outubro , 2022).

Chiang Vega, M. M., Salazar, C. M., Huerta, P. C., & Nuñez, A. (2008). Clima organizacional y satisfacción laboral en organizaciones del sector estatal (Instituciones públicas) Desarrollo, adaptación y validación de instrumentos. *Universum* (Talca), 23(2), 66-85.

Cisco, (2021) *"Global Network Trends Report 2021».* Retrieved from: https://www.cisco.com/c/dam/global/es_mx/solu- tions/pdf/2021-networking-report.pdf (visitado em 05 de outubro, 2022).

Corral, J. (2007). Dirección de personas: Escuchar, influenciar y desarrollar a los colaboradores. *La Coruña: Netbiblo*.

Cremer, F., Sheehan, B., & Fortmann, M. (2022) Cyber risk and cybersecurity: a systematic review of data availability. *Geneva Pap Risk Insur Issues* Pract 47, 698–736. Doi:10.1057/s41288-022-00266-6

Crossley, C. D., Bennett, R. J., Jex, S. M., & Burnfield, J. L. (2007). Development of a global measure of job embeddedness and integration into a traditional model of voluntary turnover. *Journal of Applied Psychology*, 92(4), 1031-1042. Doi:10.1037/0021-9010.92.4.1031

Cújar, A. D. C., Hernández, H. E., Ramos, C. D., & López, J. M. (2013). Cultura organizacional: evolución en la medición. *Estudios gerenciales*, 29(128), 350-355.

Di Girolamo, S. (2015). Global talent management: Challenges and strategies of Spanish multinationals. Retrieved from: https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/4390/TFG001227.pdf?sequence=1&isAllowed=y (visitado em 05 de outubro, 2022).

Díaz, F. J., Molinari, L. H., Venosa, P., Macia, N., Lanfranco, E. F., & Sabolansky, A. J. (2018). Investigación en ciberseguridad: un enfoque integrado para la formación de recursos de alto grado de especialización. *XX Workshop de Investigadores en Ciencias de la Computacion*, 1056-1060.

Döckel, A. (2003). The effect of retention factors on organisational commitment: An investigation of high technology employees. Unpublished MCom dissertation (Human Resources Management), *University of Pretoria*.

Duarte, M. (2016). Is Talent seduced? Retrieved from: https://www.gestiopolis.com/talento-se-seduce/ (visitado em 05 de abril , 2022).

Elliott, M., Haviland, A. (2007). Use of a Web-Based Convenience Sample to Supplement a Probability Sample. *Survey Methodology.* 33. 211-215.

Estrada, J. G., Pupo, J. C., Machado, Y. B., & Cañedo, R. (2009). Clima y cultura organizacional: dos componentes esenciales en la productividad laboral. *Acimed,* 20(4), 67-75.

Figurska, I., & Matuska, E. (2013). Employer branding as a human resources management strategy. Human resources management & Ergonomics, 7(2).

Fitzgerald, M., Kruschwitz, N., Bonnet, D., & Welch, M. (2014). Embracing digital technology: A new strategic imperative. *MIT slogan management review,* 55(2), 1.

Fortinet, 2022 Cybersecurity skills gap (2022). Retrieved from: https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf (visitado em 05 de outubro , 2022).

Foster, C., Punjaisri, K., & Cheng, R. (2010). Exploring the relationship between corporate, internal and employer branding. *Journal of Product & Brand Management.*

García, F. P. (2021). Una aproximación a la Ciberseguridad en Sistemas de Control Industrial. *Puente de Hierro,* 1(1), 12-12.

Gilley, A., Waddell, K., Hall, A., Jackson, S. A., & Gilley, J. W. (2015). Manager behavior, generation, and influence on work-life balance: An empirical investigation. *Journal of Applied Management and Entrepreneurship*, 20(1), 3.

Gomes, D. R., & Neves, J. (2010). Employer branding constrains applicants' job seeking behaviour? *Revista de Psicología del Trabajo y de las Organizaciones*, 26(3), 223-234.

Grzesiuk, K., & Wawer, M. (2018). Employer Branding Through Social Media: the Case of Largest Polish Companies. Doi:10.3846/bm.2018.42

Gutiérrez, S., Montañez, G., & Santamaría, C. (2017). La Responsabilidad Social y la Cultura Organizacional en las Empresas Familiares. *Neumann Business Review,* 4 - 22.

Haney, J. M., & Lutters, W. G. (2019). Motivating cybersecurity advocates: Implications for recruitment and retention. *Computers and People Research Conference*, 109-117).

Hanin, D., Stinglhamber, F., & Delobbe, N. (2013). The impact of employer branding on employees: The role of employment offering in the prediction of their affective commitment. *Psychologica Belgica*, 53(4), 57–83.

Heilmann, P., Saarenketo, S., & Liikkanen, K. (2013). Employer branding in power industry. *International Journal of Energy Sector Management*.

Hillebrandt, I., & Ivens, B. (2013). Scale Development in Employer Branding. Doi:10.1007/978-3-658-00427-9_4.

Holtom, B. C., & Inderrieden, E. J. (2006) "Integrating the unfolding model and job embeddedness model to better understand voluntary turnover," *Journal of Managerial Issues,* (18), 435-452.

Iglesias, A., & Sanchez, Z. (2015). Generalities of the organizational climate. *MediSur,* 13 (03), 445 - 457. Retrieved from http://www.redalyc.org/pdf/1800/180039699016.pdf (visitado em 08 de abril , 2022).

ISC², (2017). Study IT Professionals are a Critically Underutilized Resource for Cybersecurity. Retrieved from: https://www.isc2.org/-/media/Files/Research/IT-Professionals-are-a-

Critically-Underutilized-Resource-for-Cybersecurity.ashx?la=en&hash=D9DDB26BBA0F5513F590C3B7C0A71ECDA858FE1B (visitado em 05 de maio , 2022).

ISC², (2022). 2022 Workforce Study Retrieved from: https://www.isc2.org/-/media/2A313135414E400FA0DBD364FD74961F.ashx (visitado em 05 de setembro, 2022).

Ishmael, A., & Leila, H. (2022): Retention of Qualified Cybersecurity Professionals: A Qualitative Study, *Journal of Computer Information Systems*, Doi: 10.1080/08874417.2022.2049018

ISO/IEC. (2018) ISO/IEC 27000:2018 Retrieved from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en (visitado em 05 de setembro, 2022).

Iverson, R. D. & Zatzick, C. D. (2006). High-involvement management and workforce reduction: Competitive advantage or disadvantage? *Academy of Management Journal,* 49(5), 999–1015. Doi:10.5465/AMJ.2006.22798180

Jaimes, D. L. A., Estepa, J. M. S., & Uribe, A. F. (2017). Connection between internal marketing and organizational commitment in Colombian Technological Development Centers. *Estudios Gerenciales*, 33(142), 95-102.

Jayathilake, H.D., Daud, D., Eaw, H.C., & Annuar, N. (2021). Employee development and retention of Generation-Z employees in the post-COVID-19 workplace: a conceptual framework. *Benchmarking: An International Journal.*

Jimenez, A., & Aravena, V. (2015). Challenges of promoting personal strategies and incorporating work-family reconciliation policies in organizations. *Psychological Thought,* 13(02), 123 -135. Retrieved from http://www.redalyc.org/pdf/801/80143106009.pdf (visitado em 05 de setembro, 2022).

Jimenez, A., Pimentel, M., & Echeverria, M. (2010). Labor market: projections and business implications.

Joo, B., & Mclean, G. (2006). Best Employer Studies: A Conceptual Model from a Literature Review and a Case Study. *Human Resource Development Review*. 5. 228-257. Doi:10.1177/1534484306287515.

Kabir, S. M. S. (2016). Methods of data collection. Basic guidelines for research: an introductory approach for all disciplines, 1, 201-275.

Kamalaveni, M., Ramesh, S., & Vetrivel, T. (2019). A review of literature on employee retention. *Int. J. Innov. Res. Manag. Stud.* 4, 1–10.

Karatepe, O. M., Babakus, E., & Yavas, U. (2012). Affectivity and organizational politics as antecedents of burnout among frontline hotel employees. *International Journal of Hospitality Management*, 31(1), 66–75. Doi:10.1016/j.ijhm.2011.04.003

Kashyap, V., & Verma, N. (2018). Linking dimensions of employer branding and turnover intentions. *International Journal of Organizational Analysis*, 26(2), 282–295. Doi:10.1108/IJOA-03-2017-1134

Kori, K., Pedaste, M., Must, O. (2018). The Academic, Social, and Professional Integration Profiles of Information Technology Students. *ACM Transactions on Computing Education*. 18. 1-19. Doi:10.1145/3183343.

Kucherov, D., & Zamulin, A. (2016). Employer branding practices for young talents in IT companies (Russian experience). Human Resource Development International, 19(2), 178-188.

Laínez, J. (2016). El employer branding como generador del compromiso en la atracción y retención de talento, una revisión conceptual. Retrieved from: http://201.159.223.2/handle/123456789/1614 (visitado em 05 de setembro, 2022).

Lievens, F., & Slaughter, J. E. (2016). Employer Image and Employer Branding: What We Know and What We Need to Know. *Annual Review of Organizational Psychology and Organizational Behavior,* 3, 407–440. Doi:10.1146/annurev-orgpsych-041015- 062501

Mercer Marsh Benefits (2021) The Five Pillars of People Risk. Retrieved from: https://info.mercer.com/rs/521-DEV-513/images/uk-2021-mmb-the-five-pillars-of-people-risk-report.pdf (visitado em 20 de outubro , 2022).

Mitchell, T.R., Holtom, B.C., Lee, T.W., Sablynski, C.J., & Erez, M. (2001) Why people stay: Using organizational embeddedness to predict voluntary turnover. *Academy of Management Journal* (44:6), 1102-1122.

Moore, C., Detert, J. R., Treviño, L., Baker, L., & Mayer, D. (2012). Why Employees Do Bad Things: Moral Disengagement And Unethical Organizational Behavior. *Personnel Psychology* 65(1). Doi:2027.42/90243

Moroko, L. & Uncles, M. (2008). Characteristics of successful employer brands. *Journal of Brand Management.* 16. 160-175. Doi:10.1057/bm.2008.4.

Mukherjee, N., Zabala, A., & Huge, J. (2018). Comparison of techniques for eliciting views and judgements in decision-making, *Methods in Ecology and Evolution*, 9, 54–63.

Nayak, S. (2017). Antecedents to employer branding: A strategic focus on the information technology (IT) sector in India. *Polish Journal of Management Studies*. 15. 143-151. Doi: 10.17512/pjms.2017.15.2.13.

Nguyen, T. (2020). Determinants of Talent Retention in Textile and Garment Companies in Binh Duong Province. *Journal of Asian Finance, Economics and Business*, 7(6), 475– 484. Doi:10.13106/jafeb.2020.vol7.no6.475

Observatório de Cibersegurança (2022). Estudo sobre o ensino pós-secundário e o ensino superior de cibersegurança em Portugal. Retrieved from: https://www.cncs.gov.pt/docs/estudo-ensino-ciberseg-cncs.pdf (visitado em 05 de outubro , 2022).

Oltsik .J. (2017). The Life and Times of Cybersecurity Professionals, *ESG Senior Principal Analyst*, November 2017

Orye, E. & Faith-Ell, G. (2021). Cyber workforce recruitment and retention: an awareness assessment. Retrieved from: https://ccdcoe.org/uploads/2021/02/Workforce-Sep_20_v5.pdf (visitado em 05 de outubro , 2022).

Pflügler, C., Becker, N., Wiesche, M., & Krcmar, H. (2018). Strategies for retaining key IT professionals. *MIS Quarterly Executive*, 17(4), 297–314. Doi:10.17705/2msqe.00003

Prasad, A. & Tanwar, K. (2016). Exploring the Relationship between Employer Branding and Employee Retention. *Global Business Review*. 17. Doi:10.1177/0972150916631214.

Pretorius, H. W., Mawela, T., Strydom, I., Villiers, C., & Johnson, R. D. (2015). Continuing the discourse of women in Information Technology. *Gender, Technology & Development,* 19(3), 346. Doi:10.1177/0971852415597100

Rampl, L. V., Opitz, C., Welpe, I. M., & Kenning, P. (2016). The role of emotions in decision-making on employer brands: insights from functional magnetic resonance imaging (fMRI). *Marketing letters*, 27(2), 361-374.

Rodrigues Varela, José. (2021). Governo quer usar 130 milhões de euros dos fundos europeus para reforçar a cibersegurança em Portugal. Retrieved from: https://jornaleconomico.pt/noticias/para-nl-governo-quer-usar-130-milhoes-de-euros-dos-fundos-europeus-para-reforcar-ciberseguranca-em-portugal-702276 (visitado em 05 de julho , 2022).

Schlager, T., Bodderas, M., Maas, P. & Cachelin, J. (2011). The influence of the employer brand on employee attitudes relevant for service branding: An empirical investigation. *Journal of Services Marketing*. 25. 497-508. Doi:10.1108/08876041111173624.

Schmidt, G. B., Lelchook, A. M., & Martin, J. E. (2016). The Relationship Between Social Media Co-worker Connections and Work - Related Attitudes. *Computers in Human Behavior*, 55, 439–445. Doi:10.1016/j.chb.2015.09.045

Sehgal, K., & Malati, N. (2013). Employer branding: A potent organizational tool for enhancing competitive advantage. *IUP Journal of Brand Management*, 10(1), 51.

Shuck, M. B., Rocco, T. S., & Albornoz, C. A. (2011). Exploring employee engagement from the employee perspective: Implications for HRD. *Journal of European Industrial Training*.

Singh, D. (2019). A Literature Review on Employee Retention with Focus on Recent Trends. *International Journal of Scientific Research in Science and Technology (IJSRST)*, Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 6 Issue 1, pp. 425-431.

Singh, J. (2000). Performance productivity and quality of frontline employees in service organizations. *Journal of Marketing,* 64(2), 15–34.

Sokro, E. (2012). Impact of Employer Branding on Employee Attraction and Retention. *European Journal of Business and Management*, 164-173.

Sousa, B., Arriscado, P., Ferreira, P., & Quesado, H. (2017). The role of employer branding on attracting, developing and retaining talent: the case of a leading Portuguese business group. *Portuguese Marketing Magazine*, 19(36), 23 - 42.

Stan, E. (2012). The Role of Grades in Motivating Students to Learn. *Procedia - Social and Behavioral Sciences.* 69. 1998-2003. Doi:10.1016/j.sbspro.2012.12.156.

Stanca, L., Lacurezeanu, R., Bresfelean, V. P., & Pandelica, I. (2020). Determining IT Student Profile Using Data Mining and Social Network Analysis. *International journal of computers communications & control*. 15. Doi:10.15837/ijccc.2020.5.3897.

União Europeia. (2022) Flash Eurobarometer 496 SMEs and cybercrime Report 2021. Retrieved from: https://www.anacom.pt/Nyron/Library/catalogo/winlibsrch.aspx?skey=&cap=&pesq=5&thes0=954&dtype=mosaico&prn=true&doc=13720 (visitado em 05 de outubro , 2022).

Valderrama, B. (2019). Transformación digital y organizaciones ágiles. *Arandu utic*, 6(1), 15-50

Williams, L. V. (2013). Estudio diagnóstico de clima laboral en una dependencia pública. *Universidad Autónoma de Nuevo León*.

Younas, M. & Bari, M. (2020). The relationship between talent management practices and retention of generation 'Y' employees: mediating role of competency development. *Economic Research*. 33. 1330-1353. Doi:10.1080/1331677X.2020.1748510.

Anexos

Anexo A - Guião das Entrevistas de saturação

Nível de qualificação

Sexo

Idade

Qual a sua situação profissional?

Há quantos anos trabalha em cibersegurança?

Quantas vezes mudou de emprego desde que desempenha funções em cibersegurança?

O que o levou a integrar a sua empresa atual onde desempenha funções de cibersegurança?

Há quanto tempo está na sua empresa atual onde desempenha funções de cibersegurança?

Questões a realizar	Justificação das questões
O que o motiva face às outras áreas de tecnologias de informação para preferir trabalhar em cibersegurança?	Oltsik (2017) identifica o que levou os atuais profissionais de cibersegurança a entrarem para esta área em quase metade (47%) dos entrevistados ingressaram para cibersegurança face a outras áreas de tecnologias de informação para ter oportunidade para desenvolver as suas habilidades e curiosidades.
Que características deve ter uma empresa para que tenha interesse em trabalhar em cibersegurança na mesma?	Ishmael *et al*., 2022, 100% dos seus inquiridos afirmam que o principal fator para continuar ou mudar de organização é justamente a flexibilidade permitida pelo empregador. No mesmo estudo 94% dos inquiridos referem que se sentirem honrados e orgulhosos com o seu trabalho é o segundo maior fator de retenção de talento.
Os limites éticos da empresa em que está fazem-no sentir-se mais ou menos atraídos pela empresa?	Os comportamentos dentro das organizações causam diretamente danos diretos aos colaboradores (Moore *et al.,* 2012).

Os limites éticos implementados pela empresa impedem-no de desempenhar adequadamente as suas funções?	As empresas sofrem perdas anuais de US$ 2,9 trilhões como resultado de atividades fraudulentas (Moore *et al.,* 2012).
É contactado com que frequência com ofertas de emprego?	ISC² (2017) previa que o fosso entre o que as organizações precisam e o que o mercado de trabalho oferece iria aumentar estimando-se que 1,8 milhões de posições de profissionais de cibersegurança permaneceriam por preencher até 2022.
O que o estimula a continuar nesta empresa ao nível da cibersegurança?	A retenção de colaboradores é obviamente muito benéfica e importante, e as organizações estão, portanto, implementando várias estratégias de retenção de colaboradores (Jayathilake *et al.,* 2021) Pesquisas mostram que fatores importantes para a retenção de colaboradores são oportunidades de desenvolvimento, ambiente de trabalho, liderança, formação, *engagement* dos colaboradores, satisfação no trabalho entre outros (Kamalaveni *et.al,* 2019; Stan, 2012; Sokro, 2012).
O que o fez sair de cada empresa onde já desempenhou funções em cibersegurança?	Para ter uma retenção efetiva de colaboradores, é necessário conhecer as necessidades dos colaboradores para se adaptar a elas (Sokro, 2012). A visão, valores, estratégia e cultura da organização, são um fator crítico no engagement dos colaboradores (Mukherjee *et al.,* 2018)
Quais as condições cruciais que a sua empresa atual deve facultar para continuar a desempenhar as suas funções em cibersegurança?	O *employer branding* melhora o recrutamento, a retenção e o engagement dos colaboradores (Ainspan, *et al*., 2001; Moroko *et al*., 2008).
Quer continuar a desempenhar funções de cibersegurança na empresa atual?	O *employer branding* muda a identidade organizacional assim como a cultura organizacional que se reflete na fidelidade à organização (Barrow *et al*., 2005).

O que seria necessário existir noutra empresa para deixar aquela onde desempenha funções atualmente em cibersegurança?	Os resultados positivos do *employer branding* no *engagement* dos colaboradores são vistos através da satisfação dos mesmos, identificação com a organização (Schlager *et al.,* 2011). Algumas das práticas de atração que também foram marcadas como benéficas para a retenção são condições de trabalho como flexibilidade (no horário de trabalho, local e organização do trabalho), comunicação, políticas amigas da família, orientação para o bem-estar e benefícios (Beauregard *et al*., 2009; Iverson *et al*., 2006). O estudo de Döckel (2003) identificou alguns fatores de retenção como: remuneração, características do trabalho (variedade e autonomia), formação e oportunidades de desenvolvimento, suporte da liderança (reconhecimento e feedback), oportunidades de carreira, equilíbrio de vida pessoal e profissional. Os profissionais sentem-se atraídos por oportunidades de desenvolvimento profissional, desenvolvimento, formação (Kucherov *et al*., 2016; Prasad *et al*.,2016), juntamente com um ambiente de trabalho, equilíbrio entre vida profissional e pessoal (Prasad *et al*., 2016), feedback, reconhecimento pessoal e tarefas desafiadoras (Kucherov *et al*, 2016).

Anexo B – Resultados das Entrevistas de Saturação

Nível qualificação:

- 8 Licenciatura
- 1 Mestrado
- 3 Pós-graduação

Sexo:

- 12 indivíduos do sexo masculino

Idades:

- 2 indivíduos dos 45-54 anos
- 7 indivíduos dos 35-44 anos
- 3 indivíduos dos 25-34 anos

Qual a sua situação profissional?

- 12 indivíduos a trabalhar por conta de outrem e efetivos

Há quantos anos trabalha em cibersegurança?

- 2 indivíduos há mais de 20 anos
- 5 indivíduos há 4 anos
- 5 indivíduos há 15 anos

Quantas vezes mudou de emprego desde que desempenha funções em cibersegurança?

- 7 indivíduos mudaram 3 vezes
- 2 indivíduos mudaram 4 vezes
- 3 indivíduos mudaram 6 vezes

O que o levou a integrar a sua empresa atual onde desempenha funções de cibersegurança?

- 11 indivíduos referiram um projeto desafiador a par de um salário adequado e do suporte da equipa de gestão
- 1 indivíduo referiu começar um projeto de raiz

Há quanto tempo está na sua empresa atual onde desempenha funções de cibersegurança?

- 5 indivíduos referiram 1 ano e meio
- 1 indivíduo referiu 6 meses
- 6 indivíduos referiram 3 anos

O que o motiva face às outras áreas de tecnologias de informação para preferir trabalhar em cibersegurança?

- 12 indivíduos referiram paixão pela área, sendo que é das poucas áreas onde têm a possibilidade de estar em contacto com os avanços da tecnologia e ao mesmo tempo ter interação com as restantes áreas de tecnologias de informação

Que características deve ter uma empresa para que tenha interesse em trabalhar em cibersegurança na mesma?

- 5 indivíduos referiram suporte da equipa de gestão
- 7 indivíduos referiram flexibilidade, autonomia e suporte da equipa de gestão

Os limites éticos da empresa em que está fazem-no sentir-se mais ou menos atraídos pela empresa?

-12 indivíduos referiram sentir-se mais atraídos

Os limites éticos implementados pela empresa impedem-no de desempenhar adequadamente as suas funções?

- 12 indivíduos referiram que não

É contactado com que frequência com ofertas de emprego?

- 12 indivíduos referiram 3 a 4 vezes por semana

O que o estimula a continuar nesta empresa ao nível da cibersegurança?

- 5 indivíduos referiram aprendizagem contínua
- 7 indivíduos referiram que a gestão de topo compreende a importância da cibersegurança e desenvolve-o a par do negócio, o que os faz sentir valorizados.

O que o fez sair de cada empresa onde já desempenhou funções em cibersegurança?

- 7 indivíduos referiram o salário
- 3 indivíduos referiram que começou a ser algo muito rotineiro e sem possibilidade de se continuarem a desenvolver profissionalmente
- 2 indivíduos referiram a falta de suporte da equipa de gestão

Quais as condições cruciais que a sua empresa atual deve facultar para continuar a desempenhar as suas funções em cibersegurança?

- 10 indivíduos referiram a progressão do salário, as perspetivas de progressão de carreira e suporte das equipa de gestão
- 2 indivíduos referiram continuar a ter oportunidade de fazer formação nesta área pela empresa onde trabalho

Quer continuar a desempenhar funções de cibersegurança na empresa atual?

- 12 indivíduos referiram que sim

O que seria necessário existir noutra empresa para deixar aquela onde desempenha funções atualmente em cibersegurança?

- 12 indivíduos referiram um melhor kit salarial e um projeto que me permitisse evoluir mais a nível profissional

Anexo C – Guião do Questionário - *Employer Branding* nos profissionais de cibersegurança

O presente questionário insere-se no âmbito do mestrado em Gestão de Recursos Humanos e Consultadoria Organizacional, procurando estudar o *employer branding* nos profissionais de cibersegurança.

O preenchimento do questionário é de aproximadamente 5 a 10 minutos. Não existem respostas certas ou erradas sendo que as questões se tratam de opiniões e avaliações relativas a experiências pessoais.

Em nenhum momento é pedido ao participante que se identifique, sendo por isso a recolha de dados totalmente anónima, zelando pelo máximo de confidencialidade. O tratamento de dados será feito de modo agregado e nunca de forma individualizada.

Muito obrigada pela sua participação!
Andreia Nunes
Para questões relacionadas com a participação contacte: asnsa@iscte-iul.pt

QUESTÃO	**ESCALA**
Aceita participar neste estudo?	Sim
	Não

QUESTÃO	**ESCALA**
É profissional de cibersegurança?	Sim
	Não

QUESTÃO	**ESCALA**
Nível de Qualificações	2º Ciclo do Ensino Básico
	3º Ciclo do Ensino Básico
	Ensino Secundário via Ensino
	Ensino Secundário via Profissional
	Ensino Técnico-Profissional

	Licenciatura
	Mestrado
	Doutoramento

QUESTÃO	**ESCALA**
Sexo	Masculino
	Feminino
	Prefiro não divulgar

Idade (campo aberto)

QUESTÃO	**ESCALA**
Situação Profissional	Desempregado
	Trabalhador por conta própria
	Trabalhador por conta outrem, a prazo
	Trabalhador por conta outrem, efetivo

QUESTÃO	**ESCALA**
Quantos anos tem de experiência profissional em cibersegurança?	Até 2 anos
	Entre 2 anos e 5 anos
	Entre 6 anos e 9 anos
	Entre 10 anos e 14 anos
	Entre 15 anos e 19 anos
	Entre 20 anos e 24 anos
	Mais de 25 anos

QUESTÃO	**ESCALA**
Quantas vezes mudou de emprego desde que desempenha funções em cibersegurança?	Entre 1 e 2 vezes
	Entre 3 e 4 vezes
	Entre 5 e 6 vezes

	Entre 7 e 8 vezes
	Mais de 8 vezes

Qual a sua antiguidade na empresa atual onde desempenha funções de cibersegurança?	Entre 1 mês e 1 ano
	Entre 1 ano e 2 anos
	Entre 3 anos e 4 anos
	Entre 5 anos e 6 anos
	Entre 7 anos e 8 anos
	Mais de 9 anos

Atração:

Avalie de "1 - Sem importância; 2 -Pouco importante; 3 - Razoavelmente importante; 4- Importante; 5 - Muito importante" os fatores que influenciam para uma nova mudança de empresa onde desempenha funções de cibersegurança:

QUESTÃO	**ESCALA**
Salário acima do valor médio praticado na empresa	1-Sem importância
Suporte da Equipa de Gestão	2-Pouco importante
Projeto Aliciante e Desafiador	3-Razoavelmente importante
Projeto começado de Raiz	4-Importante
Projeto que o fizesse evoluir mais profissionalmente	5-Muito importante
Flexibilidade	
Progressão de Carreira	
Limites éticos impostos pela potencial empresa	
Funções rotineiras na empresa atual	

Motivação:

Avalie de "1 - Sem importância; 2 -Pouco importante; 3 - Razoavelmente importante; 4- Importante; 5 - Muito importante" os fatores que tem em conta face às outras áreas de IT para preferir trabalhar em cibersegurança:

QUESTÃO	**ESCALA**
Paixão	1-Sem importância
Possibilidade de estar em contacto com os avanços tecnológicos	2-Pouco importante
Integração possível com as restantes áreas de tecnologias de informação	3-Razoavelmente importante
Aprendizagem contínua	4-Importante
Gestão de topo compreende a importância de cibersegurança	5-Muito importante
Gestão de topo desenvolver cibersegurança a par com o negócio	
Valorização do seu conhecimento	

Retenção:

Avalie de "1 - Sem importância; 2 -Pouco importante; 3 - Razoavelmente importante; 4- Importante; 5 - Muito importante" os fatores que tem em conta para continuar na empresa onde desempenha funções de cibersegurança:

QUESTÃO	**ESCALA**
Progressão de Carreira	1-Sem importância
Suporte da Equipa de Gestão	2-Pouco importante
Progressão Salarial	3-Razoavelmente importante
Oportunidades de Formação pela Empresa	4-Importante
	5-Muito importante

Assinale a resposta que melhor descreve a sua atitude relativamente à organização onde trabalha. Escala de Integração (*job embeddedness)* no Trabalho (Crossley *et al.,* 2007)

QUESTÃO	**ESCALA**
Sinto-me ligado/a a esta organização.	1-Discordo totalmente

Seria para mim difícil deixar esta organização.	2-Discordo
Estou demasiado envolvido/a nesta organização para a deixar.	3-Não concordo nem discordo
Sinto-me vinculado/a a esta organização.	4-Concordo
Simplesmente não conseguiria deixar a organização onde trabalho.	5-Concordo totalmente
Seria muito fácil para mim deixar esta organização.	
Estou intimamente ligado/a a esta organização.	

Obrigada pela sua participação.